Eliminating Gray Holes in Mobile Ad hoc Network
Discovering a Secure Path by Threshold Mechanism
Problem Statement:
In this thesis firstly we study the effects of Black hole attack in MANET using both Proactive and Reactive routing protocols and then discovering a Secure Path in MANET by Avoiding Black/Gray Holes.

Thesis Aims and Objective

▪ This study focus on analysis of black hole attack in MANET and its consequences. Analyzing the effects of black hole attack in the light of throughput and end-to-end delay in MANET.
▪ Simulating the black hole attack using Proactive and Reactive routing protocols.
▪ Comparing the results of both Proactive and Reactive protocols to analyze which of these two types of protocols are more vulnerable to Black Hole attack.
▪ Then Discovering a Secure Path in MANET by Avoiding Black/Gray Holes.
The term MANET (Mobile Ad hoc Network) refers to a multihop packet-based wireless network composed of a set of mobile nodes that can communicate and move at the same time, without using any kind of fixed wired infrastructure.
Characteristics of an Ad-hoc Network

- Collection of mobile nodes forming a temporary network
  - Network topology changes frequently and unpredictably
  - No centralized administration or standard support services
  - Number of nodes 10 to 100 or at most 1000
Black hole Attack

- In this type of attacks, malicious node claims having an optimum route to the node whose packets it wants to intercept. On receiving the request the malicious node sends a fake reply with extremely short route.
- Once the node has been able to place itself between the communicating nodes, it is able to do anything with the packets passing between them.
Gray Hole Attack

- A grey hole attack (GH) is a special case of the BH attack, in which an intruder first captures the routes, i.e. becomes part of the routes in the network (as with the BH attack), and then drops packets selectively. For example, the intruder may drop packets from specific source nodes, or it may drop packets probabilistically or drop packets in some other specific pattern.

- BH and GH attacks on the other hand comprise two tasks:
  - The attacker first captures routes and then either drops all packets (BH attack)
  - or some packets (GH attack)
Proposed Algorithm

Notations
SN : Source Node DN : Destination Node IN : Intermediate Node
TH : Threshold
D_Seq : Destination Sequence Number
Seq : Sequence Number

1. SN broadcasts RREQ to all Nodes
2. IN receives RREQ and forwards until reach DN
3. DN receives RREQ from SN or IN
4. DN gets Seq from RREQ and verifies with Seq in its routing table
5. If Seq of RREQ is greater than Seq of its routing table
6. DN selects Seq of RREQ and plus one
7. Else
8. DN selects Seq of its routing table and plus one
9. End if
10. If Seq is greater than or equal TH
11. Seq = 0
12. Else
13. Seq = Seq
14. End if
15. DN generates RREP by using Seq as D_Seq and sends back to SN
16. If SN receives RREP for RREQ
17. SN checks the RREP message for D_seq
18. If D_Seq is greater than TH
19. Discard this message
20. Else
21. Route is established
22. End if
23. End If
Selection of protocol (AODV)  
Perfomance analysis  

Comparison  
Degradation of performance  
YES  
select receiver and transmitter  
send information to receiver from transmitter  

Hop count and delay count  
Variation  
YES  
Select the nodes in between communication  
mark the number of nodes  

Number of nodes is one  
YES  
Declare it malicious  
Broadcast to network  
NO  
evoke multipath algorithm with unicasting  
send unicast query message to the neighbors  
Fetch information from the neighbors  

If Nodes found misbehaving  
NO  
Mark it safe  
YES
Lu et al. [3] proposed the SAODV black hole detection scheme for MANETs that is designed to address some of the security weaknesses of AODV and withstand black hole attacks.

Deswal and Singh [4] created an enhanced version of the SAODV protocol that includes password security for each of the routing nodes and routing tables that are updated based on timeliness.

Ramaswamy et al. [5] proposed a method for identifying multiple black hole nodes. They were the first to propose a solution for cooperative black hole attacks. They modified the AODV protocol slightly by introducing a Data Routing Information (DRI) table and a cross checking mechanism. Each entry of the node is maintained by the table. This method uses the reliable nodes to transfer the packets.
Simulation Tool Used

- This Dissertation work using OPNET Modeler16.0 Network Simulator.
- OPNET Modeler16.0 is a Commercial Network Simulator.
- Designed for modelling communication devices, technologies, and protocols and to simulate the performance of these technologies.
<table>
<thead>
<tr>
<th>Scenarios Name</th>
<th>No. of Mobile Nodes</th>
<th>Protocol Used</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal Network</td>
<td>100</td>
<td>AODV</td>
</tr>
<tr>
<td>Under Gray Hole Attack</td>
<td>100</td>
<td>AODV</td>
</tr>
<tr>
<td>Mitigation of Gray Hole Attack</td>
<td>100</td>
<td>AODV</td>
</tr>
<tr>
<td>Normal Network</td>
<td>150</td>
<td>AODV</td>
</tr>
<tr>
<td>Under Gray Hole Attack</td>
<td>150</td>
<td>AODV</td>
</tr>
<tr>
<td>Mitigation of Gray Hole Attack</td>
<td>150</td>
<td>AODV</td>
</tr>
</tbody>
</table>

