Politechnika Warszawska
Wydział Elektroniki i Technik Informacyjnych

DZIEKAN I RADA WYDZIAŁU ELEKTRONIKI I TECHNIK INFORMACYJNYCH POLITECHNIKI WARSZAWSKIEJ

zawiadamiają o

PUBLICZNEJ OBRONIE ROZPRAWY DOKTORSKIEJ

mgr. Fahada Naima Nife

która odbędzie się w trybie zdalnym w dniu 28 września 2020 r. o godz. 12.00

Tytuł rozprawy doktorskiej: **„New Security Management Scheme for Software-Defined-Networks (SDN)"**

promotor: prof. dr hab. inż. Zbigniew Kotulski, Wydział Elektroniki i Technik Informacyjnych Politechniki Warszawskiej

recenzenci: dr hab. Bogdan Księżopolski, prof. uczelni, Uniwersytet Marii Curie-Skłodowskiej w Lublinie

dr hab. inż. Tomasz Hyla, prof. uczelni , Zachodniopomorski Uniwersytet Technologiczny w Szczecinie.

Na stronie internetowej wydziału www.elka.pw.edu.pl/Wydzial/Rada-Wydzialu/Harmonogram-obron-doktorskich-streszczenia-i-recenzje znajdują się streszczenie rozprawy oraz recenzje, jak również dostęp do tekstu rozprawy umieszczonej w Bazie Wiedzy Politechniki Warszawskiej.

Sposób uczestniczenia w publicznej obronie:

Link do obrony na platformie Microsoft Teams:

https://teams.microsoft.com/l/meetup-join/19%3ad2fadaf305d741cc8b993bd81a593b5e%40thread.tacv2/1599651605997?context=%7b%22Tid%22%3a%223b50229c-cd78-4588-9bcf-97b7629e2f0f%22%2c%22Oid%22%3a%22d9b080c1-9d77-4456-a821-ca7decf4be4e%22%7d

Dziekan

prof. dr hab. inż. Michał Malinowski

Rodzaj pracy: rozprawa doktorska

Mgr Fahad Naim Nife

Promotor – prof. dr hab. inż. Zbigniew Kotulski Wydział Elektroniki i Technik Informacyjnych Politechniki Warszawskiej

Tytuł rozprawy doktorskiej:" *New Security Management Scheme for Software-Defined-Networks (SDN)*

Abstract

Software-defined Networking (SDN) is new network architecture which promises to redefine the future of networking in terms of how the network are build, managed, and operated. The SDN architecture is a revolutionary new idea that, moving the traditional network to be software-based, makes it to offer more flexibility, high degree of automation and shorter provision time.

In fact, SDN comes up with many great capabilities for the network, such as a highly scalable centralized control, flow-based, directly programmable, and dynamically configured, with dynamic updating of forwarding rules and network openness. On the one hand, greater reliance on software, direct programming capability, and centralized logical network intelligence of the SDN-based network can support rapid updating and provide different ways and opportunities to enhance and protect the network. On the other hand, these features bring new vulnerabilities related to security, scalability, and flexibility. Furthermore, the primary design of the SDN architecture does not sufficiently take into account security requirements, what makes security issues a real challenge.

Thus, it is essential to build a robust security mechanism to protect the network from internal and external malicious activities, while respecting the objective of the SDN network. In this thesis, we construct a security system integrated with the central Controller, which is easy to manage, and which significantly improves the required security for the SDN-based network. Our system deals with many security challenges in SDNs. It combines a set of solutions rather than solving just one security issue. We build a modular security management system for OpenFlow/SDN-based network. It consists of several modules. Each module provides a specific security service (e.g., access control, firewall, and violation detection).

First, we propose an SDN-based access control system that allows network operators to implement the security policies required to verify the identity of a host upon connection to the network. It is defined to deny the access from unauthorized hosts and to specify different levels of privileges for each host, according to the provided authentication credentials. Second, the Firewall module is a state-aware, application-aware solution, which performs a deep packet inspection to protect data transmission. It presents a distributed stateful firewall solution in which the security policy is reactively enforced by an application running on the top of the Controller. Third, the violation detection module leverages the Controller's global visibility to detect and resolve direct and indirect flow violations in the OpenFlow environment. It employs two conflict detection techniques. The first method is based on periodic polls of the Flow Table data. The

second mechanism is presented as a layer between the application plane and the data plane. Both approaches utilize the directed graph to simplify tracking the forwarding rule paths. The combination of these systems (modules) helps creation of additional boundaries within the network to provide multi-levels of defense to protect the network from external attacks as well as from internal malicious users.

For our systems, the network security policy will be centralized in the Controller, where there is the place of making a decision regarding how the switches should handle the packets, while a switch will only enforce this decision. The Controller can, at any time, reconfigure the security rules and redeploy them at any device under its control. Thus, we have more efficient, flexible and centralized point of security management represented by the Controller, which in turn spreads the network security policy dynamically across the distributed checkpoints.

UNIWERSYTET MARII CURIE-SKŁODOWSKIEJ W LUBLINIE
Wydział Matematyki, Fizyki i Informatyki

dr hab. Bogdan Księżopolski, prof. uczelni | Kierownik Katedry Cyberbezpieczeństwa

Lublin, 4.08.2020 r.

