International Journal of Enhanced Research in Science Technology & Engineering, ISSN: 2319-7463
Vol. 4 Issue 6, June-2015, pp: (219-227), Impact Factor: 1.252, Available online at: www.erpublications.com

# Designing of Feed Forward Artificial Neural Network Technique to Reduce Attack of Dos in Wireless System

Nikita[1], Sudhir Malik[2], Sheetal Malik[3]

[1]M. Tech Scholar, Dept. of ECE, RNCE, Rohtak, Haryana
[2]Asst. Professor, Dept. of ECE, RNCE, Rohtak, Haryana
[3]Asst. Professor & HOD, Dept. of ECE, RNCE, Rohtak, Haryana

**Abstract: Security has become more and more important in our life according to development. A technology that is developed to assess the security of computer systems or network is one of the most popular types of security management system for computers and networks which is defined as intrusion detection system. There are various techniques of Artificial Neural Network, which can be applied to Intrusion Detection System. Each technique is suitable for some specific situation. Denial of Service (Dos) is a type of attack in which a hacker issues a huge amount of packets to congeal specific servers' services, consequently blocking legitimate users from normal access to the services. As the DOS attack will be resolved in this work, the throughput of the network will be improved and network delay will be reduced.**

**Index Terms: Artificial Neural Network (ANN), Back Propagation Neural Network, Delay of Service (DOS), Feed Forward Neural Network, Intrusion Detection System (IDS), Network Security.**

## I. Introduction

The preservation of security has become more difficult by time because the possible technologies of attack are becoming more superior. At the same time, less technical ability is required for the novice snoopier because the verified past methods are easily accessed through the organization. The main idea of protecting the information through the encrypted channel for data and also confirming the identity of the connected device through the firewall, which will not accept any connection with a stranger, firewalls do not provide full protection for the system (Rung-Ching , Kai-Fan and Chia-Fen ,2009). So, it is needed to extend the network security capabilities by complementing with other tools or intrusion detection system (IDS is not a replacement for either a good antivirus program or firewall). Since it is technically impossible to create computer systems (Hardware & Software) without any defect or security failure, intrusion detection in computer system's researches is specifically regarded as important.

IDS  is a protective system that can detect disorders occurring on the network. The procedure goes as intrusion detection can report and control occurred disorders through steps including collecting data, seeking ports, controlling computers, and finally hacking. So, intrusion detection can report control intrusion sabotage that composed of phases collecting data, probing port, gaining computer's control and finally hacking. In The purpose of an Intrusion Detection system is not to prevent an attack, but only to discover and possibly detect the attacks and to recognize security problems in system or computer networks and also to report it to the system administrator[5]. Intrusion Detection systems are generally used with Firewalls as their security complements. Detection of anomaly outside-in traffics of the network and reporting it to the administrator, or preventing suspected contacts is the other feature of IDS.

IDS is capable of detecting attacks by both internal and external users [9]. Wang et al. have declared their ideas about intrusion detection and have explored different methods of neural network. There are many different intelligent techniques for designing intrusion detection systems, such as Machine learning, data mining, and fuzzy sets which are divided into two groups of Fuzzy set and Fuzzy anomaly detection, to mention some. Neural network algorithms are also divided into two groups of Supervised Learning and Unsupervised Learning [14]. In this paper, we consider some different agents, each of which can detect one or two DOS attacks. These agents interact in a way not to interfere each other. Parallelization

Technology is used to increase system speed. Since the designed agents act separately and the result of each agent has no impact on the others, we can run each system on discrete CPUs (depending on how many CPUs are used in IDS computers) to speed up the performance.

