

## SURVEY OF TYPES OF NODES WITH IMPLEMENTATION OF MISBEHAVING NODE IN CGSR NETWORK

<sup>1</sup>Monika Gupta, <sup>2</sup>Parul Gupta

<sup>1</sup>Computer Science, Y.M.C.A. University of Science and Technology, Faridabad, India

<sup>2</sup>Computer Science, Y.M.C.A. University of Science and Technology, Faridabad, India

**Abstract** - Identification of misbehaving node is important to detect the security attacks in adhoc network. Suppose source sends a data packet to the destination and network is assigned a TTL. If the network monitors that the acknowledgement is not received then the network will identify the misbehavior. And it raises the node as misbehaving node. Here acknowledgement is must. Based on the acknowledgement only network identifies whether the node is misbehaving node or not. Hence there is need to study about how to detect malicious node present in network.

**Keywords:** MANET, CGSR, Watchdog.

### 1. Introduction

#### 1.1 Cluster Head Gateway Switching Routing Protocol

CGSR protocol is a multichannel operation capable protocol. It performs code separation between clusters. The clusters are elected by cluster head election process, which is very intensive process. It uses DSDV as the underlying routing scheme that is based on hierarchical cluster head-to-gateway routing. In CGSR the mobile nodes are grouped into clusters and a cluster-head is elected by election procedure. All nodes that are in the direct communication range of the cluster-head are in its cluster. A gateway node is a node that is in the communication range of two or more cluster-heads. In a dynamic network due to cluster head election procedure some problems may also occur like performance degradation, so CGSR uses a Least Cluster Change (LCC) algorithm. In LCC, cluster-head change occurs only if there is change in network causes two cluster-heads to come into one cluster or one of the nodes moves out of the range of all the cluster-heads. The general algorithm works in the following manner. The source transmits the packet to its cluster-head then from this cluster-head to the gateway node that connects this cluster-head and the next cluster-head along the route to the destination. In Fig.1 the gateway node sends it to the cluster-head and so on until the destination cluster-head is reached in this way. Finally destination cluster-head then transmits the packet to the destination. Each node maintains a table that has mapping from each node to its respective cluster-head.

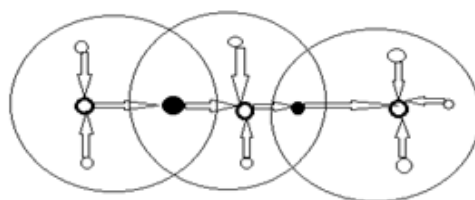


Fig.1 CGSR

Each node broadcasts its cluster member table periodically and updates its table after receiving the table from other nodes whenever required. In addition, each node also has a routing table that gives the next hop to reach the destination cluster. On receiving a packet, a node finds the minimum distance located cluster-head along with the route to the destination according to the cluster member table and the routing table. Finally it examines its routing table to find the next hop in order to reach the cluster-head that are one step away and transmits the packet to the respective node.

#### 1.2 Example of CGSR:

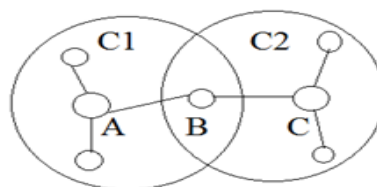


Fig.2 Example of CGSR

Fig.2 shows how the CGSR protocol manages the transfer of packet from node A to node C.

1) Node A (cluster head of C1) must get the permission to transmit in cluster C1. 2) Node B (gateway) must select the same code as node A to receive the packet from node A. 3) Node B must select the same code as node C (cluster head of C2) and get the permission to transmit in cluster C2 (receives a token from node C).

## **2. Related Work**

Literature review is a way of identification, and evaluation of all available research related to a particular research topic. Systematic literature reviews highlights on fair evaluation of a research topic by using a rigorous and balancing methodology. Systematic analysis must be carried out with a predefined search strategy.

