RESEARCH ARTICLE OPEN ACCESS

AODV Improvement by Modification at Source Node and Securing It from Black Hole Attack.

Debarati Roy Choudhury*, Dr. Leena Ragha**, Mr Nilesh Marathe***
*(Department of Computer Science, Ramrao Adik Institute of Technology, Mumbai University)
** (Department of Information Technology, Ramrao Adik Institute of Technology, Mumbai University)
** *(Department of Information Technology, Ramrao Adik Institute of Technology, Mumbai University)

ABSTRACT
MANETS suffer from constraints in power, storage and computational resources ,as a result, they are more vulnerable to various communications security related attacks. therefore we attempt to focus on analyzing and improving the security of routing protocol for MANETS viz. the Ad hoc On Demand Distance Vector (AODV)routing protocol. We propose modifications to the AODV we propose an algorithm to counter the Black hole attack on the routing protocols in MANETs. All the routes has unique sequence number and the malicious node has 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
Keywords - AODV, Black hole, receive reply, sequence number, routing table

I. INTRODUCTION

Routing in ad hoc networks faces a number of challenges like dynamic topology, node mobility, lack of infrastructure, low battery life, insecure medium and limited channel capacity, causing a significant degradation of routing performance. A number of surveys cover the security issues and intrusion detection schemes in MANETs [1]. All nodes keep updating their routing tables based on information broadcast by other nodes. Therefore, routing table overflow attacks are possible that can disrupt the routing process. Reactive protocols are more robust against replay attacks because of the nature of routing messages involved, such as with AODV [2]. We propose an algorithm to counter Black hole attack against the AODV routing protocol. By analysis we observe that by adding timer component time is saved and if destination sequence number greater than source ie value greater than threshold the malicious node is identified at the initial stage itself and immediately removed so that it cannot take part in further process.

II. AODV

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, can also add a significant amount of control traffic to the network due to query flooding.

2.1 AODV Routing Protocol.

This protocol is composed of two mechanism (1) Route Discovery and (2) Route Maintenance. AODV uses Route Re Request (RREQ), Route Reply (RREP) control messages in Route Discovery phase and Route Error (RERR) control message in Route Maintenance phase .The header information of this control messages can be seen in detail in. 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 [3]. 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 [4]. 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.

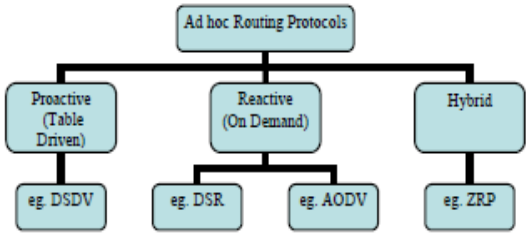

Fig 2.1: Classification of AODV routing protocol

2.2 Working of AODV

The RREQ contains the node's IP address, current sequence number, broadcast ID and most recent sequence number for the destination known to the source node. The destination node, on receipt of RREQ, ends a route reply (RREP) packet along the reverse path established at intermediate nodes during the route discovery process. In case of a link failure route error (RERR) packet is sent to the source and destination nodes. By the use of sequence numbers, a source node is always able to find new valid routes. AODV defines three types of control messages for route maintenance [5].

2.3. Security Flaws in AODV

AODV is vulnerable to routing attacks by malicious nodes due to possible applications of the paper. Although a conclusion may review the main points of the paper, do not replicate the abstract as the conclusion. A conclusion might elaborate on the importance of the work or suggest applications and extensions generally designed to have features such as authentication, integrity, confidentiality and non-repudiation. AODV can easily be manipulated by a malicious node to disrupt its routing.

The following actions can be taken by an inside attacker to disrupt routing in AODV:

1) Modify/forge RREQ or RREP packets.
2) Spoof destination or source IP address to pose as legitimate network node and thus receive or drop data packets.
3) Generate fake RERR packets to increase routing delay and degrade network performance [6].
4) Cause DoS by sending fake RREPs of highest sequence numbers (like Black hole attack)[7].
5) Create routing loops and launch sleep deprivation or resource consumption attacks to deplete node batteries.
6) Replay old routing messages or make a tunnel/wormhole.