## II. Intrusion Detection System

Nowadays, Intrusion detection systems are most original and complete parts of a network monitoring system. Intrusion detection system technologies relatively are new and promise us that we will do in order to detect network intrusion that will help. Intrusion detection is the process in which events and incidents on a system or network monitoring and monitoring of the network or system intrusion is detected[1] . The goal of intrusion detection is screening, evaluating and reporting of network activity. This system acts on the data packets that have passed access control tool. Due to the reliability limitations, internal threats, and the presence of required doubt and hesitation, the intrusion prevention system should allow some cases of suspected attacks to pass in order to decrease the probability of false detections (false positive). Intrusion detection systems (IDS), are responsible for identifying and detecting any unauthorized use of the system, abuse or any damage caused by both internal and external users[4] .

Intrusion detection systems try to detect anomaly intrusions to the network by special algorithms which can be divided into 3 categories of misuse-based, anomaly-based, and specification-based. Analyzing the user's behavior in the network, the anomaly-based system can find out the intrusions. In anomaly-based method, an index of normal behavior is created. An abnormality may be an indication of an intrusion. Indexes of normal behavior are created based on approaches like Neural Networks, Machine Learning methods, and even life style safety systems. To detect anomalous behaviors, normal behaviors should be identified and some specific patterns and rules should be designed for them. The behaviors which follow these patterns are considered as normal and events which show any deviation beyond the normal statistics of these patterns are detected as abnormal. It's extremely difficult to detect abnormal intrusions, because there is no consistent pattern to monitor them. Usually an event which shows more than two deviations from the normal behavior is assumed to be normal. According to the rapid expansion of networks over the past century, system protection has become one of the most important issues in Computer Systems due to the existence of gaps in most of the components of protection systems such as FIREWALL systems.

Thus intrusion detection systems (IDS) are used as secondary computer systems protector to identify and avoid illegal activities or gaps. The intrusion detection problem is considered as a pattern recognition, and the artificial neural network must be trained to distinguish between normal and unusual patterns [2]. Unfortunately, unusual anomaly-based intrusion detections and IDSs of this kind cause many false alarms (false positive) due to the fact that the behavior patterns of the users and the system are very previous attacks), abnormal behavior detection methods can detect any kind of new attacks. In misuse-based technique, usually known as signature-based detection, pre-designed intrusion templates (signatures) are stored as law, in a way that each template contains different types of a specific intrusion and once a template of this kind appears in the system, the intrusion occurring is alarmed. Usually, in these methods, the detector has data bases of attack signatures or templates and tries to detect patterns that are similar to those stored in its own data base. This kind of methods are able to detect known intrusions, and if new attacks appear anywhere in the network, they are not able to detect them. The administrator should continuously add the templates (patterns) of new attacks to the intrusion detection system. One of the advantages of this method is the high accuracy applied in detecting intrusions the templates of which have precisely given to the system.

## III . Set of Data

The Information System Technology Group at Massachusetts Institute of Technology – Lincoln Laboratory, sponsored by Defence Advanced Research Project Agency (DARPA) and Air Force Research Laboratory, has collected and evaluated the first standard corpora for evaluation of computer network Intrusion Detection Systems. This is called the DARPA Intrusion Detection Evaluation [7]. The data sets used in this research are the data sets from the 1998 DARPA Intrusion Detection Evaluation Program. In the dataset, the following attacks are present according to the actions and goals of the attacker. Each attack type falls into one of the following four main categories:

### A. Denial of Service Attacks

Denial of Service (DoS) is a class of attacks where an attacker makes some computing or memory resource too busy or too full to handle legitimate requests, thus denying legitimate users access to a machine. There are different ways to launch DoS attacks:

- Abusing the computers legitimate features.
- Targeting the implementations bugs.
- Exploiting the system's misconfigurations.

DOS attacks are classified based on the services that an attacker renders unavailable to legitimate users. An attack used was Apache2, Back, Mail bomb, Neptune Ping of death, Process table, Smurf, Syslogd and UDP storm [2].

### B. Probing

Probing is a class of attacks where an attacker scans a network to gather information or find known vulnerabilities. An attacker with a map of machines and services that are available on a network can use the information to look for exploits. There are different types of probes: some of them abuse the computer's legitimate features, some of them use social engineering techniques. This class of attacks is the most commonly heard and requires very little technical expertise.

