Prof. UTP dr hab. inż. Witold Hołubowicz **30.11.2019**

Recenzja rozprawy doktorskiej mgra inż. Huberta Ostap pt. „Clustering-based method for botnet detection"

Rozprawa ma objętość 178 stron, a jej główna część to cztery rozdziały, w których kolejno omówiono: przegląd literatury (21 stron), zaproponowaną przez Autora nowatorską metodę detekcji botów o nazwie BotTROP (20 stron), wykonane przez Autora środowisko symulacyjno-pomiarowe (26 stron) oraz wyniki weryfikacji skuteczności metody (92 strony). Obok tych głównych rozdziałów merytorycznych, w rozprawie znajduje się także lista rysunków i tabel, a także lista używanych skrótów. Jest także wstęp oraz 6-stronnicowe podsumowanie. W pracy umieszczono bibliografię obejmującą 101 pozycji. Praca napisana jest w języku angielskim.

W rozprawie autor zdefiniował nową metodę wykrywania sieci typu botnet, nazwaną przez niego BotTROP. Metoda ta została w rozprawie opisana, stworzono następnie programowe środowisko do testowania i pomiarów, a następnie wykonano szereg eksperymentów i wyniki uzyskane dla metody zaproponowanej przez Autora porównano z wynikami uzyskanymi dla metody BotGAD znanej z literatury. Autor rozprawy swoimi badaniami wpisuje się w rozległą i bardzo aktualną tematykę poszukiwania sposobów wykrywania, zwalczania i przeciwdziałania negatywnym skutkom aktywności sieci typu botnet. Jest to obszar, w których odbywa się swoisty „wyścig zbrojeń" pomiędzy przestępcami opracowującymi coraz to nowe narzędzia ataku, a inżynierami szukającymi nowych sposobów obrony.

Autor formułuje cel badań w dość nietypowym miejscu rozprawy, bo dopiero na końcu przeglądu literatury (str. 26). Rozprawa ma na celu znalezienie nowej, jeszcze lepszej niż metody znane dotąd, metody wykrywania sieci typu botnet działających synchronicznie. Autor zakłada przy tym, że wykrywanie sieci typu botnet odbywać się będzie wyłącznie na podstawie analizy ruchu w sieci, bez ograniczeń wynikających z konkretnego zastosowanego protokołu komunikacyjnego, a metoda powinna działać skutecznie zarówno dla sieci botnet już znanych

jak i tych jeszcze nie zidentyfikowanych. W odczuciu Recenzenta tak sformułowany cel pracy jest poprawny, a celowość podjęcia takich badań nie budzi wątpliwości.

Przegląd literatury (rozdział 2) nie budzi zastrzeżeń. Źródła dobrane zostały odpowiednio, zdecydowana większość cytowanych pozycji pochodzi z ostatnich 10 lat, a jedynie kilka jest nieco starszych i są to wówczas przede wszystkim klasyczne pozycje książkowe. W bibliografii jest także jedna wartościowa publikacja napisana przez Autora rozprawy (współautorem pracy jest promotor rozprawy). Rozdział 2 zawiera mniej więcej w połowie charakterystykę architektury sieci typu botnet oraz ich klasyfikację, a w połowie opisywane są znane już z literatury metody wykrywania sieci typu botnet. Wykonana przez Autora analiza literatury, a także dobór cytowanych pozycji literaturowych pokazują bardzo dobrą znajomość dziedziny przez Autora i swobodne poruszanie się w tematyce zagrożeń internetowych oraz metod przeciwdziałania im. Nieco więcej uwagi poświęcono algorytmowi BotGAD, który w dalszej części rozprawy stanowi główny punkt odniesienia dla Autora rozprawy jeśli chodzi o skuteczność zaproponowanego przez Autora algorytmu BotTROP. Podsumowując, Rozdział 2 jest zwięźle i syntetycznie napisany i stanowi dobre wprowadzenie do pozostałych rozdziałów przedstawiających oryginalny dorobek Autora.

