# A Reaction Based Approach to Detect Black Hole Attack using Modified AODV Protocol in MANETS

***Geeta Pattun***
*Assistant Professor*
*Dept of Computer Science and Engg*
*Vasavi College of Engineering*
*(Affiliated to OU, Hyderabad)*
*Ibrahimbagh -500031*
*Email:geeta6685@gmail.com*

***V.Sireesha***
*Assistant Professor*
*Dept. of Computer science and Eng*
*Vasavi College of Engineering*
*(Affiliated to OU, Hyderabad)*
*Ibrahimbagh-500031*
*Email: sireesha.vikkurty@gmail.com*

**ABSTRACT**

***Mobile Ad-hoc Networks (MANETS) are group of mobile devices that are connected through wireless links without any fixed infrastructure. Providing a secure routing of data in MANETS is a challenging issue. MANETS suffers from variety of attacks. Among them Black Hole Attack is one of the serious active attack network would suffer from. To defend against the Black Hole Attack this paper has proposed a new method "A Reaction Based Approach to Detect Black Hole Attack using Modified AODV Protocol in MANETS ". This method is based on examination of Immediate Response Time, late response Time taken by the nodes to send control reply packet (RREP) in response to RREQ and the comparison of minimum and maximum Response Time shared by immediate neighbour of source and replier node. This method can be implemented by including control packets to the existing AODV protocol. NS2(Network Simulator) can be employed to witness the network performance with the application of proposed method and to analyze the QOS (quality of services) of network like Packet Delivery Ratio (PDR) and Packet Drop.***

**KEYWORDS**

***AODV Protocol, Black Hole Attack, Route Discovery, Attacks in MANETs***

## I – INTRODUCTION

A Mobile Ad-hoc network [1][9][5] are self configuring networks in which the mobile nodes depends on the intermediate nodes to establish multi hop communication without the fixed infrastructure. These Ad-hoc networks are so flexible that the mobile node can join and leave a network at any point of time but this flexibility of mobility would result in dynamic topology, as a result developing secure ad-hoc routing protocols are quite challenging. The MANETS are vulnerable due to their basic characteristic [1][3] such as the **open medium** where in any node can join and leave the network due to its mobility nature , the **absence of the fixed infrastructure** as the topology of such networks changes as the nodes move out of the range of network access, **absence of centralized administration** as the network fails to fix one particular node as the centralized authority to administrate the data transfer within the Ad-hoc Network ,**limited(or constrained) bandwidth** being shared among the heterogeneous mobile devices and **battery energy constraints** being one of issue related to the mobile devices in MANETS which decides how long the devices can participate in network communication.

The design of secure routing protocol [4] must ensure both connectivity and security of the route being discovered.

The paper is organized in the following way with the section – II describes the categories of attacks in MANETs and followed by their detailed description. Section –III describes the working of the AODV protocol. Section – IV describes the Black Hole Attacks in detail. Section – V exploring the counter measures to defend the Black Hole Attack in MANETs. Section – VI deals with the proposed solution for defending against the Black Hole Attack in MANETs. Section

–VI describes various network performance matrices required to test network behaviours

-VII conclusion of the paper.

## II - ATTACKS IN MANETS

As discussed in papers [4] that based on the behaviour of attacker node either to disrupt the operations of the routing protocol or not the attacks in MANETS can be divided into 2 categories(Active Attacks and Passive Attacks).

**Wormhole Attack:** It is a passive attack where in an attacker node would be recording the packets at one location in the network and then later tunnels them to another route. Routing can be disrupted when routing control messages are tunneled. This tunnel between two colluding attackers is referred as a wormhole.

**Byzantine attack:** A compromised intermediate node works alone, or a set of compromised intermediate nodes works in collusion and carry out attacks such as creating routing loops, forwarding packets through non-optimal paths, or selectively dropping packets, which results in disruption or degradation of the routing services.

