Routing layer Node Misbehavior Detection in Mobile Ad hoc Networks using N-ack Scheme

Usha.Sakthivel and Radha.S

Abstract— Wireless Mobile ad hoc Networks suffer from a great efficiency loss due to the individual nodes that are constrained by the resources such as battery power and bandwidth. Misbehaving nodes makes the routing process a tedious task. As a result of this hefty performance degradation ropes in network throughput, packet delivery ratio, packet loss increment, etc. To mitigate this problem of routing layer node misbehavior, we analyze the existing misbehavior detection schemes and propose a novel solution. Multi hop acknowledgement is used in this scheme to detect misbehaving nodes.

Keywords— MANETS, AD HOC networks, AODV, Misbehaving nodes, N-ack.

I. INTRODUCTION

ROUTING the packets is considered as one of the difficult task which has paved way to be the primary instigator and the defying aspect in the rise of Mobile Ad hoc Networks (MANET). The main area of consideration associated with the routing techniques that are employed for MANETS are the one that has the capacity to have ultra dynamic topology of the nodes and the requirement of each node to be routers themselves. The area of concern in this routing is when the nodes become selfish and tend to project its misbehavior.. Some have used the optimistic strategy of encouraging the nodes to forward packets. These techniques [5] & [6] have been drafted with some or most of the parameters viz the routing overhead, packet delivery ratio and THROUGHPUT in mind. The credit based schemes have been the ones which are optimistic by promoting the forwarding of packets by each node. Some of the widely acclaimed techniques include Packet Purse Model and the Packet Trade Model [1].The reputation based schemes involved having separate modules which would take care of the job of detecting misbehaving nodes in the neighborhood. The techniques include watchdog, path rater [2]. Finally, the end to end schemes were expected to be the panacea for all routing problems. They depended on explicit acknowledgements between nodes. A couple of those techniques were the 2ACK [3] scheme. We begin by introducing each of these techniques one at a time discussing their pros and cons and finally propose a theory which attempts to present an explication for all of the problems.

II. RELATED WORK

PPM is one of the credit based methods in which the forwarding of packets by intermediate nodes is encouraged by providing some resources other than physical, the presence of which is made indispensable for sending packets in the future. In the PTM model each node has to buy the packets for a certain no of nuggets and can sell it to the next node for some amount of nuggets. This ensures that the packet purse which contains the nuggets need not be carried all along the path. The WATCHDOG methodology is used to detect misbehaving nodes. The Watchdog method uses the passive method of over hearing the links of the next node to see whether they have forwarded the packet. In cases where there is no link encryption, the nodes can even check for the integrity of the messages. PATHRATER model [2] proposes to use link data as well as misbehaving node data to select a path. Each node maintains a metric for every node that it knows. And each node also maintains a metric for each path it knows. So if a node finds that there are various paths that could be used to reach the destination, it chooses the one with the highest metric. The 2-ACK scheme [3] is a network layer technique to detect misbehaving links. It defines a packet (2-ACK packet), which has a fixed route of two hops in the direction opposite to the original packet flow.

III. PROPOSED SCHEME

A. N-ack scheme

B. The Nack scheme is an extension to the 2 Ack scheme in trying to isolate misbehaving nodes in a MANETs. The Nack scheme has a prerequisite of an end to end Ack packet to be sent between the source and the destination. The destination on receipt of the data packets sent by the source, responds with a Nack packet. Each node maintains a list of data packets sent and another list of data packets forwarded. As soon as a node initiates a data packet as a source, it adds the id of the packet to the list of data packet sent. As the node receives the Nack packet for the data packet it removes the corresponding data packet id from the data packet sent list.

C. The data packet and the Nack packet keep track of the route they travel. The Nack would try to reach the source from the destination with the help of the path, which is found in the actual message packet, delivered to the destination. If a node is found to be misbehaving in the pre calculated

Usha.S, is with the research student in Sathyabama University, Chennai, India (corresponding author to provide phone:9677034469; e-mail:usaha_sakthivel@yahoo.co.in).

