RELIABLE APPROACH FOR BLACKHOLE DETECTION IN MANET USING AODV PROTOCOL

[1] SHREYA SANGHVI, [2] NAREN TADA

[1]PG Student, CE Dept., V.V.P. Engineering College, Rajkot, GTU, Gujarat, India.
[2]Assistant Professor, CE Dept., V.V.P. Engineering College, Rajkot, GTU, Gujarat, India.

shreyasanghvi15@gmail.com, narentada@gmail.com

ABSTRACT- *The collection of wireless mobile nodes which forms the temporary network without using any kind of network infrastructure is called Mobile Ad hoc network. The channel is wireless, topology is dynamic so, there is no clear line of defense. Due to these reasons, the MANETs are prone to numerous security attacks. This paper focuses on the most important kind of routing attack – Black hole attack. We use AODV routing protocol to understand the attack and its prevention. In black hole attack, the malicious node will send fake RREP packet to the sender with very high destination sequence number. So the connection will be established with the malicious node and that node in turn will discard all the packets coming to it, instead of forwarding it to other nodes in the network. Here we present the solution to this type of attack by taking the nodes of the network into promiscuous mode. It means other nodes in the topology can hear the packets sent from and received by the neighbor nodes.*

Key words - AODV Protocol, Black hole Attack, Promiscuous mode, Security in MANET.

IJKRCE

1. INTRODUCTION

An ad hoc network is a collection of wireless mobile nodes dynamically forming temporary network. These types of network communicate without using any existing network infrastructure or centralized administration. The transmission range of wireless network interface is limited, so multiple hops may be needed for one node to communicate with other node in the network. In ad hoc networks, each mobile node act as the host as well as router for forwarding packets for other mobile nodes which are not in direct transmission range of each other [1].

The nodes are free to move and organize themselves arbitrarily, so the topology is highly dynamic which results in frequent and unpredictable changes of network topology, adding difficulty and complexity to routing among mobile nodes. The ad hoc network needs no existing infrastructure so it can be deployed quickly and easily whenever it is needed. This type of network is mainly used by military, researchers and emergency services where pre- established network devices are not available. Ad hoc networks are easy to install and comparatively cheaper because it requires no pre-established access points [2]. But besides its advantages there are many issues. Wireless link between two nodes in a network is more vulnerable to all type of attacks than that wired links because in wireless links, penetration or intrusion is very easy as compared to wired links. So, one of the major issues in mobile ad hoc network is security. Also mobility, dynamic topology, asymmetric links, interference due to adjacent links, limited bandwidth and energy constrained device are the challenges faced by mobile ad hoc networks [3].

The paper is organized as follows: Section II describes the operation of AODV protocol. Section III gives idea about the security threats on MANETs. In section IV, we discuss the black hole attack and the current methods to prevent it. In section V, we mention the proposed algorithm to prevent the black hole attack.

2. OPERATION OF AODV ROUTING PROTOCOL

There are mainly three types of routing protocols are available for MANETs: Proactive routing protocols, Reactive routing protocols and Hybrid routing protocols. Proactive protocols are those which continuously checks for the topology of the network nodes. So when there is need of route to any source to destination then it is always available. This protocol increases the overhead as the cost of maintaining the network might be very

high if network topology is changing frequently. Reactive protocol establishes the route only when it is required. It does not check the network topology continuously. So it is considered as resource preserving protocol. Hybrid protocols are combination of both. In this paper wee analyze the security threats on AODV protocol.

AODV is a well known and one of the standard reactive routing protocol for MANETs which provides dynamic, self-starting and multi hop network. It is the reactive routing protocol which does not need to maintain the routing table in advance for every node [4].

