Detection of Routing Misbehaving Nodes in Manet Using 2ACK Scheme

Prajakta Jadhav  
Information Technology  
Jayawantrao Sawant College of Engineering,  
Hadapsar Pune, India

Komal Lokhande  
Information Technology  
Jayawantrao Sawant College of Engineering,  
Hadapsar Pune, India

Pournima Kamble  
Information Technology  
Jayawantrao Sawant College of Engineering,  
Hadapsar Pune, India

Amruta Kollhal  
Information Technology  
Jayawantrao Sawant College of Engineering,  
Hadapsar Pune, India

Abstract: A mobile ad hoc network consists of nodes that communicate with each other directly or indirectly via wireless link. The nodes may attempt to benefit from other nodes, but some nodes refuse to share its own resources. Such nodes are called selfish or misbehaving nodes. The nodes in MANET moves freely and may change topology rapidly. These selfish nodes may severely affect the performance of network. Due to such type of node’s structure and scarcely available battery-based energy, node misbehaviors may exist. One such routing misbehavior is that some selfish nodes will participate in the route discovery and maintenance processes but refuse to forward data packets. In this paper, the 2ACK scheme is used. The 2ACK scheme serves a technique for routing schemes to detect routing misbehavior of node and to reduce their effect. The 2ACK scheme is to send two-hop acknowledgment packets in the opposite direction of the routing path. In this paper Dynamic Source Routing (DSR) protocol.

Keywords: Mobile Ad Hoc Networks (MANET), routing misbehavior, node misbehavior, network security, Dynamic source routing

I. INTRODUCTION
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. Therefore, the network topology of a MANET may change rapidly and unpredictably. All network activities such as discovering the topology and delivering data packets have to be executed by the nodes themselves either individually or collectively. Depending on its application, 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 MANET. Selfish nodes are individual mobile node may attempt to benefit from other nodes, but refuse to share its own resources. Such nodes are called as misbehaving nodes or selfish 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 dynamic source routing (DSR). Selfish and malicious nodes take advantage of MANET to misbehave, or attack.

II. TYPES OF MANETs
Closed MANET: In a closed MANET, all mobile nodes works on common goal i.e. emergency search, military and law enforcement operation.

Open MANET: In an open MANET different mobile nodes works on different goals.
III. DYNAMIC SOURCE ROUTING

3.1 Introduction of Dynamic Source Route:

The Dynamic Source Routing protocol (DSR) is a simple and efficient routing protocol designed specifically for use in multi-hop wireless ad hoc networks of mobile nodes. DSR is completely self-organizing and self-configuring, protocol. DSR is a self reactive protocol. The DSR protocol is composed of two mechanisms that network together to allow the discovery and maintenance of source routes in the ad hoc network:

a) Route Discovery: It is the mechanism which a node S wishing to send a packet to a destination node D obtains a source route to D. Route Discovery is used only when S attempts to send a packet to D and does not already know a route to D. The node discovery node route process is carried out when its needed so it is called as reactive routing protocol.

![Route Discovery](image)

Fig 3.2 Route Discovery

a node A is attempting to discover a route to node E. The ROUTE REQUEST message as a packet is send, which is received by all adjacent nodes of A. If multiple copies of same packet are received by a single node then the node discards packet. ROUTE REQUEST packet contains unique ID, a list of intermediate node information, source, destination.

When another node receives a ROUTE REQUEST, if it is target the Route Discovery, it returns a ROUTE REPLY message to the initiator of the Route Discovery.

3.3 DSR Route Maintenance:

When originating or forwarding a packet using a source route, each node transmitting the packet is responsible for confirming that the packet has been received by the next hop along the source route; the packet is retransmitted until this confirmation of receipt is received.

![Route Maintenance](image)

Fig 3.3 Route Maintenance

Route Maintenance indicates a source route is broken. If the packet is retransmitted by some node the maximum number of times and no receipt confirmation is received, this node returns a ROUTE ERROR message to the original sender of the packet, identifying the link over which the packet could not be forwarded. In Figure 3.3, if C is unable to deliver the packet to the next hop D, then C returns a ROUTE ERROR to A, stating that the link from C to D is currently “broken.” Node A then removes this broken link from its cache; any retransmission of the original packet is a function for upper layer protocols such as TCP. For sending such a retransmission or other packets it Discovers new Route for this target.[3].

3.4 Advantages of DSR

This protocol eliminates the need to periodically flood the network with table update messages which are required in a table-driven approach. In a reactive (on-demand) approach such as DSR, a route is established only when it is required and hence the need to find routes to all other nodes in the network as required by the table-driven approach is eliminated. The intermediate nodes also utilize the route cache information efficiently to reduce the control overhead. When there is already route exists, there is no need to find another route it is called as route caching.

IV 2-ACK Scheme

4.1 Introduction of 2ACK Scheme:

The proposed system is used to detect the misbehavior routing using 2ACK and also check the confidentiality of message in MANETs environment. Here, a scheme called 2ACK scheme, where the destination node of the next hop link will send back a 2 hop acknowledgement called 2ACK. It
indicate that the data packet has been received successfully.

