International Journal of Advances in Computer and Electronics Engineering
Volume: 01 Issue: 03, July 2016, pp. 17 – 21

Algorithmic Approach to Secure Route Against Black Hole Attack in AODV Protocol for MANET

[1]Esha Rani, [2]Vikas Juneja
[1]Assistant Professor, Department of Computer Science, University College, Kurukshetra, India
[2]Associate Professor, Department of Information Technology, JMIT Radaur, India
[1]eshaom17@gmail.com, [2]vikasjuneja2002@gmail.com

Abstract: *In MANETs, topology is dynamic; environment is movable; network adapted is infrastructure less; due to all these properties, the dare is to construct a safe path for transmission and communication among data packet. The subsistence of different types of attacks has been found in Mobile Ad hoc Networks (MANETs). The most popular attack against the reactive routing protocol is Black Hole Attack. The endeavor of this paper is to explore Black hole attack, and defend Ad hoc on demand Distance Vector (AODV) against Black Hole. In this research paper an algorithmic approach to provide security against Black hole attack in the MANET is planned. The algorithm is practically performed on AODV protocol. The anticipated approach is to keep a Stack to store the values of all Destination Sequence Numbers (DSNs) in declining form. An elucidation is provided which is based on the Inspection of DSN and if it is more than the mean value of all DSNs stored on Stack and difference between topmost DSN on Stack and DSN in Initial Routing Table then this node is consider as malicious node; and store in other table named as Malicious Node Table(MNI); an alarm message is given to all its neighboring nodes; and after that next phase provides the confirmation of the nodes residing in MNI table as Black hole nodes. After corroboration, obliterate all that nodes from Discovered Route Table (DRT).*

Keyword: *AODV; Black Hole; DSDV; MANET; ZRP.*

1. INTRODUCTION – ROUTING PROTOCOLS WITH HIERARCHY

To deliver the packets on time, Routing protocols are used. In ad hoc networks, an optimal path (min hops) is set up by routing protocols between source and destination with minimum bandwidth consumption and minimum overhead. A MANET protocol should function effectively over a wide range of networking context from small ad hoc group to larger mobile Multi-hop networks.

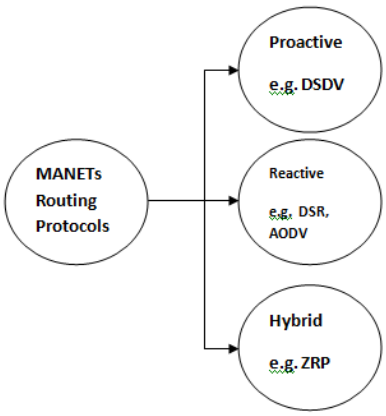


Figure 1 Routing Protocols Hierarchy

Figure 1 shows the categorization of these routing protocols. Routing protocols in MANETs are classified into 3 categories depending on the routing topology.

1.1 Proactive

Routing data is maintained in a table as which node is sending data to which node. All the information is stored in a table called as Routing Table. As nodes are mobile; network topology changes; that's the reason table should be manipulated periodically. As Route information is stored in table that's why this type of protocol is also called Table Driven Protocol. For smaller networks Proactive protocols are good but for are not suitable for larger networks because maintenance of node entries for each and every node in routing table causes overhead and bandwidth consumption is also more. e.g. Destination Sequence Distance Vector (DSDV).

1.2 Reactive

Reactive protocols are totally different from proactive as no table is maintained in Reactive protocols. It works only with active nodes. If no communication is there between any nodes then no routing information will be updated. Only information

International Journal of Advances in Computer and Electronics Engineering
Volume: 01 Issue: 03, July 2016, pp. 17 – 21

is updated when there is requirement of communication between any nodes. Suppose a node wishes to send a data packet to another node then only on demand, a route is found and path is set up to make the communication possible between these nodes. This process is done by flooding the Route Requests (RREQ) packets throughout the network. Path is established to send and receive the packets. Flooding of RREQ packets generate traffic problem to the network. Due to this problem, this protocol is less appropriate for real time traffic scenarios. Because path is established only on demand of the nodes that's why this protocol is also called source-initiated on demand protocol. e.g. Dynamic Source Routing (DSR) and AODV.

1.3 Hybrid protocols

In this type of protocol, above discussed both proactive and reactive protocol approaches are combined. Start of the routing is done by some proactively prospected routes and then demand from additionally activated nodes is taken.

The base of this scheme is that each node has a predefined zone centered at itself in terms of number of hops. Proactive routing protocols maintain temporarily routing table only for nodes within the zone. On other hand, on-demand routing scheme is espoused when inter-zone connections are required. e.g. Zone Routing Protocol (ZRP).

