Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

International Conference on Mobility in Computing- ICMiC13, Organized by Mar Baselios College of Engineering and Technology during December 17-18, 2013 at Trivandrum, Kerala, India, pg.166 – 172

SURVEY ARTICLE

Feasibility of Machine Learning Techniques to Reduce False Alarm in Intrusion Detection

Anne Dickson, Ciza Thomas
Dept. of Electronics & Communication Engineering, College of Engineering, Trivandrum , Kerala, India
annsalins2010@gmail.com, ciza_thomas@yahoo.com

Abstract- ***The sophisticated recent advances in networking increased the dependability of humans in Network technology everyday life. Now-a-days the number of attacks on networks got increased drastically. With the development of large open networks, security threats have increased significantly in the past two decades. So mitigating those attacks is one of the significant interests of researchers in the network security. The goal of an intrusion detection system is to provide a wall of defence to confront the attacks of computer systems on internet. Machine Learning algorithms have been successfully applied to intrusion detection; however the true positive and false positive trade-offs is always a major challenge in the choice of the algorithms. This paper explores the wide variety of machine learning algorithms focusing on the feasibility of these algorithms for the purpose of reducing false positives*****.**

Keywords- : Artificial Neural Network; Adaptive Learner for Alert Classification; K Nearest Neighbour ; Data Mining; Genetic Algorithm; Particle Swarm Optimization; Multilayer Perception; Detection Rate; False Positive; Support Vector Machine .

I. INTRODUCTION

Any computer connected to a network is potentially vulnerable to attacks. Hackers discover more network vulnerabilities mainly because applications and attack tools can be easily downloaded. Some programs and network services were not originally designed with strong security in mind and are inherently vulnerable to attack. The attack tools on open networks have generated an increased need for network security and dynamic security policies. A closed network provides connectivity only to trusted known parties and sites. An intrusion is the exploitation of a flaw in a computing system (Operating System, software program or user program) for purposes that are not known by the system operator and that are generally harmful. These intrusions are mostly launched automatically from infected machine by Trojans, viruses and worms without their owner's knowledge. The best way to protect against this type of attack is to disable any vulnerable services or find alternatives. According to the statistics collected by CERT Coordination Centre (CERT/CC) in the United States, the number of reported incidents related to computer security in a year has increased from 1,334 to 137,529 over the last decade. This is the result of the rapid growth of information technology applications and it shows the importance to protect our information assets from attacks and damages.

The aim of this paper is twofold. The first is to present a comprehensive survey on research contributions that investigate utilization of machine learning methods in building intrusion detection models. The benefits of machine learning algorithms, such as adaptation, superior computational speed and error resilience in the face of noisy information fit the requirements of building a good intrusion detection model. Through this paper we provide an overview of the research progress in applying machine learning methods to the problem of intrusion detection. The scope of this review will be on fundamental methods of machine learning, including Naïve Bayes, Bayesian Classifier, Genetic algorithms, decision tree, artificial neural networks, fuzzy systems, and Support Vector Machines, and swarm intelligence. The research contributions in each field are systematically summarized and compared. Applications of these methods reveal that each of them has pros and cons. The second aim is to define existing research challenges, and to highlight promising new research directions.

The remainder of this paper is divided into several sections, organized as follows. Section II discusses the various research works undertaken in the field of machine learning in Intrusion Detection Systems (IDS). Section III and IV introduce the commonly used datasets and performance evaluation measures, with the purpose of comparison of the different research works. Section V categories, compares and summarizes the fundamental methods in machine learning that have been proposed to solve intrusion detection problems. Section VI compares the strengths and limitations of these approaches, and identifies future research trends and challenges. Section VII analyses the observations made and section VIII concludes the paper.

II. RELATED WORKS

The concept of intrusion detection system to protect the network systems was first put forward by Denning[1]. This work identifies systems as complex and hence controlling an attack and achieving a desired level of damage may be harder than using physical weapons. This emphasizes the seriousness of this menace.

Y.Meng[2] proposed a practice on using machine learning for network anomaly intrusion detection. He implemented and compared the machine learning schemes of neural networks, support vector machines and decision trees in a uniform environment with the purpose of exploring the practice and issues of using these approaches in detecting abnormal behaviors.

Meng,L.Kwok[3] conducted a case study in exploring the performance of an intelligent false alarm filter developed by them by implementing a fuzzy classifier based on if-then rules. And they concluded that the if-then rule based fuzzy algorithm performs a bit better than the baseline algorithm and can be improved by selecting an appropriate fuzzy partition.

