SURVEY ON CLASSIFICATION TECHNIQUES FOR INTRUSION DETECTION

Pritam Sapate[1] and Shital A. Raut[2]

[1,2]Department of Computer Science and Engineering, VNIT, Nagpur, India
pritamsapate@gmail.com
saraut@cse.vnit.ac.in

ABSTRACT

Intrusion detection is the most essential component in network security. Traditional Intrusion Detection methods are based on extensive knowledge of signatures of known attacks. Signature-based methods require manual encoding of attacks by human experts. Data mining is one of the techniques applied to Intrusion Detection that provides higher automation capabilities than signature-based methods. Data mining techniques such as classification, clustering and association rules are used in intrusion detection. In this paper, we present an overview of intrusion detection, KDD Cup 1999 dataset and detailed analysis of different classification techniques namely Support vector Machine, Decision tree, Naïve Bayes and Neural Networks used in intrusion detection.

KEYWORDS

Intrusion Detection, Data Mining, KDD Cup 1999, Classification.

1. INTRODUCTION

Internet plays vital role in today's world. It is used in business, education, shopping, social networking etc. This has increased risk of computer systems connected to the internet becoming targets of intrusions by cyber criminals. Cyber criminals attack systems to gain unauthorized access to information, misuse information or to reduce the availability of information to authorized users. This results in huge financial losses to companies besides losing their goodwill to customers. Intrusion prevention techniques such as user authentication (e.g. using password or biometrics), information protection (e.g. encryption), avoiding programming errors and firewalls have been used to protect computer systems. But, unfortunately these intrusion prevention techniques alone are not sufficient. There will always be unknown exploitable weaknesses in the system due to design and programming flaws in application programs, protocols and operating systems. Therefore, we need mechanism to detect intrusions as soon as possible and take appropriate actions [1].

Intrusion detection system monitors data coming from the network and various system logs and analyses them to detect potential attacks. Traditional intrusion detection methods are based on extensive knowledge of signatures of known attacks. The signatures describing attacks have to be hand-coded by human experts. Newly captured events are then matched against the available signatures of attacks to detect intrusion. Whenever new type of intrusion is discovered, the

Dhinaharan Nagamalai et al. (Eds) : ACITY, WiMoN, CSIA, AIAA, DPPR, NECO, InWeS - 2014
pp. 223–231, 2014. © CS & IT-CSCP 2014 DOI : 10.5121/csit.2014.4523

signature database has to be manually revised by human expert. In other words, signature-based approach has failed to provide required level of automation. Other techniques including statistical methods, machine learning and data mining methods have been proposed as a way of dealing with limitations of signature-based approaches. These techniques provide higher automation in intrusion detection process along with good detection rate. Currently many researchers have shown an increasing interest in intrusion detection techniques based on data mining techniques [2] [3].

Data mining based intrusion detection techniques can be classified into two categories: misuse detection and anomaly detection. In misuse detection technique, each instance in a dataset is labelled either as 'normal' or 'intrusion' and learning algorithm is trained over labelled data to build model. Whenever a new type of attack is discovered, learning algorithm can be retrained with new dataset that includes labelled instances of new attack. In this way, models of misuse detection are created automatically and can be more precise than manually created signatures. In anomaly detection technique, models are built on normal behaviour and any deviation from normal behaviour is identified as intrusion [2].

This paper is organized as follows: Section 2 describes attack types, intrusion detection and general working of intrusion detection systems. Section 3 gives details of KDD Cup 1999 benchmark intrusion detection dataset. Data mining and intrusion detection are discussed in Section 4. Section 5 presents detailed analysis of different classification techniques used for intrusion detection. Finally conclusion is mentioned in section 6.

2. BACKGROUND

2.1. Attack Types

According to taxonomy proposed by kendall [4], attacks can be classified into following four categories:

2.1.1. Denial of Service (DoS)

A denial-of-service (DoS) or distributed denial-of-service (DDoS) attack is an attack in which the attacker tries to make computer resource too busy or too full to respond to its intended users. Examples of such attacks include Smurf, Teardrop, Back, Ping of death, Neptune, Land etc.

