Volume 2, Issue 1 ISSN: 2320-5288

International Journal of Engineering Technology & Management Research
Journal homepage: www.ijetmr.org

A Survey on Black Hole Attack in AODV Routing Protocol

Dr. Mamta Lambert
Associate Professor
Department of Computer Applications
Jabalpur Engineering College
Jabalpur , India
Email: lambert_mamta@yahoo.co.in

Mr. Sharda Prasad Patel
Email :- sharda21patel@gmail.com

***Abstract*—**Mobile Ad-Hoc network is an autonomous system, where station or nodes are connected with each other through air medium links. It is also called infrastructure less network. It is a collection of mobile nodes that dynamically form a temporary network without infrastructure. Each mobile node can move freely in any direction and changes their links to other devices frequently. In MANET different types of routing protocols have been recommended. Ad-hoc On demand Distance Vector (AODV) is one of the most suitable routing protocol for the MANETs and it is more vulnerable to black hole attack by the malicious nodes. In this attack, the malicious node advertises itself as having the shortest path to the destination and falsely replies to the route requests, and drops all receiving packets. In this paper, we have surveyed and compare the existing solutions to black hole attacks on AODV protocol and their drawbacks.

Keywords:— MANET, AODV, DRS, OLSR, DSDV.

1. INTRODUCTION

Wireless networks have been gaining popularity to its peak today, as the user wants wireless connectivity irrespective of their geographic position. MANET is a collection of infrastructure less nodes which cooperates with each other to form temporary network. It consists of a collection of wireless mobile nodes that have capability to communicate with each other without the use of network infrastructure or any centralized administration. The nodes in ad hoc networks act as a host as well as router to forward the data packets. MANETs have many potential applications, like Sensor Networks, Medical Service, Personal Area Network, especially in military and rescue operations. Due to the inherent characteristics like dynamic topology and lack of a centralized management security, MANETs are vulnerable to several kinds of attacks like black hole attack, wormhole, denial of services Routing table overflow, impersonation, information disclosure etc.

2. ROUTING IN MANET

In MANETs nodes communicate with each other by using some routing protocols. According the dynamic topology and characteristic there are three main routing protocol used in MANETs. These all are discussed below.

A. Reactive (On-Demand) Routing Protocol:

Reactive protocols also known as on demand driven reactive protocols. The fact they are known as reactive protocols is, they do not initiate route discovery by themselves, until they are requested, when a source node request to find a route. The reactive protocols have the low routing overhead at the expense of delay to

discover the route when desired by the source.

The two kinds of protocols are there in it AODV (Ad hoc On Demand Distance Vector Protocol), DSR (Dynamic source routing).

B. Proactive (Table Driven) Routing Protocol:

This protocol is also called as table driven protocol because routing information of nodes is exchanged, Periodically and accordingly the routing table is maintained, even when there is no communication. Proactive protocols have low latency rate in discovering the route but high routing overhead. This is because the nodes periodically exchange control messages and routing table information in order to keep up-to-date routes to any active node in the network.

The two main kind of proactive protocols are Optimized link state routing (OLSR) protocol and Destination sequenced distance vector routing (DSDV) protocol.

C. Hybrid Routing Protocol:

This protocol combines advantages of both proactive and reactive routing protocol. Two types are: Zone routing protocol (ZRP) and Temporally ordered Routing protocol (TORA).

3. AODV ROUTING SCHEME

The Ad-hoc On-Demand Distance Vector (AODV) is a reactive routing protocol in mobile ad hoc networks. It finds a route to a destination when a node likes to transfer a packet to that destination. Route discovery process is based on the route information which is stored in all intermediate nodes along the route in the form of route table entries. Every node has routing table, it has the fields like destination, next hop, number of hops, destination sequence number, and active number of hops, destination sequence number, active neighbors and lifetime respectively. AODV uses several control packets like route request packet (RREQ) is broadcasted by a node requiring a route to another node, routing reply message (RREP) is unicasted back to the source of RREQ, and route error message (RERR) is sent to notify other nodes of the loss of the link. HELLO messages are used to find active neighbors. Sequence numbers are used to find the freshness of routes towards the destination.

The format of RREQ and RREP packets are in Fig 3.1 and 3.2 respectively.

Src_ ad-dres	Src_ se-quene	Broad _ Cast_ id	Dest _ ad-dres	Dest_ se-quence	Hop cou nt

Figure 1. AODV RREQ Field

Src_ ad-dres	Dest_ addres	Dest_ se-quence	Hop count	Life time

Figure 2. AODV RREP Field

The given Fig 3 and 4 shows the propagation of the RREQ packets to all the neighboring nodes, and the path of RREP packet towards the source respectively.

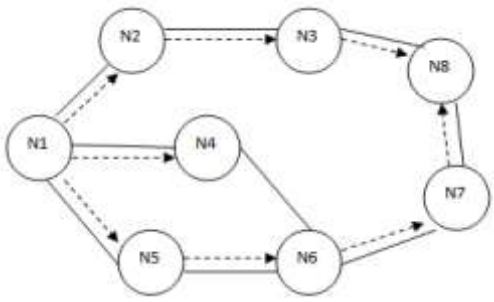

Figure 3 Propagation of RREQ

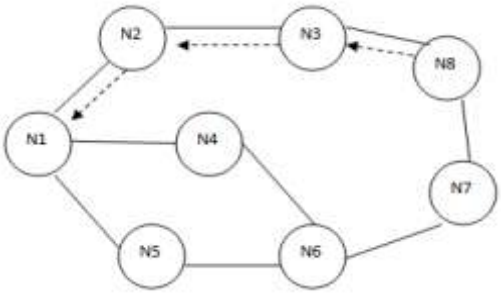

Figure 4. The Path of RREP

When a route is not available for the destination, a route request packet (RREQ) is flooded throughout the network. The RREQ contains source address along with request ID is incremented each time the source node sends a new RREQ and identifies it uniquely. On receiving a RREQ packet, each node checks the source address and the request ID. If the node has already received a RREQ with the same pair of parameters the new RREQ packet will be discarded Otherwise the RREQ will be either forwarded (broadcast) or replied (unicast) with a RREP packet: once a RREP packet is received, the route is established . A source node may receive multiple RREP packets with different routes. It then updates its routing entries if and only if the RREP has a greater sequence number, i.e. fresh information. While transmitting RREQ packets through the network, each node notes the reverse path to the source. When the destination node is found the RREP packet will travel along this path (the reverse path to the source [2].

Recently, most research on ad-hoc routing protocols, has been assumed trusted environment but, many usages of ad-hoc network run in untrusted situations. Therefore, most ad hoc routing protocols are vulnerable to different types of attacks. These attacks are divided into two categories, called external attacks and internal attacks. Internal attacks are done by authorized node in the network, where as external attacks are performed by the node that they are not authorized to participate in the network.

4. BLACK HOLE ATTACK ON AODV PROTOCOL

Black hole attack is a big problem in MANETs in which an intermediate node works as malicious and consumes data before reaching to the destination. Black hole attack works in two phases in first phase, it advertises that it has a fresh route to the destination to deliver data packets with intention to drop data packets. In second phase it drops data packets without forwarding it. In this whenever any intermediate node gets a RREQ it immediately generates a RREP with high destination sequence number and sends it to the initiator. Source stops receiving RREP and starts sending data packet to that node which has sent RREP to the source.

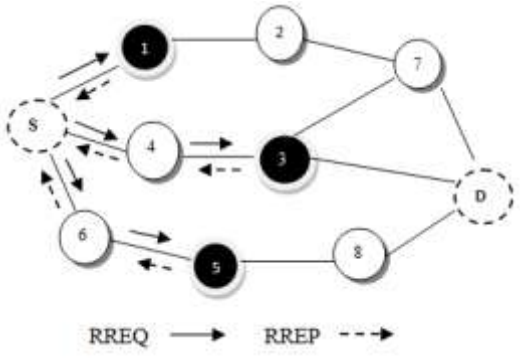

Figure 5. Multiple Black Hole Nodes

In above figure, there are more than one black hole node i.e. 1,3 and 5 exists in the network at different places in order to drop the data packets.

5. EXISTING TECHNIQUES

A. Based on Rules

Mehdi Medadian and KhossroFardad [10] use and approach where the node uses number rules to inference about honesty of reply's sender. The activities of a node are logged by its neighbors. These neighbors are requested to send their opinion about a node. When a node collects all opinions of neighbors, it decides if the replier is a malicious node. The decision is based on number rules. The judgment is based on node's activity in network. First rule says that if a node delivers many data packets to destinations, it is assumed as an honest node. According to second rule, if a node receives many packets but dose not send same data packets, it's possible that the current node is a misbehavior node. When the rule2 is correct about a node, and if the current node has sent number RREP

packets; therefore surely the current node is misbehaving. When the rule2 is correct about a node, if the current node has not sent any RREP packets; therefore the current node is a failed node..