AODV operates in two phases 1) Route Discovery and 2) Route maintenance. Whenever a source node needs to communicate with another node for which it has no routing information, Route Discovery process is initiated by broadcasting a Route Request (RREQ) packet to its neighbors. 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 broadcast-ing. RREQ ID increases one every time node S sends 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 re-ceived, 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 whose the destination

sequence number (Dst Seq) is the largest amongst

all previously received RREPs. But if Dst Seq were same, it will select the RREP whose hop count is the smallest [5]

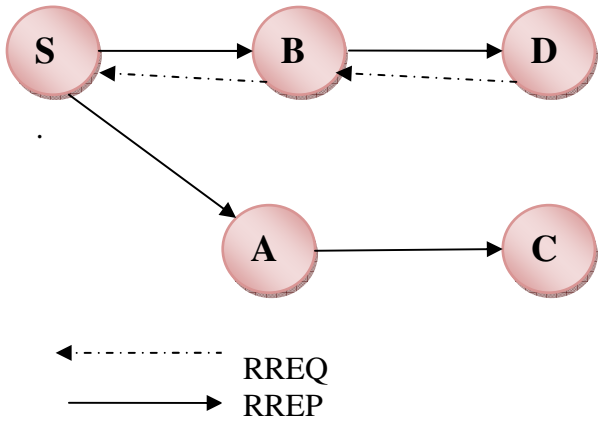

Figure. 1. Propagation of RREQ and RREP messages in AODV protocol

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 neighboring 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.

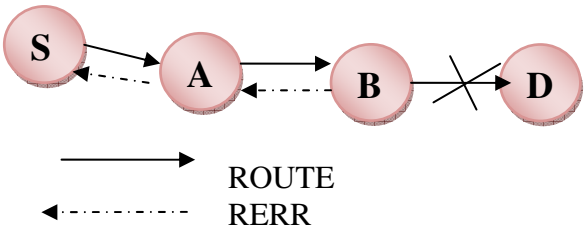

Figure. 2. Route Maintenance Process

3. SECURITY ATTACKS IN MOBILE AD HOC NETWORKS

Security has become a primary concern to provide the safe and secure communication between two nodes in ad hoc network. Many aspects of security in MANETs are different than that of wired network as there is no clear line of boundary in MANETs and also due to shared wireless medium, dynamic topology etc. As a result the security solutions for wired network do not completely apply to MANETs. The basic criteria

IJKRCE

that any security scheme for MANETs should follow is to provide security services like confidentiality, integrity, anonymity, and availability to the mobile users [6]. No well defined system is implemented to monitor the traffic or to control the access. Moreover the mostly used routing protocols like AODV assumes trusted and cooperative environment. So attacker can easily enter the network and disrupt the operations of protocols and violates the security services. Attacks are classified in number of ways in various literature based on the operations in MANETs, network layers on which the attacks are associated, location of attacker or malicious node, security services etc [7].

Passive attacks are those in which attacker does not makes any malicious activities in order to make any potential harm to the hosts. For example, eaves dropping which may leak the useful and confidential information to the intruders or attacker and traffic analysis to get information about the network topology [8].

Active attacks confuse the routing procedure and degrade the network performance of the network. The malicious node cheats the network by changing the fields of routing packets or by fabricating and propagating the false packet in the network. Active attacks cause potential harm to the network and the information flowing in a network [8]. Some of the attacks are following: Black hole attack, Message tampering , Replay attack, Gray hole attack, Sybil attack , Worm hole attack, Flooding attack, Rushing attack, Byzantine attack, Routing table overflow, Jellyfish attack , etc [9] [10].

4. BLACK HOLE ATTACK AND LITERATURE SURVEY

In AODV, Dst Seq 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 Dst Seq in the RREQ packet plus one, and then selectsthe larger one as RREP's Dst Seq. Upon receiving a number of RREP, a source node selects the one with greatest Dst Seq in order to construct a route. To succeed in the blackhole attack the attacker must generate its RREP with Dst Seq greater than the Dst Seq of the destination node. It is possible for the attacker to find out Dst Seq of the destination node from the RREQ packet. In general, the attacker can set the value of its RREP's Dst Seq base on the received RREQ's Dst Seq. However, this RREQ's Dst Seq may not present the current Dst Seq of the desti-nation node. Figure 3 shows an example of the blackhole attack. The value of RREQ and RREP using in the attack are shown in Table 1.

