Jurnal
Teknologi

Full Paper

AN INTELLIGENT NETWORK INTRUSION DETECTION USING DATA MINING TECHNIQUES

Mohd Afizi Mohd Shukran*, Kamaruzaman Maskat

Department of Computer Science, Faculty of Science & Technology Defence, Universiti Pertahanan Nasional Malaysia, 57000 Kuala Lumpur, Malaysia

Article history
Received
1 June 2015
Received in revised form
13 July 2015
Accepted
20 August 2015

*Corresponding author
afizi@upnm.edu.my

Graphical abstract

Abstract

Network Intrusion Detection is to detect malicious attacks to the networks for different uses from military to enterprise. Currently available approaches either rely on the known network attacks or have high proportion of normal network traffics that were erroneously reported as anomalous traffics. The aim of this paper is to develop an efficient algorithm for intrusion detection without prior knowledge of network attacks. Uniquely, our approach will integrate a newly developed data mining technique for data feature classification with techniques commonly used for human detection. The key idea is to achieve on-line and automated learning of new attacks for precise and real-time intrusion detection.

Keywords: Network intrusion, network security, data mining, classification, optimization

Abstrak

Rangkaian Pengesanan Pencerobohan adalah untuk mengesan serangan berniat jahat kepada rangkaian untuk kegunaan yang berbeza dari tentera kepada industri. Pada masa ini pendekatan disediakan sama ada bergantung kepada rangkaian serangan dikenali atau mempunyai nisbah yang tinggi trafik rangkaian biasa yang tersilap dilaporkan sebagai trafik janggal. Tujuan kertas kerja ini adalah untuk membangunkan satu algoritma berkesan untuk pengesanan pencerobohan tanpa pengetahuan sebelum serangan rangkaian. Uniknya, pendekatan kami akan mengintegrasikan baru dibangunkan teknik perlombongan data untuk pengelasan ciri data dengan teknik yang biasa digunakan untuk mengesan manusia. Idea utama adalah untuk mencapai dalam talian dan pembelajaran automatik serangan baru untuk pengesanan pencerobohan tepat dan tepat masa.

Kata kunci: Pencerobohan rangkaian, keselamatan rangkaian, perlombongan data, klasifikasi, pengoptimuman

1.0 INTRODUCTION

Intrusion detection has been an active field of research for more than two decades. In 1987, Dorothy Denning published a seminar paper "An Intrusion Detection Model" [1], where he discussed various security concerns, presented a definition of Intrusion Detection and discussed different types of Intrusion Detection. Most of the contemporary computer security research work is based on the milestone established by Denning. Intrusion detection is a component of detection process. It tries to identify if a network is under attack or not. IDS are classified firstly as host IDS and network IDS based on location from which it collects data; and secondly as signature based IDS and anomaly based IDS.

The most popular approach for today's network IDS is still signature-based [2], [3]. It performs intrusion detection by searching for predefined content or a fixed sequence of bytes in a single packet. This approach works well if the patterns of attacks could be found in advance. This approach is reliable and has low false negative rates for detecting known attacks, but it cannot detect new attacks or mutations of known attacks because their fingerprints have not been discovered.

Anomaly-based detection builds models of normal behavior in a system, and attempt to identify attacks based on the deviations from the profiles of normal network activities. Anomaly-based detectors can detect new and completely unknown attacks but has high false positive rates [4].

In this paper, section II will describe about the previous works on network intrusion detection system and section III will briefly describe the proposed method. Also, section IV will discuss the findings of the research and lastly section V will conclude the findings on this paper.

2.0 RELATED WORKS

2.1 Algorithms for Network Data Analysis

Because the features are used to describe the patterns to be classified, choosing the wrong features will usually influences the results of the learning phase heavily, and thus the overall performance of the recognition system. In network intrusion detection, the features to be measured are strictly related to what kind of traffic that the IDS are going to analyze and to what kind of attacks we want to detect. The extraction of suitable features representing network connections is based on expert knowledge about the characteristics that distinguish attacks from normal connections. Base on the previous work of feature extraction for intrusion detection, three main feature sets can be used to classify each connection [5], [6]: intrinsic features, traffic features and content features. In [7], the authors used Mahalanobis distance during the detection phase for the above three types of features to calculate the similarity of new data against the pre-computed profile. They considered a single byte pattern (1-gram) of payload but they have ignored the correlation between the payloads or groups of the payloads. There exist, however, many correlations between the payloads or different groups of payloads which should not be ignored.