4.2 System Model

Module 1: Sender module (Source node).
The task of this module is to read the message and then divide the message into packets of 48 bytes in length, send the packet to receiver through the intermediate node and receive acknowledgement from the receiver. After sending every packet the “Cpks” counter is incremented by 1. 2ACK time is compared with the wait time. If 2ACK is less than wait time, “Cmiss” counter is incremented by 1.

Module 2: Intermediate module (Intermediate node).
The task of this module is to receive packet from sender and send it to destination. Get 2ACK packet from the receiver and send 2ACK packet to sender.

Module 3: Receiver module (Destination node).
The task of this module is to receive message from the intermediate node, take out destination name and hash code and decode it. Send 2ACK to source through the intermediate node.

4.3 Working of 2ACK Scheme

Fig. 4.3 illustrates the operation of the 2ACK scheme. Suppose that N1, N2, and N3 are three consecutive nodes (triplet) along a route. The S is a source node and D is destination in the Route Discovery phase of the DSR protocol. When N1 sends a data packet to N2 and N2 forwards it to N3. It is not clear to N1 whether N3 receives the data packet successfully send or not. Such an ambiguity exists even when there are no misbehaving nodes

When node N3 receives the data packet successfully, it sends out a 2ACK packet over two hops to N1 (i.e., the opposite direction of the routing path as shown), with the ID of the corresponding data packet. The triplet \([N1 \rightarrow N2 \rightarrow N3]\) is derived from the route of the original data traffic. Such a triplet is used by N1 to monitor the link N2 \(\rightarrow\) N3. For convenience of presentation, we term N1 in the triplet \([N1 \rightarrow N2 \rightarrow N3]\) the 2ACK packet receiver or the observing node and N3 the 2ACK packet sender. To detect misbehavior, the 2ACK packet sender maintains a list of IDs of data packets that have been sent out but have not been acknowledged.

Each node receiving or overhearing such an RERR marks the link N2 \(\rightarrow\) N3 as misbehaving and adds it to the blacklist of such misbehaving links that it maintains. When a node starts its own data traffic, it will avoid using such misbehaving links as a part of its route.

4.7 Timeout for 2ACK Reception, \(\tau\)
The parameter \(timeout, \tau\), will be used to set up a timer for 2ACK reception. If the timer expires before the expected 2ACK packet is received, the missing 2ACK packet counter, \(Cmis\), will be incremented. Thus, an appropriate value of \(\tau\) is important for the successful operation of the 2ACK scheme.

It is clear that false alarms may be triggered if \(\tau\) is too small. On the other hand, if \(\tau\) is too large, the observing node will have to maintain a longer list, requiring a large memory size. Therefore, \(\tau\) should be set at a value that is large enough to allow the occurrence of temporary link failures (for example, the unsuccessful transmission due to node mobility or local traffic congestion).

It is essential that \(\tau\) should satisfy where a single-hop transmission delay includes packet transmission delay, random back-off delay at the Medium Access Control (MAC) layer, data processing delay, and potential retransmission delay.
4.8 Observation Period, Tobs, and Dynamic Behavior

The 2ACK scheme distinguishes link misbehaviors and temporary link failures by observing the reception of 2ACK packets over a certain period of time, termed the observation period, Tobs. Since the temporary link failures do not usually last long, such a technique is able to distinguish temporary link failures from link misbehavior.

The value of Tobs should be large enough so that several 2ACK packets are transmitted from the 2ACK packet sender to the observing node. This is especially important when the acknowledgment ratio, Rack, is small. For example, when Rack = 0.1, one 2ACK packet will be transmitted for every 10 data packets received. However, the observation period should not be too long. A long observation period means that the observing node takes more time to observe the behavior of the next-hop link before a misbehavior is declared. Data packets may be dropped over this extended period of time and the effectiveness of the misbehavior detection algorithm is reduced.

The observation process should be initiated by the observing node randomly and repeatedly. Therefore, the 2ACK packet sender or forwarder has to transmit 2ACK packets for the entire data duration (based on the acknowledgment ratio, Rack). Such repeated observations will help in the detection of misbehaving nodes which have dynamic behavior depending on their energy levels. When such nodes are well-behaved, the links associated with them will be treated as normal links and used. Once such nodes misbehave, the links associated with them will be detected as misbehaving and other nodes will stop using them.

4.9 False Misbehavior Reports and Intentional Dropping of 2ACK

A misbehaving node N1 as shown in Fig. 4.1 may send false misbehavior reports regarding the next-hop link, N2 → N3. However, the 2ACK scheme makes sure that such a behavior will not benefit node N1: 1) N1 may still be included in alternative routes and 2) N1 needs to forward data packets to N2 as necessary. Otherwise, it will be detected as part of a misbehaving link (by the node preceding it on the route).

A misbehaving node N3 may refuse to send any 2ACK packet for the data packets that have been received. As a result, N1 declares the link N2 → N3 as misbehaving and sends a misbehavior report to the source. Since N3, as a misbehaving node, refuses to forward data packets, N2 will also declare the link of N3 → N4 (the node following N3) as misbehaving. Thus, links around node N3 are declared misbehaving and will be avoided by future route selections.

