A Loom for Revealing Selfish and Malicious Node in Cluster Based Adhoc Wireless Networks

Shrikant V Sonekar
Department of CSE,
G.H.Raisoni College of Engineering,
Nagpur, M.S., INDIA
Email Id: srikantsonekar@gmail.com

Manali Kshirsagar
Department of CSE
G.H.Raisoni College of Engineering,
Nagpur, M.S., INDIA
Email Id: manali_kshirsagar@yahoo.com

Abstract- Now a day's one of the most interesting areas of research in wireless field is MANET. A Mobile Ad hoc Network (MANET) is a collection of nodes which are capable of communicating with each other through wireless links either directly or indirectly thorough routers. MANET is useful in so many crucial areas like in military application, disaster area etc. The nodes in the MANET can move anywhere in the network randomly. Due to its dynamic network topology it routing is a difficult task here. In present paper, we will see the method for detecting cluster head and malicious node then discuss how to overcome the problem of energy conservation. In next section the results and final section presents the conclusion and future scope.

Keywords- 2ACK, ALOHA, CH, MANET, SN, CSMA

NOMENCLATURE

2ACK- Two ways Acknowledgment
ALOHA- A Protocol use of Radio Transmission
CH- Terminology use for Cluster Head
MANET- Mobile Ad hoc Network
SN- Static Node
CSMA- Carrier Sense Multiple Access, a MAC Protocol which is use to sense the traffic.

I. INTRODUCTION

MANET is a technology for dynamic wireless networks, used in various applications like monitoring patient, business information sharing in the meeting, remote landscapes monitoring and emergency disaster relief in the areas after an earthquake. MANETs is a capable technology but it has certain features that are considered inclined, which leads to security weakness in this technology such as; lack of centralized management, resource availability, scalability, dynamic topology, limited power supply etc limitations. In MANET, all networking operations such as routing the message and forwarding the packet are performed by nodes themselves in a centralized manner. For these reasons, providing security to mobile ad -hoc network is very difficult task.

A Mobile Ad Hoc Network (MANET) is created by the nodes without any fixed infrastructure where all nodes are free to move about illogically and where all the nodes configure themselves. In MANET all nodes in the network act as a node and router.We need multiple access protocol when nodes are connected and used through a common link. Fig. 1 shows that there are three types of Multiple Access Protocol i.e. Random Access Protocol, Controlled Access Protocol and Channelization Protocols. Here we are using Aloha Protocol which is uses a very simple procedure called Multiple Access (MA). This method is improved by adding the procedure that sense the medium before transmission called as carrier sense multiple access (CSMA). The transport capacity of ALOHA is proportional to the square root of the density of mobiles which is very notable. Finally, this protocol is self-adapting to the node density and it does not require prior knowledge of the density. Aloha means "Hello". Fig 1 shows where Aloha comes under the multiple access protocol. The data link layer shows how the multiple terminals access the medium without interference or collision. ALOHA can be broadly divided into two types: Pure ALOHA and Slotted ALOHA. The actual ALOHA protocol is known as Pure ALOHA.
This method requires synchronization between the sending nodes to prevent collisions [1].

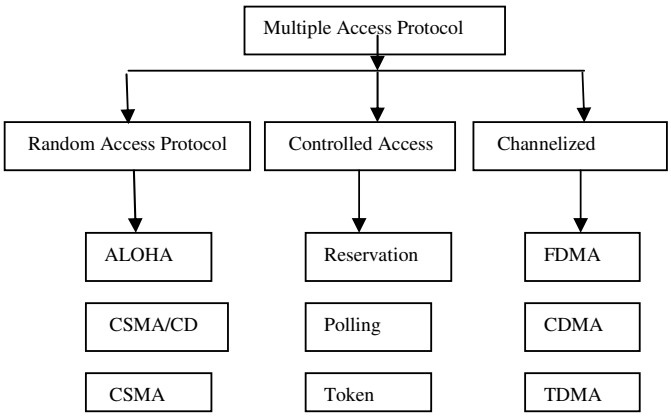

Fig.1. Organization of Multiple Accesses

It involves the station which sends a frame whenever it has a frame to send. There is an opportunity of collision between different stations. If more than one station tries to send the frame at a same time than collision occurs. The Slotted Aloha protocol divides the time interval into discrete slots and each slot interval corresponds to the time period of one frame.