Indhumathi.J, Prem Jacob.T[1,9]proposed an algorithm named as fast key generation in which TTL is assigned to the network. The source will send the data packet to the destination, and monitors all the node detail. And the network continuously updates the key of each node for data transmission. S. Marti, T. J. Giuli, K. Lai, and M. Baker[10]proposed two techniques WATCHDOG and PATHRATER. The authors explained that Watchdog is the basis of different intrusion detection system. Rasika Mali, Sudhir Bagade[2] ExWatchdog is an extension of watchdog. Using this mechanism, weakness of Watchdog mechanism has been overcome to some extent. S.Tamilarasan and Dr.Aramudan[5]:Here author analyze IDS determine whether the data is under attack or not. Buchegger[3,11,18]introduced the concept of CONFIDANT. In this each node can observe the behavior of all its neighboring nodes that are within its radio range. Bansal and M.Baker[14,15,16] gives a protocol, called OCEAN in which every node maintains rating for each neighboring node and monitors their misbehavior through promiscuous mode. Wenjia Li, Anupam Joshi.[6,8]According to the authors TWOACK is neither an enhancement nor a Watch-dog based scheme. It aims at resolving the receiver collision and limited transmission power problems of Watchdog, TWOACK detects misbehavior by sending acknowledgement through every data packets transmitted over each three consecutive nodes through the path from the source to the destination. T. Sheltani, A. Al-Roubaiey, E. Shakshuki and A. Mahmoud[4,7,13]described that Adaptive ACK is somewhat similar to TWOACK.AACK is an acknowledgement-based network layer scheme which is a combination of a scheme call and an end-to-end acknowledgement scheme called ACK. Michiardi and Molva[12,17] proposed a technique named as CORE similar to CONFIDANT which is similar to monitoring and reputation system.

## **3. NODE MISBEHAVIOUR**

Identification of malicious nodes in networks is critically important to detect security attack in the network. Selfish nodes do not intend to directly damage other nodes, but however, do not cooperate, saving battery life for their own communications. Malicious nodes do not give priority to saving battery life, and aim at damaging other nodes. It is introduced that two different types of selfish nodes. As the nodes in MANETs are battery powered, energy becomes a precious resource, and thus, role of selfish nodes draws more attention. Thus, it describes three routing behaviors of nodes in a MANET.

*Type-0:* well-behaved node: A well behaved node cooperates in the communication well, performs as required by the routing protocol, and equally participates in the communication activities like route discovery, maintenance, packet forwarding and receiving etc.

*Type-1:* active selfish node: Such a node does not participate in packet forwarding, and drops every received packet. It disables the packet forwarding mechanism for the packets which have a destination address, other than this selfish node. In fact, it helps the selfish node to save its own energy, thereby still contributing to network maintenance.

*Type 2:* passive selfish node: Such a node practically does nothing and stays idle in the network. It does not contribute to any of the activities like packet forwarding, receiving, route discovery, network maintenance. With respect to above mentioned misbehaving nodes, we evaluate the performance of DSDV, DSR and AODV routing protocols through extensive simulations, where a certain percentage of nodes behave as active and/or passive selfish nodes with the remaining nodes being well-behaved.

### **3.1 Selfish node Problem**

Another effect of node misbehaviors and failures in ad hoc networks is the node isolation problem due to the fact that coordination between nodes is completely dependent on routing and forwarding packets. In turn, the presence of selfish node is a direct cause for node isolation, which further affects network survivability. Traditionally, node isolation refers to the phenomenon in which nodes have no active neighbors. Due to the presence of selfish node, a node can be isolated even if active neighbors are present.

In Fig.3, suppose node x5 is a selfish node. When node u initiates a route discovery to another node D, the selfish neighbor x5 may be reluctant to broadcast the route request from u. In this case, x5 behaves like a failed node. It is also possible for x5 to forward control packets. However, the situation could be worse since s may select x5 as the next hop and send data to it. Consequently, x5 may discard all data to be forwarded via it, and then communications between s and D cannot proceed. When all neighbors of s are selfish, s is unable to establish any communications with other nodes at a distance of more than one-hop away.