### C. User to Root Attacks

User to root exploits are a class of attacks where an attacker starts out with access to a normal user account on the system and is able to exploit vulnerability to gain root access to the system. Most common exploits in this class of attacks are regular buffer overflows, which are caused by regular programming mistakes and environment assumptions. Attacks used was Perl and Xterm [2].

### Remote to User Attacks

A remote to user (R2L) attack is a class of attacks where an attacker sends packets to a machine over a network, then exploits machine's vulnerability to illegally gain local access as a user. There are different types of R2L attacks; the most common attack in this class is done using social engineering. Attacks used was Dictionary, FTP-write, Guest, Imap, Named, Phf, Sendmail, Xlock and Xnsnoop[2].

## IV. Artificial Neural Network

Artificial neural networks born after McCulloc and Pitts introduced a set of simplified neurons in 1943. These neurons were represented as models of biological networks into conceptual components for circuits that could perform computational tasks. The basic model of the artificial neuron is founded upon the functionality of the biological neuron [10]. By definition, "Neurons are basic signaling units of the nervous system of a living being in which each neuron is a discrete cell whose several processes are from its cell body. One can differentiate between two basic types of networks, networks with feedback and those without it. In networks with feedback, the output values can be traced back to the input values. Hence only, a forward flow of information is present. Network having this structure are called as feed forward networks. There are various nets that come under the feed forward type of nets. A multilayer feed forward back propagation network with one layer of z-hidden units. The Y output unit has Wok bias and Z hidden unit has Vok as bias. It is found that both the output units and the hidden units have bias. The bias acts like weights on connection from units whose output is always 1. This network has one input layer, one hidden layer and one output layer. There can be any number of hidden layers. The input layer is connected to the hidden layer and the hidden layer is connected to the output layer by means of interconnection weights. The bias is provided for both the hidden and the output layer, to act upon the net input to be calculated [14].

## V. Training Algorithm

The training algorithm of back propagation involves four stages [14], viz.

1. Initialization of Weights
2. Feed Forward
3. Back Propagation of errors
4. Updation of the weights and the biases.

During first stage which is the initialization of weights, some small random values are assigned. During feed forward stage each input unit (Xi) receives an input signal and transmits this signal to each of the hidden units Z1………Zp. Each hidden unit then calculates the activation function and sends its signal Zj to each output unit. The output unit calculates the activation function to form the response of the net for the given input pattern. During back propagation of errors, each output unit compares its computed activation yk with its target value tk to determine the associated error for that pattern with that unit. Based on the error, the factor $\delta k$ is computed and is used to distribute the error at output unit yk back to all units in the previous layer.

$x$: (x1, ……….xi,…., xn)
t: Output target vector
t: (t1, ……….ti,…., tn)
$\delta k$ =error at output unit yk
$\delta j$ =error at hidden unit zj
$\acute{\alpha}$= learning rate
Voj= bias on hidden unit j
zj= hidden unit j
wok=bias on output unit k
yk= output unit k.
The training algorithm used in the back propagation network is as follows. The algorithm is given with the various phases:

### D. Initialization of Weights

Step 1: Initialize weight to small random values.
Step 2: While stopping condition is false, do Steps 3-10.
Step 3: For each training pair do steps 4-9.

### E. Feed Forward

Step 4: Each input unit receives the input signal xi and transmits this signals to all units in the layer above i.e hidden units.
Step 5: Each hidden unit( zj, j=1,……,p) sums its weighted input signals.
$z\text{-}inj=voj+\Sigma xivij$ (1)
applying activation function
$Zj=f(zinj)$ (2)
and sends this signal to all units in the layer above i.e. output units.
Step 6: Each output unit (yk) sums its weighted input signals.
$y\text{-}ink=wok+\Sigma zjwjk$ (3)
and applies its activation function to calculate the output signals.
$Yk=f(y\text{-}ink)$ (4)

