International Journal of Enhanced Research in Science Technology & Engineering, ISSN: 2319-7463
Vol. 4 Issue 5, May-2015, pp: (326-332), Impact Factor: 1.252, Available online at: www.erpublications.com

# To Detect Denial of Service Attack in MANET by ANN Based Technique

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: Denials of Service (DoS) attacks are a serious threat for the prominent e-commerce internet sites such as Amazon, CNN, E*Trade, Yahoo and eBay. DoS attacks can consume memory, CPU, and network resources and damage or shutdown the operation of the resource under attack (victim). The quality of service enabled networks (QoS), which offer different levels of service, is vulnerable to such DoS attacks. 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. This paper discusses various the attack mechanisms and problems due to DoS attack, also how MANET can be affected by these attacks.**

**Keywords: ANN, DOS, IDS, Network Security, MANET, QoS.**

---

## INTRODUCTION

A MANET is a collection of mobile nodes that organize themselves into a network without any pre-defined infrastructure and mainly it is a dynamic network topology. The security goal of MANET includes availability, integrity, authentication, confidentiality and non-repudiation. Many types of attacks can threat the MANET such as Black hole, Routing loops, Network partition, Selfishness, Sleep deprivation and Denial of Services. This work mainly focuses on DOS attack. Therefore, nodes in MANETs are more vulnerable to DOS attacks. The attackers in MANET use IP spoofing to conceal their real identities and it becomes a challenging task to trace the remote attacker in MANET .Thus, the implementation of Zone Sampling-Based Trace back (ZSBT) algorithm is used for tracing DoS attackers in MANET and also improves the security level of MANET. Intrusion detection systems (IDSs) [9] are the foremost tools for providing safety in computer and network system.

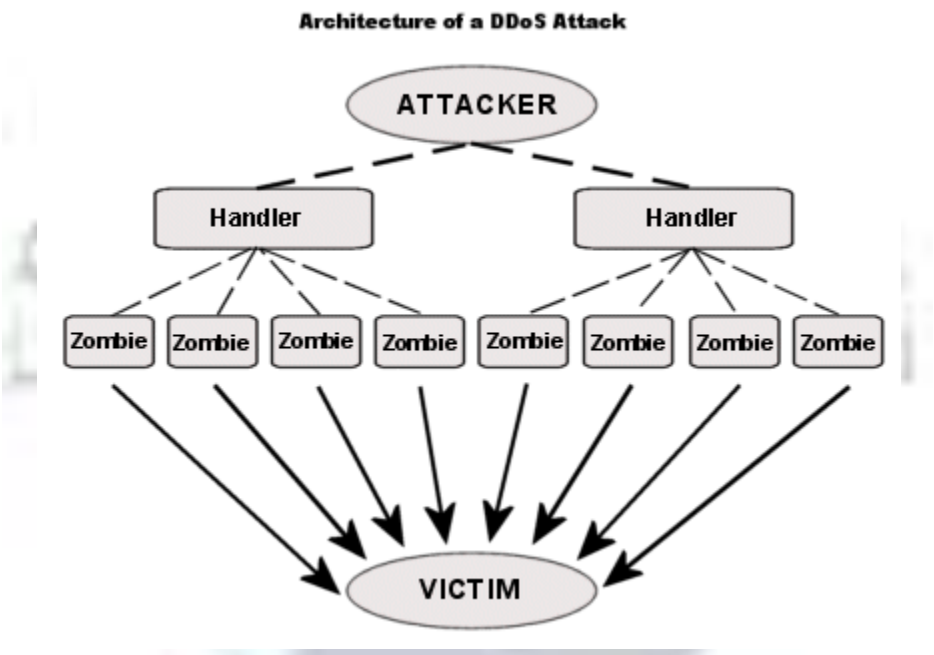
There are many limitations in traditional IDSs like time consuming, regular updating, non adaptive, accuracy and flexibility. So a new IDS is designed which is inspired by Artificial Neural Network, that provides maximum security. It evaluates new IDS against the DOS attack and evaluates the performance of the new IDS and compares the results with traditional IDSs. In a type of DOS attack, an intruder node injects a large amount of junk packets into the network and causes a denial in the services of the attacked node. ANN modeling and ZSBT method uses a simulated MANET environment for detecting nodes under DOS attack effectively. Artificial Neural Network is a Mathematical Model or Computational Model inspired by human biological neural structures. An artificial neural network is an interconnected group of nodes. ANN and ZSBT method is used for the detection of DOS attack in the network. A method called “Trace back” is to be implemented here as an IDS.

