www.ijemr.net ISSN (ONLINE): 2250-0758, ISSN (PRINT): 2394-6962

Volume-7, Issue-3, May-June 2017

International Journal of Engineering and Management Research

Page Number: 72-75

# Removal of Black Hole Attack using AODV Protocol in MANET

Manisha Sood[1], Pooja Rani[2]

[1]Department of Computer Science & Engineering (USET) Rayat Bahra University, Mohali, INDIA

[2]Assistant Professor, Department of Computer Science & Engineering (USET) Rayat Bahra University, Mohali, INDIA

**ABSTRACT**

**This paper presents a review on a major category of coordinated attacks i.e. black hole attack which is a serious threat to ad ho c network security. In black hole attack multiple nodes collude to hide the malicious activity of other nodes; hence such attacks are more difficult to detect. In this paper a survey of various security mechanisms for removal of such attacks have been presented.**

***Keywords--*** Mobile Ad-hoc Networks, black hole attack, Routing protocols

## I. INTRODUCTION

Ad-hoc network is a collection of nodes that is connected through a wireless medium forming rapidly changing topologies. The infrastructure less and the dynamic nature of these networks demands new set of networking strategies to be implemented in order to provide efficient end-to-end communication. Mobile ad hoc networks (MANETs) [6] represent complex distributed systems that comprise wireless mobile nodes that can freely and dynamically self-organize into arbitrary and temporary network topologies, such type of networks are most vulnerable to various kinds of attacks. In the presence of security protocols effect of various attacks can be reduced.

## II. BLACKHOLE ATTACK

Black hole attack [1] is a kind of Denial of Service (DoS) attacks [1] in MANET. In this attack, a malicious node advertises that it has the best path to the destination node during the route discovery process. Whenever it receives the RREQ message, it immediately sends out a fake RREP to the source node. The source node first receives the RREP from the malicious node ahead of other RREPs. However, when the source node starts sending the data packet to the destination by using this route, the malicious node drops all packets instead of forwarding.

For example, let's consider the scenario in Figure 1. In this scenario, the node 'S' is the source node, 'D' is the destination node and 'M' is assumed the malicious node. When 'S' want to send the data packets to 'D', it starts the route discovery process by broadcasting RREQ message to the neighboring nodes. So, the node 'C', 'E' and 'F' receive this message. Since M is a malicious node, it immediately sends out a RREP message to 'S' with high sequence number. 'S' assumes that it is the freshest route, ignores all other RREPs and sends any packets to the destination over it. However, the node 'M' drops all data packets instead of sending to intended destination.

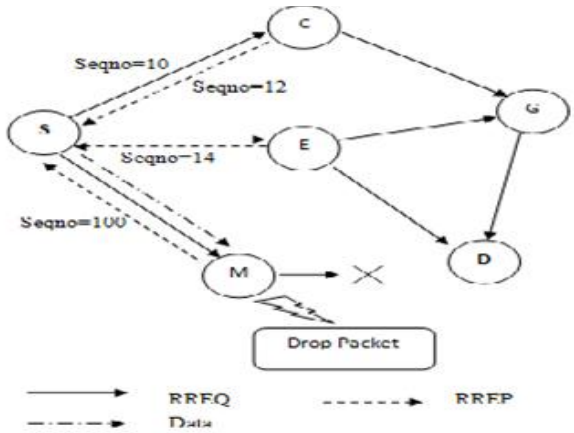


**Fig.1. Black Hole eg.[2]**

In the next section, various routing protocols used for the removal of black hole attack have been discussed

## III. ROUTING PROTCOLS

Routing protocols define a set of rules which governs the journey of message packets from source to destination in a network. In MANET, there are different

types of routing protocols each of them is applied according to the network circumstances

***A. PROACTIVE ROUTING PROTOCOLS***

Proactive routing protocols are also called as table driven routing protocols. In this each node maintain routing table which contains information about the network topology even without requiring it. The routing tables are updated periodically whenever the network topology changes[2].

There are various proactive routing protocols. Example: DSDV, OLSR, WRP etc.

***B. REACTIVE ROUTING PROTOCOLS***

Reactive routing protocol is also known as on demand routing protocol. In this type of protocol, route is discovered whenever it is needed. Nodes initiate route discovery when demanded.

There are various reactive routing protocols. Example: DSR, AODV, TORA and LMR[3].

This routing protocol has two major components:

*1) Route discovery*- In this phase source node initiates route discovery on demand basis.

