RADA NAUKOWA DYSCYPLINY
INFORMATYKA TECHNICZNA I TELEKOMUNIKACJA POLITECHNIKI WARSZAWSKIEJ

zaprasza na

OBRONĘ ROZPRAWY DOKTORSKIEJ

mgr. inż. Jędrzeja Tadeusza BIENIASZA

która odbędzie się w dniu **6 lutego 2023 roku,** o godzinie **12.00** w trybie mieszanym *

Temat rozprawy:

„Rozproszone metody ukrywania informacji w sieciach”

Promotor: dr hab. inż. Krzysztof Szczypiorski, prof. uczelni – Politechnika Warszawska

Recenzenci: prof. dr hab. inż. Aleksander Byrski – Akademia Górniczo-Hutnicza w Krakowie

dr hab. inż. Jacek Rak, prof. uczelni – Politechnika Gdańska

prof. dr hab. inż. Krzysztof Walkowiak – Politechnika Wrocławska

* Obrona odbędzie się w Gmachu Elektroniki, Warszawa, ul. Nowowiejska 15/19, w sali 476-479 oraz zdalnie na platformie MS Teams. Osoby zainteresowane uczestnictwem w obronie w trybie zdalnym są proszone o zgłoszenie chęci uczestnictwa w formie elektronicznej na adres sekretarza komisji: dr hab. inż. Artur Tomaszewski, prof. uczelni – email: artur.tomaszewski@pw.edu.pl, do dnia 03.02.2023 r., 23:59.

Z rozprawą doktorską i recenzjami można się zapoznać w Czytelni Biblioteki Głównej Politechniki Warszawskiej, Warszawa, Plac Politechniki 1.

Streszczenie rozprawy doktorskiej i recenzje są zamieszczone na stronie internetowej: https://bip.pw.edu.pl/Postepowania-w-sprawie-nadania-stopnia-naukowego/Doktoraty/Wszczete-po-30-kwietnia-2019-r/Rada-Naukowa-Dyscypliny-Informatyka-Techniczna-i-Telekomunikacja/mgr-inz.-Jedrzej-Bieniasz.

Przewodniczący Rady Naukowej Dyscypliny
Informatyka Techniczna i Telekomunikacja
Politechniki Warszawskiej
dr hab. inż. Jarosław Arabas, prof. uczelni

Streszczenie

Niniejsza rozprawa doktorska przedstawia rezultaty badań teoretycznych i praktycznych dotyczących różnych aspektów rozproszonych metod ukrywania informacji w sieciach. Steganografia, w tym steganografia sieciowa i rozproszona, w ciągu ostatnich 20 lat była intensywnie badana pod kątem możliwości jej stosowania w działaniach ofensywnych w cyberprzestrzeni. Wzrost popularności jej zastosowania przez atakujących widoczny jest w treści raportów opisujących incydenty bezpieczeństwa komputerowego. Z drugiej strony techniki ukrywania informacji wpisujące się w szeroko pojętą dziedzinę metod *cyber deception* mogą być wykorzystane w zadaniach cyberobrony systemów teleinformatycznych oraz ich użytkowników.

W ramach prac badawczych podjęto zagadnienie rozproszonych metod ukrywania informacji w sieciach w czterech komplementarnych kierunkach:

1. zbadanie charakteru i możliwości stosowania metod rozproszonej steganografii w ofensywnych operacjach w cyberprzestrzeni,
2. rozszerzenie metodyk modelowania cyberzagrożeń poprzez uwzględnienie technik ukrywania informacji w sieciach,
3. realizacja kompletnej ścieżki badań na danych na potrzeby detekcji metod steganografii rozproszonej – od stworzenia symulacji metod steganografii, przez implementację prototypu systemu detekcji, po referencyjne zastosowanie metod *data science*,
4. zastosowanie technik ukrywania informacji jako mechanizmu protekcji systemów i użytkowników w podejściu *cyberfog*.

Przedstawione osiągnięcia rozwijają stan wiedzy w dyscyplinie informatyka techniczna i telekomunikacja oraz stanowią wkład do rozwoju nauk o cyberbezpieczeństwie (ang. *science of cybersecurity*) – od poznawania metod cyberatakujących, przez budowanie rozwiązań cyberobrony opartych na tej wiedzy i danych, po proponowanie nowych mechanizmów bezpieczeństwa sieci.

Słowa kluczowe: cyberbezpieczeństwo, steganografia sieciowa, ukrywanie informacji w sieciach, cyberobrona, nauka o danych, bezpieczeństwo sieci, systemy wieloagentowe, wykrywanie cyberzagrożeń, wykrywanie włamań do sieci

prof. dr hab. inż. Aleksander Byrski
Instytut Informatyki
Akademia Górniczo-Hutnicza
im. Stanisława Staszica w Krakowie
Al. Mickiewicza 30, 30-059 Kraków
olekb@agh.edu.pl

Kraków 28.10.2022

Recenzja rozprawy doktorskiej pt. "Rozproszone metody ukrywania informacji w sieciach" opracowanej przez mgr inż. Jędrzeja Bieniasza, asystenta w Instytucie Telekomunikacji, Wydziału Elektroniki i Technik Informacyjnych Politechniki Warszawskiej

Mgr inż. Jędrzej Bieniasz (dalej "Doktorant") przedstawił do oceny rozprawę doktorską w formie cyklu następujących artykułów:

- [A1] Bieniasz, J., & Szczypiorski, K. (2017). SocialStegDisc: Application of steganography in social networks to create a file system. 2017 3rd Internatio- nal Conference on Frontiers of Signal Processing (ICFSP), 2017, pp. 76-80. DOI: https://doi.org/10.1109/ICFSP.2017.8097145. Rodzaj publikacji: materiały pokonferencyjne (IF: –; liczba cytowań: 7) Punktacja MEiN: 20
- [A2] Bieniasz, J., & Szczypiorski, K. (2019). Methods for Information Hiding in Open Social Networks. Journal of Universal Computer Science, 25(2), 74-97. DOI: https://doi.org/10.3217/jucs-025-02-0074. Rodzaj publikacji: artykuł w czasopiśmie (IF: 1.139; liczba cytowań: 2) Punktacja MEiN: 40
- [A3] Bieniasz, J., & Szczypiorski, K. (2019). Steganography Techniques for Command and Control (C2) Channels. In Botnets. Architectures, Countermeasu- res, and Challenges. (pp. 189-216). CRC Press. DOI: https://doi.org/10.1201/ 9780429329913-5. Rodzaj publikacji: rozdział w monografii (IF: –; liczba cytowań: 0) Punktacja MEiN: 50
- [A4] Bieniasz, J., Stepkowska, M., Janicki, A., & Szczypiorski, K. (2019). Mobile Agents for Detecting Network Attacks Using Timing Covert Channels. Journal of Universal Computer Science, 25(9), 1109-1130. DOI: https://doi.org/ 10.3217/jucs-025-09-1109 Rodzaj publikacji: artykuł w czasopiśmie (IF: 1.139; liczba cytowań: 7) Punktacja MEiN: 40
- [A5] Bieniasz, J., & Szczypiorski, K. (2021). Dataset Generation for Develop- ment of Multi-Node Cyber Threat Detection Systems. Electronics. 2021; 10(21):2711. DOI: https://doi.org/10.3390/electronics10212711. Rodzaj publikacji: artykuł w czasopiśmie (IF: 2.937; liczba cytowań: 1) Punktacja MEiN: 100
- [A6] Bieniasz, J., & Szczypiorski, K. (2018). Towards Empowering Cyber Attack Resiliency Using Steganography. 2018 4th International Conference on Fron- tiers of Signal Processing (ICFSP), 2018, pp. 24-28. DOI: https://doi.org/10. 1109/ICFSP.2018.8552068. Rodzaj publikacji: materiały pokonferencyjne (IF: –; liczba cytowań: 1) Punktacja MEiN: 20
- [A7] Bieniasz, J., Bąk, P., & Szczypiorski, K. (2022). StegFog: Distributed Steganography Applied To Cyber Resiliency In Multi Node Environments. IEEE Access,

2022. DOI: https://doi.org/10.1109/ACCESS.2022.3199749. Rodzaj publikacji: artykuł w czasopiśmie (IF: 3.476; liczba cytowań: 0) Punktacja MEiN: 100.

Wspomniane artykuły stanowią najważniejszą część 175-stronicowego manuskryptu. Manuskrypt zaczyna część wstępna zawierająca sformułowanie następującego celu pracy: przeprowadzenie badań teoretycznych i praktycznych w zakresie różnych aspektów rozproszonych metod ukrywania informacji w sieciach zgodnie z nowoczesnym podejściem do budowy zdolności do wykrywania i reagowania na cyberzagrożenia w oparciu na wiedzy i danych.

Po części wstępnej zamieszczono dokładny przewodnik po treści załączonych artykułów, przedstawiający najważniejsze osiągnięcia w nich zamieszczone. Manuskrypt zawiera również CV naukowe Doktoranta, co ułatwia ocenę, mimo tego iż nie jest wymagane przez obowiązujące akty prawne. Doktorant zamieścił również oświadczenia współautorów odnośnie kontrybucji do poszczególnych artykułów zarówno w formie szacowania procentowego wkładu pracy jak i podając merytoryczne aspekty przypadające na poszczególnych współautorów. Zamieszczone oświadczenia utwierdzają w przekonaniu, że Doktorant pełnił rolę wiodącą we wszystkich przedstawionych w cyklu pracach naukowych.

Steganografia a w szczególności w wydaniu prezentowanym przez Doktoranta jest niezmiernie ciekawym i niewątpliwie posiadającym wysoki potencjał zastosowania tematem badawczym. Przechowywanie wrażliwych danych w sposób ukryty, docelowo niewykrywalny w obszarze tak bardzo otwartym dla każdego, jakim są sieci komputerowe a nawet społeczne, niewątpliwie jest i będzie atrakcyjne zarówno dla osób mających w planach zarówno legalne (ukrywanie wrażliwych danych np. przez upoważnione służby) jak i nielegalne (np. komunikacja systemów biorących udział np. w atakach w cyberprzestrzeni) wykorzystanie tego typu narzędzi. Dlatego jednocześnie ważne jest opracowanie metod ukrywania danych jak i metod wykrywania tego typu działań - dokładnie w ten obszar wpisuje się przedstawiona do recenzji rozprawa.

W ramach przedstawionego do oceny cyklu artykułów, Doktorant badał naturę rozproszonych metod steganografii (artykuły [A1] i [A2]) w ramach których m.in. opracował autorski system plików o nazwie SocialStegDisc rozszerzając koncepcję StegHash opracowaną wcześniej przez jego Promotora, wprowadzając sekwencję bloków oraz definiując możliwości operacji na plikach wraz z przeprowadzeniem niezbędnych analiz i testów a także ewaluacji cechy niewykrywalności systemu, rozważając również możliwość zastosowania zaproponowanego rozwiązania jako jednej z metod cyberodporności systemu. Artykuły te można określić jako najważniejsze w cyklu, w szczególności prezentujące najistotniejsze osiągnięcia Doktoranta.

W [A3] Doktorant skupia się na analizie stanu wiedzy dotyczącej wykorzystywania steganografii do komunikacji Command and Control wraz z przeglądem metod jej wykrywania i zapobiegania, odniesienie wykorzystania steganografii do realizacji kanałów C2 w ramach metodyk modelowania zagrożeń, a także podsumowuje on najważniejsze znane ataki C&C z lat 2010-2018. Artykuł ten ma charakter przeglądowy i dowodzi szerokiej wiedzy Doktoranta w obszarze cyberbezpieczeństwa i steganografii.

W artykułach [A4] i [A5] opisana została realizacja procesu badań na danych na potrzeby detekcji metod steganografii rozproszonej - od stworzenia symulacji metod steganografii przez implementację prototypu systemu detekcji po referencyjne zastosowanie metod data science. W artykułach Doktorant stosuje systemy wieloagentowe jako podstawę wykrycia kanałów steganograficznych. Abstrahując od niedociągnięć w kontekście prezentacji samej istoty systemu wieloagentowego (odnoszę się do tej wady później) można ocenić te artykuły jako istotny komplement do artykułów [A1] i [A2], pokazujący osiągnięcia Autora w zbliżonym obszarze badań.

W artykułach [A6] i [A7] Doktorant koncentruje się na opracowaniu i przetestowaniu koncepcji nowatorskiego systemu komunikacyjnego StegFog (mającego działać w obszarze fog computing) łączącego trzy typy klasycznych podejść do steganografii w jeden system rozproszone steganografii dzieki przechowywaniu danych w obrazach, wykorzystaniu tekstu do zarządzania wskaźnikami do ukrytych danych oraz steganografię sieciową opracowanąna potrzeby realizacji ukrytej komunikacji. To kolejny element składający się na całościowy obraz wysokich umiejętności Doktoranta nie tylko w obszarze teorii ale również praktyki, pozwalający ponadto mieć duże nadzieje nie tylko na dalszą kontynuację badań, ale również na potencjalne wdrożenia.

