Detection and Mitigation of Malicious node in MANET

***D.K.Aarthy[1], V.Ashok[2]**

[1,2] Assistant Professor, Department of Computer Science and Engineering, Rajalakshmi Institute of Technology

***ABSTRACT**:* **MANETs is formed dynamically based on the infrastructure requirement. Medium of communication between the nodes in the MANETs is forwarding the packets from sender to receiver through multi hop wireless links. The network is intended with an assumption that all nodes would forward the packet that it receives from the next node on the hop, but a misbehaving node drops the packet since it wants to preserve the scarce resources and use it for its own packet transfer. The node acts selfishly. This behavior of selfish nodes greatly affects the performance of the network. It is very much significant to identify and detach such misbehaving nodes from the network. A numerous number of solutions have proposed to overcome this problem. A detailed study of such node detection and mitigation scheme is discussed.**

Keywords: MANET, Selfish node, mitigating misbehaving node, DTN.

1. INTRODUCTION

Mobile Ad Hoc Network is a collection of mobile nodes that are created dynamically based on the requirement. It is a network without a permanent infrastructure like the LAN. It does not have a fixed base stations or access points. This feature of MANET makes it popular and used in wide areas such as crisis management and civilian applications. In crisis management, mobile nodes are positioned in the battlefield, emergency search and rescue operations [1]. In civilian application MANETs allows communication between mobile nodes in conference halls and malls. In later, former application the mobile nodes are positioned to perform a common goal, whereas in the latter case, nodes belong to a different category of people. The working of MANET depends on the teamwork of mobile nodes. Hence we cannot expect all the nodes to cooperate with each other to forward the packets. Few nodes act selfish and do not forward packets of another node in order to save its resources. Such nodes are selfish/ misbehaving nodes. The resources are battery powered, computational power and bandwidth. But these nodes try to use the resources of other nodes to transfer its own packets.

MANET possibly will contain selfish node which utilized the maximum network resources, but unwilling to use it for another node. In [2,3] authors have identified the behavior of selfish nodes and they are as listed:

(i) TYPE 1: It forwards the data packet, but does not transfer the data messages purposely to the other nodes in the network.
(ii) TYPE 2: The node does not forward the data packet or the routing packets. It may modify the Route Request and sends back packets by altering the Time to live value to the least possible one.
(iii) Type 3: It changes its behavior by dropping packets based on the availability of the systems energy.
(iv) Type 4: It forwards the routing messages with a delay.

2. Data Forwarding Threats

1. Dropping data packet attack

Node's misbehaving character can be classified as follows

Malfunctioning

These type of nodes are called malfunctioning node when they undergo hardware or software failures.

3. Techniques for mitigating selfish activities

The experimental analysis conducted in [4] with 50 mobile nodes shows that th ratio of packets delivered was decreased by 50% when the available 50 nodes were acting selfishly. The routing algorithms carry out two main responsibilities: Routing and data forwarding. The routing protocol works accurately only when trusted mobile nodes are available. However the trusted atmosphere is unavailable when there exist misbehaving node. This affects the performance of the network and it is open to many attacks launched by misbehaving node.

3.1 Watchdog

Marti [5] proposed a scheme based on reputation in which watchdog and pathrater are added at every node. Buffer of recently sent data or forwarded data ia maintained by the watchdog. When the watchdog overhears that packet has been forwarded by the successor node, only then the buffer is empty. The amount of time the data resides in the buffer if it exceeds a threshold value, then it is assumed that the next node is malicious.

Pathrater maintains a rating table for all the node in the network and calculates path metric. It is done by finding the mean of the node rating in the path and then the algorithm chooses the best path.

Drawback

This technique cannot detect misbehavior when there are situations such as collisions, false misbehavior and partial drop of the packets.

3.2 CONFIDANT

Buchegger[6] proposed CONFIDANT protocol. In this protocol, trust associations and routing decision are based on experienced, observed, or reported routing and forwarding behavior of other nodes. It comprises four components: The monitor, the reputation system, the path manager, and the trust manager. Each node keeps an eye on the activities of the next hop node constantly and if any divergence observed then it is moved on to the reputation system. Then the reputation system alters the rating of the alleged node, which relies on how regular the action is. When the rating of the alleged node falls down a threshold value the path manager comes in action. The path manager gearshift the route. Warning message as an alarm message is broadcasted to other nodes in the network by the Trust Manager.

Drawback

It can generate false alarm, two nodes can declare each other misbehaving through alarm message.

3.3 TWOACK

In order to avoid selfishness in MANET a TWOACK scheme is proposed by Balakrishnan[7], which can be implemented as an add on to any routing protocol.

In this method, the TWOACK detects misbehaving link and it will avoid that link in the routing protocol to be used in the future. It does not detect a specific misbehaving node but instead detects misbehaving link.A TWOACK packet is sent on the victorious delivery of all the packets in the network.

Drawback

Sometimes a proper node will be part of the malicious node route which might not be used further. Hence many proper node resourses are wasted due to this.