**Denial of Service attack:** It is an active Attack it aims to attack the availability of a node or the entire network by sending invalid messages frequently to paralyze node. The attacker node generally uses radio signal jamming and the battery exhaustion method. This attack does not aim to change the network topology instead to disrupt the network functionality and communication.

**Impersonation:** It is an Active if authentication mechanism is not properly implemented a malicious node can act as a genuine node and can monitor the network traffic. It can also send fake routing packets, and gain access to some confidential information.

**Eavesdropping:** This is a passive attack were in the malicious node simply observes the confidential information and These confidential information like location, public key, private key, password etc. can be fetched by eavesdropper can be used by the malicious node for its evil purpose.

**Routing Attacks:** It is basically targets the reactive protocol were in such protocols suggest node to rebroadcast only first received request and ignores others requests, this feature of the protocol are take up cruelly by malicious node by flooding the network with its route request packet in network so that attacker can take up the route discovery process in to its control.

## III - WORKING OF AODV PROTOCOL

AODV (On Demand Distance Vector) [1][4][5][6]protocol is one of the most common ad-hoc routing protocol used in mobile ad-hoc networks. This discovers route only on demand from nodes within the network. A mobile node that wishes to communicate with other node in the network. It starts with route discovery process.

**This involves the following steps**

1)It broadcasts an RREQ (Route Request Packets)control packet to discover a fresh route to an intended destination node to all its neighbours.

2) On receiving RREQ packet every neighbouring node first saves the path the RREQ has transmitted from its source in its routing table.

3) This neighbour node spontaneously checks its routing table to find whether it has a fresh route entry to the destination node as mentioned in the RREQ packet. The freshness of a route is generally indicated by a destination sequence number that is attached to it.

4) If a intermediate node finds a fresh enough route, then it uncast a RREP packet (Route Reply) back along the saved path to the source node or it re-broadcasts the RREQ message otherwise.

5) The same process continues until an RREP message from the destination node or an intermediate node that has fresh route to the destination node is received by the source node. **Note**: A routing table entry maintaining a reverse path is purged after a **timeout interval.** A routing table entry maintaining a forward path is purged if *not used* for a **Active_Route_Timeout** interval.

### Linkfailure

A neighbour of node X is considered active for a routing table entry if the neighbour sent a packet within *active_route_timeout* interval which was forwarded using that entry. In order to test availability of node in network neighboring nodes periodically exchange hello message. When the next hop link in a routing table entry breaks, all active neighbours are informed by propagating Route Error (RERR) messages, which also update destination sequence numbers.

## IV - BLACK HOLE ATTACK

It is an Active attack ,it causes attack in 2 steps

1) Exploiting AODV[10][11][12], by advertise itself to have a valid shortest route to a destination node, with an intention of intercepting packets.

2) By consuming the intercepted packets without forwarding them.

However, the attacker node take the risk of getting exposed by the neighbour node about ongoing attacks though it is under continuous monitoring.

According to the authors of [7][4][5] the black hole attack is planted by malicious behaving node for example Node 4 in figure 1,which sends the RREP to source node 1 with higher destination sequence number ahead from the rest of the other intermediate node or destination

.

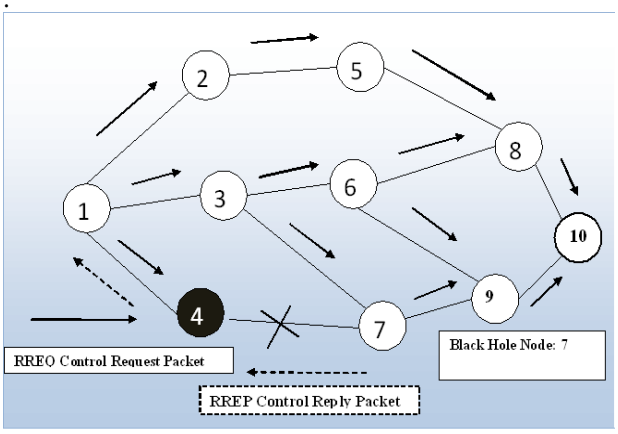

**Figure 1**, describes the scenario of black hole being injected by the malicious node 4 in MANETS by disrupting AODV protocol.