Przedstawione artykuły składające się na rozprawę należy wysoko ocenić w kontekście bibliometrycznym - Doktorant mimo tego iż jest w zasadzie na początku swojej kariery naukowej, już może się pochwalić publikacjami w czasopismach notowanych na tzw. liście filadelfijskiej, niektóre o bliskim lub przekraczającym 3 współczynniku wpływu, tudzież punktowanymi powyżej 100 punktów wg obowiązującej punktacji MEiN - i to pełniąc w nich rolę wiodącą zgodnie z zamieszczonymi oświadczeniami. Stanowi to dobry prognostyk dla dalszej działalności naukowej Doktoranta i zachęca do realnej, bardzo wysokiej oceny jego osiągnięć.

Podsumowując, osiągnięcia badawcze Doktoranta raportowane w przewodniku, można wskazać w następujący sposób:

[D1] Stworzenie środowiska symulacji rozproszonych metod steganografii na potrzeby zbierania zestawów danych do ich analizy.

[D2] Opracowanie architektury rozwiązania i implementacja prototypu systemu wieloagentowego do monitorowania i wykrywania cyberzagrożeń wykorzystujących metody ukrywania informacji.

[D3] Zbadanie efektywności metod z obszaru data science do analizy i wykrywania symulowanych metod steganografii oraz zaproponowanie nowego algorytmu lub architektury przetwarzania danych do wykrywania steganografii.

[D4] Opracowanie koncepcji nowej metody steganograficznej o charakterze rozproszonym na potrzeby badania jej stosowalności, efektywności i cech charakterystycznych.

[D5] Usystematyzowanie wiedzy o cyberzagrożeniach związanych z rozproszonymi metodami steganografii, w tym poprzez zastosowanie metod modelowania cyberzagrożeń do budowania cyberobrony opartej na wiedzy i danych.

[D6] Zbadanie możliwości stosowania metod steganografii rozproszonej w kontekście obronnym - np. jako mechanizm bezpieczeństwa danych czy zapewnienia prywatności.

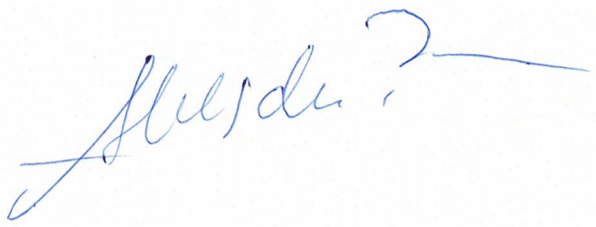
Po zapoznaniu się z planami, osiągnięciami i raportami wskazującymi jednoznacznie na realizację w.w. działań zawartymi we wspomnianych artykułach, stwierdzam, że Doktorant zajął się sprawą bardzo istotną, zrobił to w sposób kompetentny przeprowadzając szereg eksperymentów oraz analiz, nie tylko zakańczając pewien etap swojej pracy naukowej, ale wyznaczając punkt startowy dla szeregu ścieżek badawczych i rozwojowych, dla których niniejsza rozprawa może być punktem wyjścia.

Teraz chciałbym skoncentrować się na uwagach krytycznych i dyskusyjnych, które w przypadku ocenianej rozprawy nie zmieniają postrzegania jej całości w jakikolwiek sposób i nie umniejszają jej końcowej bardzo pozytywnej oceny.

1. Określenie celu pracy jest nie do końca precyzyjne, o wiele łatwiej byłoby ocenić kompletność pracy gdyby Doktorant pokusił się o sformułowanie tezy, której potem dowiódłby w swoich publikacjach i zaznaczył w przewodniku po nich, co należy do elementarnych kroków klasycznej metody naukowej. Byłbym zobowiązany gdyby Doktorant spróbował sformułować jednoznaczną tezę w czasie obrony i wskazał jej prawdziwość na podstawie wniosków z przedstawionych artykułów.
2. W artykule [A4] Doktorant wykorzystuje pojęcie agenta oraz systemu wieloagentowego, choć po lekturze można odczuć, że istotnie zastosowany został przez Doktoranta paradygmat agentowy do implementacji systemu monitoringu i detekcji zagrożeń - nie jest to w sposób precyzyjny pokazane w artykule. Proponuję przedyskutować w trakcie obrony algorytmy postępowania poszczególnych agentów (wysokopoziomowy pseudokod) z naciskiem na wykazanie autonomii i proaktywności.
3. Struktura łańcuchowa opracowanego przez Doktoranta dysku steganograficznego przypomina strukturę systemu blockchain - proponuje przedyskutować (jako potencjalną ścieżkę rozwoju systemu) możliwość zastosowania technologii blockchain w opracowanym systemie steganograficznym.
4. Chętnie usłyszałbym jak Doktorant ocenia możliwości wdrażania w modelu sprzedaży licencji lub open source zaproponowanych przez Doktoranta metod.
5. Język rozprawy jest poprawny tak samo oceniam skład wykonany w systemie LaTeX, w oczy rzucił mi się jeden błąd językowy który warto wskazać, otóż w podsumowaniu artykułów Doktorant używa sformułowania "stan sztuki" co jest bezpośrednim tłumaczeniem terminu angielskiego "state-of-the-art". W języku polskim raczej tłumaczy się ten termin jako "stan wiedzy".

Zgodnie z obowiązującą ustawą, rozprawa doktorska (...) powinna stanowić oryginalne rozwiązanie problemu naukowego (...) oraz wykazywać ogólną wiedzę teoretyczną kandydata w danej dyscyplinie naukowej (...) oraz umiejętność samodzielnego prowadzenia pracy naukowej (...). Stwierdzam, że przedstawiona do recenzji rozprawa spełnia przytoczone wymagania, gdyż opracował on szereg nowatorskich rozwiązań steganograficznych i przetestował ich charakterystyki, opracowane przez Doktoranta artykuły są poprawnie osadzone w literaturze tematu i świadczą o Jego szerokiej wiedzy fachowej (w tym jeden z nich ma charakter przeglądowy), zaś jego widoczne zaangażowanie w opracowanie wszystkich artykułów świadczy o tym, że jest gotowy do prowadzenia badań naukowych już raczej we współpracy z innymi naukowcami niż pod ich opieką.

Biorąc pod uwagę przytoczone powyżej obserwacje, zwracam się do Rady Dyscypliny Naukowej Informatyka Techniczna i Telekomunikacja Politechniki Warszawskiej z prośbą o dopuszczenie mgr inż. Jędrzeja Bieniasza do dalszych etapów postępowania w sprawie nadania stopnia doktora nauk technicznych. Ponadto, ze względu na wysoką jakość artykułów włączonych do cyklu (na 6 artykułów 3 z nich zostały opublikowane w czasopismach z tzw. impact factor), dużą samodzielność Doktoranta w realizacji badań, a także wysoką kreatywność i samodzielność w rozwiązywaniu postawionych problemów, rekomenduję wyróżnienie rozprawy.



