INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

*WINGS TO YOUR THOUGHTS…..*

# MITIGATING BLACKHOLE ATTACK IN ROUTING AODV PROTOCOL

**Poonam Rani[1] Jasbeer Narwal[2]**

[1] M.Tech Scholar, Dept.of CSE, Haryana Engineering College, Jagadhri, India. poonamsaini222@gmail.com
[2]Lecturar, CSE Deptt., Haryana Engineering College, Jagadhri, India, jasbeernarwal@gmail.com

***Abstract:*** *The main idea behind this method is to list out the set of malicious nodes locally at each node whenever they act as a source node. As mentioned in the Assumption our protocol uses the concept of Core Maintenance of the Allocation Table i.e., whenever a new node joins the network, it sends a broadcast message as a request for IP address. The backbone node on receiving this message randomly selects one of the free IP addresses. The new node on receiving the allotted IP address sends an acknowledgement to the BBN. Now since the allocation is only under the control of the Back Bone Nodes(BBN) the dynamic pool of unused/restricted IPs of the network at any point of time is known only to the BBN.*

***Keywords:*** *MANET, BLACKHOLE DETECTION, ROUTING, AD HOC.*

## 1. INTRODUCTION

Wireless network is the network of mobile computer nodes or stations that are not physically wired. The main advantage of this wireless network is communicating with rest of the world while being mobile. The disadvantage is their limited bandwidth, memory, processing capability and open medium. Two necessary system models are fixed backbone wireless system and Wireless Mobile Ad hoc Network (MANET). An ad hoc network is a collection of nodes that do not rely on a predefined infrastructure to keep the network connected. So the implementations of Ad-hoc networks are dependent on the trust and co-operation between nodes. Nodes help each other in passing on information about the topology of the network & share the responsibility of organization the network. Hence in addition to performing as hosts, each mobile node does the role of routing and relaying messages for other mobile nodes. Most important networking operations include routing and network management. Routing protocols can be divided into the proactive, reactive and hybrid protocols, depends upon the routing topology.

Proactive protocol is typically table-driven. Examples of this type include DSDV and WRP. Reactive or source-initiated on-demand protocols, in opposing, do not periodically renew the routing information. It is propagate to the nodes only when essential. Example of this type includes DSR, AODV and ABR. Hybrid protocol make use of both reactive and proactive approaches. Example of this type includes TORA & ZRP. Security is a major concern in all forms of communication networks, but ad hoc networks face the greatest challenge due to their inherent nature. so, there exist a slew of attacks that can be performed on an Ad hoc network.

### *1.1. AODV Routing Protocols*

***1.1.1. The AODV protocol:*** The Ad Hoc On-Demand Distance Vector (AODV) routing protocol is an adaptation of the DSDV protocol for dynamic link situation. Every node in an Ad-hoc network maintains a routing table, which contain information about the route to a exacting destination. Whenever a packet is to be sent by a node and it first checks with its routing table to determine whether a route to the destination is already presented. If so then it uses that route to send the packets to the destination. If a route is not presented or the previously entered route is in activate, then the node initiates a route discovery process. A RREQ (Route REQuest) packet is broadcasted through the node. Every node that receives the RREQ packet first check if it is the destination for that packet and if so, it send back an RREP (Route Reply) packet. If it is not the destination, then it check with its routing table to determine if it has got a route to the destination. If not, it relay the RREQ packet by broadcasting it to its neighbors. If its routing table does include an entry to the destination, then the next steps are the comparison of the 'Destination Sequence' number in its routing table to that present in the RREQ packet. This Destination Sequence number is the sequence number of the last sent packet from the destination to the source. If the destination series number present in the routing table is smaller than or equal to the one contained in the RREQ packet, then the node relays the request more to its neighbors. If the number in the routing table is superior to the number in the packet, it denotes that the route is a 'fresh route' and packets can be sent through this route. This intermediate node can be sending a RREP packet to the node through which it receives the RREQ packet. The RREP packet get relay back to the source through the reverse route. The source node then updates its routing table and sends its packet through this route. Throughout the operation, if any node identifies a link failure it sends a RERR (Route ERRor) packet to all other nodes that uses this link for

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS…..

their communication to other nodes. While AODV has no security mechanisms, selfish nodes can perform many attacks just by not behaving according to the AODV rules. A selfish node *M* can carry out many attacks against AODV. In this paper provides routing security to the AODV routing protocol by eliminating the threat of 'Black Hole' attacks [1]

