**International Journal of Engineering Research and Development**
*e-ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com*
*Volume 10, Issue 12 (December 2014), PP.72-77*

# Review on Detection & Prevention Methods for Black Hole Attack on AODV based MANETs

Dipali Sheth[1], Sunera Kargathara[2], Sunil Lavadiya[3]
[1]*Student of M.E., Department of E.C., MEFGI, Rajkot.*
[2]*Assistant Professor. Department of E.C., MEFGI, Rajkot.*
[3]*Assistant Professor. Department of E.C., MEFGI, Rajkot.*

**Abstract:-** Dynamic nature of Mobile Ad-hoc networks (MANET) challenges the quality of service (QoS) because route failure probability is increased in MANET due to the mobility of nodes. Lack of fixed infrastructure, wireless shared medium and dynamic topology makes MANET prone to different types of attacks. Ad-hoc On-Demand Distance Vector (AODV) routing protocol in MANETs which is vulnerable to a variety of security threats in ad-hoc networks. Black hole attack is an attack that drop considerable number of packet by performing packet forwarding misbehaviour and violate the security to cause Denial-of-Service (DoS) in Mobile Ad-hoc networks (MANET). In this paper we investigate different mechanism to detect and prevent black hole attack in AODV protocol. We also discuss about advantages and disadvantages of the methods.

**Keywords:-** MANETs, AODV, DoS Attacks, Black hole Attack.

## I. INTRODUCTION

An ad-hoc network is a group of wireless mobile nodes forming a network without the help of any stand-alone infrastructure. As Mobile Ad-hoc networks are self-organizing and self-configuring multi-hop wireless networks, the structure changes dynamically. This is mainly due to the mobile nodes. Nodes in these networks utilize the same random access wireless channel, cooperating in such a manner to engaging themselves in multi-hop fashion. The node in the network acts as both hosts as well as routers.

Each device in a MANET is free to move independently in any direction, and will therefore change its paths to other devices repeatedly. Each must forward traffic distinct to its use, and thus the router. Routing has been a challenging task for the ad-hoc network as there is the constant change in network topology because of high degree of mobile nodes. To accomplish this task number of protocols has been introduced.

AODV [8] is reactive routing protocol in MANET, which creates route from source to destination. In AODV source broadcast RREQ packet to its neighbours to find route to its destination. After receiving RREP from the neighbour‟s source select optimum route to its destination and sends data packets through it.

MANETs are liable to different active and passive attacks on the network layer. DoS attacks are the attacks that badly disrupt fundamental functionalities of an ad-hoc network. Wormhole attack, Sinkhole attack, Black hole attack are major DoS attacks in MANETs. Here we concentrate on Black hole attack that degrades performance of network by packet forwarding misbehaviour during data transmission phase.

In Black hole attack [9], the malicious node generates and propagates fictitious routing information and advertises itself as having a valid shortest route to the destination node. If the malicious node replies to the requesting node before the genuine node, a stale route will be created. As a result, packets do not reach to the specific destination node and the malicious node obstructs the packets and drops them. Thus, the network traffic is absorbed. In this paper, various mechanisms to detect and remove this attack is proposed on AODV based MANET.

The remaining of this paper is organized as follows. Section 2 explains AODV routing protocol, and also Black hole attack on AODV routing protocol. Section 3 describes the detection and prevention methods of Black hole attack. And last section is the conclusions.

## II. BACKGROUND

### A. Ad-hoc On-Demand Distance Vector (AODV) Routing

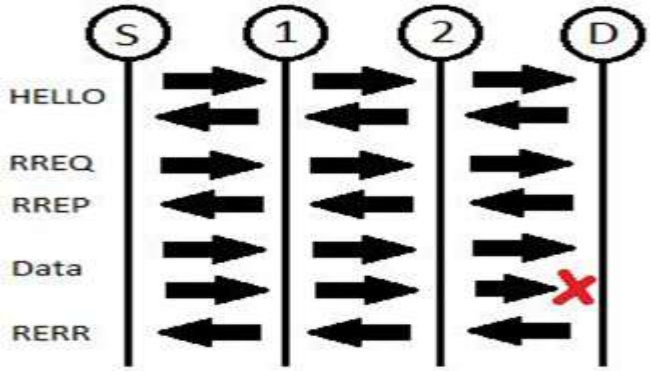


**Figure1. AODV Protocol Messaging**

The AODV [8] routing protocol is a reactive routing protocol; therefore, routes are discovered only when needed. Figure 1 shows the message exchange takes place in AODV protocol. Hello messages are used to detect and observe links to neighbours. By using Hello messages, each active node broadcast periodically a Hello message that all its neighbours accept. As nodes periodically send Hello messages, if a node fails to receive some Hello messages from a neighbour, a link break is found.