The network parameters have to be investigated to identify the existence of attacks in the network. The attacker spoofs the IP address of the other node and sends the packets with abnormal rate. This is known as IP spoofing [4]. So the IDS have to find the original DOS source node, if the DOS source node spoofs the IP. So the trace back alone is not enough to handle the DOS attack. So, “IDPF” (Inter Domain Packet Filters) is introduced to identify the spoofed nodes. This IDPF helps to find whether the IP is spoofed or not. If it is spoofed, then this method stops receiving the packets from the DOS packet’s path. By this way, the network is protected from such attacks [3]. But in the ZSBT method [5], a node forwards a packet along with the IP address and zone ID. By employing IP spoofing attackers can evade from detection. But with the help of Zone ID, the attacker node can be identified easily and the network is protected from such attacks.

## METHODOLOGY

To design the model following steps must be taken:
1. Network creation and routing
2. DOS attack implementation
3. Parameter selection
4. NS2 simulation
5. ANN and ZSBT based IDS implementation

**1. Network creation and routing:** In this module, the nodes are created in the network. The nodes in the network are configured with type of channel, data structure to be used, size of the data structure, type of routing protocol, and other necessary parameters. GOD- General Operations Director is to be created which gives reference to all the necessary c++ files for all nodes. A network topology is to be created by deploying all nodes in different areas or locations in the simulation area, and ensure that all the nodes are in the coverage area. The nodes should be mobile nodes, since the network is MANET. The nodes are provided with mobility to move randomly across the network. But in the ZSBT method, the network is partitioned into several zones and assigns unique Zone ID for each zone. Thus with the help of Zone ID, the attacker node can be easily identified




**2. DOS attack implementation**: In a type of DOS attack, an intruder node injects a large amount of junk packets into the network. This action consumes a significant portion of network resources and causes a denial the services that attacked node could provide for other nodes.

**3. Parameter selection:** In a network, the DOS attack can be detected with the help of following parameters:

**Packet loss (PL):** It calculates the average number of packets dropped in every time frame on the links from destination to host node.

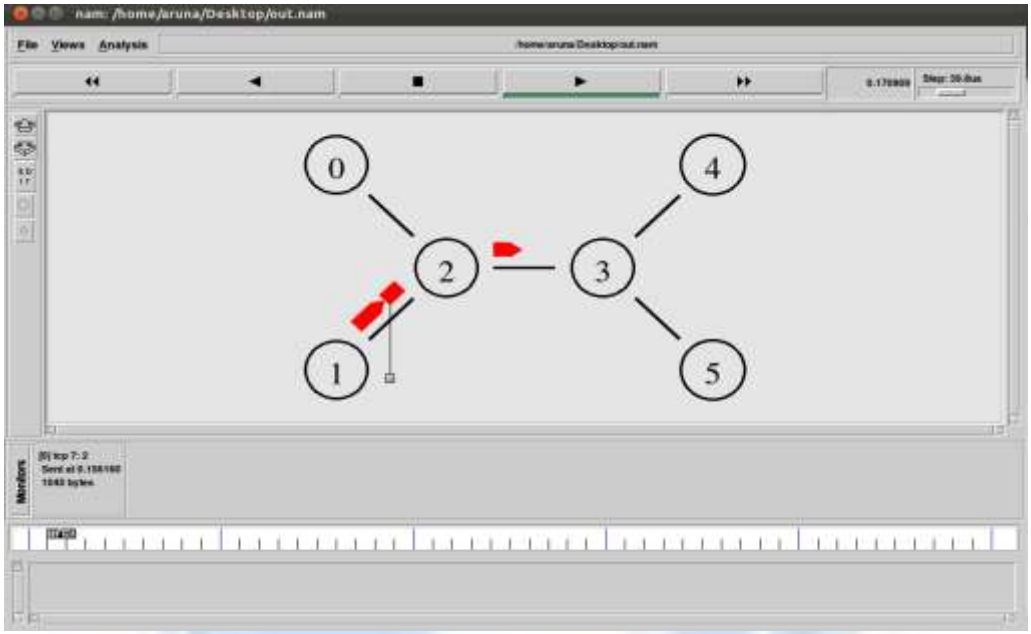
**Packet Sending (PS):** It calculates the average number of packets that are sent between two nodes and shows the traffic load of host nodes.

