ISSN No. 0976-5697

Volume 6, No. 2, March-April 2015

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

A Review on BlackHole Attack Issues

Gurbir Singh
M.Tech Computer Science
Punjab Technical University, India

Nitin Bhagat
AP, M.Tech Computer Science,
Department of CSE,India

Abstract: In MANET, each node acts as a router to establish a route and transfer data by means of multiple hops. MANET is more vulnerable to security problem. When a node wants to transfer data to another node, packets are transferred through the intermediate nodes. Thus, searching and establishing a route from a source node to a destination node is an important task in MANETs. There are several routing protocols. The existing routing protocols are optimized to perform the routing process without considering the security problem. Black hole attack is one of the routing attacks in which, a malicious node uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. AODV (Ad hoc On-demand Distance Vector) is the most suitable routing protocols for the MANETs and it is more vulnerable to black hole attack.

Keywords: Ad hoc, Source routing, malicious node, Black Hole Attack, Black Hole Attack detection and prevention techniques.

I. INTRODUCTION

In an ad-hoc network that uses the AODV protocol, a blackhole node pretends to have fresh enough routes to all destinations requested by all the nodes and absorbs the network traffic. When a source node broadcasts the RREQ message for any destination, the blackhole node immediately responds with an RREP message that includes the highest sequence number and 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 then starts to send out its data packets to the blackhole trusting that these packets will reach the destination.

A malicious node sends RREP messages without checking its routing table for a fresh route to a destination. As shown in figure 1, source node 0 broadcasts an RREQ message to discover a route for sending packets to destination node 2. An RREQ broadcast from node 0 is received by neighboring nodes 1, 3 and 4. However, malicious node 4 sends an RREP message immediately without even having a route to destination node 2. An RREP message from a malicious node is the first to arrive at a source node. Hence, a source node updates its routing table for the new route to the particular destination node and discards any RREP message from other neighboring nodes even from an actual destination node. Once a source node saves a route, it starts sending buffered data packets to a malicious node hoping they will be forwarded to a destination node. A malicious node drops all data packets rather than forwarding them on [4].

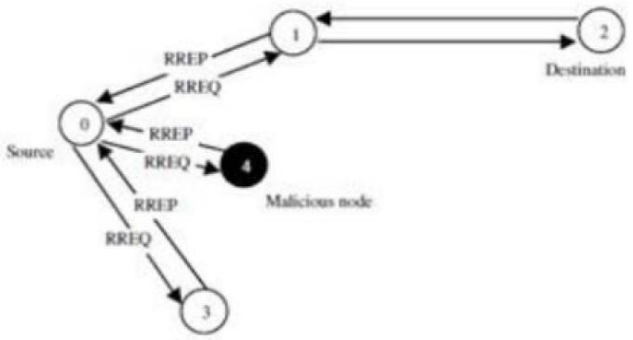

Figure 1. RREQ Broadcast[4]

A. *Attacks on network*

1. *Active Attacks:* Active attacks are those attacks, which are performed by the malicious nodes. It involves some modification of data stream or creating the false stream.
   The following attacks are active in nature:
   a) Routing Attacks in Sensor Networks
   b) Denial of Service Attacks
   c) Node Subversion
   d) Node Malfunction
   e) Node Outage
   f) Physical Attacks
   g) Message corruption
   h) False Node
   i) Node Replication Attacks
   j) Information gathering
2. *Passive Attack:* In passive attacks the attacker does not disturb the routing protocol. Passive attack is in nature of eavesdropping on, or monitoring of transmission. Passive attacks are very difficult to detect because they do not involve any modification of data.

Some of active attacks on routing:

a) *Jamming*: Jamming is one of the basic attacks in which it uses to interfere with the radio frequencies of the sensor nodes. A few jamming node can put a

considerable amount of the nodes out of order. Jamming can be of two types of constant jamming and intermittent jamming. Constant jamming complete affects on whole network whereas in intermittent jamming nodes are not communicating continuously.

b) *Tampering*: A Tampering attack is attack which damages a sensor node and replaces the entire node or part of its hardware.

c) *Worm Holes Attack*: Worm hole attack which records the packets which is send to the one location in the networks In these attacks the tunnels messages received in one part of the network over a low latency link, and another part of the network where the messages are replayed. It is leading to quick exhaustion of the energy resources.

d) Hello Flood Attack: Hello flood attack is attack in which HELLO message is send by anther neighboring node within radio transmission range. It gives illusion to the malicious node. When the nodes will send message to the base station, then it passes through the malicious node and this node provides the shortest route to the base station as an illusion. When the information reaches the attacker, the victim is betrayed by it. This leads to data congestion and data flow in the network.

