AODV Using Detection of Black Hole Attack

Aarti Madan, Anu

Research Scholar, Assistant Professor
SKIET Computer Science & Engineering, Kurukshetra University

***Abstract* - An AODVB (Ad hoc On-Demand Distance Vector with Black hole Avoidance) protocol for avoiding black-hole attack. AODVB forms link displace multi-path during path discovery to provide greater path selection in order to avoid malicious nodes in the path using legitimacy table maintained by each node in the network. Non-malicious nodes gradually isolate the black-hole nodes based on the values collected in their legitimacy table and avoid them while making path between source and destination.**

***Keywords*— AODV, Black Hole Attack, Legitimavy table**

I. Introduction

An Ad-hoc wire- less network consists of a set of mobile nodes (hosts) that are connected through the wireless links. In Ad-hoc wireless network, communication is based on the principle of broadcast radio channel and reception of electromagnetic waves. The varied characteristics of wireless networks as compared to their wired counter parts addresses various issues such as mobility of nodes, limited bandwidth, error prone broadcast channels, hidden and exposed terminal problems and power constraints . In adhoc networks, nodes are free to join and leave the network. So it has no free infrastructure and no centralized administration. Adhoc network can be static or mobile. In static adhoc network (SANET), nodes are geographically fixed. In mobile adhoc network, nodes change location, topology becomes more unpredictable and vulnerable to attacks [1]. These attacks can be classified according to the source of attack as external attack and internal attack. In internal attack, attacker node exists inside the network. Attacker node belongs to network domain. Internal attacks are actually from compromised nodes (node controlled by any node outside the network).in external attack, attacker node exists outside the domain of a network and attacks from outside. Internal attacks are more severe, when compared with external attacks, since the insider node knows vulnerable and secret information and possesses privileged access rights [2]. External and internal attacks are sometimes referred to as outsider and insider attacks respectively [3]. Attacks can also be classified as active and passive attacks [4,5]. In passive attacks, attacker involves eavesdropping of data, thus disclose information of the location and move patterns of nodes. This kind of attack is very difficult to detect; because attacker node does not exhibit abnormal activities. Active attack involves action [4]. The intruder may insert large volume of data into the network. They can intentionally drop, corrupt or delay the data packet [6]. This paper presents some general approaches for detecting black hole attack in mobile ad hoc networks. In this attack, a malicious node tries to capture the path toward itself by falsely.

claiming larger sequence number and smaller hop count (i.e. shorter path) to the destination node and absorbs all packets without forwarding them to destination node [7]. According to the AODV design, a source node will select largest sequence number and shortest path (i.e. minimum hop count) to send data packet upon receipt of several RREP packets. Thus a route via black hole node will be selected by source node for communication; black hole will then drop the received data packets [8]. Black hole attack can be both external attack and internal attack i.e. caused by node existing inside network or node outside the network. In wireless networks, transmission is done from node to node. Each node acts as a router for transmitting and receiving packets to/from other nodes. An ad-hoc network connection is temporarily created to transmit the data. If the network is established for a long time, it is called simple local area network (LAN). A wireless network uses a decentralized base station to which all nodes must communicate with. A peer-to-peer connection can increase the distance of the wireless network.

II. Ad-hoc On-Demand Distance Vector (AODV) Routing protocol

Ad-hoc On-Demand Distance Vector (AODV) [40] 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. [31]Thanks to these control messages, AODV Routing Protocol offers quick adaptation to dynamic network conditions, low processing and memory overhead, low network bandwidth utilization with small size control messages. The most distinguishing feature of AODV compared to the other routing protocols is that it uses a destination sequence number for each route entry. The destination sequence number is generated by the destination when a connection is requested from it. Using the destination sequence number ensures loop freedom. AODV makes sure the route to the destination does not contain a loop and is the shortest path.