Advantages and disadvantages

The main advantage of this protocol is having routes established on demand and that destination sequence numbers are applied to find the latest route to the destination [8]. The connection setup delay is lower. One disadvantage of this protocol is that 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 [9]. Also, multiple route Reply packets in response to a single Route Request packet can lead to heavy control overhead and unnecessary bandwidth consumption due to periodic beaconing multiple Route Reply packets in response to a single Route Request packet can lead to heavy control overhead and unnecessary bandwidth consumption due to periodic beaconing

III. BLACK HOLE 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. 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 [10]. 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 N2 has a route to node D in its route table, the node N2 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. The larger the sequence number, the fresher is the route. Node N2 will now send it to node S (Destination Sequence Number is shown in square bracket in (Figure 2.3.1). Since node N1 and node N3 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.

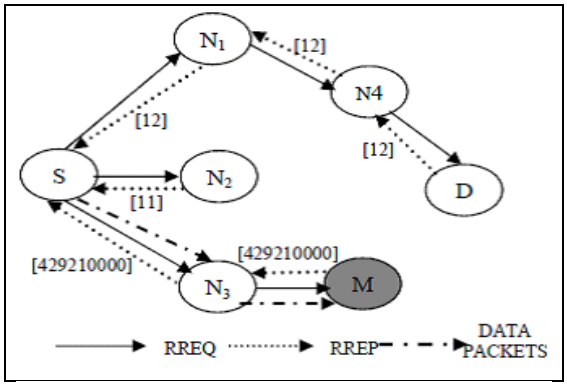

Fig 3: Traversal of Control Messages in AODV

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. The source node processed the incoming RREPs for consideration is shown .After a source node receives a RREP message, it calls *Receive Reply (Packet P)* method one of the crucial function of AODV [11].

3.1. Black hole attack caused by RREQ

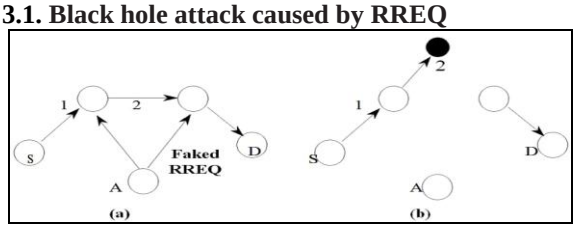

Fig 3.1: An attacker can send fake RREQ messages to form black hole attack

The attacker can generate Black hole attack by faked RREQ message as follows:

In RREQ Black hole attack, the attacker. Set the type field to RREQ (1) Set the originator IP address to the originating node's IP address; Set the destination IP address to the destination node's IP address; Set the source IP address (in the IP header) to anon-existent IP address (Black hole); Increase the source sequence number by at least one, or decrease the hop count to 1.The attacker forms a Black hole attack between the source node and the destination node by faked RREQ message.

3.2 Black hole attack caused by RREP

The attacker may generate a RREP message to form Black hole as follows: Set the type field to RREP (2); Set the hop count field to 1;Set the originator IP address as the originating node of the route and the destination IP address as the destination node of the route, Increase the destination sequence number by at least one; Set the source IP address (in the IP header) to a nonexistent IP address (Black hole).The attacker unicasts the faked RREP[12] message to the originating node. When originating node receives the faked RREP message, it will update its route to destination node through the non-existent node. Then RREP Black hole is formed

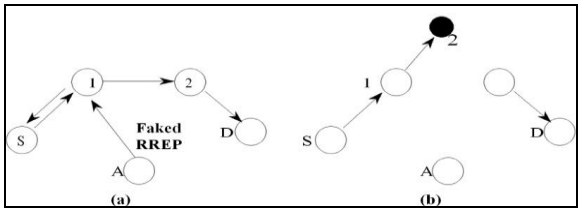

Fig 3.2: Black Hole is formed by fake RREP

IV. GENERAL PROPOSED ALGORITHM

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_Receive Reply. 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.

4.1 Algorithm: Prior-Receive Reply Method

DSN – Destination Sequence Number, NID – Node ID, MN-ID – Malicious Node ID(M node).

Step 1: (Initialization Process) Retrieve the current time and add the current time with waiting time.

Step 2: (Storing Process) Store all the Route Replies DSN and NID in RR-Table(R) 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 5: (Continue default process) Call Receive Reply 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 has the higher destination sequence number, is obtained by sorting the RR-Table according to the DSEQ-NO column, whose packet is sent to Receive Reply 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 a route request is chosen from it[13]. Thus, the operation of the proposed protocol is the same as that of the original AODV, once the malicious node has been detected.

4.2 Main benefits of modifying AODV protocol

(1) The malicious node is identified at the initial stage itself and immediately removed so that it cannot take part in further process [14].

(2) With no delay the malicious node are easily identified i.e. as we said before all the routes has unique sequence number.

