Ujjval Jain et al. International Journal of Recent Research Aspects ISSN: 2349-7688, Vol. 5, Issue 1, March 2018, pp. 100-105

A Modified AODV (MAODV) against Black Hole attacks in MANETs

Ujjval Jain[1], Ravikant[2], Jogendra Kumar[3]
Northern India Engineering College, Delhi., India
[1] Ujjvalniec123@gmail.com
[2] ravi.iims.meerut@gmail.com
[3] jogendra.kaushik@niecdelhi.ac.in

***Abstract*: A Mobile ad-hoc network (MANET) is a latest and emerging Research topic among researchers. The reason behind the popularity of MANET is flexibility and independence of network infrastructure. The most common routing protocols used in ad-hoc network are AODV (ad-hoc on demand distance vector) protocol. AODV protocol is threatened by many attacks like Black hole, Gray hole attack etc. In black hole attack a malicious node advertise itself as having the shortest path to the destination node. In this paper, we have discussed about the MANET, it's technical and security challenges. We have comprised in our study the attacks that can be mounted on the MANET and their effects. Before evaluating an attack, we have analyzed the behavior of the attack, the different way an attack can be mounted and their symptoms. Here, in this paper, we have evaluated the Black Hole attack in Random way point on the basis of throughput, packet drop ratio. In this paper we proposed a Modified AODV protocol which improve the performance and reduce the black hole attack. We take the AODV protocol to analyze this attack. Black hole attack is the most common attack in Manets which is responsible to disturb the existing infrastructure or collect the secure information from Manets. It reduces the performance of the network. We have implemented our protocol in Network Simulator 2 (NS-2).**

I. INTRODUCTION:

Mobile Ad-Hoc Networks (MANET) is autonomous and decentralized wireless systems. MANETs consist of mobile nodes that are free in moving in and out in the network [1]. Nodes are the systems or devices i.e. mobile phone, laptop, personal digital assistance, MP3 player and personal computer that are participating in the network and are mobile. These nodes can act as host/router or both at the same time. They can form arbitrary topologies depending on their connectivity with each other in the network [2]. These nodes have the ability to configure themselves and because of their self configuration ability, they can be deployed urgently without the need of any infrastructure. Internet Engineering Task Force (IETF) has MANET working group (WG) that is devoted for developing IP routing protocols. Routing protocols is one of the challenging and interesting research areas. Many routing protocols have been developed.

For MANETs i.e. AODV[3][4], OLSR[5], SAODV[6], ARAN[7], ARINDNE[8] etc.Security in Mobile Ad-Hoc Network is the most important concern for the basic functionality of network. The availability of network services, confidentiality and integrity of the data can be achieved by assuring that security issues have been met. MANETs often suffer from security attacks because of its features like open medium, changing its topology dynamically, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism. These factors have changed the battle field situation for the MANETs against the security threats.
The organization of this paper is as follows. Section II describes the AODV protocol and Black Hole attack, section III describes the various approaches proposed till date to handle this attack, section IV explains the proposed algorithm, section V provides the simulation results along with comparison to basic AODV protocol and section VI provides the conclusion and discusses the future research options.

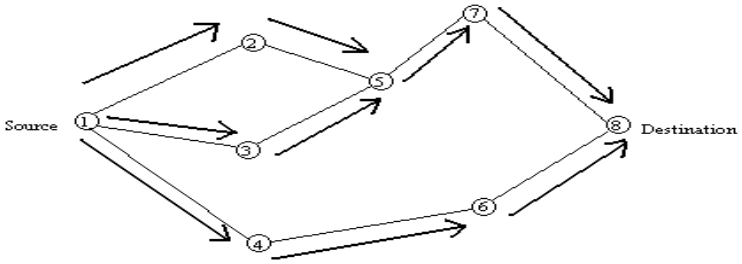
II. AODV AND BLACK HOLE ATTACK

Ad Hoc on demand Distance Vector (AODV)- AODV is a reactive routing protocol i.e. route is established whenever they required. Each node maintains a route table which stores the information about the other nodes route information like the destination address, destination sequence no, next hop address and hop count etc. The destination address confirms the freshness of the route means that if any node has the greater sequence no then it has a fresh route [9].
To establish a route, a node broadcasts the RREQ packets to its neighbors. Each node receives the packet and checks that if the node is a destination node. If the node is destination node it simply sends the RREP. If the node is not the destination node then it checks its routing table. If it has the route then it compares the destination sequence no with the incoming RREQ packet. If the node's destination sequence no is greater than the incoming RREQ packet then it sends the RREP packet. If destination sequence no is less then it simply rebroadcast the