*2) Route maintenance*- Due to dynamic topology of the network cases of the route failure between the nodes arises due to link breakage etc, so route ma intendance is required.

***C. HYBRID ROUTING PROTOCOL***

This protocol is a combination of both proactive and reactive routing protocol. It uses the on demand mechanism of reactive protocol and the table maintenance mechanism of proactive protocol[3] so as to avoid latency and overhead problems in the network.

There are various hybrid routing protocols for MANET like ZRP, SHRP etc.

## IV. AD HOC ON-DEMAND DISTANCE VECTOR ROUTING (AODV) PROTOCOL

AODV protocol is a reactive unicast routing protocol for mobile ad hoc networks. As a reactive routing protocol, AODV only needs to maintain the routing information about the active paths.

AODV defines three types of control messages for route maintenance[2]:

*A. RREQ* - A *route request* message is transmitted by a node requiring a route to a node.

Every RREQ carries a *time to live* (TTL) value that states for how many hops this message should be forwarded. Retransmissions occur if no replies are received.

Data packets waiting to be transmitted(i.e. the packets that initiated the RREQ) *should* be buffered locally and transmitted by a FIFO principal when a route is set.

*B. RREP* - A *route reply* message is unicasted back to the originator of a RREQ if the receiver is either the node using the requested address, or it has a valid route to the requested address. The reason one can unicast the message back, is that every route forwarding a RREQ caches a route back to the originator.

*C. RERR* - Nodes monitor the link status of next hops in active routes. When a link breakage in an active route is detected, a RERR message is used to notify other nodes of the loss of the link. In order to enable this reporting mechanism, each node keeps a ``precursor list", containing the IP address for each its neighbors that are likely to use it as a next hop towards each destination.

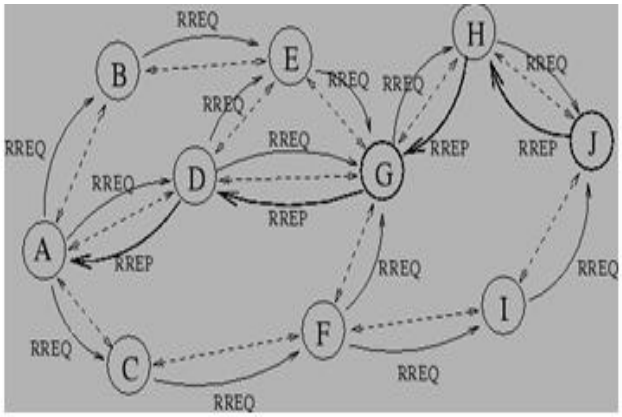


**Fig.2. Working of AODV[7]**

Figure illustrates an AODV route lookup session. Node A wishes to initiate traffic to node J for which it has no route. A broadcasts a RREQ which is flooded to all nodes in the network. When this request is forwarded to J from H, J generates a RREP. This RREP is then unicasted back to A using the cached entries in nodes H, G and D.

## V. RELATED WORK

A. S.AMUTHA and KANNAN BALASUBRAMANIAN proposed NOVEL ALGORITHM has two steps:

- Checking the difference between the sequence number of source and destination node.
- Passing the packets in secure routing.

If the first route reply will be from the malicious node with high destination sequence number, then that is stored as the first entry in the RR-Table[4]. Compare the first destination sequence number with the source node sequence number, if there exists much more differences between them, surely that node is the malicious node, immediately remove that entry from the RR-Table.

B. S.DOKURER proposed IDSAODV[5] this method modified in AODV protocol that implemented to minimize the effect of malicious node. This method implemented by modified in the routing update mechanism in AODV protocol. IDSAODV tries to eliminate the effect of the Black hole attack by ignoring the first route in the routing update process.

- The first RREP message arrived with shortest route to the destination node from the malicious node.
- IDSAODV switched to the second route, The Black hole node increasing the **data loss** to 89% when used IDSAODV decreased the data loss to 67% this solution reduce the **Black effect** by 22% as packet loss.

C. N. Khemariya proposed DPRAODV [6] method that based authenticate the RREP sequence number. RREP_seq_no is higher than the threshold value. Threshold value is dynamically updated.

- If the value of RREP_seq_no is found to be higher than the threshold value, the node is suspected to be malicious and it adds the node to the black list.
- It sends a new control packet, ALARM to its neighbors. The neighboring nodes know that RREP packet from the node is to be discarded. It simply ignores the node and does not receive reply from that node again.

