An Approach To Track Intrusion Detection In The System By Using Data Mining

[1]Ms. Ashwini D. Motghare, [2]Ms. Archana A. Nikose

[1]Student, [2]Asst. Professor

[1]Depart. of computer science and engineering,

[1]Priyadarshini Bhagwati College of Engineering, Maharashtra, India,

Abstract : **– In modern days, security of computer network has become important in most of everyone's lives. Intrusion detection is the way of identifying malicious, harmful and abuse of computer systems by both system insiders and external attackers. The machine learning techniques and research on neural network to improve the network security by studying the behavior of the network and also that of threats is done in the rapid force. There are several techniques for intrusion detection which exist at present to provide more security to the network, but most of these techniques are static. Many researchers used machine learning techniques for intrusion detection, but some shows less detection, some techniques takes more amount of training time. The proposed approach is to build a predictive model for intrusion detection. The proposed model will use Extreme Learning Machine (ELM) and Back propagation neural networks (BPN). The algorithm will detect Hardware and software activity. It will be evaluated by a benchmark intrusion dataset to verify its feasibility, effectiveness and to analyze the results by checking performance, execution efficiency, training time required.**

IndexTerms - **External attackers, Hardware, ELM, Insider attackers, Intrusion detection, Software**

I. Introduction

We are living in the era of networks and internet. Where, Internet has become an important part of our life. Almost everything, we perform through internet such as Social networking, Business, Entertainment, Education, etc. Intrusion detection and tracking is different from Intrusion retrieval. The goal of Intrusion retrieval is to find the Intrusions in a collection that best match some query. The query might be considered a very short Intrusion consisting of a few keywords, and the goal then is to find the Intrusions in the collection that are most similar to the query Intrusion.

In Statistics terminology, topic detection is a clustering problem: we want to partition C into groups such that Intrusions in each group are similar to each other, and dissimilar from Intrusions in other groups.

In its simplest form, topic tracking is a classification problem. We have a collection C of Intrusions, each labeled with a topic, and we want to assign a label to a new Intrusion. The unusual aspect of the problem is that our answer could be "none", in which case the Intrusion is taken to represent a new topic. Clustering and classification methods play a central role in the reduction of both the number of operations needed for Intrusion classification, and the retrieval time. Also, they can be designed to make accurate decisions on whether or not a Intrusion represents a new topic.

The paper consists of two learning methodology towards developing an intrusion detection system by considering Back propagation neural networks (BPN), and Extreme Learning machine (ELM). The proposed method will be tested by a benchmark intrusion dataset to verify its feasibility and Effectiveness. Some problems come from the survey such as false detection, more training time, classification of attacks, detection precision of low frequent attacks etc. To solve the problem of more amount of training time, it is necessary to work high speed learning algorithm for IDS and to test its results with old learning technique.

The use of Data mining is automated data analysis techniques to uncover previously undetected relationships among data items. It often involves the analysis of data stored in a data warehouse.

II. LITERATURE SURVEY

Mohammad Taghi Jafari , Hamdollah Ghamgin[1] in this paper, The aim of systems is to monitor and discover attempts for system safety penetration and describing these attempts to the authenticated user. Developing IDS was mainly applicable on the expert system development field and discuss the feasible implementation of neural networks in IDS development.

Hu Zheng Bing, Shirochin V. P[2] in this paper, An algorithm is proposed for use the known signature for finding the signature of the related intrusion. They discuss a structure that if they have known the signature of one existing intrusion, then they propose a more easily than the Signature Apriori algorithm to find the modified intrusion signature, the modified intrusion is derived from the known intrusion.

Dr Sreepathi .B, Santhamma, Goutami Sri Rai, Shanthala .J, Sowjanya .M.V[3] presents an intelligent learning approach using Ant Colony Optimization (ACO) based on distributed intrusion detection system and find attacks in the distributed network. Using this algorithm, it improves the efficiency of intrusion detection and minimizes false positives of intrusion detection. Prof. D.P. Gaikwad, Sonali Jagtap, Kunal Thakare, Vaishali Budhawant[4] paper proposed to build anomaly based detection system holding both the fuzzy logic and artificial neural networks. Artificial Neural Network (ANN) is one of the important and widely used techniques and useful for finding many difficult problems. But the disadvantage of ANN based IDS is lower detection precision and weaker detection stability. Loye Lynn Ray[6] in this paper, they search the different methods by using researchers to train and test their IDS models and it also found that the data can affect the results of training and testing the NN IDS models.

Hassan I. Ahmed, Nawal A. Elfeshawy, S. F. Elzoghdy, Hala S. El-sayed, Osama S. Faragallah[8] In this paper, Gradient descent with momentum (GDM)-based back-propagation (BP) and Gradient descent with momentum and adaptive gain (GDM/AG)-based BP algorithms both are used for training neural networks to run like IDS. A neural network based IDS is built using the proposed learning algorithms for searching the speed of the two proposed learning schemes.

