Volume 4, Issue 9, September 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Novel Approach for Classification and Detection of Attacks in Network Intrusion Detection System Using ANN

Ms. Deepali Ravindra Jawale
PG Student, Computer Engineering Department
Department JSPM's BSIOTR(W),
Pune, India

Prof V. K. Bhusari
Associate Professor, Computer Engineering
JSPM's BSIOTR(W),
Pune, India

Abstract-- Now a day there is drastic dependency on the internet in every sector like private, government etc. For protecting these networks from attacks is very crucial task. A single intrusion in a computer network can lead to loss of data or unauthorized use or modification of personal data. There are many methods and algorithm to detect attacks, most of the methods detects attacks and categorized it in two groups, Normal or Intrusion. A new approach to intrusion detection (ID) is based on Artificial Neural Network (ANN). This uses Multi layer Back Propagation algorithm (MLBP) to detect denial of service, probe attacks, user to root and root to local attack based on the features which are stored in the Knowledge Discovery in Databases (KDD) 99 database. The proposed system not only detect attacks but also classify them in six groups with the accuracy of identifying and classifying network activity based on limited, incomplete, and nonlinear data sources. In comparison with existing systems, the proposed system gives detection rate up to 90.43%. Although these results are theoretical but for improving the efficiency, ANN based IDS gives high performance rate than other existing systems.

Index Terms-Artificial Neural Networks, Multi layer Back Propagation algorithm Intrusion Detection System, Multi-layer Perceptron

I. INTRODUCTION

In the past years there is rapid progress in the Internet based technology, new application areas for computer network have introduced day by day. It offers intruder to launch new intrusion in network system. To provide the better security for personal data and maintain confidentiality on the network there is need for intrusion detection system. There are various techniques like Classification, Clustering, Association-Rule mining, Expert system, the techniques can used in combination to provide high performance for detecting intrusion access. The ANN has number of algorithms to provide better performance.

Among them back propagation technique is widely used to provide high detection rate. The Multi Layer back propagation (MLBP) is a part of ANN. it is composed of many neurons that are linked together according to specific network architecture. The various samples can be trained for matching the patterns of known intrusions. In this technique there is 2 or more hidden neuron [nodes]. System is a collection of processing elements that are highly interconnected and transform a set of inputs to a set of desired outputs. Neural networks are used to identify the typical characteristics of system users. It also identifies statistically appropriate variations from the user's behavior. The proposed system consists of various modules in which first the packets on the networks are observed. If any suspicious packet is observed then the data is processed that means labeled and forwarded to feature extractor. This module extracts feature vector from the network packets and submits the feature vector to the classifier module after submission it test the sample with the existing sample. If the sample is matched it generates the alarm. There are false positive and false negative rate is calculate to state the decision that whether it is a normal connection or intruder.

It is also called as NNID (Neural Network Intrusion Detector).It trained in the identification task and tested experimentally on a system of users. The system was 96% accurate in detecting unusual activity, with 7% false alarm rate. The identification of the packets and users communication is the useful way to find solution of the problem.

II. LITERATURE SURVEY

1. In order to provide better performance using ANN there are lots of research are performed some techniques uses fuzzy clustering, class association, SVM and some techniques uses expert system with ANN[1].

2. James Cannady stats that the misuse detection with artificial neural network the paper describes the misuse kind of detection of intrusion but the drawback of the system is it require accurate training of data which is very crucial task. And the rules are not hard coded so implementer has to design the rule and then implement it. But it fails to detect other attacks [2]. Some systems has MLP for detecting Probe attacks it was able to detect probe kind of attacks but the rest of the attacks are not to be detect by the system[7].

3. The Christos Siaterlis Basil Maglaris stated that the MLP can be used to detect DDOS kind of attack it can detect all kind of attack but still the various accuracy is required to detect those. But the other attacks call root to local, user to root, and probe kind of attacks was developed in that system [8].

4. The scholar Debra Anderson, Thane Frivold, Alfonso Valdes states that This version is designed to operate in real time to detect intrusions as they occur NIDES are a comprehensive system that uses new statistical algorithms for anomaly detection, as well as an expert system that encodes known intrusion scenarios. NIDES are itself a sensitive application and have security requirements in addition to those of the systems whose use is being monitored. If an intruder can read the NIDES rule base, then the penetrated site and other sites using a substantially similar rule base could be jeopardized, especially if such knowledge is shared among the intruder community. Although this system is not more reliable than the proposed system [10].

