Volume 3, Issue 4, April 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Black hole attack in AODV routing protocol: A Review

Chanchal Aghi[1], Chander Diwaker[2]
[1]Research Scholar, U.I.E.T, Kurukshetra University Kuruksheta, Haryana, INDIA
[2]Assistant Professor, U.I.E.T. KurukshetraUniversity, Kurukshetra, Haryana, INDIA

Abstract: A Mobile Ad-Hoc Network is a self-configured collection of mobile nodes in which there is no need of predefined infrastructure. In this network nodes can arbitrarily change their geographic locations. MANET is more vulnerable to cyber attacks than wired networks because of no any central coordination mechanism. The Black hole attack at network layer is the most attention seeking attack in AODV routing protocol as compared to other protocols. This paper presents a review of Black hole attack in AODV routing protocol.

Keywords: MANET, AODV, Security, Black hole Attack, Detection and Prevention Techniques

I. INTRODUCTION

MANETs is an autonomous system in which different mobile nodes are connected to each other by wireless links. Nodes in the network can be either fixed or mobile. In MANET, communication occurs between nodes directly or through intermediate nodes which act as routers [1].AODV is Adhoc on Demand Distance Vector routing protocol. AODV protocol is preferred as compare to other protocols because it minimizes the routing overhead [2].AODV provides loop free routes and repair broken links [3]. AODV is an on demand routing protocol, this means that routes are only established when needed to reduce traffic overhead. The black hole attack is one of the most severe security attacks which can significantly disrupt the communications across the network. AODV protocol use control messages to find a route from source to the destination node in the network [4]. There are three types of control messages in AODV; these are Route Request Message (RREQ), Route Reply Message (RREP), and Route Error Message (RERR).This paper presents how black hole attack occurs in AODV routing protocol and various methods to detect and prevent Black hole attack in AODV.

II. BLACK HOLE ATTACK IN AODV

In Black hole attack a malicious node advertises about the shortest path to the node whose packets it wants to intercept [5].In following figure, imagine, M is malicious node. When node A broadcasts a RREQ packet, nodes B, D 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 D. Node A assumes

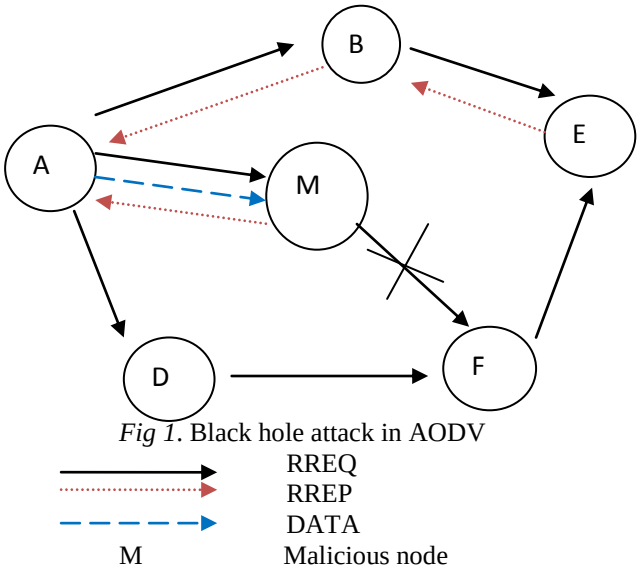

Fig 1. Black hole attack in AODV

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'.
In AODV there are two type of black hole attack [4], 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.

III. Detection And Prevention Techniques Of Black Hole Attack In Aodv

(i) Detection, Prevention and Reactive AODV (DPRAODV) Scheme

A new control packet called ALARM is used in DPRAODV [6], while other concepts are the dynamic threshold value. Unlike normal AODV, the RREP Sequence Number is extra checked whether higher than the threshold value or not. If the value of RREP sequence Number is higher than the threshold value, the sender is referenced as an attacker and updated it to the black list. The ALARM is sent to its neighbours who includes the black list, thus the RREP from the malicious node is blocked but is not processed. On the other hand, the dynamic threshold value is changed by calculating the average of destination sequence number between the sequence number and RREP packet in each time slot. According to this scheme, the black hole attacks not only be detected but also prevented by updating threshold which responses the realistic network environment. The advantage of DPRAODV is that it achieves an obviously higher packet delivery ratio than the original AODV, except for it takes a little bit higher routing overhead and end to end delay. But DPRAODV simply detects multiple black holes rather than cooperative black hole attack.

