Volume 4, Issue 7, July 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

# A Pragmatic Observation for the Detection of Selfish and Malicious Nodes in Ad-hoc Wireless Networks

**Bhakti Thakre**
Research Scholar, Department of CSE,
J D College of Engineering and Management,
Nagpur, India

**S. V. Sonekar**
Professor, Head of Department, Department of CSE
J D College of Engineering and Management,
Nagpur, India

***Abstract- A mobile Ad hoc network (MANETs) are networks composed of a set of communicating devices which are able to spontaneously interconnect without any preexisting infrastructure. Devices in the range can communicate in point to point fashion. Still there are some problems in MANET about security and privacy, especially when used in sensitive areas of computing. Secure routing protocols have been developed to provide various levels of security and privacy in the past.***

***In some cases the nodes refuses to share its resources with other nodes for its own benefits are called selfish and misbehavior node. Due to these nodes in MANET performance of the network gets affected like drooping of packets in the network. In this paper we will walk through some algorithms which will provide secure routing and can also help in improving the network throughput.***

***Keywords- Cluster Head (CH), MANET, Multiple Access (MA), Malicious Node, Node Misbehavior, OMNeT++.***

## I. INTRODUCTION

The Mobile Adhoc Wireless Network (MANET), had been deployed in military since 1970s, and thereafter it had been applied in various applications such as airplane exhaustion breakage supervision, business associates sharing information during a meeting; attendees using laptop computers to participate in an interactive conference, remote landscapes monitoring, and emergency disaster relief personnel coordinating efforts after an earthquake and monitoring the patients [1]. Adhoc means arranging or happening whenever necessary and not planned in advance. Some nodes decides to not cooperate with other nodes in the network and simply aim to save its resources to the maximum while using the network to forward its own packet these types of nodes are called as selfish nodes while malicious nodes are the nodes who participate in the route discovery and maintenance process but refuse to forward data packet.

When nodes are connected and use a common link then we need multiple access protocol. There are three types of Multiple Access Protocol i.e. Random Access Protocol, Controlled Access Protocol and Channelization Protocols. In our project we are using Aloha Protocol which uses a 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 (CDMA). This method is evolved by two another methods simultaneously i.e. carrier sense multiple access with collision avoidance (CDMA/CA) and Carrier senses multiple access with collision detection (CDMA/CD).

There are two types of ALOHA: Pure ALOHA and Slotted ALOHA. The original ALOHA protocol is known as Pure ALOHA. The idea behind the concept involves station sends a frame whenever it has a frame to send. There is a possibility of collision between different stations. If more than one station tries to send the frames at a same time than collision occurs.