The proposed system that is classification of these attacks using multi layer back propagation is able to detect and classify all kind of attacks the base paper is having capability to detect seven kinds of attacks but in the proposed system is going to detect the ten different attacks and that are from different categorize.

III. PRAPOSED SYSTEM ARCHICTURE

The positive sides of the ANN are they can provide the ability of faster information processing. It is capable of classification and detection of kind of attack also it has and the ability of self learning and self organization. The NIDS can analyze the network captured packets and detect whether it would be an intrusion or not [1].

A back propagation algorithm (BPA) uses the Delta Rule, calculating error at output units, while error at neurons in the layer directly preceding the output layer is a function of the errors on all units that use its output. The error in the output node(s) are propagated backward through the network after each training case. The better idea to use the back propagation is to combine a non-linear multi-layer perceptron-like system capable of making decisions with the objective error function of the Delta Rule [4]. Back Propagation Neural (BPN) Network architecture is is one of the most popular network architectures for supervised learning. Analysis is carried out on Internet Security and Acceleration (ISA) server 2000 log for finding out the web documents that should not be accessed by the unauthorized. From the architecture, the diagram of system includes several modules, which has shown in Figure.

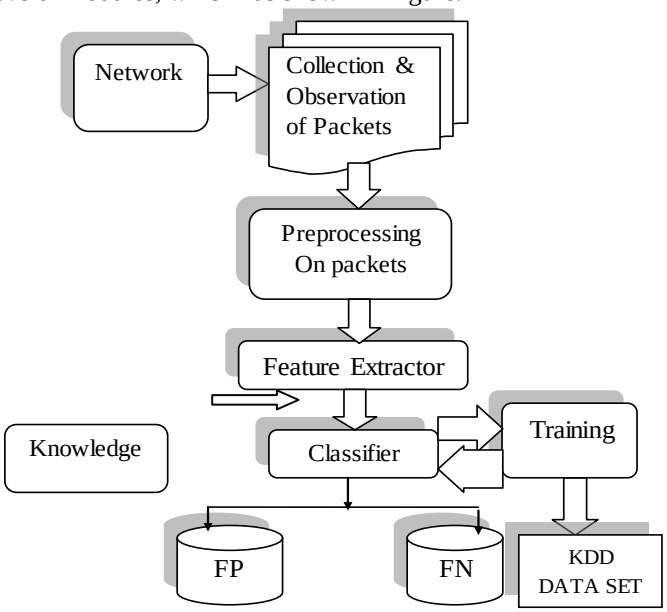


Figure: Block Diagram of System overview

There are several modules that introduce the network intrusion detection system based on the artificial neural networks architecture. They are as follows

***A. Packet monitor*:** It monitors network stream real time and collect packets to serve for the data source of the NIDS.

***B. Preprpcessor*:** In this phase, network traffic collected and processed for use as input to the system.

***C. Feature extractor**:* It extracts feature vector from the network packets and submits the feature vector to the classifier module. Feature vector extracted feature which serves for the description of the packet. Whether the feature vector can describe the network stream correctly and efficiently or not. It affect on the efficiency and correctness of the NIDS.

D. Classifier: It analyze the network stream and to state a conclusion whether intrusion happens or not. Classifier module is the most important in neural network model; The Classifier uses a three layers neural network. The dimension of the input layer is the number of the features selected, and the dimension of the output layer is the number of sorts that can be classified by the Classifier.

The transfer function: *Logsig(x)* = 1/(1+ exp (-x)) can be used in the Classifier model.

The learning function: *transfer* function can be used in the Classifier which works based on Back-propagation algorithm.

Initialization of the weight: Any values form 0 to 1 can be assigned as weights and that are applied randomly to the nodes [1].

***E. Decision**:* It detect whether the intrusion happens, or not this module will send a warning message to the user.

***F. False positive and false negative**:* False positive is nothing but it is an event when the system generates alarm for such situation which is a normal event. And the false negative is an event when alarm is not generating even the intrusion is detected.