(ii) DRI Table and Cross Checking Scheme

Data routing information (DRI) table and cross checking method is use to identify the cooperative black hole nodes, and utilize modified AODV routing protocol to achieve this methodology [7]. Every node needs to maintain an extra DRI table, 1 represents for true and 0 for false. The entry in table is composed of two bits, "From" and "Through" which stands for information on routing data packet from the node and through the node respectively. As shown in following Table , the entry 1 1 implies that node 1 has successfully routed data packets from or through node 3, and the entry of 0 0 means that node 1 has not routed any data packets from or through node 5.The procedure of proposed solution is simply described as below. The source node (SN) sends RREQ to each node, and sends packets to the node which replies the RREP packet. The intermediate node (IN) transmits next hop node (NHN) and DRI table to the SN, then the SN cross checks its own table and the received DRI table to determine the IN's honesty. After that, SN sends the further request to IN's NHN for asking its routing information, including the current NHN, the NHN's DRI table and its own DRI table. Finally, the SN compares the above information by cross checking to judge the malicious nodes in the routing path. The advantage of this technique is it can identify multiple collaborative black hole nodes. The drawback of this technique is that mobile nodes have to maintain an extra database of past routing experiences in addition to a routine work of maintaining their routing table.

Node ID	**Data routing information From**	**Data routing information Through**
5	**0**	**0**
3	**1**	**1**

Table 1. Data Routing Information (DRI)

(iii) Distributed Cooperative Mechanism (DCM)

Distributed and cooperative mechanism DCM is used to solve the collaborative black hole attacks in AODV routing protocol, Because the nodes works cooperatively, they can analyze and detect, multiple black hole attacks [8]. The DCM is composed of four sub-modules which shown in following figure. In the local data collection phase, an estimation table is constructed and maintained by each node in the network. Each node evaluates the information of overhearing packets to determine whether there is any malicious node. If there is one suspicious node, the detect node initiates the local detection phase to recognize whether there is possible black hole. The initial detection node sends a check packet to ask the cooperative node. If the inspection value is positive, the questionable node is regarded as a normal node. Otherwise the initial detection node starts the cooperative detection procedure, and deals with broadcasting and notifying all one-hop neighbours to participate in the decision making. Because the notify mode utilizes broadcasting method, the network traffic is increased. A constrained broadcasting algorithm is used to restrict the notification range within a fixed hop

count. Finally, the global reaction phase is executed to set up a notification system, and sends warning messages to the whole network. There are reaction modes in global reaction phase. Though the first reaction mode notifies all nodes in the network, but might waste lots of communication overhead. Each node only concerns its own black hole list and arranges its transmission route in other mode, however it might be exploited by malicious nodes and needs more operation time. Advantage of this technique is that, DCM has a higher data delivery ratio and detection rate even if there are various black hole nodes.

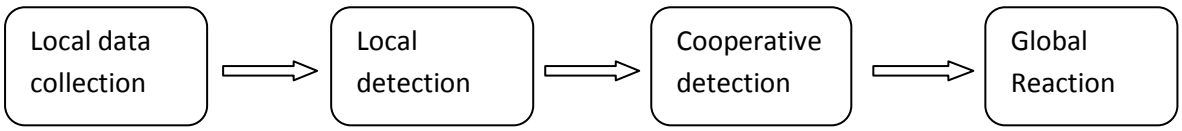

***Fig 2*. Sub-modules of Distributed Cooperative Mechanism (DCM)**

(iv) Neighborhood-based and Routing Recovery Scheme

This detection scheme based on a neighborhood-based method to recognize the black hole attack, and a routing recovery protocol to build the correct path [9][10]. This method is employed to identify the nodes which are unconfirmed .In this method, source node sends a Modify Route Entry control packet to destination node to renew routing path in the recovery protocol. In this scheme, not only a lower detection time and higher throughput are acquired, but the accurate detection probability is also achieved. The main limitation of this scheme is that it becomes useless when the attacker agrees to forge the fake reply packets.