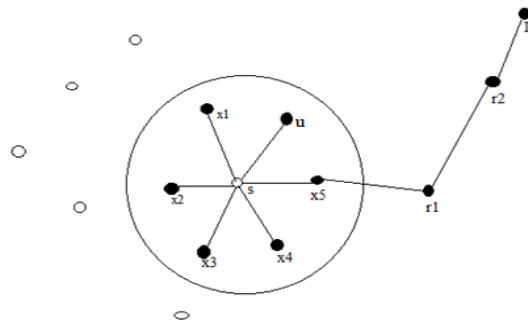


Fig.3 Node isolation due to selfish neighbor

In this case, node s is isolated by its selfish neighbors. Selfish nodes can still communicate with other nodes via their cooperative neighbors, which is different from failed nodes.

#### 4. Types of nodes

Identification of misbehaving node is important to detect the security attacks in adhoc network. Misbehaving nodes in the adhoc network may be of various types like selfish nodes. Selfish nodes do not aim at damaging other node. They intend to save their battery power for their communication. They do not participate in the communication of other nodes if the communication is not meant for it.

Further the nodes can be categorized as follows:

**Well behaved nodes:** A well behaving nodes corporate in the communication very well. It performs as per required by the protocol. And it equally participates in the communication.

**Active selfish node:** This type of node discards the entire packet passing through it if the destination is not the address of this node. It saves its battery power for itself communication only.

**Malicious nodes:** Malicious nodes are active nodes. They intentionally damage other nodes and create interruptions in the network. These nodes discard the packets and modify the routing tables. They do not intend to battery saving.

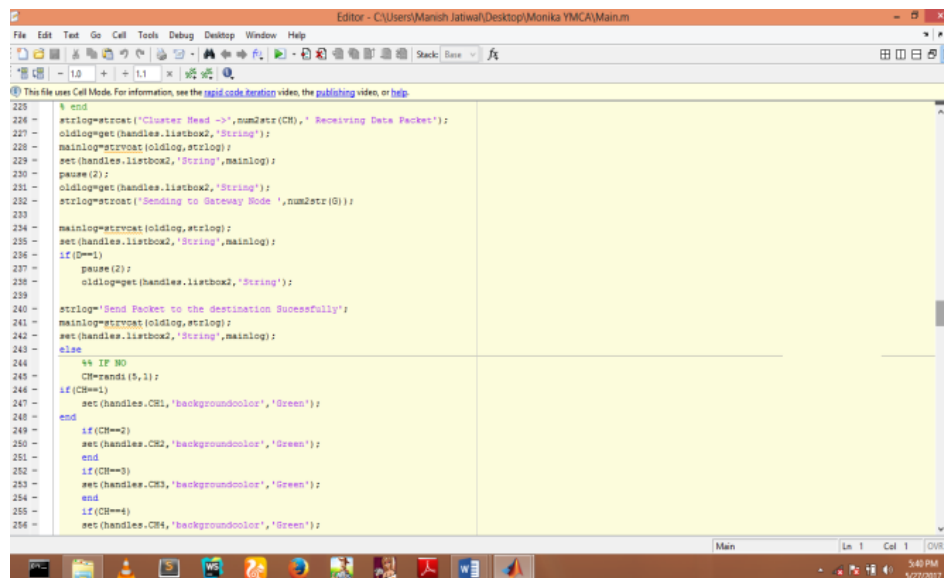
In the intrusion detection system, when source sends a data packet to the destination node. Then data packet will be send through intermediate nodes and the acknowledgment to the source will be send when data has transferred through consecutive nodes. Suppose source sends a data packet to the destination and network is assigned a TTL. If the network monitors that the acknowledgement is not received then the network will identify the misbehavior. And it raises the node as misbehaving node. Here acknowledgement is must. Based on the acknowledgement only, networks identify the misbehaving node. Here the time delay is minimized.

