A Mechanism for Detection of Black Hole Attack in Mobile Ad Hoc Networks

S. L. Dhende[1], Prof. Mrs. D. M. Bhalerao[2]

Department of E&TC, Sinhgad College of Engg., Pune, India.

Abstract

A mobile ad hoc network (MANET) is a collection of autonomous nodes that communicate with each other by forming a multi-hop radio network and maintaining connections in a decentralized manner. Security remains a major challenge for these networks due to their features of open medium, dynamically changing topologies, reliance on cooperative algorithms, absence of centralized monitoring points, and lack of clear lines of defense. Most of the routing protocols for MANETs are thus vulnerable to various types of attacks. Ad hoc on-demand distance vector routing (AODV) is a very popular routing algorithm. However, it is vulnerable to the well-known black hole attack, where a malicious node falsely advertises good paths to a destination node during the route discovery process. In this paper, a defense mechanism is presented against a coordinated attack by multiple black hole nodes in a MANET.

Keywords: ad hoc networks, AODV, black hole, security, routing,

1. Introduction

A MANET is a collection of wireless hosts that can be rapidly deployed as a multi-hop packet radio network without the aid of any established infrastructure or centralized administrator. Such networks can be used to enable next generation battlefield applications, including situation awareness systems for maneuvering war fighters, and remotely deployed unmanned micro-sensor networks. MANETs have some special characteristic features such as unreliable wireless media (links) used for communication between hosts, constantly changing network topologies and memberships, limited bandwidth, battery, lifetime, and computation power of nodes etc.

While these characteristics are essential for the flexibility of MANETs, they introduce specific security concerns that are absent or less severe in wired networks. MANETs are vulnerable to various types of attacks. These include passive eavesdropping, active interfering, impersonation, and denial-of service. Intrusion prevention measures such as strong authentication and redundant transmission can be used to improve the security of an ad hoc network. However, these techniques can address only a subset of the threats. Moreover, they are costly to implement. The dynamic nature of ad hoc networks requires that prevention techniques should be complemented by detection techniques, which monitor security status of the network and identify malicious behavior. One of the most critical problems in MANETs is the security vulnerabilities of the routing protocols. However, due to security vulnerabilities of the routing protocols, wireless ad-hoc networks are unprotected to attacks of the malicious nodes. One of these attacks is the Black Hole Attack against network integrity absorbing all data packets in the network. Since the data packets do not reach to the destination node on account of this attack, data loss will occur. There is lots of detection and defense mechanisms to eliminate the intruder that carry out the black hole attack. We present a technique to identify black attack and a solution to discover a safe route avoiding black hole attack.

2. Black Hole Problem

In an ad hoc network that uses the DSR/AODV protocol, a black hole node pretends to have a fresh enough routes to all destinations requested b all the nodes and absorb the network traffic. When source node broadcasts the RREQ message for any destination, the black hole node immediately responds with the RREP message and with next hope details. This message is perceived as, if it is coming from the destination or from a node which has a fresh enough route to the destination. The source node assume that the destination is behind the black hole node and next hope node and perceives the other RREP packets with next hope node coming from other nodes.

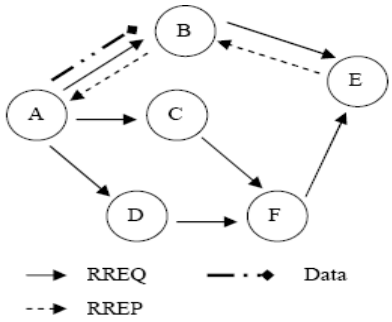

Figure 1. Propagation of RREQ and RREP from A to E

The source node then start to send out its data packets to the black hole node and after small time interval to the other node, trusting that these packets will reach to the destination either by one link.

In the following illustrated fig. 2, imagine a malicious node 'M'. When node 'A' broadcast a RREQ packets, nodes 'B' 'D' and node 'M' receives it. Node 'M' being a malicious node does not check up with its routing table for the requested route to node 'E'.

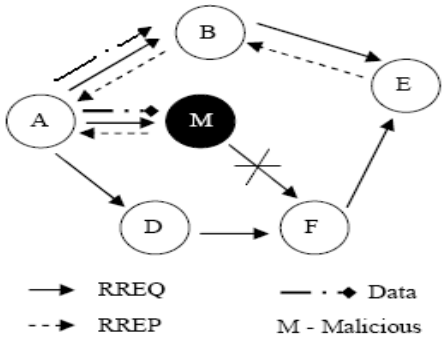

Figure 2. Black hole attack in AODV

Hence, it immediately sends back a RREP packet, claiming a route to the destination. Node 'A' receives the RREP from 'M' ahead of the RREP from 'B' and 'D'.

Node 'A' assumes that the route through 'M' is the shortest route and sends any packet to the destination through it. When the node 'A' sends data to 'M', it absorbs all the data and thus behaves like a 'Black hole'. However in that solution next hope also behaves as a malicious node they cannot identify it.

3. Solution

We proposed a solution that is an enhancement of the basic AODV routing protocol, which will be able to avoid and detect black holes. To reduce the probability it is proposed to wait and check the replies from all the neighboring nodes to find a safe route.