Recenzja rozprawy doktorskiej

Tytuł : New Security Management Scheme for Software-Defined-Networks (SDN)

Autor: MSc Fahad Naim Nife

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

Rozprawa doktorska dotyczy utworzenie systemu pozwalającego zwiększyć bezpieczeństwo sieci sterowanych programowo (SDN). Sieci sterowane programowo są stosunkowo nowym rozwiązaniem, które pozwalają zarządzać sieciami komputerowymi w sposób scentralizowany przy pomocy kontrolera. Kontroler jest odpowiedzialny za podejmowanie decyzji o przekazywaniu danych w całej sieci, podczas gdy przełączniki i routery wykonują tylko podstawowe przekazywanie pakietów. Kontrolery mają pełny widok sieci i przed podjęciem jakiejkolwiek decyzji uwzględniają jej globalny stan. Zastosowanie sieci SDN pozwala zwiększyć elastyczność oraz automatyzację zarządzania sieciami. Szczególnie istotnym dzisiaj problemem jest zapewnienie odpowiedniego poziomu ochrony dla kontrolera działającego w ramach sieci sterowanych programowo.

Autor postawił następującą tezę badawczą: **Możliwe jest zbudowanie systemu bezpieczeństwa zintegrowanego z kontrolerem centralnym, łatwego w zarządzaniu, który znacząco poprawia wymagane bezpieczeństwo dla sieci opartej na SDN**.

W celu potwierdzenia postawionej tezy określono siedem głównych zadań badawczych.

1. Utworzenie modułowego system zarządzania bezpieczeństwem dla sieci OpenFlow / SDN.

2. Utworzenie i implementacja modułu kontroli dostępu w celu zapobiegania wszelkim próbom dostępu ze strony nieautoryzowanych użytkowników poprzez weryfikację tożsamości hosta po podłączeniu do sieci.
3. Utworzenie modułu zapory sieciowej, działającej w sposób stanowy, w którym polityka bezpieczeństwa jest scentralizowana w aplikacji zapory.
4. Utworzenie modułu zapory przeznaczonego do wykrywania w oparciu o klasyfikację ruchu i głęboką inspekcję pakietów.
5. Utworzenie systemu zapewniającego głęboką inspekcję pakietów, pozwalającą sprawdzać pierwsze N pakietów przepływu w kontrolerze SDN.
6. Utworzenie struktury drzewa hash używanej do przechowywania reguł bezpieczeństwa, a nie listy linii.
7. Utworzenie modułu wykrywania naruszeń zasad zapory sieciowej poprzez sprawdzanie ścieżki przepływu względem polityki zapory sieciowej.

Postawiona teza została sformułowana poprawnie, a jej wykazanie implikowało konieczność rozwiązania sformułowanych zadań badawczych oraz implementacji stosowych rozwiązań o stopniu złożoności adekwatnym do oczekiwanego poziomu prac doktorskich.

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

Analiza źródeł została zawarta w rozdziale 2 oraz 9 rozprawy. W rozdziale 2 Autor wprowadził w tematykę sieci sterowanych programowo. Ta część ma charakter wprowadzenia w tematykę poruszoną w rozprawie. W tym rozdziale została przedstawiona koncepcja sieci SDN wraz z omówieniem architektury oraz omówieniem poszczególnych elementów wchodzących w jej skład. W rozdziale 9 przedstawiono przegląd literatury naukowej i bieżących tematów badawczych dotyczących sieci sterowanych programowo.

Zaprezentowany tam stan wiedzy prezentuje kolejno istotne zagadnienia dotyczące zadań badawczych określonych w rozprawie. Zagadnienia te dotyczą: kontroli dostępu do sieci w ramach sieci SDN, zapory sieciowej w ramach sieci SDN, wykrywania naruszeń zasad w ramach sieci SDN.

Przedłożona rozprawa doktorska obejmuje 220 pozycji bibliograficznych, które reprezentują poruszaną tematykę. Jest ona uporządkowana w kolejności alfabetycznej. Szczególnie wartościowe jest przedstawienie trzech zestawień przedstawiających zaproponowane przez Autora rozwiązania w porównaniu z innymi podejściami określonymi w literaturze (Tabele: 9.2, 9.3, 9.4). Takie zestawienia w sposób jasny i przekonywujący charakteryzują poszczególne rozwiązania zaproponowane w rozprawie.

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

W mojej ocenie postawiony w pracy problem utworzenia systemu bezpieczeństwa zintegrowanego z kontrolerem centralnym, łatwego w zarządzaniu, który znacząco poprawia wymagane bezpieczeństwo dla sieci opartej na SDN, został rozwiązany. Zaproponowane rozwiązanie polegało na przygotowaniu architektury systemu zarządzania bezpieczeństwa dla sieci opartej na technologii OpenFlow / SDN. Zaproponowane rozwiązanie składa się z kilku modułów, ale wśród nich można wyróżnić 3 główne: moduł kontroli dostępu do sieci, moduł zapory sieciowej oraz moduł wykrywania naruszeń.

Moduł kontroli dostępu do sieci SDN został oparty o dobrze znaną technologię IEEE 802.1x, która zapewnia kontrolę dostępu w oparciu o porty. Zaproponowano zostały dwa alternatywne podejścia, które różnią się od lokalizacji strony uwierzytelniającej. Proponowane rozwiązanie nie jest nowym rozwiązaniem, a raczej rozwiązaniem, które wykorzystuje już istniejące standardy. Moim zdaniem, takie podejście do problemu jest uzasadnione, ponieważ warto wykorzystywać powszechnie stosowane i sprawdzone rozwiązania, dzięki czemu zwiększamy możliwość ich zastosowania w praktyce. Potwierdzenie takiej rekomendacji można znaleźć np. w raporcie technicznym wydanym przez Open Network Foundation (ONF) w dokumencie ONF TR-511, która zaleca budowanie rozwiązań zabezpieczających dla SDN w oparciu o starsze otwarte standardy. Należy przyjąć sprawdzone protokoły i metodologie zamiast opracowywać lub projektować nowe, które powinny być proponowane jako ostatnie rozwiązanie, gdy nie można spełnić istniejących wymagań.