Table1: Scenario Used
<table>
<thead>
<tr>
<th>Simulation Statistics</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Examined Protocols Cases</strong></td>
<td>AODV with and without Gray Hole Attack</td>
</tr>
<tr>
<td><strong>Number of Nodes</strong></td>
<td>100 and 150</td>
</tr>
<tr>
<td><strong>Types of Nodes</strong></td>
<td>Vehicular</td>
</tr>
<tr>
<td><strong>Simulation Area</strong></td>
<td>55*55 km</td>
</tr>
<tr>
<td><strong>Simulation Time</strong></td>
<td>1800 seconds</td>
</tr>
<tr>
<td><strong>Mobility</strong></td>
<td>Uniform(50-100) m/s</td>
</tr>
<tr>
<td><strong>Pause Time</strong></td>
<td>100 seconds</td>
</tr>
<tr>
<td><strong>Performance Parameters</strong></td>
<td>Throughput, Delay, Network load</td>
</tr>
<tr>
<td><strong>No. of Gray Hole Node</strong></td>
<td>10</td>
</tr>
<tr>
<td><strong>Trajectory</strong></td>
<td>VECTOR</td>
</tr>
<tr>
<td><strong>Data Type</strong></td>
<td>Constant Bit Rate (CBR)</td>
</tr>
<tr>
<td><strong>Packet Size</strong></td>
<td>1024 bytes</td>
</tr>
<tr>
<td><strong>Traffic type</strong></td>
<td>FTP, Http</td>
</tr>
<tr>
<td><strong>Active Route Timeout(sec)</strong></td>
<td>3</td>
</tr>
<tr>
<td><strong>Hello interval(sec)</strong></td>
<td>1,2</td>
</tr>
<tr>
<td><strong>Hello Loss</strong></td>
<td>3</td>
</tr>
<tr>
<td><strong>Timeout Buffer</strong></td>
<td>2</td>
</tr>
<tr>
<td><strong>Physical Characteristics</strong></td>
<td>Extended rate IEEE 802.11g (OFDM)</td>
</tr>
<tr>
<td><strong>Data Rates(bps)</strong></td>
<td>54 Mbps</td>
</tr>
<tr>
<td>Parameter</td>
<td>Value</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>Transmit Power</td>
<td>0.005</td>
</tr>
<tr>
<td>RTS Threshold</td>
<td>1024</td>
</tr>
<tr>
<td>Packet-Reception Threshold</td>
<td>-95</td>
</tr>
<tr>
<td>Performance Parameters</td>
<td>Throughput, Delay, Network load</td>
</tr>
<tr>
<td>Trajectory</td>
<td>VECTOR</td>
</tr>
<tr>
<td>Long Retry Limit</td>
<td>4</td>
</tr>
<tr>
<td>Max Receive Lifetime (seconds)</td>
<td>0.5</td>
</tr>
<tr>
<td>Buffer Size (bits)</td>
<td>25600</td>
</tr>
</tbody>
</table>
Scenario of Without Gray Hole
Scenario of With Gray Hole
RESULTS
Throughput

- Throughput is one of the more important and common network performance metrics. Measured in bits/sec or in packets/sec, it represents the amount of bits or packets that are successfully transferred over a link.

- High throughput values indicate efficient network function as packets sent reach their destination without being dropped and retransmitted for various reasons.

- In first scenario of our experimentation, packets travels are shown as throughput with peak value of approx. 268678 and it is represented as bits per second.

- In second scenario which is with gray hole attack, packets drops which are represented as throughput, decreases to value of approx. 188933 bits per second.
Throughputs of all three scenarios at 100 nodes
Throughput of all three scenarios at 150 nodes
End-to-End Delay

- End-to-end delay is the average time that starts in the first node by generating the packets till the arriving the packets in destination node which shown in seconds.
- In first scenario of 100 nodes of our experimentation, packets Delay are shown as figure with peak value of approx. 0.459 seconds.
- In second scenario which is with gray hole attack, packets delay Increases to value of approx 0.00030 seconds.
- In first scenario of 150 nodes of our experimentation, packets delay are approx. 0.001 seconds.
- In second scenario which is with gray hole attack, packets delay increases to value of approx. 0.25 seconds.
Delay of all three scenarios at 100 nodes
Delay of all three scenarios at 150 nodes
Conclusion

- With the importance of Wireless Mesh Networks (WMN) comparative to its vast potential it has still many challenges left in order to overcome. Security of WMN is one of the important features for its deployment.
- The main concern of this work to show the performance of AODV under normal surroundings, under gray hole attack and performance after elimination of gray hole attack in term of End to End delay and throughput.

- The network performance with gray hole attack in term of throughput decreases around 188933 bits per second. By our proposed approach, we have recovered around 234544 in throughput.
- The network performance with gray hole attack in term of end to end delay increases around 54% and with our proposed approach, we have recovered around 45% in delay.


Continued…..
Thanks!

Any questions?
You can find us at queries@thesisscientist.com