dr hab. Jan Bazan, prof. UR
Uniwersytet Rzeszowski,
Wydział Matematyczno-Przyrodniczy
ul. Pigonia 1, 35-310 Rzeszów
bazan@ur.edu.pl

1 września 2015 r.

Recenzja rozprawy doktorskiej
mgr. inż. Przemysława Berezińskiego
zatytułowanej:
Detekcja anomalii w ruchu sieciowym z wykorzystaniem miar entropijnych

1. Problem badawczy i jego znaczenie

Rozprawa doktorska dotyczy problemu detekcji anomalii w obszarze wykrywania włamań sieciowych. Jest to dobrze znany w literaturze problem naukowy, a metody jego rozwiązania znajdują się w centrum badań wielu silnych ośrodków badawczych na świecie. Tak duże zainteresowanie tym problemem wynika z faktu, że liczba przeprowadzanych ataków cybernetycznych za pomocą specjalistycznego oprogramowania jest wysoka i rośnie z roku na rok. Tymczasem szkody powodowane przez takie oprogramowanie dla rozmaitych organizacji nogą być bardzo bolesne, gdyż obejmują np. utratę danych, reputacji lub środków finansowych. Szczególnie dotyczy to specjalnego rodzaju ataku sieciowego zwanego atakiem botnetów, który znajduje się w centrum uwagi autora pracy. Typowo, botnet to grupa zainfekowanych hostów (botów) sterowanych przez przestępców cybernetycznych w celu uzyskania korzyści finansowych. Botnety są także wykorzystywane w wojnie cybernetycznej do sabotażu i szpiegostwa.

W rozprawie podjęto wspomniany wyżej problem detekcji anomalii wykrywania włamań sieciowych, przy czym proponowane w pracy podejście wykorzystuje miary entropijne. Miary te były wprawdzie już wcześniej używane do wykrywania zagrożeń cybernetycznych, ale do tej pory nie stosowano ich do detekcji złośliwego oprogramowania typu botnet.

Ogólnie można stwierdzić, że problem wykrywania zagrożeń cybernetycznych traktowany jest w pracy jako problem aproksymacji pojęć lub klas decyzyjnych, przy czym aproksymowane klasy decyzyjne dotyczące zagrożeń sieciowych aproksymowane są w oparciu o dobrane cechy (atrybuty) wyliczane w oparciu o obserwowane parametry ruchu sieciowego. Dlatego metodologia badań naukowych opisanych w rozprawie opiera się na następujących, dobrze znanych z eksploracji danych etapach:

1. ekstrahowanie przypadków ruchu sieciowego z dostępnych danych o tym ruchu,
2. etykietowanie przypadków treningowych i testowych na przynależność do klas decyzyjnych,
3. ekstrahowanie cech potrzebnych do aproksymacji klas decyzyjnych,
4. konstruowanie klasyfikatora aproksymującego klasy decyzyjne,
5. testowanie jakości skonstruowanego klasyfikatora.

Warto tutaj podkreślić, że główne wyniki rozprawy dotyczą kroku trzeciego, tzn. innowacyjnych metod ekstrakcji cech, które pozwoliły na skonstruowanie efektywnego klasyfikatora.

2. Struktura pracy

Rozdział 1 to wprowadzenie obejmujące ogólne przedstawienie motywacji, problemu badawczego, celu pracy i opisu wkładu autora w aktualny stan wiedzy. Natomiast rozdział 2 zawiera przegląd aktualnego stanu wiedzy w dziedzinie wykrywania anomalii sieciowych ze szczególnym naciskiem na metody ściśle związane z proponowanym podejściem. W Rozdziale 3 przedstawiono opis proponowanej metody. Natomiast rozdział 4 przybliża teorię związaną z miarami entropijnymi oraz zawiera porównanie miar Shannona, Renyiego i Tsallisa na podstawie eksperymentów symulacyjnych. W rozdziale 5 zaprezentowano koncepcję zbierania i analizy ruchu sieciowego. Rozdział 6 przedstawia architekturę proponowanej metody wraz z algorytmem działania, a także wyniki implementacji. Rozdział 7 opisuje zbiór danych przygotowany na potrzeby oceny skuteczności metody. Wreszcie rozdział 8 zawiera ocenę skuteczności wskazań za pomocą standardowych i autorskich miar oraz wyniki korelacji mające na celu wskazanie właściwego zbioru parametrów dla entropii oraz właściwego zbioru cech ruchu sieciowego dla skutecznego wykrywania anomalii sieciowych. Na koniec, rozdział 9 stanowi podsumowanie rozprawy i przedstawia kierunki dalszych prac.

