International Journal of Computing and Business Research (IJCBR)
ISSN (Online) : 2229-6166
Volume 6 Issue 2 March 2015

Survey for Optimal Solution to resolve "Big Hole Attack" in AODV

Vikas Juneja
Assistant Professor
JMIT, Radaur Engg. College
Yamunanagar, India
Vikasjuneja2002@gmail.com

Ms. Esha Rani
Assistant Professor
University College, Kurukshetra, India
eshaom17@gmail.com

Abstract- **Due to dynamic topology, infrastructure less network and mobile environment adapted by MANET, to give the secure way to transmission and communication among data packets becomes a challenging and vital issue. MANET's are vulnerable to various types of attacks. Black Hole attack is one of the possible attacks. In this article, we will discuss the security issues of MANETs and concentrate on "Black-Hole Problem" that occurs in MANETs and will also try to find an optimal solution to resolve this problem. Black hole attack (also called sequence number attack) is one of the most common attacks made against the reactive routing protocol in MANETs. In black hole attack, a malicious node(s) advertises itself as impersonate node to destination node by fabricating the sequence number or by sending a spoofed route reply packet to source node, hence pretending to have the shortest and freshest route to the destination. The aim of this paper is to investigate Black hole attack, its effect on AODV & solutions to resolve Black Hole problem within the scope of ad hoc on demand distance vector (AODV) routing protocol.**
The rest of this paper is organized as follows. In Section II we will give the brief description of different types of routing protocols and detail note on AODV routing protocol. In Section III an overview of the Black Hole attack is provided. Section IV describes various solutions to resolve black hole attack problem faced in AODV with advantages and disadvantages. We conclude with recommendation plans for future work in Section V.

Keywords**: MANET, AODV, Black Hole, DSDV, ZRP**

II. Routing Protocols

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 Multi-hop networks.

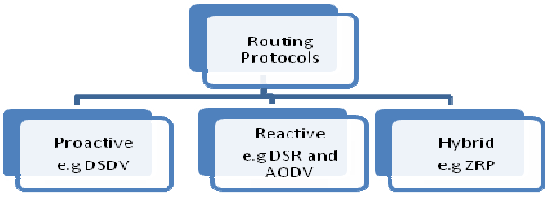

Fig.1 Hierarchy of Routing Protocols

Fig.1 shows the categorization of these routing protocols.

Routing protocols in MANETs are classified into 3 categories depending on the routing topology.

1. **Proactive:** Proactive protocols can also be called as table-driven since they maintain the routing information even before it is needed. Each and every node in the network maintains routing information to every other node in the network. Routes information is generally kept in the routing tables and is periodically updated as the network topology changes.
   There exist some differences between the protocols that come under this category depending on the routing information being updated in each routing table. Furthermore, these routing protocols maintain different number of tables.
   The proactive protocols are not suitable for larger networks, as they need to maintain node entries for each and every node in the routing table of every node. This causes more overhead in the routing table leading to consumption of more bandwidth. Examples of this type include Destination Sequence Distance Vector (DSDV).

2. **Reactive:** 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. They don't maintain routing information or routing activity at the network nodes if there is no communication. If a node wants to send a packet to another node then this protocol searches for the route in an on-demand manner and establishes the connection in order to transmit and receive the packet [1]. The route discovery usually occurs by flooding the route request packets throughout the network. 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. Example of this type includes Dynamic Source Routing (DSR) and Ad Hoc On-Demand Distance Vector (AODV).

3. **Hybrid protocols:** Hybrid protocols make use of both reactive and proactive approaches. The routing is initially established with some proactively prospected routes and then serves the demand from additionally activated nodes through reactive flooding. The basic idea is that each node has a pre-defined zone centered at itself in terms of number of hops. For nodes within the zone, it uses proactive routing protocols to maintain routing information. For those nodes outside of its zone, it does not maintain routing information in a permanent base. Instead, on-demand routing strategy is adopted when inter-zone connections are required. Example of this type includes Zone Routing Protocol (ZRP).

Introduction to AODV

Today wireless networks has become so popular MANET (Mobile Ad-hoc Network) 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.

