International Journal of Emerging Engineering Research and Technology
Volume 2, Issue 6, September 2014, PP 146-149
ISSN 2349-4395 (Print) & ISSN 2349-4409 (Online)

Intrusion Detection System Using Artificial Neural Network

Minal Z[1], Pooja D[2], Snehal P[3], Poonam P[4], Priyanka P[5]

[1]M.E. - Computer, Assistant Professor, Department of CSE, AISSMS IOIT, Pune, India
[2] B.E. - Student, Department of CSE, AISSMS IOIT, Pune, India
[3]B.E. - Student, Department of CSE, AISSMS IOIT, Pune, India
[4]B.E. - Student, Department of CSE, AISSMS IOIT, Pune, India
[5]B.E. - Student, Department of CSE, AISSMS IOIT, Pune, India

Abstract: *With the advancement in the computer Technologies and Networks, intruders and Hackers gain the new facilities of accessing confidential data. Thus the Intrusion Detection system (IDS) comes in to rescue when we see that the damage that can be caused by intrusions is limitless. The suspicious or malicious activities are being monitored by IDS continuously and as soon as it detects any such kind of activity, it informs, analyses and alarms the system administrator about it. Most of the previous IDS have focused on classification of attacks as normal or intrusion. The proposed system is able to classify the type of attack. In this paper, we present an effective IDS with layered framework integrated with neural network. The system is compared with the existing systems which uses KDD dataset. The results show that the proposed system has capability to detect the majority of attacks which are under TCP, UDP and ICMP due to real-time dataset.*

Keywords: *Intrusion Detection System (IDS), Artificial Neural Network (ANN), TCP, UDP, ICMP.*

1. Introduction

Technological advances in computers and network have changed the computing world in last decade. The highly connected computing world has equipped the intruders and hackers with new power for entering and taking possession of another's confidential data. Thus for security management system of organization from various attackers by various sources, a tool implemented is referred as Intrusion Detection System (IDS). There are two main approaches to design Intrusion Detection System. The first approach is Misuse Detection [1],[2] based Intrusion Detection System which first defines the suspicious behavior of the system and looks for this behavior in the system. If the behavior of the system found similar to the previously defined suspicious behavior then it declared it as Intrusion. Another approach is anomaly detection [1] system which first defines the normal behavior of system and when any behavior other than normal is occurred then it declared it as Intrusion. This technique is based on the detection of unusual traffic. There are two types of Intrusion Detection System. The Network Intrusion Detection Systems (NIDS) [3] are placed in the network so that they can examine data flowing inward and outward of the network. While the Host based Intrusion Detection Systems (HIDS) are used for scrutinizing the inward and outward traffic for an individual host. A host based Intrusion Detection System checks for any manipulation that may occur with files, standard binaries, password, access control files etc. It also scans the system calls that are invoked by various software applications. A Host based Intrusion Detection System can particularly check the existence of back-doors and Trojans and can alarm the system/network administrator about the same.

2. Related Work

There are several researches done in the field of IDS and different approaches are developed to detect the different attacks. In the expert system [5] approach denning's[4] profile model is used. It requires the predefined rules that describe the attack and by using these predefined rules, it detects the intrusion. It is inflexible because it fails to detect an attack when an attack description is slightly different than the predefine rule. It increases level of abstraction and reduces granularity of IDS. It also requires frequent updates.

The another approach for IDS is signature verification system [6], [7] which converts attack scenario in to the sequence of events, but it requires to specify the signature of an attack which cannot be easily discovered.

This approach is similar to virus scanner which looks for known suspicious pattern in their input. It has acceptable accuracy and fewer false rates but it cannot detect novel attack and also slight variation in the known attack.

The approach is Generic System which is based on the concept that intrusion behavior involves abnormal usage of the system. This system constructs the model of normal usage of the system and verifies the usage of same system against the normal usage model which is constructed previously. If any deviation is observed then it declares intrusion is occurred.

