AKADEMIA GÓRNICZO-HUTNICZA
IM. STANISŁAWA STASZICA W KRAKOWIE

Wydział Informatyki, Elektroniki i Telekomunikacji

KATEDRA TELEKOMUNIKACJI

Dr hab. inż. Piotr CHOŁDA, prof. AGH

Kraków, dn. 26 listopada 2019 r.

RECENZJA ROZPRAWY DOKTORSKIEJ

Tytuł rozprawy: *Mechanizm adaptacyjnego kierowania ruchem w sieciach sterowanych programowo*
Autor rozprawy: *mgr inż. Sebastian SZWACZYK*

1. WSTĘP

Niniejsza recenzja została przygotowana na potrzeby postępowania ws. nadania stopnia doktora nauk technicznych. Postępowanie prowadzi Wydział Elektroniki Wojskowej Akademii Technicznej (WAT).

Pełną dokumentację dot. rozprawy doktorskiej, wraz z informacją o powołaniu na recenzenta rozprawy przez Radę Wydziału Elektroniki WAT, otrzymałem od Pana Profesora Andrzeja P. DOBROWOLSKIEGO, Dziekana Wydziału Elektroniki WAT, w dn. 26 września 2019 r.

Oceniana rozprawa została napisana przez Pana magistra inżyniera Sebastiana SZWACZYKA. Nosi tytuł „Mechanizm adaptacyjnego kierowania ruchem w sieciach sterowanych programowo" i została napisana w całości po polsku (poza angielskojęzycznym streszczeniem, *Abstract*, zamieszczonym na str. 3). Promotorem doktoratu jest Pan prof. dr hab. inż. Marek AMANOWICZ, zaś promotorem pomocniczym Pan dr inż. Konrad WRONA.

Dostarczona mi rozprawa doktorska liczy 97 stron. Składa się z sześciu numerowanych rozdziałów: 1. Wstęp (str. 14-36), 2. Sieci sterowane programowo (str. 17-30), 3. Zarządzanie ryzykiem bezpieczeństwa informacji w systemach teleinformatycznych (str. 31-38), 4. Autorski mechanizm kierowania ruchem w sieciach SDN (str. 39-60), 5. Badanie mechanizmu RAR (str. 61-85), 6. Podsumowanie (str. 86-87). Oryginalne wyniki zasadniczo zawarto w rozdziałach 4 i 5. Uzupełnieniem zawartości pracy są: zamieszczone na początku streszczenia (w językach polskim i angielskim), spis rysunków i tabel, wykaz skrótów i oznaczeń (str. 2-13) oraz zawarta na końcu, ułożona w kolejności cytowania, bibliografia licząca 95 pozycji. Praca zawiera szereg kolorowych ilustracji, które ułatwiają odbiór tekstu. W pracy zamieszczono również pewną liczbę tabel głównie zbierających wyniki doświadczeń.

Poniżej odnoszę się do poszczególnych punktów składowych oczekiwanych ode mnie jako elementy recenzji rozprawy doktorskiej.

Akademia Górniczo-Hutnicza | Wydział Informatyki, Elektroniki i Telekomunikacji
Katedra Telekomunikacji
al. A. Mickiewicza 30, 30-059 Kraków,
tel. +48 12 617 39 37, fax +48 12 634 23 72
e-mail: kt@agh.edu.pl, www.agh.edu.pl

2. **CEL BADAŃ (W ODNIESIENIU DO TEZY ROZPRAWY). Jakie zagadnienie naukowe jest rozpatrzone w pracy (teza rozprawy) i czy zostało ono dostatecznie jasno sformułowane przez Autora?**

Zagadnienia podjęte przez Doktoranta dotyczą w ogólności projektowania bezpiecznych systemów sieciowych, przy czym pojęcie bezpieczeństwa jest jak najsłuszniej traktowane szeroko, tj. obejmuje również zagadnienia zaliczane do obszaru niezawodności. Dodatkowo, zagadnienie jest rozpatrywane w kontekście sieci sterowanych programowo SDN (*software defined networks*). Są to sieci programowalne, w których rozdzielono sterowanie (które typowo jest scentralizowane w odróżnieniu od tradycyjnych podejść w sieciach IP) od przesyłania danych. Jest to obecnie bardzo atrakcyjny i szeroko badany problem o potencjale zarówno aplikacyjnym, jak również teoretycznym. Ponadto pojęcie bezpieczeństwa jest w ramach rozprawy w sposób uniwersalny opisywane z użyciem koncepcji ryzyka, które jest wiązane ze ścieżką używaną podczas transmisji (czyli ma charakter odnoszący się do poszczególnych zapotrzebowań, usług itp.).

