Performance of AODV against Black Hole Attacks in Mobile ad-hoc Networks

SUSHIL KUMAR CHAMOLI
Graphic Era University
Dehradun, India
sushilchamoli@gmail.com

SANTOSH KUMAR
Graphic Era University
Dehradun, India
amu.santosh@gmail.com

DEEPAK SINGH RANA
Graphic Era University
Dehradun, India
deepakcham@gmail.com

Abstract

Wireless mobile ad hoc network (MANET) is a self-configuring network which is composed of several movable mobile nodes. These mobile nodes communicate with each other without any infrastructure. As 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 Black Hole attack, a malicious node falsely advertises shortest path to the destination node and absorbs all data packets in it. In this way, all packets in the network are dropped. In this paper, performance of AODV is evaluated in presence of black hole attack (malicious node) and without black hole attack with cbr traffic under different scalable network mobility. For this analysis RWP model is used.

Keywords: MANET, AODV, Black Hole attack, malicious node, PDR.

1. Introduction

Mobile Ad-hoc network (MANET) has become an individual part for communication for mobile device. Mobile devices or nodes in the network are free to enter or leave the network. As a result, network topology will change frequently. In MANET, mobile nodes which are in the same communication range can communicate directly amongst them. MANET is widely used in military purpose, disaster area, personal area network and so on [1]. The network nodes in a MANET, not only act as the ordinary network nodes but also as the routers for other peer devices [2]. The network layer in MANET is susceptible to various attacks viz. eavesdropping with a malicious intent, spoofing the control and/or data packets transacted, malicious modification/alteration of the packet contents and the Denial-of-service (DoS) attacks viz. Wormhole attacks, Sinkhole attacks, Black hole attacks [4]. Amongst these, we attempt in analyzing and improving the security of the routing protocol AODV [5] against the Black hole attacks.

Black hole is one of many attacks that take place in MANET and is considered as one of the most common attacks made against the AODV routing protocol. The black hole attack involves malicious node pretending to have the shortest and freshest route to the destination by constructing false sequence number [3] in control messages. AODV protocol was created without any security considerations [4]. Thus, no protection mechanism was built to detect the existence of malicious attack. In the AODV, maintaining a fresh route to ensure safe path to destination is very vital due to the rapid change of the network topology. The manipulation done by the malicious node will deny the genuine Route Reply (RREP) message from other nodes especially the reply message coming from the actual destination node.

We study various methods proposed to overcome the black hole attack in the AODV-based MANET. In this paper we show a node as a malicious node which behave as a black hole attack in AODV.

2. Ad-hoc On-Demand Distance Vector (AODV)

AODV is categorized as a dynamic reactive routing protocol [5]. In a reactive routing protocol, route will be established based on the demand (upon request by source node). Ad-hoc On-Demand Distance Vector (AODV) [13] Routing Protocol is used for finding a path to the destination in an ad-hoc network. To find the path to the destination all mobile nodes work in cooperation using the routing control messages. In AODV route discovery, there are two important control
messages namely Route Request (RREQ) and Route Reply (RREP). Both control messages carry an important attribute called destination sequence number and has the incremental value to determine the freshness of a particular route.

2.1 Route Discovery Process

In this, the source node will broadcast control packets, RREQ message to its neighbors in order to find the best possible path to the destination node. On receiving the RREQ message from node, the destination node will reply with the RREP message to node by forwarding the message to the node. In turn, node will forward the message to the source node. Once the source node received the RREP message, it will process the message by calling the AODV recvReply() function. This function will update the route entry for destination if either the destination sequence number in the routing table is less than the destination sequence in the RREP message or the destination sequence number in the routing table is equal with the destination sequence number in the RREQ message but the hop count is less than the one in the routing table. In case where source node received multiple RREP messages, this function will select the RREP message with the highest destination sequence number value.

3. Black Hole Attack

A Black Hole attack [5] is a kind of denial of service where a malicious node can attract all packets by falsely claiming a fresh route to the destination and then absorb them without forwarding them to the destination. Cooperative Black hole means the malicious nodes act in a group [10]. When the source node wishes to transmit a data packet to the destination, it first sends out the RREQ packet to the destination. Cooperative Black hole means the malicious nodes act in a group [10]. When the source node wishes to transmit a data packet to the destination, it first sends out the RREQ packet to the neighboring nodes. The malicious nodes being part of the network, also receive the RREQ. Since the Black hole nodes have the characteristic of responding first to any RREQ, it immediately sends out the RREP. The RREP from the Black hole reaches the source node, well ahead of the other RREPs. Now on receiving the RREP from the Black hole node, the source starts transmitting the data packets. On the receipt of data packets, the Black hole node simply drops them, instead of forwarding to the destination.

In black hole attack [6] a malicious node can detects the active route and notes the destination address or can be send a route reply packet (RREP) including the destination address field spoofed to an unknown destination address. Hop count value is set to lowest values and the sequence number is set to the highest value. Malicious node send RREP to the nearest available node which belongs to the active route. This can also be send directly to the data source node if route is available. The RREP received by the nearest available node to the malicious node will relayed via the established inverse route to the data of source node. The new information received in the route reply will allow the source node to update its routing table. New route selected by source node for selecting data. The malicious node will drop now all the data to which it belong in the route.

