International Journal for Rapid Research in Engineering Technology & Applied Science
Vol 4 Issue 5 May 2018
ISSN (Online): 2455-4723

A Review On Network intrusion detection System Using Different Technique

Pragya Chhabra , Mrs. NishaBhati
Computer Science Department, Rajiv Gandhi ProudyogikiVishwavidyalaya,Bhopal,Madhya Pradesh 462033,India
Email:chhabrapragya@gmail.com

Abstract: The computer network and internet networks are exposed to an increasing number of security threats. Intrusion Detection System plays a very important role in network security. Its main role in the network is to help computer system to create and deal with network attacks. For new types of attacks are emerging constantly, developing flexibility and adaptability safety-oriented approaches is a serious problem. In past few years, intrusion detection using data mining has captured the attention of researchers. Every researcher proposes a different algorithm for distinct categories. The increase speed of data flow information and also development in communication network along with many factors there is possibility of number of attacks on computer system. This paper provides us overview of intrusion detection system and various techniques used to implement intrusion detection system.

KEYWORDS: Intrusion detection system (IDS), Support Vector Machine, Artificial Neural, NSL-KDD, Security, Network analysis, etc.

IIntroduction

The cost of data information processing and downs availability of the Internet system, the organizations are still vulnerable to potential cyber threats, are network attacks. The computer intrusion is actions that violate the security of the system. Such situation must be detected and corrected in order to guarantee the integrity, confidentiality and/or the availability of computing resources.

Intrusion Detection System (IDS) is used to detect the intrusion which can be in form of an anomaly in the network and alert the user about the same. Intrusion detection system is mainly of two types firstly there is Signature based systems and second one is the Anomaly detection. The Signature based Intrusion Detection System (IDS) monitors packets in the network and compares them to the known signatures which are pre-configured and preidentified based on attack behavior of previously known attacks. On the other hand the anomaly based Intrusion Detection System monitors the normal network traffic such as bandwidth range, types of protocols, ports and devices used to connect and sends an alert to the administrator on detection of anomalous behavior.

The signature based IDS detects attacks on the known attack signature type. Advantage of this type of system is that it can detect known attacks with low error rate, but it cannot detect the newly created attacks that do not have similar behavior to known attacks. In contrast Anomaly based IDS can be useful in identifying the new attack pattern, but in this case the error rate is higher. Thus in order to solve the above two limitations we are building a hybrid intrusion detection method that combines misuse detection method and anomaly detection method has been proposed. In this review paper we are going to review the existing IDS methods and techniques and network attacks only.

IIIntrusion Detection System

An intrusion detection system (IDS) is a device or software that monitors network or system activities for malicious activities or policy violations and produces reports to a Management Station. An Intrusion Detection System (IDS) is an additional protection measure that helps ward off computer intrusions. IDS systems can be software and hardware devices used to detect an attack. IDS products are used to monitor connection in determining whether attacks are been launched. Some IDS systems just monitor and alert of an attack, whereas others try to block the attack.

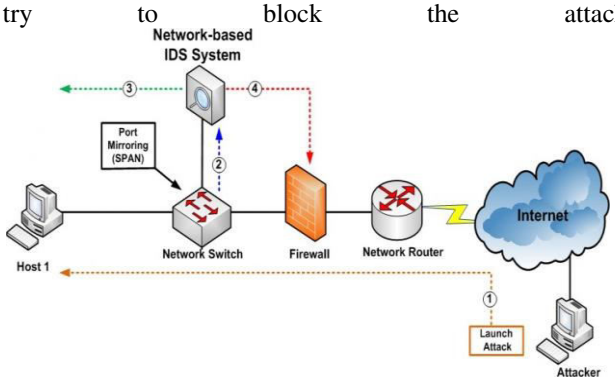

Fig. 1. Intrusion detection system

IIIRELATED WORK

The many researchers have been done in intrusion detection system with different algorithm problem some of the work is described in this paper.