### F. Back Propagation of Errors

Step 7: Each output unit receives a target pattern corresponding to an input pattern, error information term is calculated as
$\delta k=(tk-yk)f(y\text{-}ink)$ (5)
Step 8: Each hidden unit (zj) sums its delta inputs from units in the layer above
$\delta\text{-}inj=\Sigma\delta jwjk$ (6)
The error information term is calculated as
$\delta j=\delta\text{-}injf(z\text{-}inj)$ (7)

### G. Updation of Weight and Biases

Step 9: Each output unit (yk) updates its bias and weights (j=0,…..,p)
The weight correction term is given by
$\Delta Wjk=\acute{\alpha}\delta kzj$ (8)
and the bias correction term is given by
$\Delta Wok=\acute{\alpha}\delta k$ (9)
$Wjk(new)= Wjk(old)+\Delta Wjk$, $Wok(new)=Wok(old)+\Delta Wok$ (10)
Each hidden unit (zj,j=1,…….p) updates its bias and weights (i=0,…..n)
The weight correction term
$\Delta Vij=\acute{\alpha}\delta jxi$ (11)
The bias correction term
$\Delta Voj=\acute{\alpha}\delta j$ (12)
$Vij(new)= Vij\ (old) + \Delta Vij$ , $Voj(new)= Voj\ (old) + \Delta Voj$ (13)

Step 10: Test the stopping condition.

The stopping condition may be the minimization of the errors, number of epochs etc.

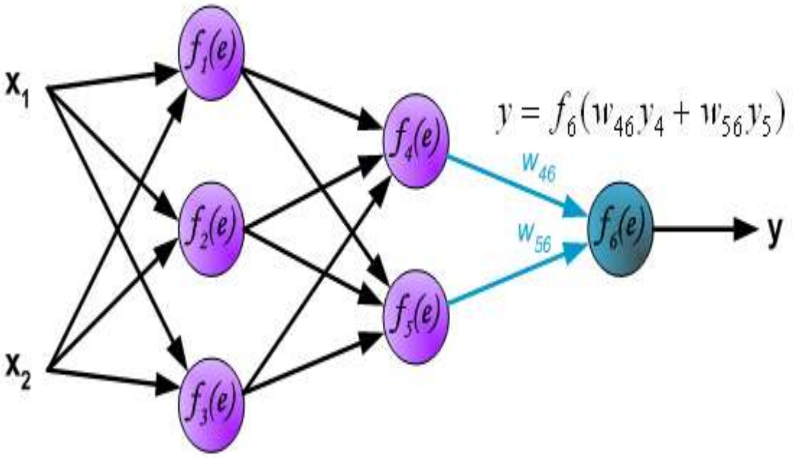

**Fig. 1: Feed Forward Networks**

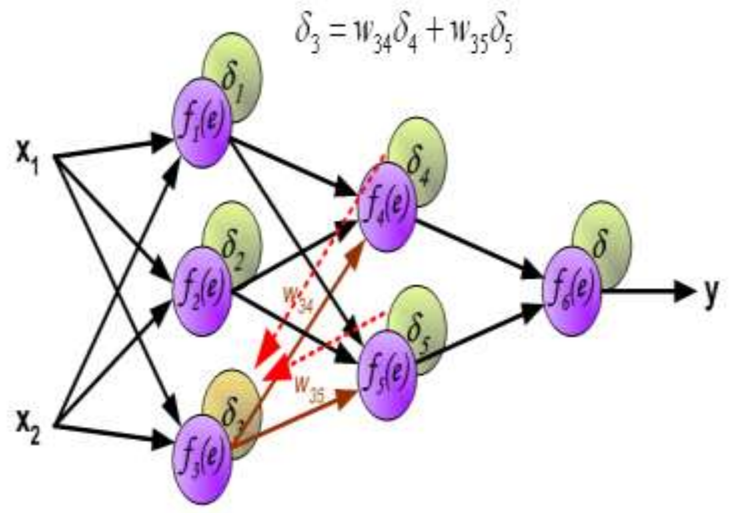

**Fig. 2: Back Propagation of Errors**

## VII. The Proposed Method

In this section, the implementation of the proposed intrusion detection system, implementation steps and evaluation criteria are described.

