Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 6, June 2014, pg.651 – 658

RESEARCH ARTICLE

An Empirical Approach for the Detection of Malicious Node in Cluster Based Adhoc Wireless Networks

Bhakti Thakre[1], S.V.Sonekar[2]

[1]Research Scholar, Department of CSE, J D College of Engineering and Management, Nagpur, M.S., India

[2]Professor, Head of Department, Department of CSE, J D College of Engineering and Management, Nagpur M.S., India

[1] bthakre@jdpoly.in; [2] svsonekar@jdcoe.in

Abstract- A Mobile Ad Hoc Network (MANET) is a collection of mobile nodes who communicates with each other via wireless links either directly or through some other nodes such as routers. Due to the dynamic change in topology finding a proper route is very difficult. Some nodes misbehave as they participate in route establishment phase but refuse to forward the data packets to drop their own energy. The misbehaving node moves from one place to another dropping the packets.

A mobile Ad hoc network (MANETs) is a multi-hop wireless network in which message is transmitted from source to destination. These networks can be setup easily anytime and anywhere without any base infrastructure, as they are infrastructure less thus they have proved to be very efficient is rescue related areas like flood and fire. MANETs are now extended to be used in military and law enforcement. 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.

Keywords: MANET, Pause Time, Cluster Head (CH), Static Node (SN), Multiple Access (MA), OMNeT++

I. INTRODUCTION

The technology for dynamic wireless networks, had been deployed in military since 1970s, and thereafter it had been applied in various applications such as patient monitoring, 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 [1].

When nodes are connected and use a common link then we need multiple access protocol. In Fig. 1, we can see 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

(CDMA). This method is evolved by two another methods simultaneously i.e. Carrier senses multiple access with collision detection (CDMA/CD) and carrier sense multiple access with collision avoidance (CDMA/CA).

Aloha Protocol transport capacity is proportional to the square root of the density of mobiles which is very impressive. Finally, this protocol is self-adapting to the node density and it does not require prior knowledge of the density [2].

Other protocols like AODV can also be used for finding the route in the network. AODV protocol is a reactive routing protocol which finds route to destination when required. It consists of routing table which helps to differentiate between expiry and fresh routes. The routing table at node contains the sequence number and next hop information.

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 [3].

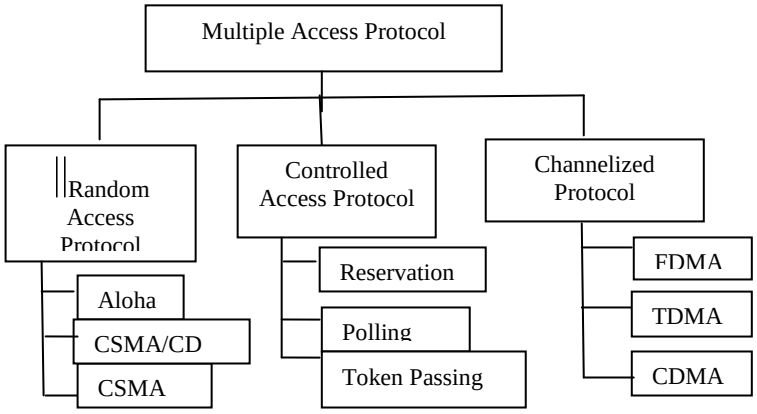

Fig. 1 Organization of Multiple Access [10]

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.

1. Cluster Head: Transmission Range of cluster head describes the limitations of Cluster.
2. Member Node: Member nodes are members of cluster and these nodes have members belonging to the cluster.
3. Guest Node: Guest node is the visiting node in the cluster that is associated with the cluster while moving in the network.

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].