### *1.2 Black hole attack*

Routing protocols are exposed to a number of attacks. Black hole attack is one such attack and a kind of Denial Of Service (DoS) in which a selfish node makes use of the vulnerabilities of the route discovery packets of the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. This attack aim at modifying the routing protocol so that traffic flows through a specific node controlled by the attacker. Throughout the Route Discovery procedure the source node sends RREQ packets to the intermediate nodes to find fresh path to the intended destination. Selfish nodes respond instantly to the source node as these nodes do not refer the routing table. The source node assumes that the route discovery process is complete, ignores other RREP messages from other nodes and selects the path through the selfish node to route the data packets. The selfish node does this by assigning a high sequence number to the reply packet. The tracker now drops the received messages instead of relaying them as the protocol requires. In AODV, Dst Seq is used to determine the freshness of routing information contained in the message from originated node. When generate a RREP message, a destination node compare its current sequence number & Dst Seq in the RREQ packet plus one, and then choose the larger one as RREP's Dst Seq. On receiving a number of RREP, a source node selects the one with greatest Dst Seq in order to build a route. To succeed in the blackhole attack the attacker must generate its RREP with Dst Seq greater than the Dst Seq of the destination node. It is feasible for the attacker to find out Dst Seq of the destination node from the RREQ packet. In common, the attacker can set the value of its RREP's Dst Seq base on the received RREQ's Dst Seq. though, this RREQ's Dst Seq may not present the current Dst Seq of the destination node [7].

## 2. LITERATURE REVIEW

Latha Tamilselvan et. al. [1] An ad hoc network is a collection of mobile nodes that dynamically form a temporary network. It operates not including the use of existing infrastructure. One of the principal routing protocols used in Ad-Hoc networks is AODV (Ad-Hoc On demand Distance Vector) protocol. The security of the AODV protocol is compromise by a particular type of attack called 'Black Hole' attack. In this attack a selfish node advertise itself as having the shortest path to the node whose packets it wants to intercept. To decrease the probability it is proposed to wait and check the reply from all the neighboring nodes to find a secure route. Computer simulation using GLOMOSIM shows that our protocol provides better performance than the conventional AODV in the presence of Black holes with minimal additional delay and Overhead.

Govind Sharma et. al. [2] Mobile Ad-hoc network (MANET) has happen to an individual part for communication for mobile device. Then, interest in research of Mobile Ad-hoc network has been rising since last few years. Due to the open medium, dynamic network topology, independent terminal, lack of centralized monitoring and lack of management point. Mobile Ad-hoc network is highly vulnerable to security attacks compared to wired network or infrastructure-based wireless network. According to this paper, they analyze the black hole attack. In this attack, a selfish node incorrectly advertise shortest path to the destination node. The intension of selfish node could be to intercept all data packets being sent to the destination node concerned.

Tarandeep Kaur et. al. [3] Mobile Ad hoc networks (MANET) are collection of wireless nodes that communicate with each other with the help of wireless links. MANET is vulnerable to various attacks due to its feature open medium, dynamic topology, no central authority and no clear defense mechanism. One of the attacks is black hole attack in which a selfish node intercepts the packets being transmitted to another node in the network. As the data packets do not reach the destination, Data loss occurs which affect the performance of network badly. Our aim of the paper is to analyze the impact of the Black hole attack on MANET performance and how it affect the different performance metrics of the network by comparing the network performance with and without black hole nodes.

Vipin Khandelwal et. al. [4] Causing packet loss due to attacks by selfish nodes is one of the most essential problem in MANETs. There are many ways by which packet loss can occur in MANETs such as broken links, transmission errors, no route to the destination and attacks caused by selfish nodes. To find out the exact cause of packet loss in wireless network is a difficult task. According to this paper, they have investigated packet loss problem caused by a selfish nodes that performs the famous attack called Black Hole attack in the network. To moderate the effects of such attack, in this paper they have also proposed a detection technique that efficiently detects the malicious nodes in the network. they have done simulations using NS-3 simulator. Black Hole attack is also called sequence number attack because it is created using and modifying sequence number field in routing control packets.

Harmandeep Singh et. al. [5] MANET Routing protocols suffer from various kinds of attacks on all the layers of its protocol stack. One of such attack which occurs at the network layer is Black Hole attack and the aim of this paper is to analyze the affect of Black Hole Attack under three various categories of MANETs Routing Protocol i.e. Reactive, Proactive and Hybrid namely as AODV, OLSR and ZRP. They have analyzed the performance degradation on these above mentioned protocols the performance evaluations of metrics chosen are throughput, end to end delay when a percentage of nodes misbehave.