2.1.2. User to Root

A User to Root is an attack that aims to gain super user access to the system. Attacker gain super user access by exploiting vulnerability in operating system or application software. The attacker starts out with access to a normal user account on the system (perhaps gained by sniffing password, a dictionary attack or social engineering) and is able to exploit some vulnerability to gain root access to the system. Most common attack in this class of attack is buffer overflow attack. Other attacks include Loadmodule, Perl, Ps, Xterm etc.

2.1.3. Remote to User

A Remote to User is an attack in which the attacker tries to gain unauthorized access from a remote machine into super user account of the target system. In this type of attack, attacker sends packets to a machine over a network and then exploits some vulnerability to gain local access as a user of that machine. Examples of remote to user attack are Dictionary, Ftp_write, Guest, Imap, Phf etc.

2.1.4. Probing

Probing is an attack in which the attacker scans a network of computers to gather information or find known vulnerabilities. An attacker who knows which machines and services are available on network can use this information to look for weak points. He will use this information to plan future attacks. There are many tools available for probe attack which can be used by even a very unskilled attacker. Examples of probing attack are Ipsweep, Mscan, Nmap, Saint, Satan etc.

2.2. Intrusion detection

Intrusion detection is the act of detecting actions that tries to compromise the confidentiality, integrity and availability of a resource. Based on analysis strategy intrusion detection techniques can be divided into [1] [24]:

Anomaly Detection. Anomaly detection tries to determine whether deviation from normal usage pattern can be flagged as intrusion. It establishes normal usage patterns using statistical measures on system audit data and network data. The major limitation of this technique is high false alarm rate.

Misuse Detection. Misuse detection uses patterns of well known attacks to identify intrusions. It is very good at detecting known attacks. The main disadvantage of such system is it is unable to detect any future (unknown) intrusions that don't have matched pattern stored in the system.
Based on the source of audit data Intrusion detection techniques can be divided as Host based and network based.

Host-Based IDS. Data coming from various host activities including audit records of operating system, system logs and process activities is used for analysis.

Network-Based IDS. Data coming from network traffic is collected for analysis using sniffing software like TCPDUMP.

2.3. Working of intrusion detection systems

Following four steps are proposed for generalized working of IDS by authors of [6].

2.3.1. Data Collection

Data useful for detecting intrusion is collected in this step. For network-based intrusion detection network traffic is collected using sniffer software like TCPDUMP. For host-based intrusion detection data such as process activity, disk usage, memory usage and system calls are collected. Commands such as netstas, ps and strace are used for this purpose.

2.3.2. Feature selection

The collected data is substantially large and cannot be used as it is, so subset of this data is selected by creating feature vectors that contain only necessary information needed for intrusion detection. In network based intrusion detection, it can be IP packet header information which includes source and destination IP addresses packet length, layer four protocol type and other flags. In host-based intrusion detection it includes user name, login time and date, duration of session and number of opened files.

2.3.3. Analysis

The collected data is analyzed in this step to determine whether the data is anomalous or not. This is the main research area where many methods have been proposed and used to detect intrusion.

2.3.4. Action

IDS alerts the system administrator that an attack has happened using several methods like e-mail, alarm icons and visualization techniques. IDS can also stop or control attack by closing network ports or killing processes.

3. INTRUSION DETECTION DATASET

In this section, brief description of KDD Cup 1999 dataset [4][16] which was derived from the 1998 DARPA intrusion detection evaluation program is provided. It is the most widespread dataset collected over a period of nine weeks for a LAN simulating a typical U.S. Air Force LAN. The dataset contains a collection of simulated raw TCP dump data, where multiple intrusion attacks were introduced and widely used in the research community. From seven weeks of network traffic, four gigabytes of compressed binary TCP dump training data was processed into five million connection records. Similarly, two weeks of test data yielded about two million connection records. The dataset contains 4,898,430 labelled and 311,029 unlabeled connection records. The labelled connection records consist of 41 features. Features characterizing each connection are divided into:

- basic features of individual TCP connections,
- content features within a connection suggested by domain knowledge,
- time based features computed using a two second time window and
- host based features computed using a window of 100 connections used to characterize attacks that scan the hosts (or ports) using much larger time interval than two seconds.