But the problem with this technique is that if it founds the node as misbehaving then it declares it as misbehaving node and delete that node but there is a possibility that acknowledgement is not received because of link failure, collision or some other reasons. The solution of the above problem can be the new algorithm as proposed.

In CGSR when a node sends a data packet to other node if that source node does not receive any acknowledgement then we cannot conclude that the node is misbehaving. There may be any other reason for not receiving acknowledgement. It may be link failure or any other reason. So in order to identify that node is misbehaving or not we can use the following concept.

## 5. Implementation of Identification of MISBEHAVING NODE

The proposed algorithm is implemented through MATLAB platform. The fig. 6 shows the MATLAB code for the identification of misbehaving node. In this first data packet is sent to the cluster head. Then cluster head randomly selects the next cluster head and then sends the data packet to the destination. If acknowledgement is not received from the destination then the node sends the hello message three times to the next node.



```

225 % end
226 strlog=strcmp("Cluster Head ->",num2str(CH),"Receiving Data Packet");
227 oldlog=get(handles.listbox2,'String');
228 mainlog=strcat(oldlog,strlog);
229 set(handles.listbox2,'String',mainlog);
230 pause(2);
231 oldlog=get(handles.listbox2,'String');
232 strlog=strcmp("Sending to Gateway Node ",num2str(G));
233
234 mainlog=strcat(oldlog,strlog);
235 set(handles.listbox2,'String',mainlog);
236 if(D==1)
237     pause(2);
238     oldlog=get(handles.listbox2,'String');
239
240 strlog="Send Packet to the destination Successfully";
241 mainlog=strcat(oldlog,strlog);
242 set(handles.listbox2,'String',mainlog);
243 else
244     % IF NO
245     CH=randi(5,1);
246     if(CH==1)
247         set(handles.CH1,'backgroundcolor','Green');
248     end
249     if(CH==2)
250         set(handles.CH2,'backgroundcolor','Green');
251     end
252     if(CH==3)
253         set(handles.CH3,'backgroundcolor','Green');
254     end
255     if(CH==4)
256         set(handles.CH4,'backgroundcolor','Green');
    
```

Fig.4 MATLAB program for identification of misbehaving node

The fig. 4 shows the MATLAB code for the identification of misbehaving node. In this first data packet is sent to the cluster head. Then cluster head randomly selects the next cluster head and then sends the data packet to the destination. If acknowledgement is not received from the destination then the node sends the hello message three times to the next node. If the reply of the hello message is not received in any of the three time then node is raised as misbehaving node.

