International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal
ISSN No: 2456 - 6470 | www.ijtsrd.com | Volume - 2 | Issue – 4

Research of Malevolent Node in CGSR Network

Neha, Ranjan Kumar Singh
Electronic Communication, S.R.C.E.M, Palwal, India

Abstract-- Detection of malevolent nodes is required to be studied in detail because wireless network work on dynamic topology, many types of problems arise in the network. Each node transmits the message from one node to another node and transfers the source to the build between the nodes. A MANET is a group of multi-hop wireless ad networks. Each node communicates in a radio communication range and adhoc network is a collection of wireless networks. MANET has applied in various types of military, disaster prone areas. MANET is weak due to various attacks due to its open medium. Destination in wireless network. This network is not perfectly safe and secure. Each device in MANET is free to move independently in any direction. Since the nodes are free to move, any node can connect or discard the network at any time.

Keywords—*AACK (Adaptive acknowledgment), MANET, CGSR, Routing, Network*

I. INTRODUCTION

A. Cluster head gateway switching routing protocol

CGSR is a multichannel operation protocol. All the node that are current 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

1. The general algorithm works in the following process. Source sends the packet to the cluster-head and cluster-head transmit the packet to gate way node that attach to the cluster-head and next cluster-head according to the route of destination. In fig 1 show that gate way node attach to the cluster –head that transmit the packet to the destination.
2. CGSR, nodes are grouped into the cluster and it is a cluster based routing table that lists all existing destination. CGSR protocol uses the DSDV (Destination-Sequence Distance-Vector) routing algorithm as the fundamental routing scheme that is based on hierarchical cluster head-to-gateway routing.
3. In a moveable network cluster head scheme can cause performance decline due to frequent cluster-head the CGSR uses a LCC (Least Cluster Change) algorithm.
4. In LCC, by any reason of any node transfer out from the range of all cluster-heads, the cluster-head altered. If during the change in the network two clusters -heads comes into one cluster then cluster-head altered.

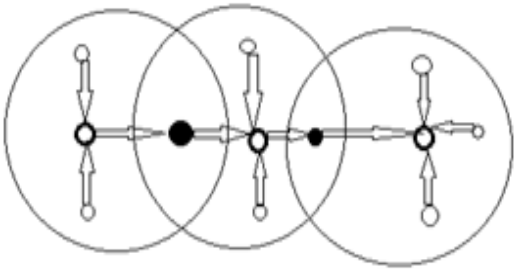

Figure1: Cluster Gateway Switching Routing Protocol

II. RELATED WORK

Literature review is a path of recognizance, 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 quest strategy.

Indhumathi. J, Prem Jacob.T [1,9] proposed an algorithm named as fast key generation in which TTL is assigned to the network. 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] Ex-Watchdog is an extension of watchdog. 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.

This algorithm for "**Detection of misbehaving node and selection of gateway node in MANET**" is based on mechanism to identify the misbehavior node. The proposed work will leads to the identikit of misbehaving node more purely. 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.

III. NODE MISBEHAVIOR

In ad-hoc network malevolent node is critically important to detect security attack in the network. In ad-hoc network ,there are two different types of selfish node Selfish node is type of node that do not intelligible to harm the other node straight, but most of the time they do not cooperate saving battery life for own contact and communication. Malevolent nodes do not give precedence to save battery life and focused at damaging other node. .In MANET there are three routing behavior of routing nodes.

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.

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.

Passive Selfish Node: Type 2:-Passive selfish node does not helps any of the activity like data transmit and catching, 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 rate 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 neighbors 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.

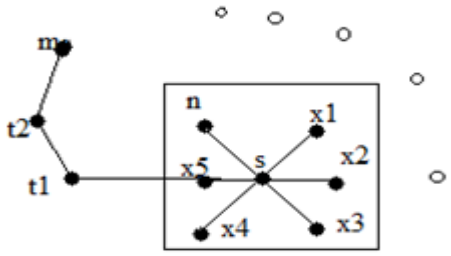

Figure 2: Selfish behavior of node separation

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:

Malevolent Node: Malevolent 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.

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.

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.