Moduł zapory sieciowej został zaprojektowany tak, żeby mógł śledzić globalny stan połączenia, wykonywać szczegółową inspekcję pakietów, wykonywać klasyfikację usług sieciowych oraz

dynamicznie tworzyć reguł dla zapory. Architektura zapory ogniowej została przedstawiona na rysunku 7.4, w jej skład wchodzi 5 jednostek głównych.

A. Tree-Rule Policy
B. Firewall Main Function (FMF)
C. Application-Aware Function (AAF)
D. Deep Packet Inspection Function (DPIF)
E. Global State Hashing Table

Przedstawione rozwiązanie ma charakter rozproszony, która analizuje stan połączenia, w którym polityka bezpieczeństwa jest reaktywnie wymuszana przez aplikację działającą na górze kontrolera. Moim zdaniem takie podejście jest odpowiednie dla sieci sterowanych programowo.

Moduł wykrywania naruszeń zakłada 3 etapy działania (rysunek 8.1, 8.2): zbieranie reguł przepływu (odpytywanie / przechwytywanie), wykrywanie naruszeń i reakcja na naruszenia. Dzięki zastosowaniu sieci sterowanych programowo, można wykorzystać fakt, że kontroler ma aktualny obraz topologii sieci generowany przez kreator wykresów topologii sieci, dzięki czemu idealnie nadaje się do wykrywania i rozwiązywania bezpośrednich i pośrednich naruszeń przepływu w środowisku OpenFlow. Zaproponowane rozwiązanie wykonuje okresowe przeglądy danych zawartych w ramach Flow Table. Tabele przepływów wysyłane są okresowo do kontrolera, dzięki czemu może on zobaczyć globalne informacje o przepływie. Głównym wyzwaniem jest utworzenie systemu, który będzie mógł reagować w czasie rzeczywistym. W tym celu zaproponowano rozwiązanie, które w czasie rzeczywistym przechwytuje wszystkie komunikaty dotyczące wstawiania / usuwania reguł wysyłane przez aplikację i weryfikuje je, zanim dotrą do sieci. Jednak ta metoda zapewnia dodatkowy czas przetwarzania dla każdego dodawania / modyfikowania wiadomości, która następnie powoduje spowolnienie działania sieci i zwiększenie opóźnień.

W celu weryfikacji stworzonego systemu zostało opracowane środowisko testowe, które składa się z dwóch głównych elementów.

- Funkcjonalność przełącznika z obsługą OpenFlow na poziomie L2 / L3 – System Ubuntu Desktop 18.04 LTS.
- Emulator sieci SDN - Mininet Network w celu utworzenia Open vSwitch (OVS).

Autor opracował system wraz ze skryptami napisanym w języku Python, który pozwala połączyć poszczególne elementy architektury w celu zilustrowania działania systemu. W celu weryfikacji rozwiązania wykonano 6 zestawów testów.

1. Walidacja rozwiązania kontroli dostępu.
2. Walidacja funkcji inspekcji stanowej.
3. Walidacja globalnej tabeli skrótów stanu.
4. Walidacja rozwiązania obsługującego aplikacje.
5. Walidacja rozwiązania do głębokiej inspekcji pakietów.
6. Walidacja rozwiązania do wykrywania naruszeń.

Proces walidacji został bardzo dobrze opisany w rozdziale 10, w którym przedstawiono szczegóły implementacji oraz weryfikacji zaproponowanych modułów. Wykonane symulacje potwierdzają postawioną w rozprawie doktorskiej tezę. Biorąc pod uwagę powyższe, uważam, że Autor wykorzystał odpowiednie metody badawcze.

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

Najważniejszym oryginalnym osiągnięciem Autora jest opracowanie systemu bezpieczeństwa dla sieci SDN dotyczącego 3 głównych aspektów bezpieczeństwa: kontroli dostępu, zapory sieciowej oraz systemu wykrywanie naruszeń.

Moduł kontroli dostępu do sieci SDN został oparty o dobrze znaną technologię IEEE 802.1x. W literaturze rozwiązania dotyczące uwierzytelniania bazują głównie na adresach MAC, aplikacjach Web lub również na standardzie IEEE 802.1X. W tym przypadku warto porównać proponowane rozwiązanie z tymi, które wykorzystują standard IEEE 802.1X, czyli: AuthFlow, FlowNAC, czy FlowIdentity. Moim zdaniem zaproponowane rozwiązanie ma dwie główne przewagi. Pierwsza z nich dotyczy oparcie systemu o protokoły, które są w podstawowym zestawie standardu, dzięki czemu zaproponowane podejście nie wymaga żadnych dodatkowych protokołów pomocniczych ani nie wymaga nowej enkapsulacji. Dzięki temu zmniejsza się złożoność systemu oraz zmniejsza

potencjalne dodatkowe obciążenia. Kolejną różnicą jest miejsce, w którym znajduje się serwer Authenticator i Authentication. W literaturze serwer uwierzytelniający jest zintegrowany z Kontrolerem, co może prowadzić do zwiększenia obciążenia Kontrolera i narazić rozwiązanie na ataki na dostępność Kontrolera, np. DDoS, które może zarządzanie siecią SDN. Zaproponowana architektura zakłada umiejscowienie serwera jako oddzielnego obiektu, co pozwala ochronić Kontroler od wspomnianych ataków oraz niepożądanego dostępu.