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

*WINGS TO YOUR THOUGHTS…..*

Monika Y. Dangore et. al. [6] A mobile ad-hoc network (MANET) is a self-configuring infrastructure less network of mobile devices. Each must onward traffic unrelated to its own use, and so be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. AODV (Ad-hoc On-demand Distance Vector) is a loop-free routing protocol for ad-hoc networks. It is designed to be self-starting in an environment of mobile nodes, withstanding a variety of network behaviours such as node mobility, link failures etc.

Rahul Sharma et. al. [7] Security is a necessary requirement in mobile ad hoc networks to provide protected communication between mobile nodes. MANETs are vulnerable to different attacks; black hole is one of the possible attacks. Black hole is a type of routing attack where a selfish node advertise itself as having the shortest path to all nodes in the surroundings by sending fake route reply. They attempt to focus on analysing and improving the security of one of the popular routing protocol for MANETS viz. the Ad hoc On Demand Distance Vector (AODV) routing protocol. Their focus particularly, is on ensuring the security against the Black hole Attacks. They propose modifications to the AODV protocol & validate the solution with appropriate implementation.

Arnab Mitra et. al. [8] This research work reports on active & Black Hole node detection if it exists in any Mobile ad hoc networks (MANETs). The dynamic topology of MANETs allows nodes to join & leave the network at any time instance. This common characteristic of MANET has showing to major security attacks including existence of black hole nodes, which adversely affects the entire routing practice. To deal with this routing mess, they have proposed an Artificial Neural Network (ANN) based automatic Black Hole node detection tactic, which is capable of detecting the existence of Black hole node(s) in the MANET and thus helps to reduce the smash up in reliable routing procedure.

## 3. PROPOSED WORK

Black hole attack is dangerous active attacks on the Mobile Ad hoc Networks. A black hole attack is performed by a single node or combination of nodes. This attacker node is also called selfish node.

The main objectives of my research are:-

[1] To develop a scheme/protocol to detect and prevent black hole node in MANET.

[2] Comparison of proposed hybrid detection technique with others.

## 4. SOLUTION TO BLACKHOLE ATTACK-MAODV

### *4.1. Working principle of MAODV*

***Actions by Source Node (SN)***

Step 1: Source Node (SN) sends a Request to Restricted IP(RRIP) to the Back Bone Node(BBN).

Step 2: On receiving the Restricted IP(RIP), from the BBN it sends the RREQ for the Destination as well as for the RIP simultaneously.

Step 3: Waits for RREP.

**Actions by Intermediate Node/Destination Node**

Step 1: On receiving the RREQ it first makes an entry in its Routing table for the node that forwarded the RREQ.

Step 2: If it is the Destination node or if it has a fresh enough route to the Destination node, it replies to the RREQ with an RREP.

Step 3: If it is neither the destination nor does it have a fresh enough route to the Destination, then it forwards the RREQ to its neighbours.

Step 4: On receiving an RREP, it again makes a note of the node that sent the RREQ in its routing table & then forwards the RREP in the reverse direction.

Step5: On receiving a request to enter into the promiscuous mode, it starts listening in the network for all the packets destined to that particular IP address & monitors its neighbors, for the movement of the dummy data packet.

Step6: In case, it finds out that the dummy data packet loss is exceptionally more than the normal data packet at any particular node, it informs back the IP of this IN.

Step7: we create a blacklist for black hole node, So that they can't participate in the route discovery again.

We propose a solution that is an enhancement of the basic AODV routing protocol, which will be able to avoid black holes. To reduce the probability it is proposed to wait and check the replies from all the neighboring nodes to find a safe route. According to this proposed solution the requesting node without sending the DATA packets to the reply node at once, it has to wait till other replies with next hop details from the other neighboring nodes. After receiving the first request it sets timer in the 'TimerExpiredTable', for collecting the further requests from different nodes. It will store the 'sequence number', and the time at which the packet arrives, in a 'Collect Route Reply Table' (CRRT). The time for which every node will wait is proportional to its distance from the source. It calculates the 'timeout' value based on arriving time of the first route request.

## 5. SIMULATION RESULTS

The simulation is done using ns2 simulator, to analyze the performance of the network by varying the nodes mobility. We are using 4 nodes in transmission and checkout the packet delivery between the nodes. After that compare the packets received in AODV with the packets received in MAODV. we also compare the end to end delay in packet received in AODV and end to end delay in packet received in MAODV protocol. With the help of table 1, fig.1, table 2 and fig.2 we can compare the results of AODV and MAODV.