POLITECHNIKA
GDAŃSKA
WYDZIAŁ ELEKTRONIKI,
TELEKOMUNIKACJI I INFORMATYKI

Gdańsk, 14.12.2022 r.

Dr hab. inż. Jacek Rak, prof. PG
Wydział Elektroniki, Telekomunikacji i Informatyki
Politechnika Gdańska

Recenzja rozprawy doktorskiej

Tytuł: Rozproszone metody ukrywania informacji w sieciach

Autor: Mgr inż. Jędrzej Tadeusz Bieniasz

Rozprawa doktorska mgra inż. Jędrzeja Bieniasza analizuje problemy oraz przedstawia wyniki badań własnych związanych z rozproszonymi formami ukrywania informacji w sieciach teleinformatycznych. Problem jest niewątpliwie ważny i aktualny, gdyż analizowana przez Doktoranta steganografia sieciowa i rozproszona stanowi rzeczywiście obszar intensywnych badań naukowych w ostatnim okresie. Doktorant we wstępie pracy słusznie podkreśla, że steganograficzne metody ukrywania informacji mogą zostać wykorzystane zarówno w działaniach defensywnych, jak i ofensywnych, toteż zrozumienie ich charakterystyk (w kontekście możliwości wystąpienia potencjalnych ataków) stanowi z pewnością ważny etap poprzedzający konstrukcję rozwiązań z zakresu przeciwdziałania atakom – w szczególności wykorzystujących steganografię jako instrument działań ofensywnych. Efektywność metod obrony zależy w dużej mierze od dopasowania ich charakterystyk do sposobu działań atakujących.

Oceniana rozprawa doktorska składa się z sześciu rozdziałów napisanych w języku polskim, stanowiących wprowadzenie do zawartości załącznika A obejmującego siedem artykułów [A1]-[A7] napisanych w języku angielskim (jako że rozprawa została przygotowana w oparciu o cykl publikacji powiązanych tematycznie). Występujący w rozprawie drugi załącznik (B) zawiera oświadczenia współautorów powyższych siedmiu prac cyklu dotyczące procentowych wkładów autorów w powstanie tychże prac. Analizując zawartość załącznika B rozprawy, stwierdzam, że

JRak

udział Doktoranta na poziomie 60-75% jest znaczący i świadczy o wiodącym zaangażowaniu Doktoranta w powstanie tych prac.

1. Jaki jest problem naukowy rozprawy i czy został on trafnie i jasno sformułowany?

Celem pracy było opracowanie metod zwiększania poziomu cyberbezpieczeństwa (oraz ocena skuteczności tychże metod) w dwóch obszarach:

- detekcji cyberzagrożeń wykorzystujących rozproszone metody ukrywania informacji wraz z reagowaniem na nie,
- projektowania i wdrożenia mechanizmów ochrony wykorzystujących rozproszone metody ukrywania informacji.

Cel rozprawy został w pracy jasno zdefiniowany. Jest on niewątpliwie także trafny z uwagi na obserwowaną tendencję wzrostową w odniesieniu do liczby, skali, jak i różnorodności form ataków. Jak ukazuje zawartość rozprawy, cel ten został osiągnięty wielotorowo m.in. poprzez działania z zakresu:

- projektu i realizacji środowiska symulacyjnego z zakresu rozproszonych metod steganografii,
- konstrukcji prototypu systemu wieloagentowego służącego do wykrywania zagrożeń wykorzystujących technki steganograficzne,
- wykorzystania metod z obszaru inżynierii danych do wykrywania steganografii wraz z zaproponowaniem techniki przetwarzania danych w tym kontekście,
- projektu rozproszonej metody steganograficznej oraz weryfikacji jej cech charakterystycznych,
- pozyskania i klasyfikacji wiedzy dotyczącej cyberzagrożeń wykorzystujących rozproszone metody steganografii,
- analizy możliwości wykorzystania metod steganografii rozproszonej w kontekście ich zastosowania w aspekcie defensywnym.

Pomimo, że teza badawcza nie została w rozprawie zdefiniowana, jasno wyrażony cel rozprawy oraz zaprezentowane w rozprawie wyniki moim zdaniem rekompensują brak tejże tezy i dowodzą możliwości poprawy poziomu cyberbezpieczeństwa poprzez wykorzystanie rozwiązań proponowanych przez Doktoranta w rozprawie bazujących na steganografii.

2. Na czym polega oryginalny dorobek Autora i jakie jest znaczenie poznawcze lub przydatność praktyczna dla nauki bądź techniki?

Do oryginalnego dorobku ukazanego w ocenianej rozprawie należy moim zdaniem zaliczyć:

1) wyniki badań Doktoranta opisane w rozdziale 2 dotyczących realizacji metody steganograficznej dedykowanej otwartym sieciom społecznościowym szczegółowo opublikowane w pracach [A1] i [A2], a w szczególności:

   a. opracowanie koncepcji steganograficznego systemu plików SocialStegDisc wraz implementacją proof-of-concept,

   b. dokonanie analizy niezawodności i niewykrywalności systemu,

   c. dokonania analizy wpływu zastosowania tejże koncepcji w cyberprzestrzeni,

2) wyniki badań Doktoranta opisane w rozdziale 3 z obszaru wykrywania skutków działań rozproszonych metod ukrywania informacji zaprezentowane w pracach [A3]-[A5] obejmujące w szczególności:

   a. analizę stanu wiedzy z zakresu stosowania metod steganografii do ukrywania informacji w sieciach; zestawienie istniejących metod detekcji i przeciwdziałania kanałom Command&Control opisane w pracy [A3],

   b. propozycje metod detekcji anomalii w procesie śledzenia ścieżki realizacji ataku, w tym wykorzystujące metody uczenia maszynowego operujące na danych zebranych podczas realizacji scenariuszy symulacyjnych (ukazane w pracy [A4]),

   c. rozszerzenie koncepcji z pracy [A4] o mechanizm celowego opóźniania i tracenia pakietów opisany w pracy [A5],

3) rezultaty badań Doktoranta z zakresu defensywnych zastosowań steganografii rozproszonej (cyber deception) opublikowane w pracach [A6], [A7] dotyczące:

   a. opracowania mechanizmów steganograficznych opisanych w pracy [A6] dedykowanych koncepcji *cyberfog*, w tym w szczególności mechanizmu indeksacji realizującego ideę metody StegHash, mechanizmu dyspersji w oparciu o metodę SocialStegDisc,

   b. zaprojektowania architektury systemu w ujęciu warstwowym wraz z analizą teoretyczną szeregu aspektów z obszaru bezpieczeństwa, niezawodności oraz ogólnie rozumianej wydajności (także praca [A6]),

   c. opracowania systemu StegFog opisanego w pracy [A7], stanowiącego rozszerzenie koncepcji z artykułu [A6] m.in. w zakresie mechanizmów i protokołów realizujących zapis/odczyt danych ukrytych, ukryte powiadamianie o dostępności danych czy też ukryty routing do kolejnych fragmentów danych.

