Research with Implementation of Detection of Malicious Node in CGSR Network

Neha[1] Ranjan Kumar Singh[2]
[1,2]Department of Electronic Communication
[1,2]S.R.C.E.M, Palwal, India

Abstract— Adhoc network is a collection of wireless network. Each node communicates in a radio communication range. A MANET is a group of multi-hop wireless ad-hoc network. Each node transfer the message from one node to another node and source to route construction among nodes. MANET has a variety of application such military, disaster struck areas. MANET is vulnerable to various attacks due to its open medium. Destination in the wireless network. The network is not fully safe and secured. Each device in a MANET is free to move independently in any direction. As the node is free to move, any node can join or leave the network at any time. Wireless network work on dynamic topology, many types of problem arries in the network in the Hence there is need to study in detail about how to detect malicious node are presented.

Key words: AACK (Adaptive acknowledgment), MANET, CGSR, Routing, Network

I. Introduction

A. *Cluster head gateway switching routing protocol*

CGSR is a multichannel operation protocol. The entire node that are present in the communication domain of cluster head belong to its cluster. A gate way node is a type of node that is in the communication range of two or more cluster-heads

CGSR, nodes are grouped into the cluster and it is a cluster based routing table that lists all available destination. CGSR protocol uses the DSDV (Destination-Sequence Distance-Vector) routing algorithm as the underlying routing scheme that is based on hierarchical cluster head-to-gateway routing.

In a dynamic network cluster head scheme can cause performance decline due to frequent cluster-head elections. So most of the CGSR uses a LCC (Least Cluster Change) algorithm.

In LCC, by any reason of any node move out from the range of all cluster-heads, the cluster-head changed. If during the change in the network two clusters-heads comes into one cluster then cluster-head change.

The general algorithm works in the following procedure. Source transmits the packet to the cluster-head and cluster-head send the packet to gate way node that connects to the cluster-head and next cluster-head according to the route of destination. In fig 1 shows that gate way node connect to the cluster –head that send the packet to the destination.

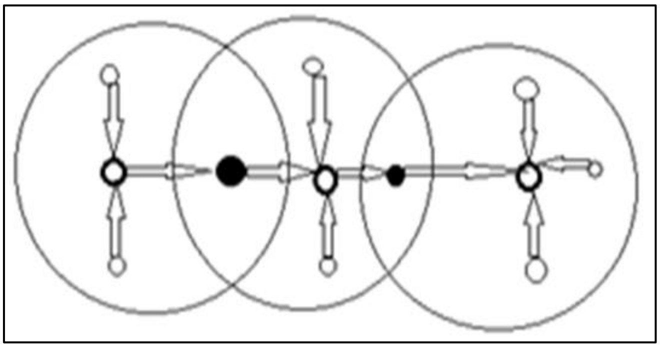


Fig. 1: CGSR

II. 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] 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.

This algorithm for "Detection of misbehaving node and selection of gateway node in MANET" is based on mechanism to identify the malicious node. The proposed work will leads to the identification of misbehaving node more accurately. To identify the misbehaving node an algorithm is developed. (1) To achieve detail knowledge of misbehaving node. (2) To find several techniques and methods for identifying different types of misbehaving node. (3) To understand the various issues related to misbehaving nodes.

III. Node misbehavior

In ad-hoc network malicious node is critically important to detect security attack in the network. Selfish node is type of node that does not intelligible to injure the other node directly, but most of the times they do not cooperate saving battery life for own communication. Malicious node does not give preference to save battery life and focused at damaging other node. In ad-hoc network, there are two different types of selfish node .In MANET there are three routing behavior of routing nodes.

1) Well Behaved Node: Type 0: A well behaved node equally performed in the communication scenario like forwarding and receiving the data, maintenance and route searching or discovery. It is necessary for routing protocol and it participates in the communication.
2) Active Selfish Node: Type 1:-Selfish node does not forwarding the message and leave every received message. Selfish node save own energy and they helps to networks problem resolving.
3) Passive Selfish Node: Type 2:-Passive selfish node does not helps any of the activity like data sending and receiving, route ,discovery, network problem resolving. such a node practically nothing and stay unique in the network .we find out the performance of DSDV, DSR , routing protocols where as some percentage of nodes work as active or passive selfish node with the remaining node being well behaved.