In AODV, we concentrate on two things:

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

2. Sequence numbers: It ensures the freshness of routes.

Ad-hoc On-Demand Distance Vector (AODV) Routing Protocol uses a reactive approach to find 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 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.
Three type of control messages are required in AODV to establish a path from source to destination:

-Route Requests (RREQs),
-Route Replay (RREPs),
-Route Errors (RERRs)

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

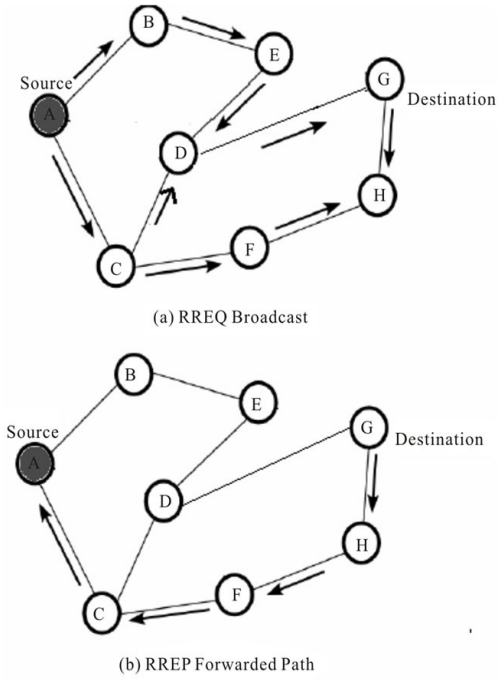

Fig.2 Flow of control messages

ATTACKS IN MANETS

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.

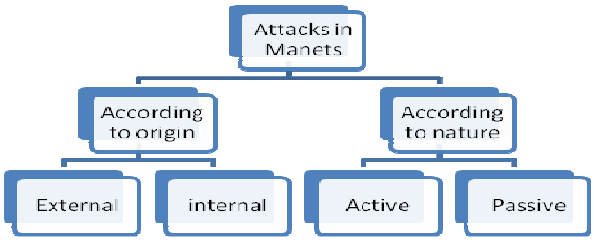

Fig. 3 Attacks in Manets

1. **External attack**
   External attacks are carried out by outside of the network. It is caused by a node that does not belong to logical network. It causes congestion sends false routing information or causes unavailability of services [2].
2. **Internal attack**
   Internal attacks are carried out by a node that belong to network. Unauthorized gain is accessed by malicious node and treated as a genuine node. Now it is authorized as a part of network and can participate in all activities of network. It can also analyze the traffic between nodes.
3. **Passive attack**
   A passive attack does not actually disrupt the operation of the network. E.g. Snooping: Snooping is unauthorized access to another person's data [3].
4. **Active attack**
   An active attack attempts to alter or destroy the data being exchanged in the network.

Here we will discuss other different types of attacks:

- **Wormhole Attack:** In wormhole attack, a malicious node, receives packets at one location in the network and tunnels them to another location 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 listen 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 a 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 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.

III. Black Hole Attack

Black hole attack is denial of service (DOS) attack in which malicious node send fake information by claiming that it has a fresh or shortest route to destination node and hence source nodes select this shortest path and go through this malicious node and result data misuse or discarded [5].

In following figure, imagine, M is malicious node. When node A broadcasts a RREQ packet, nodes B, C and M receive it. Node M, being a malicious node, this node does not check up with its routing table for the requested route to node E .Hence,

it immediately sends back a RREP packet, claiming that it has a route to the destination. Node A receives the RREP from M ahead of the RREP from B and C. Node A assumes that the route through M is the shortest route and sends any packet to the destination through it. When the node A sends data to M, it absorbs all the data and thus behaves like a "Black hole".

