Intrusion detection for computer network Using machine learning algorithms

[1] Rega Janasri [2] Dr S. Jhansi Rani
[1]M.Tech Scholar, Department of Computer Science and System Engineering,
Andhra University College of Engineering (A), Visakhapatnam, AP, India.
[2]Department of Computer Science and System Engineering,
Andhra University College of Engineering (A), Visakhapatnam, AP, India.

Abstract: In the previous decades, the fast development of Intrusion Detection and Prevention systems played a crucial role in computer networks and security. The Intrusion Detection Systems (IDS) helps to implement several incorporate methods to identify and find intrusive and non-intrusive actions involved in network. The most existing systems based on human experts to analyses the network traffic and system logs to identify the intrusive patterns. But it is a big problem for human to detect the intrusions for a numerous data of network traffic. An IDS has the ability to perform autonomously over the huge network without having intervention of human. The Intrusion detection techniques based on soft computing and machine learning techniques used to detect anonymous data. The IDS can be designed efficiently using soft computing techniques. The main function of Intrusion Detection System is to protect the resources from threats. It analyses and predicts the behaviors of users, and then these behaviors will be considered an attack or a normal behavior. In this paper, we analyses the results of the attacks classified using Intrusion Detection System, and the training time of machine algorithms are measured by increasing the size of the KDD dataset in intervals thereby observing the changes in the final evaluation metrics obtained.

Index Terms **– Classification, Intrusion detection system, KDD dataset, Evaluation metrics.**

I. INTRODUCTION

With the advancement in information and communication technology, threats like intrusions are very likely to occur. The security tools like, access control scheme, firewalls, antivirus software to protect important information from such attacks are highly desirable to enhance the security against these attacks. Intrusion Detection Systems (IDS) have been introduced as a tools designed to enhance security of systems [1]. Various IDS approaches have been proposed in the literature since inceptions, but two of them are proposed by Steniford at al., and Denning are most relevant in this context [2].

Denning's proposal for an intrusion detection system focused on how to develop effective and accurate methods for intrusion detection. During early days of development of such system combination statistical and expert systems based approaches was very popular. Now a day's machine learning based intelligent techniques are most widely accepted and used for developing a training set to detect intrusions. Classification, clustering and rule based techniques are commonly used machine learning techniques.

For intrusion detection system automatically constructing models will work as system has to be trained with latest intrusion behaviour, huge traffic on network, and imbalanced attack class distribution. Under these requirements, Artificial intelligence based machine learning techniques not sufficient alone to achieve high matching / detection accuracy and less computational times. Fortunately, machine learning based techniques has property to adapt and tuned its parameters under varying conditions and can be utilized as techniques for fault detection and fault tolerance, resilience against noisy information and high computational speed to compensate these requirements.

Intrusion detection system used to detect the malicious access, duplication, modification and destruction of information systems. The two types of intrusions include internal intrusions and external intrusions. There are two types of intrusions. The intrusions form outside the organization (External intrusions), and intrusions from inside the organization (Internal intrusions). An intrusion is defined as any set of actions that attempt to harm or damage the data which includes a deliberate Unauthorised accesses to the information, manipulate information, or make a system unreliable. Intrusion detection system is a model designed to detect attacks among the various type of packets. It is the process of examining the events which occurs in a computer system or network and analyzing them for presence of intrusions

II. BACKGROUND

A. Intrusion Detection System

An intrusion detection system is a tool used for automatic detection and removal of external attack or access to the system and takes a decision to determine whether these attacks constitute a legitimate use of the system or are intrusions [3]. Figure 1 represents the organization of IDS where solid arrows indicate data/control flow while dotted arrows indicate a response to intrusive activities.

