A Novel Approach for Malicious Node Detection in Cluster-Head Gateway Switching Routing in Mobile Ad Hoc Networks

Monika Gupta[1] , Puneet Garg[2] , Swati Gupta[3], Rakesh Joon[4]

[1,2]*J. C. Bose University of Science and Technology, YMCA, Faridabad, Haryana, India*
[3]*Vaish College of Engineering, Rohtak, Haryana, India*
[4]*Ganga Institute of Technology and Management, Kablana, Jhajjar, Haryana, India*

ABSTRACT

Ad hoc network is a group of wireless networks that permits communicating directly with another node without a router. Every node imparts inside a scope of wireless transmission. MANET is a gathering of multi-hop remote ad hoc network. Every node transmits the message to another node by means of a remote network. This network is totally hazardous and along these vulnerable to attackers. Every device in MANET is dynamic in nature and over and again changes its links to different devices. Mobile ad hoc network (MANET) is a persistent, self-arranged, adaptable, low capacity independent and infrastructure less network associated with cell phones. There are various issues that emerge in the administration and directing between nodes in the network since wireless network deal with a dynamic topology. The primary reason for algorithm routing is to give the best and optimum distance route from source to destination. When sending packet to destination, none of the nodes from the source to the destination node through intermediate nodes send an acknowledgement to the source node. At that point that node is known as a malicious node. Therefore, different techniques for perceiving that malicious node have been portrayed. The success of a ad hoc network relies upon the open's trust in its security. Different strategies are utilized to identify malicious nodes. This paper is tied in with managing malicious nodes for secure information transmission. Malicious nodes are nodes that influence the other nodes. MANET incorporates highlights, for example, military, disaster influenced zones and dynamic topology, fixed infrastructure. Anyway it has some security issues and difficulties. MANET[7] is vulnerable to against different attacks because of its open media. In this way, there is a need to concentrate in detail how to identify malicious or misbehaving nodes[8] in the network. In this paper, different strategies for distinguishing the misuse of the node are introduced. Strategies introduced in this proposition are: Watchdog, ExWatchDog, TWOK, and OCEAN.

Keywords: *MANET, Ad Hoc, Networks, CGSR, Watchdog, Routing, Malicious Node*

1. Introduction

Ad hoc network is a bunch of wireless networks. In PC organizing, ad hoc network refers to the network foundation where it doesn't require any switch or base station. For instance, in the event that you need to move a document to your companion's PC, you can set up a transitory system between your PC and others system by means of some system to move the data. It can communicate with one another utilizing a link media or a PC's remote medium. In the event that you need to impart records to PC or any systems administration gadget to another gadget, you can set up a multi-hop specially appointed system that can move information over numerous nodes. For the most part, a specially appointed system is an impermanent system association intended for a particular reason, for example, sharing information starting with one PC then onto the next.

Remote versatile [17] specially appointed systems are self-arranging, solid and dynamic systems in which nodes are moving in various ways. Rather than depending on a base station to organize the progression of messages to every hub in the system, Wireless systems don't have the complexities of framework arrangement and organization. In PC organizing, alludes to a system association built up for a transitory system meeting and doesn't require a switch or remote base station for correspondence to arrange.

1.1 Cluster Head Gateway Switching Routing (CGSR) Protocol

CGSR protocol is a multichannel activity empowered protocol. It partitions code between Clusters. Clusters are chosen through the cluster choice procedure, which is an exceptionally serious procedure. It utilizes DSDV as the fundamental steering plan dependent on various leveled bunch head-to-gateway directing. Portable hubs in CGSR are assembled into clusters and cluster heads are chosen through the selection procedure. All the correspondence between the hubs is finished by cluster head are in its group. A gateway node is a node between the correspondence scopes of at least two cluster heads. The cluster head choice procedure should be possible cautiously to keep away from issues, for example, execution corruption in powerful systems, so CGSR utilizes a decreased cluster change (LCC) calculation. In LCC, a cluster head change happens just when two cluster heads fall inside the cluster because of an adjustment in the system, or when one of the hubs falls outside the scope of all cluster heads. The clarification of cluster head gateway exchanging directing convention is as per the following. The source sends the packet to its cluster head on the off chance that the node is available inside that cluster, in the event that not, at that point goes from its cluster head to the destination node, which associates with this cluster head and the following cluster head while in transit to the destination. In Fig.1 the gateway hub sends the data to the cluster head. At long last sends a cluster head packet to the destination. Every node keeps up a table with a planning from every node to its relating cluster head.