Doktorant poświęcił tezie rozprawy podrozdział 1.2. Postawiona teza to: „Mechanizm adaptacyjnego kierowania ruchem RAR (Risk-Aware Routing) zapewnia skuteczne zaspokajanie potrzeb informacyjnych użytkowników sieci SDN narażonej na ataki cybernetyczne dążąc do równoważenia obciążeń jej zasobów". Autor doprecyzował kilka pojęć użytych w tezie: „skuteczne" oznacza, że potrzeby informacyjne użytkowników zostaną zaspokojone na maksymalnym poziome realizacji usług z jednoczesnym zapewnieniem zgodności z przyjętą polityką bezpiecznego transferu danych. W kontekście samej tezy nie do końca jasne jest pojęcie „potrzeb informacyjnych", ale potrzeby te zostają w dalszej części pracy doprecyzowane w odniesieniu do modeli optymalizacyjnych przedstawionych w rozdziale 3. Wydaje się, że trudno byłoby krótko przedstawić znaczenie tego pojęcia akurat w rozdziale prezentującym samą tezę. Nieco dyskusyjne jest użycie słowa „cybernetyczny", gdyż sugeruje ono odniesienie do dyscypliny cybernetyki; zapewne lepsze byłoby pojęcie „ataków o charakterze informatycznym", ale w tym przypadku jest to tylko kwestia terminologiczna, a na pewno użyte określenie nie zaciemnia tezy.

Podana wyżej teza, razem z uzupełnieniami, jest jasno postawiona i zasadna. Już na samym początku daje się dostrzec jej wysoki walor, na pewno z punktu widzenia aplikacyjnego, ale odniesienie do konkretnego mechanizmu adaptacyjnego wskazuje również na ambicje badawcze. Teza jest dowodzona przez zaproponowanie specyficznej metody trasowania (służącej do adaptacyjnego kierowania ruchem z uwzględnieniem zmian stanu bezpieczeństwa sieci SDN przy użyciu podejścia inspirowanego zarządzaniem ryzykiem), która następnie zostaje poddana badaniu eksperymentalnemu.

3. **CHARAKTER ROZPRAWY. Jaki charakter ma rozprawa (teoretyczny, doświadczalny, inny)?**

Jak często zdarza się w przypadku prac doktorskich z dziedziny nauk inżynieryjno-technicznych, praca doktorska przedstawiona do recenzji ma głównie charakter konstrukcyjno-doświadczalny, tj. w celu udowodnienia postawionej tezy Doktorant proponuje mechanizm określony w tej tezie, po czym prowadzi szereg eksperymentów (w tym przypadku w środowisku laboratoryjnym emulującym

zachowanie sieci SDN), dowodzących że istotnie cechy określone w tezie są zapewnione. Z tego powodu pierwsza część oryginalna pracy (rozdział 4) opisuje projekt (abstrakcyjną „konstrukcję") mechanizmu (adaptacyjnego kierowania ruchem) w oparciu o pewne postulaty wyrażone z użyciem aparatu opisu zadań optymalizacji wielokryterialnej. Natomiast druga część oryginalna pracy (rozdział 5) wprowadza koncepcję scenariuszy testowych, środowiska laboratoryjnego oraz prezentuje wyniki wraz z ich analizą i na tej podstawie dowodzi, że teza rozprawy została udowodniona. Oczywiście nie jest to formalny dowód, ale trudno wymagać w odniesieniu do telekomunikacji, aby stosować do niej podejście, które w pełni odpowiada albo matematycznemu dowodzeniu tezy albo scholastycznemu podejściu do wykazywania prawdziwości tez filozoficznych (a przecież tego rodzaju oczekiwanie cały czas pokutuje w odniesieniu do współczesnych doktoratów). Stwierdzam więc, że przyjęty charakter rozprawy jest poprawny.

W ogólności istotna część rozprawy jest poświęcona opisowi wyników eksperymentów dowodzących, że zaproponowany przez Doktoranta mechanizm faktycznie zapewnia pożądane cechy założone w tezie. W ten sposób, element doświadczalny służy prawidłowemu metodologicznie dla dyscypliny informatyki technicznej i telekomunikacji wzmocnieniu koncepcji konstrukcyjnej. Biorąc to pod uwagę, można powiedzieć, że praca ma przede wszystkim walor empiryczny oraz ilustracyjny.

Elementy analityczno-teoretyczne również występują w rozprawie, aczkolwiek służą one raczej klaryfikacji podejścia oraz opisowi mechanizmu. Proponowany i badany w rozprawie mechanizm adaptacyjnego sterowania ruchem po pierwsze opiera się na podejściu optymalizacyjnym, ale zawiera również komponent algorytmiczny.

4. SPOSÓB PRZEPROWADZENIA ANALIZY ŹRÓDEŁ. SPOSÓB SFORMUŁOWANIA WNIOSKÓW WYNIKAJĄCYCH Z ANALIZY ŹRÓDEŁ. 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?

Sama lista bibliografii liczy 95 pozycji, przeważnie angielskojęzycznych. Analizie literatury nie poświęcono w rozprawie odrębnego rozdziału i jest ona rozproszona. Większe skupienie tego rodzaju treści można znaleźć w rozdziale 2, poświęconym sieciom SDN, jak również w rozdziale 3, który dotyczy przeglądu zagadnień związanych z elementami zarządzania ryzykiem. Cytowane i omawiane prace są to w większości ważne pozycje, oczywiście publikowane w obiegu międzynarodowym.