### H. Implementation

The network attacks can be divided in four groups of DOS, R2L, U2R, Probe. In the designed IDS, the system can detect DOS -type attacks, in very high detection rate. In fact, this kind of IDS is responsible for the detection attacks, which can be included in DOS category.

In order to design this type of IDS, we identified DOS attacks and designed a separate IDS for each one to detect that specific attack. In general, considering the designed IDS, the system will detect DOS attacks in the network (if there is any). The whole process of the system is shown in Figure 3.

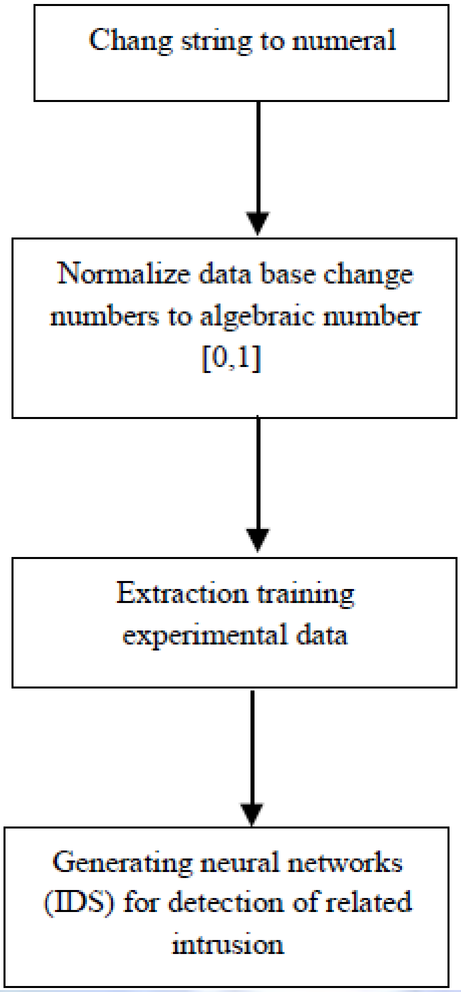
Chang string to numeral
Normalize data base change numbers to algebraic number [0,1]
Extraction training experimental data
Generating neural networks (IDS) for detection of related intrusion

**Fig. 3.The Process of generating system of intrusion detection**

As you see in figure 5, in order to train neural network and have a more qualified process, we made some changes in database which as you see didn't affect on the totality of data base. It is just done for improving the function of neural network.

**I. Evaluation Criteria**

To measure and detect the efficiency of the designed IDSs or the exact degree of their assurance and correctness the following criteria can be used [2]:

True negative = correctly detect the normal data
True positive = correctly detect the attack
False Positive = distinguish normal events as attacks
False negative = distinguish the incidents of attack as normal
TNR = TN / (TN + FP) = the total number of normal incidents that are correctly detected / the total number of normal incidents that are detected as normal.
TPR = TP / (TP + FN) = the number of incidents of attack that are correctly detected / the total number of incidents that are detected as attacks.
FNR = FN / (FN + TP) = the number of attack incidents that are detected as normal / the total number of incidents that are detected as normal.
FPR = FP / (FP + TN) = the number of normal incidents which are detected as attack / the total number of incidents which are detected as attack.

In this implementation, we used the TPR criterion and as you see in the chart above, the efficiency of this implementation is approximately more than 98%

## VIII. Results and Discussion

After executing the Program of Training of Neural Network values of y, W. W0, V, V0 are as under.
Y = 0.7593 0.9990 0.0949 0.9694 0.9234 0.1133 1.0000 1.0000 0.1660 0.8952 0.8883 1.0000 0.6756 1.0000 0.0000 0.0000 0.9569 0.0504
EPOCH = 990000
W =
[ 69.7724
-92.1417
75.1616 ]
WO =
[ 5.7396]
V =
[ -101.2418 -48.9699 238.5258
180.6523 215.8780 -0.1458
-245.0327 -305.1403 9.9378]
VO = [ 0.9382 4.7101 -1.8095

The Graphical representation of Epoch and Error is as shown in Fig. 6 which is plot between Epoch Number and Error. As we know, when iterations increases error between target value and output value decreases which is clear from Fig. 4.