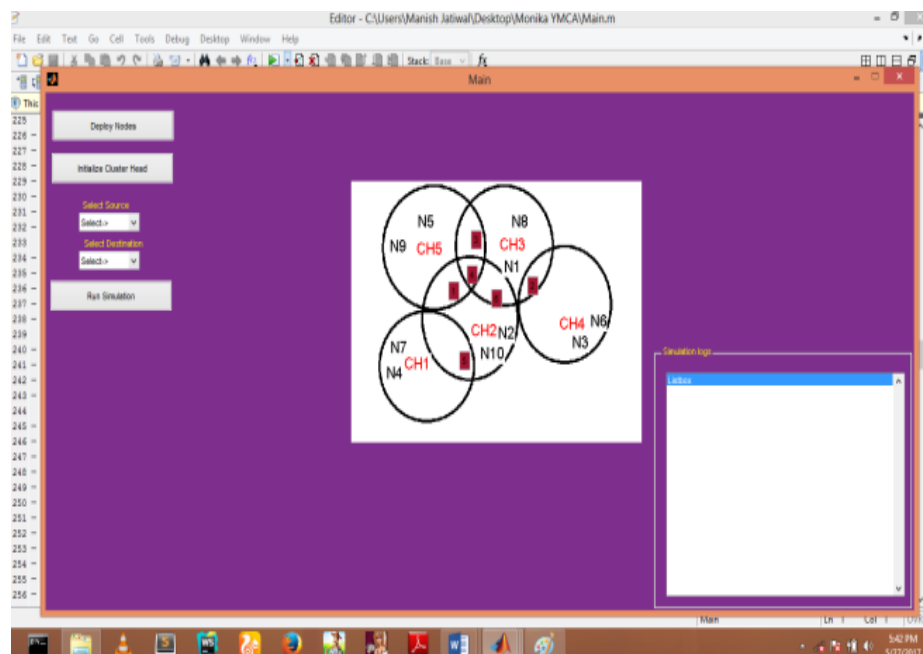


Fig.5 Interface for the implementation

The fig.5 shows the interface for the identification of misbehaving node and selection of gateway node in MANET in CGSR. The above figure shows the five clusters with their cluster heads, nodes and gateway nodes.

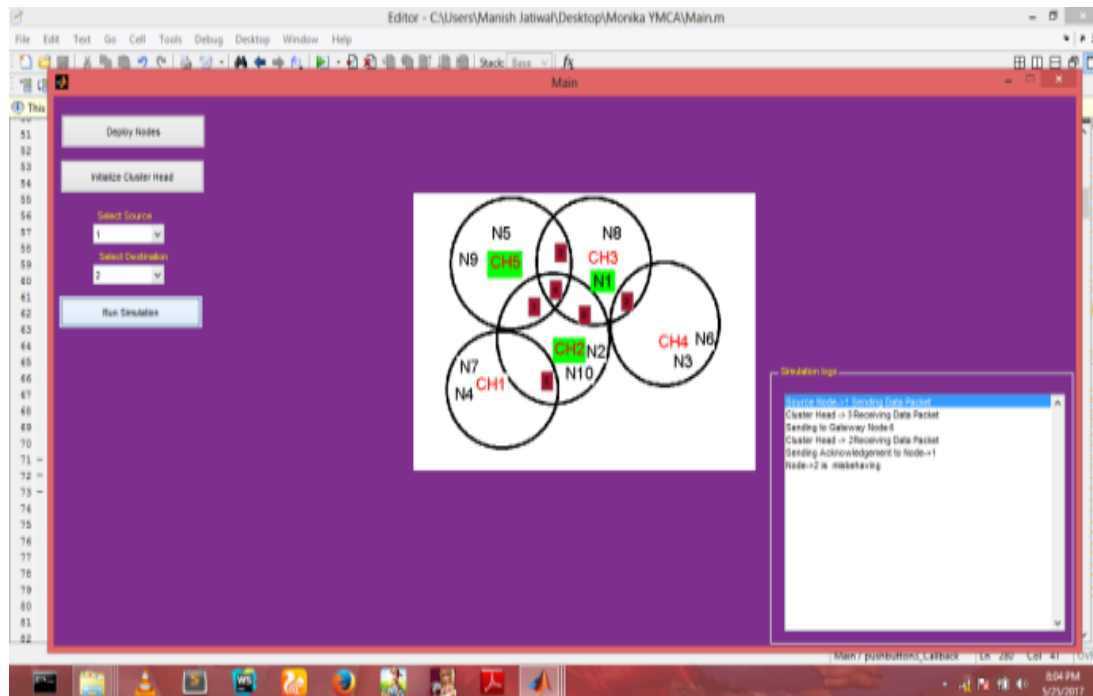


Fig.6 Transfer of packets from node 1 to node 2

Fig.6 shows the transfer of packet from node 1 to node 2. First source node 1 transfer packet to the cluster head 3. Then cluster head transfer packet to the gateway node 6. Then cluster head 2 receive the data packet. Then node 2 sends the acknowledgement to the previous node. And no reply of hello message is received in any of the three times. Then it shows that node 2 is misbehaving.

