“Routing of Misbehavior Nodes in Manets Using Acknowledgement Method”

Bhagyashree S. Madan1, Prof. R. K. Krishna2

1Computer Science & Engineering, Rajiv Gandhi College of Engineering Research & Technology, Chandrapur, India.
2Department of Electronics Engineering, Rajiv Gandhi College of Engineering Research & Technology, Chandrapur, India.

Abstract— A Mobile Ad Hoc Network (MANET) is a collection of mobile nodes (hosts) which communicate with each other via wireless links either directly or relying on other nodes as routers. The operation of MANETs does not depend on pre-existing infrastructure or base stations. Network nodes in MANETs are free to move randomly. The nodes which drop the information to send forward considered as a selfish Node. Specifically, nodes may participate in the route discovery and maintenance processes but refuse to forward data packets. To detect such misbehavior and more efficient detection process, the 2ACK technique is analyzed. The main idea of the 2ACK scheme is to send two-hop acknowledgment packets in the opposite direction of the routing path. The 2ACK scheme detects misbehavior through the use of a new type of acknowledgment packet, termed 2ACK. Thus it detects the misbehaving nodes, eliminate them and choose the other path for transmitting the data. The main aim of this application is to detect the routing misbehavior in Manets that occurs due to the presence of selfish node. The input to the system will be the number of nodes with data transmission between them. The output of the system will involve detecting the misbehaving link and misbehaving node due to which the packet loss occurs.

Keywords— Mobile Ad hoc Networks (MANETs), misbehaving path, misbehaving nodes, packet loss, Route Discovery

I. INTRODUCTION

The structure of a MANET may vary from a small, static network that is highly power-constrained to a large-scale, mobile, highly dynamic network. Most wireless infrastructure-based networks are established by a one hop radio connection to a wired network. On the other hand, mobile ad hoc networks are decentralized networks that develop through self-organization.

MANETs are formed by a group of nodes that can transmit and receive data and also relay data among themselves. Communication between nodes is made over wireless links. A pair of nodes can establish a wireless link among themselves only if they are within transmission range of each other. An important feature of ad hoc networks is that routes between two hosts may consist of hops through other hosts in the network.

The source node will be able to choose an appropriate route to send its data. The 2ACK scheme is a network-layer technique to detect misbehaving links and to mitigate their effects. The 2ACK scheme detects misbehavior through the use of a new type of acknowledgment packet, termed 2ACK. A 2ACK packet is assigned a fixed route of two hops (three nodes) in the opposite direction of the data traffic route.

Selfish Nodes: An individual mobile node may attempt to benefit from other nodes, but refuse to share its own resources. Such nodes are called selfish nodes or misbehaving nodes and their behavior is termed as selfishness or misbehavior. One of the major sources of energy consumption in the mobile nodes of MANET is wireless transmission. A selfish node may refuse to forward data packets for other nodes in order to conserve its own energy.

The nodes of a MANET are actually mobile routers that build up routes dynamically. These routers can move randomly and insert themselves automatically into dynamic wireless topologies. They perform packet forwarding using the current routing information. A path form the source to the destination, that is, a route, can be established through well-known routing protocols such as the ad hoc on-demand distance vector routing (AODV), dynamic source routing (DSR). Selfish and malicious nodes take advantage of MANET idiosyncrasies to misbehave, or attack.

A. MANET Architectural Model

An architectural model for MANETs which preserves the integrity of the IP architecture while allowing for the particularities of MANET.An architectural model considers MANET nodes as routers with hosts attached, as shown in figure 1. These attached hosts may be “external” (i.e. attached to the router via other network interfaces) or “internal” – however the important observation to make is, that the links between these hosts and the router are classic IP links.