In network data of KDD99 dataset, each instance represents feature values of a class, where each class is categorized either as normal or attack. The classes in dataset are divided into one normal class and four main intrusion classes: Denial of Service (DoS), Probe, User-to-Root (U2R), Remote-to-Login (R2L).

4. DATA MINING AND INTRUSION DETECTION

Data mining is used in applications that require data analysis. In recent years, data mining techniques have been highly researched in intrusion detection domain. Different data mining techniques such as classification, clustering, and association rules are used to acquire information about intrusions by analysing system audit data and network data [1][9]. The main approach of data mining is classification, which maps a data item into one of several predefined categories. Here we present a review of different classification techniques used for detecting intrusions.

5. CLASSIFICATION TECHNIQUES FOR INTRUSION DETECTION

Classification is the process of assigning each data instance to one of the predefined categories. Data classification is a two step process: Learning and classification. In first step, classifier is built by analysing a training set made up of data instances and their associated class labels. Because the class label of each training instance is provided, this is known as supervised learning. In second step, built classifier is used to predict the class for unlabelled data instance. Different

types of classification techniques are decision trees, neural networks, bayesian classification, support vector machines, nearest neighbour classification, genetic algorithm and fuzzy logic [10].

Intrusion detection can be thought of as a classification problem. We can gather sufficient audit data in which each data instance will be labelled as either "normal" or "abnormal". We then use classification algorithm on audit data to build classifier. This classifier will then predict class of new unseen audit data as "normal" or "abnormal". Classification approach can be used for both misuse detection and anomaly detection but it is mostly used for misuse detection [1]. In this section, we present an overview of different classification techniques used for intrusion detection.

5.1. Support Vector Machine

Support vector Machine (SVM), a promising pattern classification technique, proposed by Vapnik [19]. SVMs are supervised learning models with associated learning algorithms that have been applied increasingly to misuse detection in the last decade. SVM maps the input vector into a higher dimensional feature space and obtain the optimal separating hyper-plane in the higher dimensional feature space.

Srinivas Mukkamala and Guadalupa Janoski [20] proposed Support Vector Machine (SVM) and Neural Networks (NN) for intrusion detection system. Two main reasons for using SVM for intrusion detection are: speed and scalability. The experiments were carried using DARPA 1998 dataset. The training time for SVMs is significantly shorter (17.77 sec) than that for neural networks (18 min). This becomes an important advantage in situations where retraining needs to be done quickly. The performance of SVM showed that SVM IDS have slightly higher rate of making the correct detection than neural networks. However, SVMs can make only binary classifications which will be disadvantage when IDS requires multiple-class identifications.
Chen R. C. et al. [25] proposed use of Rough Set Theory (RST) and Support Vector Machine (SVM) for intrusion detection. They used KDDCUP99 dataset for experiment. RST is used to pre-process the data and to reduce the number of features. The features selected by RST are used to learn the SVM model and to test the model respectively. Using all 41 features accuracy was 86.79% and false positive rate was 29.97%. While with 29 features selected using RST accuracy was 89.13% and false positive rate was reduced to 13.27%. This shows that method is effective in increasing accuracy and reducing false positive rate.

Wang Hui et al. [26] proposed an intrusion detection method based on improved SVM by combining Principal Component Analysis (PCA) and Particle Swarm Optimization (PSO). KDDCUP99 dataset was used for experiment. PCA is an effective data mining technique used to reduce dimensionality of dataset. Then PSO was used to elect punishment factor C and kernel parameters σ in SVM. The intrusion detection rate (97.752%) of improved SVM by combining PCA and PSO was higher than those of PSO-SVM (95.635%) and that of standard SVM (90.476%).

