Adaptive Intrusion Detection Using Machine Learning

Neethu B

Department of Computer Science Amrita University

Abstract

This paper applies PCA for feature selection with Naïve Bayes for classification in order to build a network intrusion detection system. For experimental analysis, KDDCup 1999 intrusion detection benchmark dataset have been used. The 2 class classification is performed. The experimental results show that the proposed approach is very accurate with low false positive rate and takes less time in comparison to other existing approaches while building an efficient network intrusion detection system.

Keywords:

Naïve Bayes classifier, Principal component analysis KDD99 cup Dataset.

1. INTRODUCTION

Intrusion detection systems (IDS) are an important part of today's network security architectures, where it analyzes the network traffic and looks for potential threats. Intrusion detection techniques fall into two categories: Signature detection and anomaly detection. Signature or misuse detection searches for well known patterns of attacks, called attack signatures while anomaly detection is based on establishing a normal activity profile for a system and inspecting for any deviation from normal behavior is occured.

Intrusion detection systems (IDS) have become an integral part of today's information security infrastructures. The main aim of IDS is detecting unauthorized activities that attempt to compromise the confidentiality, integrity, and availability of computer systems or resources [1]. The concept of IDS was first introduced by James P. Anderson in 1980 [2] and later formalized by Dr. Dorothy Denning in 1986 [3]. With the sudden increase in the number of computer networks and the use of Internet has led to an increase of attacks from both external and internal intruders. One of the most important problem for intrusion detection is effective attributes selection from training dataset, because the volume of dataset that an IDS needs to examine is very large even for a small network and contains large number of attributes. It is harder to detect suspicious behavior patterns as the relationships exist between attributes of the dataset are very complex.

Intrusion detection can be considered to be a classification problem. The main issue in standard classification problems lies in minimizing the probability of error while making the classification decision. Hence, the key point is to choose an effective classification approach for building an accurate intrusion detection systems in terms of high detection rate while keeping a low false alarm rate.

Recently, data mining algorithms are using to build IDS that classifies network connections for detecting intrusions [8]. Lee developed a data mining framework for constructing attributes using domain-specific knowledge to built IDS [6]. Fan built IDS with a data mining technique that is a comprehensive study of cost-sensitive learning using classifier ensembles [29]. Maloof and Michalski investigate incremental learning algorithms and applied to intrusion detection [30]. They underline the significance of symbolic representation language and human understandability of background knowledge and criticized a neural network approach. An example of the application of symbolic learning to intrusion detection using user signatures is presented [31].

The purpose of this paper is to address some of the issues in most commonly used KDDCup 1999 dataset.

2. RELATED WORKS

The concept of intrusion detection began with Anderson's seminal paper in 1980[2].He introduced a threat classification model that develops a security monitoring surveillance system based on detecting anomalies in user behavior. Dr. Denning proposed several models for commercial IDS development based on statistics, Markov chains, time-series, etc in 1986 [14]. In the early 1980's, Stanford Research Institute (SRI) developed an Intrusion Detection Expert System (IDES) that monitors user behavior and detects suspicious events [15]. In 1988, a statistical anomaly-based IDS was proposed by Haystack [16], which used both user and group-based anomaly detection strategies. Forrest et al. proposed an analogy between the human immune system and intrusion detection that involved analyzing a program's system call sequences to build a normal profile [17]. In 2000, Valdes et al. [18] developed an anomaly based IDS that employed naïve Bayesian network to perform intrusion detecting on traffic bursts. In 2003, Kruegel et al. [19] proposed a multisensory fusion approach using Bayesian classifier for classification and suppression of false alarms that the outputs of different IDS sensors were aggregated to produce single alarm. Shyu et al. [20] proposed an anomaly based intrusion detection scheme using principal components analysis (PCA), where PCA was

Manuscript received March 5, 2013
Manuscript revised March 20, 2013

applied to reduce the dimensionality of the audit data and arrive at a classifier that is a function of the principal components. In 2003, Yeung et al. [21] proposed an anomaly based intrusion detection using hidden Markov models that computes the sample likelihood of an observed sequence using the forward or backward algorithm for identifying anomalous.