### *5.1 Comparison of basic AODV with MAODV*

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

**Table 1:** Packets received in 10 seconds using 4 nodes

| Simulation time=10 seconds 4 nodes | | |
|---|---|---|
| Simulation time | AODV packet received | MAODV packet received |
| 2 | 38 | 2 |
| 4 | 52 | 4 |
| 6 | 85 | 68 |
| 8 | 127 | 261 |
| 10 | 170 | 351 |

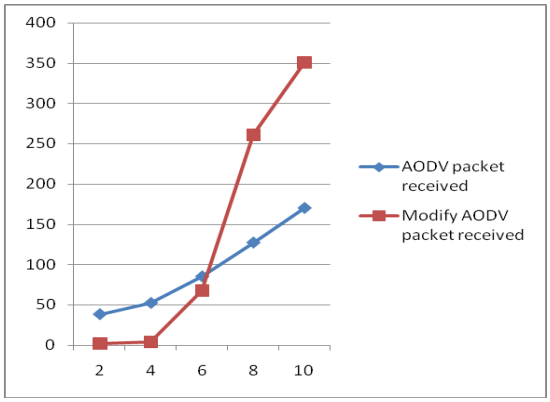


**Figure 1:** Packets received in 10 seconds using 4 nodes

**Table 2:** Delay in packet received in 10 seconds using 4 nodes

| Simulation time=10 seconds end to end delay 4 nodes | | |
|---|---|---|
| Simulation time | AODV packet received | MAODV packet received |
| 2 | 5 | 0 |
| 4 | 7 | 1 |
| 6 | 45 | 45 |
| 8 | 162 | 92 |
| 10 | 289 | 140 |

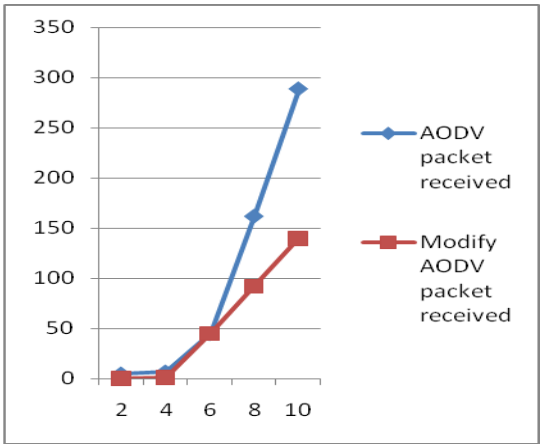


**Figure 2:** Delay in packets received in 10 seconds using 4 nodes

## 6. CONCLUSION

Black hole attack is the most important security problems in MANET. Black hole starts in route discovery phase. In proposed work focuses on detecting black hole attack, pointed out their advantages and disadvantages and at the end. Protection against black hole attack in one detection system and decreasing number of errors is the main motive. It is observed that the Black Hole effect the AODV protocol, also effect on packet loss is much lower as compare to effect on delay. As malicious node is the main security threat that effect the performance of the AODV routing protocol & their detection is the main matter of concern. Improvement for overcoming the effect of Black Hole should orient towards controlling the delay. MAODV works very well to overcoming the effect of Black hole.

## REFERENCES

**[1] Latha Tamilselvan and Dr. V Sankaranarayanan, "Prevention of Blackhole Attack in MANET" The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications (AusWireless 2007) 0-7695-2842-2/07 $25.00 © 2007**

**[2] Govind Sharma and Manish Gupta, "Black Hole Detection in MANET Using AODV Routing Protocol" International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-1, Issue-6, Jan. 2012**

**[3] Tarandeep Kaur and Amarvir Singh, "Performance Evaluation of MANET with Black Hole Attack Using Routing Protocols" International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 Vol. 3, Issue 4, Jul-Aug 2013, pp.1324-1328**

**[4] Vipin Khandelwal and Dinesh Goyal, "Black Hole Attack and Detection Method for AODV Routing Protocol in MANETs" International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 4, April 2013**

**[5] Harmandeep Singh and Manpreeet Singh, "Effect of Black Hole Attack on AODV, OLSR and ZRP Protocol in MANETs" International journal of advanced trends in computer science and engineering Volume 2, No.3, May - June 2013**

**[6] Ms Monika Y. Dangore, Mr Santosh S. Sambare, "A Survey on Detection of Blackhole Attack using AODV Protocol in MANET" International Journal on Recent and Innovation Trends in Computing and Communication ISSN 2321 – 8169 Volume: 1 Issue: 1**

**[7] Rahul Sharm1, Naveen Dahiya and Divya Upadhyay, "An Analysis for Black Hole Attack in AODV Protocol and Its Solution" IJCSMC, Vol. 2, Issue. 4, April 2013, pg.391 – 395**

**[8] Arnab Mitra, Rajib Ghosh, Apurba Chakraborty and Debleena Srivastva, "An Alternative Approach to Detect Presence of Black Hole Nodes in Mobile Ad-Hoc Network Using Artificial Neural Network" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 3, March 2013.**