Mathematical Statistician and Engineering Applications
ISSN:2094-0343
2326-9865

A Study of Detecting Black Hole Attack INAD-HOC On-Demand Distance Vector (AODV) Protocol

Research Scholar – Mohit Srivastava[1]

Department of Computer Application,Sri Satya Sai University of Technology & Medical Sciences, Sehore,MP,India

Research Guide - **Dr. Rajendra Singh Kushwah[2]**

Department of Computer Application,Sri Satya Sai University of Technology & Medical Sciences, Sehore,MP,India

Article Info
Page Number: 13590- 13596
Publication Issue:
Vol 71 No. 4 (2022)

Abstract

Security is an essential requirement in mobile ad hoc networks to provide protected communication between mobile nodes. MANETs are vulnerable to various attacks; black hole is one of the possible attacks. Black hole is a type of routing attack where a malicious node advertise itself as having the shortest path to all nodes in the environment by sending fake route reply. We attempt to focus on Analysing and improving the security of one of the popular routing protocol for MANETS viz. the Ad hoc On Demand Distance Vector (AODV) routing protocol. Our focus specifically, is on ensuring the security against the Black hole Attacks. We propose modifications to the AODV protocol and justify the solution with appropriate implementation. Mobile Adhoc Network (MANET) consists of a collection of wireless mobile without the required intervention of any existing infrastructure or centralized access point such as base station. The dynamic topology of MANET allows nodes to join and leave the network at any point of time. Wireless MANET is particularly vulnerable due to its fundamental characteristics such as open medium, dynamic topology, distributed cooperation and constrained capability. So security in MANET is a complex issue. There are many routing protocols that establish the routes between the nodes in the network. The control towards the management of the nodes in the MANET is distributed. This feature does not give assurance towards the security aspects of the network. There are many routing attacks caused due to lack of security.

Article History
Article Received: 15 September 2022
Revised: 15 October 2022
Accepted:20 December 2022

Keywords-MANET; Black hole; AODV; RREQ; RREP; RERR.

Introduction

A mobile ad hoc network (MANET) is formed by a set of mobile wireless devices with no fixed topology. The nodes can move freely, leave and enter the network at any time. Typically, nodes communicate in a peer-topeer fashion by using the wireless radio medium. In a MANET, there is no distinction between a host and a router, since all nodes can be sources as well as traffic forwarders. Some examples of the possible uses of ad hoc networking include students using laptop computers to participate in an interactive lecture, business associates sharing information during a meeting, soldiers relaying information for

situational awareness on the battlefield, and emergency disaster relief personnel coordinating efforts after a hurricane or earthquake. We have different routing protocols for route discovery and packet forwarding. The paper is organised as follows. In Section 2 we briefly describe the AODV routing protocol. Section 3 discusses about black hole attack, Section 4 we discuss our solution to AODV algorithm. Finally, we conclude in Section 5 with future scope.

Overview Of Aodv

AODV is a reactive routing protocol [1] in which the network generates routes at the start of communication. Each node has its own sequence number and this number increases when links change. Each node judges whether the channel information is new according to sequence numbers. Figure 1 illustrates the route discovery process in AODV. In this figure, node S is trying to establish a connection to destination D. First, the source node S refers to the route map at the start of communication. In case where there is no route to destination node D, it sends a Route Request (RREQ) message using broadcasting. RREQ ID increases one every time node Ssends a RREQ. Node A and B which have received RREQ generate and renew the route to its previous hop. They also judge if this is a repeated RREQ. If such RREQ is received, it will be discarded. If A and B has a valid route to the destination D, they send a RREP message to node S. By contrast, in case where the node has no valid route, they send a RREQ using broadcasting. The exchange of route information will be repeated until a RREQ reaches at node D. When node D receives the RREQ, it sends a RREP to node S. When node S receives the RREP, then a route is established. In case a node receives multiple RREPs, it will select a RREP who's the destination sequence number (DstSeq) is the largest amongst all previously received RREPs. But if DstSeq were same, it will select the RREP whose hop count is the smallest.