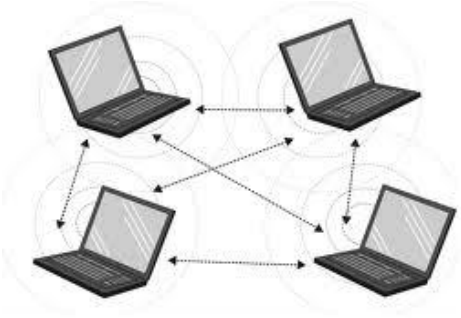

Fig. 2 Mobile Adhoc Networks

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 movement of Malicious node from one cluster to another in MANET. In Section 4, we provide Simulation Results; Section 5 concludes the paper with their future scope.

II. LITERATURE SURVEY

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.

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.

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].

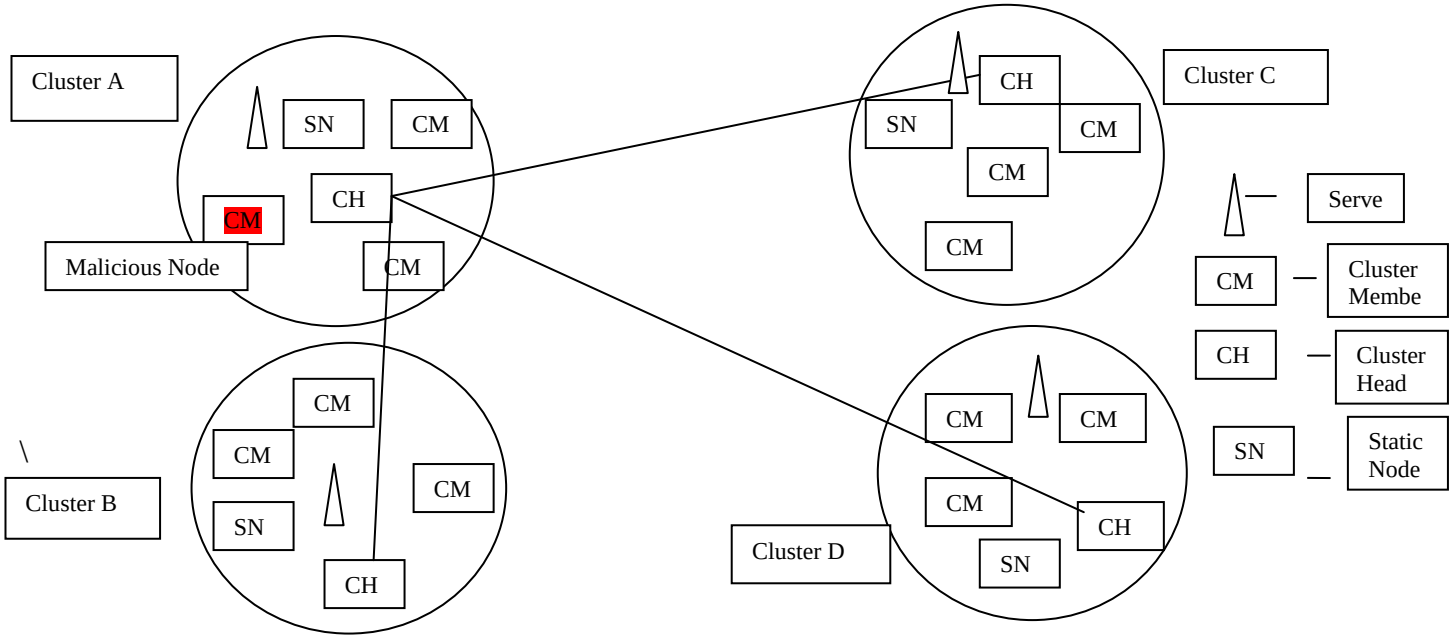

Fig. 3 Node Clustering

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 ie 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 selection 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.

In proposed scheme of Cluster head Selection Algorithm, we will take x and y Coordinates of the nodes with their IDs. The node which is having the highest number of nodes connected with it will be declared as Cluster head. Before searching for the Cluster Head the proposed algorithm will check that the cluster head is not 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 direct trust value.