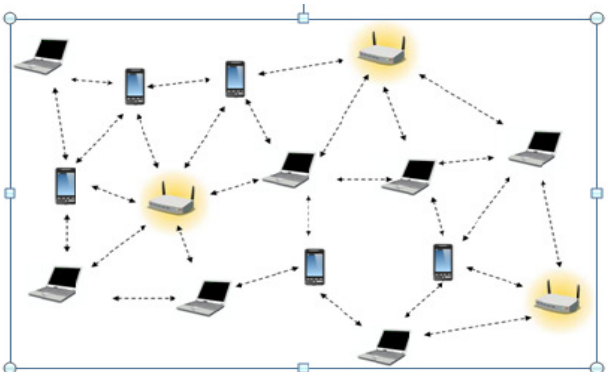

Fig.2. Mobile Ad hoc Network

Fig. 2 shows the actual working of MANET how the nodes communicate with each other in a network. In the above fig we can see the nodes as a combination of mobile devices and laptops. These devices are communicating with each other through gateway which is represented by yellow background node, the dotted arrow line shows the communication link in the network which is wireless.

II. LITERATURE SURVEY

The nodes can communicate directly if they are present in the radio range of each other otherwise an intermediate node is added in between the nodes to route i.e. the way of transmitting the packet in the network. Each of the nodes has a wireless interface to communicate with each other. Mobile Ad hoc Network (MANET) do not have any fixed infrastructure and consists of wireless nodes that move dynamically without any boundary restriction. MANETs are advantageous because they are quick to install, provide connectivity, fault tolerance and mobility [2]. In designing a MANET the following requirements should be met as far as possible:

- All nodes are mobile, thus the topology is changing over time. Multihop communication is required as the net is big for direct communication between every pair of nodes.
- The web is publicly accessible.
- No authorization is required so the unknown clients may be allowed to join the net.
- Nodes may consist of a wide range of devices with different resources.

Nodes are divided into different categorized depending on the use of the nodes as below:

1. Malevolent Nodes – Nodes that want to compromise the security of the MANET. Their actions are intended for some desired effect, but they are generally not lucid because they do not strive for their own benefit maximization.
2. Selfish Nodes – Nodes that do not forward other's packets, thus maximizing their benefit at the expense of all others.
3. Mistaken Nodes – These are nodes with incorrect hardware or software. They do not misbehave intentionally but if they mess up the working of the net, then they have to be treated just as malevolent or selfish nodes [9].

The selfish nodes are divided according to their behavior as follows:

1. Selfish Nodes Type 1 (SN1) - These nodes participate in route organization but refuse to forward data packets.
2. Selfish Nodes Type 2 (SN2) - These nodes participate in neither the route organization phase nor forward data packets. They use their energy only for transmitting their own packets.
3. Selfish Nodes Type 3 (SN3) – The behavior of such type of nodes depends on their energy levels. When the energy lies between full energy E and a threshold T, the node behaves properly. For an energy level between T and another lower threshold T1, it behaves like a node of type Selfish Node type 1 (SN1). Finally, for an energy level lower than T1, it behaves like a node of type Selfish Node type 2 (SN2). The relationship between T, T1, and E is $T1 < T < E$.

Now we will see the 2-ACK scheme, there is lots of work done by this scheme. To eliminate the packet dropping attack many schemes are proposed. 2-ACK scheme is actually worked, in between three hops. The message is send in the forward direction similarly the acknowledgement is received in the reverse direction [3].

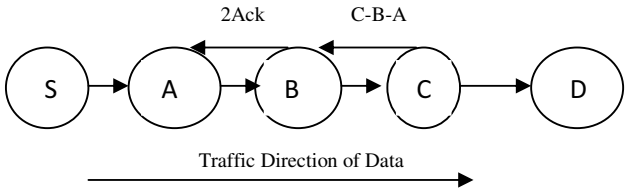

Fig. 3. 2-ACK Scheme

Fig. 3 shows the 2-ACK scheme which is based on sending the packet in a fixed route between two-hops in the opposite direction of the received data traffic path in the fixed route. In this scheme, each sender should maintain the parameters given below:

1. Identifier list which has been sent but no acknowledgement has been received yet for the same.

2. A measure for forwarded data packets and missed packets.

In MANET routing protocols are divided into three main classes; Proactive, reactive and hybrid protocols. In proactive routing, nodes use the tables for storing routing information, any changes in network topology need to be reflected by propagating updates throughout the network in order to maintain a reliable network vision. In Reactive protocol, packet searches the route in a demand way if the node wants to sends the packet to another node and creates a connection for transmission and receiving the packet. In Hybrid type of Protocol, it is a combination of both models i.e. reactive and proactive routing protocols [4].