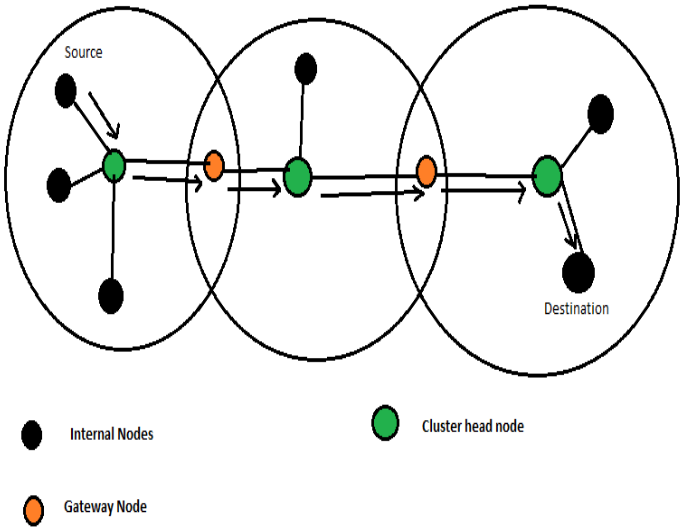


Figure 1: Cluster head gateway routing protocol

Every node intermittently shares its cluster member table and updates its table subsequent to accepting the table from neighboring nodes varying. Moreover, every node additionally keeps up its own routing table that gives the following next hop by means of which way for the destination cluster is recognized. Subsequent to getting the packet from the source node, the node predicts the base separation of the cluster head in source to the destination as per the cluster member table. At long last it checks its routing table, which identifies the next hop inside least advance of arriving at the cluster heads and sends the packet to the destination node.

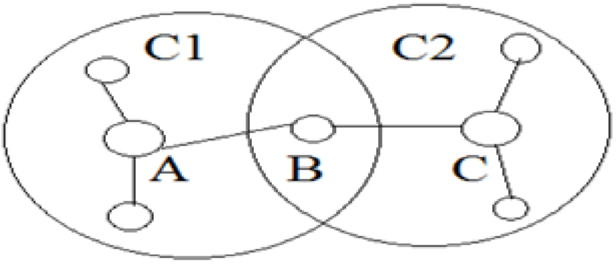


Figure 2: An example scenario of Cluster head Gateway switching routing protocol

Figure 2 shows how the CGSR protocol manages the transfer of packet from node A in cluster C1 to node C in cluster C2. Below are the steps for transferring the data from source node A in cluster C1 to destination node C in cluster C2.

1) Node A must requirement get the authorization to transmit in cluster C1 if the destination is absent inside the cluster.
2) Node B which go about as an gateway node between cluster C1 and cluster C2 must choose a similar code as node A to get the packet from node A.
3) Node B must choose a similar code as node C which is the destination node for the cluster C2 and get the consent to transmit in cluster C2 (gets a token from node C).

2. Related work

The literature review is to identify and evaluate all available research related to a specific research topic. The systematic literature highlights an impartial evaluation of the research topic using a rigorous and balanced approach. Systematic analysis should be done with a predefined search strategy.

Indumati et al [9] proposed a calculation called fast key generation, in which the TTL is relegated to the system. The source sends the data packet to the destination and screens all nodes subtleties. The system continually refreshes every node key for data transmission.
S. Marty et al [10] proposed two techniques. The author bring up that watchdog is the reason for different intrusion detection system. They utilize neighborhood data and hence are a lot more grounded for most assaults. Watchdogs are utilized to distinguish the malicious nodes[1,6] in the system. The watchdog technique utilizes the passive strategy to hear the connection to the following node to check whether they have sent the packet. Since each node can hear all connections in such a manner there is no connection encryption, nodes can likewise check the integrity of messages.

Rasika Mali et al [2] an augmentation of the watchdog algorithm. Utilizing this component, the shortcomings of the watchdog approach are to some degree survive. At the point when a node sends a failure report to different nodes dependent on that reports the system will distinguish they are getting into mischief, the malicious node can separate the system, saying that a few nodes that tail it are additionally acting up. The motivation behind the ExWatchdog framework is to distinguish such nodes. The source node first finds a way that doesn't contain a malicious nodes from the routing table. On the off chance that no such way is accessible, the source node starts root discovery to discover another way. Next, the source node sends the message utilizing the new way.