e) *Spoofed*: This is attack altered or replayed routing information this is the attack, which is directly attack on the network. By spoofing, altering or replaying routing information the attacker can complicate the network and create routing loops, attracting or repelling traffic, generating false error message, shortening or extending services router or partitioning the network shortening or extending services router or partitioning the network, which increases end-to-end latency and effect on speed on network.

f) Selective Forwarding: This layer is attack on network layer. This is selective and forwarding in sensor networks. This layer is attacks on network layer. In sensor networks the nodes are forward received messages but some compromised node refused to forward packets, however neighbors node start using connect to another route.

g) The Sybil Attack This layer is attacks on network layer: A malicious node presents multiple identities to the network. This attack is to geographic routing protocols appears to be in multiple locations at once.

h) Denial of services: DoS attack is the simplest attack. Sending extra packets which destroy the network. In wireless sensor networks, several types of DoS attacks in different layers might be performed. At physical layer the DoS attacks could be jamming and tampering, at link layer, collision, exhaustion, unfairness, at network layer, neglect and greed, homing, misdirection, black holes and at transport layer this attack could be performed by malicious flooding and desynchronization [3].

i) Black Hole Attack: Routing protocols are exposed to a variety of attacks. Black hole attack is one such attack in which a malicious node makes use of the vulnerabilities of the route discovery packets of the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept [7]. This attack aims at modifying the routing protocol so that traffic flows through a specific node controlled by the attacker. During the route discovery process, the source node sends route discovery packets to the intermediate nodes to find fresh path to the intended destination. Malicious nodes respond immediately to the source node as these nodes do not refer the routing table. The source node assumes that the route discovery process is complete, ignores other route reply messages from other nodes and selects the path through the malicious node to route the data packets. The malicious node does this by assigning a high sequence number to the reply packet. The attacker now drops the received messages instead of relaying them as the protocol requires [6].

j) Node Subversion: It is attack which Capture anode information which includes the disclosure to cryptographic keys and compromise the whole sensor network with it.

B. BLACK AND GREY HOLE ATTACK

Black hole attack is a routing layer attack in which data is revolves from other node. The transmission of packets on multiple nodes and dropping of packets is mostly occurring on routing layer. Routing protocol is targeted by the attack. Blackhole attack has great influencing attack on virtual mesh network. The busy DOS attack is black hole attack. Black hole attack is difficult to detect; it is mostly found in temporary networks like virtual/wireless mesh networks.

Black hole attack will cause powerful effect to the performance of mesh networks. In previous research, the authors have carried out on black hole attack [2].

In black hole attack, the sender node receive reply message from fault node and make smallest way to receiver node. Fault node sends reply message after authorized node to sender node and then sender become confuse in two replies. On that way, Fault node become sender node and whole data received by it. In this, the data packets fully dropped by sender node.

In Figure 2, the sender node 1 sends large amount of RREQ message to every nearby nodes. When RREQ message is received by fault node, then it sends RREP message to sender node which is non-real and also shows the shortest way to reach to receiver node.

Then sender node accepts the reply message from non-real node which is called fault node and transfers the packets. This attack is known as black hole attack [1].

In black hole attack, a fault node accepted by sender node not attention and all the data packets are dropped. This is also known as sleep derivation attack. This attack is divided into two types, i.e. Internal and External black hole attack. We explain these attacks as follows [1]:

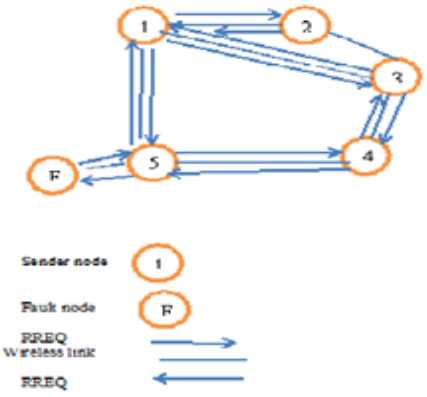

Figure 2. Black Hole Attack Specification[1].

1. *Internal blackhole attack:* It occurs in network internally. It means the internal node is become the fault node and makes route from sender node to receiver node.

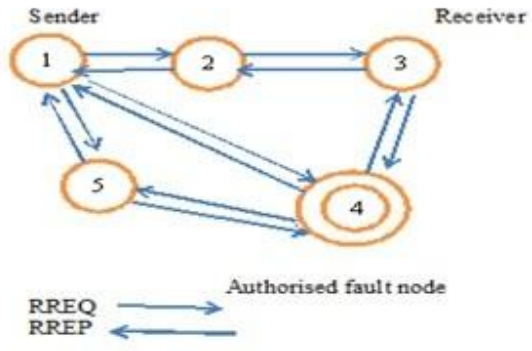

Figure 3. Internal Black Hole Attack[1].

