Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 4, Issue 3, March -2017

Filter Based Data Reduction Technique and Classification for Intrusion Detection System

[1]Kalpesh, [2]Shubham, [3]Aditya, [4]Sneha Disha

[1,2,3,4] Department of Information Technology engineering, Dr D Y Patil College of engineering

Abstract — *Redundant and tangential options in information have caused a semi permanent downside in network traffic classification. These options not solely curtail the method of classification however conjointly forestall a classifier from creating correct choices, particularly once dealing with huge information. During this paper, we have a tendency to propose a mutual info primarily based algorithmic rule that analytically selects the best feature for classification. This mutual info primarily based feature choice algorithmic rule will handle linearly and nonlinearly dependent information options. Its effectiveness is evaluated within the cases of network intrusion detection. Associate in Nursing Intrusion Detection System (IDS), named Least sq. Support Vector Machine primarily based IDS (LSSVM-IDS), is constructed exploitation the options hand-picked by our projected feature choice algorithmic rule. The performance of LSSVM-IDS is evaluated exploitation 3 intrusion detection analysis datasets, particularly KDD Cup ninety nine, NSL-KDD and urban center 2006+ dataset. The analysis results show that our feature choice algorithmic rule contributes additional important options for LSSVM-IDS to realize higher accuracy and lower process price compared with the progressive strategies.*

Keywords-*Intrusion detection, Feature selection, Mutual information, Linear correlation coefficient, Least square support vector machine.*

I. INTRODUCTION

Despite increasing awareness of network security, the prevailing solutions stay incapable of absolutely protective web applications and laptop networks against the threats from ever-advancing cyber-attack techniques like DoS attack and laptop malware. Developing effective and accommodative security approaches, therefore, has become a lot of essential than ever before. the standard security techniques, because the 1st line of security defense, like user authentication, firewall and encoding, area unit short to completely cowl the whole landscape of network security whereas facing challenges from ever-evolving intrusion skills and techniques [1]. Hence, another line of security defense is very suggested, like Intrusion Detection System (IDS). Recently, Associate in Nursing IDS aboard with anti-virus software package has become a very important complement to the protection infrastructure of most organizations. the mixture of those 2 lines provides a a lot of comprehensive defense against those threats and enhances network security.

Redundant and inapplicable options in information have caused a long-run drawback in network traffic classification. These options not solely abate the method of classification however additionally stop a classifier from creating correct choices, particularly once managing huge information. During this paper, we have a tendency to propose a mutual info primarily based algorithmic program that analytically selects the best feature for classification. This mutual info primarily based feature choice algorithmic program will handle linearly and nonlinearly dependent information options. Its effectiveness is evaluated within the cases of network intrusion detection. Associate in Nursing Intrusion Detection System (IDS), named Least sq. Support Vector Machine primarily based IDS (LSSVM-IDS), is made victimization the options elite by our planned feature choice algorithmic program. The performance of LSSVM-IDS is evaluated victimization 3 intrusion detection analysis datasets, specifically KDD Cup ninety nine, NSL-KDD and metropolis 2006+ dataset. The analysis results show that our feature choice algorithmic program contributes a lot of essential options for LSSVM-IDS to attain higher accuracy and lower machine value compared with the progressive strategies

II. LITERATURE SURVEY

1. Traffic-aware Design of a High Speed FPGA Network Intrusion Detection System

Authors: Salvatore Pontarelli, Giuseppe Bianchi, Simone Teofili.

Description: Security of today’s networks heavily believe Network Intrusion Detection Systems (NIDSs). the power to promptly update the supported rule sets and observe new rising attacks makes Field Programmable Gate Arrays (FPGAs) a really appealing technology. a vital issue is a way to scale FPGA-based NIDS implementations to ever quicker network links. Whereas a trivial approach is to balance traffic over multiple, however functionally equivalent, hardware blocks, every implementing the full rule set (several thousands rules), the apparent consist the linear increase within the resource occupation. During this work, we tend to promote a distinct, traffic-aware, standard approach within the style of FPGA-based NIDS. Rather than strictly cacophonous traffic across equivalent modules, we tend to classify and cluster homogenous traffic, and dispatch it to otherwise capable hardware blocks, every supporting a (smaller) rule set tailored to the precise traffic class. we tend to implement and validate our approach exploitation the rule set of the accepted Snort

NIDS, and that we experiment all investigate the rising trade-offs and benefits, showing resource savings up to eightieth supported universe traffic statistics gathered from AN operator's backbone.