3. Wkład autora

Choć w literaturze można znaleźć opisy licznych podejść do rozwiązania problemu detekcji anomalii sieciowych, to pojawiające się nowe zastosowania związane z detekcją nowych, coraz bardziej wyrafinowanych włamań sieciowych powodują, że problem ten znajdują się ciągle w centrum badań wielu silnych ośrodków badawczych na świecie. Natomiast opracowanie nowych metod detekcji aktualnych zagrożeń i wykazanie skuteczności tych metod w praktycznych zastosowaniach do obrony przed tymi zagrożeniami, ma kluczowe znaczenie dla bezpieczeństwa systemów informatycznych niezbędnych do poprawnego funkcjonowania i rozwoju rozmaitych przedsiębiorstw, w tym takich, które mają duży wpływ na bezpieczeństwo kraju (np. systemy informatyczne wykorzystywane przez rząd, policję, wojsko, służby ratownicze, banki i inne instytucje finansowe).

Obecnie, jednym z głównych tego typu zagrożeń dla bezpieczeństwa jest oprogramowanie typu botnet. Głównym celem rozprawy było pokazanie, że wykorzystanie miar entropijnych pozwala na efektywną detekcję złośliwego oprogramowania typu botnet w sieciach lokalnych, a ponadto takie podejście jest znacznie lepsze od wcześniej znanych podejść bazujących na tzw. sygnaturach.

Dla osiągnięcia tego celu zaprojektowano, zaimplementowano i zweryfikowano praktycznie z użyciem zbiorów danych autorską metodę bazującą na parametryzowanych entropiach i nadzorowanym uczeniu maszynowym z użyciem programu WEKA. Samą weryfikację metody wykonano na podstawie własnego, reprezentatywnego zbioru danych, jako że dostępne zbiory okazały się nierealistyczne, niekompletne i przestarzałe. Dodatkowo, dokonano analiz pod kątem

właściwych wartości parametrów, stosownych cech ruchu sieciowego i odpowiedniego klasyfikatora dla zaproponowanej metody.

Badania skuteczności wykazały, że metoda wykorzystująca parametryzowaną entropię Renyiego lub Tsallisa wraz z klasyfikatorem bazującymi na regresji logistycznej pozwala na skuteczne wykrywanie anomalii związanych ze złośliwym oprogramowaniem typu botnet przy jednoczesnym zachowaniu niskiego poziomu fałszywych alarmów. Jednocześnie pokazano, że dla problemu detekcji tego rodzaju złośliwego oprogramowania, detekcja bazująca na entropii Shannona lub podejściu wolumenowych (bazującym na prostych licznikach) okazuje się nieskuteczna.

Podsumowując, główne wyniki pracy są następujące.

1. Opracowanie koncepcji i wykonanie implementacji autorskiej metody detekcji anomalii w ruchu sieciowym o nazwie *Anode* bazującej na miarach entropijnych, która cyklicznie ze stały oknem czasowym analizuje ruch sieciowy w formie przepływów, w celu detekcji i klasyfikacji występujących w nim anomalii. W metodzie tej na podstawie przepływów tworzone są rozkłady cech ruchu sieciowego np. adresów czy portów, które są następnie agregowane do postaci liczbowej za pomocą parametryzowanych miar entropijnych. Najpierw detektor anomalii jest uczony w oparciu o dany ruch treningowy dla którego wyliczane są cechy (atrybuty warunkowe). Następnie detektor może być jest testowany na danych testowych, przy czym klasyfikacja odbywa się za pomocą popularnych algorytmów takich jak drzewa decyzyjne, sieci bayesowskie czy regresja logistyczna.

2. Wygenerowanie na potrzeby rozprawy nowego zbioru danych, zawierającego rzeczywisty ruch połączony z syntetycznymi anomaliami charakterystycznymi dla działania złośliwego oprogramowania typu botnet. Nowe dane wygenerowano ze względu na brak publicznie dostępnych danych spełniających podstawowe kryteria, takie jak aktualność, poprawność i kompletność. Było to niezbędne do oceny skuteczności prezentowanej metody. Wykonany zbiór zawiera rzeczywisty ruch sieciowy wraz z syntetycznymi anomaliami wygenerowanymi na podstawie trzech realistycznych scenariuszy zachowania złośliwego oprogramowania. Do realizacji zadania opracowano statystyczny generator anomalii modelujący ruch sieciowy.

3. Wykonanie serii eksperymentów mających na celu wybór odpowiednich cech ruchu sieciowego i odpowiednich wartości parametru α dla entropii Renyiego i Tsallisa. Na podstawie przeprowadzonych eksperymentów wskazano deterministyczny dla detekcji anomalii zbiór wartości parametrów α dla entropii. Ponadto wykazano, że zaproponowany zbiór cech ruchu sieciowego nie jest nadmiarowy, gdy nie istnieje dla nich silna korelacja wartości entropii.