S. Tamilarasan et al[5] Here the author examine the IDS to check whether the information is vulnerable. IDS implies that intrusion detection system can be grouped into two sorts of system based IDS[4] and host-based IDS. ID depends on the system runs at the network gateway that catches and screens information on the system.

The host ID depends on the working framework is utilized by the system and it screens information created by projects and clients.

Buchiger et al [11] presented the idea of Confidence Protocol. In this, every node can screen the conduct of its entire neighboring node inside its correspondence range. Certain conventions incorporate different parts, for example, screen, trust manager, path administrator and reputation system for distinguishing the behavior of the node. In this, the nodes track all the neighboring nodes inside the transmission range. Every node continually screens all nodes in its region to recognize the malicious node. On the off chance that a malicious node is expelled from the occasion depiction, it is sent to the reputation system for correspondence to the whole system.

Bansal et al [14] give a convention called OCEAN, in which every node performs appraisals for each neighboring node and screens their act up. In this, the protocol tracks fraudulent routing misconduct dependent on the rating. When sending a node cluster, the module fills the packet checksum to recognize the malicious hub in the system. The OCEAN protocol[16] tunes in to the conduct of the following next hop neighbor node.

T. Sheltoni et al[13] expressed that the positive ACK is like TWOACK. The back end is a receipt-based system layer plot, which is a hybrid of plan call and endpoint. The end to end voucher scheme is called ACK. This plan works in two sections. First (ie ACK), information packet is send to the destination node. Upon fruitful appearance of the packet to the destination, it restores the Acknowledgement (ACK) packet to the source node. At the point when the source node gets Acknowledge packet effectively, the transmission between the source and destination is performed.

Michiardi et al [12] proposed CORE (collaborative approach to using node collaboration in a hoc ad network), like Confidence protocol, in light of test and duplication programs. Thus every node gets reports from different areas. Confidence Protocol possibly considers the entry of essential positive reports when there is no malicious node in the network. Service Attack Denial (DoS) [19] has been prohibited on the grounds that it doesn't take into consideration false reports. This program is given a negative rating where the hub can't help out its diminished reputation. The repeat rate increments when a particular report is received around there.

3. Behaviors of Malicious Node

Malicious nodes are not planned to spare battery life, they are expected to influence different nodes. It presented two kinds of Selfish node closures. As the terminals on MANETs are battery fueled, they become a significant wellspring of vitality and in this way more consideration is paid to the job of the selfish terminals. In this manner, it portrays the three routing behavior of the nodes in the MANET.

Type-0: Well-working hub: The well-working node helps out correspondences, works as required by routing protocol and is similarly associated with correspondence exercises, for example, route discovery, Maintenance, packet sharing and recovery.

Type-1: Active selfish node: Such node doesn't take an interest in packet sharing and despises each pocket got. This incapacitates the pocket offering process for packet to a destination address other than this selfish node. Indeed, it enables the selfish node to spare its vitality, which further adds to organize the executives.

Type 2: Passive selfish node: Such nodes do hardly anything and are inactive on the network. It doesn't support any usefulness, for example, packet sharing, receipt, root detection, network management. For the above faulty nodes, we assess the exhibition of the DSDV, DSR and AODV directing protocol with detailed simulations, where a couple of percent of the nodes work with dynamic and/or passive selfish node[3], the rest Operate with nodes. The treatment is finished.

3.1 Selfish Node Problem

Another outcome of node misbehaves and failures in ad hoc network[18] are node isolation issues on the grounds that the coordination between nodes relies altogether upon the directing and sharing packets. In turn, the presence of a selfish node is an immediate reason for node isolation, which enormously influences network survival Traditionally, node isolation alludes to the phenomenon where nodes are not dynamic neighbors. Since it is a selfish node, a node can be separated regardless of whether there are dynamic neighbors.