A. Selfish node Problem

An instantaneous effect of node misbehaviors in the wireless ad-hoc network is wide problem due to the effect that communication is totally dependent on routing and sending and receiving the data . In term presence of selfish node is a direct reason for node isolation and network segmentation which further affects networks survival, node isolation is process in which node are not in same place and area. A node can be separated when active node are available.

In figure, assume that node x5 is a selfish node when the node n has started a route researched for a node m then the selfish neighbouring x5 can be loath to broadcast the route request from n. In this case x5 behave like misbehavior node, X5 sends the control data packet and x5 may leave all the data packet to forwarded

Between the s and m communication is not occurred and all the neighbours of s are selfish node so no forwarding and receiving the packet between the s and m node are possible. Selfish node are communicates with other node with the help of co-operative nodes.

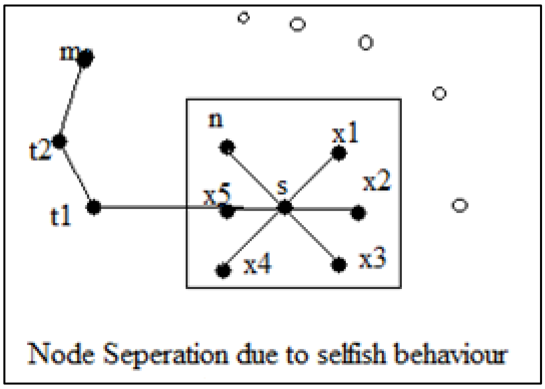


Fig. 2:

IV. Proposed work

Selfish node save their battery power for their communication and do not aim to harm other nodes. Abusive node is important for detecting security attack in the ad-hoc network can be different types like selfish node. In addition nodes can be classified as follows:

1) Malicious Node: Malicious nodes give up packets and convert routing tables. They do not intention to save battery active nodes. They deliberately harm other nodes and create interruptions in the network.
2) When the data packet is send by source on the destination node, then the data packet will be sent through intermediate nodes and continous nodes transferred the data packet. Suppose the source sends the data packet to the destination and the TTL is entrusted to the network.
3) But the problem with this technique is that if this node is found to be misbehaving, then it declares it as an abnormal node and removes that node but there is a possibility that link failure, collision or any other Approval has not been received due to other reasons. The solution to the above problem may be a new algorithm as proposed.
4) Well Behaved Nodes: Having a good deal of communication in the nodes corporate is very good, it does the necessary by the protocol and it participates in communication equally
5) Active Selfish Node: This type of node has passed the whole packet if the destination is not the address of this node. It saves its battery power automatically for communication

A. Explanation of Proposed Algorithm

From Figure 4 first source will send the packet to its cluster head. Cluster head receives the data packet. Cluster head will check in its routing table that if the destination node is present in its cluster or not, if the destination node is present in its cluster then it will send the packet to it. Otherwise the cluster head will send the data packet to the gateway node. The gateway node now sends the data packet to the next cluster head. Now this cluster head will check for the destination node.

If the destination is not present in the cluster then cluster send the data packet to the gate way and gate way send the packet to the next cluster. After that cluster-head search the data packet to the cluster if the destination is present in this cluster then cluster head will send the data packet to the destination and if the acknowledgement is not received by the source then it wait some. The process will run three times. The loop will send hello message three- four times. If any reply is received by the node in any one of the three - four times. Then the node is not misbehaving. And if the reply is not received by the node in three to four times then node is said to be misbehaving