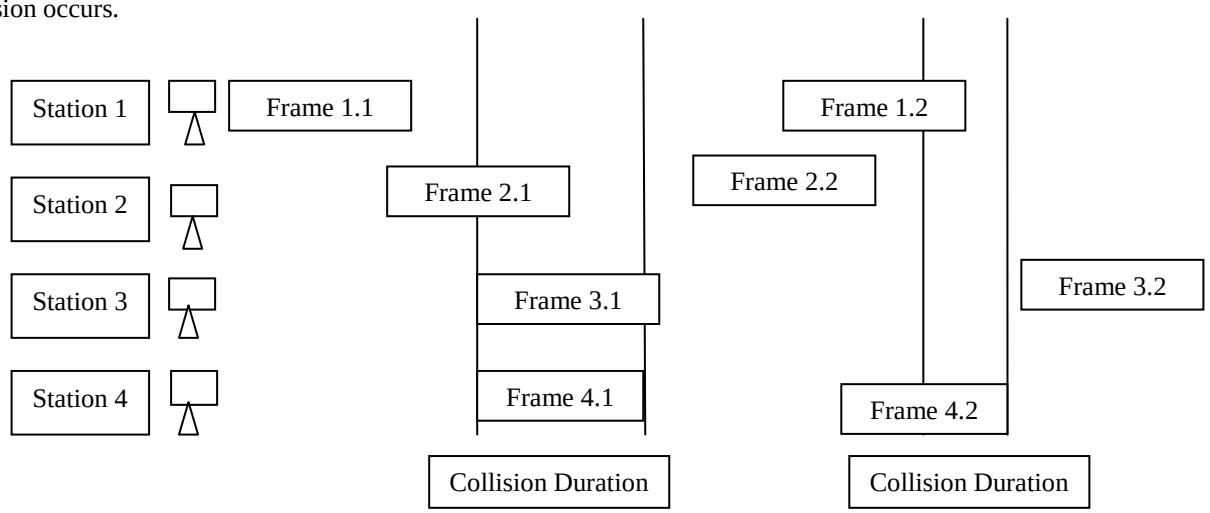


Fig. 1 Frames in Pure ALOHA Network. [10]

 

In Fig. 1, we can see four stations that are sending frames whenever they have any frame to send. Only two frames survive: one from station 1 and another frame from station 3. Even if one bit of a frame coexists on the channel with one bit from another frame, there is a collision and both will be destroyed. Pure ALOHA Protocol relies on acknowledgement from the receiver. When station sends a frame it expects an acknowledgement from the receiver.

In mobile ad hoc networks (MANETs), nodes usually cooperate and forward each other's packets in order to enable out of range communication. However, in hostile environments, some nodes may deny to do so, either for saving their own resources or for intentionally disrupting regular communications. This type of misbehaviour is generally referred to as packet dropping attack or black hole attack, which is considered as one of the most destructive attacks that leads to the network collapse.

Delivery and dynamic capability to handle dynamic connectivity are the important issues in the routing protocols in wireless communication. Packet or message moves from source to destination. There are different types of communications in MANET: Unicasting, Broadcasting, Multicasting and Anycasting.

1. Unicasting: Transmission between one to one nodes.
2. Broadcasting: Transmission is send by one node but received by all the nodes connected in the network.
3. Multicasting: Multicasting is different from Uni casting. In transmission there will be more than one node and send to the set of nodes.
4. Anycasting: It is a communication between single senders and several receivers which is nearest to the group in the topology.

Clustering is the collection of objects which are similar between them and are dissimilar to the objects belonging to other clusters. Clustering is used in earthquake studies, marketing etc. In networking, Clustering is the approach to reduce traffic during the routing process. The goal of clustering is to achieve scalability in presence of large network and scalability. The nodes in the clusters play the roles of Cluster Head, Member Node, Guest Node etc [3].

Mobile Ad Hoc Network (MANET) can be described as an autonomous collection of mobile nodes (users) that communicate over relatively low capacity wireless links, without a centralized infrastructure. In these networks, nodal mobility and the wireless communication links may lead to dynamically changing and highly unpredictable topologies. All network functions such as routing, multi-hop packet delivery and mobility management have to be performed by the member nodes themselves, either individually or collectively[4].

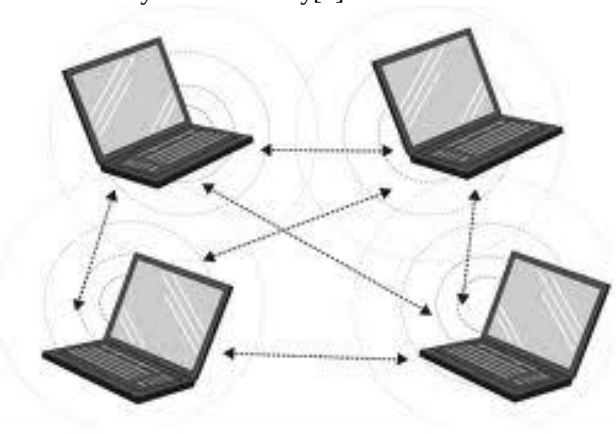

Fig. 2 Mobile Adhoc Networks

Consider the above Fig. 2, We can see that nodes are connected with each other in a wireless network. So every device in Manet is free to enter in and move from the network. Due to the dynamic nature it is vulnerable to any kind of attack. If the intermediate node does not transmit the packet to next node or sending acknowledgement to one node for so many times then that node will be the malicious node.

This paper is organized as follows: review of previous work in Section 2, In Section 3, we describe algorithm in detail and then explain the malicious node movement in the network. In Section 4, we provide Simulation Results; Section 5 concludes the paper with their future scope.