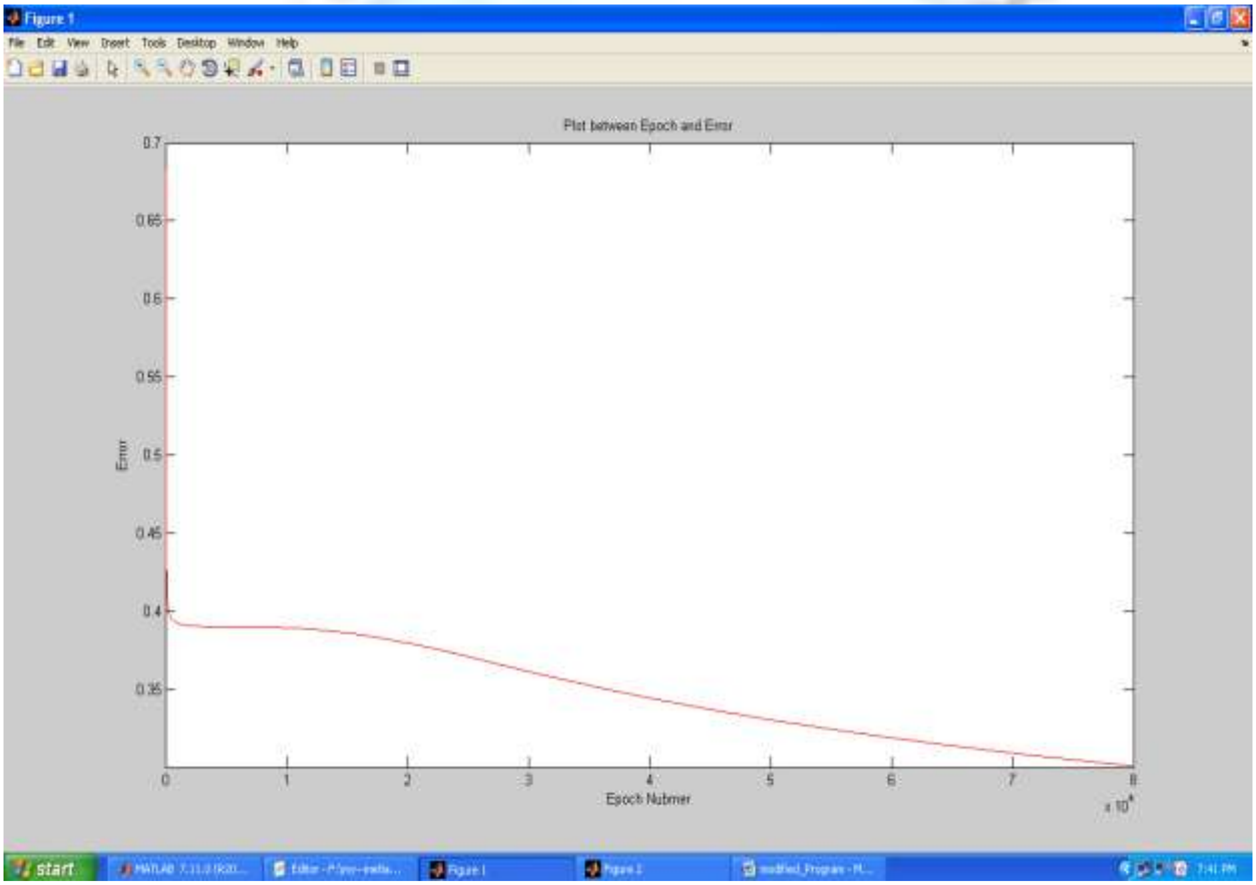

**Fig.4 Plot between Epoch Number and Error.**

Now, as we know as the iterations increases output value reaches to target value it is clearly shown in Fig. 5 which is a plot between epoch and output value.