There are two types of attack: External Attack and Internal Attack.

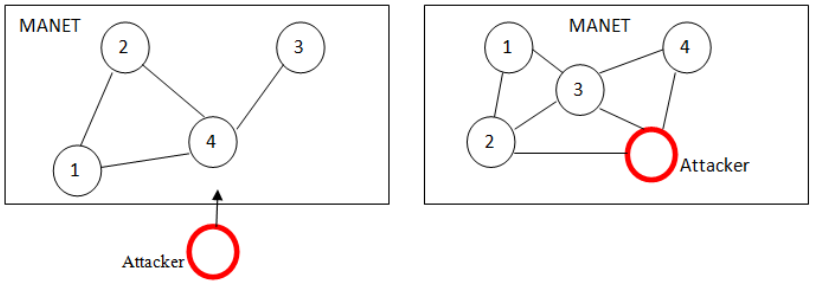

Fig. 4 External and Internal Attack in MANET

In shown in Fig 4, In External Attack, an attackers are from outside the network 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.

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 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

A. Steps of Coordinate Based Algorithm for Malicious Node Movement

Step 1: Start.

Step 2: Enter the No of Nodes in each cluster with malicious node index.

Step 3: When control is on Server it sends a “DATA” packet to static node, once receive it will send “DATA” packet to cluster head.

Step 4: Cluster head for each cluster is selected using highest connectivity and minimum ID algorithm.

Step 5: When cluster head receives “DATA” packet from static node, it broadcasts “DATA” packet among cluster members.

Step 6: When cluster members receive “DATA” from cluster members, they send “ACK” packet to Cluster head.

Step 7: When cluster head receives “ACK” packet from cluster members, then it sends each “ACK” packet to static node.

Step 8: When static node receives “ACK” packet, it sends “ACK” packet to server.

Step 9: When server receives “ACK” packet, then it sends “DATA” packet again and it continues again.

Step 10: Repeat till the malicious node (selected in step 2) doesn't follow normal behavior and moves from cluster to cluster.

Step 11: The malicious node sends "ME_MALICIOUS" packet to the nearest cluster head.

Step 12: When cluster head receives "ME_MALICIOUS" packet, it sends "NODATA" packet to malicious node.

Step 13: Also, Cluster head sends "MALICIOUS" packet to all cluster heads to inform that the given node is malicious.

Step 14: The malicious node starts from his own cluster and then goes into each cluster. After returning to original cluster, the malicious node becomes normal.
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 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.

B. Steps of Cluster Head Formation Algorithm

Step 1: Start.
Step 2: For each member of the cluster
Step 3: Calculate distance to other cluster and id
Step 4: If ID is minimum and it is closer to more nodes then make it cluster head
Step 5: Repeat step 3 to 4 for every node.
Step 6: Finally we will have a cluster head with min ID and distance to all members minimal.
Step 7: Stop.

The communication between the clusters is the responsibility of Cluster head. Cluster head is selected on the bases of connectivity with other clusters. The above discuss Algorithms will improve the performance of the system by detecting the malicious nodes in the network and avoid to send them messages.

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

Parameters	Values
Number of Nodes	40
Size of Network	600*400
Speed of Nodes	0-15 m/sec
Transmission Range	100 m
Battery Power of Node	100 Unit
Pause Time	0-20 Sec

TABLE 2: FINDING CLUSTER HEADS AND CLUSTER MEMBERS

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

The Table 1,2 and Fig.6 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 No of packets on Y Axis , throught which we can see the performance of proposed algorithm with respect to the protocols used. As we can see the performance in fig 5 the OLSR ,AODV and ALOHA protocol. The performance of proposed algorithm will increase gradually within the network as seen in the fig 5.

