International Journal of Engineering Applied Sciences and Technology, 2018
Vol. 2, Issue 12, ISSN No. 2455-2143, Pages 66-68
Published Online April 2018 in IJEAST (http://www.ijeast.com)

SURVEY OF SELFISH NODES IN MANET

AMAN
M.Tech Scholar
SKITM , Bahadurgarh, India

Shabnam Sangwan
Asst. Professor CSE
SKITM, Bahadurgarh India

***Abstract*— Ad hoc network refers to a network connection built for a single session and does not require a wireless base station and a router, it is a temporary network association made for some particular reason like for sending date from one device to other. If the network is set up for a long period of time, then it is just a plain old local area network.**

***Keywords*— MANET, DSR, MALICIOUS NODE**

I. INTRODUCTION

The mobile adhoc network is an integration of more than one wireless nodes and have the capacity of transferring data to one another without any kind of help from a centralized administrator. Every device acts as a router and end system in adhoc network. The network topology in a wireless adhoc network is dynamic due to the integration of the nodes changing with time because of the mobility of nodes, entry of new nodes and fight of nodes. Hence, a productive routing protocol is needed for these nodes to communicate.

Quick and unusual topological changes, wireless network dynamic nature, mo-bility of nodes and restricted battery power raise numerous difficulties in making up a routing protocol. Because of huge challenges in planning a routing protocol for MANET, various developments recently focusing on giving ideal solution for routing. Thus, an ideal routing protocol that can cover the greater part of the user requirements or applications and additionally adapt upto the stringent conduct of the wireless medium is constantly alluring

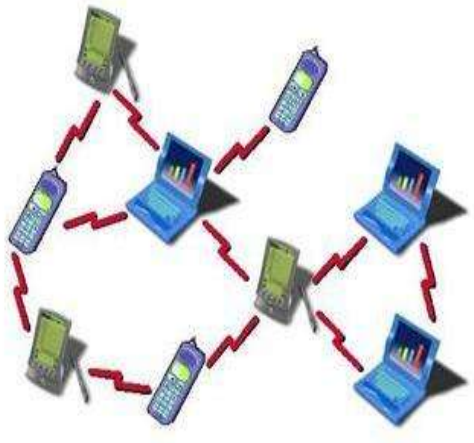

Figure 1.1: Ad hoc Network

II. CLASSIFICATIONS OF AD HOC NETWORK

Ad hoc networks can be classified on the essence of the network size, node con figuration, topology and the communication procedure (multihop/singlehop).

A. Classification based on the communication

In ad hoc networks communication can be either multihop or singlehop, depending on the configuration. Singlehop ad hoc network In single hop network all the devices which are in the communication range can communicate directly without the aid of any other devices. All these nodes are dynamic; however they must be in the communication energy of all nodes, which tells that whole network moves as a group.

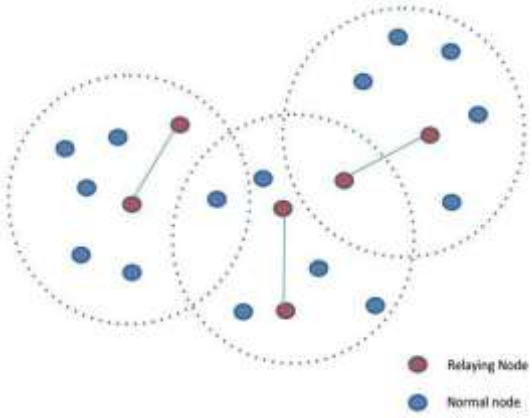

Figure 2: Single-hop Ad hoc network

Multihop adhoc network. In multihop network intermediate nodes can help in communicating if the nodes are out of communication range. The traffic of these end nodes are forwarded through some intermediate nodes. The difficulty of the network is the mobility of nodes where by the topology of the network alters continuously

B. Classification based on the node configuration

Based on node configuration of the hardware, ad hoc network is further classified.