## II. LITERATURE SURVEY

Mobile Ad hoc Network (MANET) do not have any fixed infrastructure and consists of wireless nodes that move dynamically without any boundary limitation. MANETs are advantageous because they are quick to install, provide fault tolerance, connectivity and mobility [5].

By classifying nodes into clusters, the proposed scheme allows each Cluster Head (CH) to detect false accusation by a Cluster Member (CM) within the cluster. Node clustering provides a means to mitigate false accusations [5]. The mobile nodes that are in the communication range or radio range of each other can directly communicate, whereas others need the aid of intermediate nodes to route their packets. Each of the nodes has a wireless interface to communicate with each other.

 

In Fig 3 we can see that how clusters are constructed in the proposed scheme. While each cluster consists of one CH and CMs lying within the CH's transmission range, some nodes within the transmission area of the CH might not be the member of the cluster and can be the CM of another cluster. There are four clusters having their own Cluster Head (CH). If one of the nodes in cluster A is malicious i.e. as shown in figure 3 above, the node with red color, then Cluster Head of Cluster A will send information to all other cluster Heads of B,C and D Clusters that the node with particular ID is malicious and don't send any information to the node.

Algorithms used in Cluster Head election involve so many algorithms like Identification Based Clustering, Connectivity based clustering, Mobility aware clustering etc [8]. In our project we will implement the connectivity based clustering in which the node with highest connectivity nodes will be selected as a Cluster head for the cluster.

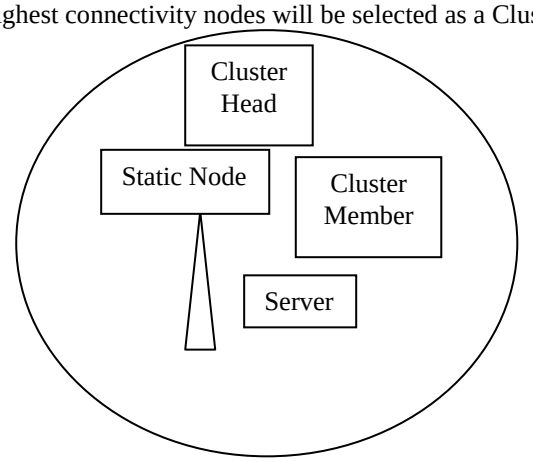


Fig. 3 Node Clustering

In fig. 3, we can see the cluster having Server, Cluster Head, Static Node and Cluster Member. In our project there will be four similar clusters which are having their own components in the cluster. There will be only one cluster head in the cluster. Cluster Head will communicate with other Cluster Heads about the information about the malicious node.

In this proposed scheme, every node in the network monitors the behavior of its neighbors, and if any abnormal action is detected, it invokes an algorithm to determine whether the node is malicious or selfish. The node that is malicious must not be the cluster head because cluster head of any cluster is the main member of any cluster who communicates with other clusters in the network.

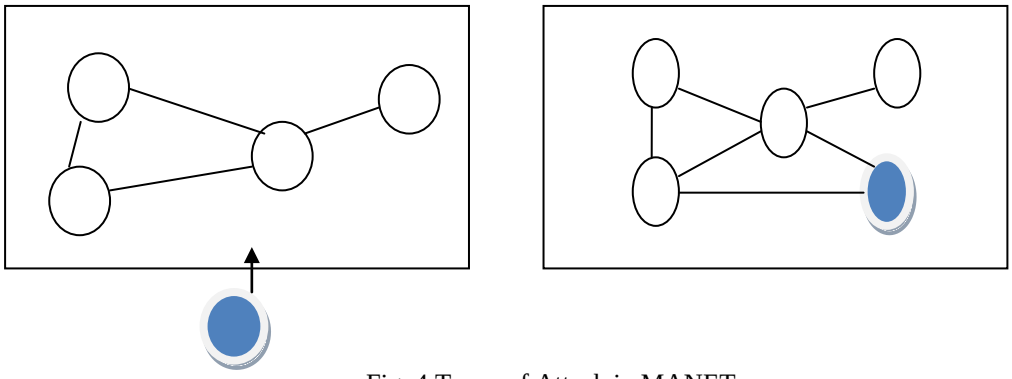

Fig. 4 Types of Attack in MANET

In shown in Fig 4, there are two types of attack in MANET i.e. External and Internal Attack. In External Attack, an attackers are from outside the network (shown with blue color node) tries to get access to the current network. Once it will become the part of the network then it will start interrupting the ongoing transmission and performance of whole network. External Attack can be prevented by implementing firewall, where the access of unauthorized person can be avoided in the network [7].