D. ANKITA CHATURVEDI, SANJIV SHARMA[1] proposed IIDSAODV[5] is based on checking the second RREP message and uses the sequence number is a 32 bit unsigned integer the Highest value (HSN).

- Checking second RREP, the difference between the broadcasted and received destination sequence number is calculated and compared to the half of the highest possible sequence number (HSN).
- The difference should be less than or equal to (HSN/2). If second RREP pass then only the source node switches to this path. If checked fails the source node continue to send the data through the path by first RREP.
- In Black hole decrease the **PDR** of AODV by 83.79%, in case IDSAODV and IIDSAODV increase by 40.41% and 78.16%. Decrease **throughput** of AODV by 77.86%, in case IDSAODV and IIDSAODV increase by 20.66% and 73.59%. Decrease **end-to-end delay** of AODV by 88.74%, in case IDSAODV and IIDSAODV increase by 44.15% and 71.61%.

E. C.E Perkins and E.M Royer proposed EVM ENCRYPTION VERIFICATION METHOD[4] reduces the multiple Black Hole nodes effectively by employing an encryption mechanism.

- Identify and verify of the suspicious node using an encrypted verification message. The messages or the sequence numbers contained in the messages cannot be modified by any malicious.
- EVM can reduce control overhead and increase the detection rate considerably compared to the SNV.

F. B.Sun et al. proposed a neighbor set based approach to detect Black hole attack and a routing recovery protocol to recover from the effect of black hole attacks.

- In detection phase collect neighbor set information and determine whether there exists a black hole attack.
- In response phase a routing recovery protocol is used to build the correct path to the destination.
- The packet throughput can be improved by least 15% and the false positive probability is usually less than 1.7%.

| Approaches Used | Author | Through put | End-End Dela y | Dat a Los s | Overhe ad |
|---|---|---|---|---|---|
| 1. NOVEL ALGORIT HM | S. Amutha and Kannan Balasubrama nian | Decrease s | ------- -- | Less | Low |
| 2. IDSAODV | S.Dokurer | Increases | More | Hig h | High |
| 3. DPRAOD V | N. Khemariya | Decrease s | Less | ----- -- | Low |
| 4. IIDSAOD V | Ankita Chaturvedi, Sanjiv Sharma | Increases | More | Hig h | High |
| 5. EVM | C.E Perkins and E.M Royer | No effect | More | Hig h | ------- |
| 6. NS2 | B.Sun | Increases | ------- - | Less | High |

**Table I. Comparison of AODV approaches**

## V. FUTURE SCOPE

In this paper we have reviewed the AODV protocol and Black hole attack in MANETs. We have discussed feasible solutions for the black hole attacks that can be implemented on the AODV protocol. The Proposed method can be used to find the secured routes and prevent the black hole nodes in the MANET. As future work, we intend to develop simulations to analyze the performance of the proposed solution based on the various security parameters like packet delivery ratio (PDR), mean delay time, packet overhead, memory usage, mobility, increasing number of malicious node, increasing number of nodes and scope of the black hole nodes.

## REFERENCES

[1] Manjeet Singh and Gaganpreet Kaur, *A Surveys of Attacks in MANET*, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 6, June 2015 ISSN: 2277 128X.

[2] Ei Ei Khin and Thandar Phyu, *Impact Of Black Hole Attack On Aodv Routing Protocol*, International Journal of Information Technology, Modeling and Computing (IJITMC) Vol. 2, No.2, May 2014.

[3] Payal N. Raj and Prashant B. Swadas, *DPRAODV: A Dyanamic Learning System Against Blackhole Attack In Aodv Based Manet*, International Journal of Computer Science Issues, Vol. 2, 2009 ISSN 1694-0784.
[4] Sathya M and Priyadharshini M, *Detection And Removal Of Black Hole Attack In Mobile Ad-Hoc Networks Using Cooperative Bait Detection Method Scheme*, International Journal of Scientific & Engineering Research, Volume 7, Issue 3, March-2016 ISSN 2229-5518.
[5] Ajesha Patel and Anurag Jain, *Modified IDS-AODV for prevention of black hole attacks in MANIT*, International Journal of Scientific & Engineering Research, Volume 6, Issue 12, December-2015 432 ISSN 2229-5518 IJSER © 2015.
[6] Gurnam Singh and Gursewak Singh, *Detection and Prevention Of Black Hole Using Clustering In MANET Using Ns2*, International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume - 3 Issue -8 August, 2014 Page No. 7420-7430.
[7] https://en.wikipedia.org/wiki/Mobile_ad_hoc_network