

Technique to Detect and Classify Attacks in NIDS Using ANN

Ms. Deepali Ravindra Jawale

PG Student, Computer Engineering Department
JSPM's BSIOTR(W), Pune, India

Prof V. K. Bhusari

Associate Professor, Computer Engineering Department
JSPM's BSIOTR(W), Pune, India

Abstract:

The rapid progress in network technology comes with the drawback of insecure data. The intruder are trying to read the data transmitting on network the idea of reading the data is observing packets and generate traffic for interrupting the communication. There are various researches are done to avoid detect and preventing these attacks happening on the network. The intrusion detection techniques are used to detect attacks on network the techniques used are fuzzy clustering, genetic algorithm, artificial neural network and many more. Among these the ANN is the technique having highest detection rate. The present system uses the Multilayer perceptron's back propagation algorithm and SVM. In these technique Self organizing map is used to trace location of the intruder. The algorithm is giving 90.43% efficiency as a result. The proposed system is consist of various modules like collection of packets over network, then preprocessing of data means extracting the feature to apply then it classify the connection in normal or attack type. The process we can kill or we can directly shutdown the system. or we can trace the location of that IP address using SOM.

Keyword: MLP, DDOS, NIDES, ANN, ISA, BPN

I. INTRODUCTION

The communication technology come with some advantages and disadvantages also the main role of internet is to provide communication and secure transmission. there are various techniques like firewall and intrusion detection systems are present to detect present intrusion on the network. the firewall is used but it is not observing packets very deeply to detect an intrusion we have to observe packets and then find whether that packet is normal or attack. The IP address and location of that attacker is also important. I have designed a network intrusion detection system based on the artificial neural networks using Multi Layer Perceptron (MLP). In many previous studies the implemented system is a neural network with the capability of detecting normal or attack connections, in the present study a more general problem is considered in which the attack type is also detected. This feature enables the system to suggest proper actions against possible attacks. 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.

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 ARCHITECTURE

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.

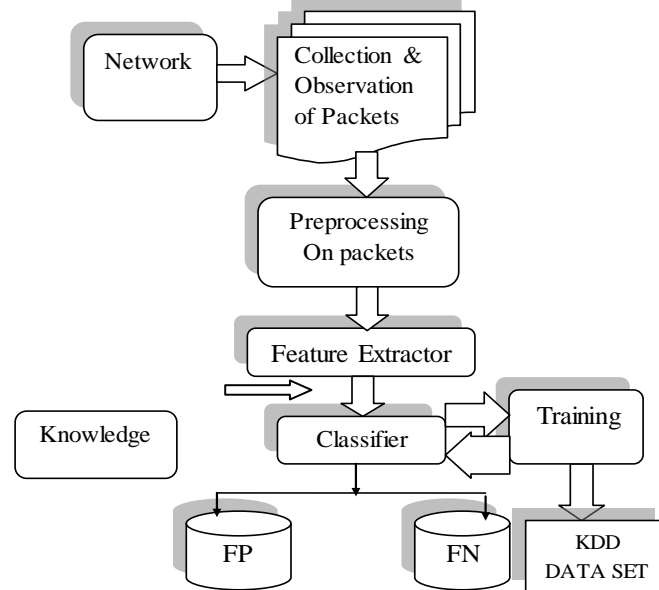


Figure: Block Diagram of System overview

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. Preprocessor: 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”.

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

IV. IMPLEMENTATION

The implementation of the system contain basic server client connection one by one we can add client to the system. After connection establishment of the connection we can transfer packets over the network then the data set is loaded and classified in various categories. The client systems then get scanned through the port scanning tool to find the network traffic and data transmission on network. We can also scan a single port and find the connection details that details we can pass to back propagation algorithm to find whether this is attack. Then the IP location is find out using SOM approach which is modified approach. the all processes running on that server we can see kill and as well as we can shutdown the system. The algorithm are back propagation and kohen self organizing map.

MODULE 1: ALGORITHM FOR MLP: The algorithm of the system using MLP is as follows

Instead of back propagation algorithm for providing more efficiency we can also use

1. Select parameter C that restrains the influence of one data pint select the type of the kernel and the associated parameters.
2. Solve the dual Qp problem or an alternative formulation.
3. Determine parameters b by means of hyper plane equation.
4. Classify a new data point x point by passing it to the decision function.