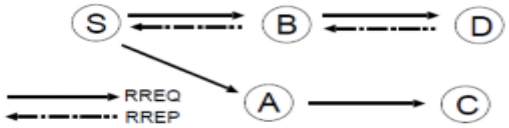

Figure 1: Route discovery process

In Figure 2, when node B detects disconnection of route, it generates Route Error (RERR) messages and puts the invalidated address of node D into list, then sends it to the node A. When node A receives the RERR, it refers to its route map and the current list of RERR messages. If there was a route to destination for node D included in its map, and the next hop in the routing table is a neighbouring node B, it invalidates the route and sends a RERR message to node S. In this way, the RERR message can be finally sent to the source node S.

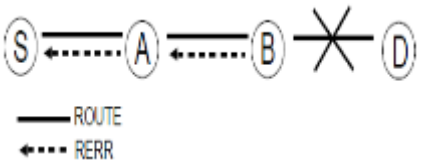

Figure 2: Transferring route error messages

Advantages Of Aodv

1. AODV protocol is a flat routing protocol it does not need any central administrative system to handle the routing process.

2. AODV tries to keep the overhead of the messages small. If host has the route information in the Routing Table about active routes in the network, then the overhead of the routing process will be minimal. The AODV has great advantage in overhead over simple protocols which need to keep the entire route from the source host to the destination host in their messages. The RREQ and RREP messages, which are responsible for the route discovery, do not increase significantly the overhead from these control messages. AODV reacts relatively quickly to the topological changes in the network and updating only the hosts that may be affected by the change, using the RRER message. The Hello messages, which are responsible for the route maintenance, are also limited so that they do not create unnecessary overhead in the network.

3. The AODV protocol is a loop free and avoids the counting to infinity problem, which were typical to the classical distance vector routing protocols, by the usage of the sequence numbers.

4. The AODV protocol will perform better in the networks with static traffic with the number of source and destination pairs is relatively small for each host.

Disadvantages Of Aodv

1. Intermediate nodes can lead to inconsistent routes if the source sequence number is very old and the intermediate nodes have a higher but not the latest destination sequence number, thereby having stale entries.

2. Multiple Route Reply packets in response to a single Route Request packet can lead to heavy control overhead.

3. The periodic beaconing leads to unnecessary bandwidth consumption.

Description Of Blackhole Attack

Routing protocols are exposed to a variety of attacks. Black hole attack is one such attack and a kind of Denial Of Service (DoS) in which a malicious node makes use of the vulnerabilities of the route discovery packets of the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept [2]. This attack aims at modifying the routing protocol so that traffic flows through a specific node controlled by the attacker. During the Route Discovery process, the source node sends RREQ packets to the intermediate nodes to find fresh path to the intended destination. Malicious nodes respond immediately to the source node as these nodes do not refer the routing table. The source node assumes that the route discovery process is complete, ignores other RREP messages from other nodes and selects the path through the malicious node to route the data packets. The malicious node does this by assigning a high sequence number to the reply packet. The tracker now drops the received messages instead of relaying them as the protocol requires. In

AODV, DstSeq is used to determine the freshness of routing information contained in the message from originating node. When generating a RREP message, a destination node compares its current sequence number, and DstSeq in the RREQ packet plus one, and then selects the larger one as RREP's Dst Seq. Upon receiving a number of RREP, a source node selects the one with greatest DstSeq in order to construct a route. To succeed in the blackhole attack the attacker must generate its RREP with DstSeq greater than the DstSeq of the destination node. It is possible for the attacker to find out DstSeq of the destination node from the RREQ packet. In general, the attacker can set the value of its RREP's DstSeq base on the received RREQ's Dst Seq. However, this RREQ's DstSeq may not present the current DstSeq of the destination node. Figure 3 shows an example of the blackhole attack. As an example, consider the following scenario in fig. 3. We illustrate a typical scenario of the protocol packet exchanges, depicting the generation and traversal of RREQ and RREP control messages.