Homogeneous Ad hoc Network in this network, all nodes have the same qualities, seeing the hardware setup as peripheral devices, display, memory and processor. Most will know wireless sensor network is the representation of homogeneous network.

International Journal of Engineering Applied Sciences and Technology, 2018
Vol. 2, Issue 12, ISSN No. 2455-2143, Pages 66-68
Published Online April 2018 in IJEAST (http://www.ijeast.com)

Heterogeneous Ad hoc Network in this network, the nodes contrast as per the hardware configuration. Each node has distinctive qualities, assets and arrangements. In this kind of ad hoc network all the nodes do not provide same kind of services.

C. Classification based on the topology

Based on the topology ad hoc network is classified. Every single node in an adhoc networks are divided with specific functions such as aggregate, hierarchical and at ad hoc network.
Flat Ad hoc Network In this network, there is no difference between every single node, all nodes convey same responsibility. All nodes are equivalent the ad hoc network.

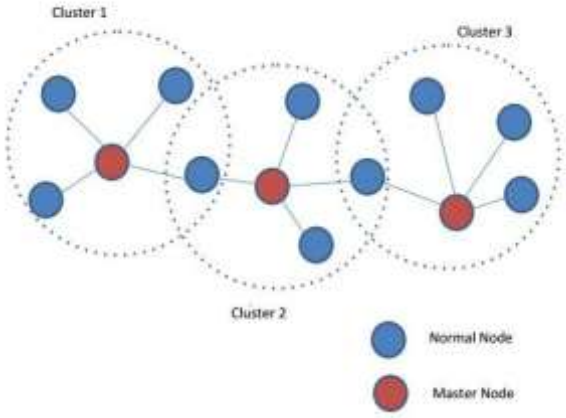

Figure 1.4: Hierarchical Ad hoc network

This kind of network comprises of many clus-ters, every cluster is considered as a network and all they are connected together. The nodes in hierarchical network can be ordered into two sorts.

Normal node: These nodes communicate directly with in the cluster and communicate with nodes in other cluster with the help of the master node.

Master node: These nodes administrate the cluster and are responsible for transferring data to another cluster.

III. SECURITY ISSUES

Due to the lack of central authority and resource constraints MANET is much more vulnerable to various attacks. They can be classified by the location of the attacker or by the mode of operation. They can be classified as internal attack or external attack, depending on the attacker's location. Also, attacks can be grouped as Active or Passive, depending upon the damage it causes to the network

A. Passive Attack

When an intruder launches the passive attack, the network continues to operate normally as there is no alteration being made to the network traffic. The attacker silently listens to the network traffic, without tampering it. The security service of confidentiality is violated here. As there are no visible changes in the network traffic, this kind of attacks is very di cult to detect. Brief information about various passive attacks is as follows.
Traffic Analysis: An intruder captures and analyzes the network traffic to know the destination information, source information.

Eavesdropping: The primary objective to launch this attack is to gain some secret information that can be later used to launch another attack. The information stolen can be passwords, private keys, locations of the nodes, etc.

B. Active Attack

This type of attack disrupts the normal behavior of the network. The attacker listens to the traffic as well as does the modification to it. An attacker may destroy the packets or alter some information in it. brief information about active attacks is as follows.

a. Network Jamming: It is a type of denial of service attack. The attacker tries to block the legitimate communication. It does so by not allowing source node to send out data packets. An attacker can also prevent a receiver from receiving the traffic from the network.
b. Fabrication: A malicious node creates its forged packets and sends it out to the network. In such attack, the malicious node does not modify or interrupt the original packets in the network. The forged packets consume the bandwidth and other network resources.
c. Black Hole Attack: This attack has two stages. Firstly, the malicious node advertises false route information and thus forces to route the data traffic to pass through it. And then this malicious node drops the received data packets without forwarding them to the destination node.
d. Wormhole Attack: An attacking node capture and stores the packets in one place in the network and transmits them to another location in the network. The attack causes more damage when control packets are tunneled. The wormhole refers to this tunnel between the malicious nodes.
e. Repudiation: The attacking node denies the responsibility of participation in part or entire communication.
f. Denial of Service attack: An attacker mood the

network with garbage traffic in gigantic amount, which causes unnecessary resource consumption. This traffic consumes network bandwidth and thus stopping the legitimate traffic to ow into the network. The actual users can not avail the services of the network.