5.2. Decision tree

Quinlan [13] proposed a decision tree classifier which is one of the most known machine learning techniques. A decision tree composed of three basic elements [14]:

- A decision node representing test or condition on data item.
- An edge or a branch which corresponds to the one of the possible attribute values which means one of the test attribute outcomes.
- A leaf which determines the class to which the object belongs.

To classify an object, one starts at the root of the decision tree and follows the branch indicated by the outcome of each test until a leaf node is reached. The name of the class at the leaf node is the class of an unknown object. The best attribute to divide the subset at each stage is selected using the information gain of the attributes.

Ben Amor et al. [14] performed experiment on KDDCUP99 intrusion data set for comparative analysis of naïve bayes versus decision tree. They found that decision tree gives slightly better results than naïve bayes. However, from computational point of view, construction of decision tree is slower than naïve bayes. The decision tree selects the best features for each decision node during the construction of the tree based on some well defined criteria. Decision trees generally have very high speed of operation and high attack detection accuracy. The Naïve Bayes classifiers make strict independence assumption between the features in an observation that result in lower attack detection accuracy when the features are correlated.

In [14] they used all 41 features in KDDCUP99 dataset. However, Gary Stein et al. [15] suggest that not all 41 features are required for classification of four categories of attack: Probe, DOS, U2R and R2L. In their work they used Genetic Algorithm to select relevant features for decision tree, with a goal of increasing detection rate and decreasing false alarm rate. They performed experiment for each of the above four categories of attack separately. The GA made drastic improvements in some of the categories like performance gain on Probe is 23% on the average. However, Performance improvement on R2L and U2R are limited. This may be because the proportions of R2L and U2R are very low in the training data, but much higher in the testing data.

S. Sheen and R. Rajesh [23] used three different approaches for feature selection namely Chi square, Information Gain and ReliefF and compared the performance of these three approaches using decision tree classifier. The KDDCUP99 dataset is used for experiment. They found that Chi square and information gain had similar performance while ReliefF was giving a lower performance.

5.3. Naïve Bayes

Naïve Bayes can be considered as an upgraded version of Bayes Theorem as it assumes strong independence among attributes. Bayesian classifier encodes probabilistic relationships among variables of interest. This means that the probability of one attribute does not affect the probability of the other.

Mrutyunjaya Panda and Manas Ranjan Patra [17] proposed a framework of network intrusion detection system based on naïve bayes algorithm. They performed experiment on 10% KDDCUP99 dataset and evaluated system using 10-fold cross validation. Their approach achieved higher detection rate than neural network based approach. The detection rate was 95%, with an error rate of 5%. Moreover, it performed faster and was cost effective. However, it generates somewhat more false positives.

Dewan Md. Farid et al. [18] proposed a new hybrid learning algorithm for adaptive network intrusion detection using naive Bayesian classifier and ID3 algorithm. They evaluated the performance of proposed algorithm for network intrusion detection using 10% of KDDCUP99 dataset. The attacks of KDD99 dataset were detected with 99% accuracy and minimized false positives.

In [29] Z. Muda et al. proposed use of a hybrid learning approach through combination of K-means clustering and naïve bayes classification. An experiment is carried out using KDDCUP99 dataset to evaluate the performance. In first stage, they grouped similar data instances based on

their behaviours by utilizing a K-Means clustering. In second stage, they used Naïve Bayes classifier to classify resulting clusters into attack classes. This approach detected better percentage of attacks with above 99% of accuracy and detection rate and below 0.5% of false alarm.

5.4. Neural Networks

A neural network consists of a collection of processing elements that are highly interconnected and transform a set of inputs to a set of desired outputs. The result is determined by the characteristics of the elements and the weights associated with the interconnections between them. By modifying the connections between the nodes, the network can adapt to the desired outputs. Neural networks have been used in both anomaly detection and misuse detection. For anomaly detection, neural networks were modelled to learn the typical characteristics of system users and identify significant variations from the user's established behaviour as anomaly. In misuse detection, the neural network would receive data from the network stream and analyze the information for instances of misuse [22].