In Internal Attack, an attacker node is already present in the network and also contributes in normal network activity. After some transmission it starts its misbehaving behavior. So, Internal Attack is more rigorous than External Attack[2].

Ad-Hoc network routing protocols are commonly divided into three main classes; Proactive, reactive and hybrid protocols. In proactive routing, each node has to maintain one or more tables to store routing information, and any changes in network topology need to be reflected by propagating updates throughout the network in order to maintain a consistent network view. In Reactive Protocols, Reactive routing is also known as on-demand routing protocol since they do not maintain routing information or routing activity at the network nodes if there is no communication [9].

If a node wants to send a packet to another node then this protocol searches for the route in an on-demand manner and establishes the connection in order to transmit and receive the packet. In Hybrid Protocols, a hybrid model that combines reactive and proactive routing protocols [6].

 

## III. ALGORITHMS

In Movement Algorithm, Malicious node will move from one cluster to another cluster. The basic idea behind this algorithm is the movement of malicious nodes in the network. When a defected or malicious node enters into its neibhour cluster then the cluster head of the main cluster will inform all other cluster heads about the ID of malicious node in the network. This will reduce the packet dropping problem in the network by avoiding forwarding any message to the defected node in the network.

### *A. Cluster Head Election*

Step 1: Start.
Step 2: For each Member nodes in the cluster
Step 3: Check whether the node is malicious or not.
Step 4: If node is not malicious then calculate the distance to other cluster and ID.
Step 5: If ID is minimum and it is closer to more nodes then make it cluster head
Step 6: Repeat step 2 to 5 for every node.
Step 7: Finally we will have a cluster head with min ID and distance to all members.
Step 8: Stop.

Cluster Head of each cluster is responsible for the communication between the clusters. Cluster head is selected on the bases of connectivity of the member nodes of the clusters. The node with highest connectivity will be selected as a Cluster Head of the Cluster. The above discuss Algorithms will improve the performance of the system by avoiding to forward the data packets to the node which is malicious.

### *B. Malicious Node Movement Algorithm:*

Step 1: Start.
Step 2: When control is on Server it sends a message to static node, once receive it will send message to cluster head.
Step 3: Cluster Head for each cluster is selected using the Connectivity Algorithm.
Step 4: Once Cluster Head receives packet from static node, it broadcasts the packet among cluster members.
Step 5: When Cluster head sends message to other cluster members in the cluster, they send acknowledgement packet to Cluster Head indicating that the message is received.
Step 6: Once Cluster Head receives acknowledgement packet from cluster members, then acknowledgement packet is send to the static node i.e. server.
Step 8: When static node receives acknowledgement packet, in return it sends an acknowledgement packet to server.
Step 9: When server receives an acknowledgement packet, then it will send data packet again and it continues.
Step 10: Repeat the same procedure till the malicious node doesn't become normal node.
Step 11: The node which is selected as a malicious will send the message to the nodes that the node is malicious like "ME_MALICIOUS" packet to the Cluster Head which is nearer to the Cluster.
Step 12: Once Cluster Head receives the message like "ME_MALICIOUS" packet then it will send NODATA packet to the malicious node which shows that the node is identified as malicious and do not send any data to it.
Step 13: Cluster Head sends the message to all Cluster Heads that the node is malicious.
Step 14: The malicious node start moving from its own cluster and move in a particular direction in the network. Once return in its own cluster again start behaving like a normal node.
Step 15: Stop.

In the project, Communication takes place according to 2 Ack based in which the communication is in between server, Static Node and the Cluster Head. Initially Initialization Method of all components is called and then communication takes place between the cluster members. In Coordinate based algorithm, malicious node moves in such a way that it covers all the clusters of the network and return to its original cluster as a normal node .After the movement of one node in a cluster a random node is selected as a malicious node and same will happens with this node as a malicious.