In Figure 3, let us accept that node x5 is a selfish node. Node U When beginning the way scan for another node D, selfish neighbors are hesitant to send the path demand from x5 U. For this situation, x5 goes about as a failed node. You can likewise send control packet for the X5. Be that as it may, the circumstance might be more awful in light of the fact that s will choose x5 as the next node and send data to it. Thus, all information transmitted by x5 can be overlooked, and afterward the association among S and D won’t proceed. While the entirety of S’s neighbors is selfish, S doesn’t impart more than one separation with different nodes.

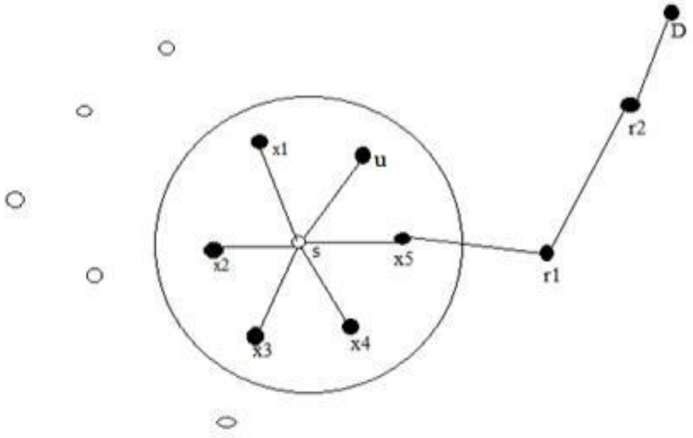


Figure 3: Node isolation due to selfish neighbor

4. Proposed Work

Identifying an abuse node is critical to detecting security attacks on ad hoc networks. Misbehaving nodes in a temporary network can be of various kinds, such as selfish nodes. Selfish nodes are not intended to harm the other node. They are expected to conserve their battery power for their communication. More nodes can be classified as follows:

(i) Well-behaved nodes: Well-behaved nodes in communication are corporate. It works according to the protocol. And it is equally involved in communication.
(ii) Active Selfish Node: This type of node passes through the entire packet if the destination is not the address of this node. It saves its battery power only for its communication.
(iii) Malicious nodes: malicious nodes are active nodes. They infect other nodes and interrupt the network. These nodes ignore packets and modify the routing table. He has no intention of saving the battery.

In the intrusion detection system, when the source data is sent to the pocket target node. Data packets are sent through intermediate nodes and are sent to the data source when data is constantly transmitted by nodes. Assume that the source sends the data packets to the destination and is assigned to the TTL network. Network receipt tracking identifies network abusers. And it expands the node to an attack node. Here is a voucher. Only identifies the wrong end of the network receipt. The time delay here is very low. But the problem with this technique is that if this node is found to be invalid, it declares it as an offensive node and removes that node, but it is unlikely to be accepted due to connection failure, conflict or other factors. There. The solution to the above problem may be the proposed new method.

The first source from Figure 4 sends the pocket to its cluster head. The cluster head receives data packets. The cluster head in its routing table checks if the target node is in its cluster, and if the target node is in its cluster, it sends the packet to it. Otherwise the cluster head sends data packets to the gateway node. The gateway node now sends the data cluster to the next cluster head. Now this cluster head checks the target node.