Black hole attack

It is kind of DoS attack where malicious node can attract all packets by pretending shortest route to the destination [35][36]. It drops all traffic destined for that node when traffic is received by it. The effect of this attack completely degrades the performance of the network because the destination node never receives any information from the source. The access to the information is denied. To perform black hole attack, malicious node waits for RREQ messages from neighbouring nodes . When the malicious node receives an RREQ message, immediately sends a false RREP message with a high sequence number and minimum hop count without checking its routing table to make an entry in the routing table of the Source node, before other nodes replies to absorb transmitted data from source to that destination and drop them instead of forwarding. Black hole attack [16] in AODV protocol can be performed in two ways : black hole attack caused by RREP and black hole attack caused by RREQ are described in table2 as follows.

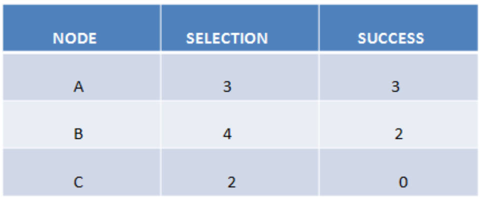
Table 2.1 Black Hole Attack

Caused by RREQ	Caused by RREP
Set the originator IP address in RREQ to the originating nodes IP address.	Set the originator IP address in RREQ to the originating nodes IP address.
Set the destination IP address in RREQ to the originating nodes IP address.	Set the destination IP address in RREQ to the originating nodes IP address.
Set the destination IP address of IP Header to broadcast address.	Set the destination IP address of IP Header to IP address of node that RREQ has been received
Set the source IP address of IP header to its own IP address	Set the source IP address of IP header to its own IP address

III. PURPOSED WORK

3.1Legitimacy Table:

In proposed system, each node is maintaining a legitimacy table having 2 values for each node, let's have a look at a sample table to understand its fields and values of fields.



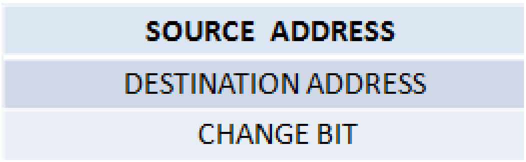
NODE	SELECTION	SUCCESS
A	3	3
B	4	2
C	2	0

Fig3.1: Legitimacy Table

One field in this table is 'selection' which indicates how much times, a node has been selected during path discovery. Other field 'success' shows how much times, the path containing this node was successful. These values are used to find legitimacy ratio as success/selection. Legitimacy ratio indicates confidence in a node to perform correct function. Lower the legitimacy ratio, higher the chances of node being malicious.

3.1.1Route change packet

It is additional packet used by proposed system. It has three fields. It is used by nodes to inform 1) the first node in backward path (which is having multiple entries for destination) to change the route to other path, which has next higher legitimacy ratio. 2) To flush the all other nodes in backward path.



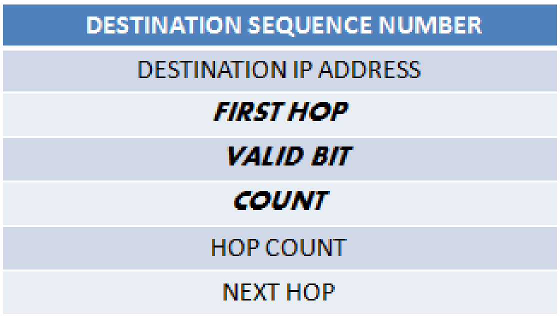
SOURCE ADDRESS
DESTINATION ADDRESS
CHANGE BIT

Fig3.2 : Route Change Packet

Change Bit will be set to 1 by the first node in the backward path which has multiple entries to the destination node, so that other nodes in the backward path would not switch the route to another path.

3.1.2Modification in routing table:

Three additional fields are added to the routing table. These are shown



DESTINATION SEQUENCE NUMBER
DESTINATION IP ADDRESS
FIRST HOP
VALID BIT
COUNT
HOP COUNT
NEXT HOP

Fig3.3 : modification in routing table

First field is first hop which stores the value of first hop immediately after the node initiating RREQ.it is used to avoid loops in the path formation. when a node receives an RREP, this field is used to store the value of originator field of RREP. Valid Bit field has only three values 0, 1 and -1. Value 0 indicates that the path to the destination through next hop may not be correct;

value 1 specifies that the path to the destination is free from malicious nodes and value -1 indicates entry has not been chosen for data transfer. count field denotes the number of RREPs received with same sequence number for the entry but its value would be -1 if the entry has been created after RREQ arrival.