2. AODV TERMINOLOGY

Today wireless networks has become so popular MANET is a continuous self-configured, dynamic and infrastructure less network of mobile devices using wireless connection. AODV is an on-demand routing algorithm as it governs or establishes a route to a destination only just on demand or requirement of a node if it has any packet to send to that destination. Routes are maintained as long as they are needed by the source. Since nodes are continuously moving from one location to another, that's why Security of packets sent by nodes becomes an issue.

AODV consists of some properties:

Originating Node: A node that initiating a Route Discovery Process and broadcasting RREQ packets.

Routing Table: Every node maintains a table, containing information about which neighbor to send the packets to in order to reach the destination.

Active/Valid Route: In Routing table, the route from any node to destination marked as valid is used to forward data packets.

Invalid Route: A route that has been expired marked as invalid in Routing Table and restricts the data packets send by this route.

Sequence Numbers: It ensures the freshness of routes.

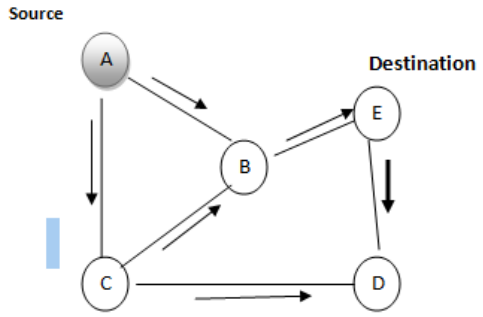
AODV Routing Protocol uses a reactive approach to find a path to the destination in an ad hoc network. AODV uses a destination sequence number for each route entry. DSN is produced or generated by destination node when demand for communication is requested from it. The advantage of using DSN is ensuring loop freedom and shortest path.

To search a route from one node to another node in ad hoc networks, three control messages are used:

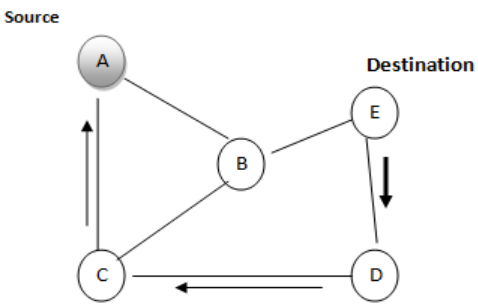
- Route Requests (RREQs),
- Route Reply (RREPs),
- Route Errors (RERRs).

AODV Routing protocols proffer swift variation to dynamic network conditions, small dispensation and storage expenses, less network bandwidth deployment with small size control messages.

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. depicts the flow of control messages



(a) Route Request Broadcast



(b) Route Reply path

Figure 2 Flow of control messages

International Journal of Advances in Computer and Electronics Engineering
Volume: 01 Issue: 03, July 2016, pp. 17 – 21

3.MANET ATTACKS

Due to open medium, dynamic topology, distributed cooperation, constrained capabilities; ad hoc networks are vulnerable to many types of security attacks according to their origin and their nature.

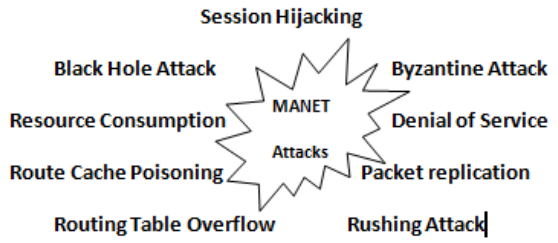


Figure 3 MANET Attacks

Explanation of various types of attacks is as follows:

Wormhole Attack: A malicious node receives packets at one site in the network and plummet them to another site in the network, where these packets are resent into the network. This tunnel between two colluding attackers is referred to as wormhole [4].

Black hole Attack: An attacker snoops the requests for the routers in a flooding based protocol .When the attacker receives a request for a route to the destination node, it creates a reply consisting of an extremely short route and enters into the pathway to do anything with the packets passing between them.[2]

Denial of Service Attack: This attack aims to attack the availability of a node or the entire network. If the attack is successful, the services will not be available. The attacker generally uses radio signal jamming and the battery exhaustion method.

Byzantine Attack: In this attack, a compromised intermediate node or an asset of compromised intermediate nodes works in collision and carries out attacks such as creating routing loops, forwarding packets on non-optimal paths and selectively dropping packets which result in disruption or degradation of the routing services.

Resource Consumption Attack: In this attack, an attacker tries to consume or waste away resources of the other nodes present in the network. The resources that are targeted are:

- Battery power,
- Band width,
- Computational power

Routing Table Overflow: In this case, the attacker create routes to nonexistent nodes, the goal is to create enough routes to prevent new routes from being created or to overwhelm the protocol implementation.