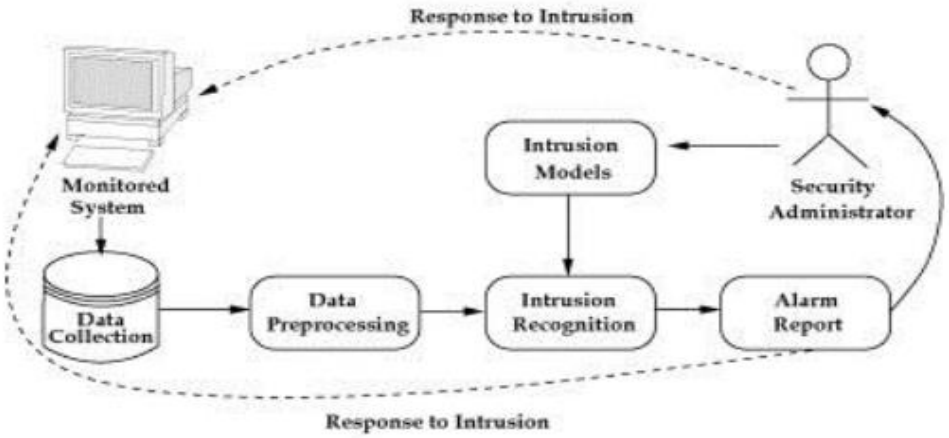

Figure 1. A general organization of a typical intrusion detection system

In general, this paper classifies IDSs on the basis of detection methods they employ into two categories, like (i) misuse detection and (ii) abnormality detection. By matching observed data, misuse detection identifies intrusions with pre-defined descriptions of intrusive behaviour. So prominent intrusions can be detected in an efficient manner utilizing a low false positive rate. Therefore, this technique is widely adopted in the majority of commercial systems. However, the types of new intrusions have evolved every moment and continuously, therefore. Misuse the previous techniques for intrusion detection will fail to detect new unknown intrusions. The only way to get rid over this issue is to learn from all intrusions and get update the data knowledge at every moment. This updating process can either be manual or automatic, the manual process might be very time consuming and also the human intervention is required at every moment of time. This process can work automatically using supervised machine learning techniques. Unfortunately, the preparation of datasets for training the supervised learning algorithms is very difficult and expensive, as this require collection and labeling of each event as normal or an intrusion type.

III. MACHINE LEARNING TECHNIQUES

The machine learning techniques have been used since 1969.The ML[1] is defined by Arthur Samuel as "field of study that gives computers the ability to learn without being explicitly programmed." It predicts and categorizes based on previously known characteristics learned from the training data. The ML algorithms need a objective from the domain. The ML Techniques consist of two stages.

i) Training
ii) Testing

The steps implemented in the Machine Learning are

- Identify class features and classes from training data.
- Select subset of features desired for classification.
- Construct the model using training data.
- Use the learned model to categorize the data.

In the testing phase, the normal pattern is defined for detecting anomalies. In the training phase, the learned model is applied into new data and each pattern is classified into normal or anomalous. There are three approaches of ML techniques [5] ***Unsupervised*** The task is finding to defined patterns, structures, knowledge in unlabeled data

- Expectation-maximization algorithm[5]
- Vector Quantization
- Generative topographic map
- Information bottleneck method
- Self-organizing map
- Apriori algorithm
- Single-linkage clustering
- K-means algorithm
- Fuzzy clustering
- Local Outlier Factor

Semi-supervised A part of data labeled when the acquirement of data by human experts is known as Semi-Supervised learning

- Generative models
- Low-density separation
- Graph-based methods

• Co-training

Supervised The task is find a function or a model in a completely labeled data.

• Artificial Neural Network
• Bayesian network
• Gaussian process regression
• Lazy learning
• Decision trees, Decision graphs
• Nearest Neighbor Algorithm
• Support vector machines
• Random Forests
• Bootstrap aggregating
• Information fuzzy networks
• Linear regression
• Naive Bayes classifier
• k-nearest neighbor
• Hidden Markov models

IV. LITERATURE SURVEY

In this section discussed about the researches carried out in the area of intrusion detection system. The two approaches used to detect intrusions are Expert based and Statistical based approaches. The expert based intrusion detection system detects the well-known attacks. The drawback is it will not detect the newly attacking intrusion.The statistical based approach used to identify the new intrusions. There are several datasets available, the KDD cup 99 and NSL KDD cup 99 datasets applied for the following research.

Kumar and Koyal [6] implementeda n IDS that classified the smurf attacked labels using genetic algorithms and achieved 0.2% low positive ratio. Abdullah [7] explained some classification rules for detecting intrusion by genetic algorithm. Ojugo et at.[8] used the fitness function on the genetic algorithm for evaluating the rules. The machine learning techniques are developed to identify intrusions. The Roshani[9] applied Artificial Neural Network (ANN) algorithm for detecting intrusions. The fuzzy clustering and ANN techniques are combined and it overcomes the weak stability detection described by Gaikwad et al[10]. Fuzzy clustering will produce several subclasses for training for decreasing the amount of subset size and difficulty. Every subset was trained by the different type of ANN techniques and get substantial results. Denning [11] was developed an Intrusion Detection System using the concept of Time series, Markov chains, and statistics. He measured the anomaly by the deviation of the normal behavior.

