A SURVEY ON BLACKHOLE ATTACK IN MANET
Jitendrakumar G Shewaramani*, Vishal A Kanjariya
Lecturer, Department of Computer Engineering, B & B Institute of Technology, V V N, Gujarat, India

ABSTRACT:
A Mobile Adhoc network (MANET) is an infrastructure less network comprising of mobile devices, which have capability of dynamically arranging themselves to form a temporary network. Because of mobility of nodes, restricted resources and decentralized administration they become susceptible to various attacks. Nodes participating in MANET have very limited transmission range and so each node in MANET acts as a Router for forwarding packets to other nodes. Hence, secure routing in MANET is the most common research interest. In this paper, we will survey several Denial of Service (DoS) attacks which are serious threats for MANETs namely Blackhole Attack, Wormhole Attack and Grayhole Attack.

KEYWORDS: MANET, Security, DoS Attack, Blackhole Attack

INTRODUCTION
MANET is a wireless network comprising of mobile nodes and capable of establishing network anywhere, any time. Here, mobile nodes randomly enter and leave the network as they have very limited transmission range. Thus each node acts as a router to establish routes between distinct nodes participating in the network. As it is infrastructure less, rapidly changing & quickly deployable network, thus its line of defense is pretty unclear.

From many constrains, in this paper we focus on the secure routing aspect. Here, we have surveyed many DoS attacks as well as proposed solutions to overcome such attacks proposed by various researchers. In Section II, we introduce routing protocols of MANET. Section III focuses on security concerns as well as various attacks possible in MANET. Section IV portrays one of the DoS attacks i.e. Blackhole attack with solutions for detection and or prevention of attack. Last section is about conclusions and future improvements.

Compared to wired network, in MANET every mobile node is working as a router. Because of that, routing overhead is less. Routing protocol used must be such that it should use less bandwidth and has minimal overhead. Below table shows the types of routing protocols.

<table>
<thead>
<tr>
<th>Type</th>
<th>Characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proactive (Table Driven)</td>
<td>Routes are found in advance</td>
</tr>
<tr>
<td></td>
<td>Periodically route are updated and</td>
</tr>
</tbody>
</table>
### Distributed Routing Protocols

<table>
<thead>
<tr>
<th>Reactive (On-demand)</th>
<th>Hybrid</th>
</tr>
</thead>
<tbody>
<tr>
<td>- On demand, routes are discovered.</td>
<td></td>
</tr>
<tr>
<td>- No need for distributing routing information to other nodes</td>
<td></td>
</tr>
<tr>
<td>- Combination of both Proactive and Reactive protocols</td>
<td></td>
</tr>
</tbody>
</table>

In proactive, already the routes to each and every other node are maintained in the routing table. So without any delay, communication process can start. But problem arise when number of nodes are in large number, as it will increase the size of the routing table. In reactive, time is consumed in route discovery as it does not have readily available route to any node.

### SECURITY CONCERNS

Due to decentralized administration, dynamic topology, wireless nodes, restricted power and bandwidth constraints; MANETs are more easily exposed to security attacks. In below table, we show types of attacks possible in MANET.

<table>
<thead>
<tr>
<th>Type of Attack</th>
<th>Characteristics</th>
</tr>
</thead>
</table>
| Active Attack  | - Attacker may be internal or external  
|                | - Attacker can disturb Network operation by modifying or deleting data, fabricating messages or a node. |
| Passive Attack | - Information can be obtained without disturbing the normal network operation  
|                | - Detection is difficult |

In our paper, we will focus on the DoS attack which comes in the category of active attack.

### DOS ATTACKS

In DoS attacks, malicious nodes generate false messages regarding route to destination node. Sender sends the packets to the malicious node which actually drops the packets as it does not have route to destination. This disrupts the normal network operation by consuming the network resources. Here, we will discuss Blackhole attack along with existing solutions to detect and overcome it.
A. BLACKHOLE ATTACK

Blackhole attack is a type of DoS attacks where the malicious node sends the message of having the shortest valid route to the destination. A bogus route is established from source to malicious node and all the packets send to malicious node will be discarded and thus utilizes the network traffic. [10]

Figure-1 Blackhole Attack

1) Blackhole Attack Operation:

In figure 1, malicious node B is node that will reply with RREP packet in response to the RREQ packet broadcasted by Source node S for finding the path towards destination node D. S will establish route to B and packets will be send to B instead of actual D. All packets received by B will be dropped.

2) Detection and Prevention of Blackhole Attack:

Several approaches have been proposed to overcome Blackhole attack. Table IV gives details of some of methods for overcoming blackhole attacks along with their limitations.

<table>
<thead>
<tr>
<th>Approach</th>
<th>Technique</th>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks [4]</td>
<td>DRI and Cross Checking</td>
<td>A higher throughput performance almost 50% than AODV</td>
<td>5-8% more communication overhead of route request</td>
</tr>
<tr>
<td>Secure Routing with the AODV Protocol [6]</td>
<td>Cryptographic mechanism based solution. Encryption using symmetric key</td>
<td>Higher throughput and PDR compared to AODV</td>
<td>Higher routing overhead due to point to point encryption/decryption</td>
</tr>
</tbody>
</table>
DPRAODV: A Dynamic Learning System Against Black hole Attack in AODV based MANET\textsuperscript{[12]}

| Implementation of Routing Security Aspects in AODV \textsuperscript{[16]} | Sequence number compared with Threshold value and ALARM packet to neighbor nodes for isolating black hole node | The PDR is improved by 80-85% than AODV when under black-hole attack | May mistakenly block some non-malicious node due to its high Seq_no also little bit higher routing overhead and end-to-end delay

| Securing AODV: The A-SAODV Secure Routing Prototype \textsuperscript{[13]} | Only DN allowed to RREP, ALARM packet for isolation of black hole node | PDR of SAODV is more immune that AODV | Takes 1% more time to pass on data packets compared to AODV

| Securing Routing Table Update in AODV Routing Protocol \textsuperscript{[8]} | Digital Signature and adaptive reply decision | Some enhancements in SAODV to improve the performance | Increased overhead and complexity

| Secure AODV protocol to mitigate Black hole attack in Mobile Ad hoc Networks \textsuperscript{[7]} | Uses Enhanced Route discovery AODV (ERDA) to control the update of the routing table. | Isolates the attacker at initial stage, PDR increases up to 77% | Minimal overhead, Delay in attacker detection

| Uses the ratio of the number of RREQ to number of RREP forwarded by node in the network to detect a black hole attack | PDR increases by 78.6% | Well-connected nodes may falsely understood as malicious node, Time consuming technique

CONCLUSION AND FUTURE WORK

A Black Hole attack is one of the most severe security problems in MANET. Here, a malicious node imitates to be a destination node by sending fake RREP to a Source Node that initiates route discovery, and consequently deprives data traffic from the SN. In this paper, several solutions for MANET against Black are presented.

The existing solutions affect the MANET performance adversely in terms of throughput, delay and overhead. Although these may not be avoided totally, there is a need for trade-offs to achieve secure optimal performance. The detection of Black Holes in MANET is still considered to be a challenging task. Future work is intended to find an efficient Black Hole attack detection and elimination algorithm with trade-offs in delay and overheads that can be adapted for ad hoc networks susceptible to Black Hole attacks.
REFERENCES