Ryan et al. in [21] performed first works to intrusion detection using NN. They trained and tested a back propagation neural network called NNID (Neural Network Intrusion Detector) on a system of ten users. The data source for training and testing was operating system logs in UNIX environment. The system showed 96% accuracy in detecting unusual activity with 7% false alarm rate.

Jirapummin et al. [27] presented a methodology for both visualizing intrusions by using SOM and classifying intrusions by using Resilient Propagation. They selected Neptune attack (SYN flooding), Portsweep and Satan attacks (port scanning) from KDD Cup 1999 dataset. For Resilient Propagation algorithm (RPROP), they utilized 3-layer NN with 70 nodes in first hidden layer, 12 neurons in second hidden layer and 4 neurons in the output layer. The transfer functions for the first hidden layer, second hidden layer and the output layer of RPROP were tan-sigmoidal, log-sigmoidal and log-sigmoidal respectively. They achieved more than 90 % detection rate and less than 5 % false alarm rate in three selected attacks.

Iftikhar Ahmad, et al. [28] performed comparison between three back propagation algorithms used in intrusion detection. These three algorithms were:

a. The basic On-Line BackProp algorithm,
b. The Batch BackProp algorithm and
c. The Resilient BackProp algorithm.

They performed experiment on KDDCUP99 dataset and found that the Resilient BackProp algorithm give better performance than online and batch.

6. CONCLUSIONS

Data mining techniques have been highly researched in the domain of intrusion detection in order to reduce the hassle of manually analysing huge volumes of audit data. In this paper, we reviewed different classification approaches used by researchers for detecting intrusion. The challenge is to achieve high detection rate and reduce false alarm rate. Any one classifier alone is not sufficient to achieve this. More than one classifier can be combined to remove disadvantages of one another. Combining classifiers lead to a better performance than any single classifier.

REFERENCES

[1] Lee, W., & Stolfo, S. (1998), "Data mining approaches for intrusion detection," In Paper presented at the proceedings of the seventh USENIX security symposium (SECURITY'98). San Antonio, TX.

[2] Paul Dokas , Levent Ertoz, V Kumar, Lazarevic, Srivastava & Pang-Nig Tan, "Data Mining for Network Intrusion Detection," In Proc. 2002 NSF Workshop on Data Mining, pp. 21-30.

[3] C. A.Catania and C. G.Garino, "Automatic Network Intrusion Detection: Current Techniques and Open Issues," Computer & Electrical Engineering 5 (2012), pp. 1062-1072.

[4] K. Kendall, "A Database of Computer Attacks for the Evaluation of Intrusion Detection Systems," Massachusetts Institute of Technology Master's Thesis, 1998.

[5] LI Min, An Yang Institute of Technology,."Application of DataMining Techniques in Intrusion Detection," 2005.

[6] Khaled Labib, "Computer Security and Intrusion Detection," from Crossroads The ACM students magazine.

[7] Chang-Tien Lu,Arnold P.Boedihardjo,Prajwal Manalwar, "Exploiting efficient data mining techniques to enhance Intrusion Detection Systems," 0-7803-9093-8/05/$20.00 2005 IEEE, pp. 512-517.

[8] Brugger S. T, "Data mining methods for network intrusion detection," Technique Report, UC davis, 2004.

[9] Portnoy, L., Eskin, E., and Stolfo, S. 2001, "Intrusion detection with unlabeled data using clustering," In Proceedings of the ACM Workshop on Data Mining Applied to Security.

[10] Data mining: concepts and techniques by jiawei Han, Michelle Kamber.

[11] Wang, H., Zhang, G., Chan, H. & Jiang, X. 2009, "Mining Association Rules for Intrusion Detection," International Conference on Frontier of Computer Science and Technology.

[12] Reema Patel, AmitThakkar, Amit Ganatra, "A Survey and Comparative Analysis of Data Mining Techniques for Network Intrusion Detection Systems," International Journal of Soft Computing and Engineering (IJSCE), Vol-2, 2012.