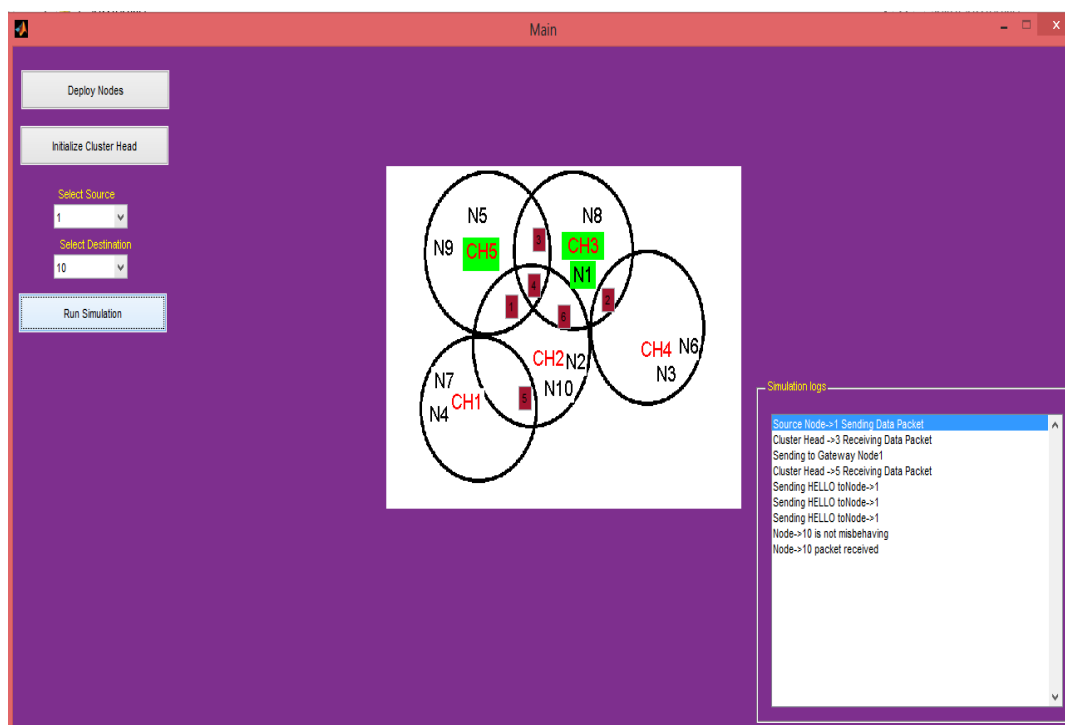


Fig.7 transfer of packet from node 1 to node 10

Fig.7 shows the transfer of packet from node 1 to node 10. Here node 10 is not misbehaving.

## **6. Conclusion**

Many researchers have done work on finding the different techniques for finding the misbehavior nodes. The Dynamic nature of the MANET is a major challenge to maintain the frequently changing topology of the network. So there is more possibility of attacker and misbehaving node. When misbehaving nodes participate in the route discovery phase but refuse to forward the data packets, the performance is degraded severely. Various types of misbehavior can be possible in MANET. This paper studied the various techniques to detect the misbehaving nodes. Various attacks possible in MANET are also described. Watchdog has good network throughput, but it suffers from various disadvantages which are resolved to very little extent by other techniques. Ex Watchdog solves the problem of false misbehavior reporting. 2ACK and AACK have reduced routing overhead and reduced network overhead respectively. And the new algorithm has been proposed in order to detect the misbehaving node. Identification of misbehaving node is important to detect the security attacks in adhoc network. Misbehaving nodes in the adhoc network may be of various types like selfish nodes. Selfish nodes do not aim at damaging other node. They intend to save their battery power for their communication. They do not participate in the communication of other nodes if the communication is not meant for it. The work in this paper is tried to analyze the misbehaving node in CGSR routing protocol in mobile adhoc networks.

## **7. Future work to be carried**

Mobile adhoc network are widely used network due to their flexibility in nature that is easy to deploy and less time to set up. These are exposed to internal and external attack due to their dynamic nature. There is decentralized security mechanism in Mobile ad hoc networks. The proposed algorithm detects the misbehaving node very well. Further this work can be extended to which takes less time to detect the misbehaving node.

## **8. Acknowledgement**

A special thank to Dr. Parul gupta for her technical support to implement this protocol and also for useful comments, discussions, and suggestions regarding this approach.