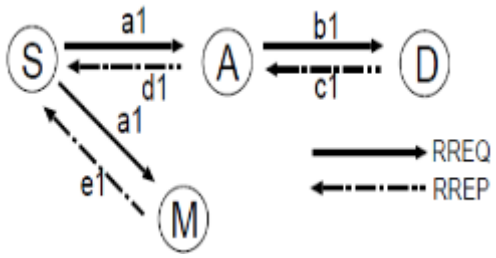

Figure 3: Blackhole attack

The node S is assumed to be the source node desiring to communicate with node D. Thus, as per the explanation earlier, node S would generate the RREQ control message and broadcast it. The broadcasted RREQ control message is expected to be received by the nodes N1, N2 and N3. Assuming that the node N3 has a route to node D in its route table, the node N3 would generate a RREP control message and update its routing table with the accumulated hop count and the destination sequence number of the destination node. Destination Sequence Number is a 32-bit integer associated with every route and is used to decide the freshness of a particular route. The larger the sequence number, the fresher is the route [3]. Node N3 will now send it to node. Since node N1 and node N2 do not have a route to node D, they would again broadcast the RREQ control message. RREQ control message broadcasted by node N3 is also expected to be received by node M (assumed to be a malicious node). Thus, node M being malicious node, would generate a false RREP control message and send it to node N3 with a very high destination sequence number, that subsequently would be sent to the node S. However, since, the destination sequence number is high, the route from node N3 will be considered to be fresher and hence node S would start sending data packets to node N3. Node N3 would send the same to the malicious node. The RREQ control message from node N1, would eventually reach node D (destination node), which would generate RREP control message and route it back. However, since the node S has a RREP control message with higher destination sequence number to that route, node S will ignore two genuine RREP control messages. If any link is disconnected during the transfer of packets then RERR control message is generated. For every RREP control message received, the source node would first check whether it has an entry for the destination in the route table or not. If it

finds one, the source node would check whether the destination sequence number in the incoming control message is higher than one it sent last in the RREQ or not. If the destination sequence number is higher, the source node will update its routing table with the new RREP control message; otherwise the RREP control message will be discarded. In Route Maintenance phase, if a node finds a link break or failure, then it sends RERR message to all the nodes that uses the route.

First set the waiting time for the source node to receive the RREQ coming from other nodes and then add the current time with the waiting time. Then in storing process, store all the RREQ Destination Sequence Number (DSN) and its Node Id in RR-Table until the computed time exceeds. Generally the first route reply will be from the malicious node with high destination sequence number, which is stored as the first entry in the RR-Table. Then compare the first destination sequence number with the source node sequence number, if there exists much more differences between them, surely that node is the malicious node, immediately remove that entry from the RR-Table. This is how malicious node is identified and removed. Final process is selecting the next node id that has the higher destination sequence number, is obtained by sorting the RR-Table according to the DSEQ-NO column, whose packet is sent to ReceiveReply method in order to continue the default operations of AODV protocol.