1. Disadvantage:

It cannot detect co-operative black hole attack.

B. Reliable Route

[2] Khamayseh,Y., Bader,A., Mardini,W. and BaniYasein, M proposed a new protocol is built on top of the original AODV It extends the AODV to include the following functionalities: source node waits for a reliable route; each node has a table in which it adds the addresses of the reliable nodes; RREP is overloaded with an extra field to indicate the reliability of the replying node. The simulation of the proposed protocol shows significant improvement in the terms of: packet delivery ratio, number of dropped packets, and end to- end delay. The conditions of passing the behavioral analysis filter are not satisfied enough to judge the reliability of the node.

1. Disadvantage:

The protocol does not consider the behavior of two black hole nodes working together as a team.

C. Route Confirmation Approach (RCA)

In [3], the authors introduce the route confirmation request (CREQ) and route confirmation reply (CREP) technique to avoid the black hole attack in the network. In this approach, the intermediate node not only sends RREP messages to the source node but also sends CREQ messages to its next-hop node toward the destination node. This is to enquire about the route to the destination node. After receiving a CREQ message, the next-hop node searches its cache for a route to the destination. If it has the route, it sends the CREP to the source. On receiving the CREP message, the source node confirms the validity of the route by comparing the route in RREP message and the one in CREP. If both are the same, the source node confirms that the route is correct.

1. Disadvantage:

It cannot avoid the black hole attack in which two consecutive nodes work in agreement with each other, that is, when the next-hop node is an attacker working together with the malicious node sending CREPs that support the incorrect path.

D. Multiple Route Replies (MRR)

In [4], the authors have discussed the AODV protocol that suffers from the Black hole attack in MANETs and has proposed a realistic solution for the black hole attacks, which can be implemented on the AODV protocol. This mechanism expects a source node to wait until an RREP packet arrives from more than two nodes. Upon receiving multiple RREPs, the source node checks whether there is a shared hop or not. If there is, the source node confirms that the route is safe and can be used.

1. Disadvantage:

The technique introduces time delay, because it has to wait until multiple RREPs arrive.

E. Anti Black Hole

In [5] Authors Ming-Yang Su et.al discussed a mechanism, called an ABM (Anti-Black hole Mechanism), which is mainly used to estimate the suspicious value of a node according to the amount of abnormal difference between RREQs and RREPs transmitted from the node. When a suspicious value exceeds a threshold level, the nearby IDS broadcasted a block message with id of IDS, the identified black hole node and the time of identification will place the
malicious nodes on their blacklists to isolate the malicious node in the network cooperatively.

1. Advantage:

It can be able to detect cooperative black hole nodes in the MANETs.

2. Disadvantage:

The mobile nodes have to maintain an extra database for training data and its updation, in addition to the maintenance of their routing table.

F. Reverse Adhoc On demand Distance Vector (RAODV)

The proposed RAODV discovers route using reverse route discovery procedure where the destination node DN sends reverse-route request (R-RREQ) messages to its neighbors to find a valid route to the source node SN after receiving RREQ from source node[6]. Their simulation results show that RAODV does improve the performance of AODV in metrics such as packet deliver ratio (PDR), end-to-end delay, and energy consumption. The original SN starts message transmission whenever it receives the first R-RREQ and saving late arrived R-RREQ for times when the primary path fails.

G. DRI Table And Cross Checking Scheme

Hesiri Weera singhe et al. proposed an algorithm to identify Collaborative black hole attack. In this the AODV routing protocol is slightly modified by adding an additional table i.e. Data routing information (DRI) table and cross checking using further request (freq) and further reply (FREP)[8,9] . If the source node (SN) does not have the route entry to the destination, it will broadcast a RREQ (route request) message to discover a secure route to the destination node same as in the AODV. Any node received this RREQ either replies for the request or again broadcasts it to the network depending on the availability of fresh route to the destination. If the destination replies, all intermediate nodes update or insert routing entry for that destination since we always trust destination. Source node also trusts on destination node and will start to send data along the path that reply comes back. Also source node will update the DRI table with all intermediate nodes between source and the destination.