**Packet Receiving (PR):** It calculates the average number of packets received in every time frame.

**Energy Consumption (EC):** DOS attack may exhaust the battery power of destination node. It measures the amount of energy every node consumes in every time frame. These parameters have to be analyzed. Therefore, a sample communication is to be performed between two nodes. The sender node is configured as DOS source node, and the sender

node sends the packet with abnormal rate to the receiver. And one more communication between two nodes is to be made. These two nodes are normal nodes. Then, the number of packets sent between two nodes (PS), number of packets dropped (PL), number of packets received (PR), and the total energy consumption (EC) are to be evaluated between two normal nodes and between the DOS source and receiver node. The analysis results are to be plotted as X-Graphs and the results are to be compared. Based on the comparison, the communication between DOS source and destination consumes more resources than the normal one.

**4. NS2 Simulation:** Here the simulation was carried out using NS-2. The network is constructed with several nodes and ensures that every node is connected at-least to one node via mobile agents. The mobile agents serve as a communication agent between nodes.



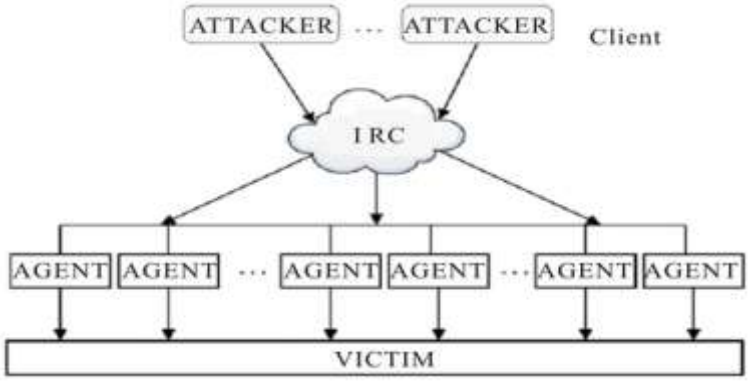

**5. ANN and ZSBT based IDS implementation:** An ANN and ZSBT based IDS are to be implemented to act against DOS attack. A method called "Trace back" is implemented here as an IDS. The attacker spoofs the IP address of the other node and sends packets with abnormal rate. So the IDS have to find the original DOS source node, if the DOS source node spoofs the IP. So the trace back alone is not enough to handle the DOS attack. So "IDPF" (Inter Domain Packet Filters) is used to identify the spoofed nodes. The trace back method monitors the packet flow from the node. If the rate is abnormal, then it avoids to receiving the packets from the node (the receiver node identifies the node by seeing the IP address of the sender node in packet's header information.

Packet's header information contains all info about the sender including IP) and denies the services to the particular node. But in case of ZSBT method sender node forwards packet along with the IP address and Zone ID. At the same time, the IDPF starts to find the source node of the attacker. IDPF sends the inquiry packet (normally a request packet), to ask about the node's abnormal flow. If the node is not a source node, then it simply gives the NO answer. So the IDPF knows that the IP is spoofed. So the IDPF stops receiving the packets from the DOS packet's path. Both the method stops further receiving of DOS packets from that path. The source of the attacker can be easily identified with the help of Zone ID. Thus the ZSBT method works well when compared with ANN. Because in ANN method, all nodes have to be searched in order to find the source node of the attacker. Thus the network is protected from DOS attacks.

## Dos Attack Scenarios

The DoS attacks that target resources can be grouped into three broad scenarios. The first attack scenario targets Storage and Processing Resources. This is an attack that mainly targets the memory, storage space, or CPU of the service provider. Consider the case where a node continuously sends an executable flooding packet to its neighborhoods and to overload the storage space and deplete the memory of that node. This prevents the node from sending or receiving packets from other legitimate nodes. Neighborhood watch and monitoring can prevent the occurrence of such events by gradually excluding such malicious nodes. The second attack scenario targets energy resources, specifically the battery power of the service

provider. Since mobile devices operate by battery power, energy is an important resource in MANETs. A malicious node may continuously send a bogus packet to a node with the intention of consuming the victim's battery energy and preventing other nodes from communicating with the node. The use of localized monitoring can help in detecting such nodes and preventing their consequences. The third attack scenario targets bandwidth. Consider the case where an attacker located between multiple communicating nodes wants to wastethe network bandwidth and disrupt connectivity.




The malicious node can continuously send packets with bogus source IP addresses of other nodes, thereby overloading the network. This consumes the resources of all neighbors that communicate, overloads the network, and results in performance degradations. Such attacks can be prevented based on the reputation information exchanged among the involved nodes or the cluster head. We attempt to prevent both selfish and malicious nodes from degrading network performance by providing incentives to encourage cooperation and punishing nodes that do not cooperate (Mieso K Denko, 2010).