III. Proposed Methodology

Proposed approach is to handle enormous amount of network traffic on the basis of the learning techniques. In traditional learning approaches large amount of training period is required. By using Extreme learning machine (ELM) and Back propagation neural network (BPN) we will build a predictive model. It will work as a classifier. To classify the data some training samples will be provided in the knowledgebase. The classifier will distinguish the malicious and normal data. The malicious data is also called as the attack data. The learning techniques will be evaluated by a benchmark intrusion dataset. The Evaluation parameters would be execution efficiency, training time required, detection rate etc.

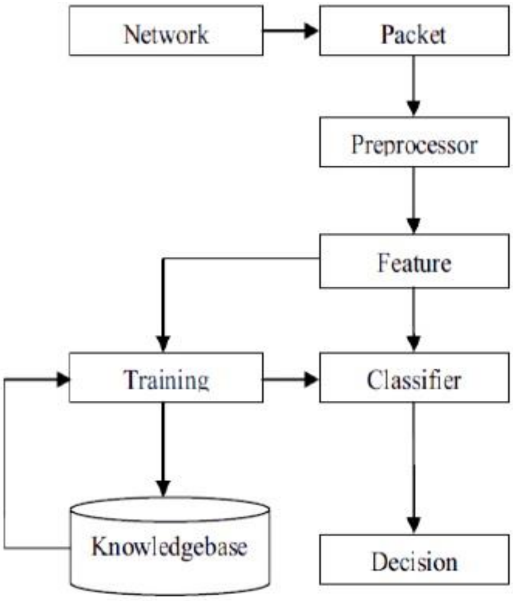

Fig: Architecture of IDS system

The detailed architecture modules have following:

•Packet Monitor
This module will examine network stream and for the serve of the data source of the NIDS it capture packets.

•Pre-processor
In this, it will be composed network traffic and send it for use as input to the system.

•Feature Extraction
After accepting the feature vector from the network packets, it will submit this to the classifier module. This process will contain both feature construction and feature selection. The quality of the feature construction and feature selection algorithms is most important factors that impact the effectiveness of IDS.

•Classifier
Classifier will study the network stream and will draw a result whether intrusion presents or not. We use both BPN and ELM techniques as a classifier. The most successful application of neural network is classification and pattern identification. The learning process is essentially an reduction process in which the parameters of the best set of connection coefficients for solving a problem are develop.

•Decision
When finding that intrusion is presents, this module will send an alert message to the user.

•Knowledgebase
Knowledgebase will provide the training samples to the classifier phase. When it has been trained correctly, the Artificial Neural Networks can work easily and correctly.

REFERENCES

[1] Mohammad Taghi Jafari, Hamdollah Ghamgin, “Artificial immune intrusion detection system”, Intl. Res. J. Appl. Basic. Sci. Vol., 4 (8), 2080-2087, 2013

[2] Hu Zheng Bing, Shirochin V. P. “Data Mining Approaches for Signatures Search In Network Intrusion Detection”, IEEE Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications 5-7 September 2005, Sofia, Bulgaria

[3] Dr Sreepathi .B1, Santhamma2, Goutami Sri Rai3, Shanthala .J 4, Sowjanya .M.V5, “Protection and Detection System by using Data Mining and Rhetorical Techniques ”,World Journal of Science and Technology April 2018, 2(3):127-133

[4] Prof. D.P. Gaikwad, Sonali Jagtap, Kunal Thakare, Vaishali Budhawant,”Anomaly Based Intrusion Detection System Using Artificial Neural Network and fuzzy clustering.”, International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181, Vol. 1 Issue 9, November- 2012

[5] K.Rajasekhar, 2B.Sekhar Babu , 3P.Lakshmi Prasanna, 4D.R.Lavanya, 5T.Vamsi Krishna, “Data Mining and Forensic Techniques for Internal Intrusion Detection and Protection System”, IJCST Vol. 2, Issue 4, Oct .- Dec. 2017

[6] Loye Lynn Ray “Training And Testing AnomalyBased Neural Network IDS” INTERNATIONAL JOURNAL OF INFORMATION SECURITY SCIENCE 2013

[7] Bini V. C, Ms. Nimmy K, Prof. P. Jayakumar, “Internal Intrusion Detection Using Data Mining and Behaviometric Technique”, International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056, Volume: 03 Issue: 07 , July -2016

[8] Hassan I. Ahmed, Nawal A. Elfeshawy, S. F. Elzoghdy, Hala S. El-sayed, Osama S. Faragallah, “A Neural Network-Based Learning Algorithm for Intrusion Detection Systems”, published in Wireless Pers Commun DOI 10.1007/s11277-017-4663-8

[9] Lawton,G, Computer,“Biometrics A new era in security,” vol. 31. Issue: 8, Aug. 1998, pp.15-18.