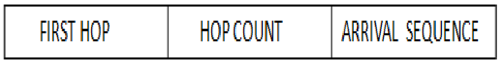
Valid bit = 0; i.e path may not be correct
= 1; i.e path is correct and non malicious
= -1; i.e path not chosen for data transfer
Count = number of RREPs received with same sequence number

3.2 Hello packet:

Proposed protocol modifies the function of hello packet. Here hello packet is used to broadcast the node id whose legitimacy ratio is below the threshold level. If legitimacy ratio of sending node is higher than the upper threshold level, then neighbors will update their legitimacy table for node after receiving hello packet so that malicious node will not be able to grab the route through them.

3.2.1Route Request procedure

Aodv uses two fields hop count and sequence for the route request of path discovery. In proposed protocol, one additional field is used, i.e. first hop.



FIRST HOP	HOP COUNT	ARRIVAL SEQUENCE

Fig3.4: fields used in RREQ procedure

First hop field is used to discard redundant packets, it checks duplicacy of RREQ packet for node receiving RREQ. Hop count is the number of nodes,a node is far away from destination. Arrival sequence is the sequence of arriving same RREQ packet at a node; i.e. if same RREQ packet is forwarded by two nodes, packet arrived first will have sequence number 1 and 2nd will have sequence as 2 and so on.

If hop count in RREQ> hop count of node’s routing table entry, then RREQ packet is simply discarded.For understanding route request procedure, let’s take an example.

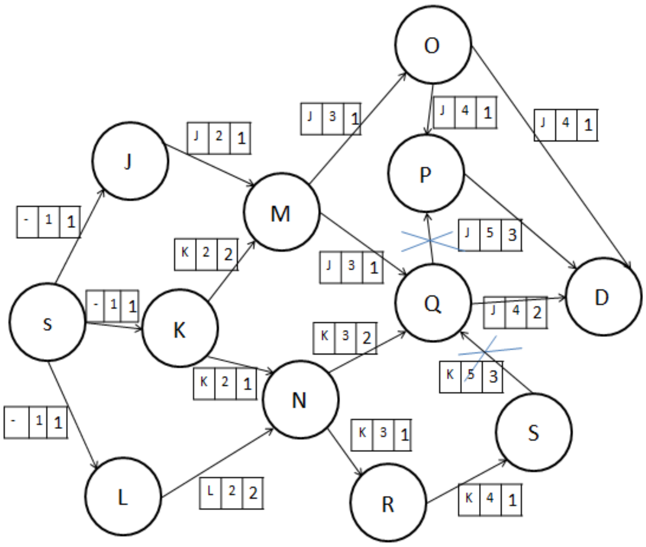


Fig3.5: Route Request procedure

Initially field first hop is emptywhen source node requests for a route. When nodes J, K and L receives RREQ they put on following values

First hop= their own ID
Hop count= hop count+1= 1+1= 2
Arrival sequence=1, {as it is the first RREQ to arrive at all J,K,l}

After adding these values they forward RREQ packet to their neighbour. When M receives first RREQ from J, it creates reverse entry for hop count=2 and first hop=J,and find that it is first RREQ from J,it will accept it and and set following values before forwarding it further.

Hop count= 2+1=3
Arrival sequence= 1, {as it is first RREQ to arrive at O and Q both}

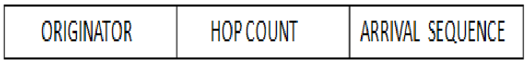
M forwards this RREQ with same field values to both O and Q. Now M will receive 2nd RREQ with same sequence number and hop count equal or smaller, but different first hop. M will create reverse entry for this RREQ and find that first hop of both RREQs is same, It will discard this RREQ.