T.Pietraszek[4] used an ALAC (Adaptive Learner Alert Classification) to reduce false positives in intrusion detection. ALAC effectively reduces the analyst’s workload. Here the real time use of analysts feedback is taken into consideration for classifying alerts generated by IDS

Hui, Lee[5] proposed a method of false alarm reduction by weighted score-based rule adaptation through expert feedback using the rule set generated by the rule learner RIPPER. This mechanism performed well without adaptation consideration.

Heng and Hsing[6] proposed a method of adaptive alarm filtering by causal correlation consideration in intrusion detection. This system can deal with the frequent changes of network environment since it makes use of an ensemble of classifiers.

According to Nitin and T.Gondaliya[7], the IDS alarm filtering can be enhanced using KNN classifier**.**

A new semi-supervised learning method is introduced by Chein, Wen and Lee[8] for false alarm reduction using only a very small amount of labelled information. This made the alarm filter more practical for the real systems. Numerical comparison with the conventional supervised learning approach with the same small portion of the labelled data has been done. Analysis showed this method as having the significantly superior detection rate as well as in the false alarm detection rate.

III. COMMONLY USED DATASETS

The commonly used datasets for intrusion detection are KDD CUP'99 which is a standard intrusion detection system benchmark dataset which is based on Lincoln lab, and DARPA datasets[9] of 1998, 1999, 2000. MIT Lincoln laboratory under DARPA and ARFL sponsorship, has collected and distributed the first corpora for evaluation of computer network intrusion detection systems. This data set is used for training as well as testing intrusion detectors. Another new data set used is UNB ISCX intrusion detection evaluation dataset[10]. This uses a synthetic approach to generate the required datasets.

IV. PERFORMANCE EVALUATION METRICS

Intrusion Detection Systems can be divided into two categories according to the detection approaches: anomaly detection and misuse detection. A vast majority of the research has focused on anomaly detection methods for intrusion detection. The anomaly network intrusion detection models have the advantage that they are able to detect new attacks. However, they usually suffer from the very high false positives. The performance of an intrusion detection model depends on its detection rates (DR) and false positives (FP). DR is defined as the number of intrusion instances detected by the system divided by the total number of the intrusion instances present in the dataset. FP is an alarm, which rises for something that is not really an attack. It is preferable for an intrusion detection model to maximize the DR and minimize the FP. For DR, we can modify the objective function to 1-DR.

V. CONVENTIONAL METHODS USED IN MACHINE LEARNING

Machine learning techniques are highly suitable for anomaly intrusion detection systems. The different machine learning methods used in intrusion detection include Association rule, Statistical preprocessing, Rule based, Naïve Bayes, Bayesian classifier, Genetic algorithm, Support Vector Machine, Hidden Markov model, Fuzzy Logic, Gaussian Mixture Model, Multilayer Perceptron (MLP), Neural Network, k-Nearest Neighbor, and Linear Model. The primary focus of using the machine learning techniques in intrusion detection has traditionally been on learning from data assumed to be sufficient and representative of the underlying distribution. This is a stringent restriction on the realistic problem domain that necessitates the need for development of sophisticated algorithms with theoretically provable performances. Hence, an overview of each of these machine learning techniques, followed by a comprehensive review of recent research for developing such a general framework is undertaken in this paper.

Statistical preprocessing and rule based:

Statistical Analysis and rule based analysis are the two general categories which are most commonly employed in intrusion detection systems. The primary advantage of Statistical Analysis is in its ability to detect unanticipated intrusion patterns because the specific patterns do not have to be predefined. The disadvantage of Statistical Analysis is that it is prone to report an unacceptable number of false alarms because of its inability to quickly adapt to legitimate changes in users behavior. Both Statistical Analysis and rule based systems suffer from an inability to detect attack scenarios which may occur over an extended period of time.

Naïve Bayes:

This is a simple classifier with less time consuming. But Naïve Bayesian network is a restricted network which has only two layers and assumes complete independence between the information nodes. Analysis shows that the detection rate of this classifier is only satisfactory. But it differs with the number of data.

Bayesian Classifier:

Bayesian methods provide a probabilistic approach to learning. A data mining oriented method using pseudo-Bayes estimators is used in a anomaly detection system called ADAM (Audit data analysis and mining).Adam consists of a preprocessor, DM engine and a classification engine. The two advantages of this system are the ability to work in real time network environment and the hierarchical wise anomaly detection. But the disadvantage is that once the behaviour of the anomalies is similar, the classifier will misclassify the attacks.

Association rule:

This method is used in data mining to extract a sufficient number of important rules for the users' purpose rather than to extract all the rules meting the criteria which are useful for detection. Initially we should find the value of support and confidence for each set of datasets and then apply the rules. But the result will fully depend on the threshold value. If the value is beyond the threshold, then we should go for other methods to find the best result.

