Modified AODV Protocol against Blackhole Attacks in MANET

K. Lakshmi[1], S.Manju Priya[2] A.Jeevarathinam[3] K.Rama[4], K. Thilagam[5]
[1]Lecturer, Dept. of Computer Applications, Karpagam University, Coimbatore.
[2 & 5]Research Scholar, Karpagam University, Coimbatore.
[3& 4] Lecturer, Dept. of Computer Science, Karpagam University, Coimbatore.
lakshmi_kathir14@yahoo.co.in, ssmp_manju2003@yahoo.co.in, jeevs_jeeth@yahoo.co.in

Abstract—**Mobile Adhoc Network (MANET) consists of a collection of wireless mobile hosts 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 features does not give assurance towards the security aspects of the network. There are many routing attacks caused due to lack of security.**

In this paper, therefore, we attempt to focus on analyzing and improving the security of one of the popular routing protocol for MANET viz. the Adhoc On Demand Distance Vector (AODV) routing protocol. Our focus specifically, is on ensuring the security against the Blackhole Attack. The proposed solution is that capable of detecting and removing black hole nodes in the MANET at the initial stage itself without any delay.

Keywords-MANET; Blackhole; AODV; RREQ; RREP; RERR.

1. INTRODUCTION

In areas in which there is little or no communication infrastructure or the existing infrastructure is expensive or inconvenient to use, wireless mobile users may still be able to communicate through the formation of an ad hoc network [1]. In such a network, each mobile node operates not only as a host but also as a router, forwarding packets for other mobile nodes in the network that may not be within direct wireless transmission range of each other. Each node participates in an adhoc routing protocol that allows it to discover "multihop" paths through the network to any other node.

The idea of adhoc networking is sometimes also called infrastructure less networking [1], since the mobile nodes in the network dynamically establish routing among themselves to form their own network "on the fly." 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. Many different protocols have been proposed to solve the multihop routing problem in ad hoc networks, each based on different assumptions and intuitions.

The rest of this paper is organized as follows. In Section 2 we briefly describes the different types of routing protocols with its descriptions and detail note on AODV routing protocol. Section 3 discusses about blackhole attack. Section 4 presents the related work in literature, Section 5 we discuss our solution to AODV algorithm. Finally, we conclude in Section 6 with future scope.

2. ROUTING PROTOCOLS

The primary goal of routing protocols in ad-hoc network is to establish optimal path (min hops) between source and destination with minimum overhead and minimum bandwidth consumption so that packets are delivered in a timely manner. A MANET protocol should function effectively over a wide range of networking context from small ad-hoc group to larger mobile Multihop networks. As fig 1 shows the categorization of these routing protocols.
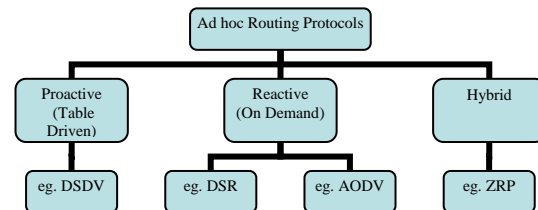

Fig 1. Hierarchy of Routing Protocols

Routing protocols can be divided into **proactive, reactive and hybrid protocols**, depending on the routing topology. Proactive protocols are typically table-driven. Examples of this type include Destination Sequence Distance Vector (DSDV). Reactive or source-initiated on-

demand protocols, in contrary, do not periodically update the routing information. It is propagated to the nodes only when necessary. Example of this type includes Dynamic Source Routing (DSR) and Ad Hoc On-Demand Distance Vector (AODV). Hybrid protocols make use of both reactive and proactive approaches. Example of this type includes Zone Routing Protocol (ZRP).

A. Proactive Routing Protocol

In a network utilizing a proactive routing protocol, every node maintains one or more tables representing the entire topology of the network. These tables are updated regularly in order to maintain up-to-date routing information from each node to every other node. To maintain the up-to-date routing information, topology information needs to be exchanged between the nodes on a regular basis, leading to relatively high overhead on the network. On the other hand, routes will always be available on request. Many proactive protocols stem from conventional link state routing, including the Optimized Link State Routing protocol (OLSR).