Radha.S, is with SSN college of Engineering (e-mail: radha_kumaran@yahoo.co.in).
path, the intermediate nodes are free to divert the Nack packet through alternative paths. But the new path will be stored in the Nack packet along with the older path, which is extracted from the original message.

D. On receipt of the Nack packet, the source node compares the two paths that are in the Nack packet. If there is no variation in the paths, then the source node concludes that there are no potential misbehaving nodes in the path. In case the two paths vary, the node in the source to destination path, from where the path varies in the destination to source path is isolated. This node is marked as a potential misbehaving node by the source node. For each potential misbehaving node, a threshold is maintained. If the number of times a node is adjudged as a potential misbehaving node exceeds the threshold, then the node is flagged as misbehaving and information is sent to all the neighboring nodes advising them about the misbehaving node. Further each node must send back a normal Ack to its immediate source node after receipt of any kind of packet. This would help the intermediate node to judge about its immediate neighboring node and advice the other nodes about the credibility of the neighboring nodes.

E. The process is similar to the protocol followed by a source node to keep track of data packets initiated. Here the intermediate nodes keep track of the forwarded data packets and Nack packets in the forwarded message packets list. The judgment of a neighboring node as potentially misbehaving node is done when an Ack is not received within a pre set time out.

F. As before, the number of times a neighboring is termed as potentially misbehaving node determines whether or not it should be termed as a misbehaving node. To consider the case in which the Nack packets are lost, the source node will wait for a certain time out period and then re send the original data packets assuming the data packets were lost.

G. If the Nack packet is lost either due to misbehaving nodes or some other reason, the destination would receive the same packet again. This should prompt them about the fact that the Nack it sent has not reached the source. Considering it as the work of misbehaving nodes the destination now should go for an alternating path. If the problem persists in multiple paths the common node in the path could be isolated as the misbehaving node.

On the other hand if the data packets are lost in the first case, the destination would receive the data packets for the first time during the subsequent retransmission by the source node and would respond to it. The combination of Nack and Ack for Nack is effective in isolating misbehaving nodes in a MANET.

H. Algorithm

- N1 forwards the packet to N2 and waits for ack
- If ack fails to arrive within the stipulated time N1 retries for K times after which it announces N2 to be misbehaving
- Then node N1 waits for the arrival of the Nack packet from the destination
- It sets up a timer
- Each intermediate node maintains a list of IDs for a data packet sent on a path
- Each packet ID will stay for a time T
- If Ack arrives within T, the ID is removed
- Else ID will be removed after the timeout
- N5 has to send back the Nack packet to the source.
- Each intermediate node has to forward the Nack packet to the source in the same path in which the initial transmission took place
- Each intermediate node also has to send to its immediate source node an Ack packet
- Each node maintains a black list of potential misbehaving nodes
- If the ack is not received by a particular node then the node to which it has forwarded the packet and has failed to receive the ack is added to the list
- After K failed attempts to send the packet without receiving the ack - misbehaving node.

Simulation Results And Discussion:

The proposed N-ack was implemented in ns 2.32 as add on to the AODV protocol Simulation Utilizes the two mobility models like RWP,RPGM

Performance metrics:

a) Throughput
b) Packet delivery ratio (PDB)
c) Dropping packets

Throughput:

Throughput refers to how much data can be transferred from one location to another in a given amount of time

Packet Delivery Ratio:-

PDR= Packets Received / Packets Sent

Packet delivery ration is measured in terms of the ratio of
data packets received to packet sent.

Corresponding graphs are shown from figures under group mobility scenario and entity mobility scenario. The results show the overall throughput and packet delivery ratio of the proposed system is improved at the same time drop in packet ratio is decreased when compared to the existing system.

IV. CONCLUSION

The schemes which are designed since the development of MANET have a back lock of fulfilling some of the requirements of an ideal MANET environment. The proposed system has a great role in curbing the major disadvantages of the earlier scheme

REFERENCES