We can classify the nodes into clusters, in cluster there will be one cluster Head who will communicate with each and every member in the cluster known as Cluster Member for maintaining the fairness in the cluster. Aloha method is used for simple communications in which each transmitter i.e source in a network sends data whenever there is a frame to send. If the frame successfully reaches the receiver i.e. destination the next frame is sent. If the frame has not been received successfully then it will be sent again [8].

Fig.4 shows the types of ALOHA i.e. Slotted ALOHA and Pure ALOHA.

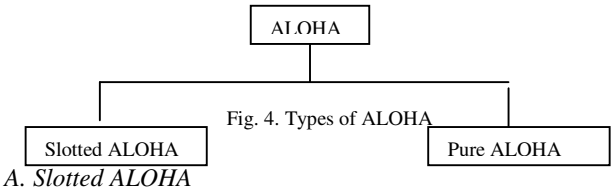

Fig. 4. Types of ALOHA

A. Slotted ALOHA

Slotted ALOHA was invented to improve the effectiveness of pure ALOHA because the collision in pure ALOHA are very high. The time of the shared channel is divided into discrete intervals called slots. The stations can send a frame only at the beginning of the slot and only one frame is sent in each slot. In slotted ALOHA, if any station is not able to place the frame onto the channel at the beginning of the slot *i.e.* it misses the time slot then the station has to wait until the beginning of the next time slot [7]. Aloha works properly in wireless broadcast system. If the communications volume is bulky, the collision problems become difficult. The result is degradation of system efficiency, because when two frames collide, the data contained in both frames is lost [5]. To reduce the rate of collision, network efficiency gets optimized and the user of the network increases, such scheme is called as slotted Aloha. More improvement is done by a more complicated protocol called Carrier Sense Multiple Access with Collision Detection (CSMA/CD).

B. Pure ALOHA

In Pure ALOHA, the stations transmit frames whenever they have data to send. When more stations transmit simultaneously, there is collision and the frames are destroyed. In this type of ALOHA, acknowledgement is expected when any station transmits a frame. If no acknowledgement is received within specified time period, the station assumes that the frame has been destroyed. If frame destroyed then the waiting time must be random otherwise same frames will collide repeatedly. If two frames try to use the same frame at same time then there will be a collision at same time [6].

ALOHA protocol uses a simple logic which says that if any node is having a packet to send then just send the packet to the destination. If any collision occurs in between the packet transmission then it will resend the packet again after some time.

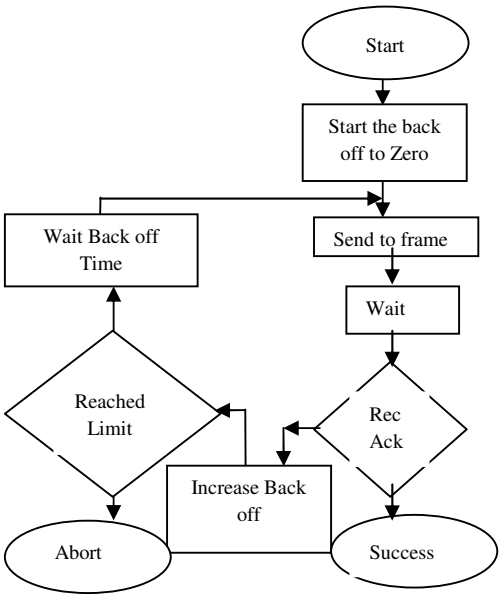

Fig. 5. Protocol Flowchart of ALOHA

Fig. 5, shows the flow chart of the ALOHA protocol which shows the procedure of forwarding the message. Initially the protocol will send the frame it will wait till it reaches the destination if it will not send the acknowledgement after reaching to the destination in a particular time then only we can decide that the frame is reached to its place successfully or not [10].

Cluster Head selection is also an important technique in MANET. So many algorithms are used in Cluster Head selection like Identification Based Clustering, Connectivity based clustering, Mobility aware clustering etc.