Ponadto, należy także pozytywnie ocenić przejrzystą strukturę rozprawy obejmującą rozdział 1 (wstęp ukazujący cel i zakres rozprawy), rozdział 2 podsumowujący wyniki badań Doktoranta w

obszarze realizacji rozproszonych metod ukrywania informacji, rozdział 3 podsumowujący uzyskane wyniki badań z zakresu wykrywania form ukrywania informacji, jak i rozdział 4 ukazujący wyniki badań Doktoranta w obszarze defensywnych zastosowań metod steganograficznych.

Powyższe osiągnięcia udokumentowane również poprzez dogłębną ewaluację charakterystyk w drodze analizy teoretycznej i symulacyjnej dowodzą łącznej realizacji celu rozprawy.

3. Czy Autor rozwiązał postawiony problem i czy użył do tego celu właściwych metod?

Analizując zawartość rozdziałów rozprawy doktorskiej mgra inż. Jędrzeja Bieniasza, w szczególności osiągnięć zaprezentowanych w rozdziałach 2-4 ukazujących wyniki opublikowane w pracach [A1]-[A7], uważam że Doktorant rozwiązał we właściwy sposób problem zdefiniowany w rozprawie dotyczący metodologii detekcji oraz ochrony przed atakami wykorzystującymi techniki steganograficzne.

W mojej ocenie, metodologia zastosowana przez Doktoranta w kolejnych etapach badań jest poprawna, odpowiada technikom stosowanym w badaniach naukowym, a stopień jej złożoności jest adekwatny do oczekiwań stawianym pracom na poziomie doktorskim.

Warto w tym miejscu podkreślić, że osiągnięcia badawcze Doktoranta opublikowane w:

- czterech artykułach w czasopismach z listy JCR (w tym w jednym artykule z roku 2022 w IEEE Access – 100 pkt, jednym artykule w czasopiśmie Electronics z roku 2021 – 100 pkt oraz dwóch artykułach w czasopiśmie Journal of Universal Computer Science z 2019 roku za 40 pkt każdy),
- jednym rozdziale monografii wydawnictwa CRC Press z roku 2019,
- sześciu artykułach w materiałach konferencji międzynarodowych w latach 2017-2020

oraz bardzo dobre (w odniesieniu do postępowań doktorskich) wartości parametrów bibliometrycznych (w tym indeksu Hirscha H=3, liczby cytowań wynoszącej 37 oraz łącznej liczby punktów MEiN związanych z siedemnastoma publikacjami Doktoranta wynoszącej 459 pkt.) łącznie dowodzą zdolności Doktoranta rozwiązywania problemów badawczych o istotnym znaczeniu na arenie międzynarodowej.

4. Jakie są słabsze strony rozprawy?

Analiza słabszych aspektów rozpraw przygotowanych w oparciu o cykl publikacji ma niewątpliwie odmienny charakter w porównaniu z rozprawami klasycznymi (tj. prac, których główną częścią nie są artykuły naukowe). Każdy z artykułów cyklu tworzący taką rozprawę, stanowi bowiem pewną zamkniętą całość poddaną uprzedniej recenzji przed ukazaniem się w czasopiśmie / materiałach konferencyjnych. W przypadku takich prac, potencjalne ograniczenia

merytoryczne mogą wynikać np. z odgórnych limitów liczby stron prac narzuconych przez wydawnictwo / organizatorów konferencji. Jedyną częścią rozprawy przygotowaną przez kandydatów podczas tworzenia rozprawy jest w takim przypadku ogólne wprowadzenie.

Oceniając rozprawę doktorską mgra inż. Jędrzeja Bieniasza nie zauważyłem istotnych uchybień zarówno w zakresie merytorycznym, jak i struktury siedmiu prac cyklu [A1]-[A7]. Forma przedstawiania osiągnięć w tych pracach jest co prawda zróżnicowana, lecz wynika ona z odmiennych standardów wydawniczych (szablonów).

Jako że prace [A1]-[A7] dotyczą wąskiego obszaru steganografii, wstępy tychże prac są dosyć podobne, co jest jednakże typowe w przypadku rozpraw składających się z cyklu prac. Jeśli traktować to jako wadę, to nie w odniesieniu do tejże konkretnej rozprawy doktorskiej, lecz ogólnie odnosząc tę uwagę ogólnie do systemowej koncepcji tworzenia prac w oparciu o zbiór publikacji. W takim przypadku umiejętności doktorantów w zakresie tworzenia rozpraw doktorskich można ocenić w zasadzie jedynie po jakości części wprowadzenia rozprawy.

W przypadku ocenianej rozprawy mgra Bieniasza wprowadzenie to składa się z sześciu rozdziałów o objętości łącznej ok. 50 stron. Moja ocena tejże części jest wysoka. Uważam, że została przygotowana bardzo dobrze pod względem struktury i zawartości merytorycznej. Zauważalne są sporadycznie drobne niedociągnięcia stylistyczne czy literówki, np.:

- na stronie 9: „metod podnoszenia cyberbezpieczeństwa" → „metod podnoszenia poziomu cyberbezpieczeństwa"
- na stronie 11: „IF: 1.056ui" → „IF: 1.056"

Warto byłoby poszerzyć badania o analizę dotyczącą stopnia niezawodności systemu sieciowego w obliczu ataków wykorzystujących steganografię, jak i analizę wpływu metod Doktoranta na niezawodność. Bezpieczeństwo i niezawodność są bowiem aspektami mającymi szereg powiązanych atrybutów jak choćby dostępność (ang. availability).

Powyższe uwagi w mojej ocenie nie rzutują na moją jednoznacznie pozytywną ocenę łączną rozprawy doktorskiej mgra inż. Jędrzeja Bieniasza.

5. Do której z następujących kategorii Recenzent zalicza rozprawę:

a/ nie spełniająca wymagań,
b/ wymagająca wprowadzenia poprawek i ponownego recenzowania,
c/ zadowalająco spełniająca wymagania,
d/ wykraczająca ponad poziom zadawalający (spełniająca wymagania z nadmiarem),
e/ wybitna?