When a source has data to transmit to an unknown destination, it broadcasts a Route Request (RREQ) for that destination. At each intermediate node, when RREQ is received, a route to the source is generated. If the receiving node not received this RREQ before, it is not the destination and it does not have a current route to the destination, then it rebroadcasts the RREQ again. If the receiving node is the destination or has a current route to the destination, it generates a Route Reply (RREP). The RREP is unicast in a hop-by-hop fashion to the source. Each transitional node creates a route to the destination as the RREP propagates. Source records the route to the destination and can begin sending data when it receives the RREP. If source receives multiple RREPs, the route with shortest hop count should be chosen. As data is flowing from source to destination, each node along the route updates the timers related with the routes to the source and destination and maintains the routes in the routing table. If a route is not used for some specific time, a node cannot be persuaded whether the route is valid. As a result, the node removes the route from its routing table. If data is forwarding and a link break is detected, a Route Error (RERR) is sent to the source of the data in a hop-by-hop manner. As the RERR propagates towards the source, each intermediate node in validates routes to any unreachable destinations. When the source receives the RERR, it nullify the route and reinitiates route discovery if necessary.

### B. Black hole Attack on AODV Routing Protocol

In a Black hole attack [9], a malicious node sends fake routing information, claiming that it has an optimal route and causes other good quality nodes to route data packets through the malicious one. Source node considered it as a fresher path and then false route will be created. The effect generated is Black hole absorbs traffic and start to drop the data packet forwarded through it to destination.

In case of AODV, the attacker can send a fake RREP (including a fake destination sequence number that is to be equal or higher than the one contained in the RREQ) to the source node, claiming that it has a suitably fresh route to the destination node and causes the source node to choose the route that passes through the attacker. Thus, all traffic will be passed through the attacker, and therefore, the attacker can exploit or discard the traffic.

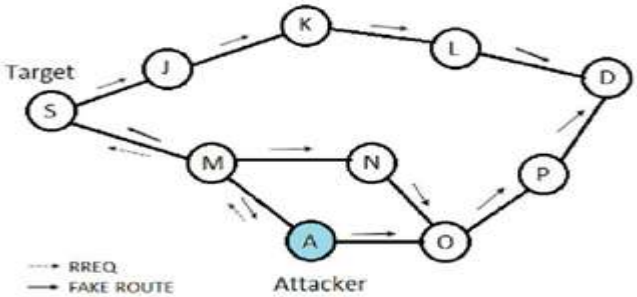


**Figure2. Example of a black hole attack**

Figure2 shows an example of a black hole attack, where attacker A sends a fake RREP to the source nodes, claiming that it has a suitable route than other nodes. Since the attacker‟s advertised sequence number is higher than other nodes‟ sequence numbers, the source node S will choose the route that passes through node A.

## III. OVERVIEW OF DETECTION AND PREVENTION METHOD

In this section, seven different methods for detection and removal of Black hole presented.

### A. Watchdog Method [1, 10]:

First method is watchdog timer. By using it, malicious node can be detected. Each node monitors its next node in the route. If it finds any packet forwarding misbehaviour or any packet dropping in a predefined period of time for its next node, it considers its next node as a malicious to the source.

**Advantages**

- As it is a simplest method, one node only monitors its next node in the route.

**Disadvantages**

- In this method, each node should always monitor its next neighbor nodes.
- Source node should trust the other node's information about one node's misbehavior.
- There is no predefined limit to differentiate malicious nodes and increases the numbers of mistakes to find black hole attack.

### B. Strong Node Method [2]:

Strong nodes are the additional nodes, which help source and destination to find black hole attack. These nodes are supposed to be trustful and also able to tuning its antenna to large ranges and short ranges. Each node is within the range of one of these strong nodes. With the help of these strong nodes, source and destination nodes start an end-to-end inspection and can recognize whether the data packets have reached the destination or not. If any differences found in number of messages sent from source and received at destination, strong nodes inquire the nodes in their areas regarding to monitoring results of one node‟s performance. If the inspection results show misbehaviour, then the backbone network runs a protocol which detects black hole attack. At the end announces malicious node to the network by broadcasting messages.

**Advantages**

- Strong nodes decrease the number of monitoring of neighbors, only nodes in particular area of malicious node start monitoring.

**Disadvantages**

- Differentiate between signal strength of strong and normal nodes in the network, makes this method unsuitable for MANET.
- This method assumes that strong nodes are trustable, but there is no solution given for attacks.
- There is no boundary for detection of maliciousness of node, so that mistakes to distinguish between normal and strong nodes increases.