Generally the malicious node has 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.

(5) Less memory overhead occurs because only few new things are added.

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 [15]. 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.

V. Recv Reply algorithm At Source Node: AODV

```
Receive Reply (Packet P)
{   if(P has an entry in Route Table)
{ select Dest_Seq_No from routing table
  If (P.Dest_Seq_No>Dest_Seq_No)
{  update entry of P in routing table, unicast data
 packets to the route specified in RREP   }
 else   { discard RREP } }
 else {  if(P.Dest_Seq_No>= Src_Seq_No)
{   Make entry of P in routing table }
else { discard this RREP }
```

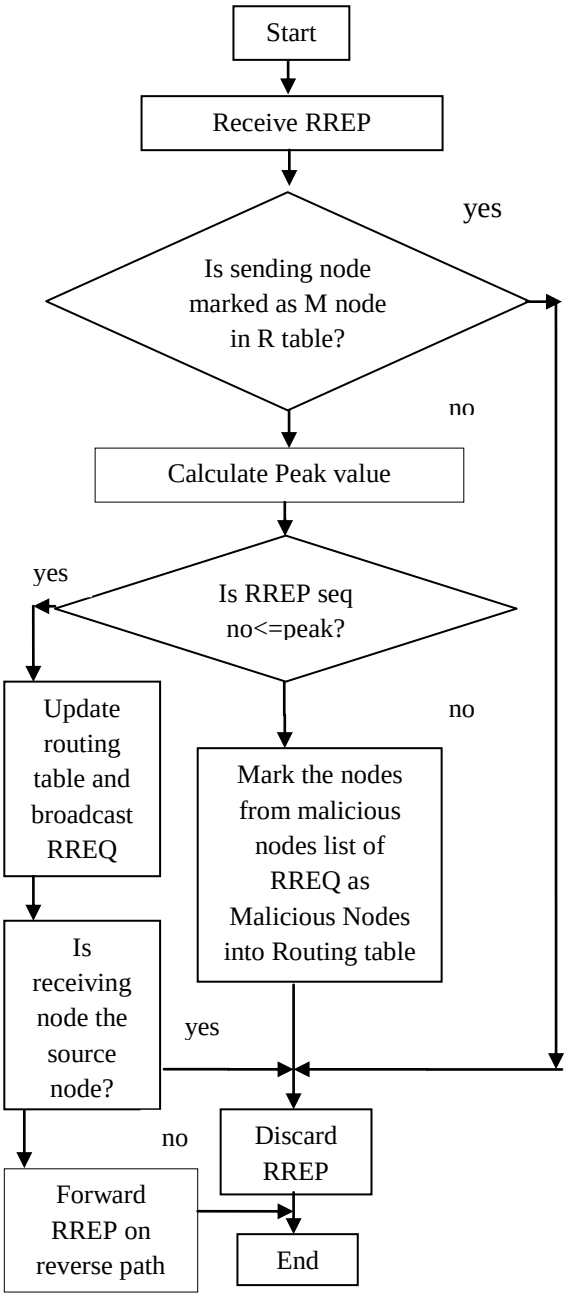

Fig 4.3(a):flow-chart for node receiving RREP

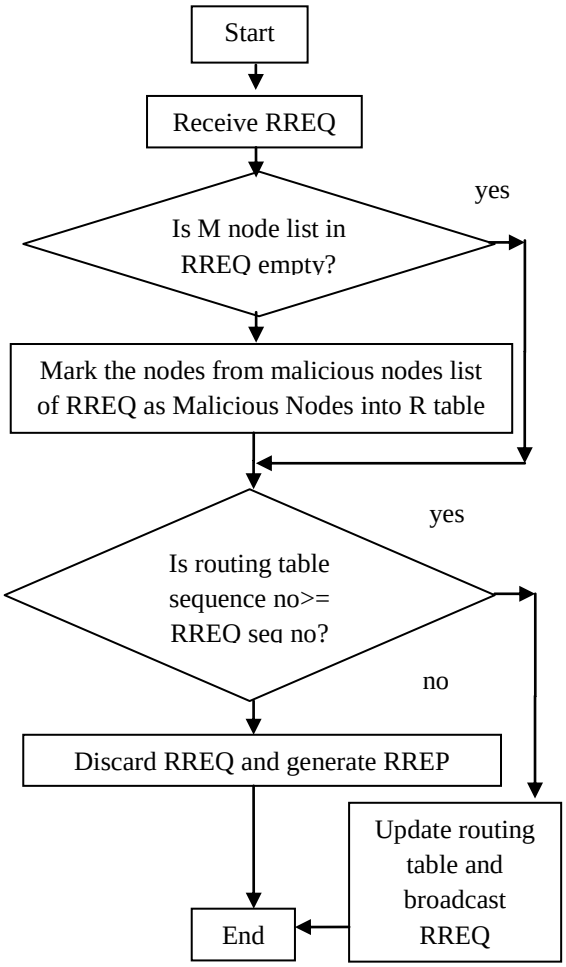

Fig 4.3(b): Basic Flow-chart for node broadcasting RREQ

VI. CONCLUSION

As compared to the other approaches, we believe the proposed algorithm is simple and efficient and has very less delay and congestion in implementation .We also emphasize that the proposed algorithm will be implemented and simulated for the AODV routing algorithm .

REFERENCES

[1] International Journal of Scientific and Research Publications, Volume 2, Issue 8, ISSN 2250-3153, August 2012 .

[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 6thInternational Workshop on Ant Algorithms and Swarm Intelligence, Brussels, Springer, LNCS 5217, 2008.

[3] F. Maan, Y. Abbas, N. Mazharg," *Vulnerability Assessment of AODV and SAODV Routing Protocols Against Network routing Attacks and Performance Comparisons*" National University of Sciences and Technology (NUST), wireless advanced2011.

[4] K. Lakshmi, S.Manju Priya, A. Jeevarathinam, K. Rama, K. Thilagam, Lecturer, "*Modified AODV Protocol against Blackhole Attacks in MANET*", Coimbatore, International Journal of Engineering and Technology Vol.2 (6), 2010.

[5] Rajesh J. Nagar, KajalS. Patel,"*Securing AODV Protocol against Blackhole Attacks*" International Journal of Engineering Research and Applications ISSN: 2248-9622 , Vol. 2, Issue 1, pp.1116-1120Jan-Feb 2012.