**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 (Afrah Nazir, 2013). 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. However there are networks wherein for every input vector laid on the network, an output vector is calculated and this can be read from the output neurons.

There is no feedback. 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 zhidden 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 (Amit Garg and Ravindra Pratap Singh, 2013).

**Training Program in Matlab**

Now from these different values of Start Time, Duration and Service a neural network is trained through a x: which is a input training vector as. Input training vector in this case is Start Time, Duration and Service. Output target vector t is Attack or Normal Traffic in this case. If it is a Normal traffic output t is 0 if it would be attack it would be 1. Weight W and v are initialized to small random values. W0 and V0 are bias. Initially Neural Network is trained using 18 different values of Start Time, Duration and Service. Iterations done in this program are 990000.

```
 clc;
 clear;
W=[-3.2184; -12.5463; 0.6328];
```

```
Wo=[9.5708];
 v=[0.8153 -0.0614 0.9105; 6.6872 19.4263 0.2000; 0.1294 0.0324 0.2064];
 vo=[0.4346 0.8483 -0.4499];
x=[.020 .020 .040 .040 .040 .040 .008 .008 .015 .015 .030 .030 .035 .035 .002 .002 .004 .004; .004 .004 .010 .010 .015 .015
.025 .025 .002 .002 .002 .002 .002 .002 .010 .010 .020 .020; 005 .010 .005 .010 .005 .010 .005 .010 .005 .010 .005 .010
.005 .010 .005 .010 .005 .010];
t= [1 1 0 1 1 0 1 1 0 1 0 1 1 1 0 0 1 0 ];
 epoch=1;
 alpha=.3;
while(epoch<990000);
 for I=1:18
for i=1:3
zin1=0;
 for j=1:3
zin1=zin1+x(j,I)*v(j,i);
end
zin(i)=zin1 + vo(i)*1;
z(i)=1/(1+exp(-zin(i)));
end
 yin1=0;
for i=1:3
yin1=yin1+z(i)*W(i,1);
 end
epo(epoch)=epoch;
 error(epoch)=t(5)-y(5);
 n(epoch)=y(5);
 epoch=epoch+1;
 end figure plot(epo,error,'r');
xlabel('Epoch Nubmer');
ylabel('Error');
 title('Plot between Epoch and Error');
 figure plot(epo,n,'b');
title('Plot between Epoch and Output Value');
 y
epoch
```

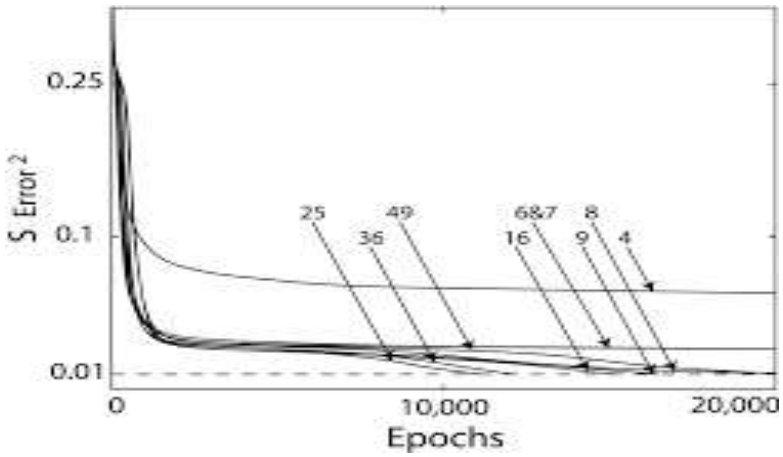
Output of the Training Program are Weights (W and V) and Bias (W0 and V0 ). Now using these values of Weights and Bias in Neural Network at any values of Start Time, Duration and Service and the condition of Attack or Normal Traffic can be easily forecasted through a program in MATLAB