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

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

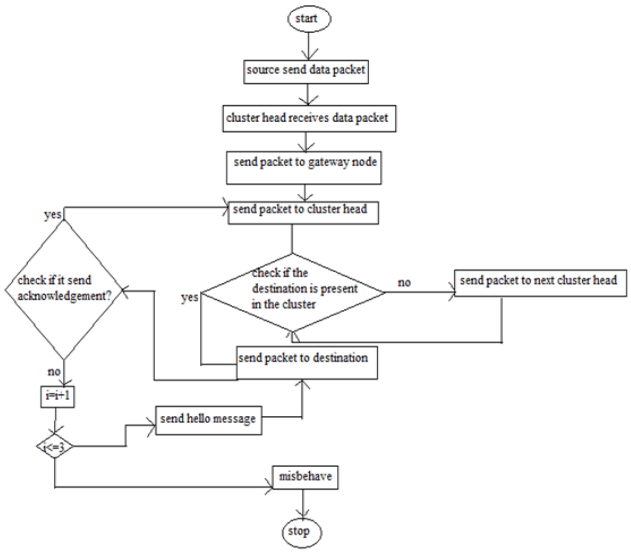

Figure 3: Use of Flow chart to find the detection of misbehaving node

V. SELECTION OF GATEWAY NODE IN CGSR

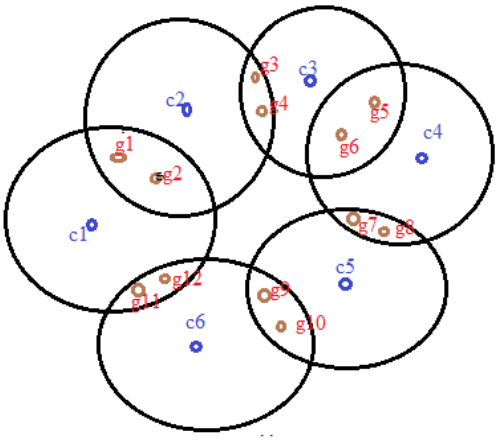

Figure 4: Gateway Node with Cluster

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

Table 1: For Network Gateway Nodes are Available

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

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

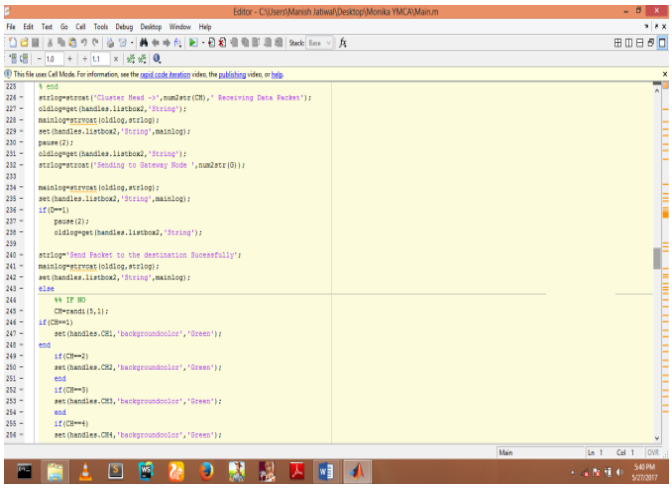

Figure 5: MATLAB program for identification of misbehaving node

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.

CONCLUSION

Many researchers have to recognize the different method for searching the misbehaving of nodes. Searching the best route is the main aim of routing algorithm from source to destination. One more problem find during the sending of packet, one of the node from the network not send the acknowledgement to the source. These nodes in the network named as malevolent nodes we mention one method to recognize that kind of malevolent nodes in the paper. Let us study to identify such malevolent nodes in the network. Different attack possible by MANET are also describe. Watchdog suffer many disadvantages and it has a good network throughout. These disadvantages are resolved by applying some other method. 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.

VII. FUTURE WORK TO BE CARRIED

Mobile ad-hoc network are widely used network due to their flexibility in nature that is easy to diffuse and low time to maintain. These are exposed to internal and external aggression due to their movable 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.

VIII. 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 Research 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, fairness, 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," 1st Int. Conf. Information Science and Engineering (ICISE), 2009.