Impact Factor (SJIF): 5.301

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 5, Issue 2, February-2018

IDS: Policy-based Security Using Software-Defined Networking System

[1]Utkarsh Kanse, [2]Dnyaneshwar Shinde, [3]Vikas More, [4]Shon Nikam, [5]Prof. Amrita Shirode

[1]Student of Department of Computer Engineering, AISSMS Polytechnic, Pune, Maharashtra, India
kanse.utkarsh1@gmail.com ,
[2]Student of Department of Computer Engineering, AISSMS Polytechnic, Pune, Maharashtra, India
2017dnyaneshwarshinde@gmail.com,
[3]Student of Department of Computer Engineering, AISSMS Polytechnic, Pune, Maharashtra, India
vikasmore995@gmail.com,
[4]Student of Department of Computer Engineering, AISSMS Polytechnic, Pune, Maharashtra, India
shonnikam18@gmail.com
[5]Asst.Prof. of Department of Computer Engineering, AISSMS Polytechnic, Pune, Maharashtra, India
amrita.shirode@gmail.com

Abstract: *Dismissed and unrelated features in data have caused a long-term problematic in network traffic classification. These geographies not only slow down the procedure of organization but also prevent a classifier from making precise choices, especially when coping with big data. In this paper, we propose a shared information based algorithm that logically selects the optimum feature for classification. This shared information based feature selection algorithm can handle linearly and nonlinearly dependent data features. Its effectiveness is evaluated in the cases of network intrusion detection. An Interruption Finding Scheme, named Least Honest Support Vector Machine based IDS (LSSVM-IDS), is built using the constructions selected by our proposed article selection algorithm. The presentation is estimated using three interruption finding estimation datasets, namely KDD Cup 99, NSL-KDD and Kyoto 2006 dataset. The estimation results show that our feature selection algorithm enhances more serious features to achieve better correctness and lower computational cost associated with the state-of-the-art methods.*

Keywords: Least Honest Support Vector Machine based IDS (LSSVM-IDS), feature selection algorithm, Intrusion Detection System (IDS).

I. INTRODUCTION

Despite increasing awareness of network security, the existing solutions remain incapable of fully protecting internet applications and computer networks against the threats from ever-advancing cyber-attack techniques such as DoS attack and computer malware. Developing effective and adaptive security approaches, therefore, has become more critical than ever before. The traditional security techniques, as the first line of security defense, such as user authentication, firewall and data encryption, are insufficient to fully cover the entire landscape of network security while facing challenges from ever-evolving intrusion skills and techniques s. Hence, another line of security defense is highly recommended, such as Intrusion Detection System (IDS).

Recently, AN ID alongside with anti-virus software has become an important complement to the security infrastructure of most organizations. The combination of these two lines provides a more comprehensive defense against those threats and enhances network security.

II. LITERATURE SURVEY

1. Unsupervised feature selection method for intrusion detection system, in: International Conference on Trust, Security and Privacy in Computing and Communications

Author: A. M. Ambuscade, X. He, P. Nanda

The feature selection problem for data classification in the absence of data labels. It first proposes an unsupervised feature selection algorithm, which is an enhancement over the Laplacian score method, named an Extended Laplacian score, EL in short. Specifically, two main phases are involved in EL to complete the selection procedures. In the first phase, the Laplacian score algorithm is applied to select the features that have the best locality preserving power. In the second phase, EL proposes a Redundancy Penalization (RP) technique based on mutual information to eliminate the redundancy among the selected features. This technique is an enhancement over Battiti's MIFS. It does not require a user defined parameter such as β to complete the selection processes of the candidate feature set as it is required in MIFS. After tackling the feature selection problem, the final selected subset is then used to build an Intrusion Detection System.

2. A novel feature selection approach for intrusion detection data classification, in: International Conference on Trust, Security and Privacy in Computing and Communications

Author:A. M. Ambusaidi, X. He, Z. Tan, P. Nanda, L. F. Lu, T. U. Nagar

interruption finding system play a important role in monitor and analyze daily behavior taking place in computer systems to detect occurrence of security threats. However, the routinely produced analytical data from computer networks are usually of very huge in size. This creates a major challenge to IDSs, which need to examine all features in the data to identify intrusive patterns. The objective of this study is to analyze and select the more discriminate input features for building computationally efficient and effective schemes for an IDS. For this, a hybrid feature selection algorithm in combination with wrapper and filter selection processes is designed in this paper. Two main phases are involved in this algorithm. The upper phase conducts a preliminary search for an optimal subset of features, in which the mutual information between the input features and the output class serves as a determinant criterion.

3. A novel hybrid intrusion detection method integrating anomaly detection with misuse detection, Expert Systems with Applications

Author:G. Kim, S. Lee, S. Kim

A new hybrid interruption finding method that hierarchically integrates an exploitation detection model and an irregularity-finding model in a decomposition structure is proposed. First, a misuse detection model is build

based on the C4.5 decision tree algorithm and then the normal preparation data is decomposed into smaller subsets using the model.