MODULE 2 : ALGORITHM FOR KOHEN SELF ORGANIZING MAP

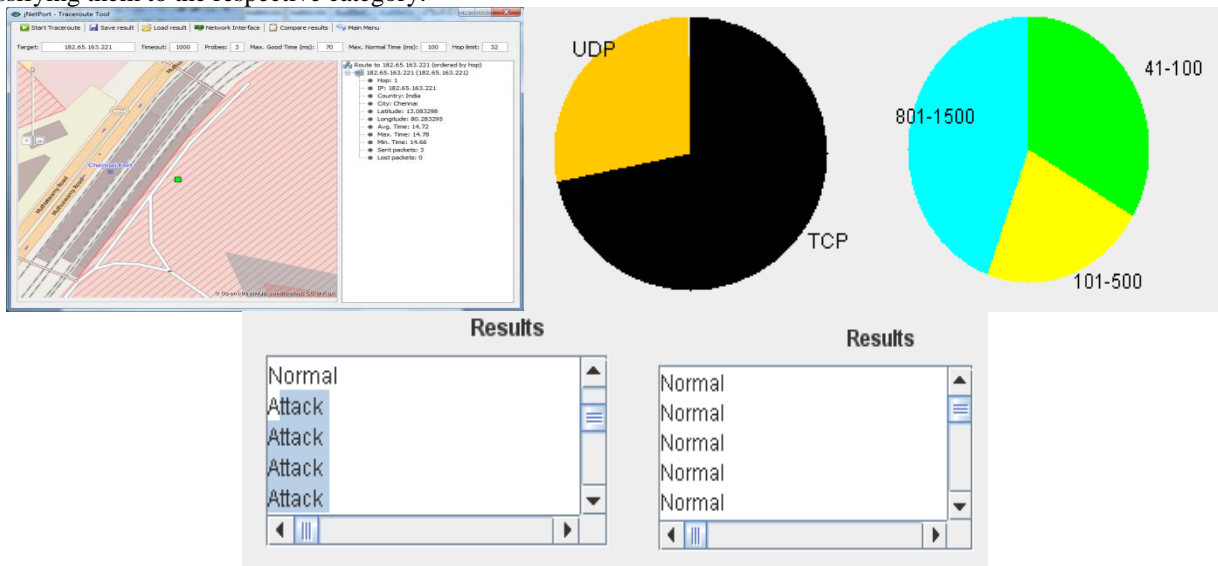
1. Set topological neighbourhood parameters. Set learning rate, initialize weight.
2. While stopping condition is false do 3 to 9.
3. For each input vector x, do 4 to 6.
4. For each j, determine squared Euclidean distance.

$$D_{ij} = \sum (W_{ij} - x_i)^2$$
 where i=1 to n, and j=1 to m.
5. Find the index J , when D(j) is minimum.
6. For all units j, with the specified neighbourhood of j and for all i, updates the weights.

$$w_{ij}(\text{new}) = w_{ij}(\text{old}) + \alpha(x_i - w_{ij}(\text{old}))$$
7. Update the learning rate.
8. Reduce the radius of topological neighbourhood at the specified time.
9. stop.

V. 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.



VI. 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] KDD CUP 1999 DATA [Online]Available : www.ll.mit.edu
- [12] AL-Rashdan, W, Naoum, R, Al_Sharafat, W & Al-Khazaaleh, M. (2010). Novel network intrusion detection system using hybrid neural network (Hopfield and Kohonen SOM with conscience function). IJCSNS International Journal of Computer Science and Network Security, 10(11). Retrieved January 26, 2012, http://paper.ijcsns.org/07_book/201011/20101103.pdf
- [13] Al-Rashdan, W. (2011). A Hybrid Artificial Neural Network Model (Hopfield- SOM with Conscience) for Effective Network Intrusion Detection System, (Doctoral dissertation), The Arab Academy for Banking and Financial Sciences, Jordan.
- [14] Bernacki, M. & Włodarczyk, P. (2004). Backpropagation. Retrieved October 31, 82 2011, from http://home.agh.edu.pl/~vlasi/AI/backp_t_en/backprop.html
- [15] Best Security Tips [Image] (2007). Retrieved March 14, 2012, from <http://www.bestsecuritytips.com/modules/soapbox/images/firewall/2/firewall1.gif>