Table 1. Comparison of Various Existing Techniques

TECH-NIQUE PRO-POSED	ATTACK	DRAWBACKS
Based on Rules	Single black hole	Cannot detect co-operative black hole nodes.
Reliable route	Single black hole	Does not consider the behavior of two black hole nodes working together
Route Con-firmation Approach *(RCA)*	Single black hole	Can be applied only to avoid one mali-cious node
Multiple Route Re-plies(MRR)	Coopera-tive black holes	Inefficient in terms of time delay
Anti Black Hole(ABH)	Multiple black holes	Time delay
Reverse AODV *(RAODV)*	Single black hole	More overhead
DIR Table and Cross Checking Scheme	Coopera-tive black holes	Maintenance of DRI tables apart from normal routing infor-mation.

6. CONCLUSION

This paper has amalgamated various works related to black hole attack detection mechanism in AODV-based MANETs. The various authors have given several proposals for detection and prevention of black hole attacks in MANET but every

proposal has its own disadvantages in their respected solutions and we made a comparison among the existed solutions. We observe that the mechanisms detects black hole node, but no one is reliable procedure since most of the solutions are having more time delay, much network overhead because of newly introduced packets and some mathematical calculations.

REFERENCES:

[1] Pooja Jaiswal, Dr. Rakesh Kumar "Prevention of Black Hole Attack in MANET", IRACST – International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 2250-3501 Vol.2, No5, October 2012.Ding, W. and Marchionini, G. 1997 A Study on Video Browsing Strategies. Technical Report. University of Maryland at College Park.

[2] Y. Khamayseh, A. , Bader, W. Mardini and M. BaniYasein, "A New Protocol for Detecting Black Hole Nodes in Ad Hoc Networks "International Journal of Communication Networks and Information Security (IJCNIS) Vol. 3, No. 1, April 2011.

[3] Bounpadith Kannhavong, Hidehisa Nakayama, Yoshiaki Nemoto, and Nei Kato; "A SURVEY OF ROUTING ATTACKS IN MOBILE AD HOC NETWORKS", IEEE Wireless Communications • October 2007. PP: 85-90.Sannella, M. J. 1994 Constraint Satisfaction and Debugging for Interactive User Interfaces. Doctoral Thesis. UMI Order Number: UMI Order No. GAX95-09398., University of Washington.

[4] Modified AODV Protocol against Black hole Attacks in MANET by K. Lakshmi1, S.Manju Priya, A.Jeevarathinam, K.Rama, K.Thilagam, Lecturer, Dept. of Computer Applications, Karpagam University, Coimbatore, International Journal of Engineering and Technology. Vol.2 (6), 2010.Brown, L. D., Hua, H., and Gao, C. 2003. A widget framework for augmented interaction in SCAPE.

[5] Ming-Yang Su; Kun-Lin Chiang; Wei-Cheng Liao, "Mitigation of Black-Hole Nodes in Mobile Ad Hoc Networks," Parallel and Distributed Processing with Applications (ISPA), 2010 International Symposium on, vol., no., pp.162-167, 6-9 Sept. 2010.

[6] C. Kim, E. Talipov and B. Ahn, "A Reverse AODV Routing Protocol in Ad Hoc Mobile Networks," Pro- ceeding from EUC'06: The 2006 International Confer- ence on Emerging Directions in Embedded and Ubiqui- tous Computing, Seoul, 1-4 August 2006, pp. 522-531.

[7] S. Dokurer, Y. M. Erten and E. A. Can, "Performance Analysis of Ad -Hoc Networks under Black Hole Attacks," Proceeding from SECON'07: IEEE Southeast Conference, Richmond, 22-25 March 2007, pp. 148-153.

[8] K. Makki, N. Pissinou, and H. Huang, "Solutions to the black hole problem in mobile ad-hoc network," 5th World Wireless Congress, pp.508–512, 2004.Ding, W. and Marchionini, G. 1997

[9] Video Browsing Strategies. Technical Report. University of Maryland at College Park

[10] Ms Monika. Dangore1, Mr Santosh S. Sambare2 1G.H. Raisoni College of Engineering, 2Pimpri Chinchwad College of Engineering Pune, India "A Survey On detection Of Blackhole

[11] Attack In AODV protocol in

MANET" IJRITCC Jan 2013

[12] S. Lu, L. Li, K.Y. Lam, L. Jia, "SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack.," International Conference on Computational Intelligence and Security, 2009.