Akademia Górniczo-Hutnicza
im. Stanisława Staszica w Krakowie

Wydział Elektrotechniki, Automatyki, Informatyki i Inżynierii Biomedycznej

KATEDRA INFORMATYKI STOSOWANEJ

AUTOREFERAT ROZPRAWY DOKTORSKIEJ

DETEKCJA ANOMALII W RUCHU SIECIOWYM Z WYKORZYSTANIEM MIAR ENTROPIJNYCH

ENTROPY-BASED NETWORK ANOMALY DETECTION

MGR INŻ. PRZEMYSŁAW BEREZIŃSKI

PROMOTOR:
dr hab. Marcin Szpyrka, prof. AGH

PROMOTOR POMOCNICZY:
ppłk dr inż. Bartosz Jasiul

Kraków 2015

Streszczenie

Przedstawiona rozprawa doktorska dotyczy detekcji anomalii w obszarze wykrywania włamań sieciowych. Tematyka ta jest bardzo ważna, gdyż liczba przeprowadzanych ataków cybernetycznych jest alarmująco wysoka i co gorsza rośnie z roku na rok. Jest to częściowo spowodowane tym, że powszechnie stosowane rozwiązania ochrony cybernetycznej są nieskuteczne w detekcji aktualnego złośliwego oprogramowania. Szkody powodowane przez takie oprogramowanie, szczególnie to działające w ramach botnetów, obejmują utratę danych, reputacji czy pieniędzy. Typowo, botnet to grupa zainfekowanych hostów (botów) sterowanych przez przestępców cybernetycznych w celu uzyskania korzyści finansowych. Obecnie botnety są także wykorzystywane w wojnie cybernetycznej do sabotażowania czy też szpiegostwa.

Detekcja anomalii sieciowych to temat szeroki i mocno eksplorowany. Pierwsze metody pojawiły się prawie 40 lat temu, ale problem znalezienia metod generycznych nie został do tej pory rozwiązany. Istnieją metody dedykowane do określonych typów anomalii związanych ze złośliwym oprogramowaniem, w tym metody bazujące na miarach entropijnych, które ostatnio cieszą się dużą popularnością. Nikt do tej pory nie zastosował ich jednak do detekcji złośliwego oprogramowania typu botnet.

Głównym celem niniejszej rozprawy jest dowiedzenie, że wykorzystanie miar entropijnych pozwala na detekcję złośliwego oprogramowania typu botnet w sieciach lokalnych i podejście to może być stosowane jako uzupełnienie obecnie wykorzystywanych metod bazujących na sygnaturach. W celu potwierdzenia postawionej tezy w rozprawie przedstawiono oryginalny wkład w obecny stan wiedzy. Porównano kilka miar entropijnych pod kątem ich zastosowania w detekcji anomalii sieciowych. Zaproponowano, zaimplementowano i zweryfikowano autorską metodę bazującą na parametryzowanych entropiach i nadzorowanym uczeniu maszynowym. Weryfikację 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 parametryzowana entropie Renyiego lub Tsallisa wraz z klasyfikatorem bazującym na regresji logicznej pozwala na skuteczne wykrywanie anomalii związanych ze złośliwym oprogramowaniem typu botnet przy jednoczesnym zachowaniu niskiego poziomu fałszywych alarmów. Odpowiadające detekcja bazującą na entropii Shannona lub podejściu wolumenowych bazującym na prostych licznikach takich jak liczba przepływów, pakietów i bajtów okazuje się nieskuteczna.

Abstract

This Dissertation focuses on application of anomaly detection in the field of network intrusion detection. This is a very important issue as the number of cyber-attacks is alarmingly high and to make things worse it increases each year. Partially, this is due to the fact that widely used security solutions are ineffective against modern malicious software (malware). Damage from a malware, especially this which acts in botnets, can take many serious forms including loss of important data, reputation or money. Typically, botnet is a group of infected hosts (bots) operated by cyber-criminals who are focused on making money. Recently, botnets are also used in a cyber warfare to conduct sabotage and espionage.