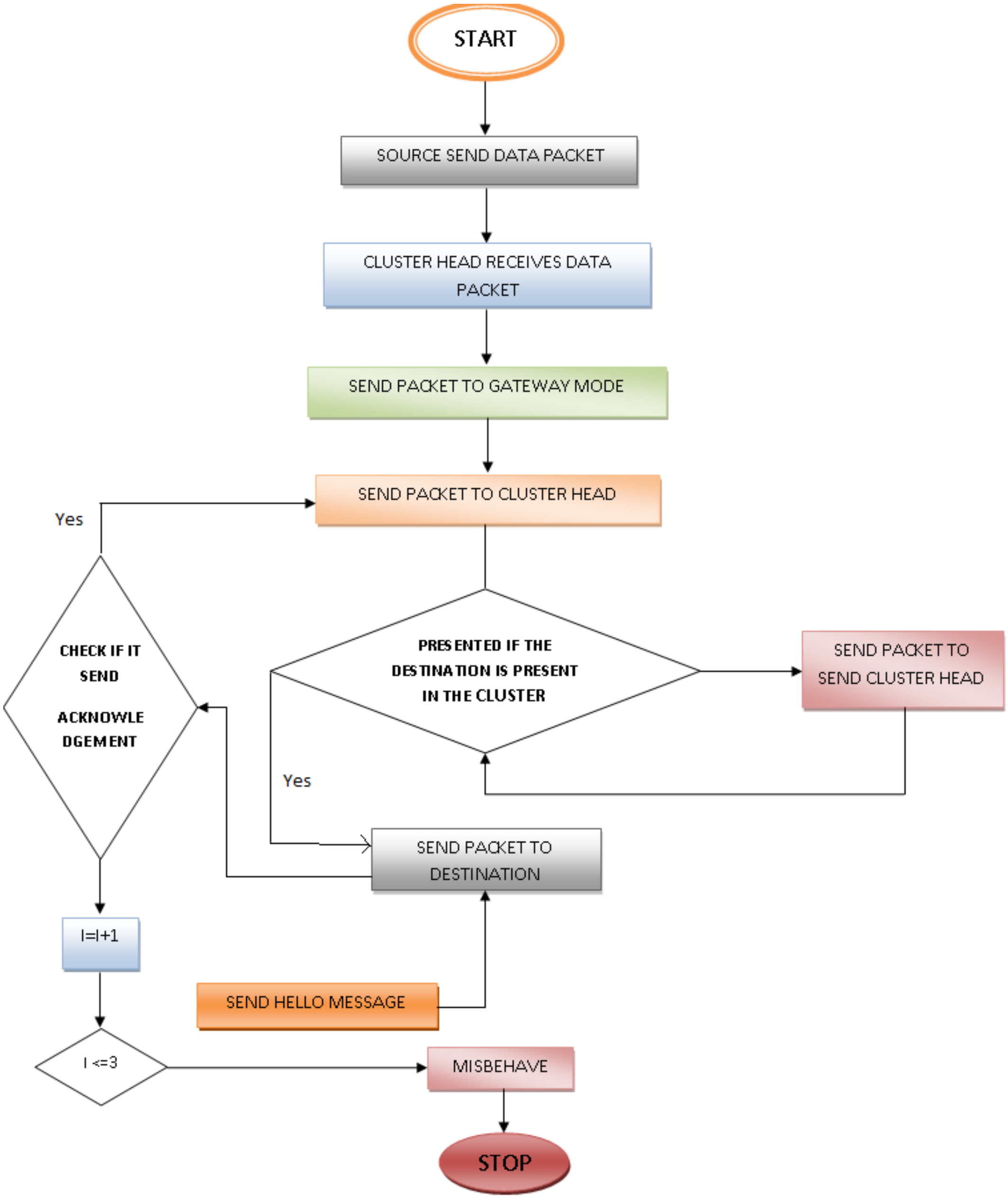

START
SOURCE SEND DATA PACKET
CLUSTER HEAD RECEIVES DATA PACKET
SEND PACKET TO GATEWAY MODE
SEND PACKET TO CLUSTER HEAD
Yes
CHECK IF IT SEND ACKNOWLE DGEMENT
PRESENTED IF THE DESTINATION IS PRESENT IN THE CLUSTER
SEND PACKET TO SEND CLUSTER HEAD
Yes
SEND PACKET TO DESTINATION
I=I+1
SEND HELLO MESSAGE
I <=3
MISBEHAVE
STOP

Figure 4: flow chart for detection of misbehaving node

ISSN: 2233-7857 IJFGCN

If this cluster does not have a destination node, it sends the data cluster to the next cluster head through the Cluster Head Gateway node. If there is a destination in this cluster, the cluster head sends data packets to the destination and waits to receive it from the destination. If the receipt is not received within the specified period, the loop will be executed according to the proposed task. The loop checks the receipt from the destination. The loop runs three times. The loop sends three hello messages. If answered three times by the previous node. Then the node cannot be abused. And if the answer is not found in all three of these, the node will be abused.

4.1 Selection of gateway node in CGSR

Cluster head gateway switching routing protocol includes many clusters. Now a single gateway node[15] must be selected from multiple gateway nodes for communication between source and destination. So the following concept can be applied to selecting the gateway node. There are many clusters in CGSR. Some clusters transfer packets through the same gateway node. Remove these types of inflorescences and separate them. Select cluster heads that share more than one gateway node between them. Then check the common gateway nodes. Now we check what gateway is left with the node. Of those nodes, some choose the gateway node on a specific basis, whether it's battery or some other factor.