Genetic Algorithm:

Genetic algorithm is a family of computational models based on principles of evolution and natural selection. These algorithms convert the problem in a specific domain into a model by using a chromosome like data structure and evolve the chromosomes using selection, recombination and mutation operators. Applying GA to intrusion detection seems to be a promising area. It can be used to evolve simple rules for network traffic. These rules are used to differentiate normal network connections from anomalous connections. Genetic algorithm is used to optimize the fuzzy rules so that they can better fit to the purpose.

Artificial Neural Network:

Neural Networks could provide a valuable addition to intrusion detection systems because of the flexible pattern recognition capabilities of the technology. The ability to adaptively model users and system behaviors, and the capability to effectively handle intrusive events are some of the potential advantages of the NN. Neural Networks are useful in identifying gradual changes to a system or in the user behavior. Since expert systems are currently capable of recognizing rapid changes in a system, the identification of slower changes in behavior requires the use of sophisticated techniques. Semi-supervised learning is a class of machine learning techniques that make use of small amount of labelled data and with large amount of unlabelled data. Semi-supervised learning comes between supervised and unsupervised learning. Using Semi-supervised learning an alert filter is built in the paper proposed by Chein-Yi Chin and a result of 85% of false alarm reduction with high detection rate got achieved.

Fuzzy Systems:

A fuzzy intrusion recognition engine (FIRE) is proposed by Dickerson et.al.[11] for detecting malicious intrusion activities. The fuzzy part of the system is mainly responsible for both handling the large number of input parameters and dealing with the inexactness of input data. The performance of the fuzzy if-then rules depends on the selection of a fuzzy partition.

The more the number of fuzzy subsets, the more will be performance. But the disadvantage is that it takes more time to build the classifier model than many other algorithms. Thus a trade off should be made between the performance and the consuming time for the fuzzy if-then algorithm.

Decision Tree(J48):

Decision trees work well with large data sets. The high performance of decision trees makes them useful in real-time intrusion detection. Decision trees construct easily interpretable models. These models can be used in the rule-based models with minimum processing. Generalization accuracy of decision trees is a useful property for intrusion detection model. There will always be some new attacks on the system which are small variations of known attacks after the intrusion detection models are built. The ability to detect these new intrusions is possible due to the generalization accuracy of the decision trees. Decision tree induction is one of the classification algorithms in data mining. The classification algorithm is inductively learned to construct a model from the pre-classified data set. Each data item is defined by the values of the attributes. The decision tree classifies the given data item using the values of its attributes. The decision tree is initially constructed from a set of pre-classified data.

Support Vector Machine (SVM):

Support Vector Machine has been proposed as a novel technique for intrusion detection and they are powerful tools for providing solutions to classification, regression and density estimation problems. It first maps the input vector into a high dimensional feature vector space and then obtain the optimal separating hyper-plane in the higher dimensional feature space. Moreover, a decision boundary i.e., the separating hyper-plane is determined by support vectors rather than the whole training samples and this is extremely robust to outliers. The main advantage of this method is speed of SVM’s since the capability of detecting intrusions in real-time is very important. It can learn a larger set of patterns and be able to scale better, because the classification complexity does not depend on the dimensionality of the feature space. SVMs also have the ability to update the training patterns dynamically whenever there is a new pattern during classification. The main disadvantage is SVM can only handle binary-class classification whereas intrusion requires multi-class classification.

Swarm intelligence:

Swarm Intelligence is the property of a system whereby the collective behaviours of agents interacting locally with their environment cause coherent functional global patterns to emerge. For each type of attack find the detection rate, false positive rate, true positive rate, precision and recall value to apply this swarm intelligence. This is an optimization technique which can be applied in any of these values for intrusion detection, which has strong global search capability. The binary PSO is used to obtain the optimum feature subset at building intrusion detection system. Thus PSO is a novel optimization technique, which shows high performance in numeric problems as illustrated in Table I. Initially when we apply this optimization method, a trade-off between false negatives and true positives should be found out. Analysis shows that this method performs best in finding the U2R type of attacks [10]. The success of any Intrusion Detection System (IDS) is a complicated problem due to its nonlinearity and the quantitative or qualitative network traffic data stream with irrelevant and redundant features. How to choose the effective and key features to IDS is very important topic in information security.

TABLE I
DETECTION PERFORMANCE USING DT, NN, PSO[13]

Attacks	Decision Tree	Neural Network	Particle Swarm Optimization
Normal	99.96%	99.19%	95.69%
DoS	100%	98.75%	90.4%
R2L	99.02%	99.09%	98.10%
U2R	88.33%	99.70%	100%
Probe	99.66%	98.39%	95.53%

The performance comparison of the different machine learning algorithms discussed in this section is given in terms of the DR and the FP in Table II.