Głównym wkładem Autora w ramach utworzonego moduł zapory ogniowej jest utworzenie zapory jako aplikacji działającej w warstwie nad kontrolerem. Kosztem takiego podejścia jest obniżenie wydajności, ale pozwala mieć wgląd w globalny stan sieci, który zapewnia większe bezpieczeństwo całej sieci. Aktualnie proponowane rozwiązania wykorzystują podejście lokalne, gdzie każdy przełącznik utrzymuje lokalny stan aktywnych przepływów. Ze względu na brak zaangażowania kontrolera metoda ta ma dobrą wydajność i wysoką dostępność. Jednak reguły oparte na przepływie powinny zostać z wyprzedzeniem wypełnione stanową zaporą ogniową (przełącznikami) we wszystkich przychodzących strumieniach. Takie podejście wymaga wcześniejszej wiedzy o wszystkich zdarzeniach w sieci oraz o tym, jak sobie z nimi radzić.

Innym oryginalnym rezultatem jest zaproponowanie metody wykrywania konfliktów w ramach stosowanych reguł na aktywnych urządzeniach sieciowych. W literaturze wykrywanie naruszeń reguł przepływu wykonywane jest przez przechwycenie reguł przepływu, zanim dotrze do data plane. Mechanizmy te zapewniają dokładne wykrywanie naruszeń zasad w czasie rzeczywistym, niestety wykonywane to jest kosztem dodatkowego czas przetwarzania wymaganego na śledzenie nowych reguł przepływu z aktualnie aktywnymi zasadami przepływu. Zaproponowana metoda wykorzystuje globalny widok kontrolera, aby uzyskać obraz sieci reprezentującego całą topologię sieci. Obraz całej sieci (topologia) służy do śledzenia reguł przepływu i wykrywania bezpośrednich lub pośrednich naruszeń dotyczących reguł przepływu realizowanych w ramach sieci sterowanej programowo.

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

Praca została napisana w języku angielskim. Język jest na bardzo dobrym poziomie, nie zauważyłem większych problemów językowych. Praca została zredagowana w sposób bardzo dobry. Autor

wykazał się umiejętnością poprawnego i przekonywującego przedstawienia uzyskanych przez siebie wyników. Zaproponowana architektura oraz moduły zostały doskonale oraz licznie zilustrowane odpowiednimi grafikami, schematami, tabelami oraz przykładami. Moim zdaniem poziom redakcyjny rozprawy doktorskiej jest na bardzo wysokim poziomie.

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

Przedstawione wyniki przez Autora mają duży aspekt praktyczny, inżynierski, co w moim odczuciu jest zaletą pracy. Przy pracach o charakterze praktycznym warto zadbać o weryfikację zaproponowanego system w środowisku rzeczywistym. Według mnie pewnym minusem pracy jest fakt, że weryfikacja zaproponowanego systemu została wykonana wyłącznie w emulatorze sieci SDN Mininet. Oczywiście wykorzystanie środowiska Mininet pozwoliło przeprowadzić Autorowi eksperymenty, które zweryfikowały postawione tezy, ale przeprowadzanie analizy w ramach realnej sieci SDN, pozwoliłoby uzyskać dodatkowe wymiary analizy, co mogłoby zaprowadzić do interesujących wniosków badawczych. Myślę, że warto w przyszłości przeprowadzić analizę utworzonych modułów w realnym środowisku sieci sterowanej programowo. Dodatkowo weryfikacje rozwiązania w środowisku zbliżonym do rzeczywistego, pozwoliłby przesunąć poziom gotowości technologicznej rozwiązania (TRL) z poziomu TRL 4 (Przeprowadzono walidację technologii w warunkach laboratoryjnych) na bardzo wysoki poziom TRL 5 (Dokonano walidacji technologii w środowisku zbliżonym do rzeczywistego) lub TRL 6 (Dokonano demonstracji technologii w środowisku zbliżonym do rzeczywistego). Nie mniej jednak uważam, że osiągniecie poziomu TRL 4 jest również bardzo dobry rezultatem w ramach pracy doktorskiej.

7. Jaka jest przydatność rozprawy dla nauk technicznych?

Przydatność uzyskanych wyników w naukach technicznych oceniam wysoko. Zaproponowany system bezpieczeństwa zintegrowany z kontrolerem centralnym dla sieci opartej na SDN dotyczy aktualnego problemu zarządzania sieciami komputerowymi. Warte podkreślenia jest, że Autor w ramach rozprawy doktorskiej przedstawił rozwiązanie wraz z jej realizacją praktyczną, której gotowość technologiczną rozwiązania oceniam na poziom - TRL 4 (Przeprowadzono walidację technologii w warunkach laboratoryjnych). Myślę, że komercjalizacją zaproponowanego rozwiązania mogą być zainteresowani operatorzy sieci komputerowych.

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.**

Uważam, że rozprawa doktorska magistra Fahada Naim Nife spełnia wymogi stawiane rozprawom doktorskim przez obowiązujące przepisy. Należy podkreślić, że część wyników rozprawy została już opublikowana w literaturze międzynarodowej, a w szczególności w czasopiśmie Journal of Network and Systems Management indeksowanym w JCR.