3. Proposed System

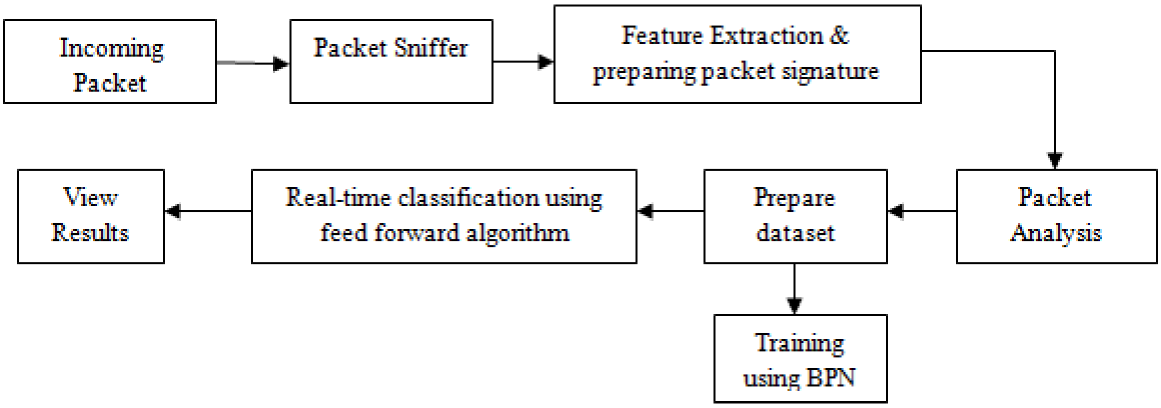
Incoming Packet
Packet Sniffer
Feature Extraction & preparing packet signature
Packet Analysis
Prepare dataset
Real-time classification using feed forward algorithm
View Results
Training using BPN

Fig1. Proposed System Architecture

In this system, we present an effective IDS which classifying different types of attacks by using Artificial Neural Network. Artificial Neural Network (ANN) [8] is an information processing system which works similar to human nervous system in which large number of processing elements (Neurons) which are highly interconnected to each other. Processing element (Neuron) is summing element followed by an activation function [8].Output of each neuron is fed as input to all the neurons in next layer. For the training process of the ANN back-propagation neural network (BPN) is used. Layered framework uses only those features which contribute to the classification process, so that the dimensionality of dataset is reduced. Thus this paper proposes IDS using these two approaches. In IDS under consideration, firstly dataset is generated by using attacker module. The attacker module is manually prepared tool which is used to make attack on the system to capture intrusion packets. Packet capturing is done by packet sniffer. Then the features are extracted from the packet header and packet analysis is done by packet analyzer. Then these features of the packets are stored in the database depending on whether the packet is intrusion or not. Further the training of ANN is done with the help of this dataset using BPN.

4. Artificial Neural Network

The idea behind the Artificial Neural Network (ANN) is the structure of human brain nervous system. The brain basically learns from the experience. The main component of nervous system is a neuron which is responsible for information processing in the brain. Similarly Artificial Neural network is a network of tightly connected neurons. It stores information, utilizes the information and then solves problems as that of man brain in the new field of computation. These neurons in the ANN are arranged in layered format and neuron form each layer is tightly connected to the neuron in the next layer and this connection has certain weight (w). It mainly consist of three layers- Input Layer, Hidden Layer and Output Layer. Initially any value for the weight for each connection is assigned. Then the inputs (x) are applied to the neurons which are present in the input layer. This input layer neurons processes the input and produces the output (considering the weight and input) which then transmitted to the connected neurons. In this way each neuron computes the output and transmits it to the next neurons. At the output layer, the output of the network is compared with the required output and error is calculated. For minimizing this error we transmit this output back in the network and repeat the whole procedure again with assigning new value for the weights for every connection till we get the required output. In the following fig.2 x_i are the inputs to ANN and W is the weight of an artificial neuron. These weights are assigned with each arrow, which represent information flow.

These weights are multiplied by the values which go through each arrow, to give more or less strength to the signal which they transmit. Depending on the weights, the computation of the neuron will be different. The neurons of this network just sum their inputs. It is not so complicated to adjust the weight of neurons for small network, but if we have thousands of neuron in a network so to adjust them there are some methods. The Backpropogation Algorithm is one of them.

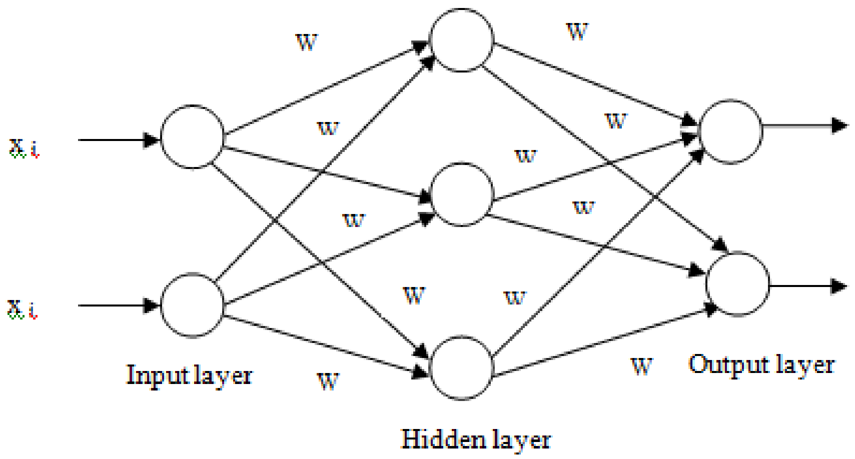

Fig2. An artificial neural network is an interconnected group of nodes

5. Back Propagation Algorithm

Let p the incoming packet and $\{x_1, x_2, \ldots.., x_n\}$ be the feature of packet p.