## IV. SIMULATION BASED RESULTS

This section describes the working and performance of the algorithm through the OMNeT++ Simulator. In this paper we proposed, a better solution for energy saving process by improving quality in selection of nodes which are best fitted for routing in between wireless nodes. 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 1: SIMULATION PARAMETER

| Meaning | Values |
|---|---|
| Simulation Tool | OMNet++ |
| Number of Nodes | 50 |
| Size of Network | 600*400 |
| Speed of Nodes | 0-15 m/sec |
| Transmission Range | 10-250 m |
| Simulation Time | 300 sec |
| Pause Time | 0-30 Sec |

 

TABLE 2: FINDING CLUSTER HEADS AND CLUSTER MEMBERS

| Name of Cluster | Number of Nodes | Cluster Head |
|---|---|---|
| Cluster 1 | 4 | 1 |
| Cluster 1 | 8 | 6 |
| Cluster 1 | 12 | 10 |
| Cluster 2 | 4 | 3 |
| Cluster 2 | 8 | 5 |
| Cluster 2 | 12 | 9 |
| Cluster 3 | 4 | 3 |
| Cluster 3 | 8 | 6 |
| Cluster 3 | 12 | 5 |
| Cluster 4 | 4 | 2 |
| Cluster 4 | 8 | 7 |
| Cluster 4 | 12 | 8 |

The Table 1,2 shows all network nodes that are involved in clsuter and the node that are isolated with the network. In Fig 5, time is on X axis and Throuput on Y Axis , Throught is defined as a rate of succeful message delivery over a communication channel. Througput is generaly measure in bits per second In fig 5 blue bars are result of our algorithm and red bars represent the result of AODV. The graph shows the sending througput for TCP packet. In time interval 200-250 maximum amount of TCP packets has been deliveredfrom souse to destination in respect to our algorithm because it is a proactive type routing protocolwho have no delay to find out the route from source to destination as the path becomes available immediately to them. The performance of proposed algorithm is changes according to the network in the fig 5.