Przegląd literaturowy dobrze oddaje wiedzę Doktoranta oraz stan dziedziny szczególnie w odniesieniu do podstaw techniki sieci sterowanych programowo SDN, ich działania (w szczególności sposobu sterowania ruchem), jak również narażenia na ataki. Odpowiednie dane przedstawiono zwięźle, ale trafnie. Niewielkie niedociągnięcia w zakresie samej prezentacji to tylko brak jasnego rozróżnienia między interfejsami zachodnim i wschodnim w przypadku użytego modelu referencyjnego czy pozostawienie nieobjaśnionej bliżej czynności sterownika „przetwarzanie pakietu przez inne mechanizmy urządzenia sieciowego". Ponadto, opis literaturowy jest w zasadzie głównie skupiony na pokazaniu najnowszego stanu wiedzy, co oczywiście jest jednym z głównych celów analizy źródeł. Doktorant

bardziej po macoszemu potraktował jednak drugi cel tej analizy, tj. jasne wskazanie, co konkretnie inspirowało go do prowadzenia takich badań, które postanowił prowadzić oraz jakie konkretnie podejścia obecne w literaturze uznał za warte wykorzystania, a które za nieadekwatne do tematyki, która go interesuje. Tego rodzaju uwagi znajdują się gdzieniegdzie rozsiane w pracy doktorskiej, ale nie są konsekwentne. Czytelniejsza klasyfikacja różnych podejść byłaby tutaj bardzo pomocna, szczególnie w zakresie formułowania wniosków z analizy literaturowej. Właściwie główny podrozdział, w którym zawarto autorską analizę źródeł to 3.3.3, przy czym dotyczy on tylko różnych podejść do oceny ryzyka i — chociaż same wyniki analizy są ciekawe i trafne, tworząc cenny fragment pracy — pewnym jego brakiem jest niejasność zdefiniowania metodologii porównawczej.

Poniżej zwracam również uwagę na dwa obszary, które warto byłoby jednak omówić w pracy.

- Wprawdzie Doktorant odniósł się do zagrożeń, które stanową ryzyka dla systemów SDN, jak również do wielu podejść służących zarządzaniu ryzykiem (w szczególności do aspektu analizy ryzyka), to w zasadzie bardzo mało miejsca poświęcił konkretnym metodom łagodzenia ryzyka, tj. np. zabezpieczeniom systemów SDN przed konkretnymi atakami. Wprawdzie nie jest to istotny aspekt jego rozprawy, gdyż Doktorant nie skupia się na żadnych konkretnych grupach ataków (co oceniam bardzo pozytywnie), ale w zakresie analizy literaturowej można byłoby oczekiwać jednak odniesienia się do szerszego kontekstu bezpieczeństwa.
- Ze względu na fakt, że praca dotyczy uniwersalnego technicznego problemu projektowania systemów w oparciu o inżynierię ryzyka, można byłoby spodziewać się nieco bogatszego odniesienia do zagadnień analizy ryzyka (także w ujęciu matematycznym), jak również zastosowań w szerszym kontekście informatyki i telekomunikacji (np. do różnych wskaźników i miar ryzyka, modelowania niepewności albo do teorii zdarzeń rzadkich). Ponadto, biorąc pod uwagę, że Doktorant posługuje się co najmniej językiem optymalizacji, warto byłoby przedstawić nieco więcej prac poświęconych optymalizacji łagodzenia ryzyka sieciowego.

W ogólności stwierdzam jednak, że dobór źródeł jest aktualny i zasadniczo trafny, tj. Doktorant skupił się na szczególnie przydatnych pracach. Wybór pozycji literaturowych wskazuje, że Autor rozprawy jest dobrze zorientowany w zagadnieniach sterowania w sieciach SDN, w problematyce tworzenia takich sieci, jak również w obszarze zarządzania ryzykiem odnoszącym się do sieci telekomunikacyjnych.

5. Rozwiązanie przedstawionego zadania, właściwości przyjętych metod i założeń. Czy Autor rozwiązał postawione zagadnienia, czy użył właściwej do tego metody i czy przyjęte założenia są uzasadnione?

Przy okazji definiowania celu oraz tezy rozprawy, Doktorant sam nakreślił problemy badawcze, którymi postanowił się zająć:

1. Określenie reguł dynamicznej polityki bezpieczeństwa w procesach udostępniania i transferu informacji w sieci SDN.
2. Identyfikacja i ocena ryzyka związanego z transferem informacji w sieci SDN narażonej na cyberataki.

3. Określenie zasad kierowania ruchem w sieci SDN w celu minimalizacji ryzyka transferu zasobów informacyjnych z ograniczeniami ze względu na spełnienie wymogów bezpieczeństwa i równoważenia obciążeń sieci.
4. Przygotowanie środowiska badawczego, realizacja badań i analiza uzyskanych wyników.

Istotnie, Doktorant zrealizował wskazane powyżej cztery punkty, tym samym dowodząc zaprezentowanej wcześniej tezy. W związku z tym, że podany schemat wydaje mi się trafnym programem na udowodnienie przedstawionej tezy, poniżej odnoszę się do sposobu realizacji poszczególnych punktów.

Najpierw Autor zdefiniował matematyczny model sieci SDN w postaci grafu ważonego, w którym reprezentowane są elementy sieci (węzły, łącza) oraz właściwości opisujące te elementy w odniesieniu do zagadnień bezpieczeństwa oraz jakości transmisji (poufność, integralność, gotowość, przepustowość, reputacja). Zdefiniowane parametry w sposób uniwersalny opisują najważniejsze cechy odnoszące się do zabezpieczania transmisji i jako takie mogą być używane w różnych kontekstach, nie tylko np. cywilnych sieci SDN. Brak skupienia się na konkretnych zagrożeniach jest w tym przypadku cechą pozytywną, gdyż pozwala wypełnić ogólny schemat zaproponowany przez Autora treścią związaną z typem sieci, nowymi zagrożeniami (które przecież wciąż się pojawiają) itd. Warto tutaj zwrócić uwagę na ujęcie wszystkich trzech podstawowych elementów triady CIA (*confidentiality*, *integrity*, *availability*) oraz — co w ogóle jest dosyć rzadkie i nietypowe, ale przecież pożądane — reputacji (odnoszącej się do węzłów sieci).