If we consider the Mahalanobis Distance Map (MDM) [8] for representing multi-gram data, the output matrix will have a very big dimension. This output matrix may contain thousands of dimensions. This big dimension data is not suitable and not easy to be used by the unsupervised learning methods. Therefore, in this paper, we will adopt a technique to reduce the dimension using a feature selection (FS) technique to select the useful features from MDM matrix output by eliminating irrelevant and redundant features, while maintaining or enhancing model performance.

2.2 Unsupervised Learning Vs. Supervised Learning for Intrusion Detection

In 1998, Wenk Lee *et al*. first proposed rule-based learning algorithms for supervised, host-based anomaly detection [9], and for network intrusion detection by combining with other classification and statistical techniques [10]. Other approaches include those methods using neural networks, support vector machines, nearest neighbors, and other statistical methods [11], [14], [15], [16]. The main limitation of their method is that they need to label all the training data set in order to create their classification rules. Due to this reason, the supervised approach is difficult to apply in the general case. In the real applications, we can only label a small portion of the available data for training and learning. We could not guarantee that we can label all the possible attacks which include the new attacks.

For the unsupervised anomalous detection technique, the required data does not need to be labeled and it does not require having a purely normal training set. Unsupervised anomaly detection algorithms can be performed over unlabeled data, which can be obtained easily since it is simply raw audit data collected from the system. However, there has not been much exciting work done based on unsupervised learning. The Searching-for-clusters approach is the most common unsupervised learning method for intrusion detection. It performs clustering to try to discover the inner nature of the data structure as a whole, and to divide the data into groups according to their similarities. It can partition the data set into groups so that the points in each group are as similar as possible to each other and as different as possible from points in the other groups. Although it is good to recognize unknown attack patterns, it usually has high false positive rates. We still need a lot of research in this approach if we would like to comfortably apply the unsupervised learning to intrusion detection.

In [17] and [18], the authors have reported that their unsupervised clustering algorithms based on data mining clustering techniques can have around 90% intrusion detection rate with only less than 4% false alarm rate. This stimulates us to use data mining technique to find the rules according to the centroids of the clustered results for intrusion. Other approaches such as [17] [18] did not consider further use of clustered result to find the rules. However, the centroids of clusters derived from an unsupervised learning (clustering algorithm) are discrete data. There has only very few existing data mining algorithms suitable for finding rules to classify the discrete data. Biology inspired algorithms such as Genetic Algorithms (GA) [19] and swarm-based approaches like Ant Colonies have been successfully used. The Particle Swarm Optimization (PSO) [20] has been proved to be competitive with GA in several tasks mainly in optimization areas. However, there are some shortcomings in the GA and PSO approaches such as premature convergence. Therefore, GA and PSO are not suitable to classify the discrete data sets. In this paper, we will use DIS, which has been proved to be a sufficient data mining tool for the discrete dataset, as our unsupervised learning method for rule extraction.

3.0 PROPOSED METHOD

The aim of this paper is to develop an efficient algorithm for intrusion detection without prior knowledge of network attacks. Uniquely, our approach will integrate a newly developed data mining technique for data feature classification with techniques commonly used for human detection to recognize and distinguish 'normal' and 'attack (anomalous)' patterns in a network packet. The key idea is to achieve on-line and automated learning of new attacks for precise and real-time intrusion detection. The proposed unlabeled (i.e., instances not classified as being attack or not) anomaly detection does not go through a time consuming, supervised learning process that is to predict the value of a function for any valid input object after having seen a number of training examples. Most of the existing Intrusion Detection Systems (IDSs) are using pre-defined rules (or static rules) and are based on a supervised learning which needs to label all the attack patterns in advance.

In this paper, we will apply Mahalanobis Distance Map (MDM), a pattern recognition technique that has been used by the Prof. He for human detection, to represent normal and anomalous patterns according to given network packets based on their geometrical structures [1], [2] in terms of network connections. We will then develop an unsupervised learning approach based on Discrete Intelligent Swarm (DIS), a data mining technique that was newly developed by the PROF. Yeh and Dr Chung, to find the dynamic rules for all of the attack patterns (that can be either existing or newly discovered). Unsupervised learning is distinguished from supervised learning in that the learner is given only unlabeled examples. Each connection between a pair of hosts will be viewed as an object in an image, and each image will be viewed as a pattern to be classified as normal or anomalous traffic class based upon the given information about the connections. We will use KDD Knowledge Discovery and Data Mining (KDD-99) dataset [3] as a benchmark to evaluate the robustness of our algorithms with high recognition rate and low false alarm rate (i.e., low proportion of normal network traffics that were erroneously reported as anomalous traffics). In the following, we list the objectives of this program according to two main challenges of the proposed work as follows.