Packet replication: In this case, an attacker replicates stale packets.

Route Cache Poisoning: In the case the route cache is destroyed or damaged

Rushing Attack: On-Demand Protocols (such as AODV or DSR) that use duplicate suppression during the route discovery process are vulnerable to this attack.

Session Hijacking: At first the attacker spoofs the IP address of target machine and determines the correct sequence number. After that he performs s Denial of Service (DoS) attack on the victim. As a result the target system becomes unavailable for some time. The attacker now continues the session with the other system as a legitimate system.

Repudiation: In simple term, repudiation refers to the denial or attempted denial by a node involved in a communication of having participated in all or part of the communication.

4.BLACK HOLE ATTACK

Black hole attack is DoS attack. Malicious Node sends fake information and declared that it has a fresh or shortest path to destination node. Source node attracts to malicious node by this declaration and chooses the shortest path given by malicious node. Source Node sends all the data packets through this malicious node. The consequence is data loss or misuse [5]. In following figure, suppose, M is malicious node. When broadcasting of a RREQ packet is started by source node A, the packets are received by nodes B, E and M. Node M, being a malicious node, having no link with routing table, does not check the routing table for the requested route to node F.

Hence, it sends back a RREP packet without delay and stating that that it has a route to the destination. Node A receives the RREP from M ahead of the RREP from B and E. Node A assumes that the route through M is the shortest route and sends data packet to the destination through M As data send by node A to M, it absorbs all the data and thus behaves like a "Black hole".

M=Malicious Node
A= Source
D=Destination
RREQ
RREP
Data

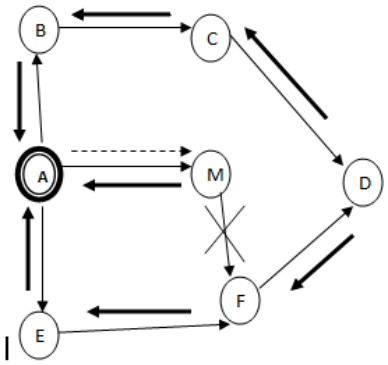


Figure 4 Black hole attack

International Journal of Advances in Computer and Electronics Engineering
Volume: 01 Issue: 03, July 2016, pp. 17 – 21

In AODV there are two type of black hole attack, these are following.

Internal Black hole attack An internal malicious node is fitted in between the routes of given source and destination, when it gets the opportunity this malicious node makes itself an active data route element. Now this node is able for attack with the start of data transmission. This is an internal attack because node itself belongs to the data route.

External black hole attack External attack virtually denies access to network. It itself physically stays outside of the network and from there handle the process of attack. External attack can become a kind of internal attack when it take a control of internal malicious node and control it to attack other nodes in MANET.

External black hole attack can be summarized as following points:

1. Malicious node detects the active route and notes the destination address.
2. Malicious node sends a route reply packet (RREP) including the destination address field spoofed to an unknown destination address. Hop count value is set to lowest values and the sequence number is set to the highest value.
3. Malicious node send RREP to the nearest available node which belongs to the active route. This can also be send directly to the data source node if route is available.
4. The RREP received by the nearest available node to the malicious node will relayed via the established inverse route to the data of source node.
5. The new information received in the route reply will allow the source node to update its routing table.
6. New route selected by source node for selecting data.
7. The malicious node will drop now all the data to which it belong in the route. [6]

5. PROPOSED PLAN

In this paper, a secure and efficient algorithm is described to tackle against Black Hole Attack. By this algorithm, Black Hole Node is firstly detected and after then entry of that node is removed from Routing list after confirmation. The algorithm is implemented in AODV Routing Protocol. With the help of the proposed algorithm, both Single Black hole attack and Co-operative Black hole Attack can be detected.

Source node S starts the route discovery procedure for the destination D by preparing a Route Request packet, called RREQ packet and broadcast this RREQ packet to all its neighboring nodes. All the nodes getting this packet, forward to their neighboring node and the process continue until the packet reaches to the Destination node. When destination node get this RREQ packet, prepares a new packet for the reply, called RREP packet and unicast this packet to the source node S. The source node waits for all the replies for a predefined time and stores them into its own DRT. After the collection of all replies from nodes in DRT, the nodes are sorted in terms of increasing order of Destination Sequence Numbers (DSNs). When sorting process completes, the nodes are picked one by one from DRT and PUSH onto STACK. POP the topmost entry of DSN from STACK and compare it with MEAN (Average of all DSNs on STACK). If topmost DSN of STACK is very much higher than MEAN and with this difference between NUID existed in IRT and DSN is very high then make the value of that NUID is 1.