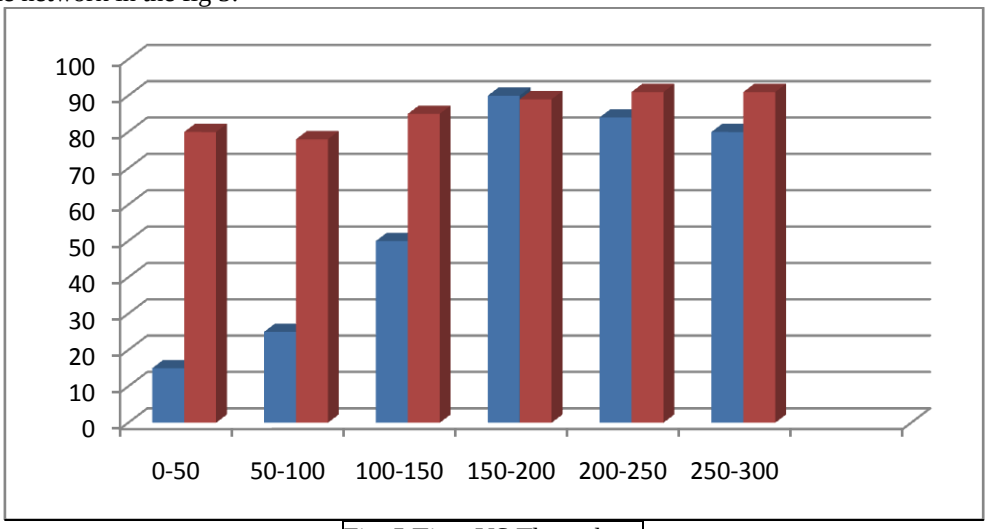


Fig. 5 Time VS Throughput

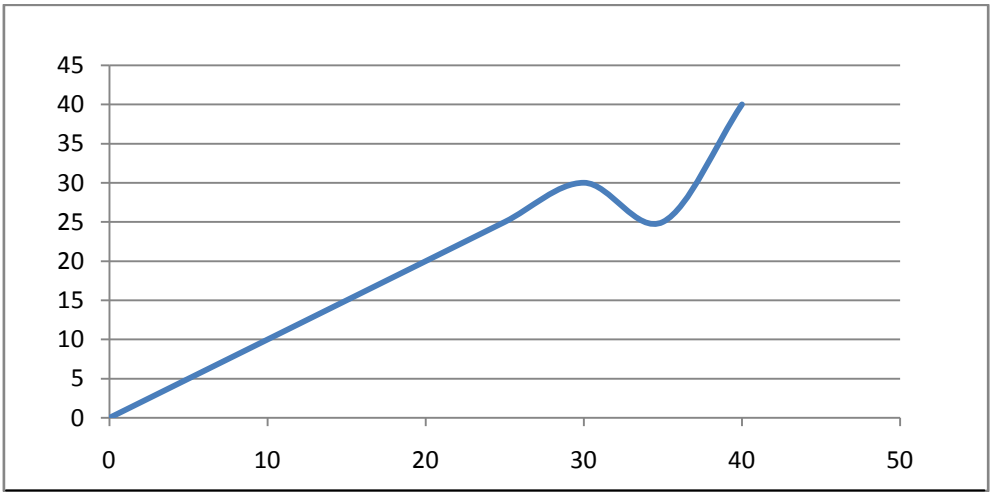


Fig. 6 Graph between No of Nodes Vs Speed

In Fig.6 , graph shows the No of Nodes (Mobiles) on X axis and Speed on Y axis. Speed of Node is defined as a time in which node moves from one location to another location. As soon as mobile node arrives at a selected destination.

 

In Fig.7 , graphs shows the No of nodes on X Axis and Packet Dilivery Ratio on Y Axis, Packet Delivery Ration represent the range in which the nodes are sending packets to another node . The below graph shows the packet delivery ratio of the system in the network on Omnetpp simulator.

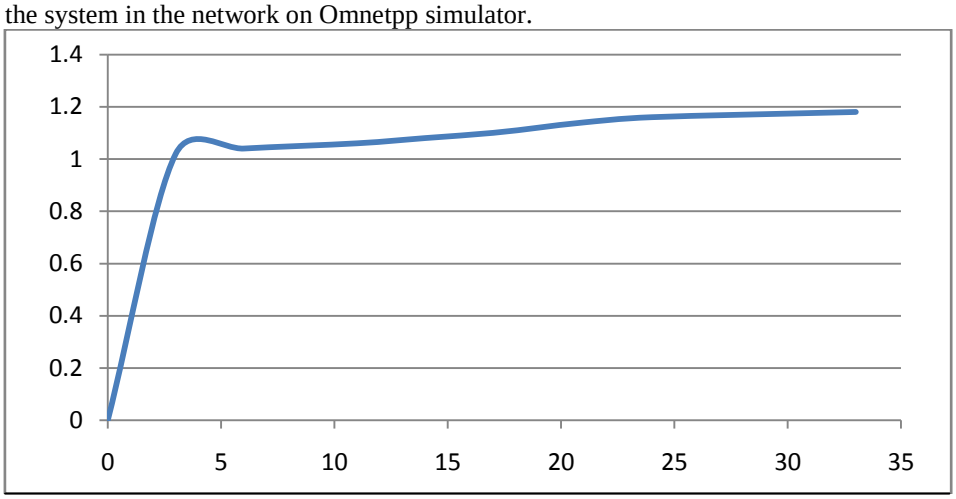


Fig. 7 Graph between No of Nodes Vs Packet Delivery ratio

In Fig.8 shows No of nodes on X axis and packet dropping ratio on Y axis. Packet Dropping Ratio represents the amount of message dropped while travelling from one node to another across a network. Packet dropping is one of the major problems in the network. If more than one message has been send through same channel at a same time then collision may occur. Due to this problem some nodes may drop the packets or few of them drop the packets intentionally. The graph below show the ratio of packet dropped due to malicious nodes in the network.