III. ALGORITHM

In Coordinates Based Algorithm, Malicious node will move from one cluster to another cluster. Once the malicious node enters into some other cluster then the cluster head of the new cluster will not send any information to the malicious node as the ID of the malicious node is send by its own cluster head to all other Cluster Heads present in the network. This will reduce the packet dropping problem in the network

Steps of Coordinate Based Algorithm for Malicious Node Movement

Step 1: Begin.
Step 2: Select the No of Nodes in the Cluster.
Step 3: Message will be send to Static Node (SN) if control is on server.
Step 4: Define X, Y and ID variables for each node.
Step 5: Cluster Head (CH) will get elected and message will get sent to the Cluster Members (CM) if message is received by Cluster Head (CH).
Step 6: Once Cluster Member receives message from Cluster Head they will send acknowledgement to CH.
Step 7: When CH receives "ACK" from CM, then it sends each "ACK" packet to SN.
Step 8: Once Static Node (SN) receives ACK packet then it will send ACK packet to server.
Step 9: When server receives the Acknowledgement packet it will send the message again.
Step 10: This process will repeat till the malicious node will not become the normal node.
Step 11: When cluster head receives "ME_MALICIOUS" packet from malicious node, it sends "NODATA" packet to malicious node.
Step 12: Cluster head will broadcast the malicious node address to all other Cluster head in the network.
Step 13: When node starts behaving normally.
Step 14: Stop.

In our research work, communication takes place according to 2Ack based in which the communication is in between server, Static Node and the Cluster Head. Initially Initialization Method is called and then communication takes place between the cluster members. In Coordinate based algorithm, malicious node moves in a square fashion in the network from one cluster to another cluster. Once the malicious node returns back to its own cluster it will become the normal node.

Steps of Cluster Head Election Algorithm

Step 1: Begin.
Step 2: For every member in the cluster.
Step 3: Calculate the distance using x and y variables with other clusters and ID.
Step4: If ID is smallest and it is closer to maximum number of nodes i.e having highest connectivity with other nodes in the cluster.
Step 5: Repeat step 3 to 4.
Step 6: Finally we will get the elected Cluster Head with minimum ID and max Connectivity.
Step 7: Stop.

In both algorithms i.e. Cluster Head (CH) election algorithm and malicious node movement algorithm we can see the parameters for deciding the threshold value through which we can identify that whether the node will be selected as Cluster Head and Malicious node respectively. Mathematical equations are drawn on the bases of algorithm as below:

$$\text{Efficiency} = 1/(\text{Memutilization}*\text{CPUUtilization}*\text{time}) \quad (1)$$

Equation 1 shows that if CPU utilization, memory Utilization and time is less than the efficiency is high. We can say that the efficiency is inversely proportional to CPU Utilization, Memory Utilization and time. For Cluster Head Election Algorithm we are finding the type of node whose ID number is smallest and having the highest connectivity with the cluster members in the cluster.

$$CH = \begin{cases} ID = \min(a,b) = a \text{ if } b > a \\ \text{otherwise } \min(a,b) = b \text{ if } a > b \\ Conn = \max(a,b) = a \text{ if } a > b \\ \text{otherwise } \max(a,b) = b \text{ if } b > a \end{cases} \quad (2)$$

Equation 2 shows the two major parameters for electing Cluster Head i.e. Lowest ID and Highest Connectivity which represents the variables a and b. Variable a represents the single node and b represents the remaining nodes in the cluster. So from the above equation we can find out that if the node is of smallest ID will be selected as Cluster Head if it is having the highest connectivity with other nodes in the network.

IV. SIMULATION AND RESULTS

On the bases of the algorithm few results have been discovered.

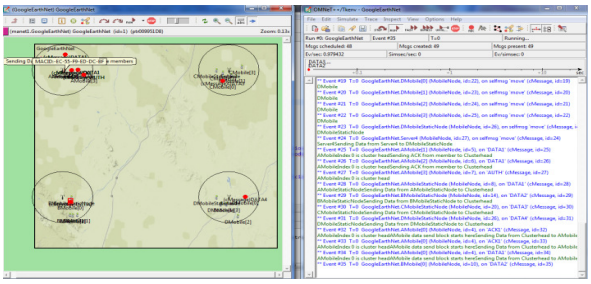

Fig. 6.Snapshot of Cluster Head Election

The Cluster Head will be selected using the algorithm of Cluster Head Election. Fig 6 shows, the red dot of the Cluster head is selected by the Election of Cluster Head Algorithm. The static window in the right hand side of the snapshot shows the steps of cluster head selection in which the distance of neighbor is calculated by every node. The node that is having the highest connectivity and lowest ID will be selected as a Cluster Head. After selected as Cluster head it will send the MAC address to other Cluster heads in the network.