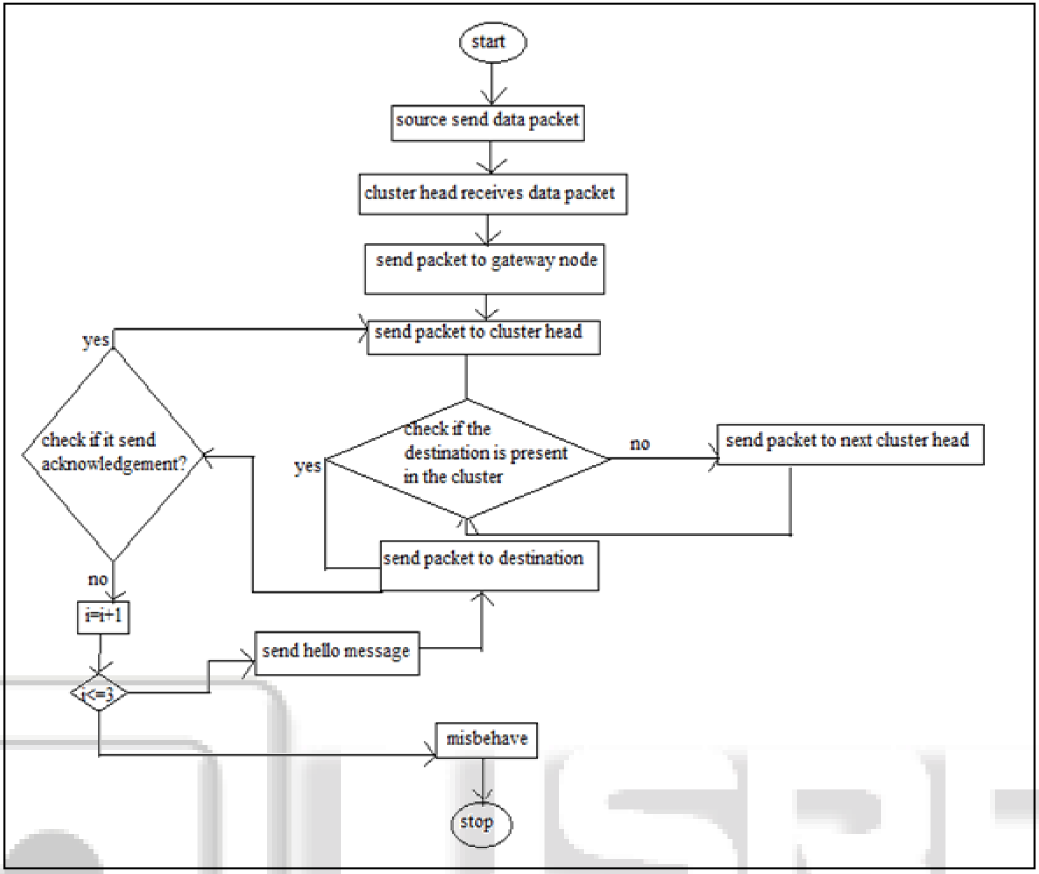
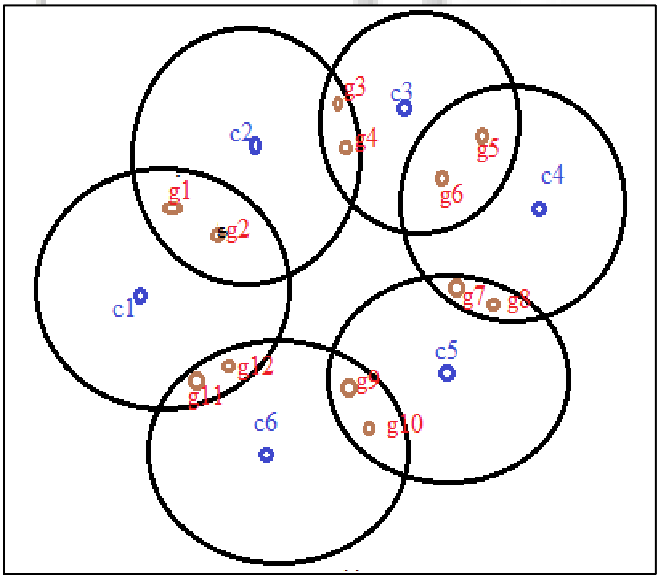

start
source send data packet
cluster head receives data packet
send packet to gateway node
send packet to cluster head
yes
check if it send acknowledgement?
check if the destination is present in the cluster
yes
no
send packet to next cluster head
send packet to destination
no
i=i+1
send hello message
i<=3
misbehave
stop

Fig. 3: Flow chart for detection of misbehaving node

V. Selection of Gateway Node in CGSR



There are multiple clusters in the cluster head gateway switching routing protocol. Now for the communication between the source and destination one requires to select one single gateway node from the multiple gateway nodes. So to select the gateway node following concept can be applied. There are multiple clusters in CGSR. In fig.4 some clusters are such that they transfer packets through the single gateway node. Remove these types of clusters and separate them out. Then select those cluster head which share more than one gateway node between them. Then check the gateway nodes which are common. Now will check with which gateway node we are left with. Out of those nodes, will select the gateway node on some particular base which can be either battery or any another factor.