Similarly N processes RREQ from K and L. at last stage, node Q on receiving RREQ from S, will discard it without creating reverse entry, because hop count of RREQ from S is greater than existing entries of RREQ.

When P receives RREQ from O and Q with same hop count creates reverse entry for firstly arrived RREQ and drop second RREQ because first hop field of both RREQs are same.

3.2.2.Route Reply procedure:

A node replies each RREQ if it have greater sequence number in its routing table than RREQ sequence number. Intermediate nodes reply to RREQ when they have an entry to destination node with valid bit=1 in its routing table. It uses three fields for route reply. These are shown below:



ORIGINATOR	HOP COUNT	ARRIVAL SEQUENCE

Fig3.6: fields used for Route Reply

Originator field contains the Id of node originating RREP packet. Count indicates the number of RREPs received with same sequence number. RREP having originator= Destination address have higher probability to be correct, other nodes may be claiming older paths to destination. other fields have same function.

Node receiving RREP will check legitimacy ratio of sender node, if it is lower than the threshold value, it simply discards RREP packet assuming it to be a malicious node. Otherwise it forwards RREP to its neighbor having higher legitimacy ratio from multiple backward entries and flush other entries.

After receiving RREP, node creates RREP in routing table as:

Valid bit= 0; {path may or may not be correct}
Count= 1
Originator= 1 {if node itself is generating RREP}
= 0 {if it received RREP from other node}

Intermediate node will create only one forward entry for an RREP regardless of number of RREPs received with same sequence number. Malicious node sends RREP with its own Identity (i.e node B1 in example) or with identity of destination (spoofed, node B2 in example) in originator field and very high sequence number because it does not know exact sequence number of destination node. intermediate node accepts first RREP and discard other. Following figure illustrates an example.

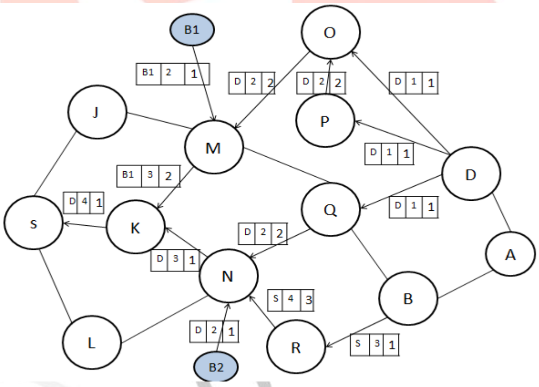


Fig3.7 : Route Reply procedure

In figure, S represents source node and D represents destination node. Nodes B1 and B2 are two malicious nodes. Node O receives two replies from node D and H. on first RREP arrival, O creates forward entry towards destination and forwards packet to backward entry towards M. On second RREP arrival, node O finds out entry to destination having same sequence number, which has least hop count, i.e. first RREP, and sets count field in routing entry to 2.

When node Q receives reply, it will check its legitimacy table to find which backward entries has higher legitimacy ratio (i.e M or N) and chooses node N. node N receives 3 replies, from B2, Q and R. B2(black hole) replies with higher sequence number and spoofs the destination node identity in originator field, Next hop will be chosen on following criteria.

As node N will receive RREP from Q,R and B2. N will create forward entries for each Q, R and B2.

If Q and R have same sequence number for destination, it creates one forward entry for Q and R, towards either Q or R based on their legitimacy ratio, if they have same hop count to destination, entry is created towards node having lower hop count value. It creates 2nd forward entry towards B2. First will be selected because it have higher value of count field (i.e. number of times RREP of this sequence number received is greater).

If reply of node B has an older sequence number of node D, then each reply has different sequence number. Node N will create three entries for each reply arrived from B2, Q and R respectively. The RREPs with destination address in the □□□□□□□□ field have a higher probability of correct path to destination than other RREPs because RREP originated by other nodes may claiming an older path to destination. two replies had different sequence number with the □□□□□□□□□□□ field containing destination address (it means any of them comes from malicious node), node N would choose forward entry whose next hop has higher legitimacy ratio inspite of their hop count by setting its □□□□□□□□=0 and others with -1. If both entries have similar legitimacy ratio then node N will randomly choose any of them.