Mukkamala et al. [3] demonstrated the use of genetic programming approach for building an efficient network intrusion detection system. In [32], the authors propose various feature reduction techniques in order to build a network intrusion detection model in terms of detection accuracy and computation time. Network intrusion detection using Naïve Bayes classifiers is proposed in [33]. In [34], the authors use Bayesian belief network with genetic local search for intrusion detection. An evolutionary support vector machine for intrusion detection is proposed in[35].In this, the authors have combined evolutionary programming into support vector machines. They concluded that their model is able to detect new attacks as well as experienced attacks. A hybrid statistical approach which includes data mining and decision tree classification is used in [36]. Authors used decision tree and rule based classifiers for the performance comparisons in terms of accuracy and false alarm rate. A hybrid DTNB approach is used in [37] by combining Decision Table (DT) with Naïve Bayes to design an efficient intrusion detection model. The authors used Neuro-Fuzzy techniques (NEFCLASS) and JRip classifier to reduce false alerts in [38]. They take SNORT alerts as input and learning from training in order to achieve their goal. All the above papers used the KDDCup 1999 dataset for their experimentation.

3. INTRUSION DETECTION SYSTEMS

Intrusion Detection Systems are normally categorized into misuse detection and anomaly detection. The misuse detection system refers to known attacks that exploit the system. They can match the pattern on single events or multiple combinations of events. Anomaly detection refers to model the statistical knowledge about normal activity. Intrusions correspond to deviations from the normal activity of system. The main challenge in anomaly detection IDS is the difficulty in defining the normal activity because of the high variability in nominal usage. The false positive/ negative alarm rate in anomaly detection is high, compared to misuse detection systems. However, the anomaly detection is more effective in detecting new attacks or deviation from the nominal usage. The IDS is also classified based on the data source: Network IDS (NIDS) and Host-based IDS (HIDS) systems. The NIDS watch network traffic usually from one location or network interface. Therefore, NIDS can detect probes ,scans, malicious and anomalous activity across the whole sub network. It is also effective in identifying general traffic patterns for network and troubleshooting network problems. Its susceptibility to generate false alarms, as well as its inability to detect false negatives is its inherent weakness. HlDS technology does not have the benefits of watching the network to identify patterns like NlDS does. Instead, it watches the traces to access servers through the log data. A combination of host and network intrusion detection systems, in which a NlDS is placed at the network entry point and an HlDS at critical servers, is the best way to significantly reduce risk. Current intrusion detection systems are unsuccessful to cope with new, elegant and structured attacks, due to sever practical and theoretical limitations. These limitations have lead many researchers to apply different machine learning approaches for detecting anomalies.

4. MACHINE LEARNING

One of the main challenges for IDSs is to build effective behavior models or patterns to distinguish normal behaviors from abnormal behaviors by observing collected audit data. To solve this problem, earlier IDSs usually rely on security experts to analyze the audit data and construct intrusion detection rules manually. Since the amount of audit data, increases vary fast, it has become a time-consuming, tedious and even impossible work for human experts to analyze and extract attack signatures or detection rules from dynamic, huge volumes of audit data. Also the detection rules constructed by human experts are usually based on fixed features or signatures of existing attacks, so it will be very difficult for these rules to detect deformed or even completely new attacks.

Due to the above deficiencies of IDSs based on human experts, intrusion detection techniques using data mining have attracted more and more interests in recent years. As an important application area of data mining, intrusion detection based on data mining algorithms, which is usually referred to as adaptive intrusion detection, aims to solve the problems of analyzing huge volumes of audit data and realizing performance optimization of detection rules. By making use of data mining algorithms, adaptive intrusion detection models can be automatically constructed based on labeled or unlabeled audit data.

5. IMPLEMENTATION

A methodology for intrusion detection is proposed which involves a attribute selection method for selection of relevant attributes and there on applying a classifier for classifying network data to two classes : Normal Classes and attack classes.