Let $\{w_1, w_2, \ldots.., w_n\}$ be the connection weights.

The $\{x_1, x_2, \ldots.., x_n\}$ are applied as input to the network.

The activation function is a weighted sum of the inputs x_i multiplied by their respective weights w_{ij}.

$$A_{j(x,w)} = \sum_{i=0}^{n} x_i w_{ji} \quad (1)$$

The output function at the end of the network is,

$$o_j(x,w) = \frac{1}{1+e^{A(x,w)}} \quad (2)$$

Now the goal of the back propagation is to obtain the required output when certain inputs are given. Since the error is the difference between the actual and the required output .The error function for the output of each neuron,

$$E_j(x, w,d) = \left(O_j(x,w) - d_j\right)^2 \quad (3)$$

The error of the network will simply be the sum of the errors of all the neurons in the output layer

$$E_j(x, w,d) = \sum_j \left(O_j(x,w) - d_j\right)^2 \quad (4)$$

As error is depends upon the weights, we can adjust the weight using the method of gradient descendent to minimize the error.

$$\Delta w_{ji} = -\eta \frac{\delta E}{\delta w_{ij}} \quad (5)$$

This formula is used until we find the appropriate weight i.e. minimum error.

Then we need to find out how much error depends on the output, which is the derivative of E in respect to $O_j$from (3)

$$\frac{\delta E}{\delta O_j} = 2\left(O_j - d_j\right) \quad (6)$$

Now from (1) & (2) we get,

$$\frac{\delta o_j}{\delta W_{ji}} = \frac{\delta o_j}{\delta A_j}\frac{\delta A_j}{\delta w_{ji}} = O_j(1 - O_j)x_i \tag{7}$$

From (6) and (7) we get

$$\frac{\delta E}{\delta W_{ji}} = \frac{\delta E}{\delta o_j}\frac{\delta o_j}{\delta w_{ji}} = 2(O_j - d_j)O_j(1 - O_j)x_i \tag{8}$$

From (5) & (8) the adjustment to each weight will be as follows,

$$\Delta w_{ij} = -2\eta(O_j - d_j)O_j(1 - O_j)x_i \tag{9}$$

Now we can use the equation (9) for training the ANN with two layers.

6. Results and Discussion

The proposed system gives the classification and type of attack. It also gives the details of source of attacks. As we are producing our own realtime dataset for training the neural network, we easily update our dataset according to newly generated attacks. In the previous IDS the KDD cup 99 dataset [9] is used so it can only detect the attacks which are in the KDD dataset.

7. Conclusion

Intrusion detection is a process of detection of intrusion in a computer system or network in order to increase the security. The proposed IDS is using the realtime dataset. This system is classifying the intrusion in the computer system and gives the details of source of attack. So it is useful to secure the confidential data in the large organization and one can provide security to confidential data in the computer system.

References

[1] Tejaswini Badgujar, Prof. Priyanka More, “A Review for an Intrusion Detection System Combined with Neural Network”, IJARCSSE, vol.4, March 2014.

[2] Neethu B, “Classification of Intrusion Detection Dataset using machine learning approaches” proceeding of IJECSE, pp 1044 - 1051, 2013.

[3] Mrutyunjaya Panda and Manas Ranjan Patra,” NETWORK INTRUSION DETECTION USING NAÏVE BAYES ”, IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.12, December 2007

[4] D. E. Denning, “An intrusion detection model,” IEEE Transactions on Software Engineering, vol. 13, no. 2, pp. 222 – 232, 1987.

[5] Suseela T. Sarasamma, Qiuming A. Zhu, Julie Huff, “Hierarchical Kohonenen Net for Anomaly Detection in Network Security,” IEEE Transactions on Systems, Man and Cybernetics—Part B: Cybernetics, vol. 35(2), 2005.

[6] Manish Kumar, Dr. M. Hanumanthappa, Dr. T. V. Suresh Kumar “Intrusion Detection System Using Decision Tree Algorithm”, 978-1-4673-2101-3/12/$31.00 ©2012 IEEE.

[7] Garuba, M., Liu, C. & Fraites, D. (2008). Intrusion Techniques: Comparative Study of Network Intrusion Detection Systems. In Proceeding of Fifth International Conference on Information Technology: New Generation, IEEE, 2008

[8] Carlos Gershenson, “Artificial Neural Networks for Beginners”

[9] Mahbod Tavallaeev, Ebrahim Bagheri, Wei Lu, and Ali A. Ghorbani, “A Detailed Analysis of the KDD CUP99 Data Set” Proceedings of the 2009 IEEE Symposium on Computaional Intelligence in Security and Defense Application (CISDA 2009), IEEE 2009.