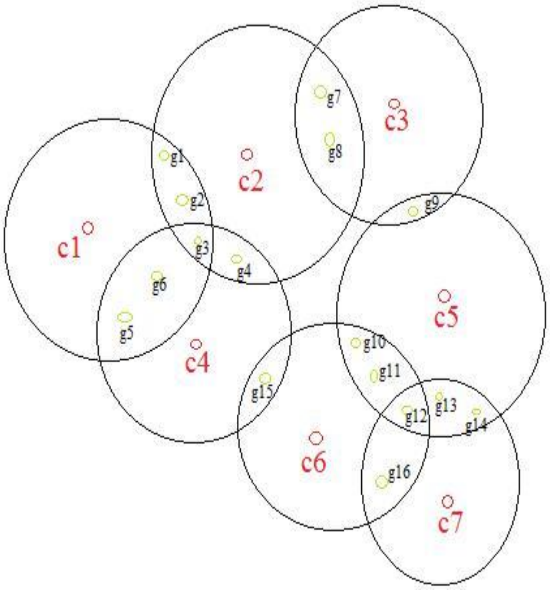


Figure 5 Clusters with gateway nodes

The following scenario shows only the gateway nodes that the nodes can communicate with after deleting the gateway nodes that are the busiest in the communication process.

As shown in Table 1, three gateway nodes from cluster 1 to cluster 2 are available here for packet transfer between G1, G2 and G3. Table 2 G3 of the three gateway nodes also serves as the gateway node between clusters 1 and 4. In this case the communication between clusters 1 and 2 is through G1 or G2. The three gateway nodes for communication between groups 5 and 6 are G10, G11 and G12. Of these three gateway nodes, G12 also serves as a gateway node for cluster 6, and in this case G12 is deleted and cluster 5 and 6 use communication between G10 and G11. The three gateway nodes for communication between groups 5 and 7 are G12, G13 and G14. Of these three gateway nodes, g12 also serves as a gateway node for clusters 5 and 6. So in this case g12 will be skipped and for the communication between the cluster 5 and 7, g13 and g14 will be used.

Table 1: Gateway Nodes Available for Network

Cluster head (Source, Destination)	**Gateway nodes**
C1 ,C2	g1 g2
C1 ,C4	g5 g6 g7
C2 ,C4	g3 g4
C2 ,C3	g7 g8
C4 ,C6	g15
C3 ,C5	g9
C5 ,C6	g10 g11 g12
C6 ,C7	g16 g12
C5 ,C7	g12 g13 g14

Table 2: Gateway Node Selected

Cluster heads (Source ,Destination)	**Gateway nodes**
C1 ,C2	g1 g2
C1 ,C4	g5 g6
C2 ,C4	g4
C2 ,C3	g7 g8
C4 ,C6	g15
C3 ,C5	g9
C5 ,C6	g10 g11
C6 ,C7	g16
C5 ,C7	g13 g14

4.2 Pseudo code for identification of misbehaving node

The figure 6 shows the pseudo 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.

```
Input: Nodes
    1. Source wants to send data to destination.
    2. Data will be sending through the cluster head.
    3. Cluster head will pass the data to gateway node if the destination
       node is in other cluster.
    4. Send the data packet to the cluster head of the destination cluster.
    5. If the destination node is present in the cluster the data packet will
```

Figure 6: pseudo code for identification of misbehaving node

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.