A. Attributes Selection from Dataset

Effective attributes selection from intrusion detection datasets is one of the important research challenges for constructing high performance IDS. Irrelevant and redundant attributes of intrusion detection dataset may lead to complex intrusion detection model as well as reduce detection accuracy. This problem has been studied during the early work of W.K. Lee [5], research on KDD99 benchmark intrusion detection dataset, where 41 attributes were constructed for each network connection. The attribute selection methods of data mining algorithms identify some of the important attributes for detecting anomalous network connections. Attributes selection in intrusion detection using data mining algorithms involves the selection of a subset of attributes from the total original attributes of dataset, based on a given optimization principle. The attribute selection methods search through the subsets of attributes, and try to find the best one among the candidate subsets according to some evaluation function. Therefore, building IDS based on all attributes is infeasible, and attributes selection becomes very important for IDS. The attribute selection is done by using Principal Component Analysis (PCA).

A.1 Principal Component Analysis

PCA is a common statistical method used in multivariate optimization problems in order to reduce the dimensionality of data while retaining a large fraction of the data characteristic. First, PCA is used to project the training set onto eigenspace vectors representing the mean of the data. These eigenspace vectors are then used to predict malicious connections in a workload containing normal and attack behavior.

PCA reduces the amount of dimensions required to classify new data and produces a set of principal components, which are orthonormal eigenvalue/eigenvector pairs[11]. In other words, pca projects a new set of axes which best suit the data. In the implementation, these set of axes represent the normal connection data. Outlier detection occurs by mapping live network data onto these 'normal' axes and calculating the distance from the axes. If the distance is greater than a certain threshold, then the connection is classified as an attack. The principal components are derived from the covariance matrix When some values are much larger than others, then their corresponding eigenvalues have larger weights.

Each eigenvalue of a principal component corresponds to the relative amount of variation it encompasses. The larger the eigenvalue, the more significant its corresponding projected eigenvector. Therefore, the principal components are sorted from most to least significant ie in descending order. If a new data item is projected along the upper set of the significant principal components, it is likely that the data item can be classified without projecting along all the principal components. The eigenvectors of the principal components represent axes which best suit a data sample. Points which lie at a far distance from these axes would exhibit abnormal behavior. Outliers measured using the euclidian distance are the network connections that are anomalous. Using a threshold value (t), any network connection with a distance greater than the threshold is considered an outlier. In our work, an outlier is implied to be an attack.

1) Algorithm

1. Get input data
2. Subtract the mean
3. Calculate the covariance matrix
4. Calculate the eigenvectors and eigenvalues of the covariance matrix.
5. Sort the Eigen values in descending order.
6. Calculate the feature vectors.

Final Data=Row Feature vectors x Row Data Rowfeaturevector is the matrix in which eigenvectors in the columns transposed and RowDataAdjust is the mean adjusted input data

B . Classifier Construction

Classifier construction is another important challenge to build efficient IDS. Nowadays, many data mining algorithms have become very popular for classifying intrusion detection datasets such as decision tree, naïve Bayesian classifier, neural network, genetic algorithm, and support vector machine etc. However, the classification accuracy of most existing data mining algorithms needs to be improved, because it is very difficult to detect several new attacks, as the attackers are continuously changing their attack patterns. Anomaly network intrusion detection models are now used to detect new attacks but the false positives are usually very high. 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. Therefore classifier construction for IDS is another technical challenge in the field of data mining. The classifier used in the work is Naïve bayes Classifier.

B.1 Naïve Bayes Classifier

The Naive Bayes classifier is a classifier which uses a supervised learning algorithm based largely off of Bayes Theorem

$$P(A|B) = \frac{P(B|A)P(A)}{P(B)}$$

According to this theorem, calculate the probability of event A conditioned on data B by first calculating the probability of the data B conditioned by event A multiplied by the probability of event A and normalized by the probability of the data B. In regards to intrusion detection, this means calculating the probability that an attack is occurring based on some data by first calculating the probability that some previous data was part of that type of attack and then multiplying by the probability of that type of attack occurring.

The algorithm then works as follows: for each classification, look at every entry in the training set that was classified as the given classification. Assuming each feature is independently and identically distributed [5], the probability of the data given the classification is assumed to be normally distributed making the expected value of the probability the sample mean. So for each feature in the set of entries corresponding to this classification, model the probability by the mean value.For discrete values, this is calculated using the sample mean and for continues values, this is calculated via the definition of the normal distribution.

$$N(x|\mu, \sigma^2) = \frac{1}{(2\pi\sigma^2)^{1/2}} \exp\{-\frac{1}{2\sigma^2}(x-\mu)^2$$

Similarly, calculate the probability of the classification by again taking the sample mean i.e. counting all entries in the training set with this classification and dividing by the total number of entries. From these two values, calculate the probability that an event belongs to a given class. Do this for every class and the data is assigned whichever class yields the highest probability.