B. ReactiveRrouting Protocol

Reactive routing protocols [1] are on-demand protocols. These protocols do not attempt to maintain correct routing information on all nodes at all times. Routing information is collected only when it is needed, and route determination depends on sending route queries throughout the network. The primary advantage of reactive routing is that the wireless channel is not subject to the routing overhead data for routes that may never be used. While reactive protocols do not have the fixed overhead required by maintaining continuous routing tables, they may have considerable route discovery delay. Reactive search procedures can also add a significant amount of control traffic to the network due to query flooding. Because of these weaknesses, reactive routing is less suitable for real-time traffic or in scenarios with a high volume of traffic between a large numbers of nodes.

C. Hybrid Routing Protocol

Wireless hybrid routing is based on the idea of organizing nodes in groups and then assigning nodes different functionalities inside and outside a group [1]. Both routing table size and update packet size are reduced by including in them only part of the network (instead of the whole); thus, control overhead is reduced. The most popular way of building hierarchy is to group nodes geographically close to each other into explicit clusters. Each cluster has a leading node (*cluster head*) to communicate to other nodes on behalf of the cluster. An alternate way is to have implicit hierarchy. In this way, each node has a local scope. Different routing strategies are used inside and outside the scope. Communications

pass across overlapping scopes. More efficient overall routing performance can be achieved through this flexibility. Since mobile nodes have only a single omni-directional radio for wireless communications, this type of hierarchical organization will be referred to as logical hierarchy to distinguish it from the physically hierarchical network structure.

D. An Overview of AODV Routing Protocol

AODV routing protocol is based on DSDV and DSR algorithm and is a state-of-the-art routing protocol that adopts a purely reactive strategy: it sets up a route on-demand at the start of a communication session, and uses it till it breaks, after which a new route setup is initiated [2]. This protocol is composed of two mechanism (1) Route Discovery and (2) Route Maintenance. AODV uses **R**oute **Req**uest (RREQ), **R**oute **Rep**ly (RREP) control messages in Route Discovery phase and **R**oute **Err**or (RERR) control message in Route Maintenance phase. The header information of this control messages can be seen in detail in [3].

In general, the nodes participating in the communication can be classified as source node, an intermediate node or a destination node. With each role, the behavior of a node actually varies. When a source node wants to connect to a destination node, first it checks in the existing route table, as to whether a fresh route to that destination is available or not. If a fresh enough route is available, it uses the same. Otherwise the node initiates a Route Discovery by broadcasting a RREQ control message to all of its neighbors. This RREQ message will further be forwarded (again broadcasted) by the intermediate nodes to their neighbors. This process will continue until the destination node or an intermediate node having a fresh route to the destination. At this stage eventually, a RREP control message is generated. Thus, a source node after sending a RREQ waits for RREPs to be received. Fig. 2 depicts the traversal of control messages.
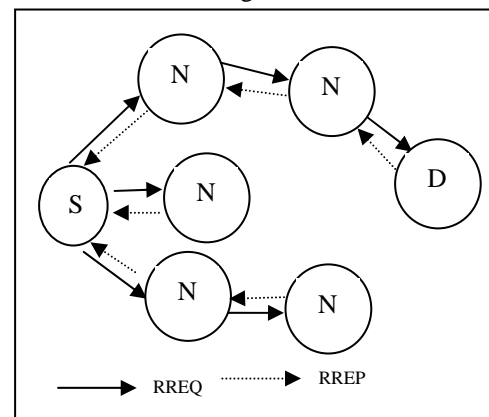

Fig 2. Traversal of Control Messages

3. 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 [3]. 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 attacker now drops the received messages instead of relaying them as the protocol requires.