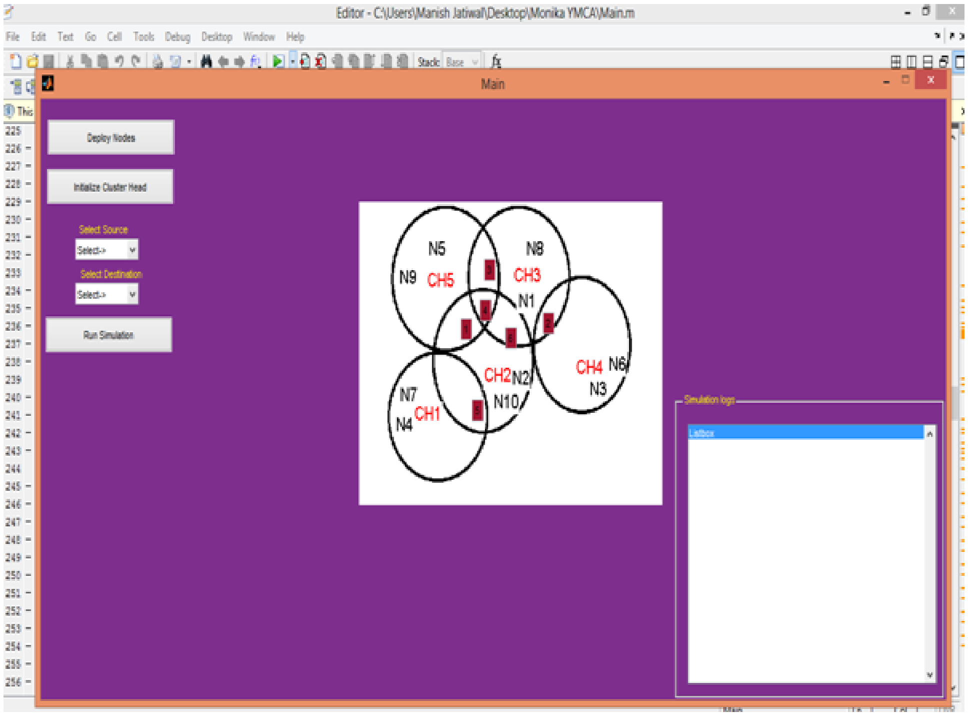
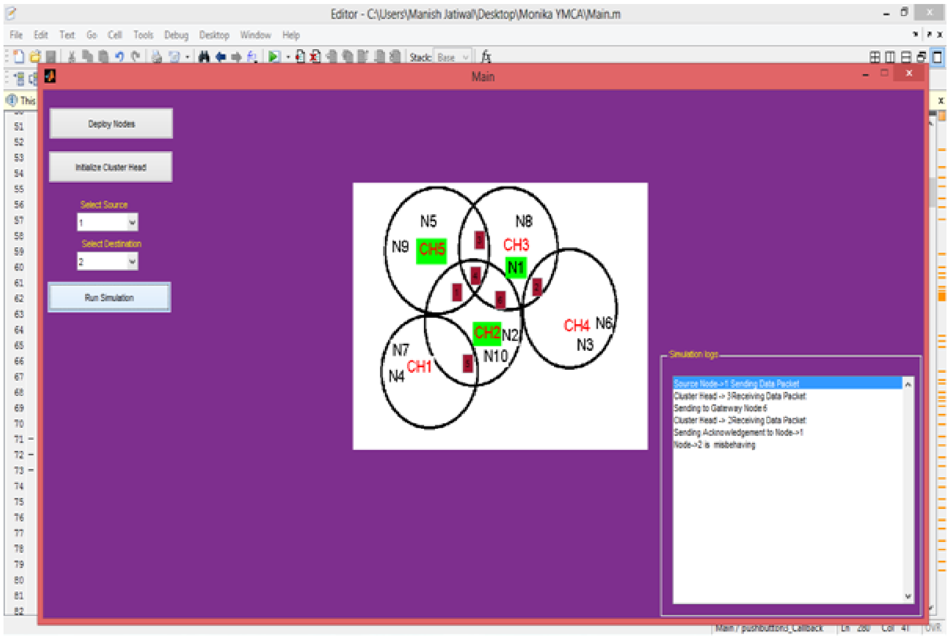
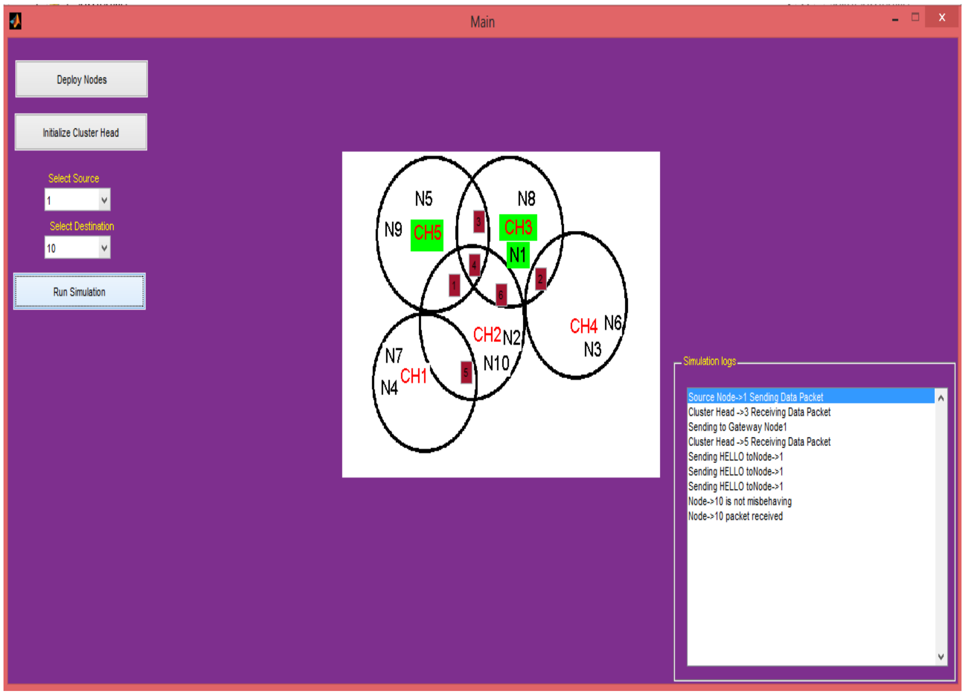