6. EXPERIMENTAL RESULTS

A. Dataset

The dataset used in the experiment is KDD99 cup dataset. The KDD Cup '99[13] dataset was created by processing the tcpdump portions of the 1998 DARPA Intrusion Detection System (IDS) Evaluation dataset, created by Lincoln Lab. Since one cannot know the intention (benign or malicious) of every connection on a real world network , the artificial data was generated in a closed network, using some proprietary network traffic generators, and hand-injected attacks.

The input to the system should be in ARFF (Attribute Relation File Format) format, because it is necessary to have type information about each attribute which cannot be automatically deduced from the attribute values. Before applying any algorithm to the data, it must be converted to ARFF format.

B. Evaluation And Results

Each data sample in KDD99 dataset represents attribute value of a class in the network data flow, and each class is labeled either as normal or as an attack with exactly one specific attack type. In total, 42 features have been used in KDD99 dataset 26] and each connection can be categorized into two main classes (normal class anomaly class).

1) Normal connections are generated by simulated daily user behavior such as downloading files, visiting b pages.
2) Anomaly class shows the anomalous behavior.

There are total 42 input attributes in KDD99 dataset [26] for each network connection that have either discrete or continuous values and divided into three groups. The first group of attributes is the basic features of network connection, which include the duration, prototype, service, number of bytes from source IP addresses or from destination IP addresses, and some flags in TCP connections. The second group of attributes in KDD99 is composed of the content features of network connections and the third group is composed of the statistical features that are computed either by a time window or a window of certain kind of connections. The experiment was conducted by comparing the results of the project with the other types of similar systems that uses different methods. The comparison results are given below: The total number of instances in the dataset is 125973.

Table 1 Classification

Classifier	Correctly classified instances	Misclassified instances
Naïve bayes +PCA	113902	12071
J48	92341	33632

The table shows that the newly devised system has lower misclassification error compared to the other approach. The comparison of various classifiers with the detection rates of normal and anomaly classes as the evaluation criteria.

From the table 2 we can understand the Naïve bayes+ PCA system as high accuracy compared with other method. The experiment was carried out over 10% KDDCup'99 data set. The performance of our system was evaluated by the detection rate and the false positive rate. The detection rate is the number of attacks detected by the system divided by the number of attacks in the data set. The false positive rate is the number of normal connections that are misclassified as attacks divided by the number of normal connections in the data set

Table 2 Performance Evaluation

Classifier	TP Rate	FP Rate	Precision	Recall	F-measure	Class
NB+ PCA	0.937	0.134	0.947	0.937	0.913	normal
	0.866	0.063	0.923	0.866	0.894	anomaly
J48	0.867	0.056	0.929	0.867	0.897	normal
	0.833	0.133	0.895	0.944	0.911	anomaly

Next, calculate the error rate, which is an estimate of the true error rate and is expected to be a good estimate, if the number of test data is large and representative of the population. It is defined as follows:

$$\text{Error Rate} = \frac{\text{(Total test data} - \text{total correctly classified data)}}{\text{Total test data}}$$

A “Confusion Matrix” is sometimes used to represent the result of testing. The Advantage of using this matrix is that it not only tells us how many got misclassified but also what misclassifications occurred.

The experiment was carried out using 125973 instances of which 113902 are correctly classified to the original classes and 12071 are incorrectly classified. The other performance measures were given in the above table. From these evaluation , it can be concluded that the system performs comparatively well.

