Intelligent self adaptive routing mechanism for AODV against black hole attack in manet
Rashmi Mishra* and Harsh Khatter
CSE Department, ABES Engineering College, Ghaziabad, U.P, India.

ABSTRACT
Ad Hoc Network provides quick communication among nodes to convey the packets from one node to other. These networks are independent of any fixed infrastructure or central entity like cellular networks [10] which requires fixed infrastructure to operate. Any malicious node in the network can disturb the whole process or can even stop it. Several attacks like Replay attack, black hole, wormhole, rushing etc [13], in which legitimate knob behaves like malicious knob and disturbed whole the network. To define and detect the malicious behavior of a knob, it becomes obligatory to define the regular and malicious behavior of a knob. Whenever a knob exhibits a malicious behavior under any attack, it assures the breach of security principles like availability, integrity, confidentiality etc [13].

© 2014 Elixir All rights reserved.

Introduction

Literature Review
In Year 2012 Ms. Nidhi Sharma et. al. proposed solution for Black hole attack in MANETs- Source node waits for the RREP packet to arrive from more than two nodes. During this time, the two or more nodes/hops shared the redundant paths. From these shared hops the source node can recognize the safe route to the destination. If no shared nodes appear to be in these redundant routes, the sender will wait for another RREP until a route with shared nodes identified or routing timer expired. This solution can guarantee to find a safe route to the destination, but the main drawback is the time delay. If there are no shared nodes or hops between the routes, the packets will never be sent[2][6].

In year 2012 Mr. Rutvij H. Jhaveri et. al. proposed a novel approach for black hole and gray hole attacks in Mobile ad-hoc Network. proposed approach, an intermediate node dynamically calculates a PEAK value after every time interval that uses three parameters for calculation: RREQ sequence number, routing table sequence number and number of replies received during the time interval. when an intermediate node receives RREP having sequence number higher than the calculated PEAK value, it is marked as DO_NOT_CONSIDER [4][9].

Proposed Methods To Detect Different Types Of Attack
Numerous methods have been proposed to detect the status of knob which are as follows:
Intrusion Detection Systems (IDS) – Anomaly based IDS is mainly used in MANETs to detect any kind of intrusion in the network. Profiles are maintained in databases of IDS to match the anomaly. These profiles can be static or dynamic in nature. The problem with such system is that it is difficult to make a perfect profile. Moreover false alarm rate is higher [5][12].
Random Walker Detectors (RWD) – This detector moves randomly from one knob to other knob to detect the knob’s activities. It monitors each knob for a malicious behavior and migrates to the selected knob. This RWD has a specification based detection engine for comparing the behavior of knob [6].
2.3 Watchdog – This method proposed the concept of a watchdog knob which has high power and high transmission range than other ordinary knob. This knob watches and monitors the surrounding knob. It keeps the knob’s data in its buffer and compares it after a new knob receives it. Watchdog knob is also called path rather [7].

A securing routing protocol against black hole attack in manet problem
According to the original AODV protocol, any intermediate node may respond to the RREQ message if it has a fresh rough route, which is checked by the destination sequence number contained in the RREQ packet. This Mechanism is used to decreases the routing delay, but makes the system a target of a malicious node. The malicious node easily disrupts the correct functioning of the routing protocol and makes at least part of the network crash.

Previously the works done on security issues i.e. attacks (Black Hole attack) involved in MANET were based on reactive routing protocol like AODV. Black Hole attack is studied under the AODV routing protocol and its effects are elaborate by stating how this attack disrupt the performance of MANET.

Mitigation Scheme
Different scheme is used in MANET to overcome the effect of black hole attack. Here, I have used behavioral based scheme in which the destination sequence no is traced. Since the malicious node always try to send the big destination sequence no. , it is easy to trace out the black hole node and after detecting the node the legitimate node just discards the RREP packet sent by the malicious node. Hence, the effect of the black hole attack can be minimized.

Destination sequence no. sent from the malicious node is compared with the expected destination sequence no. If the destination sequence no is greater than the expected sequence no then it is found that the RREP is malicious.

Evaluation Criteria
To evaluate the black hole I have considered the mobility patterns that are very realistic and close to the real world scenario. I have used different parameters such as Throughput, Packet Drop Ratio and End to end delay to analyze the black hole attack effect on the network.
Proposed Algorithm

Parameters: DSN- Destination Sequence Number, NID: Node ID, MN-ID: Malicious Node ID, ESN-Expected Sequence Number, NRC- Node Route Counter.