Devikrishnaet al [12] used Multi-Layer Perceptron (MLP) model and it classified the attacks into six types. But it was a failure model since it was not produce the relevant results. Jaiganesh et al[13] proposed a back propagation model for intrusion detection system. It achieved a high detection rate and low false alarm rate. Cannedy [14] identified the misuse intrusions by the multi-category classifier of ANN. Ten thousand events were used for this research. Bivens et al.[15] proposed a new IDS that had a preprocessing stage. It used the techniques such as clustering the normal traffic, normalization, an ANN training stage, and an ANN decision stage. The detection rate for normal behavior was denoted as 100%. Zhengning et al. [16] employed the Signature Apriori algorithm and suggested a novel algorithm to detecting the new patterns of attacks from the previously known attacks. Tajbakhsh et al. [17] used Fuzzy Association Rule mining to identify the anomaly patterns. The clustering approach was used todefine the fuzzy membership functions of the attributes. The anomaly behavior detection rate was 100% and the FP was 13% as stated. Livadas et al. [18] worked on the filtered Internet Relay Chat (IRC) traffic and find the botnet traffic. The data was collected from Dartmouth University's wireless campus network. The filter layer was used to extract the IRC data from network. Jemili et al. [19] used Bayesian network[5]to build an anomaly based detection system. It had used KDD cup 99 dataset and classified the five classes. Kruegal et al. [20] employed on the Bayesian network to calculate the probability between usual and anomaly behavior. The DARPA 1999 dataset was used to classify events.

Benferhat et al. [21] used Simple Logfile Clustering Tool(SLCT) to generate clusters for normal and anomaly network. The DARPA 2000 dataset was used for the experiment. Blowers and Williams [22] grouped normal and anomalous network packets using clustering method. The KDD data is used and the detection performance was 98% for attack. It has achieved a good result on the anomaly based detection. Zhang et al [23] provided a solution for a signature based attack predictor [1], a pattern database and a outlier detector. The database used to hold the anomaly patterns identified by user or the system. The random forest algorithm was used and the KDD cup 99 dataset was utilized. Li et al[24] used Genetic Algorithm[5] for evolving rules for misuse detection for DARPA intrusion detection system. The Chromosome contains the Source and target IP address, source and target port number, duration of connection, no of bytes, the protocol used and the connection state. Abraham et al. [25] proposed a technique based on Genetic Programming to classify the attacks.The three techniques are used i) Linear Genetic Programming (LGP), ii) Multi- Expression Programming (MEP), iii) Gene Expression Program.

V. DATASET USED

DARPA Dataset The DARPA Intrusion Detection Evaluation Group has collected the dataset for the Computer network intrusion detection. It was the first typical dataset for the identification of intrusion detection systems. It has collected using the fund provided by Defense Advanced Research Projects Agency (DARPA ITO) and Air Force Research Laboratory (AFRL) [34], [35]. The first standard, repeatable, statistical evaluations of intrusion detections systems are distributed in 1998 &1999 by AFRL. These data sets are provided to detect the attacks and false alarm rate by the researchers. The dataset was designed to emphasis on technology issues, concern about security and privacy and by its ease of use the dataset were usually used by major intrusion detection. KDD CUP 1999 Dataset The KDD CUP dataset[37] is subset of DARPA[34] dataset prepared by Stolfo and Lee[36], in 1998 and 1999, Lincoln Laboratory at Massachusetts Institute of Technology(MIT), for network intrusion detection. The project sponsored by DARPA and ARFL and this dataset can be used for evaluation of and classification of attacks without any further preprocessing. The dataset was used for The Third International Knowledge Discovery and Data Mining tools Competition to build a network intrusion detection system. Each record in KDD CUP 1999[37] dataset is labeled as either normal or attack. There are totally 41 types are attacks are available and they are categorized into four major groups.

1. Denial of Service(DoS): Unable to handle legitimate requests to a network resource. Eg. Smurf, Neptune
2. Unauthorized access to root privileges(U2R): Login to the user account and gain the root access of the system by exploits the system vulnerabilities. Eg. Load module.
3. Probing: Gains information about the victims machine, Eg. Port Scanning.
4. Unauthorized access from remote system (R2L): The intruder access the remote machine and gains the local access of the victims machine. Eg. Password guessing

NSL – KDD 1999 Dataset

The KDD CUP 1999 intrusion detection dataset is used by many researchers to build an effective network intrusion detection system during past years. But the recent study illustrate there are some limitations are present in the KDD CUP 1999 dataset. It shows that the dataset has 78% training and 75% testing records having redundant records, it inhibits the IDS from detecting rare attacks such as U2R and R2L. The new dataset NSL-KDD dataset [38] is the advanced version of KDD CUP 1999 dataset. Now it is commonly used by the researchers to apply their experiments for analyze the intrusions. The Duplicate records are eliminated to produce an un-biased result. Anming (GEP)[1]. The DARPA 1998 dataset was used and 24 attacks can be classified into four types. Adequate numbers of records are available in the train and test datasets to execute the experiments completely. In each record there are 41 attributes are available and a label is present to categorize the data either as normal or an attack type. The attack classes grouped into four types as its predecessor