IV. CONCLUSION

The principle target of this sort of selfish node is hiding itself and to abstain from being included in the others transmission way. Because of this kind of selfish behavior whole network will be paralyzed. In AODV, the source node will get a RREP message from the destination node through some intermediate nodes to establish a complete transmission path, but here the communication path will not be established because this kind of selfish nodes will not forward the RREP message. Hence the source node will broadcast Route Request(RREQ) message continuously.
It is a scheme for selfish node detection in MANET by overhearing other nodes. A buffer is maintained by each node for the packets sent recently and the packets within the buffer are compared with overhearing packet to check if there is a duplicate. Then the packet in the buffer is discarded and blank out by the watchdog. If the packet has stayed longer than a certain time-out in the bu er, then the watchdog will increase the fault count for the node culpable for sending the packet. If the count crosses some threshold, the node is considered to be misbehaving and a message about this node is sent to the source.

Total number of packets incoming are equal to total number of packets out-going in watchdog. Watchdog is presented in every node in the network. In the following Fig 3.1. Node S is a source and node D is a destination. Node S forward the packets to node Watchdog present in node S overhears the neighbor node A whether it forward the packets to neighbor node B. Here node A forward the pack-ets to node B. Similarly, watchdog present in node A overhears whether node B forward the packets to node D. The problem with watchdog is partial dropping, false misbehavior, limited transmission power, receiver collisions and ambiguous collisions might not be detected. The watch dog method discuss in second paper.

V. REFERENCE

[1] Wu, Lien-Wen, and Rui-Feng Yu. "A threshold-based method for selfish nodes detection in MANET." Computer Symposium (ICS), 2010 International. IEEE, 2010.

[2] Liu, Kejun, et al. "An acknowledgment-based approach for the detection of routing misbehavior in MANETs." Mobile Computing, IEEE Transactions on 6.5 (2007): 536-550.

[3] Kargl, Frank, et al. "Advanced detection of selfish or malicious nodes in ad hoc networks." Security in Ad-hoc and Sensor Networks. Springer Berlin Hei-delberg, 2005. 152-165.

[4] Buttyn, Levente, and Jean-Pierre Hubaux. "Stimulating cooperation in self-organizing mobile ad hoc networks." Mobile Networks and Applications 8.5 (2003): 579-592.

[5] Safaei, Zahra, Masoud Sabaei, and Fatemeh Torgheh. "An effcient reputation-based mechanism to enforce cooperation in MANETs." Application of Informa-tion and Communication Technologies, 2009. AICT 2009. International Con-ference on. IEEE, 2009.

[6] Tarannum, Rubana, and Yogadhar Pandey. "Detection and deletion of self-ish MANET nodes-a distributed approach." Recent Advances in Information Technology (RAIT), 2012 1st International Conference on. IEEE, 2012.

[7] Processing, IEE Proceedings -, vol. 152, pp. 561-574, 2005.

[8] Samreen, Shirina, and G. Narasimha. "An e cient approach for the detection of node misbehaviour in a MANET based on link misbehaviour." Advance Computing Conference (IACC), 2013 IEEE 3rd International. IEEE, 2013.

[9] Gonzalez, Oscar F., Michael Howarth, and George Pavlou. "An algorithm to detect packet forwarding misbehavior in mobile Ad-Hoc networks." Integrated Network Management, 2007. IM'07. 10th IFIP/IEEE International Symposium on. IEEE, 2007.

[10] Marti, Sergio, et al. "Mitigating routing misbehavior in mobile ad hoc net-works." Proceedings of the 6th annual international conference on Mobile com-puting and networking. ACM, 2000.

[11] Molva, R., and P. Michiardi. "Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks." Institute Eurecom-Research Report RR-02-062 (2001).