7. CONCLUSION AND FUTURE WORK

The paper described a framework of Network IDS based on Naïve Bayes and Principal Component Analysis algorithm. The framework builds the patterns of the network services over data sets labeled by the services. With the built patterns, the framework detects attacks in the datasets using the naïve Bayes Classifier algorithm. Compared to the neural network and tree algorithm based approach, our approach achieve higher detection rate, less time consuming and has low cost factor. However, it generates somewhat more false positives. As a naïve Bayesian network is a restricted network that has only two layers and assumes complete independence between the information nodes. This poses a limitation to this research work. In order to alleviate this problem so as to reduce the false positives, active platform or event based classification may be thought of using Bayesian network. The work were continued in this direction in order to build an efficient intrusion detection model.. The system provides about 94% accuracy using this approach . The performance evaluation with KDD99 cup benchmark dataset is also done. The result obtained is encouraging as the approach is faster and accurate compared to some existing systems. This shows the accuracy of the system is greater compared with some of the earlier approaches. This approach can be extended to include more types of novel attacks and attacks can be classified to four classes that are (DOS, U2R, R2l, Probe) as a further improvement.

ACKNOWLEDGEMENT

I would like to record our gratitude to Dr. Ramachandra Kaimal of Computer Science Department, Amrita School of Engineering for his motivation and direction towards preparation of this paper. I would also like to express our gratitude to Amrita School of Engineering, Computer Science Department for providing us with facilities to complete our project.

REFERENCES

[1] Richard Heady, George Luger, Arthur Maccabe, and Mark Servilla, “The Architecture of a Network Level Intrusion Detection System,” Technical report, University of New Mexico, 1990.

[2] James P. Anderson, “Computer Security Threat Monitoring and Surveillance,” Technical report, James P. Anderson Co., Fort Washington, Pennsylvania. April 1980.

[3] Dorothy E. Denning, “An Intrusion Detection Model,” IEEE Transaction on Software Engineering, SE-13(2), 1987, pp. 222-232.

[4] Mukkamala S., Sung A. H. and Abraham A., “Intrusion Detection using Ensemble of Soft Computing paradigms,” In Proceedings of the 3rd International Conference on Intelligent Systems Design and Applications, Springer Verlag Germany, 2003, pp. 209-217.

[5] Commission of the European Communities, “Information Technology Security Evaluation Criteria,” Version 1.1.1991.

[6] MIT Lincoln Laboratory, http://www.ll.mit.edu/IST/idaval/

[7] Marcus A. Maloof, and Ryszard S. Michalski, “Incremental learning with partial instance memory,” In Proceedings of Foundations of Intelligent Systems: 13th International Symposium, ISMIS 2002, volume 2366 of Lecture Notes in Artificial Intelligence, Springer-Verlag, 2002,pp. 16-27.

[8] M. M. Sebring, E. Shellhouse, M. E. Hanna, and R. Alan Whitehurst. “Expert systems in intrusion detection: A case study”, In Proceedings of the 11th National Computer Security Conference, Baltimore, Maryland,

[9] W.K. Lee, S.J.Stolfo. “A data mining framework for building intrusion detection model”, In: Gong L., Reiter M.K. (eds.): Proceedings of the IEEE Symposium on Security and Privacy. Oakland, CA: IEEE Computer Society Press, 1999.

[10] W.K. Lee, et al., "Mining audit data to build intrusion detection models", In Proc. Int. Conf. Knowledge Discovery and Data Mining (KDD'98), pp.66-72, 1998.

[11] J. Ryan, M-J. Lin, R. Miikkulainen. “Intrusion detection with neural networks”, In Proceedings of AAAI-97 Workshop on AI Approaches to Fraud Detection and

A. Risk Management, 1997.

[12] Selecting Features for Intrusion Detection: A Feature Relevance Analysis on KDD 99 Intrusion Detection Datasets H. Güneş Kayacık, A. Nur Zincir-Heywood, Malcolm I. Heywood Dalhousie University, Faculty of Computer Science

[13] A Detailed Analysis of the KDD CUP 99 Data Set ,Mahbod Tavallaee, Ebrahim Bagheri, Wei Lu, and Ali A. Ghorbani

[14] N. B.Amor, S.Benferhat, and Z. Elouedi. “Naive Bayes vs decision trees in intrusion detection systems”, In Proc. 2004 ACM Symp. on Applied Computing, 2004.

[15] Feature selection using principal component analysis ,Fengxi Song, Zhongwei Guo, Dayong Mei ,Department of Automation and Simulation New Star Research Inst. of Applied Tech. in Hefei City Hefei, China.

[16] Correlation-based feature selection for intrusion detection design ,te-shun chou, kang k. yen, and jun luo, department of electrical and computer engineering florida international university Miami.