<u>For network data analysis:</u>

- To develop a framework for extracting, representing and visualizing data for different applications and conditions (i.e., high-level knowledge) from a large dataset by means of pattern recognition technique (i.e., MDMs).
- To develop an intrusion detection model of single byte pattern distribution (namely, 1-gram distribution) in the payload of network packets using a correlation based feature selection algorithm based on the difference of the average MDMs of normal sample packets and anomalous packets. This model will select the important features for intrusion detection.
- To develop an intrusion detection model of two and/or multiple byte pattern distribution (namely, 2-gram and/or *n*-gram distribution) for feature selection using a correlation based feature selection algorithm based on MDMs based on the knowledge from constructing the 1-gram model.

<u>For unsupervised learning:</u>

- To develop an unsupervised training technique based on two-level learning. The first level uses a clustering technique to cluster the data into "normal" or "anomalous" based on the features selected using the MDM-based techniques. The second-level performs a dynamic rule-extraction to classify the discrete data clustered in the first-level using DIS algorithms. The two-level rule based system will then be used for intrusion detection of network packets of various types of services between the hosts.
- To develop an algorithm that maps the dynamic rules extracted to the real-time intrusion detector for the anomaly detection in order to determine the new attacks.

4.0 DISCUSSION AND FINDINGS

Information System security is important in this computer age. According to a recent survey, the rate of cyber attacks are increasing more than double every year. Attacks on the nation's computer infrastructures are becoming an increasingly serious problem. Therefore, it is important to make information systems resistant to and tolerant from such attacks. This is particularly important for computer-assisted financial transactions and for the protection of military systems. It is evident that an automatic way to perform security audit is needed. Intrusion Detection System (IDS) plays an increasingly role in our modern society. It detects and responds to inappropriate activity, computer attack and/or misuse etc. in networks and computers. Therefore, a real-time intrusion detection system will be an effective solution to detect and prevent the various attacks.

Computer networks are usually protected against attacks by a number of access restriction rules. Despite the effort devoted to carefully design of different kinds of filters, network security is very difficult to guarantee as attacks exploiting unknown bugs are always contained in computer systems and application software. IDS is usually designed inside a protected network and is looking for the known or potential threats in network traffic or audit data recorded by hosts. Traditionally available IDS systems usually compare the network data to sets of pre-defined patterns. These pre-defined pattern sets needs to be manually updated frequently by security experts to handle all kinds of attacks that they know so far. These systems require human intervention in order to operate effectively. Therefore, we really need a more advance IDS to detect the known and unknown intrusions intelligently and automatically to distinguish the normal and anomalous data with minimum human inputs. In this work, we propose a new unsupervised learning which does not need to label all the network data. The proposed system can automatically extract the rules from the input network data and those rules will automatically embed into a real-time intrusion detector to detect the new attacks.

From the previous and current research work [11-16], researchers are mainly focus on four research directions: (1) Signature-based system by comparing the signatures of the already known attacks or vulnerabilities; (2) Anomaly-based on comparing the profiles of normal network; (3) Supervised learning algorithm to classify the normal or attack (anomalous); (4) Unsupervised learning algorithm to classify the normal or attack. Most of the available IDSs are using (1) signatures and (3) supervised learning. For the (2) anomaly and (4) unsupervised learning, we still need a lot of research to overcome the limitations of them as mentioned in Section c(viii)(a) in order to get better performance than (1) and (3). In this paper, we aim at solving the problems in (2) and (4).

4.1 Innovation

We address the innovation of the proposed system in terms of the two challenges/research topics mentioned in previous section as follows.

For network data analysis

The primarily signature-based detectors fail to recognize new attacks. The other existing payload-based anomaly detectors only compare the new data sets with their pre-computed profiles, and ignore the correlation information between data sets. In this paper, the proposed pattern recognition technique use a correlation based feature selection algorithm in order to achieve higher detection accuracy rate than hand-coded signature approaches and payload-based anomaly detection techniques.

As network IDS must be able to cope with network traffic at a speed above 1GB/s without slowing down the traffic or missing intrusion relevant events, commonly available IDS works only on a subset of data such as meta-data like network packet headers [15] in order to perform intrusion detection at needed speeds but is at the cost of correctness of detection. In this paper, we will develop a real-time detection algorithm that will improve the intrusion detection accuracy by detecting data on packet payload instead of header.