[6] Jin Taek Kim, Jeong-Ho Kho, Chang-Young Lee, Do-Won Lee, Cheol-Soo Bang, Geuk Lee Dept.of Computer Engineering, Hannam University, "*A Safe AODV Security Routing Protocol*", Korea International Conference on Convergence and Hybrid Information Technology 2008.

[7] Mehdi Medadian, Khossro Fardad, "*Proposing a Method to Detect Black Hole Attacks in AODV Routing Protocol*", European Journal of Scientific Research ISSN 1450-216X Vol.69 No.1, pp.91-101, 2012.

[8] Sushil Kumar Chamoli, Santosh Kumar, Deepak Singh Rana, "*Performance of AODV against Black Hole Attacks in Mobile ad-hoc Networks*", International .J. Computer Technology & Applications, Vol 3 (4), 1395-1399, july -august 2012.

[9] Dr. S. Tamilarasan, "*Securing AODV Routing Protocol from Black Hole Attack*", International Journal of Computer Science and Telecommunications [Volume 3, Issue 7, July 2012]

[10] Abhilasha Sharma, Rajdeep Singh, Ghanshyam Pandey, "*Detection and Prevention from Black Hole attack in AODV protocol for MANET*", International Journal of Computer Applications (0975 – 8887) Volume 50 – No.5, July 2012.

[11] Ipsa De, Debdutta Barman Roy, "*Comparative study of Attacks on AODV-base Mobile Ad Hoc Networks*", International Journal on Computer Science and Engineering ISSN: 0975-3397 Vol. 3 No. 1 Jan 2011.

[12] Watchara Saetang and Sakuna Charoenpanyasak, "*CAODV Free Blackhole Attack in Ad Hoc Networks*", International Conference on Computer Networks and Communication Systemsvol.35 2012.

[13] Abhilasha Sharma, Rajdeep Singh, Ghanshyam Pandey, "*Detection and Prevention from Black Hole attack in AODV*

protocol for MANET", International Journal of Computer Applications (0975 – 8887) Volume 50 – No.5, July 2012.

[14] Ipsa De, Debdutta Barman Roy, "*Comparative study of Attacks on AODV-base Mobile Ad Hoc Networks*", International Journal on Computer Science and Engineering ISSN: 0975-3397 Vol. 3 No. 1 Jan 2011.

[15] Watcha Saetang and Sakuna Charoenpanyasak , "*CAODV Free Blackhole Attack in Ad Hoc Networks*", International Conference on Computer Networks and Communication Systemsvol.35 2012.