Note that this might seem to have achieved the goal of slandering node N2 by N3. On the contrary, our mechanism of misbehaving link detection instead of misbehaving node detection protects node N2. The link N2 → N3 will be marked as misbehaving, but there is no accusation of N2 (or N3). Other links associated with node N2 might still be used. Detection of the misbehaving node N3 and its punishment are trickier. Essentially, consensus needs to be developed among the majority of neighbors of node N3 to punish it. Similarly, when there on the route, the first misbehaving node and its forwarding link will be detected and reported to the source. Such a route will be avoided in the next round of route discovery. Topology changes may also lead to false misbehavior reports. When two well-behaved neighboring nodes move out of each other’s range, the link between them will fail in terms of data delivery. In 2ACK, this is taken care of by the routing scheme in use (DSR). When the sender of the link notices that the receiver is out of range, it will submit a Route Error (RERR) message to report the link failure.

V. Algorithm

5.1 PSEUDOCODE OF THE 2ACK SCHEME:

The triplet N1 → N2 → N3 in Fig. 4.2 as an example to illustrate 2ACK’s pseudo code. Note that such codes are run on each of the sender/receiver of the 2ACK packets.

A.1 2ACK Packet Sender Side (Node N3)

1: publish hn // Send authenticated element to node N1
2: Cpkts ← 0, Cack ← 0, i ← n // Initialization at node N3
3: while true do
4: if (data packet received) then
5: Cpkts += // Increase the counter of received packets
6: if (Cack = Cpkts < Rack) then // The data packet needs to be acknowledged

International Journal of Innovations & Advancement in Computer Science
IJIAS
ISSN 2347 – 8616
Volume 7, Issue 3
March 2018
7: prepare MAC with hi–1
8: prepare 2ACK with ID, MAC, hi // Add authentication to 2ACK packet
9: send 2ACK
10: Cack ++, i ← i + 1 // Increase the counter of acknowledged packets
11: end
12: end
13: end

A.2 Receiver (Observer) Side (Node N1)
Parallel process 1 (receiving hn)
1: while true do
2: if receive hn from the 2ACK packet sender then
3: record hn, i ← n
4: end
5: end
Parallel process 2 (receiving 2ACK packets)
6: while true do
7: randomly select Tstart > current time // Start the observation
8: while current time < Tstart do
9: // null
10: end
11: LIST ← φ, Cpkts ← 0, Cmis ← 0 // Initialization at node N1
12: while current time < Tstart + Tobs do // Observation period is not expired
13: if (data packet forwarded) then
14: LIST ← LIST U data ID // Add a data ID to LIST
15: Cpkts ++ // Increase the counter of forwarded packets
16: setup timer (τ) for data ID // Record the time
17: end
18: if (2ACK packet received) then
19: search data ID carried by 2ACK from LIST
20: if (found) then == A 2ACK packet for a data ID received
21: check validity of hi
22: LIST ← LIST - data ID // Remove data ID from LIST
23: clear timer for ID
24: end
25: end
26: if (timeout event happens) then // 2ACK packet for a data ID is not received
27: LIST ← LIST - data ID == Remove data ID from LIST
28: Cmis ++ // Increase misbehavior counter
29: end
30: end
31: if (Cmis = Cpkts > Rmis) then // The observation period expires
32: send link misbehavior report
33: end
34: end

5.2 Advantages and Disadvantage:
Advantages
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.

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.

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.

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. The 2ACK scheme is immune to the limited overhearing range issue.

Disadvantage
Disadvantage of the 2ACK scheme has a higher routing overhead. This additional routing overhead is caused by the transmission of 2ACK packets. So by reducing the acknowledgment ratio, $R_{ack}$, the number of 2ACK transmissions can be significantly lowered overhead.
5.3. APPLICATION

1) Military Battlefield: Military equipment now routinely contains some sort of computer equipment. Ad hoc networking would allow the military to take advantage of commonplace network technology to maintain an information network between the soldiers, vehicles, and military information headquarters.

2) Commercial Sector: Ad hoc can be used in emergency/rescue operations for disaster relief efforts, e.g. in fire, flood, or earthquake. Other commercial scenarios include e.g. ship-to-ship ad hoc mobile communication, law enforcement

3) Local Level: Ad hoc networks can autonomously link an instant and temporary multimedia network using notebook computers or palmtop computers to spread and share information among participants at e.g. conference or classroom

4) Personal Area Network (PAN): Short-range MANET can simplify the intercommunication between various mobile devices (such as a PDA, a laptop, and a cellular phone). The PAN is potentially a promising application field of MANET in the future pervasivecomputing context.

CONCLUSION

MANETs are Mobile Ad Hoc Networks (MANETs) have been used for application in military and civilian communications. Such a network is highly dependent on the cooperation of all its members to perform networking functions. We also studied types of misbehavior a node can have and different ways to misbehave. When selfish misbehaving nodes participate in the Route Discovery phase but refuse to forward the data packets, routing performance may be degraded severely. To improve the performance of the system, 2ACK Scheme is used.

REFERENCES