- Start the route discovery phase with the source node S.
- Store the Route Replies DSN and NID in RR-Table.
- If DSN is much greater than ESN then discard entry from RR-Table as Select Dest_Seq_No rom table
- If(Dest_Seq_No>= ESN_Seq_No)
  - Mal_Node=Node_Id;
  - Discard entry from table;

If Node=Good // if route is fine and Node is fine

\[
\text{AvgThroughput} = \frac{\text{Sum of bytes sent through the data packets}}{\text{time}}
\]
\[
\text{End to end delay} = \frac{\text{Transmitted time of packet} - \text{Sending time of the packet}}{\text{No. of connection}}
\]
\[
\text{PacketDrop Ratio} = \frac{\text{Sent Packet} - \text{Received Packet}}{\text{Sent Packet}}
\]

Then NRC=NRC+1;
- If Node=Mal
Then NRC=NRC-5; //if packet is unable reach Destination (black node)

**References**
Rutvij H. Jhaveri et.al., “Improving Route Discovery for AODV to Prevent Blackhole and Grayhole Attacks in MANETs”, INFOCOMP, vol. 11, no. 1, p. 01-12, March of 2012.

**Attacks against routing message and its defensive method**

<table>
<thead>
<tr>
<th>S.No.</th>
<th>Malicious Behavior</th>
<th>Affected Security Principle</th>
<th>Suggested Defensive Methods</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Message Tampering, Information Disclosure Attack</td>
<td>Integrity</td>
<td>Cryptography-MD5 [16], Polynomial based personal keys[26][1]</td>
</tr>
<tr>
<td>2</td>
<td>Stealing Information</td>
<td>Confidentiality</td>
<td>Cryptography[16][1]</td>
</tr>
<tr>
<td>3</td>
<td>Bandwidth consumption, Battery Drained Buffer Overflow, Node Not Available</td>
<td>Availability</td>
<td>TTP (RWD, Watchdog)[12][19] and IDS[20][21][1]</td>
</tr>
<tr>
<td>4</td>
<td>Entering Malicious node in the Network</td>
<td>Authentication</td>
<td>PKICertification System[17][1]</td>
</tr>
<tr>
<td>5</td>
<td>Node Denies of sending message</td>
<td>Non-Reputation</td>
<td>Digital Signature[16][1]</td>
</tr>
</tbody>
</table>

**Table 2. Attacks on Routing Message And its Suggested Defensive Methods**

<table>
<thead>
<tr>
<th>S.No.</th>
<th>Attack</th>
<th>Suggested Defense Methods</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>All Network Layer Attack</td>
<td>Model using acknowledgment approach[14], Cross-validation of nodes using certificates[8]</td>
</tr>
<tr>
<td>2</td>
<td>Wormhole Attack</td>
<td>Connectivity Graph[16], Enhanced OLSR[17], EDWA[18], Distance method based on RSS[19], Public key cryptography</td>
</tr>
<tr>
<td>3</td>
<td>Blackhole Attack</td>
<td>Authentication of node using PKI[21], Trust value of neighboring nodes[22], ABM using IDS[23], Enhancement of AODV[26]</td>
</tr>
<tr>
<td>4</td>
<td>Byzantine Attack</td>
<td>Public key using cryptographic mechanism[25]</td>
</tr>
<tr>
<td>5</td>
<td>Routing Attack</td>
<td>CRADS[27] and SRDV[15]</td>
</tr>
<tr>
<td>6</td>
<td>Flooding attack</td>
<td>uses a statistical analysis to detect malicious RREQ floods, CUSUM algorithm, each node is to monitor its neighbors’ RREQ. If the RREQ rate of any neighbor exceeds the predefined threshold, the node records the ID of this neighbor in a blacklist.</td>
</tr>
<tr>
<td>7</td>
<td>Message with holding attack</td>
<td>intrusion detection system to detect TC link, TC message and a HELLO message(if TC message &lt; Hello message ,then node is suspicious)</td>
</tr>
<tr>
<td>8</td>
<td>Link Spoofing attack</td>
<td>detection method by using cryptography with a GPS and a time stamp</td>
</tr>
<tr>
<td>9</td>
<td>Replay Attack</td>
<td>time stamp with the use of an asymmetric key</td>
</tr>
<tr>
<td>10</td>
<td>Colluding Misrelay attack</td>
<td>conventional acknowledgment-based approach might detect this type of attack in a MANET</td>
</tr>
</tbody>
</table>
Rutvij H. Jhaveri et al., “Improving Route Discovery for AODV to Prevent Blackhole and Grayhole Attacks in MANETs”, INFOCOMP, vol. 11, no. 1, p. 01-12, March of 2012.
Panos, C. Xenakis, C and Stavrakakis, I - A Novel Intrusion Detection System for MANETs International Conference on Security and Cryptography (SECrypt) 2009