The following scenario shows the entire possible gateway node through which the nodes can communicate.

A. Gateway nodes for the different clusters

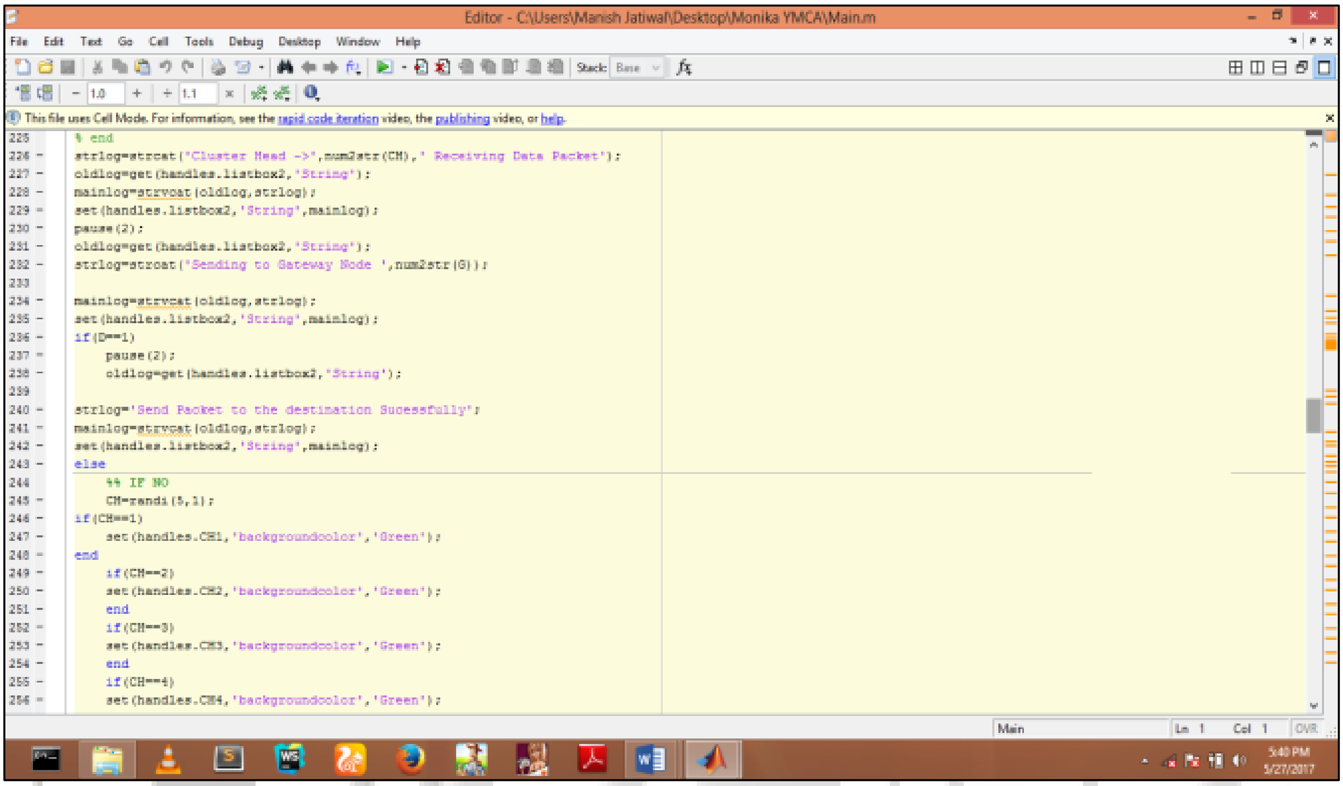
Cluster head (Source, Destination)	Gateway nodes
C1 ,C2	g1 g2
C1 ,C6	G11 g12
C2 ,C3	G3 g4
C3,c4	G5 g6
C4 ,C5	G7,g8
C5,c6	G9,g10