### C. DRI Method [3,15]:

This method uses Data Routing Information (DRI) table for each node that has two fields called„ from‟ and „through‟. „From‟ means that from this node gets a routing message and „through‟ means that from current node sends a message to that node or not. In this first, source tries to discover a route from source to destination. Source sends RREQ packets to destination. If destination returns RREP, source trust its answer. If an intermediate node returns RREP, that node should also send its DRI table and ID of next node in the route to source. Node is trustable if source previously sent a message to that node and source starts sending data packets through that to destination. If source does not identify that node, it sends a packet to its next node and asks it for DRI table and also ID of its next node. The same process is done on the next node until source receives a DRI table of a trustable node and then stops this process and checks DRI table of both neighbour nodes to find maliciousness by checking „from‟ and „through‟ field of them. If source finds any differences in two neighbours‟ DRI tables announces all the nodes in the network regarding maliciousness.

**Advantages**

- This method can find any cooperative black hole attacks.

**Disadvantages**

- This method works very slowly if there is not any attack in the network and generates huge overhead for checking all nodes in a route.

**D. SCAN Method [4]:**

SCAN uses two ideas to protect AODV in MANET: Local collaboration and information cross-validation. In Local collaboration, nodes monitor each other and also maintain routing tables of each other. Each node uses a token that authenticates itself to the network. If one node is found to be malicious, another node revoke its token and alert token revocation to all other nodes in network and they insert that node in their token revocation list. So, the malicious node cannot access the network.

In Information cross-validation, each node checks routing packets comes from its neighbours nodes. Each node knows neighbour routing tables and they can cross-check the overheard transmissions of them. Figure1 shows this example, node M use routing tables of X and Y, if X or Y declares a new fault routing update, M equate routing tables of two neighbours and if any difference found, announces that node to be malicious and revokes its token.

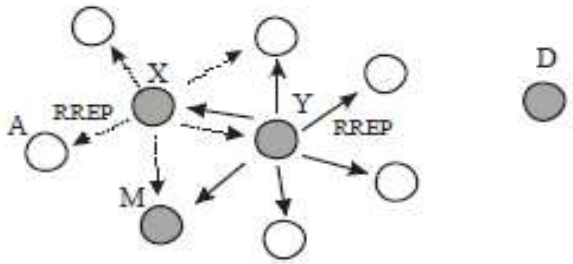


**Figure3. Cross-checking routing updates of neighbours**

**Advantages**

- Each node uses a token which authenticates the node to the entire network. Without a suitable token, a node cannot take part in the network and using token to some extend enhances the security of network.

**Disadvantages**

- Due to mobile nodes, routing table changes and mistakes in finding malicious nodes will be increased. Also this method needs renewal of Neighbors table entry in certain period of time.
- If there is no neighbor in the network that can cross-checks the route, this method fails.

**E. R-AODV Method [5]:**

Reliable-AODV (R-AODV) improves route discovery process of AODV by bringing in security into AODV protocol and prevents Black hole and Grayhole nodes from taking part in data transmission phase. when a malicious node is detected by an intermediate node after receiving RREP, R-AODV marks the RREP as DO_NOT_CONSIDER and marks the node sending RREP as MALICIOUS_NODE in the routing table; the RREP is then forwarded on the reverse path to the source which updates routing tables of all the nodes on the reverse path with malicious node entry; a route towards destination is chosen by selecting unmarked RREPs.

**Advantages**

- It helps to isolate multiple black hole and grey hole nodes.
- It provides simple and efficient way to detect and isolate multiple malicious nodes without introducing any control packet.
- It provides high packet delivery rate with noticeable normalized routing overhead and acceptable average ent-to-end delay under attack.
- This mechanism can be adopted by other reactive protocols also.

**Disadvantages**

- It increases routing overhead by forwarding RREP after detection of misbehavior.

**F. MR-AODV[6]:**

Modified Reliable-AODV (MR-AODV) used to detect and isolate multiple Black hole and Grayhole nodes during route discovery process to improve the performance of MANET. In MR-AODV, when a node detects a malicious node, it updates the routing table with malicious node entry and rejects the RREP. it is not forwarded on the reverse path and also not requires a DO_NOT_CONSIDER flag. Hence, all RREPs attaining to the source node will be sent by genuine nodes only; the RREP indicating shortest fresher path will be chosen for data transmission by the source node.

**Advantages**

- MR-AODV attempts to reduce routing overhead by not forwarding RREP after detection of misbehavior.
- MR-AODV isolates Black hole and Grayhole nodes during route discovery phase as R-AODV and sets up a secure route for data transmission.
- It attempts to further reduce normalized routing overhead by decreasing number of forwarded reply packets sent by adversaries.