3.4 Extension to TWOACK

An extension to the TWOACK scheme is proposed by Usha and Radha [8]. In this each node should send a ACK to its previous hop.. An ACK(Nack) should be sent from the destination to the source. On receiving the data packets sent by the source, the destination replies it with Nack. When the Nack reaches the source through the routing path which is available in the actual data that was sent to the destination. If the node is identified as malicious then the will node will divert the Nack to an alternate path. Now this modified path shall be stored along with the older path in the Nack, that can be obtained from the original message. On receiving the Nack the source evaluates the two paths. If any deviation is found out, then the node from which variation is out-of-the-way and the node is mentioned as misbehaving node by the source node else it is concluded that there are no misbehaving node in that path by the source.

Drawback

The potential drawback is that the algorithm includes lot of routing operating cost because of Ack and Nack packets.When there are larger number of nodes, the probability of Nack reaching the source becomes smaller. This happens due to nodes mobility.

3.5 Two-fold approach

Zeshan[9] has proposed a two-fold approach to identify and segregate nodes that drop packets. It aims to identify the misbehaving node. Every intermediate node should send an ACK to confirm the onset receipt of packets. When the ACK is not received by the source node, the packets are resent to the destination node by the source after a period of time.

When the same activity is find out then source node sends a broadcast msg to announce that there is a malicious action in the network.

Another approach is to identify which intermediate node is behaving malicious. It is to be identified by monitoring the intermediate nodes of active route by the nodes which are near to active path.

The work of monitoring node is to count number of incoming and outgoing packets. It also maintains a list of sent and dropped packets. When the dropped packets count of a node exceeds the threshold, then the node will be declared as misbehaving by the monitoring node and will broadcast this information. Once the broadcast is received all the neighboring node will abandon their transmission to the misbehaving node. Now this node will be entered into the record of misbehaving node.

Drawback

The main disadvantage of this scheme is the overhead due to transmission of acknowledgement packets by every intermediate node to the source. The second disadvantage is the working of every node in the promiscuous mode.

3.6 CORE

CORE[10] is a mechanism based on reputation to bring about mutual aid among every node in the MANET, to avoid selfish activity. Every node keeps track of the other nodes association using a procedure called reputation.

The reputation is calculated depending on different types of information on the node's pace of collaboration. In this scheme the following three mechanism are used:network entity, reputation table and the watchdog mechanism.

The network entity will be a mobile node and every node will have a set of repute table(RT) and a Watchdog mechanism(WD). The CORE scheme uses two different types of protocol entities, a requester and one or more providers. A requester is an entity that asks for the implementation of a function F and the contributor is any entity that correctly executes F.

CORE do not permit a node to allocate negative ratings about other nodes and can resist itself to DoS attacks.

REFERENCES

[1] J. Hoebeke, I. Moerman, B. Dhoedt and P. Demeester, "An overview of mobile ad hoc networks: applications and challenges ", Journal- Communication Network, vol.3, no 3, pp60-66, 2004.

[2] S.Subramaniyan, W. Johnson and K. Subramaniyan, "A distributed framework for detecting selfish nodes in MANET using Record and Trust Based Detection (RTBD) technique", EURASIP Journal on Wireless Communications and networking, vol. 2014, no. 1, 2014.

[3] J. Sengathir and R. Manoharan, "Exponential reliability coefficient based routing mechanism for isolating selfish nodes in MANETs", Egyptian Informatics Journal, vol.16, no.2, pp231-24, 2015.

[4] F. Kargl, A. Klenk, S. Schlott and M. Weber, "Adavanced detection of selfish or malicious nodes in ad hoc network", In Security in Ad- hoc and Sensor Networks Springer Berlin Heidelberg, pp.152-165, 2004.

[5] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," in Proc. of the Sixth Annual International Conference on Mobile Computing and Networking (MobiCom 2000), August 2000, pp. 255-265.

[6] Sonja Buchegger Jean-Yves Le Boudec, "Performance Analysis of the CONFIDANT Protocol Cooperation Of Nodes Fairness In Dynamic Ad-hoc NeTworks" in Proc. IEEE/ACM Workshop Mobile Ad Hoc Netw. Comput. (MobiHoc 2002), June 2002, pp. 226-236.

[7] K. Balakrishnan, D. Jing and V. K. Varshney, "TWOACK: Preventing Selfishness in Mobile Ad hoc Networks," in Proc. of Wireless Communications and Networking Conference (WCNC'05), vol. 4, March 2005, pp. 2137-2142.

[8] S. Usha, S. Radha, "Co-operative Approach to Detect Misbehaving Nodes in MANET Using Multi-hop Acknowledgement Scheme," in 2009 International Conference on Advances in Computing, Control, and Telecommunication Technologies, December 2009, pp. 576-578.

[9] Muhammad Zeshan, Shoab A. Khan, Ahmad Raza Cheema, and Attique Ahmed, "Adding Security against Packet Dropping Attack in Mobile Ad Hoc Networks," in 2008 International Seminar on Future Information Technology and Management Engineering, November 2008, pp. 568- 572.

[10] P. Michiardi, R. Molva, CORE: A Collaborative Reputation Mechanism to enforce node cooperation in Mobile Ad Hoc Networks, Research Report RR-02-062, 2001.