Table 1: Gateway Nodes Available for Network

The following table shows the only gateway nodes through which the nodes can communicate after removing the gateway nodes

As shown in Table 1 here for the transfer of packet between the clusters two gate way node are available. if in the mid of the communication one gate way node is failed in this condition other gate way node is proceed . cluster 1 to cluster 2 two gateway nodes g1, g2 and are available. So in this case the communication between the cluster 1 and 2 will take place through g1 or g2. For the communication between the clusters 5 and 6 there are two gateway nodes g10,G9 .For the transfer of packet of between the cluster1 and cluster6 two gate way node G11 and g12 are Transmission is occurred between the cluster2and cluster3 via the g3,g4 .if any of the case g3 is failed then in case g4 is worked as a gateway node. Communication is occurred between the cluster4 and cluster 5 via G7 and g8 if any of the case G7 is failed then in this case g8 work as gate way node.

VI. IMPLEMENTATION OF IDENTIFICATION OF MISBEHAVING NODE


Editor - C:\Users\Manish Jatiwal\Desktop\Monika YMCA\Main.m
File Edit Text Go Cell Tools Debug Desktop Window Help
Stack: Base
This file uses Cell Mode. For information, see the rapid code iteration video, the publishing video, or help.
Main
Ln 1
Col 1
OVR
5:40 PM
5/27/2017

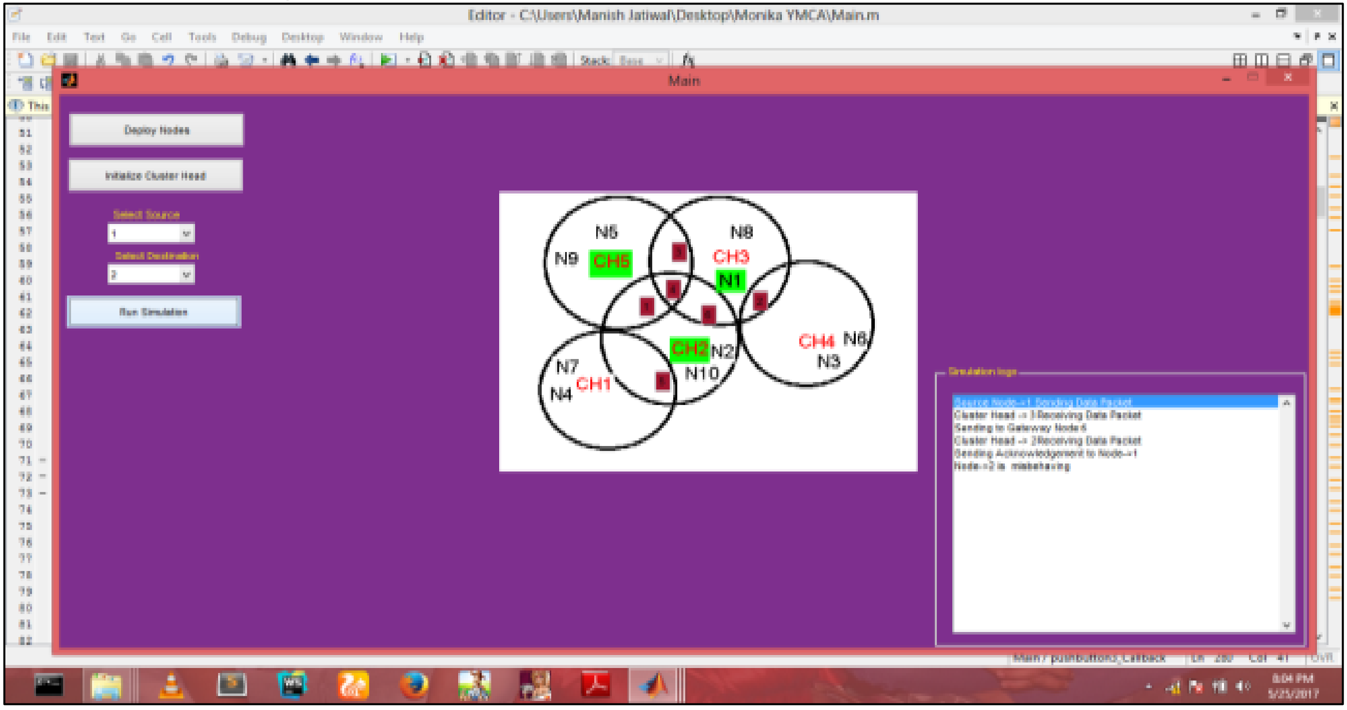
```
% end
strlog=strcat('Cluster Head ->',num2str(CH),' Receiving Data Packet');
oldlog=get(handles.listbox2,'String');
mainlog=strvcat(oldlog,strlog);
set(handles.listbox2,'String',mainlog);
pause(2);
oldlog=get(handles.listbox2,'String');
strlog=strcat('Sending to Gateway Node ',num2str(G));

mainlog=strvcat(oldlog,strlog);
set(handles.listbox2,'String',mainlog);
if(D==1)
    pause(2);
    oldlog=get(handles.listbox2,'String');

strlog='Send Packet to the destination Sucessfully';
mainlog=strvcat(oldlog,strlog);
set(handles.listbox2,'String',mainlog);
else
    %% IF NO
    CH=randi(5,1);
if(CH==1)
    set(handles.CH1,'backgroundcolor','Green');
end
    if(CH==2)
    set(handles.CH2,'backgroundcolor','Green');
    end
    if(CH==3)
    set(handles.CH3,'backgroundcolor','Green');
    end
    if(CH==4)
    set(handles.CH4,'backgroundcolor','Green');
```