Następnie Autor zaproponował sposób obliczania poszczególnych parametrów przy założeniu, że dla zapotrzebowań (czyli przepływów w sieci SDN) znane są ścieżki, którymi przebiega ruch z nimi związany (tj. znane jest trasowanie). Potem zdefiniował poziomy ryzyka skojarzone z poszczególnymi parametrami bezpieczeństwa. Doktorant zdecydował się na ujęcie ryzyka w rozumieniu wartości średniej, czyli iloczynu konsekwencji zrealizowania się zdarzeń niepożądanych oraz prawdopodobieństwa ich wystąpienia. Jest to podejście najbardziej popularne i zasadne. Mimo że istnieją inne podejścia, to są one dużo trudniejsze do analizy i być może niezbyt przydatne w praktyce sieciowej. Poziom naruszenia różnych parametrów jest w dalszej części rozprawy definiowany z użyciem kary określonej logarytmicznie (czyli z odpowiednim poziomem wypukłości funkcji).

W dalszej kolejności Doktorant zdefiniował szereg problemów związanych z określonym w tezie rozprawy mechanizmem (a właściwie rodziną mechanizmów) sterowania ruchem w oparciu o inżynierię ryzyka, tj. wprowadził problemy optymalizacyjne, w których wyróżnił odpowiednie funkcje kryterialne (zasadniczo nastawione na minimalizację różnie rozumianego ryzyka) oraz ograniczenia (związane z zapewnieniem odpowiednich poziomów ryzyka). Jedno z ujęć całkiem realistycznie zakłada poluzowanie (relaksację) ograniczeń, by jednak zapewnić możliwość realizacji zapotrzebowań. Inny problem jest skupiony na zagadnieniu minimalizacji nierównomierności obciążenia zasobów, czyli na cesze również będącej przedmiotem zainteresowania tezy rozprawy. Jest to problem rozpatrywany dosyć wszechstronnie, gdyż Doktorant rozważa różne sposoby rozumienia poziomu wykorzystania zasobów.

Następnie Doktorant pokazuje, w jaki sposób ma wyglądać wdrożenie w praktyce działania sieci SDN wyróżnionych sposobów optymalizacji trasowania, tj. omawia w jaki sposób konstruuje moduły wsparcia sterownika SDN oraz jak z ich pomocą dobiera ścieżki przepływów. Czyni to, definiując poszczególne algorytmy realizowania wymienionego w tezie mechanizmu RAR. Algorytmy zostały opisane

z użyciem czytelnego pseudokodu. Są to bardzo ciekawe pomysły praktyczne. Z drugiej strony w koncepcji badawczej w zasadzie brak podejścia korzystającego z bogactwa metod optymalizacyjnych. Mimo wprowadzenia opisu sugerującego oparcie się na programowaniu matematycznym, zasadniczo procedury poszukujące rozwiązań są dosyć proste i w zasadzie nie korzystają z zaawansowanych metod kojarzonych z rozwiązywaniem zadań optymalizacji. Oczywiście prostota może być dużą zaletą, ale w zasadzie Doktorant wcale nie stara się dowieść, że takie podejście jest faktycznie bliskie optimum. W ramach procedur poszukiwania rozwiązań problemu trasowania przepływów stosuje algorytmy poszukiwania tzw. *k* najkrótszych ścieżek, co jest zasadniczo podejściem popularnym i poprawnym, ale już wybór algorytmu Yena, stosowanego w celu znalezienia tych ścieżek, jest podany bez głębszej analizy i uzasadnienia, dlaczego akurat Autor rozprawy postępuje w ten sposób (skoro np. istnieją ulepszenia tych algorytmów). Ponadto, biorąc pod uwagę, że Doktorant proponuje pewne algorytmy służące sterowaniu ruchem, byłoby ciekawe poznać, jaka jest ich złożoność czasowa lub pamięciowa. Jeśli Doktorant nie zdecydował się na ich analizę od strony teoretycznej, to byłoby co najmniej zasadne podać zbadane eksperymentalnie wartości odnoszące się do czasu wykonywania czy zajętości pamięci. Akurat w przypadku sieci programowalnych jest to szczególnie istotne.