Characteristic of AODV make Node 1 to believe that the first RREP received (from node 4) is the shortest and up-to-date path to destination node 10. As a result, node 1 updates its routing table by taking node 4 as its next hop to send data to node 10. As described in figure 2, The data packets are forwarded to node 4, then it's up to the node 4 to either keep or drops the packet without forwarding it to the destination node 10 as if the packet is disappeared in a black hole as the name of attack implies. Black Hole Attack in MANETs is a serious security problem to be solved.

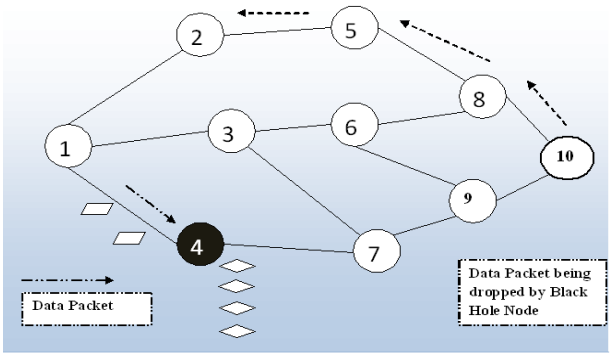


***Figure 2:*** *Packet being dropped by malicious node 4*

## V - RELATED WORK

**Anomaly Detection on MANETS**

According to IDAD system [1] particular node are isolated from further interaction. Implementation of IDAD system has many disadvantages like need to maintain activities of all the nodes ,need to update audit data frequently, no clear separation between normalcy and anomaly..

**Authentication based mechanism:**

The author of [5] has suggested symmetric cryptosystem to be adapted by all nodes i.e $M=D_{Ki}(E_{Ki}(M))$where $E_{ki}$ and $D_{Ki}$ encryption and decryption functions respectively. This mechanism suffers from MAC being forged during the transmission and chances of key getting disclosed before receiving the packet.

**ERDA based Mechanism:**

According to the author of [7] heuristic method is used for identifying the node with exceptionally high destination sequence number and those nodes are added to the MALI_LISTS & such nodes are exempted from participating in route discovery process by discarding the RREP received from them. The problem with this approach is that N number of RREP entries need to stored till actual RREP from Destination is received which consumes a lot of memory though the author have included the flush facility after receiving RREP from actual node. Network traffic is unnecessary can get disturbed as there is no provision to stop the malicious node from sending RREP message in network.

**SETX protocol Based mechanism :**

The author has suggested mechanism [3] whose sole concept is based on the matrix used to find the highest throughput route including the retransmitted packets. The matrix $d_r$ & $d_f$ are used to find the probability of number of packets successfully received by the node and the probability of number of packets successfully delivered by the neighbouring node. The mechanism adapted by the author to counter the black hole attack is by allowing the initiator to broadcast the probe message to their neighbours containing the stream of probe random values. The author is quite optimist that recipient cant give the different random number values than the numbers in the probe message received which is not always possible.

**Bait Dynamic source routing mechanism:**

As per the author of [6] has proposed BDSR.,the detection mechanism is based on the 2 changes incorporated each in RREP, RREQ ie.. Record Address in RREP and Target Address(which happened to be an virtual and non existing address)which helps in tracing the black hole problem quite in advance which reflects the proactive mechanism proposed by author. The reactive mechanism is portaged in the situation where in destination learns about the decrease in packet delivery rate to threshold and intimating the same to the initiator node to take up the defense against such loss to network. In response to that initiator broadcast the bait RREQ, on receiving the RREP from virtual destination address then the initiator starts adverse tracing procedure is triggered immediately and records the address of malicious node in the black hole list.