[17] A tutorial on principal component analysis, Lindsay I Smith.

[18] ADAM:A test bed for exploring the use of datamining in intrusion detection SIGMOD, vol30, no.4, pp 15-24, 2001.

[19] Tomas Abraham, “IDDM: INTRUSION Detection using Data Mining Techniques”, Technical report DTSO electronics and surveillance research laboratory,Sailsbury.

[20] Wenke Lee and Salvatore J.Stolfo, "A Framework for constructing features and models for intrusion detection systems”, ACM transactions on Information and system security (TISSEC), vol.3, Issue 4, Nov 2000.

[21] S.chavan, K.Shah, N.Dave, S.Mukherjee, A.Abraham, and S.Sanyal, "Adaptive neuro-fuzzy Intrusion detection syatems”, ITCC, Vol 1, 2004.

[22] Z. Zhang, J. Li, C.N. Manikapoulos, J.Jorgenson, J.ucles, "HIDE: A hierarchical network intrusion detection system using statistical pre-processing and neural network classification”, IEEE workshop proceedings on Information assurance and security, 2001, pp.85-90.

[23] Roy-I Chang, Liang-Bin Lai, et al, "Intrusion detection by back propagation network with sample query and attribute query”, International Journal of computational Intelligence Research,Vol..3, no.1, 2007, pp 6-10.

[24] S. Axelsson, "The base rate fallacy and its implications for the difficulty of Intrusion detection”, Proc. Of 6th.ACM conference on computer and communication security 1999.

[25] R.Puttini, Z.marrakchi, and L. Me, "Bayesian classification model for Real time intrusion detection”, Proc. of 22nd. International workshop on Bayesian inference and maximum entropy methods in science and engineering, 2002.

[26] An Introduction to the WEKA Data Mining System,Zdravko Markov Central Connecticut State University markovz@ccsu.edu ,Ingrid Russell University of Hartford.

[27] An evaluation of machine learning techniques in intrusion detection By Christina lee.

[28] Dimensionality Reduction by Manoranjan Dash.

[29] Wei Fan, “Cost-Sensitive, Scalable and Adaptive Learning using Ensemble-based Methods,” PhD thesis, Columbia University, 2001.

[30] M.A. Maloof and R.S. Michalski, “A partial memory incremental learning methodology and its applications to computer intrusion detection,” Reports of the Machine Learning and Inference Labor

[31] atory MLI 95-2, Machine Learning and Inference Laboratory, George Mason University, 1995.

[32] Kenneth A. Kaufman, Guido Cervone, and Ryszard S. Michalski, “An application of Symbolic Learning to Intrusion Detection: Preliminary Result from the LUS Methodology,” Reports of the Machine Learning and Inference Laboratory MLI 03-2, Machine Learning and Inference Laboratory, George Mason University, 2003.

[33] V. Venkatechalam and S. selvan, Performance comparison of intrusion detection system classification using various feature reduction techniques. International journal of simulation. Vol. 9, No. 1, pp.30-39, 2008.

[34] M. Panda and M.R.Patra, Network intrusion detection using Naïve Bayes . International journal of computer science and network security, Vol. 7, No. 12, pp. 258-263, 2007.

[35] M.Panda and M.R. Patra, Bayesian belief network using genetic local search for detecting network intrusions. International journal of secure digital information age (IJSDIA), Vol. 1, No. 1, pp. 34-44, 2009.

[36] Sung –Hae Jun and Kyung –whan oh, An evolutionary support vector machine for intrusion detection. Asian journal of information technology, Vol. 5, No. 7, pp. 778-783, 2006.

[37] N. B. Annur, H.Sallehudin, A. Gani and O.zakari. identifying false alarm for network intrusion detection system using hybrid data mining decision tree. Malaysian journal of computer science, Vol.21, No. 2, pp.101-115, 2008.

[38] M. Panda and M.R. Patra. A semi-Naïve Bayesian method for detecting network intrusions. LNCS, Vol. 5863, pp. 614-621, 2009.

[39] P.Gaonjur, N. Z. Tarapore and S.G.Pokale. using neuro-fuzzy techniques to reduce false alerts in intrusion detection. In: Proceedings of International conference on Computer Networks and Security, India, pp. 1-6, 2008. IEEE Press.