## Results and Discussion

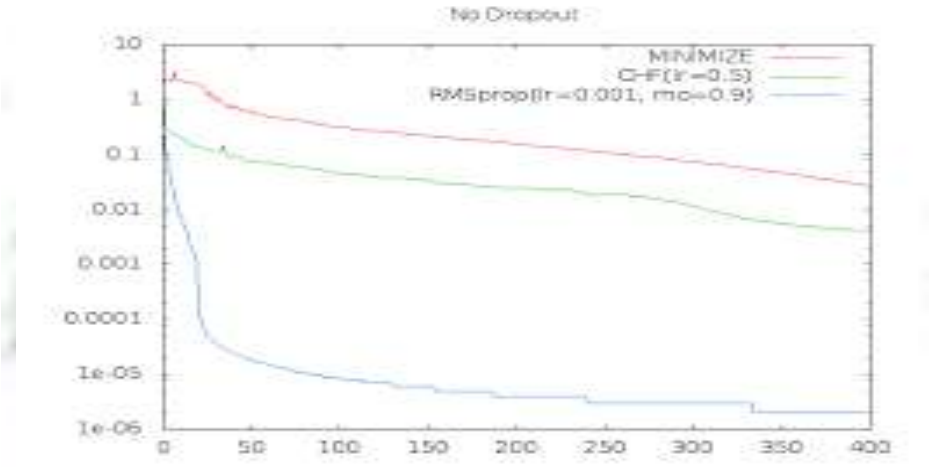
After executing the Program of Training of Neural Network specified in section IV values of y, W. W0, V, V0 are as under.

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 Figure 7.1 which is plot between Epoch Number and Error. As we know, when iterations error between target value and output value decreases which is clear from Figure 1.




Now, as we know as the iterations increases output value reaches to target value it is clearly shown in Figure 7.2 which is a plot between epoch and output value.




## 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. Change in the number of nodes in hidden layer resulted in the change in classification rate and also change in the false positive rate and false negative rate for the neural network based intrusion detection systems. 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]. **Afrah Nazir (2013),** "A Comparative Study of different Artficial Neural Networks Based Intrusion Detection Systems" International Journal of Scientific and Research Publications, Vol. 3, No. 7.
[2]. **Amit Garg and Ravindra Pratap Singh (2014),** "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, Vol. 6, No. 1.
[3]. **Bhavin Shah and Bhushan H Trivedi (2012),** "Artificial Neural Network Based Intrusion Detection System", International Journal of Computer Applications, Vol. 39, No. 6.
[4]. **M Dondo and J Treurniet (2004),** "Investigation of a Neural Network Implementation of a TCP Packet Anom Detection System", Defence Research and Development Canada.
[5]. **Manoranjan Pradhan, Sateesh Kumar Pradhan and Sudhir Kumar Sahu (2012),** "Anomaly Detection Using Artificial Neural Network" International Journal of Engineering Sciences & Emerging Technologies.
[6]. **Mehdi Moradi and Mohammad Zulkernine (2009),** "A Neural Network Based System for Intrusion Detection and Classification of Attacks".
[7]. **Mieso K Denko (2010),** "Detection and Prevention of Denial of Service Attacks in Mobile Adhoc Networks Using ReputationBased Incentive Scheme", Systemics, Cybernetics and Informatics, Vol. 3, No. 4.
[8]. **Przemyslaw Kukielka and Zbigniew Kotulski (2012),** "Adaptation of the neural networkbased IDS to new attacks detection".
[9]. **Przemyslaw Kukielka and Zbigniew Kotulski (2010),** "Analysis of Neural Networks Usage for Detection of a New Attack in IDS", Annales UMCS Informatica AI X, Vol. 1, pp. 51-59.
[10]. **S Devaraju and S Ramakrishnan (2012),** "Detection of Accuracy for Intrusion Detection System Using Neural Network Classifier", International Journal of Emerging Technology and Advanced Engineering (IJETAE).
[11]. **Samaneh Rastegari, M Iqbal Saripan and Mohd Fadlee A Rasid (2009),** "Detection of Denial of Service Attacks Against Domain Name System Using Neural Networks", IJCSI International Journal of Computer Science Issues, Vol. 6, No. 1.
[12]. **Sudhakar Parate, S M Nirkhi and R V Dharaskar (2013),** "Application of Neural Forensics for Detection of Web Attack Using Neural Network", National Conference on Innovative Paradigms in Engineering and Technology(NCIPET-2013).
[13]. **Tariq Ahamad and Abdullah Aljumah (2009),** "Hybrid Approach Using Intrusion Detection System", International Journal of Computer Networks and Communications Security, Vol. 2, No. 2, pp. 87-92.
[14]. **V Sivakumar1, T Yoganandh and R Mohan Das (2012)**, "Preventing Network From Intrusive Attack Using Artificial Neural Networks", International Journal of Engineering Research and Applications (IJERA), Vol. 2, No. 2, pp. 370-373.
[15]. **Zahra Moradi1 and Mohammad Teshnehlab (2011),** "Intrusion Detection Model in MANETs Using ANNs and ANFIS", International Conference on Telecommunication Technology and Applications, Singapore.