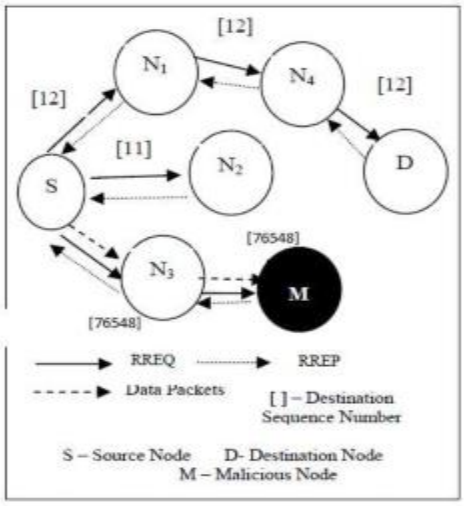

Fig 4: Protocol Packet Exchanges

Table 1 Content of RR-table with malicious node

RNO	DSEQ-NO	NODE-ID
1.	76548	N3
2.	11	N2
3.	12	N1

Table 2 Content of RR-table without malicious node

RNO	DSEQ-NO	NODE-ID
1.	12	N1
2.	11	N2

Solutions For Blackhole Attack

Latha Tamilselvan, Dr. V Sankaranarayanan[4] proposed a solution with the enhancement of the AODV protocol which avoids multiple black holes in the group. A technique is give to identify multiple black holes cooperating with each other and discover the safe route by avoiding the attacks. It was assumed in the solution that nodes are already authenticated and therefore can participate in the communication. It uses Fidelity table where every node that is participating is given a fidelity level that will provide reliability to that node. Any node having 0 value is considered as malicious node and is eliminated. HesiriWeerasinghe [5] proposed the solution which discovers the secure route between source and destination by identifying and isolating cooperative black hole nodes. This solution adds on some changes in the solution proposed by the S.Ramaswamy to improve the accuracy. This algorithm uses a methodology to identifymultiple black hole nodes working collaboratively as a group to initiate cooperative black hole attacks. This protocol is a slightly modified version of AODV protocol by introducing Data Routing Information (DRI) table and cross checking using Further Request (FREQ) and Further Reply (FREP). Most of the papers have addressed the black hole problem on the protocol such as AODV. Payal N. Raj, Prashant B. Swadas [6] proposed "DPRAODV: A dynamic learning system against black hole attack in AODV based MANET" (detection, prevention and reactive AODV) to prevent security of black hole by informing other nodes in the network. It uses normal AODV in which a node receives the Route reply (RREP) packet which first checks the value of sequence number in its routing table. The RREP is accepted if its sequence is higher than that in the routing table. It also check whether the sequence number is higher than the threshold value, if it is higher than threshold value than it is considered as the malicious node. The value of the threshold value is dynamically updated in the time interval. The threshold value is the average of the difference of destination sequence number in each time slot between the sequence number in the routing table and the RREP packet. The node that is detected as the anomaly is black listed and ALARM packet is sent so that the RREP packet from that malicious node is discarded. The routing table for that node is not updated nor is the packet forwarded to others. The main advantage of this protocol is that the source node announces the black hole to its neighbors in order to be ignored and eliminated. Their solution increases the average end to end delay and normalized routing overhead. Zhao Min et.al [7] has proposed a cryptographic based solution (ZHAO), that is, an authentication mechanism for identifying black hole nodes in MANETs. An authentication mechanism is constructed based on the concept of the hash function and Message Authentication Code (MAC) which is used for checking the RREPs at source node to send the data packets. The proposed mechanism eliminates the need for a PKI (Public Key Infrastructure) or other forms of authentication infrastructure, however it needs to be discussed, how to handle unlimited message authentication by switching one-way-hash chains and how to prevent a malicious node cannot forge a reply if the hash key of any nodes to be disclosed to all nodes. This solution consumes much of the computation power of the MANET nodes.

Conclusion

In this paper we have mentioned the AODV protocol and Black hole attack in MANETs. We have proposed a feasible solution for the black hole attacks that can be implemented on the AODV protocol. These Proposed methods can be used to find the secured routes and prevent the black hole nodes in the MANET. As future work, we intend to develop an algorithm which can detect the Black hole attack and save our network when a number of malicious nodes attack network at same time.

References

[1] C. E. Perkins, E. M. B. Royer, and S. R. Das, Ad hoc On-Demand Distance Vector (AODV) routing, RFC3561, July 2003

[2] Nital Mistry, Devesh C Jinwala, Improving AODV Protocol against Blackhole Attacks, International MultiConferenceOf Engineers and Computer Scientists 2010 Vol II IMECS 2010.

[3] Satoshi Kurosawal, Hidehisa, Nakayama, Nei Kato, Abbas Jamalipour and Yoshiaki Nemoto. Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method. International Journal of Network Security, Vol. 5, No.3, pp.338–346, Nov. 2007

[4] Tamilselvan, L. Sankaranarayanan, V. Prevention of Blackhole Attack in MANET ,JournalOfNetworks. Vol.3, No.5, May2008.

[5] HesiriWeerasinghe and Huirong Fu, Member of IEEE, Preventing Cooperative Black Hole Attacks in Mobile Adhoc Networks: Simulation implementation And Evaluation, IJSEA,Vol2,No.3,July 2008.

[6] Payal N. Raj and Prashant B. Swadas (2009) DPRAODV: A dynamic learning system against black hole attack in AODV based Manet. International Journal of Computer Science Issues (IJCSI), Vol. 2, Issue 3, pp: 54-59.

[7] Zhao Min; Zhou Jiliu.(2009). Cooperative Black Hole Attack Prevention for Mobile Ad Hoc Networks. International Symposium on Information Engineering and Electronic Commerce, 2009. IEEC '09 26 – 30

[8] ImrichChlamtac, Marco Conti, Jennifer J.-N. Liu “Mobile ad hoc networking: imperatives and challenges”, School of Engineering, University of Texas at Dallas, Dallas, TX, USA, 2003.

[9] Gianni A. Di Caro, Frederick Ducatelle, Luca M. Gambardella. “A simulation study of routing performance in realistic urban scenarios for MANETs”. In: Proceedings of ANTS 2008, 6th International Workshop on Ant Algorithms and Swarm Intelligence, Brussels, Springer, LNCS 5217, 2008