Rozdział 3 zawiera opis metody detekcji, nazwanej przez Autora BotTROP, którą Autor zaproponował, a następnie szczegółowo przeanalizował w rozprawie. Metoda składa się z trzech etapów: grupowania, filtracji i klasyfikacji, a kolejne etapy opisane są w rozdziale. Mimo tego, Autor stwierdza w rozprawie (str. 30), że metoda BotTrop jest 2-etapowa, co Recenzentowi wydaje się nielogiczne. Opisy poszczególnych etapów są spójne i czytelne, ale w odczuciu Recenzenta Autor zbyt rzadko odwołuje się w tym rozdziale do metod już znanych i opisywanych wcześniej w przeglądzie literatury. Takie częstsze odwoływanie się i przyrównywanie do metod już znanych lepiej pokazałoby te aspekty, w których metoda BotTROP różni się od rozwiązań znanych, tymczasem w obecnym kształcie rozprawy to porównanie leży w znacznym stopniu po stronie czytelnika. Alternatywnie, można się tego doszukać w kończącym rozprawę rozdziale szóstym (str. 168), ale wymaga to znacznej cierpliwości po stronie czytelnika. Poza tym, zdaniem Recenzenta, warto byłoby podać w rozprawie w jakim stopniu znana z literatury klasyfikacja metodą SPRT, opisywana w podrozdziale 3.4 i dla której Autor przytacza obszerne wzory, musiała zostać przystosowana przez Autora rozprawy do potrzeb jego badań. Wykresy podane w rozprawie na rysunkach 3.5 i 3.6 zdecydowanie wskazują na istnienie takiego wkładu po stronie Autora, jednak zdaniem Recenzenta praca zyskałaby na czytelności gdyby Autor zdecydował się opisać to w sposób jednoznaczny. Sam algorytm BotTROP umieszczono w podrozdziale 3.5 w postaci 35 wierszy

kodu, Autor nie dodał przy tym w tym rozdziale żadnego komentarza. Z kolei w podrozdziale 3.6 nazwanym „Podsumowanie", Autor *de facto* opisuje faktyczne działanie algorytmu, którego kod umieszczono w poprzednim podrozdziale. Byłoby bardziej logicznie i zrozumiale, zdaniem Recenzenta, gdyby podrozdziały 3.5 i 3.6 połączyć. Pomimo powyższych uwag i sugestii Recenzenta, głównie natury organizacyjnej i logicznej, wydźwięk łączny Rozdziału 3 jest dla Recenzenta jasny i pozytywny. W rozprawie zaproponowano i opisano nową metodę detekcji sieci typu botnet, zaimplementowano ją oraz sprawdzono jej działanie w szczególności w porównaniu ze znaną z literatury metodą BotGAD.

W kolejnej części rozprawy (Rozdział 4) opisano implementację algorytmów BotTROP i BotGAD. Autor rozprawy wybrał metodę BotGAD jako swój główny punkt odniesienia, ale informację o tym podał jedynie lakonicznie w Rozdz. 2 (str. 20), w trakcie robienia przeglądu literatury. W dalszych rozdziałach rozprawy nie ma już ani przez chwilę obszerniejszego wyjaśnienia takiego założenia. Recenzent odczuwa pewien niedosyt w kwestii braku takiego szerszego uzasadnienia, a przecież jest to jedno z głównych założeń omawianej rozprawy, szczególnie w kontekście tego, że na początku podrozdziału 2.4 (str. 15) Autor pisze o „ogromnej liczbie metod detekcji zagrożeń opisanych w literaturze". Warto podkreślić, że Recenzent nie kwestionuje tego wyboru Autora, sugeruje jedynie, że decyzję taką warto byłoby staranniej skomentować w rozprawie.