4. Wykonanie serii eksperymentów mających na celu zbadanie skuteczności zaproponowanej metody i porównanie jej z metodą bazującą na entropii Shannona oraz metodą bazująca na analizie wolumenu ruchu. Do oceny skuteczności posłużono się typowymi miarami takimi jak uśrednione Accuracy i FPR (ang. False Positive Rate) oraz autorską miarę uśredniającą krzywe ROC. Wykazano, że zaproponowana metoda pozwala osiągnąć zadowalającą skuteczność wykrywania charakterystycznych dla botnetów anomalii przy zachowaniu relatywnie niskiego

poziomu fałszywych alarmów. Konkurencyjne metody bazujące na entropii Shannona i miarach wolumenu okazały się znacznie mniej efektywne. Oceniono, że dla proponowanego podejścia wykorzystanie klasyfikatora opartego na regresji logistycznej pozwala na osiągnięcie najlepszych wyników.

Moim zdaniem, spośród powyższych wyników na szczególną uwagę zasługuje zaproponowanie przez autora miar entropijnych, które okazały się bardzo użyteczne do percepcji anomalii na testowym zbiorze danych. Miary te mogą okazać się bardzo potrzebne do przyszłych zastosowań związanych z detekcją nowych, jeszcze bardziej wyrafinowanych włamań sieciowych.

4. Poprawność

Z formalnego i matematycznego punktu widzenia rozprawa nie budzi zastrzeżeń recenzenta.

Podczas lektury rozprawy nasuwają się jednak pewne drobne uwagi, które można traktować jako sformułowanie pewnych mankamentów lub sugestii co do dalszych prac. Kilka tych uwag podaję poniżej.

1. W całej pracy prawie nie pojawiają się formalne opisy algorytmów wyspecyfikowane np. w postaci listy kroków lub pseudokodu. Fakt ten może budzić zdziwienie, gdyż praca dotyczy przecież konstruowania algorytmów eksploracji danych.
2. Z informatycznego punktu widzenia, mankamentem pracy jest prawie całkowicie brak dyskusji na temat złożoności obliczeniowej proponowanych podejść. W związku z tym Autor praktycznie nie odniósł się do problemu skalowalności zaproponowanych algorytmów. Ta sprawa powinna zostać wyjaśniona podczas obrony rozprawy.
3. Pewną słabością metody prezentowanej w pracy jest to, że opiera się ona na ręcznym definiowaniu przez eksperta modeli entropijnych. Tymczasem w praktyce ekspert często nie będzie wstanie podać wszystkich użytecznych modeli. Zdaniem recenzenta, dobrze by było pomyśleć o mechanizmach automatycznego dobierania użytecznych cech na potrzeby aproksymacji klas decyzyjnych opisujących anomalie w ruchu sieciowym.
4. W pracy rozpatrzono szereg scenariuszy dokonywania włamań i pokazano, że przedstawione metody nadają się dobrze do ich rozpoznawania. Nasuwa się jednak pytanie, czy metody te będą równie skuteczne dla innych schematów włamań, a jeśli nie, to czy istnieje jakaś metoda automatycznej adaptacji tych metod do innych schematów lub innych typów anomalii.
5. Drobnym, ale istotnym mankamentem pracy jest to, że do budowy klasyfikatorów Autor używał jedynie algorytmów z biblioteki WEKA. Jest to wprawdzie bardzo znana biblioteka, zawierająca wiele użytecznych algorytmów, jednak jest wiele innych bibliotek i systemów do konstrukcji klasyfikatorów, które można by było tutaj przetestować (darmowych i komercyjnych). Ktoś mógłby powiedzieć, że nie było takiej potrzeby, ponieważ metody z WEKA dały już bardzo dobre wyniki. Jednak trzeba pamiętać, że nie istnieje metoda tworzenia klasyfikatora dobra dla wszystkich danych (zasada *no free lunch*). Dlatego efektywna detekcja przyszłych włamań może wymagać użycia innego klasyfikatora (np. opartego na całkiem innym paradygmacie). Ponadto, zdaniem recenzenta, na potrzeby tak złożonego środowiska eksperymentalnego jakie powstało na potrzeby rozprawy, lepiej by było, aby głównym klasyfikatorem używanym do eksperymentów

był autorski klasyfikator, który mógłby być łatwo dopasowywany do potrzeb analizy danych związanych z rozprawą.