2. KDD-99 Classifier Learning Contest LLSoft's Results Overview
Authors: Itzhak Levin LLSoft
Description: Kernel mineworker could be a new data-mining tool supported building the optimum call forest. The tool won second place within the KDD'99Classifier Learning Contest, August 1999. we tend to describe the Kernel Miner's approach and methodology used for resolution the competition task. The received results area unit analyzed and explained. Kernel mineworker could be a data-mining tool for the outline, classification and generalization of knowledge, and for predicting the new cases. Kernel mineworker could be a totally machine-controlled tool that offer solutions to information users. Though Kernel mineworker applies a system of subtle mathematical models and algorithms, it's very simple for users. The tool has been developed for Windows 95/98/NT and works with completely different databases such as dBase, MS Access, SQL Server, Oracle, etc. directly or through ODBC or OLEDB.

3. Network-Based Intrusion Detection with Support Vector Machines
Author: Dong Seong Kim1 and Jong Sou Park1
Description: This paper proposes a technique of applying Support Vector Machines to network-based Intrusion Detection System (SVM IDS). Support vector machines (SVM) could be a learning technique that has been with success applied in several application areas. Intrusion detection will be thought-about as two-class classification downside or multi-class classification downside. we tend to used dataset from 1999 KDD intrusion detection contest.SVM IDS was learned with coaching set and checked with test sets to judge the performance of SVM IDS to the novel a tacks. And that we additionally measure the importance of every feature to boost the general performance of IDS. The results of experiments demonstrate that applying SVM in Intrusion Detection System will be economical a good and efficient approach for sleuthing intrusions.

4. An Effective Technique for Intrusion Detection Using Neuro-Fuzzy and Radial SVM Classifier
Author: A. M. Chandrasekhar and K. Raghuveer
Description: Intrusion detection isn't nevertheless an ideal technology. This has given data processing the chance to create many vital contributions to the sector of intrusion detection. during this paper, we've projected a brand new technique by utilizing data processing techniques like neuro-fuzzy and radial basis support vector machine(SVM) for the intrusion detection system. The projected technique has four major steps during which, opening is to perform the Fuzzy C-means agglomeration (FCM). Then, Neuro-fuzzy is trained, such every of the info purpose is trained with the corresponding neuro-fuzzy classifier related to the cluster. afterwards, a vector for SVM classification is made and within the fourth step, classification victimisation radial SVM is performed to notice intrusion went on or not. knowledge set used is that the KDD cup ninety nine dataset and that we have used sensitivity, specificity and accuracy because the analysis metrics parameters. Our technique might win higher accuracy for all kinds of intrusions. It achieved concerning ninety eight.94% accuracy just in case of DOS attack and reached heights of ninety seven.11%accuracy just in case of PROBE attack. just in case ofR2L and U2R attack sit has earned ninety seven.78 and 97.80% accuracy severally. we have a tendency to compared the projected technique with the opposite existing state of art techniques. These comparisons proved the effectiveness of our technique

5. Intrusion detection using an ensemble of intelligent paradigms
Author: Srinivas Mukkamalaa,*, Andrew H. Sunga, Ajith Abrahamb
Description: Soft computing techniques area unit progressively getting used for drawback resolution. This paper addresses mistreatment associate ensemble approach of various soft computing and arduous computing techniques for intrusion detection. thanks to increasing incidents of cyber attacks, building effective intrusion detection systems area unit essential for shielding data systems security, associated nonetheless it remains an elusive goal and a good challenge. we tend to studied the performance of Artificial Neural Networks (ANNs), Support Vector Machines (SVMs) and variable adjustive Regression Splines (MARS). we tend to show that associate ensemble of ANNs, SVMs and MARS is superior to individual approaches for intrusion detection interms of classification accuracy.

III. PROPOSED SYSTEM

We propose a scourge observation system placed at the network egress points to detect malware infection that depends on DNS to find command and management servers. we tend to build a name engine to make your mind up whether or not associate scientific discipline address i.e. information coming back from that system is infected or not by victimisation these feature vectors along..

IV. SYSTEM ARCHITECTURE

IDS is designed to detect malicious domain issued for crafted malware in virus attacks and to detect infected machines. For this purpose, we did analysis of large volumes of DNS traffic which can be called big data. And we also analyzed the network traffic of large numbers of suspicious malware C&C servers.

