Black Hole Gray Hole Detection or Prevention by Using Table Driven Voting Approach in MANET

Sweta Dixit¹ Krishna K Joshi²
¹²Department of Computer Science Engineering/Information Technology
¹²MPCT Gwalior, India

Abstract—Mobile Ad-hoc Network is a dynamic environment, where nodes are moving from one network to other. This network is independent and autonomous. The dynamic infrastructure makes MANET vulnerable to different attacks which are responsible for degrading the network performance. Black hole attack pretends of having optimal path attract the sending node, once receives the packet, it results in dropping all the packets received by it. In case of gray hole, only selective packets are dropped. Detecting these attacks is a challenging issue. The proposed approach is based on table driven voting, which detects and prevent these attacks.

Key words: MANET, Black Hole Gray Hole Detection

I. INTRODUCTION

Unless like the existing or surviving networks Mobile Ad-hoc network (MANET) differ in the way that it does not depends on central control infrastructure for the functionality of the network, furthermore, all the links for transmission are made through wireless medium. In this all nodes in the network and itself acts as host and router and forward packets to the other neighboring node and in this way to the destination. MANET has many essential applications such as in disaster relief operations, military services in battlefield and in communication purposes, PANS and so on. The complexity in MANET is due to its dynamic infrastructure and the nodes are moving in nature. However there are still many open problems in the MANET few are as follows: security issues [1], transmission of bandwidth is finite [2], broadcasting of abusive messages [3], delivery of data is reliable [4], establishment of dynamic links [5] and because of use of hardware is restricted it causes capabilities in processing [6].

There are many issues related to security which have been seen in the recent years. MANET is vulnerable to various attacks they are snooping, black hole, wormhole, Gray Hole and poisoning, packet replication, denial of service (DoS), distributed `DDoS` attacks. But the key problem is when a node behaves maliciously [11] is the important issue and is popularly known as black hole attacks. Many researchers have proposed ideas to resolve this security issue, but still they are not able to prevent this problem completely from the network.

In this paper, we focus on gray hole and black hole attacks in MANET. Different detection schemes are discussed in a simple and clear way. Some areas of detection are routing overhead detection, PDR, throughput, packet drop etc.

In the following first we will discuss various attacks namely Black Hole and Gray Hole in MANET environment. Then will anatomiize various related literatures and discuss their problems. After that will give the proposed algorithm and work which we have discuss the outcomes of the same [3].

II. ATTACKS IN MANET

A. Single black hole attack

when a single malicious node makes use of routing protocol to pretend as it can provide the shortest route to the target node and drops all coming data packets from the source node and does not forward it to the neighbor. Such kind of attack is very common in MANET and it happens very easily. So when any node in the network wishes to exchange information with other node in between both nodes there is a misbehaving node replies to the sender node falsely as it is having the fastest route to the target. And on getting the request from the malicious node source node wrongly judges that the discovery for the route is completed and it forward packets to the misbehaving node. As explained above that misbehaving node either consumes packets or drops them. So this misbehaving node is generally known as black hole in MANET. This malicious node misroute data packets very easily and its result is that network suffers from its operations. It effects critically on PDR as it diminishes severely.

B. Collaborative Black hole attack

Some nodes with malicious behavior communicate with each other and collaborate and then mislead the normal route to their own created or fabricated route for the routing information. Generally the techniques which are applied on the single black hole attack are not applicable on collaborative/cooperative black hole attack as they are unable to find the cooperative black hole attack.

C. Single Gray hole

Gray Hole attack can be understood as a special case in black hole attack. It can be understood as a slow poison. In this type of attack the malicious or misbehaving node can either drop packets selectively or can refuse to forward the data packets and then drop them (i.e. it can drop in any way like it may drop half of the packet i.e. 50%, also can accept all the TCP packets coming to it and rejecting all the UDP packets, or can drop the packets having some possibility). The node which is behaving wrongly can sometimes behave just like other normal nodes after dropping the data packets. So due to these issues it is very hard to keep the network performance good. And also it is very difficult to find the attacks of such kind in the network. It generally has two phases. When the AODV algorithm advertises as having the new and valid route up to the destination is considered as the phase-I and so when nodes with malicious behaviour drops the 50% of probability and start behaving as normal node by switching is the second phase. It is also called as the misbehaving attack as it misbehaves while forwarding packets. So because of its misbehaving nature it is hard to detect such kind of attacks in the network.
D. Cooperative Gray Hole Attack

It is similar to cooperative black hole attack but in the cooperative Gray hole the nodes which form a group to cooperate and accomplish such attack are Gray Hole nodes in place of Black hole nodes. Gray Hole itself cannot be identified easily as it toggles its behaviour between normal and malicious and if group of them collude to perform an attack then the situation is worst. In node C is the Cooperative Gray Hole node which supports the Gray Hole node G to perform the attack.