A new concept will be introduced to represent network traffic/connections as objects in the images based on the concepts for human detection. Profiles for the normal and for the attack patterns will be developed for the classification of network traffic as normal or attack based on geometric structure of network connections.

Other researches (see, for example, e.g., [7], [21], [22]) do not consider the correlation between the payloads. In this paper, we will use the pattern recognition tools for human detection to represent the normal and anomalous patterns in the network traffic. We will map the transformed data to a two-dimensional image and find out all the correlation between different payloads using multi-byte pattern distribution instead of single byte (1-gram) distribution. We can easily find out the anomalous data by comparing the correlation between different groups of payload information.

For unsupervised learning

a. *Easier for the human to interpret*: The clustering results are hard for human to interpret. These difficulties make human experts hard to improve the IDS. The proposed dynamic rule extraction algorithm can provide easier human interpretability by generating rules to those domain experts for further inspection and make it easier for them to interpret the clustered results.
b. *Real-time intrusion detection*: We will utilize the rules generated by our proposed rule learning algorithm on the clustered results. Then, we will embed these rules into a real-time intrusion detector by matching the data against the rule set. This can easy be implemented on the IDS in real-time.
c. *On-line learning*: Most of the existing IDSs are only trained in the off-line mode. The real-application environment may change gradually with time so we will implement and test our system with on-line parameters to update the rules in our proposed IDS dynamically.

5.0 CONCLUSION

Most of the common intrusion detection algorithms are using supervised learning. However, they need to manually label the large volumes of network data which is difficult and extremely expensive. Also, the analysis of network traffic and audit logs is very time-consuming. In our approach, we will develop an unsupervised learning for which the data does not need to be labeled. The searching-for-clusters is the most common unsupervised learning method for intrusion detection but its clustered results are hard for human to understand as it can only show how the data group together and do not show the relationship between output parameters and input parameters. In this paper, we will design and implement the IDS using two-level unsupervised learning. We will extract the rules from the clustered results. These extracted rules can be inspected and modified by the human experts easily. The proposed new two-level unsupervised learning will be a breakthrough in both IDS and unsupervised learning research areas.

Acknowledgement

The author would like to thank Malaysia Ministry of Higher Education (MOHE) for financial assistance while conducting this project.

References

[1] Shukran, M. A. M., Chung, Y. Y., Yeh, W. C., Wahid, N., & Zaidi, A. M. A. 2011. Artificial Bee Colony Based Data Mining Algorithms for Classification Tasks. *Modern Applied Science*. 5(4): 217.

[2] Shukran, M. A. B. M., Yunus, M. S. F. B. M., Maskat, K. B., Shariff, W. S. S. B., & Ariffin, M. S. B. 2013. Pixel Value Graphical Password Scheme-Graphical Password Scheme. *Australian Journal of Basic and Applied Sciences*. 7(4): 688-695.

[3] http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html.

[4] D. E. Denning. 1987. An Intrusion-Detection Model. IEEE *Transactions on Software Engineering*. 13(2): 222–232.

[5] T. Chou, K. K. Yen, J. Luo, N. Pissinou, K. Makki. 2007. Correlation-based Feature Selection for Intrusion Detection Design. IEEE Xplore.

[6] http://www.ll.mit.edu/IST/ideval.

[7] Shukran, M. A. M., Chung, Y. Y., Yeh, W. C., Wahid, N., & Zaidi, A. M. A. 2011. Image Classification Technique using Modified Particle Swarm Optimization. *Modern Applied Science*. 5(5): 150.

[8] B. K. Sy. 2005. Signature-based Approach for Intrusion Detection. In: P. Perner, A. Imiya (eds.) LNAI, Vol. 3587. *Proceedings of the 4th Intern. Conf. on Machine Learning and Data Mining in Pattern Recognition, Leipzig, July 9-11*. 526-636,

[9] D. Brumley, J. Newsome, D. Song, H. Wang, S. jha. 2006. Towards Automatic Generation of Vulnerability-Based Signatures. *Proceedings of the IEEE Symposium on Security and Privacy (S&P'06), May*. 2-16.

[10] J. P. Anderson. 1980. Computer Security Threat Monitoring and Surveillance. Technical report, J. P. Anderson Co., Ft. Washington, Pennsylvania, Apr.