Network anomaly detection is a very broad and heavily explored area. The first methods were proposed almost 40 years ago but the problem of finding a generic network anomaly detection method still remains unsolved. Dedicated methods for different types of network anomalies caused by malware can be found in the literature. Recently entropy-based methods for detection of various types of anomalies have gained a lot of attention. The use of entropy to detect botnet-like malware has not been investigated so far.

The main goal of this Dissertation is to prove that entropy-based approach is suitable for detection of modern botnet-like malware in local networks and thus it can be used to complement existing signature-based solutions. In order to reach this goal and prove the claim of the Thesis, the Dissertation makes several original contributions. Comparison of different entropy measures to use in network anomaly detection is provided. Original network anomaly detection method based on parameterized entropies and supervised machine learning is proposed, implemented and verified with the representative semi-synthetic dataset prepared for this purpose due to the lack of realistic, complete and up-to-date datasets available. Moreover, analysis of proper parameters, suitable network features and right classifier to use with the method is conducted. Results of the verification shows that the proposed method with parameterized Renyi or Tsallis entropy acting together with classifier based on logistic regression allows to detect botnet-like malware with satisfactory level of detection rate while keeping low rate of false alarms. Comparable detection based on Shannon entropy or volume counters (number of flows, packets and bytes) turns out to be ineffective.

Cel pracy

Głównym celem pracy jest dowiedzenie, że: *podejście bazujące na miarach entropijnych jest odpowiednie do wykrywania anomalii charakterystycznych dla złośliwego oprogramowania typu botnet na podstawie analizy ruchu w sieciach lokalnych*. W szczególności celem było znalezienie odpowiedzi na następujące pytania:

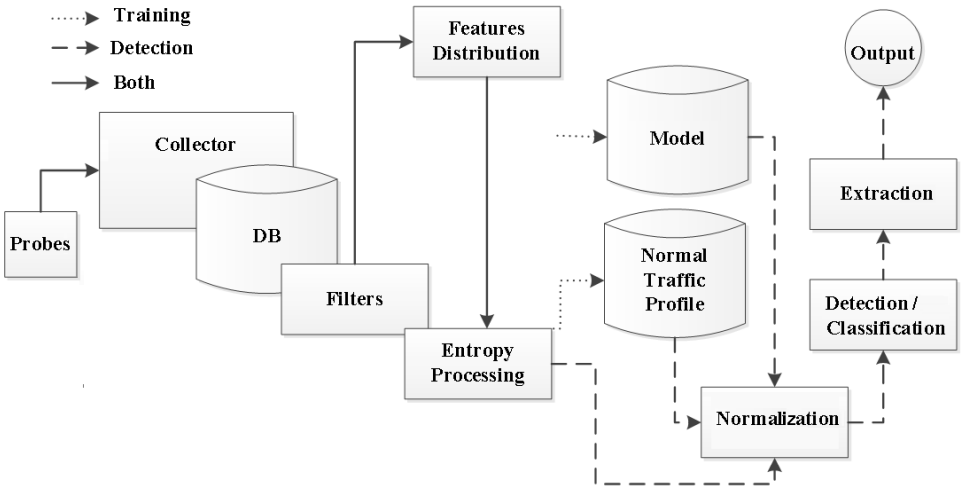
- Czy miary entropijne są użyteczne w kontekście detekcji anomalii sieciowych?
- Czy jest możliwa z wykorzystaniem tych miar skuteczna detekcja i klasyfikacja małych i rozciągniętych w czasie anomalii charakterystycznych dla złośliwego oprogramowania typu botnet?
- Czy podejście bazujące na entropii cech ruchu sieciowego jest skuteczniejsze od tradycyjnego podejścia bazującego na wolumenie?
- Czy wykorzystanie parametrycznych entropii w miejsce powszechnie stosowanej entropii Shannona pozwala na uzyskanie lepszych wyników?
- Jaki jest właściwy zbiór wartości parametru α dla entropii Renyiego i Tsallisa, aby skutecznie wykrywać anomalie sieciowe?
- Jakie cechy ruchu sieciowego należy brać po uwagę, aby skutecznie wykrywać szerokie spektrum anomalii charakterystycznych dla złośliwego oprogramowania typu botnet?
- Jakie metody klasyfikacji działają najlepiej z proponowanym podejściem?