***G. Knowledgebase**:* This module is used for the training samples of the classifier phase. That is KDD Cup'99 Intrusion Detection Dataset (KDD). The dataset is the collection of network related information that consists of a number of basic features: duration of the connection, protocol type, such as TCP, UDP or ICMP, service type, such as FTP, HTTP, Telnet, status flag, total bytes sent to destination host, total bytes sent to source host, whether source and destination addresses are the same or not, number of wrong fragments, number of urgent packets. Each record consists of 41 attributes and one target. The target value indicates the attack name. There are 41 features for each connection. Specifically, "a connection is a sequence of TCP packets starting and ending at some well-defined times, between which data flows from a source IP address to a target IP address under some well-defined protocol" [4].

H. Dataset: The following table shows the trained sample of attacks in KDD cup data set of a particular kind of attack.

IV. IMPLEMENTATION

This system detects normal or attack connection and also classifies them into six groups and provides detection rate of each attack with its false positive rate and false negative rate. Multilayer Perceptron classifier used BPA to train neural network. It can monitor neural network during training. Basically network is formed by nodes which are in input, hidden and output layers. Here all the nodes including the neural using MLP are sigmoid. The network trained by back propagation used nodes which are the processing unit they all work together to produce the output. MLBP learned by set of weights for predicting the class label here the class label is attacks of each connection. Neural network formed by MLP made up of input, one or more hidden and an output layer. Here input layer denotes attributes that to be measured for each values that to be trained. When we passed input through the input layer firstly node are weighted and produced to hidden layer simultaneously. Now, the output of hidden layer can be feed directly as input to other hidden layer or taken as output [3]. Mainly back propagation calculates derivative of all the values of target with respect large set of database which is provided as input. These values are actually used for pattern classification. For better accuracy we have to reduce the training time of neural network and also consider size of the input to be small. the SOM and NEIVE bias is used for classification and generating maps to trace out the IP address within the network.

A. Module 1: ALGORITHM FOR MLP*:* The algorithm of the system using MLP is as follows

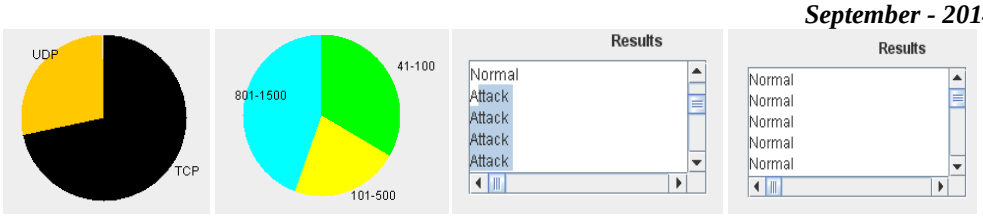
1. Initialize weights.
2. If stopping condition are false, do steps 3 to 10.
3. For each training pair do step 4 to 12
4. Apply input Xi and transmit these signals to the hidden node in forward direction.
5. $[V]^o$ ={random weights}, $[W]^o$ = {random, weights, $[\Delta V]^o = [\Delta W]^o = [O]$
6. Each input and Hidden unit sums its weighted input signals an send the signals to the output layer/units
   $\{I\}_H = \{V\}^T\{O\}I$ where I and V sets are m*1 and and o is l*1
7. Each output unit sums its weighted input signals and applies its activation function to calculate the output signals.
   $\{O\}_H = \{- - -1/(1+e^{(-I_{Hi})}) - - -\}$
8. Each output unit receives a target pattern corresponding to an input pattern and error information calculated. error rate $= ((\sum E_P)/nset)$
9. Each hidden unit sums its delta inputs. The error information is calculated. $\{d\} = \{(T_K - O_{ok})O_{ok}(1-O_{ok})\}$
10. For back propagation of delta $[Y] = \{O\}_H$ <d>
11. For training network for a fix pattern $[\Delta W]t+1 = \alpha[\Delta w]t + \eta[Y]$
12. Final delta term is calculated as $\{d^*\} = \{ei(O_{Hi})(1-O_{Hi})\}$ where $\{e\} = [w]\{d\}$

B. Module 2 :

1. Naive Bias :- It is used as classifier, it is an learning algorithm for neural network**.**
2. Self organizing Map :- The SOM is used for producing a low dimensional , and representation of map. it is a unsupervised learning kind of algorithm. which help us to trace out location of IP Address in network.
3. SVM :- it is also a unsupervised kind of algorithm of MLP it gives more detection rate to system. The SVM provides more efficiency than others but the drawback is it uses only binary values for calculation.