[11] K. Wang and S. Stolfo, p. Chan. 1997. Learning Patterns from Unix Process Execution Traces for Intrusion Detection. AAAI Workshop: AI Approaches to Fraud Detection and Risk Management, July.

[12] K. Wang and S. Stolfo, Kui Mok. 1999. A Data Mining Framework for building Intrusion Detection Models. *Proceedings of the 1999 IEEE Symposium on Security and Privacy, Oakland, CA, May*.

[13] S. Mukkamala, G. Janoski, and A. Sung. 2002. Intrusion Detection Using Neural Networks and Support Vector Machine. In *International Joint Conference on Neural Networks (IJCNN)*.

[14] L. Ertoz, E. Eilertson, A. Lazarevic, P. Tan, J. Srivastava, V. Kumar, P. Dokas. 2004. *The Minds- Minnesota Intrusion Detection System*. Next Generation Data Mining, MIT Press.

[15] X. Xu, X. Wang. 2005. An Adaptive Network Intrusion Detection Method Based on PCA and Support Vector Machines. *Proc. of 1st International Conference on Advanced Data Mining and Applications (ADMA'05), Wuhan, china*. July 22-24.

[16] L. Ertoz, A. Lazarevic, J. Srivastava, V. Kumar, A. Ozgur. 2003. A Comparative Study of Anomaly Detection Schemes in Network Intrusion Detection. Proc. of 3rd SIAM Conference on Data Mining, San Francisco, May.

[17] Q. Wang, V. Mega. 2005. A Clustering Algorithm for Intrusion Detection. *Proceeding SPIE Defense, Security and Sensing: Materials, Systems and Devices*.

[18] Y, Guan, A, Ghorbani, N. Belacel. 2003. Y-means: A Clustering Method for Intrusion Detection. *Proceeding of Canadian Conference on Electrical and Computer Engineering. Montreal, Quebec, Canada, 3-4 May*.

[19] R. K. Belew and M. D. Vose. 1997. Foundations of *Genetic Algorithms*. Morgan Kaufmann. 4: 117-139.

[20] J. Kennedy, R. Eberhart. Particle Swarm Optimization. *Proc. IEEE Int'l. Conf. on Neural Networks (Perth, Australia), IEEE Service Center, Piscataway, NJ*. IV: 1942-1948.

[21] K. Wang and S. Stolfo. 2005. Anomalous Payload-Based Worm Detection and Signature Generation. *International Symposium on Recent Advances in Intrusion Detection (RAID)*.

[22] K. Wang, J. J. Parekh, and S. Stolfo. 2006. Anagram: A Content Anomaly Detector Resistant to Mimicry Attack. *International Symposium on Recent Advances in Intrusion Detection (RAID)*.

[23] W. Yeh, W. Chang, Y. Y. Chung. 2008. A New Hybrid Approach for Data Mining Breast Cancer Pattern Using Discrete Particle Swarm Optimization and Statistical Method. Paper submitted to Expert Systems and Applications, Elsevier. (Accepted 01/12/2008).

[24] Rafael, C. Gonzalez and Paul, WintzA tutorial on Principal Components Analysis, *mail.iiit.ac.in/~mkrishna/PrincipalComponents.pdf*.

[25] X. He. 2007. *Journal of Network and Computer Applications*. Elsevier. 30.

[26] X. He and Z. Lu. 2007. *International Journal on Agent-Oriented Software Engineering*. Inderscience. 1(2).

[27] Y. Y. Chung, E. Choi, Z. Zhao, M. Shukran, D. Shi, F. Chen. 2007. Application of Vector Quantization for Content Based Music Retrieval System. *WSEAS Transactions on Computers*. 5(6): 793-798. ISSN 1109-2750. (EI, MathSci).

[28] Y. Y. Chung. 2004. Evaluation of Clustering Algorithms for Image Retrieval System. *International Journal of Information Technology*. 1(1-4): 198-201. ISSN: 1305-239x.

[29] H-S.Wang, Wei-Chang Yeh, P-C. Huang, W-W. Chang. Using Association Rules and Particle Swarm Optimization Approach for Part Change. *Expert Systems with Applications*. doi: 10.1016/j.eswa2008.10.026.

[30] C. Bae, W. Yeh, Y. Y. Chung, X. He. 2008. A New Universal Generating Function Method for Estimating the Novel Multi-Resource Multistate Information Network Reliability. *IEEE Transactions on Reliability*. (TR2008-085, under review 09/2008) *(Tier A Journal in CORE list 2008)*.