Zawartość pracy

Z podanych wyżej celów pracy wynika jej struktura.
Rozdział 1 to wprowadzenie obejmujące przedstawienie motywacji, zakresu i problemu badawczego, celu pracy, oryginalnego wkładu w aktualny stan wiedzy i listy zagadnień świadomie pominiętych w pracy.
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 ogólny opis proponowanej metody, wymieniono jej cechy oraz dokonano ogólnej klasyfikacji.
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. Przedstawiono cechy dostępnych podejść i opisano pewne słabości z nimi związane. Przedstawiono, również szczegółowo rozwiązanie wykorzystane w niniejszej pracy.
Rozdział 6 przedstawia architekturę proponowanej metody wraz z algorytmem działania. Zaprezentowano tu także wyniki implementacji.
Rozdział 7 dotyczy zbioru danych opracowanego na potrzeby oceny skuteczności metody.
Rozdział 8 zawiera ocenę skuteczności wskazaną za pomocą standardowych i autorskich miar oraz wyniki korelacji mające na celu wskazanie właściwego zbioru parametrów α dla entropii oraz właściwego zbioru cech ruchu sieciowego dla skutecznego wykrywania anomalii sieciowych.
Rozdział 9 stanowi podsumowanie rozprawy i przedstawia kierunki dalszych prac.

Najważniejsze wyniki

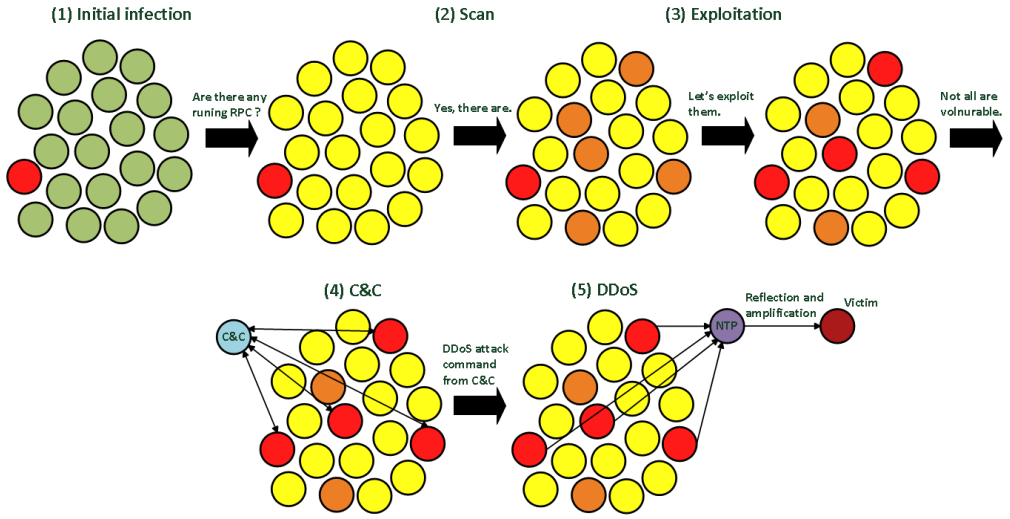
W celu zrealizowania zamierzeń postawionych w pracy wykonano następujące elementy.
1. Koncepcję i implementację autorskiej metody detekcji anomalii w ruchu sieciowym bazującej na miarach entropijnych.