4. Selection of candidate support vectors in incremental svm for network intrusion detection

Author: R. Chitrakar, C. Huang

In an Incremental Support Vector Machine classification, the data objects labelled as nonsupport vectors by the previous classification are re-used as training data in the next classification along with new data samples verified by KarusheKuhneTucker (KKT) condition. This paper proposes Half-partition strategy of selecting and retaining non-support vectors of the current increment of classification e named as Candidate Support Vectors (CSV) e which are likely to become support vectors in the next increment of classification. This research work also designs an algorithm named the Candidate Support Vector based Incremental SVM (CSV-ISVM) algorithm that implements the proposed strategy and materializes the whole process of incremental SVM classification.

III. EXISTING SYSTEM

Feature selection is a technique for eliminating irrelevant and redundant features and selecting the most optimal subset of features that produce a better characterization of patterns belonging to different classes. Methods for feature selection are generally classified into filter and wrapper methods. Filter algorithms utilize an independent measure (such as, information measures, distance measures, or consistency measures) as a criterion for estimating the relation of a set of features, while wrapper algorithms make use of particular learning algorithms to evaluate the value of features. In comparison with filter methods, wrapper methods are often much more computationally expensive when dealing with high-dimensional data or large-scale data. In this study hence, we focus on filter methods for IDS.

Disadvantages of Existing System

1. Redundant and irrelevant features in data have caused a long-term problem in network traffic classification.
2. These features not only slow down the process of classification but also prevent a classifier from making accurate decisions, especially when coping with big data.
3. Low performance.

IV. PROPOSED SYSTEM

We propose a virus detection system placed at the network egress points to detect malware infection which relies on DNS to locate command and control servers. We build a reputation engine to decide whether an IP address i.e. data coming from that system is infected or not by using these feature vectors together.

Advantages of Proposed System

1. Recently, an IDS alongside with anti-virus software has become an important complement to the security infrastructure of most organizations.
2. IDns is designed to detect malicious domains used for crafted malware in APT attacks and to detect infected machines.
3. In Proposed system we analysed the network traffic of large numbers of suspicious malware C&C servers.

V. SYSTEM ARCHITECTURE

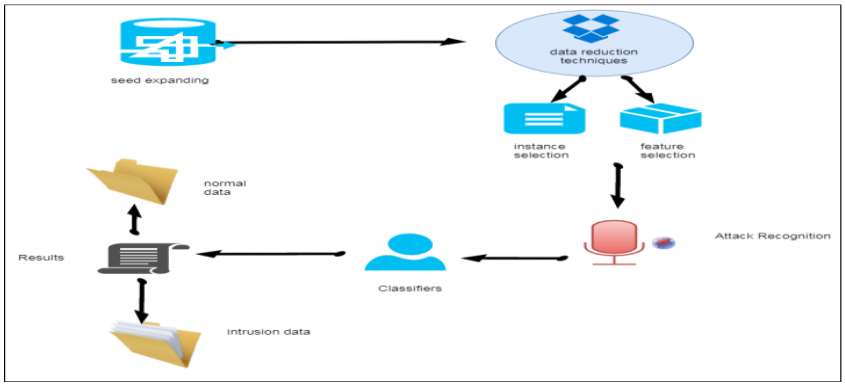

Fig. System Architecture

The user brows multiple files to send, one or some files may contains virus files or all virus free files. When malicious file affect the non-malicious file, the system will create replica or duplicate copy of the file, which is going to affect to cheat the malicious file, hence malicious file affect the duplicate file and original file is send to receiver. Then, system will detect and block the malicious file to reach at server pc.

VI. CONCLUSION

In this, a proposed a system IDnS placed at the network egress points to detect malware infections inside the network combined with DNS traffic analysis. Extracted new features and built a reputation engine based on big data, which includes approximately 400 million DNS queries. The system processes advantages of high efficiency and accuracy. The experimental results show that this security approach is feasible for improving the sustainability of the system and is good at detecting APT malware infections. A useful intrusion system can help to fight against cyber-crime such as theft of information from infected host.

VII. REFERENCES

[1] S. Pontarelli, G. Bianchi, S. Teofili, Traffic-aware design of a high speed fpga network intrusion detection system, Computers, IEEE Transactions on 62 (11) (2013) 2322–2334.

[2] A. Chandrasekhar, K. Raghuveer, An effective technique for intrusion detection using neuro-fuzzy and radial svm classifier,in: Computer Networks & Communications (NetCom), Vol. 131, Springer, 2013, pp. 499–507.

.

[3] S. Mukkamala, A. H. Sung, A. Abraham, Intrusion detection using an ensemble of intelligent paradigms, Journal of network and computer applications 28 (2) (2005) 167–182.

[4] A. N. Toosi, M. Kahani, A new approach to intrusion detection based on an evolutionary soft computing model using neurofuzzyclassifiers, Computer communications 30 (10) (2007) 2201– 2212.

[5] Z. Tan, A. Jamdagni, X. He, P. Nanda, L. R. Ping Ren, J. Hu, Detection of denial-of-service attacks based on computer vision techniques, IEEE Transactions on Computers 64 (9) (2015) 2519– 2533.