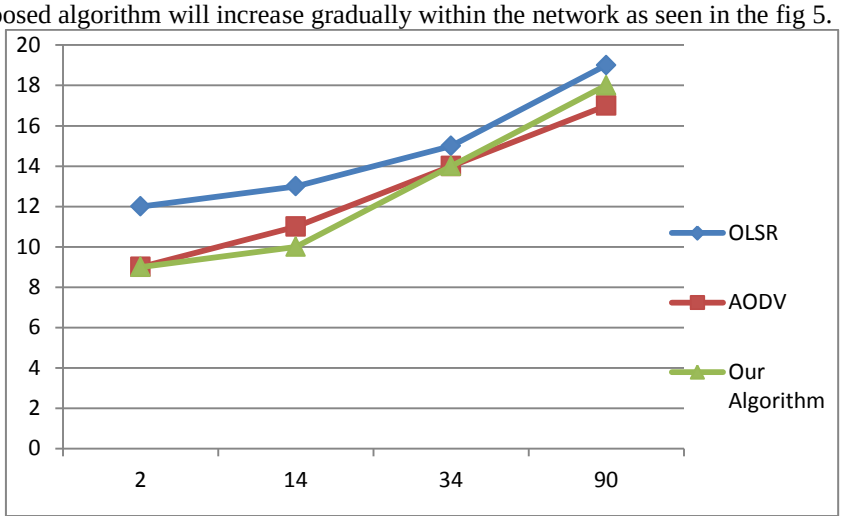

Fig. 5 Protocol Varient performance for High Mobility Network Scenarios

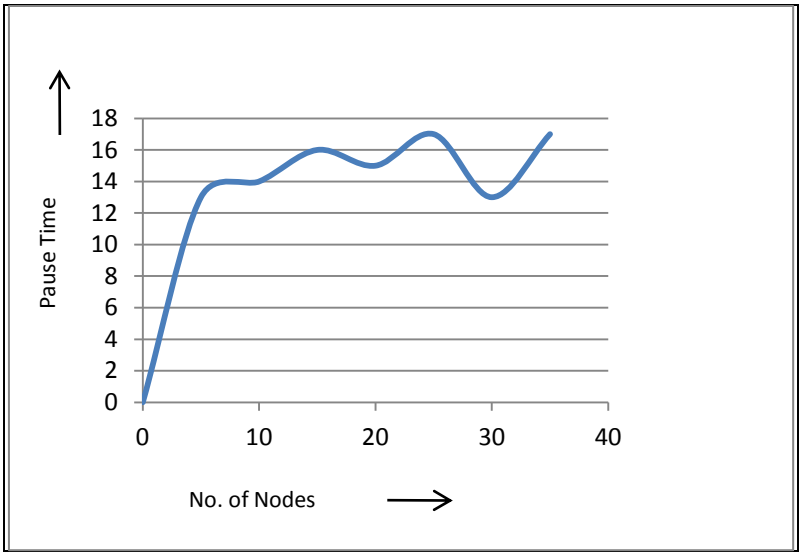

Fig. 6 Graph between No of Mobiles Vs Pause Time

In Fig.6 , graph shows the No of Nodes (Mobiles) on X axis and Pause Time on Y axis. Pause Time is defined as a time till which the node will stay in one location or we can say that the mobile node stay in one location for a specified period of time. Once the pause time is elapsed the mobile node randomly selects the next destination in the simulation area and chooses

a speed V which is in the interval of $(0,V_{max})$. V_{max} is some parameter to reflect the degree of mobility. As soon as mobile node arrives at a selected destination , it stay again there for the indicated pause time before repeting the process.

In Fig.7 , graphs shows the No of nodes on X Axis and Transmission range on Y Axis, transmission range represent the range under which the nodes can communicte within the network.