Fig. 5: MATLAB program for identification of misbehaving node

The figure 5 shows the misbehaving node in the MATLAB code for the identification. 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.



```
Source Node->1 Sending Data Packet
Cluster Head -> 3Receiving Data Packet
Sending to Gateway Node 6
Cluster Head -> 2Receiving Data Packet
Sending Acknowledgement to Node->1
Node->2 is misbehaving
```

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

Figure 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.

VII. Conclusion

Much researcher work to identify the different technique for finding the misbehaving of nodes. Finding the best route is the main target of routing algorithm from source to destination. One more problem observed during the sending of packet, one of the nodes from the network not sends the acknowledgement to the source. This node in the network named as malicious nodes we mention one technique to identify that kind of malicious nodes in the paper. We have to study about how to identify the malicious node present in the network. Different attack possible in the MANET is also described. Watchdog has a good network throughout but many times it suffers many disadvantages. These disadvantages are resolved by applying some other technique. Example watchdog resolve the problem of false misbehaving reporting. AACK and 2ACK have reduced network overhead and routing overhead both. And new algorithm has been proposed to detect the misbehaving node. Very important task is to identifying the misbehaving node to detect the security attack in the ad-hoc network. Misbehaving node which present in the ad-hoc network may be many kind like selfish node. In this paper we try to analyze the misbehaving node the CGSR routing protocol in mobile ad-hoc network.

VIII. Future work to be carried

Mobile ad-hoc 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.

Acknowledgement

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

References

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] Zaiba Ishrat "Security Issues, Challenges and Solution in MANET," International Journal of Current Science and Technology, vol. 2, Issue 4, Oct. - Dec. 2011.

[7] Usha Sakthivel and S. Radha," Misbehaving Node Detection in Mobile Ad Hoc Networks using Multi Hop Acknowledgement Scheme", Journal of Computer Science, 2011.

[8] 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.

[9] S. Buchegger and J. Y. Le-Boudec, "Nodes bearing grudges: Towards routing security, fair-ness, and robustness in mobile ad hoc networks", In Proceed

[10] S. Bansal and M. Baker. "Observation-Based Cooperation Enforcement in Ad-hoc Networks", Techical Report, Stanford University, '03.

[11] 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*, 2009, pp. 48-54.

[12] H. Ammari , and H. El-Rewini, "Integration of mobile ad hoc networksand the internet using mobile gateways," in *Proc. IEEE InternationalParallel and Distributed Processing Symposium (IPDPS'04)*, USA,2004, p. 218b.

[13] X. Zhanyang, H. Xiaoxuan, and Z. Shunyi, "A scheme of multipathgateway discovery and selection for MANET using Multi-Metric," *1stInt. Conf. Information Science and Engineering (ICISE)*, 2009.