## **9. References**

- [1] Isha V. Hatware, Atul B. Kathole, Mahesh D. Bompilwar, "Detection of Misbehaving Nodes in Ad Hoc Routing" IJETE, Volume 2, Issue 2, February 2012.
- [2] Rasika Mali, Sudhir Bagade, "Techniques for Detection of Misbehaving Nodes in MANET: A Study", International Journal of Scientific & Engineering Research, Volume 6, Issue 8, August-2015.
- [3] Sumiti, S. Mittal "Identification Technique for All Passive Selfish Node Attacks in a Mobile Network," International Journal of Advance Re-search in Computer Science and Management Studies, vol. 3, Issue 4, Apr. 2015.
- [4] M. S. Alnaghes and F. Gebali "A Survey on Some Currently Existing Intrusion Detection Systems for Mobile Ad Hoc Networks," In Proceedings of Second International Conference on Electrical and Electronics Engineering, Clean Energy and Green Computing, Konya, Turkey, 2015.
- [5] S.Tamilarasan and Dr.Aramudan, "A Performance and Analysis of Misbehaving node in MANET using Intrusion Detection System", IJCSNS, VOL.11 No.5, May 2011.
- [6] Wenjia Li, Anupam Joshi (IEEE Senior Member), and Tim Finin, "Coping with Node Misbehaviors in Ad Hoc Networks: A Multi- Dimensional Trust Management Approach". Eleventh International Conference on Mobile Data Management, IEEE, 2010.
- [7] Zaiba Ishrat "Security Issues, Challenges and Solution in MANET, "International Journal of Current Science and Technology", vol. 2, Issue 4, Oct. - Dec. 2011.
- [8] Usha Sakthivel and S. Radha, "Misbehaving Node Detection in Mobile Ad Hoc Networks using Multi Hop Acknowledgement Scheme", Journal of Computer Science, 2011.
- [9] Indhumathi.J., Prem Jacob.T "Identification of Misbehavior Activities in Mobile adhoc Networks", IJCSIT, volume 5(2), 2014.
- [10] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks" Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MobiCom'00), pp. 255-265, August 2000.
- [11] S. Buchegger and J. Y. Le-Boudec, "Nodes bearing grudges: Towards routing security, fairness, and robustness in mobile ad hoc networks", In Proceedings of EUROMICRO- PDP02, 2002.
- [12] P. Michiardi and R. Molva, "CORE: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks", In Proc. 6th IFIP Communication and Multimedia Security Conf., Sept.2002.

- [13] T. Sheltani, A. Al-Roubaiey, E. Shakshuki and A. Mahmoud ,“Video Transmission Enhancement in Presence of Misbehaving Nodes in MA-NETs,” *Journal of Multimedia Systems*, Springer, Oct. 2009.
- [14] S.Bansal and M.Baker, "Observation-Based Cooperation Enforcement in Ad-hoc Networks", Technical Report, Stanford University, 2003.
- [15] R. Manoharan, S. Rajarajan, S. Sashtinathan, and K. Sriram, “A novel multi-hop b3g architecture for adaptive gateway management in heterogeneous wireless networks,” in *Proc. 5th IEEE WiMob*, pp. 48-54, 2009.
- [16] Y. Yan, L. Ci, Z. Wang, and W., “QoS-based gateway selection in MANET with Internet connectivity”,15th Int. Conf. Advanced Communication Technology (ICACT), pp.195-199, 2013.
- [17] H. Ammari, and H. El-Rewini, “Integration of mobile ad hoc networks and the internet using mobile gateways,” in *Proc. IEEE International Parallel and Distributed Processing Symposium (IPDPS04)*, USA, p. 218b, 2003.
- [18] X.Zhanyang, H. Xiaoxuan and Z. Shunyi, “A scheme of multi path gateway discovery and selection for MANET using Multi-Metric”, 1<sup>st</sup> International Conf. Information Science and Engineering (*ICISE*), 2009.