Doktorant skonstruował całe środowisko laboratoryjne, z użyciem którego przedstawił działanie zaproponowanego mechanizmu przy różnych scenariuszach testowych oraz w różnych konfiguracjach. Jest to w pełni działające środowisko sieci SDN, na którym faktycznie przeprowadzono różnego rodzaju emulacje działania. Biorąc pod uwagę możliwości oferowane przez tak elastycznie zdefiniowane środowisko, zdziwiło mnie dlaczego Doktorant zdecydował się prowadzić badania z użyciem jedynie dwóch topologii (które być może są jakoś reprezentatywne, ale kwestia ta nie podlegała głębszym rozważaniom, które znalazłyby odbicie w tekście rozprawy). Od strony praktycznej środowisko SDN jest dokładnie opisane, podobnie jak koncepcja wszystkich zaprogramowanych modułów, które czytelnie dzielą funkcje realizowane w sterowniku oraz w elementach wspierających. Z użyciem tego środowiska Doktorant przeprowadza 4 eksperymenty, które służą sprawdzeniu różnych sposobów zachowania się zdefiniowanego mechanizmu, tj. przy zróżnicowanych: strategiach generacji ataków na zasoby sieciowe, konfiguracjach heurystyki wyboru ścieżki, opcjach relaksowania polityki bezpieczeństwa, obciążeniach sieci ruchem. Na uwagę i pochwałę zasługuje z jednej strony pomysłowość w doborze różnych scenariuszy, jak też fakt że z różnych perspektyw obrazują one działanie zaproponowanych mechanizmów. Doktorant prezentuje wyniki w sposób czytelny, używając szeregu wskaźników, dokumentując wyniki z użyciem przejrzystych rysunków i tabel. Ponadto, jasno komunikuje własną interpretację wyników oraz konkluzje z niej wynikające. Proponowane mechanizmy oraz prowadzone doświadczenia oczywiście opierają się na szeregu założeń upraszczających, ale są one prezentowane wprost i bez niedomówień. Nie budzą zatem wątpliwości. Po stronie uwag krytycznych dotyczących badań eksperymentalnych podkreślić muszę brak właściwej analizy danych eksperymentalnych od strony wiarygodności statystycznej: mimo generowania wyników w sposób randomizowany (jak rozumiem, z użyciem metody Monte Carlo) Doktorant nie podejmuje głębszej refleksji nad istotnością statystyczną wyników ani nie przedstawia przedziałów ufności dla prezentowanych średnich. Niemniej jednak wyniki wydają się wiarygodne.

Zaprezentowane badania eksperymentalne w sposób szeroki i wielostronny pokazują, że mechanizm proponowany przez Doktoranta spełnia pokładane w nim nadzieje, które zdefiniowano w tezie rozprawy. W podsumowaniu tego punktu stwierdzam, że Doktorant w sposób prawidłowy rozwiązał postawione zagadnienie.

6. ORYGINALNOŚĆ ROZPRAWY, SAMODZIELNY DOROBEK AUTORA, POZYCJA ROZPRAWY W STOSUNKU DO STANU WIEDZY (POZIOM TECHNIKI) PREZENTOWANEGO W LITERATURZE ŚWIATOWEJ. 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 rozprawie doktorskiej Autor podjął bardzo istotne obecnie zagadnienie sterowania sieciami z punktu widzenia zapewnienia szeregu parametrów bezpieczeństwa, przy czym oparł się na podejściu inspirowanym różnymi aspektami zarządzania ryzykiem. Obecnie faktycznie trudno sobie wyobrazić zajmowanie się sterowaniem ruchem bez uwzględnienia aspektów zabezpieczenia się przed atakami. Faktem jednak jest, że wcale nie jest to podejście bardzo często spotykane w literaturze; zapewne wynika to z trudności tematyki. Dlatego wysoko oceniam fakt, że Doktorant postanowił zmierzyć się z zagadnieniem stanowiącym nietrywialne wyzwanie. Poza tym, przyjął podejście, w którym jawnie uwzględnia się zarówno możliwość zrealizowania się zagrożenia, jak również potencjalne konsekwencje — czyli właśnie podejście oparte na inżynierii ryzyka. Również takie ujęcie nie jest wcale popularne, mimo że — przynajmniej moim zdaniem — żaden wartościowy sposób odniesienia do bezpieczeństwa sieciowego nie powinien od niego abstrahować. Proponowany w ramach takiego podejścia mechanizm jest unikalny i nie był dotychczas prezentowany. Zagadnienia ryzyka są odniesione do strategii poszukiwania odpowiedzi na ryzyko, tj. do minimalizacji ryzyka. Jest to bez wątpienia najpopularniejsze ujęcie i nie powinno go nigdy zabraknąć w rozważaniach uwzględniających zarządzanie ryzykiem. Doktorant nie odniósł się do innych sposobów postrzegania zagadnienia optymalizacji ryzyka, np. poszukiwania kompromisu między kosztem łagodzenia ryzyka a samą wartością ryzyka, ale podjęcie takiej decyzji nie umniejsza oryginalności rozprawy oraz jej atrakcyjności na tle poziomu techniki reprezentowanego w literaturze światowej.

Ponadto dużym atutem podejście przyjętego przez Doktoranta jest ciekawe połączenie zagadnień bezpieczeństwa i problemów związanych z poszukiwaniem tras przepływów. Zazwyczaj oba te obszary są rozpatrywane oddzielnie, co najwyżej w zagadnieniach optymalizacji trasowania uwzględnia się jako element dotyczący bezpieczeństwa tylko kwestie niezawodnościowe. Te ostatnie oczywiście też są obecne w pracy (parametr tzw. dostępności), ale Doktorant zajmuje się również innymi (być może zresztą ważniejszymi) aspektami, tj. poufnością, integralnością czy reputacją. Innym walorem pracy jest przedstawienie wyników w środowisku sieci sterowanych programowo SDN. Jest to w tej chwili bardzo żywy temat badawczy, a Autor rozprawy wykorzystał bardzo dużo zalet zyskiwanych dzięki takiemu właśnie podejściu (np. elastyczność trasowania). Umożliwiają one badanie różnych scenariuszy, m.in. skupionych na doborze trasy w oparciu o wiele różnych składników wpływających na bezpieczeństwo i jakość. Zatem przyjęte przez Autora rozprawy podejście nie tylko jest prawidłowe, ale również nowatorskie. Warto przy

okazji zwrócić uwagę na sprawność implementacyjną i umiejętności praktyczne Doktoranta.