Intermediate Node is now assumed as Malicious Node. Store this Malicious node in Malicious Node Table. An ALARM message is sent to all neighbours. Repeat this process while STACK becomes EMPTY. After collecting all the malicious nodes, Repeat the same procedure for another Destination just only for confirmation of Black Hole Nodes. After confirmation, All the entries existed in DRT are removed from DRT and continue the normal process of AODV. In this way AODV is secured against Black Hole Attack.

5.1 Algorithm to secure AODV against Black Hole Attack

SN - Source Node
IN - Intermediate Node
MN - Malicious Node
IRT – Initial Routing Table in AODV
DSN - Destination Sequence Number
RREQ – Route Request Packet
RREP – Route Reply Packet
NUID - Node Unique ID
STK – Stack
DRT-Discovered Route Table
MNT- Malicious Node Table

Step 1: Root Discovery Process (RDP)

The source node SN prepares RREQ packet (S, D, LSM, NUID) and broadcast it to all neighbours to initialize the route discovery process for the Dest D.

Step 2: Collecting Acknowledgement in form of replies.

The Source node stores all the replies sent by the destination node or the intermediate nodes in form of RREP packet (D, S, HP, DSN) until predefined time in DRT table.

Step 3: Arrangement of DSNs

Sort the replies in terms of increasing order of DSNs.

Step 4: Arrangement of RREP packets on Stack

Pick the RREP packets one by one from DRT table and PUSH onto STK.

Step 5: Calculation of Mean Value

Mean value is computed by taking the average of all DSNs in Stack.

Step 6: Identification of Malicious Node

Repeat while STK become empty.

```
{
POP the topmost entry of DSN from STK.
IF (DSN >> Mean) then
   IF (NUID – DSN is high) then
        Make the value of NUID of that node 1.
         IN is assumed as MN.
         Store IN to MNT with NUID.
         Send ALARM message to all neighbours.
    ENDIF
ENDIF
ELSE
Store the DSN with information in new DRT table.
}
Increment the TOP by 1.
```

Step 7: Confirmation of the Black hole Nodes

S Broadcasts a RREQ packet for another destination D1. Repeat steps 2 to 6 and values are stored in new tables. Match this new MNT list with previous MNT list. The nodes existed in both of the list assumed as the Black hole Nodes.

Step 8: Removal of Black hole Node

The Entry of all the Black hole nodes detected in step 7 is removed from DRT table.

Step9: Node Selection Process for Secure Routing

Sort the contents of DRT entries according to the DSN in decreasing order and select the node which has highest DSN.

Step 10: Continue Default Routing Process

Continue with the normal procedure of AODV Protocol.

6. CONCLUSION AND FUTURE WORK

In this paper, a simple approach for preventing the Black Hole attack in AODV is proposed. The proposed algorithm can be applied to identify and remove the black hole node and to gain the secured route from source to destination in the MANET. By this approach, loss of data packets will be less. As future work, we will implement this algorithm on simulator and intend to analyze the performance of the proposed solution based on the various security parameters and to prevent the cooperative black hole attack in the network. As the future work, this algorithm can be implemented for some other dangerous network layer attacks such as Grey hole or Wormhole attack etc and also it can modify for providing the better result for the large MANETs and large number of Black hole attacker nodes.

REFERENCES

[1] K. Lakshmi 1, S.Manju Priya2, A.Jeevarathinam3, K.Rama4, K. Thilagam5 "Modified AODV Protocol against Blackhole Attacks in MANET " International Journal of Engineering and Technology Vol.2 (6), 2010, 444-449

[2] Priyanka Goyal1, Vinti Parmar2, Rahul Rishi3 "MANET: Vulnerabilities, Challenges, Attacks, Application" IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011 ISSN (Online): 2230-7893

[3] Rusha Nandy, Debdutta Barman Roy "Study of Various Attacks in MANET and Elaborative Discussion Of Rushing Attack on DSR with clustering scheme " Int. J. Advanced Networking and Applications Volume: 03, Issue: 01, Pages:1035-1043 (2011)

[4] Abhay Kumar Rai, Rajiv Ranjan Tewari & Saurabh Kant Upadhyay "Different Types of Attacks on Integrated MANET-Internet Communication" International Journal of Computer Science and Security (IJCSS) Volume (4): Issue (3) 265

[5] Vinay P.Virada "Securing And Preventing Aodv Routing Protocol From Black Hole Attack Using Counter Algorithm" International Journal of Engineering Research & Technology (IJERT) Vol. 1 Issue 8, October - 2012 ISSN: 2278-0181.

[6] Chanchal Aghi, Chander Diwaker, "Black hole attack in AODV routing protocol: A Review" International Journal of Advanced Research in Computer Science and Software Engineering ISSN: 2277 128X.