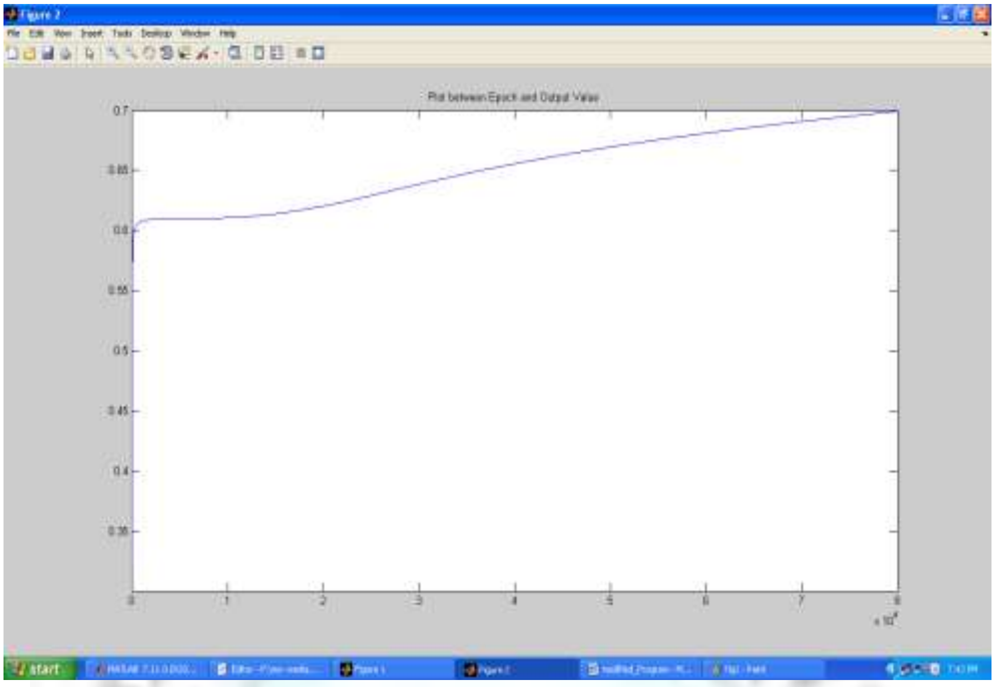
Figure 2
File Edit View Insert Tools Desktop Window Help
Plot between Epoch and Output Value
0.7
0.65
0.6
0.55
0.5
0.45
0.4
0.35
0
1
2
3
4
5
6
7
8
x 10^4
start

**Fig. 5 Plot between Epoch Number and Output Value**

Now, Using these values of W, W0, V, V0 in the program of Forecasting of Attack or Normal Traffic by Neural Network value of y forecasted is 1 which is clearly a attack. So this is an excellent technique of forecasting of attack or normal traffic.

## IX. Future Scope

As mentioned above, there has been a lot of research on intrusion detection, and also on the use of neural networks in intrusion detection. As showed in this thesis, back propagation neural networks can be used successfully to detect attacks on a network. The same experiments should also be conducted with other types of neural networks to see if these types can improve the detection rate we got from the experiments with a back propagation neural network.

## X. Limitations

As for many studies; there are some different challenges viewed in the intrusion detection systems. In this study, some limitations were faced. They can be summarized as follows:

1) Intrusion detection systems need a periodic update to the training set and profiles.
2) Using a static training data might become outdated and deficient for prediction.
3) The accuracy of classification for the data do not 100%.