Chciałbym tutaj jednocześnie zwrócić uwagę, że dorobek Doktoranta nie ogranicza się jedynie do wyników zawartych w pracy. Niektóre tematy związane z opracowywanym zagadnieniem, ale jednak ujęte w inny sposób niż w rozprawie doktorskiej, były przez Autora zaprezentowane we współtworzonym przez niego artykule opublikowanym w prestiżowym periodyku telekomunikacyjnym *IEEE Communications Magazine*. Autorstwo artykułu tego rodzaju stanowi duże osiągnięcie i nie jest bynajmniej standardem w naszym kraju.

Wszystkie wspomniane tu aspekty wskazują na istotny (tj. adekwatny do zakresu oczekiwanego od kandydata do stopnia doktora nauk technicznych) dorobek Autora rozprawy w obszarze wiedzy, którego ona dotyczy.

7. Poprawność przedstawienia uzyskanych wyników (zwięzłość, jasność, umiejętność przekonywania, poprawność redakcyjna)

Praca jest zwięzła, napisana jasnym językiem, zasadniczo wolna od żargonu. Doktorant umie przedstawić wyniki w sposób przekonujący. Zasadniczo nie narzuca żadnych kontrowersyjnych poglądów, a mniej oczekiwane założenia lub wyniki są przeważnie oparte na przedstawionej analizie. Struktura pracy jest logiczna i przejrzysta. Główne rozdziały zawierające opis zastanej wiedzy, jak również oryginalne wyniki, mają zrównoważoną długość. W pracy zawarto pomysłowe i bardzo czytelne rysunki, z których przeważająca większość jest najwyraźniej autorstwa Doktoranta. Cenne są również tabele syntetycznie ujmujące wykorzystane konfigurację oraz prezentujące uzyskane wyniki.

Edycja pracy jest staranna, czemu — na ile mogę to ocenić na podstawie wydruku — przysłużył się również skład z użyciem systemu LaTeX. Praktycznie w ogóle nie dostrzegłem literówek. Wprawdzie w rozprawie można dostrzec pewną liczbę niedoróbek edycyjnych, ale zasadniczo nie utrudniają one odbioru treści, a ich liczba nie jest duża (poza dosyć irytującymi niedoróbkami w opisie bibliograficznym). Główne z nich, które zauważyłem to (uszeregowałem je w kolejności od nieco bardziej istotnych do dużo mniej ważnych):

- Uwagi terminologiczne:
  - Autor nazywa uogólnione obszary działania sieci „warstwami" (tj. niekiedy mówi o „warstwie sterowania" czy „warstwie transferu danych"), mimo że na ich określenie używa się przecież jednak pojęcia stanowiącego dosłowne tłumaczenie angielskiego terminu *plane* („płaszczyzna") w celu odróżnienia od warstwy technologicznej (jak w przypadku warstwy TCP czy warstwy łącza itp.). Pojęcie płaszczyzny jest już jednak przyjęte w języku polskim, zresztą Doktorant używa go na str. 17 (chociaż na tej samej stronie wraca też do słowa „warstwa", którego potem używa do końca rozprawy).
  - Autor zdecydował się konsekwentnie nazywać „dostępnością" jeden z ważnych z punktu widzenia doktoratu terminów. Chodzi o wielkość określaną w języku angielskim jako *availability*. Warto zwrócić uwagę, że w polskiej tradycji szkoły niezawodnościowej pojęcie to powinno nosić raczej nazwę „gotowość" i tak funkcjonuje ono nawet w Polskich Normach; przy czym pojęcie

„dostępności" dotyczy nieco innego terminu, który po angielsku nosi nazwę *accessibility*. Faktem jednak jest, że w kolokwialnym języku inżynierów informatyki i telekomunikacji przeważa kalka językowa, tj. tłumaczenie użyte w rozprawie, więc decyzja Doktoranta nie zaburza zrozumiałości.