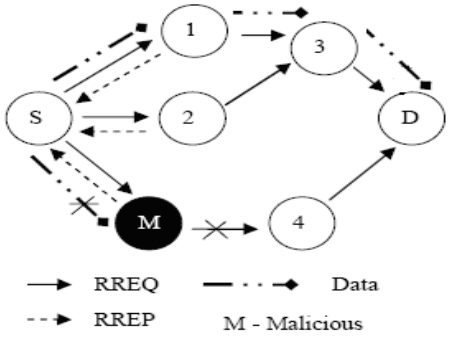

Figure 3. Solution to Black hole

According to this proposed solution the requesting node without sending the DATA packets to the reply node at once, it has to wait till other replies with next hope details from the other neighboring nodes. After receiving the first request it sets timer in the 'Timer Expired Table', for collecting the further requests from different nodes. It will store the 'Sequence number, and the time at which the packet arrives, in a 'Collect Route Reply Table' (CRRT).

After the timeout value, it chooses first two paths with the next hope details to transmit the DATA packets and simultaneously send same DATA packets along with first path and along with second path and check the DATA packets arrive at next hope node. If the DATA packets receive at next hope node, it automatically generates 2 ACK acknowledgments and sends it back on same link to inform to the sending node. If the DATA packets will become

unable to receive at next hope node then it will not generate any acknowledgment. From this the immediate node to the next hope node along with the same link which becomes unable to send the 2 ACK acknowledgments will be a malicious node. Then it chooses another link which transmits DATA packets to the next hope node for whole transmission.

Thus Black hole attacks can greatly be detected and reduced and DATA packets can be transmitted along with chosen path.

4. Working principle of AODV/DSR

In the above figure 3, S wants to transmit to D. So it first transmits the route request to all the neighboring nodes. Here node 1, node M and node 2 receive this request. The malicious node has no intention to transmit the DATA packets to the destination node D but it wants to intercept/collect the DATA from the source node S. So it immediately replies to the request as (M-4). Instead of transmitting the DATA packets immediately through M, S has to wait for further reply from the other nodes. After some time it will receives the reply from node 1 as (1-3) and node 2 as (2-3). According to this proposed solution it first selects first two links which contains next hope details and then transmit simultaneously same DATA packets along with first link and along with second link.

Table 1. Routing details

Source	Intermediate node	Destination
S	**M - 4**	**D**
S	**1 - 3**	**D**
S	**2 – 3**	**D**

If the DATA packets receive at next hope node, it automatically generates 2 ACK acknowledgments and sends it back on same link to inform to the sending node. If the DATA packets will become unable to receive at next hope node then it will not generate any acknowledgment. From these the immediate node to the next hope node along with same link which becomes unable to send the 2 ACK acknowledgments will be a malicious node. Then it chooses another link which transmits DATA packets to the next hope node for whole transmission. The routing table from S to D is given in table 1.

5. ACK algorithm

Figure 4. The 2ACK scheme

The detection and prevention of Black hole attacks can be done by using 2ACK algorithm which works in triplet.

As shown in fig. 4, node N1 send DATA packets to node N2 and node N2 send to node N3. When node N3 receives DATA packets send by node N1, then it generate 2ACK packets and send these packets to node N1 on same link in reversed direction.

If the node N3 will become unable to receive DATA packets send by node N1 then it will not generate 2ACK packets. The immediate node to the next hope node which becomes unable to send 2ACK packets will be a malicious node and the link will be a misbehaving link.

6. Conclusion and future work

According to the proposed solution the required security in MANET can be achieved with minimum delay and control overhead and simultaneously we can detect the Black hole attack and transmit DATA packets to the destination. As future work, we intend to develop simulations to analyze the performance of the proposed solution.

7. References

[1] Latha Tamilselvan, Dr. V Sankaranarayanan, “Prevention of Black hole Attacks in MANET”, The 2nd international Conference on Wireless Broadband and Ultra Wideband Communications, 2007 IEEE.

[2] N. Bhalaji, Dr. A Shanmugam, "Assosiation Between Nodes to Combat Blackhole Attacks in DSR Based MANET", 2009 IEEE.
[3] Mehdi Medadian, M. H. Yektaie, A. M. Rahmani, "Combat with Blackhole Attack in AODV Routing Porotocol in MANET", 9th Malaysia International Conference on Communication, 15-17 December 2009.
[4] Yanzhi Ren, Mooi Choo Chuah, Jiee Yang Yingying Chen, "Detecting Blackhole Attacks in Disruption-Tolerant Networks through Packet Exchange Recording", 2010 IEEE
[5] Jaydip Sen, Sripad Koilakoda, Arijit Ukil, "A Mechanism for Detection of Cooperative Blackhole Attack in Mobile Adhoc Networks", 2nd International Conference on Intelligent Systems Modeling and Simulation, 2011.
[6] Saurabh Gupta, Subrat kar, S Dharmaraja, "BAAP: Blackhole Attack Avoidance Protocolfor Wireless NEtworks", International Conference on Computer and Communication Technology, 2011.
[7] Lalit Himral, Vishal Vig, Nagesh Chand, "Preventing AODV Routing Protocol from Blackhole Attack", International Journal of Engineering, Science and Technology, May 2011.
[8] Payal N. Raj, Prashant B. Swadas, "DPRAODV: A Dynamic Learning System Against ackhole Attacks in AODV Based MANET", International Journal of Computer Science Issues, Vol.2 2009.
[9] Kejun Liu, Jing Deng, "An Acknowledgment Based Approach for the Detection of Routing MIsbahavior in MANETS, IEEE Transaction in Mobile Computing, Vol. 6, Vol. 5, May 2007.
[10] Satyajayant Misra, Kabi Bhattarai, Guoliang Xue, "BAMBi: Blackhole Attacks Mitigation Multiple Base station in Wireless Sensor Networks", IEEE 2007.