Figure 7: Interface for the implementation



```
Source Node->1 Sending Data Packet
Cluster Head -> 3Receiving Data Packet
Sending to Gateway Node6
Cluster Head -> 2Receiving Data Packet
Sending Acknowledgement to Node->1
Node->2 is misbehaving
```

Figure 8: Transfer of packets from node 1 to node 2



```
Source Node->1 Sending Data Packet
Cluster Head ->3 Receiving Data Packet
Sending to Gateway Node1
Cluster Head ->5 Receiving Data Packet
Sending HELLO toNode->1
Sending HELLO toNode->1
Sending HELLO toNode->1
Node->10 is not misbehaving
Node->10 packet received
```

Figure 9: Transfer of packet from node 1 to node 10

The Figure 7 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. Figure 8 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. Figure 9 shows the transfer of packet from node 1 to node 10.Here node 10 is not misbehaving.

5. Conclusion and future scope

Many researchers have worked on finding different ways to find nodes of abuse. The main purpose of the routing algorithm is to find the most suitable route from the source to the desired destination in the network. There is situation when node in the middle of the network does not send the acknowledgment to the source node when sending packets. Then such nodes in the network are called malicious nodes. So, a technique is mentioned in this method to detect this malicious node. Therefore, studies must be performed to identify malicious nodes in the network. Various attacks occurring in MANET are also described. The watchdog has good network throughput, but it suffers from various disadvantages that have been somewhat solved by other technologies. X Watchdog fixes abuse reporting problem. 2ACK and AACK reduce root overhead, respectively, and reduce network overhead. And new algorithms have been proposed to detect malicious nodes. Identifying malicious nodes is very important for detecting security attacks on ad hoc networks. The misuse of nodes in ad hoc networks can be as varied as selfish nodes. This paper attempts to analyze the offensive node in the CGSR routing protocol in a mobile ad hoc network. Due to their ease of use, mobile ad-hoc networks are widely used and have little time to set up. Because of their dynamic nature they are vulnerable to internal and external attacks. The mobile ad hoc network has a decentralized security system. The proposed algorithm better identifies the abused node. In addition, this function can be extended for a short time to detect the misused node.

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 Misbehaviour Activities in Mobile Adhoc Networks”, IJCSIT, Vol. 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, fair-ness, and robustness in mobile ad hoc networks”, In Proceedings of EUROMICRO- PDP‟02, 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 Communications and Multimedia Security Conf., Sept. ’02.

[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", Techical Report, Stanford University, ’03.

[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,* 2009, pp. 48-54.

[16] Y. Yan, L. Ci, Z. Wang, and W. He, “QoS-based gateway selection in MANET with Internet connectivity,” *15th Int. Conf. AdvancedCommunication Technology (ICACT)*, 2013, pp.195-199.

[17] 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.

[18] 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.

[19] Garg, Puneet, “Distributed Denial of Service attacks in Mobile Ad hoc Networks”, National conference in advances in Computational Intelligence (NCACI-2011), Rohtak, Haryana, July, 2011