## VI - PROPOSED SOLUTION

To defend against a Black Hole Attack the proposed method involves design of two control packets in addition to existing control packets of AODV routing protocol.

The Two control packets are

**REACTION-TO-DISCOVERY-PACKET**
**REACTION-_TO-_SEND-_DATA-_PACKET**

As per the proposed method after receiving the route reply packet (RREP) for the Route Discovery packet (RREQ) sent by the source node in to the network with the intension to send the transmit the data traffic to destination Node.Source nodes are are programmed to examine the originality of the Intermediate Node (Immediate Replier of RREQ) Prior to routing the data traffic Source Node by requesting it to share the REACTION-TO-DISCOVERY-PACKET which has a reaction time variable (which automatically get updated the movement the Node responds to a Route discovery packet (RREQ)) with respect to the REACTION_TO_SEND_DATA_PACKET which has a reaction time variable (which automatically get updated the movement the one of the neighbouring node receives data packet from other neighbouring node or Immediate replier of RREQ)

If the (REACTION_TO_DISCOVERY _PACKET is much lesser than REACTION_TO_SEND_DATA_PACKET)

Then
its symbolizes very clearly that the intermediate node is not a genuine or trust worthy node as the reaction of maliciously behaving nodes are too responsive at RREQ just to convince the nodes to divert the Data traffic toward them with the intension to either paralyze the network or drop the urgent-cum (critical) data which can't be maintained for greater span of time at the specific node by sending the fair destination sequence number and hop count number.

The comparison process is carried with respect to the parameters shared by replier of RREP and immediate neighbour of source node.

**Algorithm:**

1: Set Simulation Time

2:Start simulation Time

3: Source_ Node( )

3.1 Has_ Data_To_Send

3.1.1 Discover the Genuine Route from source_Node to Destination_node

3.1.2 on Receiving RREP

3.1.2.1 test the NODE_PROPERTY // test whether node good node or maliciously behaving node

- ✓ Request the sender of rrep to share the REACTION_ TO_DISCOVERY _PACKET
- ✓ request the immediate neighbour to > REACTION_TO_SEND_DATA_PACKET
- ✓ IF (REACTION_TO_DISCOVERY _PACKET > REACTION_TO_SEND_DATA_PACKET)
- ✓ Declare the nodes behaviour's as Maliciously behaving node and nodes having maliciously behaving as intermediate node would discard the route and may identify the route through fresher route discovery process

Else

DATA Traffic is diverted to through the same route

4 Followed by normal other activities of the nodes in the network .

5 The simulation end when timer expires.

## V- RESULT ANALYSIS

The network performance can be evaluated based on the Trace file and Xgraphs generated for the following performance metrics under Black Hole Attack Model.The metrics used to evaluate the performance of AODV protocol are given below:

### Packet Delivery Ratio(PDR):

The ratio between the number of packets sent from the application layer and the number of received at the destination nodes. It is desirable that a routing protocol keep this rate at a high level since efficient bandwidth utilization is important in wireless networks where available bandwidth is a limiting factor

**Routing Overhead(ROH):**

The routing overhead metric used to calculate the bandwidth (which often is one of the limiting factors in a wireless system) that is consumed by the routing message s(like RREQ, RREP, RERR etc) to the amount of bandwidth available to the data packets in the simulation model.

**Packet Drop :**

The total number of packets dropped in the network..The main cause of data loss is attacks planted by misbehaving nodes in the network or sometimes link failures.

## IX - CONCLUSION & FUTURE WORK

In this paper the routing security issues of MANETs are discussed. Various threats to Mobile ad-hoc Networks are

discussed. Working of on demand routing protocol AODV protocol is discussed. With the core interest towards the most common Black Hole Attack which can be deployed by any malicious node is been discussed. The solution can be simulated using the NS2.34 (Network Simulator) and can Some to conclusion that Packet Delivery Ratio is better than normal AODV in presence of Black Hole Attack, but the Routing Overhead is quite more as extra Reaction based packets are included in to the working of Modified AODV protocol, that can be compromised at the cost of higher Packet Delivery Ratio and lower Packet Drop while defending against Black Hole Attack.
In focus to future work a method would be proposed to reduce the routing overhead still maintaining the higher PDR and very Low Packet Drop.