Basant Subba et.al, in this paper present neural network based Intrusion Detection Systems and attack. Normally based Intrusion Detection Systems (IDSs) are known to achieve high accuracy and detection rate. In this paper, we aim to address this issue by proposing a simple Artificial Neural Network (ANN) based IDS model. The proposed IDS model uses the feed forward and the back propagation algorithms along with various other optimization techniques. Experimental results on the benchmark NSL-KDD dataset shows that the performance accuracy and detection rate of the proposed ANN based IDS model. ANN based IDS model uses only a single hidden layer, its computational overhead is comparatively less than that of the complex SVM and C4.5 based IDS models **[1].**

Shi-Jinn Horng et.al, proposed an intrusion detection system, which combines a clustering algorithm, a simple feature selection algorithm, and the Support Vector Machine (SVM). In this study, in addition to a simple feature selection method, it proposed an SVM-based network intrusion detection system with BIRCH hierarchical clustering for data pre-processing. The BIRCH hierarchical clustering provides a highly qualified and reduced datasets, in place of original large dataset, for SVM training. In addition to reduction of the training time, the resultant classifiers showed better performance than the SVM classifiers using the originally redundant dataset. However, in terms of accuracy, the proposed system could obtain the best performance at 95.72%. This approach provides better performance in terms of accuracy in comparison to the other NIDS (Network based IDS). It only detects Dos and Probe attacks not U2L and R2L attacks **[2].**

Sodiya A.S et.al, done study in this paper, the present a Neural Network-based approach that combined supervised and unsupervised learning methods designed to correct some of these problems. In the training phase, Multiple Self–Organizing Map algorithm (SOM) was constructed to capture a number of different input patterns, discover significant features in these patterns and learn how to classify input. Sigmoid Activation Function (SAF) was used to transform the input into a reasonable value (0, 1). In this paper SOM was able to perform good mapping for the MLP in classification task. The experimental results show that proposed algorithm improve that detection accuracy 4%. The simulation results, achieve more than 96 % detection rate and less than 3 % false alarm rate **[3].**

Gisung Kim et.al, presents a new hybrid intrusion detection method that hierarchically combines a misuse detection and anomaly detection in a decomposed structure. First, the C4.5 decision tree was used to create the misuse detection model that is used to disintegrate the normal training data into smaller subsets. Then, the one-class support vector machine (1-classSVM) was used to create an anomaly detection model in each decomposed region. Throughout the integration, the anomaly detection model can indirectly use the known attack information to enhance its ability when building profiles of normal behavior. This is the first attempt to use the misuse detection model to enhance the ability of anomaly detection model.C4.5 decision tree does not form a cluster, which can degrade the profiling ability thus reducing the accuracy of the system **[4].**

F. Amiri et.al, proposed Feature Selection method in order to improve the performance of existing classifiers by excluding non-related features. Furthermore, an improved Partial Least Squares Support Vector Machine called PLSSVM has been introduced. A linear and non-linear measure for the feature selection within pre-processing phase has been considered in this work. PLSSVM performed well in classifying normal and probe attacks records, respectively at 95.69% and 86.46%.In this work, the effect of changing feature goodness measure and evaluation function has been investigated by linear correlation- based feature selection (LCFS), forward feature selection (FFSA) and modified mutual information feature selection algorithms (MMIFS). Experiments on KDDcup99 dataset demonstrate that feature selection algorithms can greatly improve the classification accuracy. In contrast, PLSSVM missed a big number of dynamic attacks such as DoS and U2R attacks that behave quite similar to the normal behavior, which were recorded at 78.76% and 30.7% respectively **[5].**

Dighe Mohit S. et.al, in this paper used artificial neural network (ANN) and Invention of Intrusion in Network Intrusion Detection technique. Detect attack and classify attack In a NIDS and categorized them, IDS is important for protecting computer and network from Misuse. The intrusion detection system is a one type of art of detecting unauthorized use of computer and any attempt to break network. Multilayer perception(MLP) and apriority algorithm used for IDS.MLP based improved intrusion detection system. propose system detect the attack and classify them In 10 groups with the approximately 94% accuracy with the two hidden layer of neurons in the

neural network. The cause of an intrusion detection system is to invention a potential intruder as possible as.