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. 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 [11] 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 [4]. 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.
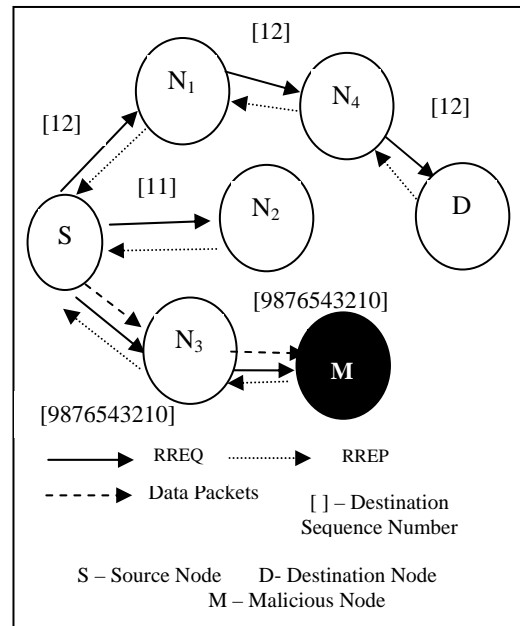

Fig 3. Protocol Packet Exchanges

4. RELATED WORK

There indeed have been numerous attempts published in the literature that aim at countering the Black attacks. We survey them in the following.

In [5], the authors discuss a protocol that requires the intermediate nodes to send RREP message along with the

next hop information. When the source node get this information, it sends a RREQ to the next hop to verify that the target node (i.e. the node that just sent back the RREP packet) indeed has a route to the intermediate node and to the destination. When the next hop receives a FurtherRequest, it sends a FurtherReply which includes the check result to the source node. Based on information in FurtherReply, the source node judges the validity of the route. In this protocol, the RREP control packet is modified to contain the information about next hop. After receiving RREP, the source node will again send RREQ to the node specified as next hop in the received RREP. Obviously, this increases the routing overhead and end-to-end delay. In addition, the intermediate node needs to send RREP message twice for a single route request.

In [6], the authors describe a protocol in which the source node verifies the authenticity of a node that initiates RREP by finding more than one route to the destination. When source node receives RREPs, if routes to destination shared hops, source node can recognize a safe route to destination.

Sanjay Ramaswamy, et al [7] proposed a method for identifying multiple black hole nodes. They are first to propose solution for cooperative black hole attack. They slightly modified AODV protocol by introducing data routing information table (DRI) and cross checking. Every entry of the node is maintained by the table. They rely on the reliable nodes to transfer the packets.

Latha Tamilselvan, Dr. V Sankaranarayanan[8] 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.

Hesiri Weerasinghe [9] 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 identify multiple 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.

5. THE PROPOSED SOLUTION

The solution that we propose here is basically only modifies the working of the source node without altering intermediate and destination nodes by using a method called Prior_ReceiveReply. In this method three things are added, a new table RR-Table(Request Reply), a timer WT (Waiting Time) and a variable MN-ID (Malicious Node ID) to the data structures in the default AODV Protocol.

Algorithm: Prior-ReceiveReply Method
DSN – Destination Sequence Number, NID – Node ID, MN-ID – Malicious Node ID.

Step 1: (Initialization Process)
    Retrieve the current time
    Add the current time with waiting time
Step 2: (Storing Process)
    Store all the Route Replies DSN and NID in
        RR-Table
    Repeat the above process until the time exceeds
Step 3: (Identify and Remove Malicious Node)
    Retrieve the first entry from RR-Table
    If DSN is much greater than SSN then
        discard entry from RR-Table
        and store its NID in MN-ID
Step 4: (Node Selection Process)
    Sort the contents of RR-Table entries according
        to the DSN
    Select the NID having highest DSN among
        RR-table entries
Step 6: (Continue default process)
    Call ReceiveReply method of default
        AODV Protocol

The above algorithm starts from the initialization process, 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 have 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.

In addition, the proposed solution maintains the identity of the malicious node as MN-Id, so that in future, it can discard any control messages coming from that node. Now since malicious node is identified, the routing table for that node is not maintained. In addition, the control messages from the malicious node, too, are not forwarded in the network. Moreover, in order to maintain freshness, the RR-Table is flushed once an route request is chosen from it. Thus, the operation of the proposed protocol is the same as that of the original AODV, once the malicious node has been detected.