Rysunek 1: Zasada działania detektora *Anode*

Zaproponowane rozwiązanie nazwane *Anode* cyklicznie (stałe okno czasowe) analizuje ruch sieciowy w formie przepływów, w celu detekcji i klasyfikacji występujących w nim anomalii. 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. Wyróżniamy dwa tryby pracy detektora: uczenie i detekcja. W trybie uczenia budowany jest profil legalnego ruchu poprzez zapisywanie brzegowych wartości entropii odnotowanych w przesuwnym oknie o zadanej długości. W fazie tej, dostarczany jest też model anomalii zawierający ich charakterystykę entropijną. Model jest niezależny od ruchu legalnego. W fazie detekcji aktualne wskazania entropii dla poszczególnych rozkładów cech są w pierwszej kolejności normalizowane z wykorzystaniem profilu i następnie porównywane z modelem. Klasyfikacja odbywa się za pomocą popularnych algorytmów takich jak drzewa decyzyjne, sieci Bayesowskie czy regresja logiczna. Szczegóły anomalii takie jak lista związanych adresów czy portów są ekstrahowane z przepływów na podstawie największego wkładu w wartość entropii.

2. Zbiór danych testowych zawierający rzeczywisty ruch połączony z syntetycznymi anomaliami charakterystycznymi dla działania złośliwego oprogramowania (ang. *malware*) typu botnet.



Rysunek 2: Jeden z zaimplementowanych w zbiorze danych scenariuszy zachowania złośliwego oprogramowania

Ze względu na brak publicznie dostępnych danych spełniających podstawowe kryteria, takie jak aktualność, poprawność i kompletność niezbędne okazało się wykonanie własnego reprezentatywnego zbioru danych 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. Serię eksperymentów mających na celu wybór odpowiednich cech ruchu sieciowego i odpowiednich wartości parametru α dla entropii Renyiego i Tsallisa.

Tabela 1: Wyniki korelacji wartości entropii dla różnych cech

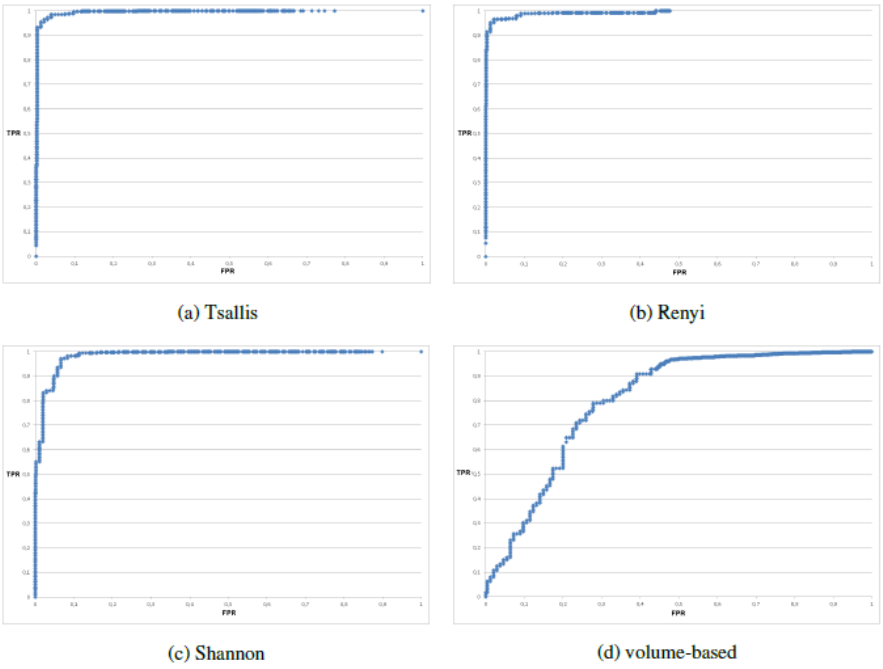
		src ip	dst ip	src port	dst port	in-degree	out-degree
Pearson	src ip	1	-0.07	-0.34	-0.02	-0.07	0.44
	dst ip	-	1	-0.29	0.05	0.08	-0.28
	src port	-	-	1	-0.42	0.59	-0.04
	dst port	-	-	-	1	-0.39	0.01
	in-degree	-	-	-	-	1	0.03
	out-degree	-	-	-	-	-	1

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, gdyż nie istnieje dla nich silna korelacja wartości entropii.