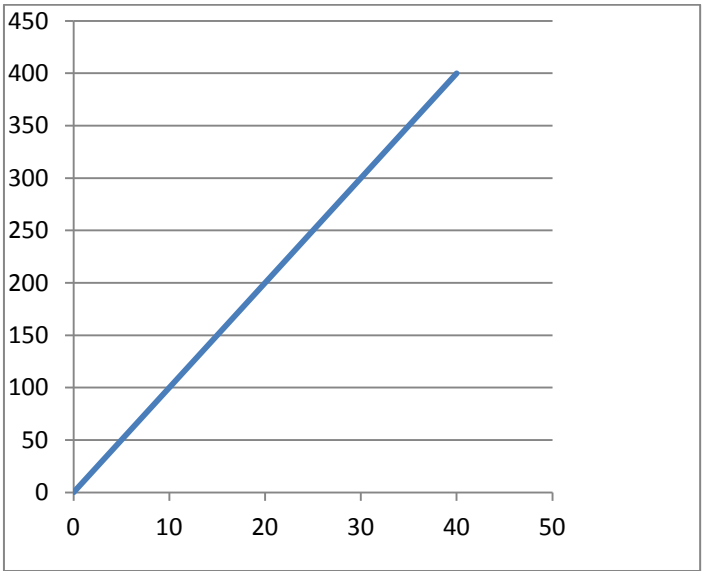

Fig. 7 Graph between No of Mobiles Vs Transmission Range

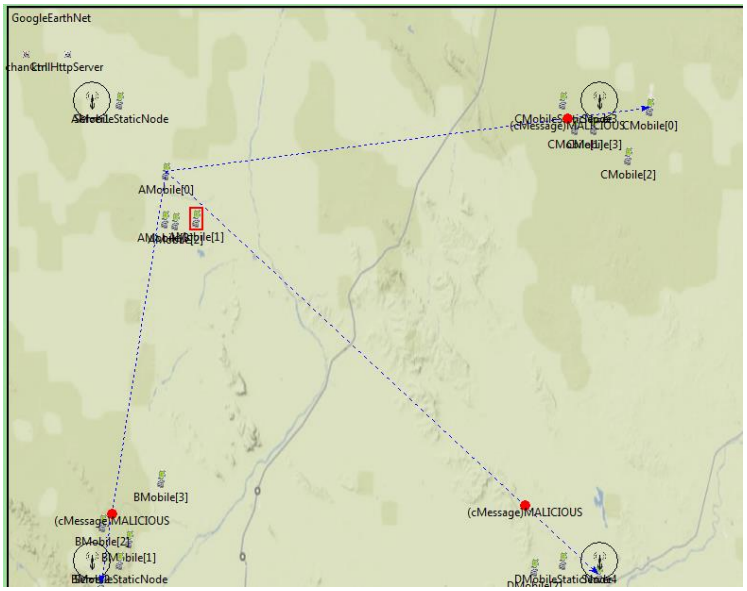

Fig. 8 Cluster Head Communication and Malicious Node Movement on Omnetpp Simulator.

The Fig. 8 shows the snapshot of our project in which we can see the communication between the Cluster Heads of all clusters and movement of malicious node from one cluster to another cluster. In the above figure, there are four clusters and blue dotted line shows the cluster head communications in between the clusters.

In our simulation we have taken four clusters and malicious node is present in cluster A. Cluster A will send information to another Cluster Head that the malicious node is detected with its ID. So that other cluster heads will not send any message to the malicious node in the network. The Malicious node will move from Cluster A to Cluster C to D to B and again return back to Cluster A. After returning to the Cluster A it will become the normal node and start sending packets and sending acknowledgement normally. Then we will select any new malicious node randomly

Basic parameters like energy carrying capacity, buffer size, speed of nodes, and mobility rate and transmission range for Aloha have been monitored to have changes for desired results.

V. CONCLUSION

The attack schemes, as well as prevention, detection and reaction mechanisms have been explored. We categorized them into three categories according to their goals and their specific strategies. A comparative study between them was then conducted to highlight their respective effectiveness and limitations. 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] Behrouz A. Forouzan, "*Data Communications and Networking*", Fifth Edition, p. 325.