(v)Redundant Route Method and Unique Sequence Number Scheme

In this scheme there are two techniques to prevent the black hole attack. The first technique is to find a true path to the destination [6]. A method based on neighbour set information is designed to deal with the black hole attack, which consists of two parts: detection and response. In detection procedure, two steps are: 1- Collect neighbor set information. 2-Determine whether there exists a black hole attack. In Response procedure, Source node sends a modify Route Entry (MRE) control packet to the Destination node to form a correct path by modifying the routing entries of the intermediate nodes (IM) from source to destination. This scheme effectively detects black hole attack without introducing much routing control overhead to the network find at least two routes from the source to the destination node. The working of this scheme is as follow: Firstly the source node sends a ping packet (a RREQ packet) to the destination. The receiver node with the route to the destination will reply to this RREQ packet and then the acknowledge examination is started at source node. Then the sender node will buffer the RREP packet sent by different nodes until there are it represents that there are at least two routing paths existing at the same time. After that, the source node identifies the safe route by counting the number of hops or nodes and thus prevents black hole attacks. In the second technique, unique sequence number is used. The sequence value is aggregated; hence it's ever higher than the current sequence number. In this technique, two values are recorded in two additional tables. These two values are last-packet-sequence-numbers which is used identify the last packet sent to every node and the second one is for the last packet received. Whenever a packet are transmitted or received, these two table values are updated automatically. Using these two table values, the sender can analyze whether there is malicious nodes in network or not. Simulation result shows that these techniques have less numbers of RREQ and RREP when compared to existing AODV. Second technique is considered to be good as compared to first technique because of the sequence number which is included to every packet contained in the original routing protocol. The limitation for this technique is these both techniques fail to detect cooperative black hole attacks.

IV. Conclusion

Black hole attacks in AODV routing protocol are severe attacks that can easily be launched even with confidentiality and authenticity. Malicious nodes usually targets the routing control messages related to routing information. In this paper, we introduced the Black hole attack in AODV routing protocol along with its classification that can have serious consequences. Various techniques used for the detection and prevention of Black hole attacks such as DPRAODV,DRI Table and cross checking scheme ,DCM and many other along with their advantages and limitations.

References

[1] Samba Sesay, Zongkai Yang and Jianhua He, "A Survey on Mobile Ad Hoc Wireless Network", Information Technology Journal 3 (2): 168-175, 2004.

[2] Amandeep and Gurmeet Kaur, "Performance Analysis of Aodv Routing Protocol in Mantes", International Journal of Engineering Science and Technology, p.p 3620-3625, 2008.

[3] Charles E. and Elizabeth M., "Adhoc on Demand Distance Vector Routing", p.p 1-11.

[4] Irshad Ullah ,Shoaib Ur Rehman, "Analysis of Black Hole Attack on MANETs Using Different MANET Routing Protocols" in Thesis no: MEE 10:62 in June, 2010.

[5] Latha Tamilselvan and Dr. V Sankaranarayanan, "Prevention of Blackhole Attack in MANET", 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, 2007.

[6] Ankita singh Kushwah, Krittika Khator and Atul Singhal, "A Review on Prevention and detection Techniques for Black hole Attack in Manet", ISSN: 2319-6327, Vol. 2, No. I (2013), pp. 24-27.

[7] H.Weerasinghe and H. Fu.Preventing, "Cooperative black hole attacks in mobile adhoc networks:simulation implementation and evaluation", Future generation communication and networking, volume 2,IEEE 2007, pp. 362-367.

[8] Tamilselven L and Sankaranarayanan, "Prevention of Black hole Attack in MANET" International Conference on wireless Broadband and Ultra Wideband Communications, 27-30 August 2007.

[9] Sun B,Guan Y and Pooch UW, "Detecting Black hole Attack in Mobile Adhoc Networks" ,Paper presented T 5th European Personal Mobile Communication Conference, April 2003.

[10] Fan-Hsun Tseng, Li-der chou and Han-chieh chao, "A survey of black hole attack in wireless mobile adhoc networks", springer journal 2011.