Szczecin, dn. 23 czerwca 2020 r.

dr hab. inż. Tomasz Hyla, prof. ZUT
Katedra Inżynierii Oprogramowania
Wydział Informatyki
Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

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

Tytuł rozprawy: New Security Management Scheme for Software-Defined-Networks (SDN)

Autor rozprawy: mgr Fahad Naim Nife

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)?**

   Przedmiotem recenzowanej rozprawy doktorskiej są mechanizmy zabezpieczeń dla sieci zdefiniowanych programowano (SDN, ang. Software Defined Networks). Koncepcja SDN pojawiła się około 10 lat temu w celu umożliwienia lepszej kontroli nad sieciami komputerowymi. W przeciwieństwie do tradycyjnych sieci komputerowych, w SDN urządzenia sieciowe zajmują się tylko przekazywaniem pakietów według zasad określonych przez centralny kontroler. Kontroler zna stan całej sieci i może ją dynamicznie rekonfigurować w zależności od potrzeb, np. w celu nadania wyższego priorytetu pakietom pochodzącym od konkretnej aplikacji. Znajomość stanu całej sieci i możliwość jej dynamicznej rekonfiguracji daje też potencjalnie większe możliwości z zakresu bezpieczeństwa sieci. SDN są w pewnym sensie ewolucją systemów zarządzania sieciami, jako że w tradycyjnych sieciach używa się także oprogramowania do zdalnego monitorowania i konfiguracji urządzeń. Jednak nie pozwala ono na tak szeroką i automatycznej konfigurację sieci. SDN udostępnia szerokie możliwości z zakresu zarządzania bezpieczeństwem, ale jednocześnie powoduje powstanie nowych zagrożeń np. udany atak na kontroler umożliwia przejecie całkowitej kontroli nad siecią.

Mechanizmy zabezpieczeń projektowane dla sieci SDN muszą uwzględniać również aspekty wydajnościowe, gdyż przy wielu urządzeniach sieciowych i dużym ruchu dosyć łatwo można przeciążyć kontroler sieci. Mechanizmy te są też dużo bardziej złożone, gdyż biorą pod uwagę widok całej sieci, a nie tylko jednego punktu. Autor w rozprawie zajmuje się zagadnieniem bezpieczeństwa sieci SDN.

Rozprawa doktorska ma charakter teoretyczno-doświadczalny. Jej rezultaty mają duże znaczenie praktyczne w projektowaniu mechanizmów zabezpieczeń, a w szczególności zapór ogniowych dla sieci SDN.

W rozprawie sformułowano następującą tezę: *It is possible to construct a security system integrated with the central Controller, which is easy to manage, and which significantly improves the required security for the SDN-based network.* W uzasadnieniu do tezy autor wyznaczył siedem zadań do wykonania, tj. budowę: modularnego systemu zarządzania dla sieci SDN, modułu kontroli dostępu, rozproszonej zapory ogniowej z pamięcią stanu, modułu rozszerzającego zaporę ogniową o badania pakietów na poziomie aplikacji, systemu ochrony bazującego na metodach wykrywania intruzów, struktury drzewiastej do przechowywania zasad bezpieczeństwa oraz modułu detekcji naruszeń (wykrywającego sytuację gdy np. dynamiczna rekonfiguracja trasowania w celu polepszenia jakości spowoduje ominięcie reguł zapór ogniowych). Rezultatem wykonania wszystkich zadań jest system ochrony dla sieci SDN. Autor przed sformułowaniem tezy wymienia cztery wyzwania technologiczne, które zamierza rozwiązać.

Pewną wadą takiego sformułowania tezy jest brak precyzyjnego zdefiniowania sformułowania „łatwości zarządzania" (*easy to manage*). Domyślnie można przyjąć, że dotyczy to zarządzania z jednego punktu, ale nie wiadomo jak skomplikowany będzie interfejs do zarządzania proponowanym system i czy np. „łatwość zarządzania" znaczy, że systemem będą mogły zarządzać osoby bez przeszkolenia z działania systemu. Drugim pojęciem niezdefiniowanym wprost w objaśnieniach do tezy jest „znaczna poprawa wymaganego bezpieczeństwa" (*significantly improves the required security*). Autor wymienia komponenty mające wchodzić w skład proponowanego systemu i domyślnie, z lektury całej rozprawy, można przyjąć, że pojęcie to jest rozumiane jako wzmocnienie bezpieczeństwa poprzez zaoferowanie właściwości niedostępnych dotąd w sieciach SDN. Jednak w opisie brakuje konkretnych definicji właściwości bezpieczeństwa jakie system ma osiągnąć, czy kategorii lub grup ataków jakim ma zapobiec, co utrudnia odbiór rozprawy. W tezie lub jej opisie brakuje także wprost informacji o zakładanych parametrach dotyczących wydajności i skalowalność, jako że rozprawa zawiera szereg eksperymentów potwierdzających te cechy. Podsumowując, na podstawie lektury całej rozprawy można uznać, że teza pracy została sformułowana dostatecznie jasno.

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?**

Recenzowana rozprawa doktorska została przygotowana w języku angielskim. Na jej zawartość składa się jedenaście rozdziałów, streszczenie (w języku angielskim i polskim), spisy akronimów, rysunków i tabel oraz obszerna bibliografia obejmująca 220 pozycji literaturowych. Całość pracy obejmuje 186 stron. Wynik własne doktoranta są przedstawione w rozdziałach 5, 6, 7, 8 oraz 10 i 11.