In Figure 2, the sender node 1 sends RREQ to each node and gets reply back from every node; the whole network is set up by authorized nodes. Suddenly, the authorized node becomes fault node and internal black hole attack occurs [1].

2. *External blackhole attack:* This attack occurs outside from the network. It is mainly called DOS (denial of service) attack in this attack, network take advantage from network traffic and collapse the whole network. It is done by External fault node and then working as same as internal node. It follows some steps which is given below:
   - *a)* Fault node becomes active node and makes way to receiver node.
   - *b)* Fault node send RREP message and shows the smallest way to receiver node and become part of network.
   - *c)* It receives all the data packets from sender node which is transmit in network.
   - *d)* The series of RREQ and RREP message occur and data transfer is done and black hole attack occurs.
   - *e)* The data is receiving the fault node and 100% packets are dropped in network.

The black hole and Grey hole attack will carry a large price of effect to the performance of wireless mesh network. In multiple ways the false behavior may exhibits by Grey hole attack, Grey hole attack is a node which react maliciously for some specific time duration by releasing packets but may come to balanced behavior and later forward the packets through packet ID to other packet. A Grey hole may also behave a random behavior by which it rejects some the packets randomly when it forward to other packets. Thereby its detection is even more difficult than black hole attack.

II. LITERATURE SURVEY

We review five different methods for the detection and prevention of blackhole attacks in AODV based mobile ad-hoc networks:

A. Detection, Prevention and Reactive AODV (DPRAODV) scheme

In normal AODV, the node that receives the RREP packet first checks the value of sequence number in its routing table. If its sequence number is higher than the one in routing table, this RREP packet is accepted. In this solution, it has an addition check whether the RREP sequence number is higher than the threshold value. If it is higher than the threshold value, then the node is considered to be malicious node and it adds to the black list. As the node detected as anomaly, it sends ALARM packet to its neighbors.

B. *ABM (Anti-Blackhole Mechanism) scheme*

The paper [4] attempts to detect and separate malicious nodes, which selectively perform black hole attacks by deploying IDSs in MANETs (mobile ad hoc networks). All IDS nodes perform an ABM (Anti-Blackhole Mechanism), which estimates the suspicious value of a node, according to the amount of abnormal difference between RREQs and RREPs transmitted from the node. With the prerequisite that intermediate nodes are forbidden to reply to RREQs, if an intermediate node, which is not the destination and never broadcasts a RREQ for a specific route, forwards a RREP for the route, then its suspicious value will be increased by 1 in the nearby IDS's SN (suspicious node) table.

C. *Honeypot based detection scheme*

Authors propose a novel strategy by employing mobile honeypot agents that utilize their topological knowledge and detect such spurious route advertisements. They are deployed as roaming software agents that tour the network and lure attackers by sending route request advertisements. We collect valuable information on attacker's strategy from the intrusion logs gathered at a given honeypot [5].

D. Enhance Route Discovery for AODV (ERDA) scheme

Have designed an ERDA solution to improve AODV protocol with minimum modification to the existing route discovery mechanism recvReply() function. a method called ERDA (Enhance Route Discovery for AODV). The proposed method is able to mitigate the foresaid problem by introducing new conditions in the routing table update process and also by adding simple malicious node detection and isolation process to the AODV route discovery mechanism. The proposed method does not introduce any additional control message and moreover, it does not change the existing protocol scheme.

E. Cryptographic based technique

This paper focuses that many investigations have been done in order to improve the security in MANETs, most of which are relied on cryptographic based techniques in order to guarantee some properties such as data integrity and availability.

III. REFERENCES

[1] Rupinder Kaur, Parminder Singh, "REVIEW OF BLACK HOLE AND GREY HOLE ATTACK" The International Journal of Multimedia & Its Applications (IJMA), Vol.6, No.6, December 2014.

[2] Rupinder Kaur, Parminder Singh, "Black Hole and Greyhole Attack in Wireless Mesh Network" American Journal of Engineering Research, Volume-3, Issue-10, pp-41-47, 2014.

[3] Kalpana Sharma, M K Ghose, "Wireless Sensor Networks: An Overview on its Security Threats" IJCA, Special Issue on MANETs, 2010.

[4] Bhoomika Patel, Khushboo Trivedi, "A Review - Prevention and Detection of BlackHole Attack in AODV based on MANET" IJCSIT, Vol. 5 (3), 2014.

[5] Ming-Yang Su,"Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems" Elsevier, 2011.

[6] E.A. Mary Anita, V. Vasudevan, "Black Hole Attack Prevention in Multicast Routing Protocols for Mobile Ad hoc networks using Certificate Chaining" International Journal of Computer Applications, Volume 1, 2010.

[7] E. A. Mary Anita, V. Vasudevan, "Black Hole attack on multicast routing protocols" JCIT, Vol.4, No.2, pp. 64–68, 2009.