III. AODV ROUTING PROTOCOL

Ad-hoc- on -demand distance vector (AODV) is a routing protocol which is generally used in the wireless ad-hoc MANET. It is the most widely used reactive protocol which creates its routes only when they are needed.

When two nodes wish to exchange data, they establish routes to transfer data packets. AODV protocol used DSDV protocol to establish the dynamic links. So when a node wishes to send data to other node first it find the fresh route if it is available and if not then it starts route discovery mechanism. For that the sender broadcasts RREQ(Route Request Message) to all the neighboring nodes. Then all the nodes who receives this RREQ message checks whether they are destination node or else they will find a fresh route for the destination and if the route requested is available then its sends a RREP(Route Request Reply) . Otherwise it forwards the RREQ message to its neighboring node in the same way by using flooding technique. This process is repeated till it gets the destination node. After finding the route then finally two nodes can communicate. RERR (Router Error) message is send to all the nodes if any node finds a breakage or error in the link.

Black hole has two phases: Firstly the black hole node exploits the routing protocol says it is AODV, to advertise as it is having the quickest path to the destination although the route available is spurious, with the intention of stopping packets to reach the destination. And secondly it consumes who the packets that are coming to it. The black hole attack in AODV protocol is mainly divided into mainly two kinds: RREQ and RREP Black Hole attack. Same as this gray hole also have II phases in first it claims as it can provide shortest path and in the second it drop packets in some random way and then switch to the normal node which makes it hard to detect.

A. V Related works

<table>
<thead>
<tr>
<th>S. no.</th>
<th>Paper</th>
<th>Year published in</th>
<th>Attacks detected</th>
<th>Technique used</th>
<th>Limitations</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>“Technique for Detection of Cooperative Black Hole Attack In MANET”</td>
<td>2014</td>
<td>Cooperative black hole attack.</td>
<td>Modifies existing AODV algorithm by introducing DRI and cross checking</td>
<td>PDR is less than 60% and is not able to detect gray hole attack.</td>
</tr>
<tr>
<td>2.</td>
<td>“Detection of Black Hole &amp; Gray Hole in MANET”</td>
<td>2014</td>
<td>Black hole and gray hole attacks.</td>
<td>It asks for the BBN for any restricted IP and after obtaining the RIP from any of the untouched IP.If the RREQ received by source node is just from the destination then it is considered to be normal otherwise malicious.</td>
<td>Does not address the problem of Cooperative gray hole.</td>
</tr>
<tr>
<td>3.</td>
<td>“Prevention of Cooperative Black Hole attack in MANET on DSR protocol using Cryptographic Algorithm”</td>
<td>2014</td>
<td>Both single and cooperative black hole attacks are detected.</td>
<td>It uses the concept of cryptographic algorithm RSA and sequence no. calculation for detecting black hole</td>
<td>It does not address the problem of gray hole attack and suffers from computational overhead.</td>
</tr>
<tr>
<td>4.</td>
<td>“A Technique To Establish Shortest Route In MANET By Detecting Multiple Cooperative Black Hole Attack”</td>
<td>2014</td>
<td>Single and cooperative black hole attack.</td>
<td>It uses a mechanism to attract malicious node by using false RREQ packets and for these false RREQ malicious node will reply with false RREQ.</td>
<td>Not providing any solution for gray hole attack.</td>
</tr>
<tr>
<td>5.</td>
<td>”Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks”</td>
<td>2003</td>
<td>Detects co-operative black hole attack.</td>
<td>Works on trust between the nodes.</td>
<td>Not able to detect gray hole attack and also due to cross-checking</td>
</tr>
</tbody>
</table>
2007
It detects both types of gray hole attacks.
Not effective if the neighboring nodes colludes.

7. A Defense Model for Black hole and Gray hole attacks in MANET
2014
Black Hole and gray hole attack, also reliable transmission of data.
It tries to construct a robust system by considering weaknesses of existing reactive protocol and give four different steps to solve such problem.
Not provide complete solution for all types of attacks.