Podsumowując, moja recenzja pracy doktorskiej mgra inż. Jędrzeja Bieniasza jest **pozytywna**. Zarówno wartość merytoryczna rozprawy jak i ranga wyników opublikowanych w siedmiu głównych pracach rozprawy (oznaczonych jako pozycje [A1]-[A7]) kwalifikują w mojej ocenie rozprawę mgra inż. Jędrzeja Bieniasza do kategorii **d/ wykraczająca ponad poziom zadawalający (spełniająca wymagania z nadmiarem)**.

Z uwagi na spełnione przez Doktoranta ustawowe wymagania, **wnoszę o dopuszczenie rozprawy doktorskiej mgra inż. Jędrzeja Bieniasza do publicznej obrony**. Ponadto, z uwagi na szereg znaczących publikacji Doktoranta, z których składa się oceniana rozprawa (w tym czterech prac z listy JCR o wiodącym udziale Doktoranta), wskazanych w sekcji 3 niniejszej recenzji, jak wobec szeregu nagród i wyróżnień, które Doktorant uzyskał w związku ze swoją pracą badawczą, opisanych na stronach 43-44 rozprawy, **wnoszę o wyróżnienie rozprawy**.

Jacek Rak

Wrocław, 8 grudnia 2022

Prof. dr hab. inż. Krzysztof Walkowiak
Wydział Informatyki i Telekomunikacji
Politechnika Wrocławska

RECENZJA ROZPRAWY DOKTORSKIEJ
DLA RADY DYSCYPLINY INFORMATYKA TECHNICZNA I TELEKOMUNIKACJA
POLITECHNIKI WARSZAWSKIEJ

Autor rozprawy doktorskiej: mgr inż. Jędrzej Bieniasz
Tytuł rozprawy doktorskiej: *„Rozproszone metody ukrywania informacji w sieciach”*
Promotor: dr hab. inż. Krzysztof Szczypiorski, prof. uczelni

1. Zakres i charakter rozprawy

Recenzowana rozprawa doktorska mgr inż. Jędrzeja Bieniasza dotyczy zagadnień związanych z bezpieczeństwem sieci teleinformatycznych, w szczególności rozprawa koncentruje się na problematyce cyberbezpieczeństwa i steganografii. Cyberbezpieczeństwo jest bardzo aktualnym i ważnym obszarem badawczym. Wynika to głównie z nieustannie rosnącej popularności różnych systemów informatycznych stosowanych w praktycznie każdym aspekcie ludzkiej aktywności i gospodarki. Dodatkowo w ostatnich latach obserwowany jest duży wzrost liczby różnorakich zagrożeń i ataków na systemy informatyczne mających związek z działaniami przestępczymi, także w sferze konfliktów międzynarodowych. Steganografia, w szczególności steganografia sieciowa i rozproszona w ciągu ostatnich dwóch dekad jest przedmiotem badań naukowych w obszarze cyberbezpieczeństwa. Głównym kierunkiem badań jest analiza możliwości zastosowania tych metod w różnych atakach na cyberbezpieczeństwo. Ponadto, raporty opisujące incydenty bezpieczeństwa komputerowego potwierdzają rosnącą skalę wykorzystania steganografii przez atakujących systemy informatyczne.

Recenzowana rozprawa doktorska jest przedstawiona jako cykl następujących siedmiu artykułów naukowych:

- Bieniasz, J., & Szczypiorski, K. (2017). SocialStegDisc: Application of steganography in social networks to create a file system. 2017 3rd International Conference on Frontiers of Signal Processing (ICFSP), 2017, pp. 76-80.
- Bieniasz, J., & Szczypiorski, K. (2019). Methods for Information Hiding in Open Social Networks. Journal of Universal Computer Science, 25(2), 74-97.

- Bieniasz, J., & Szczypiorski, K. (2019). Steganography Techniques for Command and Control (C2) Channels. In Botnets. Architectures, Countermeasures, and Challenges. (pp. 189-216). CRC Press.
- Bieniasz, J., Stępkowska, M., Janicki, A., & Szczypiorski, K. (2019). Mobile Agents for Detecting Network Attacks Using Timing Covert Channels. Journal of Universal Computer Science, 25(9), 1109-1130.
- Bieniasz, J., & Szczypiorski, K. (2021). Dataset Generation for Development of Multi-Node Cyber Threat Detection Systems. Electronics. 2021; 10(21).
- Bieniasz, J., & Szczypiorski, K. (2018). Towards Empowering Cyber Attack Resiliency Using Steganography. 2018 4th International Conference on Frontiers of Signal Processing (ICFSP), 2018, pp. 24-28.
- Bieniasz, J., Bąk, P., & Szczypiorski, K. (2022). StegFog: Distributed Steganography Applied To Cyber Resiliency In Multi Node Environments. IEEE Access, 2022.

Należy podkreślić, że wybrana tematyka rozprawy jest aktualnym obszarem badań poszerzającym dotychczas realizowane prace badawcze w zakresie cyberbezpieczeństwa i steganografii. Warto również zauważyć, że publikacje wchodzące w skład rozprawy zostały opublikowane w renomowanych czasopismach naukowych i w materiałach dobrych konferencji naukowych oraz uzyskały oddźwięk w środowisku naukowym potwierdzony cytowaniami.

2. Zawartość rozprawy

Rozprawa składa się z 6 rozdziałów oraz dwóch aneksów. Pierwszy rozdział to wprowadzenie przedstawiające motywację tematu rozprawy, cel rozprawy oraz opis podstawowych zagadnień związanych z tematyką rozprawy doktorskiej. Rozdziały 2-4 opisują badania nad: realizacją rozproszonych metod ukrywania informacji w sieciach, wykrywaniem rozproszonych metod ukrywania informacji w sieciach oraz defensywnymi zastosowaniami rozproszonych metod ukrywania informacji w sieciach przedstawionymi w artykułach naukowych wchodzących w skład rozprawy. W rozdziale 5 Doktorant przedstawił podsumowanie zrealizowanych badań. Rozdział 6 zawiera opis dorobku naukowego Doktoranta. Aneks A zawiera treść siedmiu artykułów naukowych wchodzących w skład rozprawy doktorskiej. Aneks B zawiera oświadczenia współautorów tych artykułów.

W mojej ocenie struktura rozprawy doktorskiej jest prawidłowa. Doktorant w logiczny i przejrzysty sposób przedstawił kolejne zagadnienia, co ułatwia lekturę i analizę zawartości rozprawy. Ponadto, pragnę podkreślić bardzo wysoką jakość rozprawy pod kątem językowym, stylistycznym i edycyjnym.