Analiza prac pokrewnych została przedstawiona przez autora w sposób wyczerpujący w rozdziale 9. Analiza źródeł obejmuje cztery główne tematy: (1) ogólną wiedzę na temat sieci SDN, (2) mechanizmy uwierzytelniania stosowane w kontroli dostępu w sieciach SDN, (3) zapory ogniowe dla sieci SDN, (4) mechanizmy detekcji naruszeń polityk w sieciach SDN. Obszary te odpowiadają zakresowi proponowanego systemu bezpieczeństwa dla sieci SDN. Dla każdego z zakresów (2)-(4) została zamieszczona tabela zawierająca porównanie cech rozwiązań zawartych w pozycjach literaturowych z proponowanym rozwiązaniem. W tekście zamieszczono także informację opisową o nowych elementach w stosunku do istniejących rozwiązań.

Pewną wadą w strukturze pracy jest zamieszczenie różnic w stosunku do istniejących rozwiązań w rozdziale 9 zamiast częściowo na początku rozprawy. Taka struktura utrudnia ocenę czytelnikowi co jest nowego w proponowanych rozwiązaniach. Jest to szczególnie istotnie, że istnieją moduły/rozwiązania mające podobne cechy do tych jakie proponuje autor i które są omówione w rozdziale 9.

Rozległość przywoływanej literatury oraz omawianych na jej podstawie zagadnień świadczy o dobrej, pogłębionej wiedzy autora na temat systemów zabezpieczeń dla sieci SDN. Zaletą przeprowadzonej analizy jest również uwzględnienie pozycji literaturowych z lat 2018-2020, a więc tych które zostały opublikowane już po rozpoczęciu prac przez autora. Wnioski z przeprowadzonej analizy przeprowadzono w sposób w miarę jasny i przekonywujący. Pewnym brakiem w analizie rozwiązań pokrewnych jest brak zestawienia ich wydajności i skalowalności.

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

W rozprawie autor wykorzystał metodologię nauki o projektowaniu (*design science methodology*) choć nie jest ona wymieniona wprost z nazwy. W tej metodologii proponowany jest artefakt, który później ewaluuje się według określonych kryteriów. Artefakt musi rozwiązywać nowe problemy lub musi rozwiązywać istniejące problemy w sposób bardziej efektywny. Metodologia ta jest popularna i często stosowana w informatyce. Układ poszczególnych rozdziałów jest zasadniczo zgodny z tą metodologią, a więc należy uznać, że autor użył właściwej metody.

Autor na początku pracy opisuje wyzwania technologiczne na tle istniejących rozwiązań w zakresie sieci SDN. W opisach brakuje krótkiego odniesienia do tradycyjnych sieci komputerowych i sposobu rozwiązania problemów z zakresu bezpieczeństwa, które poruszane są w rozprawie. W tym brakuje informacji, czy pod względem bezpieczeństwa w sieciach SDN można osiągnąć wyższy poziom bezpieczeństwa niż w tradycyjnych sieciach komputerowych. Intersujące jest też zagadnienie od jakiego rozmiaru sieci (liczby urządzeń sieciowych) lepiej jest stosować SDN/OpenFlow.

Podsumowując, wyzwania technologicznie są poprawnie sformułowane na tle sieci SDN, a w szerszym kontekście brakuje uzasadnienia wyzwania technologicznego na tle tradycyjnych sieci komputerowych. W opisie zagadnienia 4 wymieniona jest informacja, że nowe reguły (do zapory ogniowej) może w tradycyjnych sieciach dodawać tylko administrator, gdzie obecnie systemy wykrywania intruzów są w stanie same automatycznie dodawać reguły do zapór ogniowych. Wyzwania są poprawnie sformułowane przy założeniu, że sieci SDN stosujemy w celu zwiększenia wydajności/jakości i wymagane są odpowiednie mechanizmy bezpieczeństwa, a nie wprowadzamy sieci SDN dla samych mechanizmów bezpieczeństwa.

Na podstawie wyzwań technologicznych (problemów do rozwiązania) sformułowano tezę oraz przedstawiono w sposób ogólny proponowany system bezpieczeństwa dla sieci OpenFlow/SDN poprzez wyszczególnienie i krótki opis jego składników. Przyjęte założenia są poprawne. Kryteria dla proponowanego systemu przedstawiono w sposób umożliwiający ocenę zero-jedynkową tj. spełnia - nie spełnia (kryteria nie są też w jasny sposób wypunktowane). Nie przedstawiono kryteriów mierzalnych np. dotyczących wydajności.

W rozdziałach 5-8 został opisany proponowany system. W rozdziale 5 został opisany system od strony ogólnej, w rozdziale 6 został opisany moduł kontroli dostępu, w rozdziale 7 – moduł zapory ogniowej, w rozdziale 8 – moduł detekcji naruszeń. W rozdziale 10 zostały przedstawione wyniki walidacji poprawności, które pokazały, że system spełnia zakładane na początku kryteria. W podrozdziale 10.3 przedstawiono także wyniki testów wydajność, które zwróciły dobre wyniki dla scenariuszy testowych. Autor na początku pracy nie przedstawił zakładanych kryteriów dotyczących wydajności, ale przedstawione wyniki sugerują, że opracowany system nadaje się do praktycznego zastosowania. Podsumowując, autor rozwiązał postawione zagadnienie.