- Ze względu na fakt, że rozprawa doktorska ma jednak charakter monograficzny, zgodnie ze zwyczajem akademickim należało uporządkować bibliografię nie według kolejności cytowania, a raczej z uwzględnieniem porządku opartego na nazwisku pierwszych autorów prac, do których odwołuje się Autor.
- Opis bibliograficzny:
  - referencja do [79] jest chyba w ogóle nieprawidłowa: klasyczny artykuł „Fault-tree analysis by fuzzy probability" ukazał się w IEEE Transactions on Reliability w 1983 r. i ma czterech autorów (drugi z nich na pewno nie nazywa się M. Ieee);
  - niekiedy brak bliższych danych bibliograficznych, które zwyczajowo są podawane i często są bardzo pożądane (na przykład w przypadku roku obrony pracy magisterskiej Autora [8] albo w przypadku książek – jak w [94], [95]: brak wydawnictwa, roku i miejsca wydania); odnośnie do niektórych publikacji w ogóle nie jest jasne, gdzie się ukazały lub jaki jest ich charakter, np. [62], [64], [70], [89];
  - w przypadku [23], [35] brak tytułów czasopism, w których zamieszczono odpowiednie artykuły;
  - tytuły czasopism są pisane w niekonsekwentny sposób, np. w przypadku [3] to *Proceedings of the IEEE*, ale już w przypadku [13] to *IEEE COMMUNICATIONS SURVEYS & TUTORIALS*;
  - materiały konferencyjne są opisywane w różny sposób, np. w przypadku [22] *Proceedings of...*, zaś w przypadku [25] *Proceeding of* (być może jest to akurat literówka), ale w [24] wprowadzono w ogóle nazwę konferencji bez podania że są to materiały konferencyjne; zaś w przypadku [28] czy [52] użyto w ogóle tylko skrótu nazwy konferencji, natomiast w przypadku [85] i [87] nazwy konferencji włączono do tytułów referatów;
  - tytuł pozycji [29] powinien raczej brzmieć: „Reflections on the REST architectural style and >>Principled design of the modern web architecture<<," (tzn. w tytule artykułu jest odniesienie do tytułu innego artykułu, co w sumie nie jest do końca jasne w wersji podanej w rozprawie);
  - niekiedy roczniki nazywa się tomami (t.), jak w przypadku [3], a innym razem — woluminami (vol.), jak w przypadku [13];
  - w niektórych przypadkach roczniki czasopism w ogóle nie są wprost podane (np. [1] czy [9]);
  - niektóre tytuły używają wielkich liter według konwencji brytyjskiej a inne — amerykańskiej (np. [20] w opozycji do [21]); zdarzają się również referencje, w przypadku których format tytułu jest zupełnie inny niż w pozostałych przypadkach (np. [70]);
  - do opisów niektórych numerów DOI wdarły się symbole, które w nich raczej nie występują (np. „{_}" w [32] i [93]);
  - ten sam artykuł jest cytowany dwa razy jako [86] i [90];

    - w przypadku [66] prawie na pewno podano nieprawidłowe numery stron.
- Bardzo cenne jest dostarczenie na początku rozprawy Wykazu skrótów. Byłoby jednak zasadne podać odpowiedniki terminów angielskich albo nawet rozszerzyć wykaz o słownik definiowanych skrótów.
- Zauważyłem pewną liczbę potknięć interpunkcyjnych, które w ogólności są bolączką polskich autorów piszących teksty techniczne. O ile w niektórych przypadkach kwestia interpunkcji faktycznie nie jest trywialna do rozstrzygnięcia, o tyle w rozprawie zdarza się stawianie przecinków w dosyć nieoczekiwanych miejscach — przynajmniej z punktu widzenia reguł języka polskiego (np. „W protokole *OpenFlow*, wyróżniono" na str. 20; „Kierowanie ruchem w nowoczesnych systemach teleinformatycznych, może być kluczowym elementem" na str. 23).
- Zdarzają się, chociaż dosyć rzadko, niezbyt zręczne anglicyzmy (np. „bazują na"). Niekiedy Autor używa nie do końca trafnie dobranych przyimków (np. „poprzez" w rozumieniu abstrakcyjnym, jak w „poprzez płynne przejście" na str. 18). Bywa, że występuje niezgodność przypadków, która nie ma miejsca w języku angielskim, ale w polskim jest gramatycznie niepoprawna (np. zamiast „odpowiedzialne za monitorowanie, zarządzanie i realizację funkcji sieciowych" na str. 19 powinno być „odpowiedzialne za monitorowanie i realizację funkcji sieciowych oraz zarządzanie nimi").
- Niedopatrzenia redakcyjne, np.:
    - tabele (w przeciwieństwie do rysunków) używają różnej wielkości czcionek, co wygląda nienaturalnie; w niektórych przypadkach czcionki są zresztą bardzo małe i utrudniają czytanie;
    - definiowanie podsekcji, które nie tworzą dalszego ciągu (np. jest podsekcja 4.4.1, ale nie ma już 4.4.2; podobnie dla 4.6.1);
    - niekonsekwencje lub niewielkie niepoprawności opisu, np.:
        - w wielu przypadkach dywiz błędnie zastępuje myślnik (np. zamiast „Risk-Aware Routing — Basic Formulation" jest „Risk-Aware Routing - Basic Formulation" na str. 11);
        - opuszczony styl kursywy matematycznej (np. w przypadku opisu z użyciem x czy y, jak np. w przypadku wykazu oznaczeń — tj. zamiast „reputacja wierzchołka x" jest „reputacja wierzchołka x" na str. 12);

Przypuszczam, że szczególnie w przypadku opisu bibliograficznego wiele potknięć stosunkowo łatwo da się uniknąć i w sumie tylko one mogą bardziej razić z punktu widzenia edycji.