Initialization of parameters is done at the beginning. The node that crosses the threshold value of the respective parameter then the node may be malicious. But the node will be declared as malicious only when that node will check few more parameters because the node which is not forwarding the packet may be because of the network congestion. When it will not receive the message then the problem of congestion is avoided.

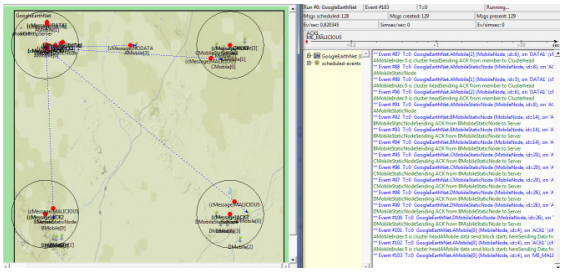

Fig. 7. Detection of Malicious Node and CH Communication to other CH's

Fig. 7 shows the malicious node i.e. mobile 3 in cluster A as shown in the above snapshot.

TABLE I. SIMULATION PARAMETER

Parameters	Values
Simulation Tool	OMNet++
Number of Nodes	25
Size of Network	500*400
Speed of Nodes	0-10 m/sec
Transmission Range	100 m
Battery Power of Node	100 Unit
Pause Time	0-20 Sec

TABLE II. FINDING CLUSTER HEADS AND CLUSTER MEMBERS

Number of Nodes	Cluster Head	Cluster Members
04	3	1,2,4
08	6	1,2,3,4,5,7,8
12	2	1,3,4,5,6,7,8,9,10,11,12

The Tables I and II shows all network nodes that are involved in clsuter and the node that are isolated with the network. Fig 8 shows the No of Nodes on X axis and Transmission range on Y Axis, the behaviour of the graph shows that the transmission range of node increases gradually

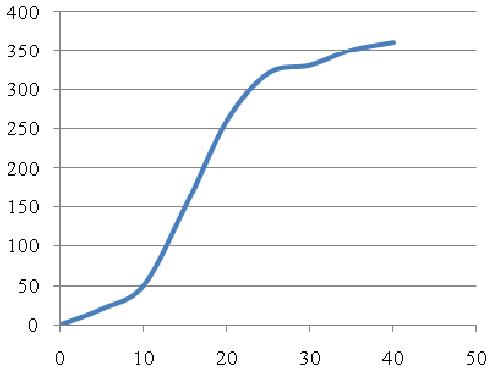

Fig. 8.No of Nodes Vs Transmission Range

The most important parameter used for finding the route is the transmission range of the node. Node who is in the middle of the cluster can transmit the packet for long time. So, that node will be declared as a cluster head of the network. Aloha Protocol is used for transmitting packets because its transmission range is better than any other protocol.

TABLE III. FINDING CLUSTER HEADS AND CLUSTER MEMBERS

Name of Cluster	Number of Nodes	Cluster Head
Cluster 1	4	2
Cluster 1	8	4
Cluster 1	12	6
Cluster 2	4	1
Cluster 2	8	7
Cluster 2	12	9
Cluster 3	4	2
Cluster 3	8	6
Cluster 3	12	8
Cluster 4	4	3
Cluster 4	8	5
Cluster 4	12	4

Table III shows all network nodes that are involved in clsuter and the node that are isolated with the network.

Graphical Representation of Result

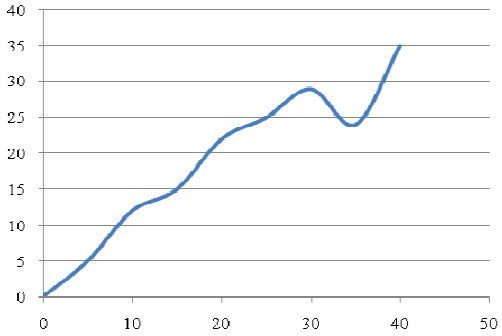

Fig.9. Graph between No of Nodes Vs Speed

The above graph shows the behaviour in which the energy of the node chnages with time. As time increases the energy will lose gradually. The behaviour of the nodes shows the fall and then increase in the graph which shows the gain of energy from server once lose it in forwarding the packet.