3. Poprawność i oryginalność postawionej tezy

Rozprawa nie zawiera precyzyjnego zdefiniowania tezy badawczej (ang. *research question*). Określony jest jedynie główny cel pracy sformułowany w następujący sposób:

"*Celem niniejszej rozprawy doktorskiej jest opracowanie i ocena skuteczności metod podnoszenia cyberbezpieczeństwa w kontekście dwóch obszarów zastosowania rozproszonych metod ukrywania informacji w sieciach:*
1. inteligentnego wykrywania i reagowania na cyberzagrożenia wykorzystujące rozproszone metody ukrywania informacji,
2. mechanizmów ochrony sieci opartych na rozproszonych metodach ukrywania informacji."

W mojej opinii cel rozprawy jest sformułowany w poprawny sposób. Mgr inż. Jędrzej Bieniasz na podstawie przeglądu literaturowego i własnej wiedzy prawidłowo określił zakres rozprawy doktorskiej, koncentrując się na aktualnych i ważnych zagadnieniach związanych z cyberbezpieczeństwem i steganografią.

Cel rozprawy został osiągnięty w rozprawie doktorskiej poprzez:

- Opracowanie, zaimplementowanie i ocenę rozszerzenia koncepcji steganograficznego systemu plików SocialStegDisc opartego o metodę StegHash, w tym w zakresie możliwości zastosowania metod StegHash i SocialStegDisc w rozwiązaniach bezpieczeństwa sieci zgodnych z koncepcją cyberfog.
- Opracowanie nowego sposobu modelowania komunikacji steganograficznej złośliwego oprogramowania za pomocą kanałów Command & Control.
- Opracowanie, zaimplementowanie i ocenę nowego rozwiązania dotyczącego detekcji metod ukrywania informacji przy zastosowaniu koncepcji systemów wieloagentowych, w tym w zakresie zdolności do wykrywania węzłów sieciowych stanowiących źródło ataków.
- Opracowanie i zaimplementowanie nowego systemu komunikacyjnego opartego o rozproszoną steganografię opartą na wcześniejszych metodach analizowanych przez Doktoranta – StegHash i SocialStegDisc oraz dopasowanie systemu do podejścia cyberfog.

Według mojej opinii mgr inż. Jędrzej Bieniasz w prawidłowy sposób określił cel badań oraz metody realizacji postawionego celu.

4. Analiza źródeł (w tym literatury światowej i stanu techniki) świadcząca o dostatecznej wiedzy autora w danej dyscyplinie naukowej

Rozprawa doktorska mgr inż. Jędrzeja Bieniasza dotyczy bieżących zagadnień związanych z cyberbezpieczeństwem. Doktorant przeprowadził dokładny przegląd literaturowy. Lista pozycji bibliograficznych umieszczona w pierwszej części rozprawy zawiera 57 publikacji naukowych. Ponadto, każda z siedmiu publikacji wchodzących w skład cyklu zawiera swój własny przegląd literatury dotyczącej tematyki danego artykułu. Wśród omówionych prac naukowych znajdują się najważniejsze prace związane z tematyką poruszaną w rozprawie, w szczególności z: cyberbezpieczeństwem, steganografią, zagrożeniami w zakresie cyberbezpieczeństwa, analityką danych, metodami uczenia maszynowego. Przedstawiony przegląd literaturowy stanowi dobre wprowadzenie do dalej przedstawionych oryginalnych koncepcji Doktoranta. Moim zdaniem,

Doktorant posiada odpowiednią wiedzę i znajomość współczesnej literatury z zakresu związanego z tematyka rozprawy.

5. Pozycja rozprawy w stosunku do stanu wiedzy i stanu techniki reprezentowanych przez literaturę światową

Tematyka rozprawy doktorskiej jest związana z aktualnie rozwijanymi kierunkami badań w zakresie cyberbezpieczeństwa. Zagadnienia dotyczące podniesienia bezpieczeństwa działania sieci teleinformatycznych, w tym w zakresie rozproszonych metod ukrywania informacji w sieciach są bardzo ważnym tematem badawczym. Wynika to z jednej strony z nieustannego wzrostu liczby różnego rodzaju cyberzagrożeń, a z drugiej strony z rosnącej popularności stosowania metod ukrywania informacji.

Rozważane w rozprawie cyberzagrożenia w obszarze steganografii i przeciwdziałanie tym zagrożeniom stanowi wyzwanie dla bardzo wielu instytucji i przedsiębiorstw. Doktorant w prawidłowy sposób określił zakres tematyczny rozprawy i następnie zaproponował właściwe metody rozwiązania postawionych problemów stosując koncepcje zgodne z aktualnym stanem wiedzy i techniki reprezentowanym w światowej literaturze. Na szczególne podkreślenie zasługuje zastosowanie metod uczenia maszynowego oraz uwzględnienie w realizowanych badaniach najnowszych trendów w zakresie cyberbezpieczeństwa, w tym *intelligence-driven cyber defense*, *intelligence-driven incident response*, *data-driven network intrusion detection*, *cybersecurity data science*, *big data analytics for information security*.

Należy zaakcentować, że wyniki przedstawione w rozprawie zostały zrealizowane w ramach projektów badawczo-rozwojowych dofinansowanych w programie CyberSecIdent Narodowego Centrum Badań i Rozwoju (NCBiR):

- Projekt „*Zaawansowane Laboratorium Kryminalistyki Śledczej*”, 2017–2019. Numer projektu CYBERSECIDENT/369234/I/NCBR/2017.
- Projekt „*Platforma detekcji anomalii sieciowych (PDAS)*”, 2017–2019. Numer projektu CYBERSECIDENT/369532/I/NCBR/2017.

6. Znaczenie uzyskanych wyników dla danej dyscypliny naukowej

Jako najważniejsze oryginalne osiągnięcia rozprawy doktorskiej mgr inż. Jędrzeja Bieniasza w dyscyplinie informatyka techniczna i telekomunikacja należy wymienić:

- Opracowanie koncepcji steganograficznego systemu plików SocialStegDisc, w którym mechanizm indeksacji danych jest rozszerzeniem rozwiązania StegHash. W ramach zrealizowanych badań:
    - Zdefiniowano steganograficzne metody realizacji podstawowych operacji klasycznego systemu plików, w tym tworzenie pliku, odczyt pliku, usuwanie pliku.
    - Zaimplementowano system SocialStegDisc w postaci proof-of-concept.

- Przeprowadzono wszechstronne analizy i testy systemu SocialStegDisc pod kątem różnych dodatkowych funkcjonalności, w tym: możliwości skalowania rozmiaru dysku, sposobu tworzenia sekretów, wydajności działania w realnym środowisku otwartej sieci społecznościowej.
- Opracowano ocenę różnych aspektów działania systemu, w tym:
  - w zakresie niewykrywalności i niezawodności systemu;
  - w zakresie procesów kryminalistyki śledczej;
  - w zakresie nierównomierność przestrzeni adresowej.
  - w zakresie możliwości wykorzystania systemu jako mechanizmu cyberodporności.