8. Słabe strony rozprawy, jej główne wady

W przypadku rozprawy można wskazać trzy główne punkty, do których muszę odnieść się nieco bardziej krytycznie (do części z nich odniosłem się już wcześniej):

- Brak ścisłego podejścia skupionego na optymalizacji w oparciu o programowanie matematyczne. Wprawdzie Doktorant przedstawił opis matematyczny, który sugeruje silne skupienie na zagadnieniach optymalizacji i faktycznie nawet poszukuje pewnych rozwiązań, które ocenia z punktu widzenia postawionych funkcji kryterialnych, ale jednak

trzeba stwierdzić, że nie korzysta z całego dorobku badań operacyjnych przeniesionych do telekomunikacji. Przyjęte podejście do optymalizacji wielokryterialnej jest jednym z wielu możliwych (w zasadzie oparte na tzw. programowaniu celowym) i można było odnieść się także do innych opcji. Sam dobór ścieżek jest dokonywany z użyciem jednego z algorytmów poszukiwania tzw. k najkrótszych ścieżek, dla których następnie wyliczane są parametry, na podstawie których stwierdza się, czy spełnione są ograniczenia nałożone przez operatora. Zasadniczo jest to poprawne podejście heurystyczne, ale wykorzystanie całego aparatu programowania matematycznego dałoby szansę na stwierdzenie, na ile suboptymalne wyniki znalezione w ten sposób odbiegają od absolutnie najlepszego rozwiązania możliwego do znalezienia (czyli — faktycznie optymalnego). Z drugiej strony, precyzyjne podejście do optymalizacji systemu, o którym mowa w rozprawie, wymagałoby zapewne zastosowania programowania dyskretnego oraz uwzględnienia nieliniowości wprowadzanych przez funkcje celu oraz niektóre z ograniczeń, co nie byłoby zadaniem trywialnym i przekierowywałoby pracę na nieco inne tory. Doktorant zdaje sobie zresztą z tego sprawę, gdyż zagadnienie ścisłego podejścia optymalizacyjnego zadeklarował jako temat badań w przyszłości.

- Autor rozprawy bardzo mało miejsca poświęca analizie statystycznej wyników, które są przecież uzyskiwane w wyniku działania pewnych procedur randomizacji. Nie dostrzegłem głębszej analizy wiarygodności statystycznej. Doktorant zrezygnował również z podawania przedziałów ufności dla wartości stanowiących podstawę do interpretacji i analiz, co nie zostało przez niego wyczerpująco skomentowane.
- Analiza literaturowa jest dokonana nieco pobieżnie, tj. brak jasnego wskazania ewidentnych inspiracji literaturowych (poza kilkoma przypadkami). Warto byłoby również bliżej przyjrzeć się literaturze poświęconej matematycznemu podejściu do zagadnień modelowania ryzyka (w aspekcie jego analizy oraz optymalizacji łagodzenia).

Mimo występowania wskazanych słabości, w ogólności przedstawiona rozprawa doktorska jest cenna.

9. Przydatność rozprawy dla nauk technicznych, przemysłu, obronności kraju itp.

Rozprawa wnosi wkład w zakresie (1) zarządzanie współczesnymi sieciami telekomunikacyjnymi, (2) sterowania takimi sieciami oraz (3) w zakresie zabezpieczania tego rodzaju sieci. Wszystkie te trzy aspekty, zresztą powiązane ze sobą, stanowią istotnie przydatne wyniki w następujących obszarach:

- Nauki techniczne: tutaj można wskazać przede wszystkim uzysk badawczy, skupiony na oryginalnym podejściu o charakterze optymalizacyjnym do zarządzania zasobami w sieciach SDN oraz sterowania przepływami w takich sieciach.
- Przemysł: praca skupia się na obecnie jednym z najtrudniejszych w telekomunikacji (ale też najżywiej badanych) problemach zabezpieczania transmisji, proponując ujęcie, które może posłużyć do

redukowania strat operatorów (w tym przypadku sieci SDN) wynikających z różnego rodzaju ataków.

- Obronność: przede wszystkim zagadnienia bardzo uniwersalnego podejścia do zabezpieczania sieci, wcale nie skupionego na zastosowaniach cywilnych, dają możliwość użycia zaprezentowanych mechanizmów do sterowania obiektami abstrakcyjnymi, które będą używane np. w kontekście militarnym, kiedy reagowanie na różnego rodzaju zagrożenia i zdarzenia niepożądane jest kluczowe.

10. Podsumowanie (czy rozprawa spełnia wymagania przez obowiązujące przepisy)

Moim zdaniem przedstawiona rozprawa doktorska stanowi oryginalne rozwiązanie problemu naukowego poprawnie postawionego przez Doktoranta w dziedzinie nauk techniczno-inżynieryjnych w dyscyplinie informatyka techniczna i telekomunikacja. Z przedstawionej analizy literaturowej wynika, że Doktorant posiada aktualną wiedzę odnoszącą się do: z jednej strony — technik związanych z sieciami sterowanymi programowo SDN, z drugiej strony — zna aktualne trendy w odniesieniu do zabezpieczania sieci przewodowych, z trzeciej strony — orientuje się w problematyce zarządzania ryzykiem i sterowania sieciami w oparciu o elementy inżynierii ryzyka. Ponadto Autor na podstawie wyżej wskazanych elementów i w połączeniu z jego umiejętnościami praktycznymi dotyczącymi oprogramowywania i konfiguracji sieci SDN był w stanie zaproponować oryginalne rozwiązanie, które przetestował i przeanalizował, a na tej podstawie wysnuł ciekawe konkluzje. Ponadto Doktorant przedstawił rozprawę prezentującą propozycje oraz uzyskane wyniki, ale również dowodzącą, że jest w stanie prowadzić z powodzeniem badania naukowe oraz je dokumentować.

Stwierdzam zatem, że recenzowana rozprawa doktorska spełnia wymagania stawiane przez obowiązujące przepisy. Z tego powodu wnoszę o dopuszczenie jej do publicznej obrony.

Piotr Chołda