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?**

W ramach rozprawy autor zaproponował nowy system bezpieczeństwa dla sieci SDN. Przeanalizował istniejące rozwiązania z zakresu bezpieczeństwa sieci SDN i zaproponował system składający się z kilku komponentów, który wypełnił luki w istniejących rozwiązaniach. System składa się z następujących elementów:

a) modułu kontroli dostępu – moduł weryfikuje tożsamość hosta przed podłączeniem go do sieci, zapewnia różne poziomy uprawnień zależne od danych uwierzytelniających;
b) modułu zapory ogniowej – rozproszona zapora stanowa (*a distributed stateful firewall*) – posiada scentralizowaną politykę bezpieczeństwa zintegrowaną z aplikacją zapory ogniowej działającą ponad kontrolerem; zawiera system ochrony umożliwiający głęboką analizę pakietów z użyciem systemu Snort, który wykorzystywany jest do analizy pierwszych N pakietów z nowego przepływu pakietów;
c) modułu detekcji naruszeń polityk bezpieczeństwa – sprawdza, czy rekonfiguracja przekazywania pakietów nie narusza istniejących polityk zapory ogniowej (bezpieczeństwa).

Moduł kontroli dostępu (a) w porównaniu do istniejących rozwiązań jest uwierzytelnianiem opartym o tożsamość, nie wymaga dodatkowych protokołów oraz nowej metody enkapsulacji, serwer uwierzytelniania jest zaimplementowany jako osobny podmiot (różnice przedstawia tabela 9.1).

Moduł zapory ogniowej (b), w porównaniu do istniejących rozwiązań, łączy rozwiązania z zakresu różnych typów zapór ogniowych: stanu, aplikacji i głębokiej inspekcji pakietów. Takiej opcji nie posiadają łącznie istniejące rozwiązania dla sieci SDN (różnice w stosunku do prac pokrewnych przedstawiają tabele 9.2 i 9.3).

Moduł detekcji naruszeń polityk bezpieczeństwa (c), w porównaniu do istniejących rozwiązań, posiada bardziej optymalną implementację (tabela 9.4). Moduł wykorzystuje posiadany przez Kontroler widok sieci, aby stworzyć graf skierowany reprezentujący topologię sieci. Graf ten jest używany do śledzenia reguł przepływu i wykrywania pośrednich oraz bezpośrednich naruszeń polityki bezpieczeństwa.

Oryginalność (nowość) rozprawy polega na zaproponowaniu spójnego systemu bezpieczeństwa dla sieci SDN. Autor wykorzystuje istniejące komponenty powszechnie wykorzystywane w tradycyjnych sieciach i dostosowuje je do sieci SDN. Samodzielny i oryginalny dorobek autora stanowią moduły wchodzące w skład systemu bezpieczeństwa jak i sam system rozumiany jako całość.

Autor opublikował częściowe wyniki przedstawione w rozprawie w serii artykułów. Wyniki dotyczące modułu (a) zostały przez autora opublikowane w artykule na konferencji *International Conference on Computer Networks 2018*. Wyniki dotyczące zapory ogniowej (b) opublikował na konferencji *International Conference on Computer Networks 2017* i w czasopiśmie *Journal of Network and Systems Management* w 2020 roku, a wyniki odnośnie całości systemu w czasopiśmie *Applied Mathematics & Information Sciences* w 2018 roku. Artykuły doktoranta posiadają 14 cytowań (Google Scholar).

Biorąc pod uwagę podane cechy systemu, porównania do innych rozwiązań, a także cytowania artykułów w których opublikowano fragmenty rozprawy, to rozprawa wpisuje się w obecne badania prowadzone na świecie z zakresu bezpieczeństwa sieci SDN i zawiera nowe elementy w stosunku do istniejących rozwiązań zawartych w literaturze światowej.

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

Rozprawa od strony redakcyjnej jest przygotowana poprawnie. Drobnymi błędami w formatowaniu jest brak w wielu miejscach wcięć na początku akapitu. Rozprawa jest napisana w języku angielskim na dobrym poziomie językowym i posiada nieliczne błędy gramatyczne oraz stylistyczne. Zdania są zrozumiałe i poprawnie sformułowane.

Analiza układu rozprawy oraz jej zawartości wskazuje na poprawne określenie obszaru badań i problemów do rozwiązania. Wynik eksperymentalne są zaprezentowane poprawnie. Natomiast proponowany system jest w wielu miejscach opisany zbyt ogólnie, co utrudnia zrozumienie jego działania. W rozdziałach 5-8 autor opisuje kolejno cały system oraz poszczególne moduły. Opisy te na poziomie ogólnym są dobrze przedstawione, ale brakuje dokładnych, precyzyjnych opisów. W szczególności brakuje opisów w postaci pseudokodów (lub innego bardziej formalnego sposobu opisu algorytmów). Kody źródłowe mogłyby być umieszczone jako załącznik lub udostępnione na jednym z portali w postaci linku do repozytorium ze źródłami. Rysunki w wielu miejscach są niewystarczająco opisane. Główne wady w sposobie przedstawienia proponowanego systemu to:

- w rozdziale 5 na str. 60 opis *L-3 based learning swicth for packet delivery* powinien być przedstawiony w sposób bardziej przejrzysty (schemat i/lub pseudokod), gdyż opis w formie bloku tekstu utrudnia jego zrozumienie;
- na str. 64 opisywana jest zawartość rysunków 6.4 i 6.5, które są umieszczone dopiero kilka stron dalej;
- kolejne kroki na rysunkach 6.6 i 6.7 mogłyby być ponumerowane; w tekście zamiast opisu ciągłym tekstem, poszczególne kroki mogłyby być wypunktowane lub ponumerowane;
- rysunki 7.1 i 7.2 zawierają numery kroków, ale brak odwołań do nich w tekście;