In Fig. 10 shows the energy conservation graph in the network. Energy on X axis and time on Y axis..

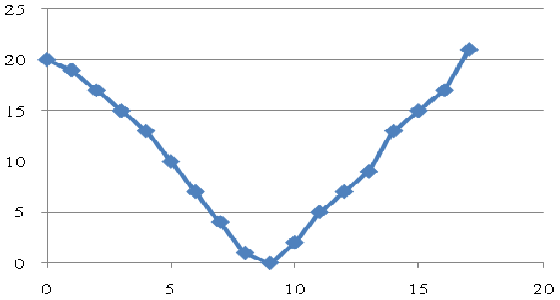

Fig. 10. Graph between Energy Vs Time

TABLE IV. COMPARISON BETWEEN EXISTING AND PROPOSED ALGORITHM

Parameters	K Hop Connectivity (KCONID)	Lowest ID (LID)	Weighted Cluster Algorithm (WCA)	Election of CH (ECH)
	Existing Algorithm			Proposed Algorithm
Broadcast	Yes	No	No	Yes
Throughput	No	Yes	Yes	Yes
Location	Yes	No	Yes	Yes
Energy	Yes	No	Yes	Yes

Table IV shows the comparison done on the bases of Broadcast Throughput, Location, Energy and. In the algorithm we can see the performances of all algorithms. The proposed algorithm is a combination of highest connectivity and lowest ID. We can see that the proposed algorithm is stable as compare to other algorithms.

V. CONCLUSION AND FUTURE SCOPE

We have explored all the prevention and detection mechanisms in our project. We categorized them into the categories according to their aim and their specific strategies. A comparative study between them was then conducted to show the effectiveness of the system. Apart from election and detection of Cluster Head and Malicious node respectively we have seen the energy conservation problem in the network. For which we have concluded that the energy is neither be created nor be destroyed it will remain present in the network in some form. Cluster Head will gain energy from server once it will lose its energy in the network. In future, we can enhance the system by adding some more algorithms according to the existing algorithms. We can implement the system for malicious and selfish node for some other behavior of the Mobile Ad hoc Network.

ACKNOWLEDGMENT

We would like to thank the anonymous reviewers for valuable comments and suggestions.

REFERENCES

[1] Anshul Chaturvedi, “Impact of Malicious node in MANET”, International Journal of Computer Applications, (0975 – 8887) 2013.

[2] Dang,Packel,Thomas,”On the Selection of Cluster Head in MANET’s”, IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 2, March 2011.

[3] N.Radhika,Thejiya,”Trust Based Solution for Mobile Adhoc Network”,International Journal of Advance Research in Computer Science and Software Engineering,Volume 4 Issue 5, May 2014.

[4] Priyanka,Mukesh Dalal,”Security in MANET: Effective value based Malicious node detection and removal scheme”, International Journal of Advance Research in Computer Science and Software Engineering,Volume 4 Issue 5, May 2014.

[5] M.A. Rizvi,”Issues and challenges in Energy Aware Algorithms using clusters in MANET”, International Journal of computing communication and networking,Volume 2 April –June 13.

[6] A.Rajaram,S.Palanswami,,”Malicious Node Detection system for Mobile Adhoc Network”, (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 1 (2) , 2010, 77-85.

[7] Pravin Gosekar,Girish Katkar,Pradep Gorpade,”Mobile Adhoc Networking: Imperatives and challenges”,IJCA special Issue on MANET 2010.

[8] Poonam Thakur,Vinaya Raju,”Survey on Routing Techniques for MANETS and Wireless Sensor networks: A Comparision,”,International Journal of Computer Engineering and Technology, Volume 4 Issue 1 January 2013.

[9] Vivek Richariya, Pravin Kaushik,”A Survey on Network Attack in Mobile Adhoc Network”, International Journal of Advance Research in Computer Science and Software Engineering, Volume 4 Issue 5, May 2014.

[10] Aditi Kumar, Praveen Thakur, “Routing Attack and their Counter Strategies in MANET”,International Journal of Advance Research in Computer Science and Software Engineering, Volume 4 Issue 5, May 2014.