Table 1

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of nodes</td>
<td>Variables (14,20, ...30)</td>
</tr>
<tr>
<td>Topographical dimensions</td>
<td>840 m x 541 m</td>
</tr>
<tr>
<td>Traffic Type</td>
<td>CBR</td>
</tr>
<tr>
<td>Signal Propagation Model</td>
<td>Two Ray Ground Model</td>
</tr>
<tr>
<td>MAC Type</td>
<td>802.11 MAC Layer</td>
</tr>
<tr>
<td>Packet size</td>
<td>1500 bytes</td>
</tr>
<tr>
<td>Mobility Model</td>
<td>Static</td>
</tr>
<tr>
<td>Antenna Type</td>
<td>Omni directional</td>
</tr>
</tbody>
</table>

IV. RESULTS
Table 2: Parameter Setting

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile Ad-hoc Routing</td>
<td>Protocol: AODV</td>
</tr>
<tr>
<td>Interface Queue</td>
<td>Drop Tail/ PriQueue</td>
</tr>
<tr>
<td>Maximum Packets in</td>
<td>Interface Queue: 50</td>
</tr>
<tr>
<td>Channel</td>
<td>Wireless Channel</td>
</tr>
<tr>
<td>Link Layer type</td>
<td>LL</td>
</tr>
<tr>
<td>Network Interface Type</td>
<td>Wireless Phy</td>
</tr>
<tr>
<td>Number of gray hole</td>
<td>attackers: Varies with scenario</td>
</tr>
<tr>
<td>attackers</td>
<td>14 nodes= 1 black and 1 gray hole</td>
</tr>
<tr>
<td></td>
<td>20 nodes=2 black and 2 gray hole</td>
</tr>
<tr>
<td></td>
<td>30 nodes=3 black and 3 gray hole</td>
</tr>
</tbody>
</table>

1) **Drop packet**

The number of packets drops when sender and receiver communicate and exchange information. In this the total number of packets drops is measured in seconds but here we defined in msec. The result below shows two graphs red line shows results for base work and green line shows results for our proposed work. Results are calculated when the number of nodes are 14.

2) **Packet Delivery Ratio (PDR)**

This parameter shows the total number of packets received by the receiver from the total number of packets send by the source node. It is also given in msec. Results show for 14 nodes.

3) **Throughput**

This parameter is used to calculate total number of data packets received over a period of time, it can be defined as: Throughput= \( \frac{N}{1000} \)

Where,

With the red line the graph for base graph is shown and with green line graph for our proposed algorithm is shown. Graph is basically drawn by considering mobility of nodes in X-axis verses drop packets delay on Y-axis (in milliseconds).

4) **Receiving Packet**

This parameter is basically used to calculate total receive packets by destination nodes. It is measured in msec. Red line show base algorithm results and green line shows proposed algorithm results.
Black Hole Gray Hole Detection or Prevention by Using Table Driven Voting Approach in MANET

(IJSRD/Vol. 3/Issue 1/2016/010)

All rights reserved by www.ijsrd.com

5) Routing Overhead
This parameter generally shows the traffic in the channel of network. If the traffic is more, then it will take more time for updating of routing table which ultimately will reduce performance. So it should be less. It is measured in seconds. But in these graphs end to end delay is given in msec. With the red line the graph for base graph is shown and with green line graph for our proposed algorithm is shown. Graph is basically drawn by considering mobility of nodes in X-axis verses drop packets delay on Y-axis (in milliseconds). able bandwidth of a communications protocol.

6) Forward Packet
Packet forwarding is the relaying of packet from one network segment to another by nodes in a computer network. It is measured in msec. With red line base results are shown and green line shows proposed algorithm results.

V. CONCLUSION
Various defense mechanisms have been implemented against these attacks. But has certain flaws. Detecting the behavior of theses attack is major issue. gray hole attacker behavior detection is difficult as this node acts as both in normal scenario and malicious way. On basis of voting the node is used for transmission. Voting is done on the basis of number of positive and negative nodes. If the number of positive nodes are more than the node will stay in the network and if the number of votes are equal or negative, then the node will be marked as blacklisted and every node will get message and it will be isolated from the network. This approach provides better results in terms of throughput, packet delivery ratio, routing parameters. The number of packets received is more and dropping of packet is low.

REFERENCES
in electronics and computer engineering (IJAEECE), Volume 1, Issue 6, pp.152-157, ISSN2278-1412Sep 2012.


