*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 5, May-2018***

# Building an Internal Intrusion Detection System

Prof. Kailash Shaw, Department of Computer Engineering, DYPCOE, Akurdi- Pune

Bhor Ganesh [1], Bhor Akshay [2], Deepanshu Raj [3], Mane Suraj [4], Kapade Prashant [5]

*Department of Computer Engineering, D. Y. Patil College of Engineering, Akurdi.*

**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. 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:** Support Vector Machine (SVM), Intrusion Detection System (IDS), Design Methodology—Classifier design and evaluation; Optimization- Genetic Algorithm.

## 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 IDS 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. Internal Intrusion Detection and Protection System (IIDPS), is proposed to detect insider attacks at SC level by using data mining and forensic techniques.

## II. LITERATURE SURVEY

| Sr. No | Paper Name | Year | Advantages | Disadvantages |
|---|---|---|---|---|
| 1 | **Unsupervised feature selection method for intrusion detection system, in: International** | 2015 | The effectiveness and the feasibility of the proposed detection system are evaluated using three well-known intrusion detection dataset | This will be very useful since the proposed method is sensitive to the selection of this parameter |
| 2 | **A novel feature selection approach for intrusion detection data classification, in: International Conference on Trust, Security and Privacy in Computing and Communications** | 2014 | select the more discriminate input features for building computationally efficient and effective scheme | High accuracy of wrapper approaches and the efficiency of filter Approaches. |
| 3 | **A novel hybrid intrusion detection method integrating anomaly detection with misuse detection, Expert Systems with Applications** | 2014 | anomaly detection model in a decomposition structure is proposed | to decompose the normal training data into smaller subsets |
| 4 | **Selection of candidate support vectors in incremental svm for network intrusion detection** | 2014 | Half-partition strategy of selecting and retaining non-support vectors of the current increment of classification | a more efficient and faster Support Vector selection method |
| 5 | **Intrusion detection using naive bayes classifier with feature reduction.** | 2012 | efficient classifier naive bayes on reduced datasets for intrusion detection | more improvement on classification accuracy with compared to CFS but takes more Time. |

## III. EXISTING SYSTEM

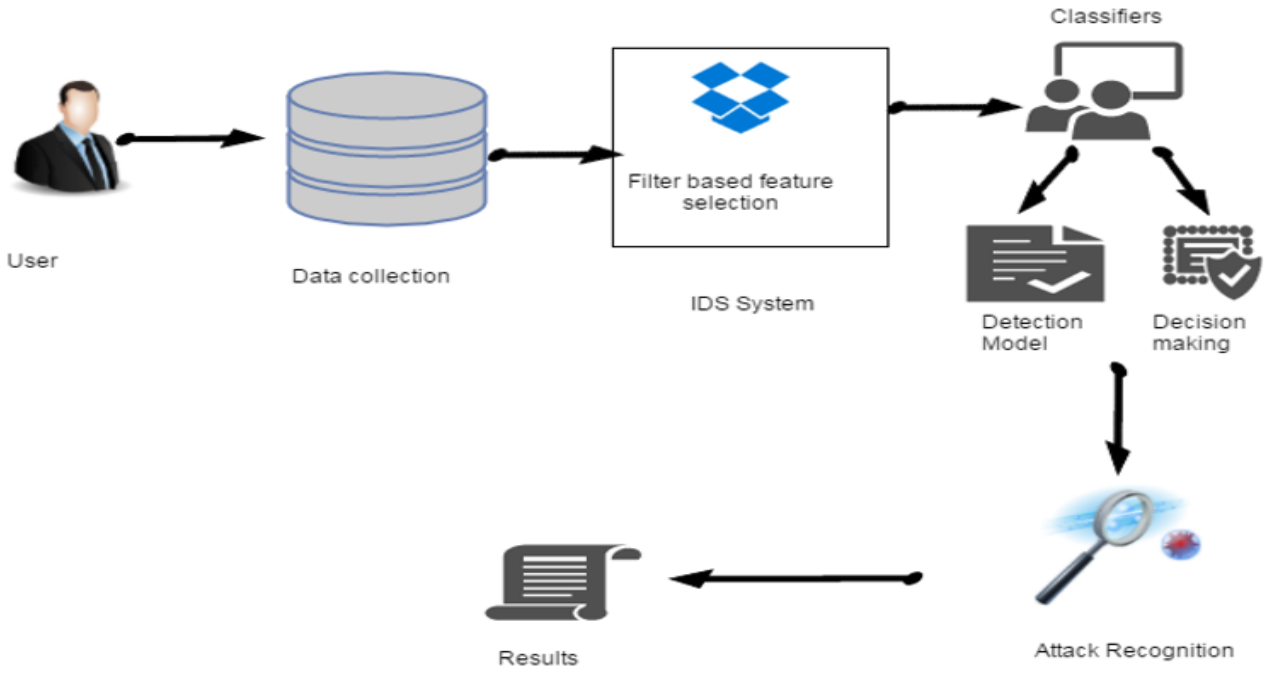
Feature selection is a technique for eliminating irrelevant and redundant features and selecting the most optimal subset of features that produce a better characterization of patterns belonging to different classes. Methods for feature selection are generally classified into filter and wrapper methods. 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 analyzed the network traffic of large numbers of suspicious malware C&C servers.

## V. CONCLUSION

In this, a proposed a system IISPS which employs data mining and forensic techniques to identify the user behavioral patterns for a user. The time that a habitual behavior pattern appears in the user's log file is counted, the most commonly used patterns are filtered out, and then a user's profile is established. By identifying a user's behavior patterns as his/her computer usage habits from the user's current input, the IIDPS resists suspected attackers at the network egress points to detect malware infections inside the network combined network traffic analysis. Proposed an approach for network intrusion detection for KDD Cup 99 dataset with genetic algorithm (GA).

## REFERENCES

[1] S. Pontarelli, G. Bianchi, S. Teofili, "Traffic-aware design of a high speed 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", 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 neuro fuzzy classifiers, 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.

[6] Ch Satya Keerthi N.V.L., Prasanna P.I., Priscilla B.M., "Instuction Detection system Using Genetic Algorithm",Int. Journal of P2P Network rends and Technology, vol.1.no. 2.pp 1-7, 2011.

[7] Janusz Starzyk ,Jing Pang," Evolvable Binary Artificial Neural Network for Data Classification", Evolutionary Computation pp 5576-5783(2000).

[8] Guoqiang Peter Zhang,"Neural Networks for Classification: A Survey", IEEE Transaction on systems management and Cybernatics - Applications and Reviews Vol-30, No-4,pp 451-462(2000).