IV. RESULTS

The backpropagation algorithm provides 90.78% detection rate which is comparatively higher also it provides the classification according to the attack's category. The various methods provide higher detection rate but all they are facing problem while classification and accuracy so those all algorithms are attack specific i.e those algorithm provide detection for a specific category. the back propagation is an algorithm which provide detection for all kinds of attack also classifying them to the respective category.



V. CONCLUSION AND FUTURE SCOPE

In this project, neural networks are of use in an intrusion detection system. The user model developed here is the complement of a statistical model, because neural networks cannot adequately handle all the available data. The tight coupling between the neural net and the expert system is necessary to analyze the output of the net and propose explanations and a clear diagnosis to the security administrator. The deviations to the normal behavior of the user seem to be diagnosed fairly quickly by the neural network. This capability is interesting since the goal of an intrusion detection system is to detect a potential intruder as soon as possible.

VI. FUTURE ENHANCEMENT

It should be mentioned that the long training time of the neural network was mostly due to the huge number of training vectors of computation facilities. However, when the neural network parameters were determined by training, classification of a single record was done in a negligible time. Therefore, the neural network based IDS can operate as an online classifier for the attack types that it has been trained for. Although the classification results were slightly better in the three layer network, application of a less complicated neural network was more computationally and memory wise efficient.

REFERENCES

[1] Norouzian M.R., Merati. S., "Classifying Attacks in a Network Intrusion Detection System Based on Artificial Neural Networks" Proceedings of the Advanced Communication Technology (ICACT), 2011 13th International Conference on Publication Year: 2011 , Page(s): 868 – 873.

[2] James Cannady ," Artificial Neural Networks for Misuse Detection" School of Computer and Information Sciences,Nova Southeastern University Fort Lauderdale, FL 33314.

[3] Vu N.P. Dao 1 Rao Vemuri,"A Performance Comparison of Different Back Propagation Neural Networks Methods in Computer Network Intrusion Detection" University of California, Davis, One Shields Ave., Davis.

[4] Devi Krishna K S, Ramakrishna B B," " International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 3, Issue 4, Jul-Aug 2013, pp. 1959-1964

[5] Hari Om, Tapas K. Sarkar," Designing Intrusion Detection System for Web Documents Using Neural Network", *Department of Computer Science and Engineering, Indian School of Mines, Dhanbad, India.(2009).*

[6] Aida O. Ali,Ahmed saleh, Tamer Ramdan," Multilayer perceptrons networks for an Intelligent Adaptive intrusion detection system" IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.2, February 2010.

[7] Iftikhar Ahmad, Azween B Abdullah, Abdullah S Alghamdi "Application of Artificial Neural Network in Detection of Probing Attacks" IEEE Symposium on Industrial Electronics and Applications (ISIEA 2009), October 4-6, 2009, Kuala Lumpur, Malaysia,2009.

[8] Christos Siaterlis Basil Maglaris,"Detecting DDoS attacks using a multilayer Perceptron " classifier National Technical University of Athens Iroon Politechniou 9, Zographou, 157 80 Athens, Greece March 2004.

[9] Gang Wang, Jinxing Hao, Jian Ma, Lihua Huang,"A new approach to intrusion detection using Artificial Neural Networks and fuzzy clustering"School of Management, Fudan University, Shanghai, PR China Department of Information Systems, City University of Hong Kong, Tat Chee Avenue, Kowloon, Hong Kong.

[10] Debra Anderson, Thane Frivold, Alfonso Valdes,"Next-generation Intrusion Detection Expert System (NIDES) A Summary" This report was prepared for the Department of the Navy, Space and Naval Warfare Systems Command, under Contract N00039-92-C-0015, May 1995.

[11] Purva Adlakha, Priti Subramanium," Detecting and Classifying AttacksNetwork Intrusion Detection System Using Multi-layer Perceptron Based on Artificial Neural Network**"** presented in IJARCSSE, Volume 3, Issue 6, June 2013.

[12] KDD CUP 1999 DATA [Online]Available : www.11mit.edu.