- brakuje pseudokodu lub schematu blokowego lub innego bardzie formalnego przedstawienia *IPTables: Connection Tracking System* ze str. 78;
- algorytmy *TCP Stateful Tracking Algorithm* (str. 89), *UDP Tracking Algorithm* (str. 91) i *ICMP Stateful Tracking Algorithm* (str. 93) powinny posiadać opis formalny (np. pseudokod) oprócz ilustracji w postaci rysunków i opisów w ciągłym tekście;
- funkcja *Deep Packet Inspection (DPIF)* (str. 96) jest niedostatecznie opisana;
- brakuje pseudokodu lub schematu blokowego lub innego bardzie formalnego przedstawienia algorytmów *Violation Detection NetworkGraph-based flow rule tracking* oraz *Violation Detection flow rule tracking Algorithm* z rozdziału 8.

Podsumowując, taka prezentacja utrudnia odbiór pracy czytelnikowi i szczegółową analizę rozwiązań. Sposób przedstawienia opisanych wyników jest na poziomie dostatecznym.

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

Mocne strony rozprawy to:

a) przedstawienie zagadnienia od wyzwania technologicznego do eksperymentów;
b) eksperymentalne potwierdzenie wyników dotyczących wydajności;
c) zaprezentowanie systemu bezpieczeństwa o cechach lepszych od istniejących rozwiązań;
d) możliwość praktycznego zastosowania wyników.

Niewątpliwie, pomimo wymienionych powyżej zalet pracy, można w niej wskazać także słabe stron i wady. Dotyczą one kwestii dyskusyjnych i sposobu opisu (prezentacji) wyników i nie dotyczą głównych kwestii merytorycznych poruszanych w rozprawie.

Głównymi słaby stronami pracy są:

a) brak precyzyjnych, formalnych opisów algorytmów, czy dostępu do kodów źródłowych tj. opisano wyżej;
b) brak porównania wyników dotyczących wydajności z innymi rozwiązaniami oraz niewystarczająca dyskusja wyników w kontekście różnych konfiguracji sieci;
c) brak testów na rzeczywistych sieciach, z wykorzystaniem sprzętu sieciowego wspierającego OpenFlow;
d) brak zdefiniowania dokładnych wymagań odnośnie bezpieczeństwa. Proponowane są różne mechanizmy bezpieczeństwa, ale brak jest precyzyjnej, zebranej w jednymi miejscu informacji jakim dokładnie atakom lub jakim adwersarzom mają one zapobiegać.

Dodatkowo następujące drobne kwestie są dyskusyjne:

e) na stronie 118 jest użyty zwrot *a graphical representation*, a powinno być *a graph representation;*
f) na stronie 128 autor używa stwierdzenia *provide better security*; jednak nie jest dokładnie określone co znaczy lepsze bezpieczeństwo; czy jest to możliwość wykrywania większej liczby ataków pochodzących od intruzów wewnętrznych?

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

Rozprawa jest przydatna dla nauk technicznych. Autor zaprezentował system który rozwiązuje konkretne wymagania technologiczne z zakresu bezpieczeństwa sieci SDN. Zaproponowane w rozprawie rozwiązanie (opublikowane częściowo w artykułach) powiększa zakres wiedzy z zakresu bezpieczeństwa sieci SDN. W tym kontekście warto nadmienić, że moduł kontroli dostępu opublikowany przez autora w artykule F. Nife, Z. Kotulski, „*New SDN-oriented authentication and access control mechanism*" został uwzględniony przez Chang et al. (doi: 10.4236/jcc.2019.710010) przy budowie swojego rozwiązania z zakresu kontroli dostępu w sieciach SDN, co dodatkowo potwierdza wartość naukową rozprawy autora i przydatność rozprawy dla nauk technicznych.

8. **Do której z następujących kategorii Recenzent zalicza rozprawę?**

Przedstawione powyżej uwagi merytoryczne i formalne nie umniejszają osiągnięć doktoranta, ani nie podważają praktycznej przydatności proponowanego systemu bezpieczeństwa dla sieci SDN. Mocne strony rozprawy przewyższają słabe strony, z których większość zapewne wynika z dużego zakresu prac, co spowodowało, że autor musiał wybrać aspekty do przedstawienia w rozprawie. Przedstawioną do oceny rozprawę oceniam pozytywnie, zarówno z uwagi na aktualność i ważność tematyki rozprawy, jak również wiedzę autora oraz znajomość literatury z zakresu bezpieczeństwa sieci SDN.

Uważam, że autor zrealizował cel rozprawy, udowodnił tezę oraz wykazał się umiejętnościami i odpowiednim przygotowaniem do samodzielnej pracy naukowej w dyscyplinie informatyka techniczna i telekomunikacja. Na tej podstawie stwierdzam, że przedstawiona do oceny rozprawa doktorska mgra Fahad Naim Nife pt.: „New Security Management Scheme for Software-Defined-Networks (SDN)" **spełnia wymagania stawiane rozprawom doktorskim** zawarte w Ustawie *Prawo o szkolnictwie wyższym i nauce* z dnia 20 lipca 2018 roku (Dz. U. 2018 poz. 1668 z późn. zmn.) i wnoszę o dopuszczenie jej autora do publicznej obrony.

Tomasz Hyla

Żołnierska 49, 71-210 Szczecin-Poland, Tel. (48-91) 449 56 62/55 52, Fax:. (48-91) 449 55 40,
NIP: 852-254-50-56, www.wi.zut.edu.pl