6. Na koniec warto skomentować fakt, że wspomniana metoda polega na tym, że predykcja anomalii odbywa się po zarejestrowaniu całego okna czasowego. Tymczasem w praktycznych zastosowaniach może pojawić się potrzeba szybszego reagowania na anomalię lub jej brak. Mam tutaj na myśli szybką klasyfikację testowanego okna jako bezpieczne lub niebezpieczne (jeszcze przed zebraniem informacji o całym testowanym oknie czasowym). W rozprawie nie są rozważane tego typu metody. Jednak w kontekście przyszłych zastosowań i projektów związanych z potrzebą szybkiej analizy bardzo dużych danych testowych, tego rodzaju podejście może być konieczne, celem wstępnego odrzucenia bardzo dużej liczby przepływów lub pakietów, które nie muszą już być dalej analizowane głównymi metodami opisanymi w rozprawie.

5. Wiedza kandydata

W rozprawie Autor zamieścił obszerny przegląd aktualnego stanu wiedzy w dziedzinie wykrywania anomalii sieciowych ze szczególnym naciskiem na metody ściśle związane z proponowanym podejściem (głównie w rozdziale 2). Opisy te zostały wykonane z wysoką starannością i z licznymi odwołaniami do literatury. Bez wątpienia świadczą one o dużej wiedzy kandydata. Chodzi tutaj o wiedzę z zakresu sieci komputerowych, matematycznych metod ekstrakcji cech ruchu sieciowego oraz konstrukcji i testowania klasyfikatorów. Należy tutaj mocno podkreślić, że napisanie rozprawy wymagało wcześniejszego skonstruowania skomplikowanego środowiska eksperymentalnego związanego choćby z takimi działaniami jak wygenerowanie danych eksperymentalnych, ekstrahowanie zaetykietowanie przypadków treningowych i testowych obiektów, ekstrahowanie cech potrzebnych do aproksymacji klas decyzyjnych, konstruowanie klasyfikatora aproksymującego klasy decyzyjne oraz testowanie jakości skonstruowanego klasyfikatora. Autor aktywnie uczestniczył w wykonaniu tego środowiska, które powstało w Wojskowym Instytucie Łączności w Zegrzu. Prace te były prowadzone w ramach projektu SECOR, finansowanym przez Narodowe Centrum Badań i Rozwoju.

Bibliografia jest wystarczająca i nie budzi zastrzeżeń.

6. Podsumowanie

Uzyskane wyniki są interesujące zarówno z teoretycznego, jak i praktycznego punktu widzenia. Dlatego niezależnie od wspomnianych wyżej drobnych mankamentów, uważam pracę za bardzo wartościową. Autor wykazał bardzo dobre opanowanie wielu różnorodnych technik matematycznych i informatycznych. Sposób wykorzystania tych technik wskazuje na rzetelne opanowanie przez Niego warsztatu naukowego.

Biorąc pod uwagę opinie zaprezentowane w poprzednich punktach i wymagania zdefiniowane przez artykuł 13 Ustawy z dnia 14 marca 2003 r. o stopniach naukowych i tytule naukowym (z

późniejszymi zmianami) [1] moja ocena rozprawy pod względem trzech podstawowych kryteriów jest następująca:

A. Czy rozprawa zawiera oryginalne rozwiązanie problem naukowego? (wybierz jedną opcję stawiając znak **X**)

[X]	[ ]	[ ]	[ ]	[ ]
Zdecydowanie TAK	*Raczej TAK*	*Trudno powiedzieć*	*Raczej NIE*	*Zdecydowanie NIE*

B. Czy po przeczytaniu rozprawy zgadzasz się, że kandydat posiada ogólną wiedzę teoretyczną w dyscyplinie?

[X]	[ ]	[ ]	[ ]	[ ]
Zdecydowanie TAK	*Raczej TAK*	*Trudno powiedzieć*	*Raczej NIE*	*Zdecydowanie NIE*

C. Czy kandydat umiejętność samodzielnego prowadzenia pracy naukowej?

[X]	[ ]	[ ]	[ ]	[ ]
Zdecydowanie TAK	*Raczej TAK*	*Trudno powiedzieć*	*Raczej NIE*	*Zdecydowanie NIE*

Ponadto, mając na uwadze osiągnięcia publikacyjne kandydata (7 publikacji, z których jedna w czasopiśmie z listy A, a druga w materiałach konferencji międzynarodowej CISIM 2014, gdzie otrzymała nagrodę za najlepszy artykuł), wysoką wartość techniczną przedstawionej rozprawy, której napisanie wymagało wykorzystania złożonego środowiska sprzętowo-programowego oraz realne zastosowanie zaproponowanych w rozprawie metod w systemie komputerowym tworzonym w ramach projektu finansowanego przez NCBiR , rekomenduję wyróżnienie rozprawy doktorskiej.

Jan G. Baran

Podpis

[1] http://www.nauka.gov.pl/g2/oryginal/2013_05/b26ba540a5785d48bee41aec63403b2c.pdf