## REFERENCES

[1] Yibeltal Fantahun Alem ,Zhao Cheng Xuan "*Preventing Black Hole Attack in mobile Ah-hoc Network using Anomaly Detection*" 2010 2nd international conference on future Computer and Communication.

[ 2] Guo Xian ,Feng Tao,Yuan Zhan-Ting,Ma jian feng "*The Hierarchical threat model of Routing security for wireless Adhoc networks*"2010 first International Conference on Networking and Distributed Computing.

[3] Kitisak sathanunkul and Ning Zhang "*A Counter Measure to black hole Attacks in Mobile Adhoc Networks* "2011 International Conference on networking sensing and Control delft the Netherlands
11-13 April 2011.

[4] Mehdi Medadian, Ahmed Mehdabi, Elham Shahri "*combat with black hole attack in AODV Routing protocol*" 9th Malaysia International Conference on communications 15-17 December 2009 kuala Lumpur Malaysia.

[5] Junhai Luo, Mingyu fan & Danxia Ye "*Black Hole attack Prevention Based on Authentication mechanism*" International conference on computational science ,2008.

[6] Po-Chun TSOU, Jian –Ming CHANG,Yi Hsuan LIN, Han-Chieh CHAO, Jiann –Liang CHEN "*Developing a BDSR Scheme to Avoid Black Hole Attack Based On Proactive and Reactive Architecture in MANETS*" 13th International Conference on Advanced Communication Technology Feb 13-16, 2011 ICACT.

[7] Kamarularifin Abd, Jalil, Zaid Ahmed, Jamalul-Lail-Ab Manan "*Mitigation of Black Hole Attacks for AODV routing protocol*".

[8] Maha Abdelhaq,Semi Serhan, Raed Alsaqour and Rosilah Hassan" *A local Instrusion Detection Routing security over MANET Network*" 2011 International Conference on Electrical Engineering and informatics 17-19 July 2011,Bandung ,Indonesia.

[9] venkat balaKrishan, Vijay Varadharajan, UdayTupakuluand Phillip Lucs "*TEAM:Trust Enhance Security Archirtecture for Mobile Adhoc Networks*" ICON-2011: 9th International Conference on NaturalLanguage Processing 16-19 December,2011.

[10] G.S Mamatha ,S.C Sharma "*A highly Security Approach against Attacks in MANETS*" International journal of Computer theory and Engineering Vol 2 No 5 October 2010.

[11 ] E. A Mary Anitha, V. Vasudevan "*Black Hole Attack Prevention in Multicast Routing Protocols for Mobile Ad hoc networks using Certificate Chaining*" 2010 International Journal of Computer Applications (0975– 8887)Volume 1 – No.12.

[ 12] Harsh Sadawarti, Anuj K.Gupta, Member,IAENG "*Secure Routing Techniques for MANETs*" International Journal of Computer Theory and Engineering, Vol. 1, No. 4, October2009.

[13] Ahmed Nabet ,Rida Khatoun, Lyes Khoukhi ,Jiliette Dromard and Dominique Gaiti "*Towards secure Route Discovery protocol in MANETS*" International Conference on Advanced Communication Technology Feb 13-16, 2011 ICACT.

[14] Luc Hogie,pascal Boury,Frederic Guinand "An Oveview of MANETs simulation" URL: www.elsevier.nl/locate/entcs.

[15] Parth Shah,Vishwas Raval,Ami Nayak,Amit Ganatra,Yogesh Kosta "*International Journal of Computer Theory and Engineering*", Vol 3,No.1,February ,2011 pg no 1793-8201.

[16] Geeta pattun, Suresh kumar ," international c c onference on atmospheric research and communication" dec
21st-22nd,2012