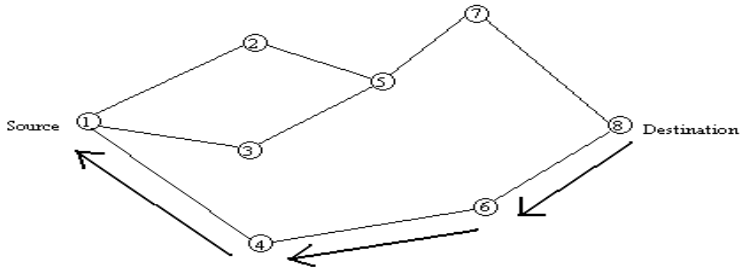
packet to its neighbors. The RREP packet travels the reverse route from that it came to the source node. The source node updates the routing table according to the packet. During this operation, if any link is broken then node sends the error message RERR to all the nodes which have used it.

Black Hole Attack: The Black Hole attack is kind of denial of service attack. In this attack, the malicious node send a route reply very early. It does not look into the route table for route information, it just send the route reply immediately it finds the RREQ .with higher sequence no and appears that it has the freshest route for destination. As a result of this, the route is established through the malicious node. When the data packet is transmitted through this node it simply drops the packet.

The malicious node always send the fresh route, this is the main symptom of this attack. The malicious node can perform this task by two methods:



(a) Propogation of Route Request (RREQ) Packet



(b) Path taken by the Route Reply (RREP) Packet

Fig 1 AODV routing

- By sending constant destination seq. no. : In this way the malicious node sends the RREP for every RREQ with same destination seq. no. assuming that the seq. no. will always greater.
- By sending the variable destination seq. no: Using this, the malicious node calculates the destination seq. no with respect to the destination seq. no. came with the RREQ. First and then send this with the RREP. Hence, the destination seq. no. is different for different RREQ.

III. RELATED WORK

Source node waits for the RREP packet to arrive from more than two routes. During this time, the Two or more nodes/hops shared the redundant paths From these shared hops the source node can recognize the safe route to the destination [10]. If no shared nodes appear to be in these redundant routes, the sender will wait for another RREP until a route with shared nodes identified or routing timer expired. If there are no shared nodes or hops between the routes, the packets will never been sent.. This solution can guarantee to find a safe route to the destination, but the main drawback is the time delay.

They proposed a trust model based on Packet forwarding Ratio (PFR). PFR measured at a node based on ratio of number of packets forwarded to the number of packets received. Based on PFR, node trust will be assigned[11]. If node forwards packets correctly trust values increases otherwise trust values decreases. In this trust model, trust values are assigned in the range between 0 to I. The trust value 0 signifies distrust node and trust value I signifies absolute trust. Trust value between 0 and 0.5 treated as malicious node, value between 0.5 and 0.75 treated as suspected node, 0.75 to 0.9 less trustworthy node, 0.9 to 1 treated as trust worthy node. If node has less trust values, it is not allowed to send packets for forwarding.

Modify the structures of RREQ and RREP and add a field in the routing table. In R-AODV, a MALICIOUS_ NODE_LIST is appended to RREQ packet to notify other nodes about malicious nodes in the MANET [12]. In

Paper, they added a flag called DO_NOT_CONSIDER to RREP to mark/identify reply from a malicious node. In addition, they add another field to this called MALICIOUS_NODE for marking a node as malicious node.