VI. EVALUATION METRICS

Evaluation metrics are used calculating and observing the performance of the IDS and for comparing the results obtained from the dataset. [3]The performance of the intrusion detection system (IDS) is evaluated by calculating four metric values, Accuracy, Precision, Recall and F-score, out of which accuracy plays a major role and the performance evaluation of the IDS is mainly dependent on accuracy metric.

1. Accuracy

This metric is calculated by finding the total number of instances that are correctly predicted as positive cases to the total number of data that is present, the instances are classified into positive or negative cases by calculating the data that are divided into True Positive(TP), True Negative(TN), False Positive(FP), False Negative(FN).True Positives(TP) are the data which are correctly classified as true instances, True Negatives(TN) are the data which are correctly classified as false instances, False Positives (FP) refers to the data that are negative instances but are predicted as positive and False Negative(FN) refers to the data that are positive instances which are predicted as negative. The accuracy rate at the maximum times can be taken as high though there are less number of negative instances which does not play a major role in decreasing the accuracy rate, it is calculated as:

Accuracy =TP+TN/TP+TN+FP+FN

2. Precision

Precision refers to the total data which are correctly predicted to be positive over the total number of data that are predicted to be positive, by observing the false positive and true positive instances, precision can be calculated as:

Precision = TP / TP+FP

3. Recall

Recall also known as a True Positive Rate (TPR), sensitivity (SN) or detection rate indicates the total number of instances that are correctly predicted as positive over the total number of actually positive instances present. While detecting the overall positive data in the dataset the recall serves as the main evaluation metric or the best performance indicator of positive data, it is calculated as follows:

Recall = TP / FN+TP

Precision and Recall are equally important for calculating the performance of the IDS, each individual is not sufficient for the evaluation of the performance of IDS.

4. F-score

F-score is calculated by considering both the metrics of precision and recall equally, the f1 and f2 scores are calculated, in case of f1 both the metrics are treated equally and the value is obtained by substituting 1 in the place of f-beta, in the case of f2 score the recall is considered two times more important than precision.

V. EVALUATION

The procedure of the experiment and the evaluation results obtained are discussed in this section.

1 Data Preparation

KDD dataset is well known for benchmarking intrusion detection techniques. The dataset is a massive collection of 9123 KB of data collected over months. [1]The KDD dataset, the authors collected consists of approximately 1,27,426 records, each of consists of 41 features and is labelled either normal or an attack. With exactly one specific attack type and the attacks simulated falls in one of the following four categories, DOS (Denial of service), U2R (used to root attack), R2L (Remote to local attack), and probing attack. Therefore, we set the duration of the data collected a month, so that dataset contains different attack types and has enough data per attack.

2 Selection of evaluation metrics and Machine Learning Algorithm

For Intrusion Detection Algorithm it is important to have knowledge on Recall more important than that of precision, so we require F-score. The Algorithms were implemented in Python.

3 Calculation of Training time

The dataset is divided into subparts and it is subjected to training, with the increase in the size of the dataset, the time taken to train the model will increase sequentially, which is known as training time, this training time is observed.

4 Increase in percentage of evaluation metrics

With the increase in the size of the dataset, in particular sequence, the values of evaluation metrics are increased accordingly, and these percentage increase in Accuracy, Precision, Recall, F-score is observed for all data samples is observed

VI. RESULTS

After training the dataset with the algorithm the following results are obtained

CONCLUSION AND FUTURE WORK

The authors have analyzed the class specific detection with the KDD dataset, using the supervised machine learning algorithm Random Forest for IDS and the test data and the training data is constructed for evaluating the performance to detect different types of attacks. The training time of the model is observed with the respective increase in the size of the dataset. The increase in the values of evaluation metrics (Accuracy, Precision, Recall, F-score) by increasing the size of the dataset in steps is observed. From the experiment conducted the authors obtained the results with an accuracy of 96%. The criteria included accuracy, complexity, time for training a model, time for classifying a unknown data and understating final solution. It is difficult to identify a better approach of ML method based on only one factor like accuracy. If the ML methods compared based on accuracy, these methods should be trained on same accurate training data and tested on same accurate testing data. In this study several authors used same dataset for same methods but they have used subset of the same dataset (selected attributes), and they are not necessarily same.