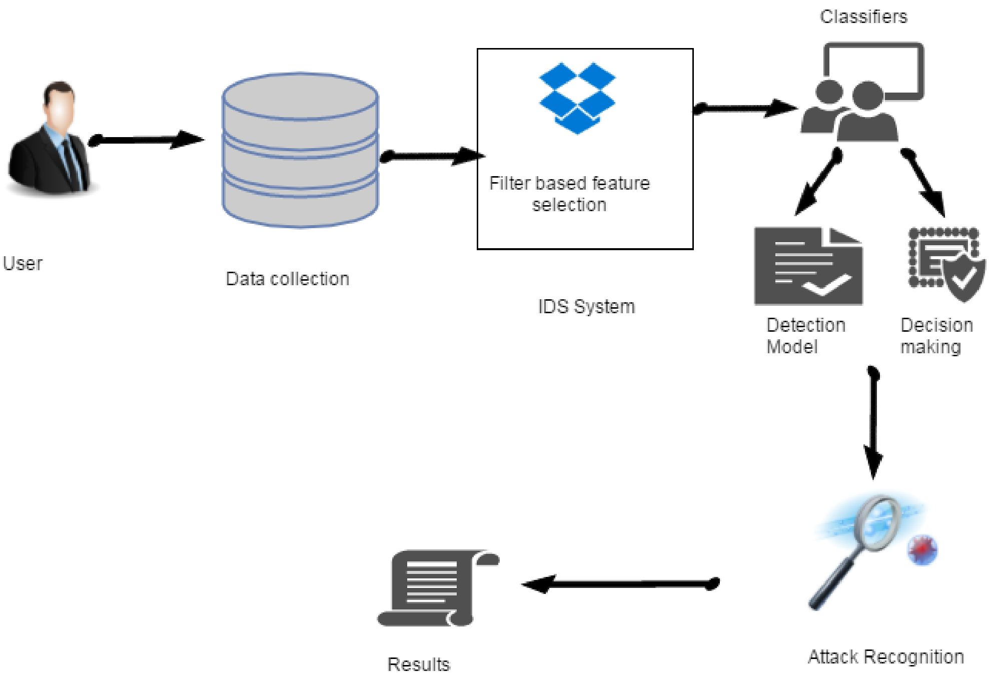

Fig.1: System Architecture

V MATHEMATICAL MODEL

Let w is the set of whole system which consist
W= {input, process, output}
Input:-
File={f1, f2,.................,fn}
Process:-
In this project we have used Filter Based Feature selection algorithm.
This algorithm filters the features or attributes & provide the exact results to query.
Output:-Accurate Results

VI. ADVANTAGES

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.

VII. CONCLUSION AND FUTURE SCOPE

In this, a planned a system IDS placed at the network egress points to sight malware infections within the network combined with DNS traffic analysis. Extracted new options and designed a name engine supported huge information, which has around four hundred million DNS queries. The system processes benefits of high potency and accuracy. The experimental results show that this security approach is possible for up the property of the system and is nice at detection APT malware infections. it's a helpful intrusion system which will facilitate to fight against cyber-crime like larceny of data from infected host.

ACKNOWLEDGMENT

We might want to thank the analysts and also distributers for making their assets accessible. We additionally appreciative to commentator for their significant recommendations furthermore thank the school powers for giving the obliged base and backing.

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 svmclassifier,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.

[6] A. M. Ambusaidi, X. He, P. Nanda, Unsupervised feature selection method for intrusion detection system, in: International Conference on Trust, Security and Privacy in Computing and Communications, IEEE, 2015.

[7] A. M. Ambusaidi, X. He, Z. Tan, P. Nanda, L. F. Lu, T. U. Nagar, A novel feature selection approach for intrusion detection data classification, in: International Conference on Trust, Security and Privacy in Computing and Communications, IEEE, 2014, pp. 82– 89.

[8] E. Stalmans and B. Irwin, ‘‘A framework for DNS based detection and mitigation of malware infections on a network,’’ in Proc. Inf. Secur. South Africa (ISSA), Aug. 2011, pp. 1–8.

[9] M.Antonakakis,R.Perdisci,D.Dagon,W.Lee,andN.Feamster,‘‘Build- ing a dynamic reputation system for DNS,’’ in Proc. 19th USENIX Secur. Symp., 2010, pp. 273–290.

[10] T.Holz,C.Gorecki,K.Rieck,andF.C.Freiling,‘‘Measuringanddetecting fast-flux service networks,’’ in Proc. NDSS, 2008.

[11] V. Kumar and D. O. P. Sangwan, ‘‘Signature based intrusion detection system using SNORT,’’ Int. J. Comput. Appl. Inf. Technol., vol. 1, no. 3, pp. 35–41, 2012.

[12] P. Garcia-Teodoro ,J.Diaz-Verdejo,G.Maciá-Fernández, and E.Vázquez, ‘‘Anomaly-based network intrusion detection: Techniques, systems and challenges,’’ Comput. Secur., vol. 28, nos. 1–2, pp. 18–28, 2009.