TABLE II1
FALSE POSITIVE RATE AND DETECTION RATE OF ML TECHNIQUES[8][13]

Method	False Positive	Detection Rate
Naïve Bayes	0.101	0.904
Neural Network	0.189	0.66
Decision Tree(J48)	0.005	0.840
SVM	0.23	0.703
Semi-supervised	0.665	0.646
Fuzzy systems	0.70	0.660

VI. FUTURE RESEARCH DIRECTIONS

Six different generic phases to consider while doing future study in IDS are as follows [12]. In initial probing phase, Intruder collects information regarding the Operating system, firewall and user profile. Gaining initial access phase includes parameter like invalid/incorrect password attempt, user terminal, user networking hours, port addresses of the machines used. Gaining full system access phase includes illegal password file access attempt, illegal directory access attempt, illegal application access etc. Performing the hacking attempt means the intruders action to use system facilities and information. Covering hacking attempts includes audit log access i.e., the action of the intruder to erase all the track or clues leading to the exposure of access routes and directory. The last phase is modifying utilities to ensure future access by creating an illegal user account by the intruder. That means creating a backdoor in the system for the use by intruder for the future use. Study the feasibility of the methodology going to be used in machine learning in the real world scenario.

VII. ANALYSIS FROM THE ABOVE OBSERVATIONS

The above result is taken by experimenting using the data set KDDCUP'99. In this paper machine learning techniques are used for feature reduction in IDS. Here dimension and complexity of data are reduced and hence feature space is optimally reduced for getting the better detection rate. Decision tree outperforms well in almost all attacks [8][13]. But these values will differ with number of instances and set of classifiers like 2-class classifier, 5-class classifier we consider[13]. All the conventional methods of machine learning have their own limitations to get best detection rates. An optimization method like PSO can be applied after finding some tradeoff between false positives and true positives.

VIII. CONCLUSION

An IDS is a program or set of programs that analyzes what happens or has happened during an execution and tries to find indications that the computer or network system has been misused. An IDS does not eliminate the use of preventive mechanism but it works as the last defensive mechanism in securing the system. All the conventional methods of machine learning have their own limitations to get best detection rates as observed from the earlier research in this area. Any new optimization method can be applied after finding some tradeoff between false positives and true positives for better detection rate without the false alerts exceeding an acceptable value.

References

[1] Dorothy E. Denning, *Information warfare and security*, 1st ed., Amazon, USA, 1999.

[2] Yu-Xin Meng, The practice on using machine learning for network anomaly intrusion detection. In proceedings of international conference on machine learning and cybernetics, pages576-581(2011).

[3] Yu-Xin Meng, Lam-for Kwok, A case study: Intelligent false alarm reduction using fuzzy if-then rules in network intrusion detection, In international conference on fuzzy systems and knowledge discovery(FSKD)IEEE, pp 505-509,(2012)

[4] T.Pietraszek: Using adaptive alert classification to reduce false positives in intrusion detection." In: Recent advances in intrusion detection (RAID), Lecture notes in Computer Science, pp. 102--124 (2004)

[5] Hui-Hsuan Lin, Ching-Hao Mao, Hahn-Ming Lee, False alarm reduction by weighted-Score based rule adaptation through expert feedback, IEEE (2009).

[6] Heng-Sheng lin, Hsing-Kuo Pao et.al., Adaptive alarm filtering by causal correlation consideration in intrusion detection, pp.437-447, Springer-Verlag Berlin Heidelberg (2009).

[7] Nitin Mohan Sharma, Tapan P. Gondaliya, Enhance IDS false alarm filtering using KNN classifier, Research article, International journal of Emerging research in Management & Technology, May (2013).

[8] Chein-Yi Chiu, Yuh-Jye-Lee et.al., Semi-supervised learning for false alarm reduction,pp.595-605, Springer-Verlag Berlin Heidelberg (2010).

[9] DARPA intrusion detection evaluation, http://ww.ll.mit.edu/IST/ideval.

[10]UNB ISCX intrusion detection evaluation dataset, http:// www.iscx.ca/datasets.

[11] John E. Dickerson, Jukka Juslin, Ourania Koukousoula, Julie A. Dickerson, Fuzzy intrusion detection,pp.1506-1510,IEEE (2001).

[12]Peyman Kabiri and Ali A. Ghorbani, Research on intrusion detection and response:A survey, International journal on network security,pp84-102, September (2005).

[13]M.Bahrololum, E.Salahi and M.Khaleghi, Machine learning techniques for feature reduction in intrusion detection systems: A comparison, Fourth international conference on computer science and convergence information technology, IEEE (2009).