Implementacja wykonana przez Autora rozprawy składa się faktycznie z dwóch odrębnych części. Z jednej strony chodzi tu o realizację narzędzia analizującego ruch w sieci zgodnie z algorytmami BotTROP and BotGAD, z drugiej strony konieczne jest w badaniach posiadanie generatora wytwarzającego ruch sieciowy zawierający zarówno elementy ruchu prawidłowego, tj. pochodzącego z legalnych źródeł, jak i elementy związane z działaniem sieci typu botnet. Autor rozprawy zdecydował się umieścić na rysunkach w rozprawie szereg zrzutów ekranowych obrazujących działanie symulatora, co sprawia, że rozdział jest czytelny i logicznie napisany. Także pokazanie w formie graficznej, na ekranie komputera, wyników symulacji jest plastyczne i daje czytelnikowi dobre wyobrażenie co do działania środowiska symulacyjnego stworzonego przez Autora. W podrozdziale 4.5 Autor proponuje swój własny wariant procedury pozwalający na analizę działania sieci typu botnet w sieciach społecznościowych, a implementacja opisana w rozprawie dotyczy sieci Twitter. Podsumowując, Rozdział 4 pokazuje bez wątpienia, że podczas badań opisanych w rozprawie wykonano znaczną pracę, sensownie zaplanowaną i jasno opisaną, a Autor rozprawy jest osobą o wysokich kompetencjach technicznych i świetnej orientacji w temacie.

Piąta część rozprawy, o objętości prawie 100 stron, zawiera opis eksperymentów symulacyjnych i pomiarowych wykonanych przez Autora rozprawy. Ten rozdział, zdaniem Recenzenta, jest zdecydowanie zbyt długi, a rozprawa zyskałaby na wartości gdyby objętość tego rozdziału zredukowano o połowę. Na przykład, szereg wielostronicowych tabel umieszczonych w rozprawie na stronach 130-158 można by zastąpić jedynie ich przykładowymi fragmentami, pozostawiając przy tym w tekście ich analizę i syntezę, a także wnioski wynikające z porównania metod. W rozprawie do badań wykorzystano zarówno ruch z sieci rzeczywistych jak i ruch generowany w symulatorze. Wyniki zbiorcze badań opisanych w rozprawie podano na wykresach przeglądowych 5.63-5.67, a zaraz za nimi podano ich analizę oraz wnioski. Co do ich treści i formy Recenzent nie ma zastrzeżeń. Wynika z nich, że w kontekście danych użytych w rozprawie zaproponowana przez Autora metoda BotTROP detekcji działania sieci typu botnet jest znacząco lepsza od opisywanej w literaturze metody BotGAD.

Ostatni, szósty rozdział rozprawy zawiera podsumowanie badań i wnioski z nich wynikające. Z jednej strony, co dla Recenzenta jest nieco zaskakujące, dopiero tam umieszczono szereg ważnych stwierdzeń wyjaśniających ważne założenia badawcze, m.in. informację o tym, że zaproponowany przez Autora algorytm BotTROP jest modyfikacją znanego z literatury algorytmu BotGAD oraz wskazanie na elementy tej modyfikacji. Te informacje, zdaniem Recenzenta, lepiej byłoby *explicite* umieścić dużo wcześniej, np. w Rozdziale 3 rozprawy. Z drugiej strony, wnioski z wykonanych badań podane przez Autora w podsumowaniu są czytelne, zwięzłe i logiczne. Może warto byłoby jeszcze w tym rozdziale, jak to jest w zwyczaju większości doktorantów, dodać także informację o potencjalnych obszarach dalszych badań, kwestiach czekających na rozwiązanie.

Na zakończenie warto dodać, że rozprawa napisana jest w języku angielskim, co zawsze stanowi dodatkowe wyzwanie dla Autora. Doktorant bardzo dobrze poradził sobie z tą kwestią, pracę czyta się bez problemów. Recenzent zauważył wprawdzie w rozprawie kilka, nieuniknionych zapewne, błędów redakcyjnych, ale pomimo tego ten aspekt rozprawy Recenzent ocenia bardzo wysoko.

Podsumowując, w odczuciu Recenzenta, rozprawa opisuje ważne badania, jest wartościowa i poprawnie wykonana i spełnia wszystkie wymagania stawiane rozprawom doktorskim przez obowiązujące przepisy.

Witold Kordan