[13] Quinlan, C4.5: Programs for Machine Learning, 1993, Morgan Kaufmann Publishers, San Mateo, CA.

[14] Ben Amor, Benferhat, Elouedi, "Naive Bayes vs. Decision Trees in Intrusion Detection Systems," Proc. of the 2004 ACM symposium on applied computing, 2004, pp. 420–424.

[15] Stein G, Chen B, Wu AS, Hua KA (2005), "Decision tree classifier for network intrusion detection with GA-based feature selection," In: Proceedings of the 43rd annual southeast regional conference ACM vol 2, pp 136–141.

[16] KDD. http://kdd.ics.uci.edu/databases/kddcup99.

[17] Mrutyunjaya Panda, Manas Ranjan Patra, "Network Intrusion Detection Using Naïve Bayes," International Journal of Computer Science and Network Security,vol.7 no.12, 2007, pp.258-262.

[18] Dewan Md. Farid, Nouria Harbi, Mohammad Zahidur Rahman, "Combining Naive Bayes and Decision Tree for daptive Intrusion Detection," Proc. Of Intl. Journal of Network Security & Its Applications (IJNSA), Vol. 2, No. 2, 2010, pp.12-25.

[19] Cortes, Vapnik, Support-vector networks, Machine Learning, vol.20, 1995, pp.273–297.

[20] Srinivas Mukkamala, Guadalupe Janoski, Andrew Sung, "Intrusion Detection: Support VectorMachines and Neural Networks," In Proceedings of the IEEE International Joint Conference on Neural Networks, 2002, pp. 1702-1707

[21] 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 Task Management, 1997, pp. 92–97.

[22] J. Cannady, "Artificial Neural Networks for Misuse Detection," National Information Systems Security Conference, 1998.

[23] S. Sheen and R. Rajesh, "Network Intrusion Detection using Feature Selection and Decision tree classifier," IEEE Region 10 Conference, TENCON08 (2008), pp. 1–4.

[24] A. Lazarevic, V. Kumar and J. Srivastava, "Intrusion detection: A survey," Managing Cyber Threats, pp.19 -78, 2005.

[25] Chen R. C., Cheng K. F., and Hsieh C. F., "Using rough set and support vector machine for network intrusion detection," International Journal of Network Security & Its Applications (IJNSA), Vol. 1, No. 1, 2009, pp. 1–13.

[26] WANG Hui, ZHANG Guiling, E Mingjie, SUN Na, "A Novel Intrusion Detection Method Based on Improved SVM by Combining PCA and PSO," Wuhan University Journal of Natural Sciences, 2011, vol. 16, No. 5, pp. 409-413.

[27] Jirapummin, C., Wattanapongsakorn, N. and Kanthamanon P, "Hybrid Neural Networks for Intrusion Detection System," The 2002 International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC 2002), pp. 928-931, Phuket, Thailand.

[28] Iftikhar Ahmad, Dr. M.A Ansari, Dr. Sajjad Mohsin,"Performance Comparison between Backpropagation Algorithms Applied to Intrusion Detection in Computer Network Systems," Proceedings of the 7th WSEAS International Conference on Applied Computer and Applied Computational Science as ACM guide, pp. 47-52, 2008.

[29] Z. Muda, W. Yassin, M.N. Sulaiman, N.I. Udzir. "Intrusion Detection based on K-Means Clustering and Naïve Bayes Classification," 7th International Conference on IT in Asia (CITA), 2011.

AUTHORS

Mr. Pritam Sapate is currently an M.Tech student at Visvesvaraya National Institute of Technology, Nagpur. He has received his B.Tech degree in Information Technology from S.G.G.S.I.E. & T, Nanded (M.H).

Mrs. Shital A. Raut is an Assistant Professor at Visvesvaraya National Institute of Technology, Nagpur. Her areas of interest include Data Mining and Warehousing and Business Information Systems.