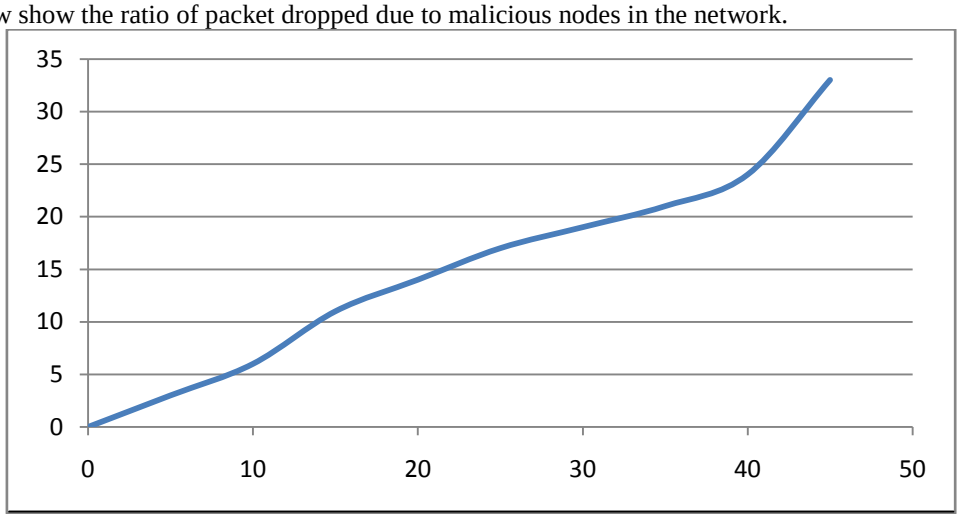


Fig. 8 Graph between No of Nodes Vs Packet Dropped Ratio

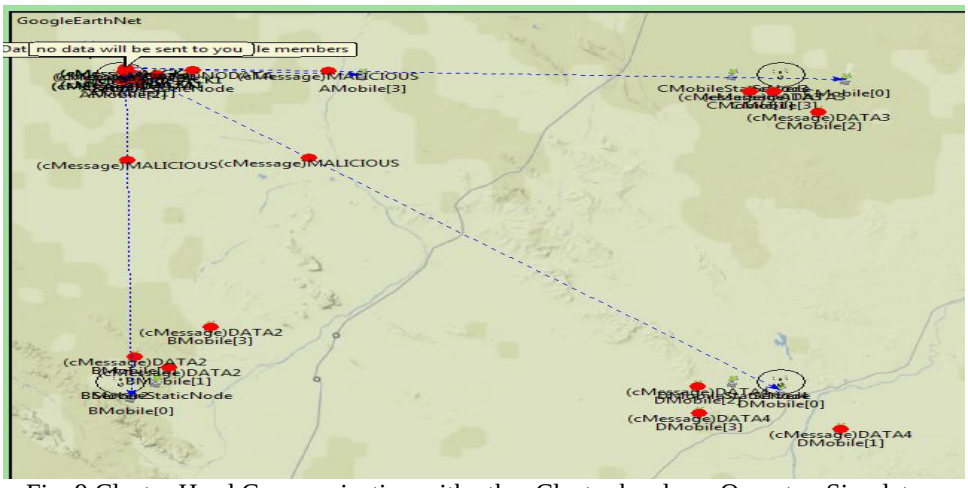


Fig. 9 Cluster Head Communication with other Cluster heads on Omnetpp Simulator.

The Fig. 9 shows the snapshot of our on Omnetpp Simulator which shows the communication between cluster heads through the blue dotted line. The line in the snapshot shows that once the malicious node is detected then the information about the malicious node will be send to other Cluster Heads in the network.

 