The malicious node will claim that it has the ‘fresh enough route’ information to the destination. If the other nodes fall into this trap, they will send their data packets through the malicious node.

4. Related Works in Detecting Black Hole Attack

There have been quite a number of works done in securing the routing protocol in MANET from the black hole attack.

M.A. Shurman [5] in his work has proposed for the source node to verify the authenticity of the node that initiates the RREP messages by finding more than one route to the destination, so that it can recognize the safe route to the destination. This method can cause routing delay, since a node has to wait for a RREP packet to arrive from more than two nodes.

S. Yi [7] proposed a solution which looked at the Security-Aware Ad hoc Routing (SAR) using the security attributes such as trust values and relationships.

N.H. Mistry in [8] has proposed for the source node to verify the RREP destination sequence number by analysing the RREP messages which arrived within the predefined waiting period by using the heuristic method. If the sequence number is found to be exceptionally high, the sender of the respective RREP
will be marked as malicious node. The major issue in this method is the latency time during the route discovery process since the source node has to wait until the waiting time period expired before the routing table can be updated. In the event where there is no attack in the network, the node still suffers with the latency time.

Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto’s [9], proposed an anomaly detection scheme using dynamic training method in which the training data is updated at regular time intervals.

S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, K. Nygard [10] proposed a solution that contain a data routing information table where 1 stands for ‘true’ and 0 for ‘false’. Whenever a RREP is received a cross check is done to verify whether the reply is from a legitimate node or not.

According to V Sankaranarayanan and Latha Tamilselvan [11], they projected a technique that source will verify the reply packet coming from various nearest nodes to wait and check the replies from all the neighboring nodes to discover best possible and secure route.

5. Analysis of Black Hole Attack in AODV

In this section, analysis performed on different topologies to compare the performance of AODV with and without black holes (malicious node) in the network.

Without malicious node: In present analysis first, AODV protocol (without any malicious node) is used to calculate PDR and End to end delay with different parameters.

With malicious node: To simulate Black Hole attacks, we first create a new Black Hole node (malicious node) in AODV. To create a node as a malicious node in AODV first we declare a malicious variable. With this malicious variable we are trying to define if the node is malicious or not. This parameter can be either true or false value. By default, the value is set to false. Now we add a code in recvRequest() function for a malicious node. Since the malicious node is the first node to response with the RREP message to source node, the routing table of source node is updated with the information of malicious node. The malicious node receives the packets from source node and drops all packets. In this analysis, node number 5 is created as a malicious node and will drop all the packets. To compare the performance PDR and End to end delay are calculated with different parameters as node 20, 30, 40, 50 and mobility from 1m/s to 50m/s.

6. Simulation Environments

For the simulations, NS-2 (v-2.35) network simulator is used. At the physical and data link layer, IEEE 802.11 is used. The channel used is Wireless Channel with Two Ray Ground radio propagation model. At the network layer, AODV is used as the routing protocol. UDP is used at the transport layer. All the data packets are CBR (continuous bit rate) packets. The size of the packet is 512 bytes. The packets transmission rate is 0.2 Mbps, simulation time is 500s, pause time is 20s. The connection pattern is generated using cbrgen and the mobility model is generated using setdest utility. The terrain area is 800m X 800m with 20, 30, 40, 50 nodes and maximum speed up to from 1 m/s to 50 m/s. Each data point represents an average of five runs as malicious node and without malicious node. The same connection pattern and mobility model is used in simulations to maintain the uniformity across the protocols.
In Figure 1(b) node number 5 is as a black hole node which drops all the packets on receiving from source node.

6.1 Metrics used for Simulation

On the bases of simulation parameters we calculate PDR and End to end delay with malicious node and without malicious node.

PDR (Packet Delivery Ratio): Packet Delivery Ratio = Total Packets Received / Total Packets Sent. The ratio of the number of data packets successfully delivered to the destinations to those generated by CBR sources. Packet delivery ratio describes the loss rate.

Average End to End delay: This is the average delay between the sending of the data packet by the CBR source and its receipt at the corresponding CBR receiver. It is measured in milliseconds.
then, PDR is decreasing with malicious node (black hole) and End to End delay is increasing with black hole attack.

Figure 3 (a) shows the graph when mobility of nodes is varying then, PDR is decreasing with malicious node. Figure 3 (b) shows End to End delay when mobility varying it effect on AODV with presence of the malicious node.

7 Conclusions and Future Work

In this paper, we analyze the performance of AODV with and without black hole (malicious node) attack under the circumstances of different parameters. Simulation results show, that when a node become as a malicious node it will effect on the AODV performance. The route discovery process in the AODV is susceptible to black hole attack and therefore, it is vital to have an efficient security functions in the protocol in order to avoid such attacks.

As future work, we intend to perform the solution for the black hole attack and apply this for with different routing protocols like DSR, TORA.

References:


