STUDY AND EVALUATION OF IMPROVED PERFORMANCE AGAINST BLACK HOLE ATTACK IN MANET

1Bhavesh Batra, 2Sadhna Rai, 3Monal Jain

Department of Computer Science Engineering, Swami Vivekanand University, Sagar (M.P), India

1bhaveshbatra257@gmail.com, 2raisadhna@gmail.com, 3monaljain92@gmail.com

Abstract: mobile ad-hoc network is a self organizing network that consists of mobile nodes that are capable of communicating with each other without the help of fixed infrastructure. In this research work the effect of black hole attack using AODV routing protocol. The simulation has been done using the network simulator. The performance metrics like average end to end delay, packet delivery ratio and routing overhead has been detected and analyzed with the variable node mobility. The user can analyse the results in base station where any physical mechanical change in environment are send by nodes of wireless mobile adhoc network. Suddenly the topologies of network can changes without reason. There is limitation in support system where each node play role like router and different node connect anywhere and diffuse the network at any time. The simulation results shown in the result section that when the black hole node exists in the network, it can be affected and decreased the performance of AODV routing protocol. So, the detection and prevention of black hole attack in the network exists as a challenging task, implement alternative path in AODV and best results.

Keywords: Black Hole Attack, AODV, Improved AODV, Performance Matrices.

I INTRODUCTION

Mobile ad-hoc network is a kind of wireless and is a self configuring network of mobile nodes connected by wireless link. The nodes are free to move independently and randomly bit capability of changing its link to other devices frequently. They should be capable to ensure that the packet is being transferred from source to destination. MANET is exposed to various kinds of attacks. Black holes are the places or the areas within which the attacker can either passively intercept or actively block information delivery and black hole is a malicious node that falsely replies for any route requests and drops all the receiving packets which are forwarded towards the destination. Each and every mobile node in an ad-hoc network moves arbitrarily and acts as both a router and a Host. The interconnections between nodes have the capacity of changing on a continuous and arbitrary basis. Nodes within the same radio range communicate directly via wireless links, but the nodes that are far away use other nodes as relays.

The rest of the paper is organized as follows. In Section 2, we introduce overview of overview of AODV, Section 3 black hole attack and Next Sections; we present a methodology to prevent a black hole attack. Finally, we conclude result, conclusion and discuss future work.

II AODV ROUTING PROTOCOL

AODV is one of the most common ad-hoc routing protocols used for mobile ad-hoc networks. As its name indicates AODV is an on-demand routing protocol that discovers a route only when there is a demand from mobile nodes in the network. The maintenance of routes to destination nodes that are not in active communication. Instead, it allows mobile nodes to quickly obtain routes to new destination nodes. Every mobile node maintains a routing table that stores the next hop node information for a route to the destination node. When a source node wishes to route a packet to a destination node, it uses the specified route if a fresh enough route to the destination node is available in its routing table. If such a route is not available in its cache, the node initiates a route discovery process by broadcasting a Route Request (RREQ) message to its neighbors. On receiving a RREQ message, the intermediate nodes update their routing tables for a reverse route to the source node. All the receiving nodes that do not have a route to the destination node broadcast the RREQ packet to their neighbors. Intermediate nodes increment the hop count before forwarding the RREQ. A Route Reply (RREP)
message is sent back to the source node when the RREQ query reaches either the destination node itself or any other intermediate node that has a current route to the destination. As the RREP propagates to the source node, the forward route to the destination is updated by the intermediate nodes receiving a RREP. The RREP message is a unicast message to the source node. AODV uses sequence numbers to determine the freshness of routing information and to guarantee loop-free routes. In case of multiple routes, a node selects the route with the highest sequence number. If multiple routes have the same sequence number, then the node chooses the route with the shortest hop count. Timers are used to keep the route entries fresh.

III BLACK HOLE ATTACK

In an ad-hoc network that uses the AODV protocol, a Black Hole node absorbs the network traffic and drops all packets. To explain the Black Hole Attack we added a malicious node that exhibits Black Hole behavior in the scenario. In this attack, a malicious node advertises that it has the best path to the destination node during the route discovery process. Whenever it receives the RREQ message, it immediately sends out a fake RREP to the source node. The source node first receives the RREP from the malicious node ahead of other RREPs. However, when the source node starts sending the data packet to the destination by using this route, the malicious node drops all packets instead of forwarding. We simulated the Black Hole attack in wireless ad-hoc networks and evaluated its damage in the network. Damage network means path break by using malicious node and solve out this problem by using Improved AODV.

First we need to modify aodv.cc and aodv.h files:
In aodv.h:
bool malicious;
In aodv.cc:
malicious = false;
if(strcmp(argv[1], "malicious") == 0) {
    malicious = true;
    return TCL_OK;
}

Next we need to modify the TCL file to set a malicious node:
$ns at 0.0 [\$mnode_(i) set ragent_] malicious"
if (malicious == true ) {
drop (p,DROP_RTR_ROUTE_LOOP);
}

Algorithmic approach to avoid black hole attack in MANETs

The solution that we propose here, basically, only modifies the working of the source node without altering intermediate and destination nodes. In this method two main things are added namely Data Routing Information table and cross checking.

Step1: Source node broadcasts RREQ to neighbors
Step2: Source node receives RREP from neighbors
Step3: Source node selects shortest and next shortest path based on the number of hops
Step4: Source node checks its routing table for single hop neighboring nodes only
Step5: If the neighbor node is in its routing table then route data packet
Else
The node is malicious and sends false packets to that node
Step 6: Invoke the route discovery
Inform all the neighboring nodes about the stranger
Step 7: Add the status of stranger to the routing table of source node
Step 8: Again send packet to neighboring node
Step 9: If step 5 repeats then broadcast the malicious node as black hole
Step 10: Update the routing table of source node after every broadcast
Step 11: Repeat step 4 to 10 until packet reaches the destination node correctly

From an actual destination node.

In an Improved AODV routing protocol used multiple path in routing protocol establishes multiple paths and data send using alternative path data transfer continuously.
IV IMPROVED AODV ROUTING PROTOCOL

In AODV routing protocol is not resetting a new alternative routing path during expire time, because it must maintain it until disconnecting nodes. So, we proposed improved AODV routing protocol for reset a new multiple routing path during sending packet. In order to minimize the route break recovery overhead. This scheme provides multiple routes on the intermediate nodes on the primary path to destination along with source node. The primary path is failed due to the attack and packet loss continuously the alternate path received by the source node after initiating the route discovery. so improved aodv routing protocol is best for reduced packet loss. So we used in this work focus on this methodology.

V RELATED WORKS

In wireless ad-hoc networks lack an infrastructure, they are exposed to a lot of attacks. One of these attacks is the Black Hole attack. In the Black Hole attack, a malicious node absorbs all data packets in itself, similar to a hole which sucks in everything in. In this way, all packets in the network are dropped. A malicious node dropping all the traffic in the network makes use of the vulnerabilities of the route discovery packets of the on demand protocols, such as AODV. In route discovery process of AODV protocol, intermediate nodes are responsible to find a fresh path to the destination, sending discovery packets to the neighbor nodes. Malicious nodes do not use this process and instead, they immediately respond to the source node with false information as though it has fresh enough path to the destination. Therefore source node sends its data packets via the malicious node to the destination assuming it is a true path. Black Hole attack may occur due to a malicious node which is deliberately misbehaving, as well as a damaged node interface. In any case, nodes in the network will constantly try to find a route for the destination.

an Improved AODV routing protocol used multiple path in routing protocol establishes multiple transmission paths between source nodes and destination node, which can not only transmit data in parallel, but also one as main path and others as backup paths for solve out link break problem and data send continuously without interruption.

VI SIMULATION PARAMETERS

Simulation Parameters is as follows

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routing Protocol</td>
<td>AODV, Blackhole aodv, Im aodv</td>
</tr>
<tr>
<td>Traffic Type</td>
<td>CBR</td>
</tr>
<tr>
<td>Simulation Time</td>
<td>100 to 400s.</td>
</tr>
<tr>
<td>Number Of Nodes</td>
<td>50</td>
</tr>
<tr>
<td>Pause Time</td>
<td>1.0 s</td>
</tr>
<tr>
<td>Maximum Connection</td>
<td>20</td>
</tr>
<tr>
<td>Maximum Speed</td>
<td>10 m/s</td>
</tr>
<tr>
<td>Transmission Rate</td>
<td>2.0 Mbps</td>
</tr>
<tr>
<td>Area of Networks</td>
<td>800m X 500m</td>
</tr>
</tbody>
</table>

VII PERFORMANCE METRICS

Protocols can be compared by evaluating various performance metrics as shown below:

*Packet Delivery Ratio (Fraction)*- It is calculated by dividing the number of packet received by destination through the number packet originated from source.

\[ \text{PDF} = \frac{\text{Pr}}{\text{Ps}} \]

where Pr is total Packet received and Ps is the total Packet sent.

*Average end-to end delay*- It is defined as the time taken for a data packet to be transmitted across an MANET from source to destination.

\[ D = \text{Tr} - \text{Tt} \]

where Tr is receive Time and Ts is sent Time.

*Normalized Routing Overhead*- It can also be defined as the ratio of routed packets to data transmissions in a single simulation. It is the routing overload per unit data delivered successfully to the destination node.
VIII SIMULATION MODEL

In this section, The Simulation environment consists of an area of 800x500, where randomly 50 mobile nodes are placed. A source and a destination is selected randomly. Data sources generate data according to Constant bit rate traffic pattern. Source destination pairs are spread randomly over the network. A packet size of 512 bytes is used. Mobility pattern of the mobile nodes is generated using Random waypoint model. By observing the performance of the network under mobility we can test the stability of design in real time scenario. Rate of 2Mbps is used [6, 9].

IX SIMULATION RESULT AND DISCUSSION

In the section, we analyzed the performance of under black hole attack using ns-2. The overall performance metrics gives in above. In random simulation environment, the first step is to determine the network delay on network performance with and without attack. Results are analyzed carefully by obtaining from NS-2 simulation. Its simulate a network of 50 mobile nodes. There is no prevention is applied, and then attacks will occurs. The false node is choose randomly in simulation test, and increases delay in network. The graphs show that with no black hole we get a maximum value of throughput and almost minimum delay. In this case all the packets send by the sender reaches the destination accurately i.e. there is minimum packet loss. So PDF is maximum in improved aodv. The overall results shown in below by using xgraph with Varying Simulation time.

X CONCLUSION & FUTURE WORK

In this paper simulations are analyzed having simulated the Black Hole Attack using NS-2 software find out the results in wireless environment. We saw that the packet loss is increased in the ad-hoc network with the affect of black hole attack. The simulation results show the difference between the number of packets lost in the network with and without a Black Hole Attack and improved AODV. This also shows that Black Hole Attack affects the overall network connectivity and the data loss could show the existence of the Black Hole Attack in the network. If the number of Black Hole Nodes is increased then the data loss would also be expected to increase.

REFERENCES:

[9] Nital Mistry, Devesh C Jinwala, Member, IAENG, Mukesh Zaveri “Improving AODV Protocol against Blackhole Attacks” proceeding of the international multi conference of engineers and computer scientists 2010 VOL II.