This implies that, from the point of view of the hosts, and the applications on these hosts, connectivity is via a classic IP link.
In MANETs, routing misbehavior can severely degrade the performance at the routing layer. Specifically, nodes may participate in the route discovery and maintenance processes but refuse to forward data packets. To detect such misbehavior and more efficient detection process, the 2ACK technique is analyzed. This the 2ACK technique detects misbehaving nodes or links. Routes containing such nodes will be eliminated from consideration. The source node will be able to choose an appropriate route to send its data. The 2ACK scheme is a network-layer technique to detect misbehaving links and to mitigate its effects. The 2ACK scheme detects misbehavior through the use of a new type of acknowledgment packet, termed 2ACK. A 2ACK packet is assigned a fixed route of two hops (three nodes) in the opposite direction of the data traffic route.

C. Misbehavior Nodes in Manet

Ad hoc networks increase total network throughput by using all available nodes for forwarding and routing. Therefore, the more nodes that take part in packet routing, the greater is the overall bandwidth, the shorter is the routing paths, and the smaller the possibility of a network partition. But, a node may misbehave by agreeing to forward packets and then failing to do so, because it is selfish, overloaded, broken, or malicious.

In MANETs, as there is no retransmission of packets once it is sent, hence care is to be taken that packets are not lost. Noting that a misbehaving node can either be the sender or the receiver of the next-hop link, we have focused on the problem of detecting misbehaving links instead of misbehaving nodes using 2ACK scheme.

In the next-hop link, a misbehaving sender or a misbehaving receiver has a similar adverse effect on the data packet. It will not be forwarded further. The result is that this link will be tagged. Our approach is used to discuss the significantly simplification of the routing detection mechanism and also checking the confidentiality of the message in MANETs environment.

II. Literature Review

David B. Johnson and David A. Maltz present a protocol for routing in ad hoc networks that uses dynamic source routing. First, unlike conventional routing protocols, our protocol uses no periodic routing advertisement messages, thereby reducing network bandwidth overhead; particularly during periods when little or no significant host movement is taking place. This paper has presented a protocol for routing packets between wireless mobile hosts in an ad hoc network. The protocol presented here is explicitly designed for use in the wireless environment of an ad hoc network. There are no periodic router advertisements in the protocol. Instead, when a host needs a route to another host, it dynamically determines one based on cached information and on the results of a route discovery protocol. Based on results from a packet-level simulation of mobile hosts operating in an ad hoc network, the protocol performs well over a variety of environmental conditions such as host density and movement rates [1].

Elizabeth Royer and C-K Toh provide a classification of these schemes according to the routing strategy (i.e., table-driven and on-demand). Challenges facing ad hoc mobile wireless networks. On-Demand Distance Vector (AODV) routing protocol described builds on the DSDV algorithm. Table-driven routing protocols attempt to maintain consistent, up-to-date routing information from each node to every other node in the network. These protocols require each node to maintain one or more tables to store routing information, and they respond to changes in network topology by propagating updates throughout the network in order to maintain a consistent network view [6].

Buchegger S. and Le Boudec J.-Y. Presents the CONFIDANT protocol works as an extension to a reactive source-routing protocol for mobile ad-hoc networks. Dynamic Source Routing is a protocol developed for routing in mobile ad-hoc networks. This paper recognizes the special requirements of mobile ad-hoc network in terms of cooperation, robustness, and fairness. Reputation systems are used in some online auctioning systems. They provide a means of obtaining a quality rating of participants of transactions by having both the buyer and the seller give each other feedback on how their activities were perceived and evaluated. [4].
Quansheng Guan, F. Richard Yu, Shengming Jiang In this paper, they focus on authentication and topology control issues. A joint authentication and topology control (JATC) scheme is proposed to improve the throughput. Simulation results have been presented to show that JATC works well in MANETs. The ultimate objective of JATC is to optimize the joint authentication and topology configuration to maximize the per node aggregate throughput capacity, i.e., the sum of all the throughput of links associated with the node. [7].

Erman Ayday, Faramarz Fekri presents in conventional Mobile Ad hoc Networks (MANETs), the existence of end-to-end paths via contemporaneous links is assumed in spite of node mobility. Define the packet delivery ratio as the ratio of the number of legitimate packets received by their destinations to the number of legitimate packets transmitted by their sources. [8].