**G. MOS AODV Method [7]:**

In Source Modified AODV (MOS AODV) proposed to prevent any alterations in the default operations of either the intermediate nodes or that of the destination nodes. The approach follows, basically only modifies the working of the source node. It stores all the RREPs in the newly created table viz. Cmg_RREP_Tab until the time, MOS_WAIT_TIME. Based on the assumption and initialize MOS_WAIT_TIME to be half the value of RREP_WAIT_TIME – the time for which source node waits for RREP control messages before regenerating RREQ. In this solution, the source node after receiving first RREP control message waits for MOS_WAIT_TIME. For this time, the source node will save all the coming RREP control messages in Cmg_RREP_Tab table.

Thus after receiving first RREP, the source node waits for a specific time period. For this period the source node saves all the received RREP message in a table; Source node discards all RREP having very high sequence number.

**Advantages**

- It increases PDR.
- It can trivially be extended for use by any other routing algorithm other than AODV.
- It is simple and efficient algorithm.

**Disadvantages**

- It increases average end-to-end delay and normalize routing overhead.
- It is heuristic approach.

## IV. CONCLUSION

Designing of most routing protocols are based on requirement of continuously changing topology of MANET, but security have been left unobserved. DoS attack breach the security of network and disrupt network operations. This paper provides security concerns for MANET. We introduced some of the proposed methods in detecting DoS attack like black hole with some of the advantages and disadvantages of it. Most of these algorithms suffer from overload and low speed, which is a research area for developing a detection system against black hole attack.

## REFERENCES


[1]. Marti, S., Giuli, T. J., Lai, K., and Baker, M. 2000. " Mitigating routing misbehavior in mobile ad hoc networks", In Proceedings of the 6th Annual International Conference on MOBICOM, Boston, Massachusetts, United States, 255-265.

[2]. Agrawal, P., Ghosh, R. K., and Das, S. K. 2008. "Cooperative black and gray hole attacks in mobile ad hoc networks". In Proceedings of the 2nd International Conference on Ubiquitous Information Management and Communication, Suwon, Korea, 310-314.

[3]. Ramaswamy, S., Fu, H., Sreekantaradhya, M., Dixon, j., and Nygard, K. 2003. "Prevention of cooperative black hole attack in wireless ad hoc networks". In Proceedings of the International Conference on Wireless Networks.

[4]. Yang, H., Shu, J., Meng, X., and Lu, S. 2006. SCAN: "Self-organized network-layer security in mobile ad hoc networks", J. IEEE Selected Areas in Comm. Vol. 24, No. 2 (Feb. 2006), 261-273.

[5]. RUTVIJ H. JHAVERI, SANKITA J. PATEL, DEVESH C. JINWALA, "Improving Route Discovery for AODV to Prevent Black hole and Grayhole Attacks in MANETs", INFOCOMP, v. 11, no. 1, p. 01-12, March-2012.

[6]. Rutvij H. Jhaveri, "MR-AODV : A solution to mitigate blackhoe and grayhole attacks in AODV based MANETs",

[7]. Third international conference on advance computing and communication technologies, 2013.

[8]. Nital Mistry, Devesh C Jinwala, Member, IAENG, Mukesh Zaveri : "Improving AODV Protocol against Black hole Attacks" In proceeding of International Multiconference of Engineering and

Computer Science, March 17, 2010.
[9]. Mahesh K. Marina, Samir R. Das, "Ad hoc on-demand multipath distance vector routing", wireless communications and mobile computing, John Wiley & Sons, Ltd., 2006
[10]. Rutvij H. Jhaveri, Sankita J. Patel and Devesh C. Jinwala, "DoS Attacks in Mobile Ad- hoc Networks: A Survey",
[11]. In Proc. of International Conference on Advanced Computing & Communication Technologies: Conference Publishing Services (CPS), January 2012, pp.535-541.
[12]. Surana K.A., Rathi S.B. Thosar T.P. and Snehal Mehatre, "Securing Black Hole Attack in Routing Protocol AODV in MANET with Watchdog Mechanisms", World Research Journal of Computer Architecture, Vol. 1 Issue
[13]. 1, 2012, pp. 19-23.
[14]. Akanksha Saini and Harish Kumar, "Comparison between Various Black Hole Detection Techniques in MANET", In Proc. of National Conference on Computational Instrumentation, March 2010, pp. 157-161.
[15]. Biswas, K., and Liakat Ali, M. D. 2007 "Security Threats in Mobile Ad Hoc Network". Master Thesis. Thesis no: MCS-2007:07. , Blekinge Institute of Technology.
[16]. Marjan K. R., Zahra Z. A., and shahla G., "Methods of Preventing and Detecting Black/Gray Hole Attacks on AODV-based MANET", IJCA Special issue on "Network Security and Cryptography", 2011.
[17]. C. Perkins, E. Royer, and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing," IETF, RFC 3561, 2003.
[18]. Hesiri W. and Huirong Fu, "Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks".
[19]. Simulation Implementation and Evaluation", International Journal of Software Engineering and Its Applications, Vol. 2, No. 3, July, 2008.