Node M receives the first reply from B1 and it copies the reply content into the routing entry and forward the reply to the backward entry having higher legitimacy ratio i.e K. When node M received another reply from node O which had originator field filled with the destination address and different sequence number with an existing entry, then node M sets the second entry for data transfer regardless of the legitimacy ratio of next hop by setting its valid bit=0 and others valid bit=-1. It will not delete previous entry because the second RREP could have been generated by malicious node by spoofing destination address (not in this case). Node K will perform in a similar way to node M.

When source node receives RREP it starts sending data to destination. While forwarding data packet, each node will set counter to an interval to get data packet or route change packet within interval time. If time interval expires, node will increment selection field of next hop in legitimacy table and send route change packet to backward entry node.

Assume that SKNB2 is the path formed. Nodes in path will set counter interval as they forward data packet. Since B2 is a black hole, it will drop the packet, when counter interval of node N expires, it will increment 'selection' field of node B2 in its legitimacy table and delete corresponding entry in routing table and send route change packet to node K with change bit=1(because N has changed node to Q).Node K flushes counter and does not take decision to switch to next path, because node ahead in the route (i.e node N) already had changed path by setting change bit=1. Each node sends route change packet along reverse route unless source node reached. Assume remaining entries in routing table of node N towards destination node are dropped, then node N will send route change packet to node K with change bit=0. At the end of data communication, destination node will send final data acknowledgement packet to source node. All nodes in path will change sequence number of forwarding entry as listed in acknowledgement packet and set valid bit=1 in routing entry, delete other entries in table towards destination and increment 'selection' and 'success' field of previous hop and next hop of acknowledgement.

REFERENCES

[1] Ramaswamy S, Fu H, Sreekantaradhya M, Dixon J, Nygard K, " Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks", International Conference on Wireless Networks, Las Vegas, Nevada, USA, 23-26 June 2003

[2] Juan-Carlos Ruiz, Jesús Friginal, David de-Andrés, Pedro Gil "Black Hole Attack Injection in Ad hoc Networks"IEEE 2012

[3] Mohammad Al-Shurman and Seong-Moo Yoo, Seungjin Park" Black Hole Attack in Mobile Ad Hoc Networks" IEEE 2012

[4] Latha Tamilselvan, Dr. V Sankaranarayanan "Prevention of Co-operative Black Hole Attack in MANET" JOURNAL OF NETWORKS, VOL. 3, NO. 5, MAY 2008

[5] Jathe S.R. And Dakhane D.M. "A Review Paper On Black Hole Attack and comparison of different blackhole attack techniques" International Journal of Cryptography and Security ISSN: 2249-7013 & E-ISSN: 2249-7021, Volume 2, Issue 1, 2012, pp.-22-26.

[6] Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon and Kendall Nygard "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks " IEEE 2011

[7] Mr. Rajdipsinh Vaghela Mr. Divyesh Yoganand Mrs. Monika Changela "A Survey on Approaches towards the Black Hole Attack in Manet" Indan Journal Of Research Volume : 1 | Issue : 12 | December 2012.

[8] Deepak Singh Rana, Performance of AODV against Black Hole Attacks in Mobile ad-hoc Networks"IJCTA july 2012

[9] Ming-Yang Su1 , Kun-Lin Chiang "Mitigation of Black-Hole Nodes in Mobile Ad Hoc Networks "International Symposium on Parallel and Distributed Processing with Applications 2011

[10] Nidhi Purohit, Richa Sinha and Khushbu Maurya" Simulation study of Black hole and Jellyfish attack on MANET using NS3" INSTITUTE OF TECHNOLOGY, NIRMA UNIVERSITY, AHMEDABAD – 382 481, 08-10 DECEMBER, 2011.