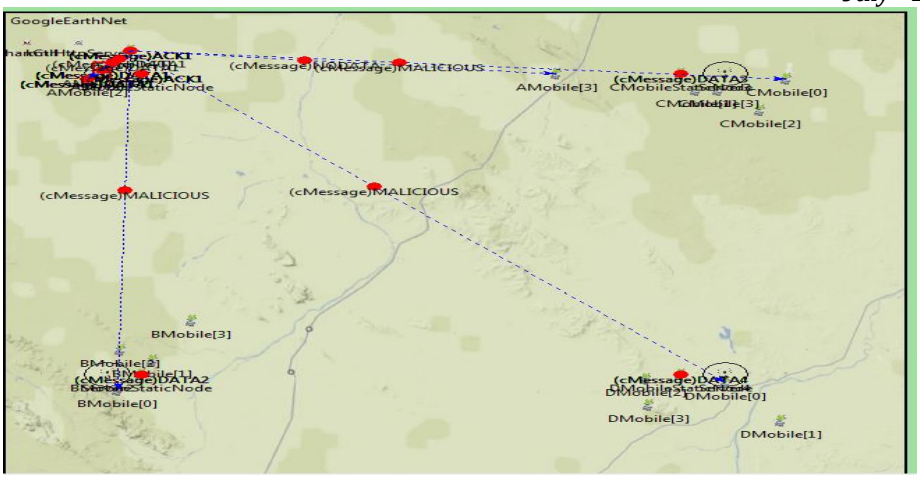


Fig. 10 Cluster Head Communication and movement of malicious node from cluster A to Cluster C on Omnetpp imulator.

In Fig. 10 we can see the movement of malicious node from Cluster A to Cluster C i.e. square movement of the defected node. Cluster A is sending information to remaining Cluster Heads in the network that the malicious node is detected. The Malicious node will move from Cluster A to C to D to B. Once complete the movement then again returns back to its original cluster and behave like a normal node and start sending packets and sending acknowledgement normally. Movement of malicious node ( AMobile with index 3 in this scenario) from Cluster A to Cluster C. When AMobile with index 3 who is malicious enters into the range of Cluster C, then the Cluster Head of Cluster C will pop up the message like " Malicious node don't send message to this node".

## V. CONCLUSION

A comparative study between them was then conducted to highlight their respective effectiveness and limitations. Prevention, detection and reaction mechanisms have been explored. We concluded that most of the proposed schemes in the first, second or third defense line are based upon certain assumptions that are not always valid due to the dynamic nature of MANETs and their specific characteristics.

In this paper, investigation is done on the misbehavior of nodes and a new approach is proposed for the detection of misbehaving nodes while moving in the network from one cluster to another cluster. Suggested approach can be united on top of any source routing protocol such as ALOHA and is based on sending acknowledgement packets for reception of data packets and using promiscuous mode for counting the number of data packet such that it overcomes the problem of misbehaving nodes.

## REFERENCES

[1] Nada M. Badr1 and Noureldien A. Noureldien , "*Review of mobile ad hoc networks security attacks and countermeasures*", International journal of computer engineering & Technology 2013.

[2] François Baccelli, Bartłomiej Błaszczyszyn, and Paul Mühlethaler, "*An Aloha Protocol for Multihop Mobile Wireless Networks*," IEEE transactions on information theory, vol. 52, no. 2, february 2006

[3] Prof. Shalini V. Wankhade," *2ACK-Scheme: Routing Misbehavior Detection in MANETs Using OLSR*", July 2012.

[4] Abhilash Sharma and Birinder Singh, "*Fault Tolerance with Clustering Approach in Ad-Hoc on Demand Protocol*", International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 Vol. 2 Issue 9, September – 2013.

[5] Namrata Marium Chacko, Getzi P. Leelaipushpam, "*A Reactive Protocol For Privacy Preserving Using Location Based Routing In Manets*", IJCSN International Journal of Computer Science and Network, Vol 2, Issue 2, April 2013

[6] Aarti , Dr. S. S. Tyagi " *Study of MANET: Characteristics, Challenges, Application and Security Attacks* " , International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 5, May 2013

[7] Ms.T.R.Panke, "*Clustering Based Certificate Revocation Scheme for Malicious node in MANET* ", International Journal of Scientific and Research Publications, Volume 3, Issue 5, May 2013.

[8] Manoj V. Mori1, G.B. Jethava,"*Node registration in MANET*", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) Volume 2, Issue 1 January - February 2013.

[9] Aravindh S, Vinoth R S and Vijayan R, "*A Trust Based Approach For Detection And Isolation Of Malicious Nodes In Manet*", International Journal of Engineering and Technology (IJET) Vol 5 No 1 Feb-Mar 2013.

[10] ehrouz A. Forouzan, "*Data Communications and Networking*", Fifth Edition, p. 327.

 