- Przeprowadzenie syntezy stanu wiedzy w zakresie stosowania metod steganografii do komunikacji typu C2 (ang. *Command & Control*). Rozważono różne metody, metody steganografii obejmujące stegnaografię multimedialną, sieciową oraz hybrydową, realizowaną jako metoda rozproszona. W ramach zrealizowanych badań:
  - Opracowano modele teoretyczne kanałów C2 wykorzystujących steganografię.
  - Przeanalizowano wykorzystania steganografii do realizacji kanałów C2 w ramach różnych metodyk modelowania cyberzagrożeń.
  - Opracowano przegląd możliwych metod wykrywania i przeciwdziałania kanałom C2 zabezpieczonym steganografią.
  - W oparciu o autorską taksonomię przeanalizowano cyberataki z lat 2010–2018, w których zastosowano kanały C2 wykorzystujące metody steganografii.
- Opracowanie koncepcji teorii obserwacji zmiany oraz metod monitorowania i detekcji kanałów steganograficznych w rozproszonych środowiskach teleinformatycznych z wykorzystaniem systemów wieloagentowych. Stosując opracowane metody można m.in. wykryć i śledzić kradzież danych w ramach komunikacji C2. Opracowane metody opierają się na wykrywaniu węzłów źródłowych realizowanych operacji, co umożliwia podjęcie odpowiednich działań, np. blokada ruchu sieciowego. W ramach zrealizowanych badań:
  - Opracowano syntezę stanu wiedzy w obszarze badań.
  - Opracowano scenariusze testowe w zakresie realizacji symulacji metod steganografii we wskazanym środowisku wraz ze sformułowaniem hipotez badawczych.
  - Opracowano metody analizy uzyskanych danych.
  - Zaimplementowano i zbadano jakość działania metod uczenia maszynowego.
  - Opracowanie oceny uzyskanych wyników oraz sformułowanie wniosków końcowych.
- Opracowanie koncepcji rozproszonego systemu steganograficznego dla urządzeń internetu rzeczy wykorzystującej mechanizmy StegHash i SocialStegDisc. System ma możliwość realizacji rozproszonej komunikacji kanałami steganograficznymi o charakterze hybrydowym, tj. łączącym steganografię komunikacyjną i steganografię przechowywania danych. W ramach zrealizowanych badań:

- Opracowano architekturę warstwową systemu. Każda z warstw zawiera, obok komponentu realizacji zadań podstawowych, uzupełniający komponent steganograficzny właściwy dla danej warstwy.
- Opracowano podstawowe mechanizmy steganograficzne dla komunikacji zgodne z koncepcją cyberfog, w tym:
  - mechanizm indeksacji wykorzystujący metodę StegHash;
  - mechanizm dyspersji wykorzystujący metodę SocialStegDisc;
  - rozszerzenie zbioru nośników ukrytych informacji poza materiały multimedialne;
  - możliwość zastosowania platform komunikacji steganograficznej np. TrustMAS.
- Opracowano założenia dla protokołu komunikacji i aspektów operacyjnych systemu końcowego.
- Analiza systemu pod kątem:
  - bezpieczeństwa;
  - niezawodności;
  - zużycia pamięci;
  - czasu działania.

- Opracowanie nowego system steganografii rozproszonej StegFog, bazującego na schemacie indeksowania wprowadzony przez StegHash. W ramach zrealizowanych badań:
  - Zaprojektowano architektury systemu.
  - Zdefiniowano podstawowe mechanizmu systemu StegFog w zakresie:
    - zapisywania i odczytywania danych ukrytych w systemie;
    - ukrytej notyfikacji o dostępności danych;
    - ukrytego routingu do kolejnych fragmentów danych;
    - mechanizmu adresacji kolejnych fragmentów danych.
  - Zaimplementowano prototyp systemu.
  - Analiza systemu pod kątem:
    - projektu architektury oraz zdefiniowanych protokołów;
    - bezpieczeństwa mechanizmu adresacji;
    - parametrów operacyjnych systemu, w tym czas działania, zużycie pamięci, przepływności steganograficznej.

Należy podkreślić, że opracowane w recenzowanej rozprawie koncepcje oraz uzyskane wyniki mają duże znaczenia praktyczne. Doktorant zdefiniował i następnie rozwiązał realne i aktualne problemy badawcze związany z cyberbezpieczeństwem w obszarze steganografii stosując wiele różnych narzędzi badawczych, w tym metody uczenia maszynowego.

7. Główne wady rozprawy, słabe stron wraz z krytycznymi uwagami szczegółowymi

Uwagi natury ogólnej:

- Brak przedstawienia tezy rozprawy (pytania badawczego), Doktorant nie sformułował głównej tezy rozprawy, sformułowany został jedynie główny cel rozprawy.
- W rozprawie brakuje próby generalizacji uzyskanych wyników w zakresie inteligentnego wykrywania i reagowania na cyberzagrożenia wykorzystujące rozproszone metody ukrywania informacji. Moim zdaniem brakuje szerszego spojrzenia na poszczególne zagrożenia i próby zaproponowania bardziej uogólnionych metod.
- W podsumowaniu nie przedstawiono propozycji dalszych prac badawczych stanowiących rozszerzenie osiągnięć uzyskanych w rozprawie.

Uwagi natury polemicznej:

- Czy w kontekście stosowania metod uczenia maszynowego do wykrywania przypadków użycia steganografii były rozważane niestacjonarne strumienie danych dotyczące przypadków gdy rozkłady statystyczne danych mogą ulec zmianie, zmuszając model do uwzględnienia ich dynamiki w trakcie eksploatacji? Zjawisko to nazywa się dryfem koncepcji (ang. *concept drift*).

8. Konkluzja

Recenzowana rozprawa stanowi oryginalne rozwiązanie jednoznacznie sformułowanego zagadnienia naukowego. Autor rozprawy mgr inż. Jędrzej Bieniasz w przekonujący sposób wykazał umiejętność samodzielnego prowadzenia badań naukowych, a także ich prawidłowej i wnikliwej interpretacji. Wymienione powyżej uwagi ogólne, polemiczne oraz szczegółowe nie mają znaczącego wpływu na pozytywną ocenę rozprawy. W związku z powyższym uważam, iż przedstawiona mi do recenzji rozprawa doktorska mgr inż. Jędrzeja Bieniasza spełnia wymogi zawarte w ustawie dnia 20 lipca 2018 r. *Prawo o szkolnictwie wyższym i nauce* i wnoszę o dopuszczenie jej do publicznej obrony.