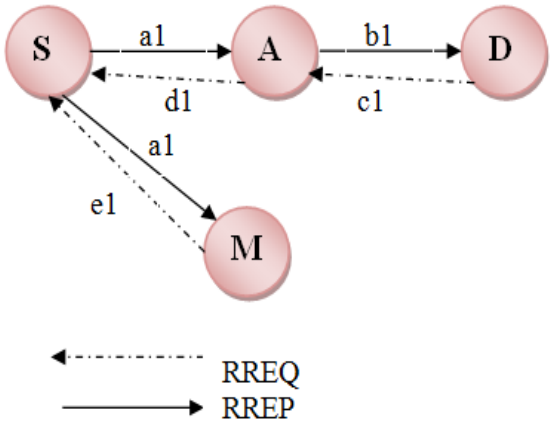

Figure. 3. Black hole attack on AODV protocol

IJKRCE

	RREQ		RREP		
	A1	B1	C1	D1	E1
IP.Src	S	A	D	A	D
Des.t	D		D		D
DSNo	60		61		65
SRc	S		-		-

Table 1 Reply packets and destination sequence number in case of black hole attack

In Table 1, IP.Src indicates the node which generates or forwards a RREQ or RREP, AODV.Dst indicates the destination node and AODV.Src indicates the source node. Here, we assume that the destination node D has no connections with other nodes. The source node S constructs a route in order to communicate with destination node D. Let the destination node D's Dst Seq that the source node S has is 60. Hence, source node S sets its RREQ (a1) and broadcasts as shown in Table 1. Upon receiving RREQ (a1), node A forwards RREQ (b1) since it is not the destination node. To impersonate the destination node, the attacker M sends spoofed RREP(e1) shown in Table 1 with IP.Src, AODV.Dst the same with D and increased Dst Seq (in this case 65 as) to source node S. At the same time, the destination node D which received RREQ (b1) sends RREP

(c1) with Dst Seq incremented by one to node S. Although, the source node S receive two RREP, base on Dst Seq the RREP (e1) from the attacker M is judged to be the most recent routing information and the route to node M is established. As a result, the traffic from the source node to the destination node is deprived by node M [11].

Payal Raj and Prashant Swadas [12] proposed solution as, In normal AODV, the node that receives the RREP packet first checks the value of sequence number in its routing table. RREP packet is accepted by the node if it has RREP_seq_no higher than the one in the routing table. If more than one RREP arrives to a node, then node selects the RREP having the higher RREP_seq_no. This solution introduces the threshold value which is dynamically updated in every time interval. If the value of RREP_seq_no is higher than threshold then, it is detected as malicious node. This solution introduces the ALARM packet. ALARM packet contains the node id of the malicious node once it is detected. So when a node finds that the RREP_seq_no is higher than a threshold, then it generates the ALARM packets and broadcasts it to its neighbors. So now the neighbors know which is the malicious node. So when again it will receive the RREP from malicious node, they will check if it is same as in ALARM packet. If so then all the entries in the routing table about that malicious node is removed and thus the malicious node is isolated. This method introduces only one new control packet ALARM. So the routing overhead added to due to the new control packet is very less. It provides increased packet delivery ratio, with minimum end to end delay.

A.vani and D. Sreenivasa Rao [13] solutions uses the threshold value to compare the highest RREP_seq_no. At every time interval the threshold value is updated. If the number in the RREP is higher than threshold then that node is detected as malicious node. This threshold is calculated as the average of difference of dest_seq_no in each time slot between the seq_no in the route table and RREP packet. This method increases the PDR with minimal increase in average end to end delay and minimal increase in routing overhead.

Another solution proposed by M. Al-Shurman, S.M. Yoo, and S. Park [14] in which source node to wait until a RREP packet arrives from more than two nodes. After receiving multiple RREPs, the source node checks whether there is a shared hop or not. If there is, the source node judges that the route is safe. And depending on its sequence number it selects that route or other route.The main limitation of this solution is that it introduces time delay, because it must wait until multiple RREPs arrive to the source node [14].