4. Serię eksperymentów mających na celu zbadanie skuteczności zaproponowanej metody i porównanie jej z metodą bazującą na entropii Shannona oraz metodą bazującą na analizie wolumenu ruchu.

Tabela 2: Uśrednione wyniki skuteczności klasyfikacji dla jednego z testowych scenariuszy

		ZeroR	Bayes Network	Decision Tree	Random Forest	Simple Logistic
Accuracy	Tsallis	0.68	0.83	0.83	0.87	0.93
	Renyi	0.68	0.83	0.83	0.85	0.94
	Shannon	0.68	0.76	0.80	0.85	0.90
	volume-based	0.68	0.68	0.62	0.65	0.66
FPR	Tsallis	0.68	0.13	0.17	0.22	0.10
	Renyi	0.68	0.13	0.16	0.22	0.06
	Shannon	0.68	0.23	0.16	0.22	0.13
	volume-based	0.68	0.68	0.57	0.45	0.67



Rysunek 3: Porównanie skuteczności metod za pomocą uśrednionej miary ROC

Do oceny skuteczności posłużono się typowymi miarami takimi jak uśrednione Accuracy i FPR (ang. *False Positive Rate*) oraz autorską miarą uśredniającą krzywe ROC (ang. *Receiver Operating Characteristics*). Wykazano, że zaproponowana metoda pozwala osiągnąć zadowalającą skuteczność wykrywania charakterystycznych dla botnetów anomalii (do 94%) przy zachowaniu relatywnie niskiego poziomu fałszywych alarmów (6%). Konkurencyjne metody bazujące na entropii Shannona i miarach wolumenu okazały się znacznie mniej efektywne. Oceniono, że dla proponowanego podejścia wykorzystanie klasyfikatora SimpleLogistic pozwala na osiągnięcie najlepszych wyników.

Podsumowanie

Główny cel pracy osiągnięto. Dowiedziono tezę, że podejście bazujące na miarach entropijnych jest odpowiednie do wykrywania anomalii charakterystycznych dla złośliwego oprogramowania typu botnet na podstawie analizy ruchu w sieciach lokalnych. Do osiągnięcia tego celu opracowano autorska metodę bazującą na entropii Renyiego i Tsallisa. Zaimplementowano rozwiązanie i przetestowano je pod kątem skuteczności. Wybrano odpowiedni zestaw wartości parametru α dla wykorzystywanych entropii. Zaproponowano szeroki zakres cech ruchu sieciowego dla metody i potwierdzono zasadność ich stosowania. Wykazano wyższość proponowanego rozwiązania nad metodami bazującymi na entropii Shannona i miarach wolumenowych. Empirycznie dobrano odpowiedni dla podejścia klasyfikator.
W pracy zrealizowano także kilka celów pobocznych: wykonano reprezentatywny zbiór danych do oceny skuteczności proponowanej metody, opracowano narzędzie pozwalające w statystyczny sposób modelować anomalie sieciowe, a także zaproponowano autorską miarę oceny skuteczności klasyfikacji typu *multi-class*.
Autor planuje dalsze badania nad metodą, a w szczególności:

- zastosowanie podejścia wykorzystującego zbiór klasyfikatorów dedykowanych do wykrywania określonego typu anomalii;
- zbadanie możliwości zastosowanie podejścia pozwalającego przypisać badaną próbkę ruchu do więcej niż jednej klasy jednocześnie;
- rozwinięcie i upublicznienie wykonanego zbioru danych.