Juan Wang et.al, presented an intrusion detection system based on decision tree technology. In the process of constructing intrusion rules, information gain ratio is used in place of information gain. The experiment results show that the C4.5 decision tree is feasible and effective, and has a high accuracy rate. His experimental study shows that the C4.5 decision tree is an effective technique for the implementation of decision tree and it gives almost 90% of classifier accuracy. But in this approach the error rate remains the same **[6].**

Table. 1 Litereture use different algorithm

S.no	Author	Algorithm	Topic
1	**Basant Subba**	ANN, SVM, NSL-KDD dataset.	A Neural Network Based System for intrusion Detection and Attack Classification
2	**Shi-Jinn Horng**	Support Vector Machine NIDS	Novel Intrusion Detection System Based On Hierarchical Clustering and Support Vector Machines
3	**Sodiya A.S, Ojesanmi O.A**	Organizing Map algorithm Sigmoid Activation Function	Neural Network based Intrusion Detection Systems
4	**Gisung Kim and Seungmin Lee**	SVM	A Novel Hybrid Intrusion Detection Method Integrating Anomaly Detection With Misuse Detection

IVConclusions

The various papers and literature has been studied for intrusion detection system. In this paper, we have discussed the internet and commuter network, various types of attacks that hamper the security of the network security, intrusion detection system (IDS) to monitor and analyze the attacks. Research findings of different authors have been discussed and the future research scope is discussed.

References

[1] Basant Subba , Santosh Biswas, Sushanta Karmakar, "A Neural Network Based System For Intrusion Detection And Attack Classification", IEEE, 2016.
[2] Shi-Jinn Horng and Ming-Yang Su, "Novel Intrusion Detection System Based On Hierarchical Clustering and Support Vector Machines", ELSEVIER, Expert Systems with Applications, 2011
[3] Sodiya A.S, Ojesanmi O.A, Akinola O.C, "Neural Network based Intrusion Detection Systems", International Journal of Computer Applications, Volume 106 – No. 18, November 2014.
[4] Gisung Kim and Seungmin Lee, "A Novel Hybrid Intrusion Detection Method Integrating Anomaly Detection With Misuse Detection", ELSEVIER, Expert Systems with Applications vol. 41 pp. 2014.
[5] F. Amiri, M. Yousefi, C. Lucas, A. Shakery and N. Yazdani, "Mutual Information-Based Feature Selection for Intrusion Detection Systems", Journal of Network and Computer Applications, Vol. 34, 2011.
[6] Prof.Dighe Mohit S., Kharde Gayatri B., Mahadik Vrushali G., Gade Archana L., Bondre Namrata R, "Using Artificial Neural Network Classification and Invention of Intrusion in Network Intrusion Detection System", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 3, Issue 2, February 2015.
[7] Juan Wang, Qiren Yang, Dasen Ren, "An intrusion detection algorithm based on decision tree technology", In the Proc. of IEEE Asia-Pacific Conference on Information Processing, 2009.
[8] Surana S., "Intrusion Detection using Fuzzy Clustering and Artificial Neural Network, Advances in Neural Networks Fuzzy Systems and Artificial Intelligence", ISBN- 978-960-474-379-7, 2013.
[9] Osoba O., Kosko B., "Noise-enhanced clustering and competitive learning algorithms, Neural Networks", 2013.
[10] Lisehroodi M. M., Muda Z., and Yassin W., "A hybrid framework based on neural network MLP

and Kmeans Clustering for Intrusion Detection System", 4th International Conference on Computing and Informatics, 2013 .

[11] Sakthi M., Thanamani A. S., "An Enhanced K Means Clustering using Improved Hopfield Artificial Neural Network and Genetic Algorithm", International Journal of Recent Technology and Engineering (IJRTE) Volume-2, Issue-3, 2013.

[12] Aneetha A.S., Bose S., "The Combined Approach for Anomaly Detection using Neural network and Clustering Techniques", Computer Science & Engineering: An International Journal (CSEIJ), 2012.