Nital Mistry, Devesh Jinwwala and Mukesh Zaveri[15] proposed a solution in which they introduced Pre_ReceiveReply(Packet P), a new table Cmg_RREP_Tab, a timer MOS_WAIT_TIME and a variable Mali_node in AODV protocol. In the operation of AODV protocol, the source node accepts the first fresh RREP coming to it. In this approach, the source node after receiving first RREP waits for MOS_WAIT_TIME. All RREP messages coming in this time are stored in Cmg_RREP_Tab. MOS_WAIT_TIME initialized as half the value of RREP_WAIT_TIME (it is time a node waits of RREP before sending new RREQ). Now, the source node will analyze the entries of Cmg_RREP_Tab and the discard the RREP whose destination sequence number is higher than presumed value. Once the malicious node is identified as Mali_node, other nodes discard any control messages coming from this node, messages are not forwarded into the network. Cmg_RREP_Tab is flushed once the RREP is chosen from it, to maintain the freshness.

Here the ReceiveReply (Packet P) is called at last, after the pre receiving of reply packet is executed. In this method no new control messages are added in the protocol. This approach adds little over head but it is worth as it significantly improves the packet delivery ratio of AODV under black hole attack. Its advantage is that it adds no additional control messages and also regeneration of any control messages is also not required [15].

In Latha Tamilselvan, Dr. V Sankaranarayanan's [16] method, the source node will wait for reply packets from other nodes instead of sending data packets at once. After receiving the first request it sets timer for collecting further requests. It will store the sequence number and time at which packet arrived, in collect route reply table (CRRT). Then it calculates time out. After the timeout value, it first checks in CRRT whether there is any repeated next hop node. If any repeated next hop node is present in the reply paths it assumes the paths are correct or the chance of malicious paths is limited. Then it chooses any one of the paths with the repeated node to transmit the data packets. If there is no repetition select random route from CRRT. The chances of malicious route selected are reduced.

Pramod Kumar Singh, Govind Sharma [17] they proposed a method as follow. Consider node S

IJKRCE

needs to communicate to node D and node G is a malicious node. Node S floods a RREQ packet in the network and waits for the RREP packet to obtain a fresh route to the destination node D. Now, there are two possibilities; the RREP packet may be received either from the destination node itself or from an intermediate node. In case 1, when the RREP packet is received from the destination node itself, a route is established. In case 2, when the RREP packet is received from an intermediate node, a node preceding to the node which sent RREP packet switches on its promiscuous mode and sends a hello message to the destination node through this node. If the hello message is forwarded by this node to the destination, the node and hence the route is safe; otherwise, the node is a malicious node. In latter case, the preceding node floods an alarm message to the network about the malicious node to isolate it.

The limitation of this method is that, if attacker node drops only the control and reply packets but not the hello packets. So in such case this method is resolved in proposed algorithm.

5. PROPOSED METHOD TO PREVENT BLACHKOLE ATTACK

We propose a method which uses promiscuous mode of the node. This mode allows a node to intercept and read each network packet that arrives in its entirety. It means that if node A within the range of node B, it can overhear communication to and from B even if those communication do not directly involve A.

Consider a scenario, S needs to communicate to node D and node G is a malicious node. Node S floods a RREQ packet in the network and waits for the RREP packet to obtain a fresh route to the destination node D. Now, there are two possibilities; the RREP packet may be received either from the destination node itself or from an intermediate node. In case 1, when the RREP packet is received from the destination node itself, a route is established. In case 2, when the RREP packet is received from an intermediate node, a node preceding to the node which sent RREP packet switches on its promiscuous mode and sends a check_packets to the destination node through this node. If the check message is forwarded by this node to the destination, the node and hence the route is safe; otherwise, the node is a malicious node. In latter case, the preceding node floods an alarm message to the network about the malicious node to isolate it.

Step 1: (Initialization Process)

Start the route discovery phase with the source node S.
Source node will broadcast the RREQ to its neighbors.