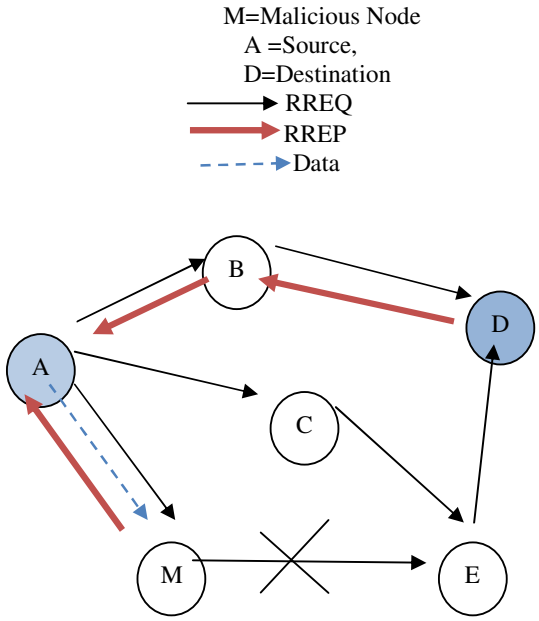

Fig.4 Black hole attack in AODV

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

Internal Black hole attack

This type of black hole attack has an internal malicious node which fits in between the routes of given source and destination, when it gets the chance this malicious node makes itself an active data route element. Now this node is capable of conducting 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 physically stays outside of the network and denies access to network. 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]

IV. Solutions for Resolving the problem of Black Hole Attack

1. **Check Authentication:** The first solution the sender node needs to verify the authenticity of the node that initiates the RREP packet by utilizing the redundancy of the network. The idea of this solution is to find more than one route for the destination. The SN unicast the ping packet using different routes. The IN or destination node or malicious node will ping requests. The SN checks the acknowledgment and processes them to check which one is safe or having malicious node. In the meantime the SN buffered its packet until it found the safe route. When the route is identified the buffered packets will be transmitted to it. The drawback of the solution is the time delay.

2. **Sequence Number:** The second solution is to store the last sent packet sequence number and the last received packet sequence number in the table. It is updated when any packet is arrived or transmitted. When node receives reply from another node it checks the last sent and received sequence number. If there is any mismatch then an ALARM indicates the existence of a Black hole node. This method is faster and more reliable and has no overhead.

3. **DRI and Cross checking:** 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.

4. **Discover the Safe Route:** 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 values is considered as malicious node and is eliminated.

5. 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).

The solution that we are proposing here only modifies the working of the source node without altering intermediate and destination nodes by using a method called Prior_RceiveReply. In this method we add the two things, a new routing table RR-Table (Request Reply), a timer WT (Waiting Time) to the data structures in the AODV Protocol.

The main benefits for modifying AODV protocol is:
a) The malicious node is identified at the initial stage itself and immediately removed so that it cannot take part in further process.
b) With no delay the malicious node are easily identified. Generally the malicious node having the highest DSN and its RREP is first to arrive.
c) No modification is made in the default operation of AODV.
d) Better performance produced in little modification.
e) Less memory overhead.

Two metrics are discussed in this method:
PDR - The percentage of data packets delivered to destination with respect to the number of packets sent. This metric shows the reliability of data packet delivery.

Packet Loss - This metric informs us about the amount of control packets fails to reach its destination in a timely manner, there is very less packet lost percentile in the proposed AODV as compared to the AODV various security parameters like mean delay time, packet overhead, memory usage, increasing number of malicious node, increasing number of nodes and scope of the black hole nodes and also focusing on resolving the problem of multiple attacks against AODV.

6. The method requires the intermediate node to send a RREP packet with next hop information. When a source node receives the RREP packet from an intermediate node, it sends a Further Request to the next hop to verify that it has a route to the intermediate node who sends back the RREP packet, and that it has a route to the destination. When the next hop receives Further Request, it sends Further Reply which includes check result to source node. Based on information in Further Reply, the source node judges the validity of the route

V. CONCLUSIONS AND FUTURE WORK

This article would be a great help for the people conducting research on MANET security. A lot of concepts regarding various security problems are mentioned in this paper. More concentration is given to find the optimal solution to resolve the Black Hole Attack. For that purpose, various solutions are discussed. But each and every solution has advantages and disadvantages. Our future aspect will be to detect the Black Hole at initial stages and find a solution to remove at that stage either by remove the drawbacks of methods or to combine the features of two or more methods.

Recommendations for future work:
While significant work has been done in this area, but still exploration is needed in this field. Work that should follow this work is to remove the drawbacks of all the techniques discussed above and find a suitable technique to resolve the problem of Black Hole at initial stage so that it should not become a hard problem later.

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