Balakrishnan K., Deng J., and Varshney P. K present two network-layer acknowledgment-based schemes, termed the TWOACK and the S-TWOACK schemes. Selfishness, which is notably different from malicious behavior. Selfish nodes use the network for their own communication, but simply refuse to cooperate in forwarding packets for other nodes in order to save battery power. [3].

III. PROPOSED MODEL

The 2ACK technique differs from the ACK and the SACK schemes in the TCP protocol:

The 2ACK scheme tries to detect those misbehaving nodes which have agreed to forward data packets for the source node but refuse to do so when data packets arrive. TCP, on the other hand, uses ACK and SACK to measure the usefulness of the current route and to take appropriate action.

The proposed work (2ACK with confidentiality) is as follows.

- If the 2ACK time is less than the wait time and the original message contents are not altered at the intermediate node then, a message is given to sender that the link is working properly.
- If the 2ACK time is more than the wait time and the original message contents are not altered at the intermediate node, then a message is given to sender that the link is misbehaving.
- If the 2ACK time is more than the wait time and the original message contents are altered at the intermediate node, then message is given to sender that the link is misbehaving and confidentiality is lost.
- If the 2ACK time is less than the wait time and the original message contents are altered at the intermediate node then, a message is given to sender that the link is working properly and confidentiality is lost.

When Node 1 wishes to send the data packets to node 3, so in this process node 2 considered as an intermediate node. In figure 4, the path from node2 to node3 is seems to be misbehaving. After the proper timing sender get message the link is misbehaving.

For this first we have to implement a model connecting node in adhoc network and each node in an adhoc networking act as a client and act as destination. We are implementing here source and destination that source sending message to other node in a range and if the message received by other node, it sends back an acknowledgement to the source. When source get an acknowledgement source have conform that message is received by destination. The result is that this link will be tagged. Our approach is used to discuss the significantly simplification of the routing detection mechanism and also checking the confidentiality of the message in MANETs environment.
IV. ADVANTAGES OF 2ACK SCHEME

It solves the problems of ambiguous collisions, receiver collisions, and limited transmission power:

A. Ambiguous Collisions: Ambiguous collisions may occur at node N1. When a well-behaved node N2 forwards the data packet toward N3, it is possible that N1 cannot overhear the transmission due to another concurrent transmission in N1’s neighborhood. The 2ACK technique solves this problem by requiring N3 to send a 2ACK packet explicitly.

B. Receiver Collisions: Receiver collisions take place in the overhearing techniques when N1 overhears the data packet being forwarded by N2, but N3 fails to receive the packet due to collisions in its neighborhood. A misbehaving N2 will not retransmit the data packet, which costs extra energy. Again, the 2ACK technique overcomes this problem due to the explicit 2ACK packets.

C. Limited Transmission Power: A misbehaving N2 may maneuver its transmission power such that N1 can overhear its transmission but N3 cannot. This problem is similar to the Receiver Collisions problem. It becomes a threat only when the distance between N1 and N2 is less than that between N2 and N3. The 2ACK scheme is immune to limited transmission power problem.

D. Limited Overhearing Range: A well-behaved N2 may use low transmission power to send data toward N3. Due to N1’s limited overhearing range, it will not overhear the transmission successfully and will thus infer that N2 is misbehaving, causing a false alarm. Both this problem and the limited transmission power problem are caused by the potential asymmetry of communication links. The 2ACK scheme is immune to the limited overhearing range issue.

V. EXPERIMENTAL RESULTS

Node 1 Wishes to send packets to node 3. Message forwarded from node1 but not receive by node 3 because the link is misbehaving. After Some time node1 get message that the path is misbehaving.
VI. CONCLUSION

When selfish misbehaving nodes participate in the Route Discovery but refuse to forward the data packets, routing performance may be degraded severely. The 2ACK scheme maintains packet delivery ratio even when there are misbehaving nodes in the MANET. The 2ACK scheme detects misbehaving node and reduces the number of ACKs.

For applying directly 2ACK Scheme on number of nodes, it is necessary to connect nodes in adhoc network and implement sending message and receiving acknowledgment between the nodes and after that applying 2ACK scheme for detecting misbehaving link and in this and then detecting the misbehavior node.

REFERENCES