Step 2: (Set flag value)
Set original_destination_path = false;
flag=true;

Step 3: (the neighboring nodes are in promiscuous mode so they are monitoring the intermediate node)

```
While(flag = = true)
{
    If(RREP from the destination)
    {
            Set original_destination_path = true;
            Flag= true;
    }

Step 4:
If( RREP from intermediate node N)
{
    Monitor the number of packets received by N.
    Count the number of packets forwarded by N.

    If( number_of_packets_forwarded = = 0)
    {
            //it is blackhole node
            Broadcast the Alarm_packets
    }
    Else
    {
            //n is good node
            Set_original_destination_path= true
            Flag =false;
    }
}
If(RRTO expire)
{
            Flag= false;
}
}
Step 5:
    If(original_destination_path = true)
    {
            Establish path and send data;
    }
```

6. CONCLUSION

Mobile ad hoc network faces the security problems mainly due to its dynamic nature and wireless communication links. The malicious node sends reply packet with very high destination sequence number, so the source node thinks that, it is genuine node having fresh route, so it will establish the connection with it. This is black hole attack; this can be prevented by operating the node in the topology into promiscuous mode, so the

neighbor can monitor the number of packets arriving at the node and number of packets leaving the node. If the number of packets being forwarded by node is zero it means that it is black hole node. And it can be isolated by using alarm packets. It eliminates the limitation that if hello messages are not dropped, still the attack can be detected.

7. REFERENCES

[1] B. Dahill, B. Levine, E. Royer and C. Shields. "A Secure Routing Protocol for Ad Hoc Networks", Technical Report UMCS- 2001, 2001.

[2] M. Dasgupta, S. Choudhary, N. Chaki, "Routing Misbehavior in Ad Hoc Network", International Journal of Computer Application, 2010.

[3] S. K. S Sarkar, T. G. Basavaraju, C. Puttamadappa, " Ad hoc Mobile Wireless Networks Principle, Protocols and Applications " , page 21,22.

[4] S. Gandhi, N. Chaubey, N. Tada, S. Trivedi, "Scenario-based Performance Comparison of Reactive, Proactive & Hybrid Protocols in MANET", International Conference on Computer Communication and Informatics, 2011.

[5] Perkins, C.E., Royer, E.M. :Ad-Hoc On Demand Distance Vector Routing , Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications (WMCSA), New Orleans, LA, 1999, pp. 90-100.

[6] Shreya Sanghvi, Tejas Patalia, Naren Tada, "Mitigating The Attacks In Mobile Ad Hoc Networks: Proposals And Challenges", International Journal Of Computer And Electronics Engineering.

[7] H Yang, H Y. Luo, F Ye, S W. Lu, and L Zhang, "Security in mobile ad hoc networks: Challenges and solutions". IEEE Wireless Communication, 2004.

[8] B. Soujanya, T. Sitamahalakshmi, C. Divakar, "Study of routing protocols in mobile ad hoc networks", International journal of engineering science and technology, 2011.

[9] N. S. Raote, "Defending Wormhole Attack in Wireless Ad hoc Network, International journal of computer science and engineering survey, 2011.

[10]Wu B., Chen J., Wu J., Cardei M., "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks", Wireless/Mobile Network Security, Chapter 12, Springer, 2006.

[11]Satoshi Kurosawa, 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.

[12]Payal N. Raj, Prashant B. Swadas, "Dpraodv: A Dyanamic Learning System Against Blackhole Attack In Aodv Based Manet" International Journal Of Computer Science.

[13]A. Vani, D. Sreenivasa Rao, "Removal Of Black Hole Attack In Ad Hoc Wireless Networks To Provide Confidentiality Security Service", International Journal Of Engineering Science And Technology.

[14]M. Al-Shurman, S-M. Yoo, and S. Park, "Black Hole Attack in Mobile Ad Hoc Networks," ACM Southeast Regional Conference, 2004.

[15]N. Mistry, D. Jinwala, M. Zaveri, "Improving AODV protocol against Black hole attacks" , IMECS, 2010.

[16]Lalit Himral, Vishal Vig, Nagesh Chand, "Preventing AODV Routing Protocol From Black Hole Attack", International Journal Of Engineering Science And Technology.

[17]Pramod Kumar Singh, Govind Sharma, "An efficient prevention of black hole problem in AODV Routing protocol", international conference on trust. Security and privacy in computing and communications, IEEE.

IJKRCE