REFERENCES

[1] G. C. Kessler, “Defenses against distributed denial of service attacks,” SANS Institute, vol. 2002, 2000.View publication stats

[2] H. A. Nguyen and D. Choi, “Application of data mining to network intrusion detection: classifier selection model,” in *Asia-Pacific Network Operations and Management Symposium*. Springer, 2008, pp. 399–408.

[3] S. Paliwal and R. Gupta, “Denial-of-service, probing & remote to user (r2l) attack detection using genetic algorithm,” *International Journal of Computer Applications*, vol. 60, no. 19, pp. 57–62, 2012.

[4] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed analysis of the kdd cup 99 data set," in *Computational Intelligence for Security and Defense Applications, 2009. CISDA 2009. IEEE Symposium on*. IEEE, 2009, pp. 1–6.

[5] P. Amudha, S. Karthik, and S. Sivakumari, "Classification techniques for intrusion detection-an overview," *International Journal of Computer Applications*, vol. 76, no. 16, 2013.

[6] M. K. Lahre, M. T. Dhar, D. Suresh, K. Kashyap, and P. Agrawal, "Analyze different approaches for ids using kdd 99 data set," *International Journal on Recent and Innovation Trends in Computing and Communication*, vol. 1, no. 8, pp. 645–651, 2013.

[7] F. Haddadi, S. Khanchi, M. Shetabi, and V. Derhami, "Intrusion detection and attack classification using feed-forward neural network," in *Computer and Network Technology (ICCNT), 2010 Second International Conference on*. IEEE, 2010, pp. 262–266.

[8] Z. Zhang, J. Li, C. Manikopoulos, J. Jorgenson, and J. Ucles, "Hide: a hierarchical network intrusion detection system using statistical preprocessing and neural network classification," in *Proc. IEEE Workshop on Information Assurance and Security*, 2001, pp. 85–90.

[9] W. Alsharafat, "Applying artificial neural network and extended classifier system for network intrusion detection." *International Arab Journal of Information Technology (IAJIT)*, vol. 10, no. 3, 2013.

[10] N. Bhargava, G. Sharma, R. Bhargava, and M. Mathuria, "Decision tree analysis on j48 algorithm for data mining," *Proceedings of International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 3, no. 6, 2013.

[11] C. Fleizach and S. Fukushima, "A naive bayes classifier on 1998 kdd cup," 1998.

[12] M. Alkasassbeh, G. Al-Naymat, A. B. Hassanat, and M. Almseidin, "Detecting distributed denial of service attacks using data mining techniques," *International Journal of Advanced Computer Science & Applications*, vol. 1, no. 7, pp. 436–445.

[13] S. D. Bay, "The uci kdd archive [http://kdd. ics. uci. edu]. irvine, ca: University of california," *Department of Information and Computer Science*, vol. 404, p. 405, 1999.

[14] M. Al-Kasassbeh, "Network intrusion detection with wiener filter-based agent," *World Appl. Sci. J*, vol. 13, no. 11, pp. 2372–2384, 2011.

[15] S. K. Pal and S. Mitra, "Multilayer perceptron, fuzzy sets, and classification," *IEEE Transactions on neural networks*, vol. 3, no. 5, pp. 683–697, 1992.

[16] A. Cutler and G. Zhao, "Pert-perfect random tree ensembles," *Computing Science and Statistics*, vol. 33, pp. 490–497, 2001.

[17] L. Breiman, "Random forests," *Machine learning*, vol. 45, no. 1, pp. 5–32, 2001.

[18] J. R. Quinlan, *C4. 5: programs for machine learning*. Elsevier, 2014.

[19] M. S. Bhullar and A. Kaur, "Use of data mining in education sector," in *Proceedings of the World Congress on Engineering and Computer Science*, vol. 1, 2012, pp. 24–26.

[20] N. Friedman, D. Geiger, and M. Goldszmidt, "Bayesian network classifiers," *Machine learning*, vol. 29, no. 2-3, pp. 131–163, 1997.

[21] R. Kohavi and D. Sommerfield, "Targeting business users with decision table classifiers." in *KDD*, 1998, pp. 249–253.

[22] P. Aditi and G. Hitesh, "A new approach of intrusion detection system using clustering, classification and decision table," 2013.

[23] M. Hall, E. Frank, G. Holmes, B. Pfahringer, P. Reutemann, and I. H. Witten, "The weka data mining software: an update," *ACM SIGKDD explorations newsletter*, vol. 11, no. 1, pp. 10–18, 2009