The main benefits of modifying the AODV protocol is (1) The malicious node is identified at the initial stage itself and immediately removed so that it cannot take part in further process. (2) With no delay the malicious node are easily identified ie. as we said before all the routes has unique sequence number. Generally the malicious node have the highest Destination Sequence number and it is the first RREP to arrive. So the comparison is made only to the first entry in the table without checking other entries in the table. (3) No modification is made in other default operations of AODV Protocol (4) Better performance produced in little modification and (5) Less memory overhead occurs because only few new things are added.

RNO	DSEQ-NO	NODE-ID
1	**9876543210**	**N3**
2	11	N2
3.	12	N1

Table 1: Content of RR-table with malicious node

RNO	DSEQ-NO	NODE-ID
1.	**12**	N_1
2	11	N_2

Table 2: Content of RR-table without malicious node and sorted according to DSEQ-NO.

6. 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. The Proposed method can be used to find the secured routes and prevent the black hole nodes in the MANET. As future work, we intend to develop simulations to analyze the performance of the proposed solution based on the various security parameters like packet delivery ratio (PDR), mean delay time, packet overhead, memory usage, mobility,

increasing number of malicious node, increasing number of nodes and scope of the black hole nodes.

REFERENCES

[1]   Imrich Chlamtac, 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.

[2] 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

[3]   C. Perkins. "(RFC) request for Comments-3561", Category: Experimental, Network, Working Group, July 2003.

[4]   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." In: International Journal of Network Security, Vol. 5, No.3, pp.338–346, Nov. 2007.

[5]   H. Deng, W. Li, and D. P. Agrawal. "Routing Security in Adhoc Networks." In: IEEE Communications Magazine, Vol. 40, No. 10, pp. 70-75, Oct. 2002.

[6]   M. A. Shurman, S. M. Yoo, and S. Park, "Black hole attack in wireless ad hoc networks." In: Proceedings of the ACM 42nd Southeast Conference (ACMSE'04), pp 96-97, Apr. 2004.

[7]. Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon, and Kendall Nygard, "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks", 2003 International Conference on Wireless Networks (ICWN   03), Las Vegas, Nevada, USA.

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

[9] Hesiri Weerasinghe and Huirong Fu, Member of IEEE, Preventing Cooperative Black Hole Attacks in Mobile Adhoc Networks: Simulation mplementationAndEvaluation,IJSEA,Vol2,No.3,July 2008.

[10] Nital Mistry, Devesh C Jinwala, Member, IAENG, Mukesh Zaveri, "Improving AODV Protocol against Blackhole Attacks", Proceedings of the International MultiConference of Engineers and Computer Scientists 2010 Vol II, IMECS 2010, March 17-19, 2010, Hong Kong..

Lakshmi K has completed MCA M.Phil from Bharathiar University. Currently working as a lecturer in the department of Computer Application in Karpagam University. She has presented more than 5 papers in national conferences. Her research area includes network security, mobile computing.

Manju Priya .S has completed M.Sc, M.Phil in Computer Science from Bharathiar University, Coimbatore. She has 6 years of teaching experience. Currently she is pursing Ph.D in Computer Science in Karpagam University. She has presented more than 5 papers in national conferences. Her research area includes wireless sensor network, Computer communications.

Jeevarathinam A has completed M.Sc M.Phil from Bharathiar University. Currently working as a lecturer in the department of Computer Science in Karpagam University. She has presented more than 5 papers in national conferences. Her research area includes network security, mobile computing, sensor networks.

K. Rama, has completed M.C.A., M.Phil., from Bharathiar University. Currently working as a Lecturer in the department of Computer Science in Karpagam University. She has presented more than 7 papers in national conferences. Her research area includes digital image processing, stenography.

Thilagam K has completed MCA M.Phil in Computer Science. Currently she is pursing Ph.D in Computer Science in Karpagam University, Coimbatore. She has 7 years of teaching experience. She has presented more than 5 papers in national conferences. Her research area includes image processing, data compression, stenography, digital image processing.