## Conclusion

There are various techniques of Artificial Neural Network, which can be applied to Intrusion Detection System. Each technique is suitable for some specific situation. BPNN is easy to implement, supervised learning artificial neural network. Number of the epochs required to train the network is high as compare to the other ANN techniques. But, detection rate is very high. BPNN can be used when one wants to not only detect the attack but also to classify the attack in to specific category so that preventive action can be taken. By combining the different ANN techniques, one can reduce the number of the epochs required and hence can reduce the training time. As the DOS attack will be resolved in this work, the throughput of the network will be improved and network delay will be reduced. The work does not require any additional hardware and is software based. In the future this system could be extended to an online system by little effort.

## References

[1] Bhavin Shah, Bhushan H Trivedi, "Artificial Neural Network based Intrusion Detection System", International Journal of Computer Applications" Volume 39– No.6, February 2012.

[2] Manoranjan Pradhan, Sateesh Kumar Pradhan, Sudhir Kumar Sahu, "Anomaly Detection using Artificial Neural Network","International Journal of Engineering Sciences & Emerging Technologies, April 2012".

[3] Zahra Moradi1, Mohammad Teshnehlab , "Intrusion Detection Model in MANETs using ANNs and ANFIS", 2011 International Conference on Telecommunication Technology and Applications, Singapore

[4] Mehdi MORADI and Mohammad ZULKERNINE, "A Neural Network Based Ssytem for Intrusion Detection and Classification of Attacks".

[5] Przemysław Kukiełka, Zbigniew Kotulski, "Adaptation of the neural network- based IDS to new attacks detection".

[6] M. Dondo and J. Treurniet, "Investigation of a Neural Network Implementation of a TCP packet Anomaly Detection System", Defence Research and Development Canada, May 2004.

[7] V.Sivakumar1,T.Yoganandh,R.Mohan Das, "Preventing Network From Intrusive Attack Using Artificial Neural Networks", International Journal of Engineering Research and Applications (IJERA), Vol. 2, Issue 2,Mar-Apr 2012, pp.370-373.

[8] Samaneh Rastegari, M. Iqbal Saripan and Mohd Fadlee A. Rasid, "Detection of Denial of Service Attacks against Domain Name System Using Neural Networks", IJCSI International Journal of Computer Science Issues, Vol. 6, No. 1, 2009.

[9] S. Devaraju, S. Ramakrishnan, " Detection of Accuracy for Intrusion Detection System using Neural Network Classifier", International Journal of Emerging Technology and Advanced Engineering (IJETAE).

[10] Afrah Nazir, " A Comparative Study of different Artficial Neural Networks based Intrusion Detection Systems" International Journal of Scientific and Research Publications, Volume 3, Issue 7, July 2013.

[11] Sudhakar Parate, S. M Nirkhi, R.V Dharaskar, "Application of Neural Forensics for detection of Web Attack using Neural Network", National Conference on Innovative Paradigms in Engineering and Technology(NCIPET-2013).

[12] Przemysław Kukiełka, Zbigniew Kotulski, "Analysis of Neural Networks usage for detection of a new attack in IDS", Annales UMCS Informatica AI X, 1 (2010) 51-59.

[13] Tariq Ahamad and Abdullah Aljumah, "Hybrid Approach using intrusion Detection System", International Journal of Computer Networks and Communications Security, VOL. 2, NO. 2, FEBRUARY 2014, 87–92.

[14] Amit Garg and Ravindra Pratap Singh, " Voltage Profile Analysis in Power Transmission System based on STATCOM using Artificial Neural Network in MATLAB/SIMULINK", International Journal of Applied Information Systems(IJAIS), Foundation of Computer Science, New York, USA, Volume 6- No. 1, September 2013.

## AUTHORS BIOGRAPHY

**Nikita Balhara** has completed her B. Tech in Electronics and Communication Engineering from PDM College of Engineering, Bahadurgarh, Haryana, India and now pursuing her M.Tech in Electronics and Communication Engineering from RN Engineering College, Rohtak, Haryana, India. Her interests include Intrusion Detection System and Artificial Neural Network.

**Sudhir Malik** is working as an Assistant Professor in Electronics and Communication Engineering Department in RN Engineering College, Rohtak, Haryana, India.