In MR-AODV, when a node detects a malicious node, it updates the routing table with malicious node entry and discards the RREP . it is neither forwarded on the reverse path nor requires a DO_NOT_CONSIDER flag; thus, all RREPs reaching 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. Thus, MR-AODV attempts to reduce routing overhead by not forwarding RREP after detection of misbehavior[13]. proposed a novel approach for detecting and preventing these attacks and securing a route to the destination in an efficient manner [14]. True-Link-crosschecking method is designed to isolate and mitigate the effect of black hole attacks in MANET. True-Link-crosschecking enhances AODV protocol to improve the network performance by improving routing update condition [15]. Modified AODV, which is TAODV (Trust based AODV), is a network. TAODV has several salient features as Nodes perform trusted routing behavior mainly according to the trust relationship s among them. A node that performs black hole behavior will be detected and disprove by the whole network[16]. An another modified AODV, which is Dymo (Dynamic manet on demand) shows better performance than AODV. It has a special path accumulation function. DYMO also has a multipath characteristic which allows source to have many different alternates. This work will be conducted at the real time platform and it should be tested on cross layer [17].

IV. PROPOSED ALGORITHM :THE MAODV PROTOCOL

Different scheme is used in MANET to overcome the effect of black hole attack. Here, I have used behavioural based scheme in which the destination sequence no is traced. Since the malicious node always try to send the big destination sequence no. , it is easy to trace out the black hole node and after detecting the node the legitimate node just discards the RREP packet sent by the malicious node. Hence, the effect of the black hole attack can be minimized. Destination sequence no. sent from the malicious node is compared with the expected destination sequence no. If the destination sequence no is greater than the expected sequence no then it is found that the RREP is malicious.

Algorithm-

Parameters: DSN – Destination Sequence Number, NID – Node ID, MN-ID – Malicious Node ID, ESN- expected sequence number, NRC- Node Route Counter.

1) Start the route discovery phase with the source node S.
2) Store the Route Replies DSN and NID in RR – Table
3) If DSN is much greater than ESN then discard entry from RR-Table as

```
Select Dest_Seq_No from table
 if (Dest_Seq_No >= ESN_Seq_No)
    {
      Mal_Node=Node_Id;
      Discard entry from table; }
```

4) If Node = Good // if route is fine and Node is fine
then NRC= NRC+1;
5) If Node=Mal
then NRC=NRC-3; // if packet is unable reach Destination(black node)
6) Call ReceiveReply method of default AODV Protocol.

V. SIMULATION GRAPHS AND ANALYSIS

In this section we discuss experimental setup, performance metrics, simulation results and analysis.

A. Experimental Setup

The simulations are carried out on NS-2 (Ver. 2.35) simulator installed in Ubuntu environment. We implement BlackholeAODV to add Blackhole behaviors, M-AODV protocol is implemented as a solution to attacks. We use random waypoint model as the mobility model and set the traffic source to Continuous Bit Rate (CBR); nodes move within an area of 650 m x 650 m; we have used packet size of 512 Bytes. Simulation parameters are presented in Table I.

TABLE 1

Parameter	Value
Routing Protocol	AODV
Mac layer	802.11

Region	650 x 650 m2
No. of nodes	20
Movement Model	Random Way Point
Traffic type	CBR
Black Hole node	1
Simulation time	1000ms

We analyzed the traffic by analyzing the throughput and number of packet drop with respect to the every 200 seconds of simulation time.

B. Performance Metrics:

We use following metrics to compare performance between Black hole AODV, AODV and MR-AODV:

Packet drop ratio: the ratio of the number of packet drop by the nodes including malicious node to the total no of packet sent. It is most significant metric that should be considered especially with respect to the black hole attack. Packet Drop Ratio is calculated with the following formula.

Throughput : An important parameter to be considered in sending and receiving a data packet is throughput rate which directly affect the Quality of Service of the MANET. This the ratio of total data bytes sends to the transmission delay.

C. Results: We calculated the packet drop for every 200 seconds by calculating the difference of sent packets and receive packets. We perform the operation on NS-2 for 50 iterations. Then calculate the result on averages basic.

It is clearly shown that Packet Drop Ratio with Black Hole attack (shown by red line) is increased by 12% to 22% with respect to the normal AODV (shown by blue line). When we implemented the MAODV (green line), the packet drop ratio is decreased up to 5% from Black hole ratio. This is average of 50 iterations.

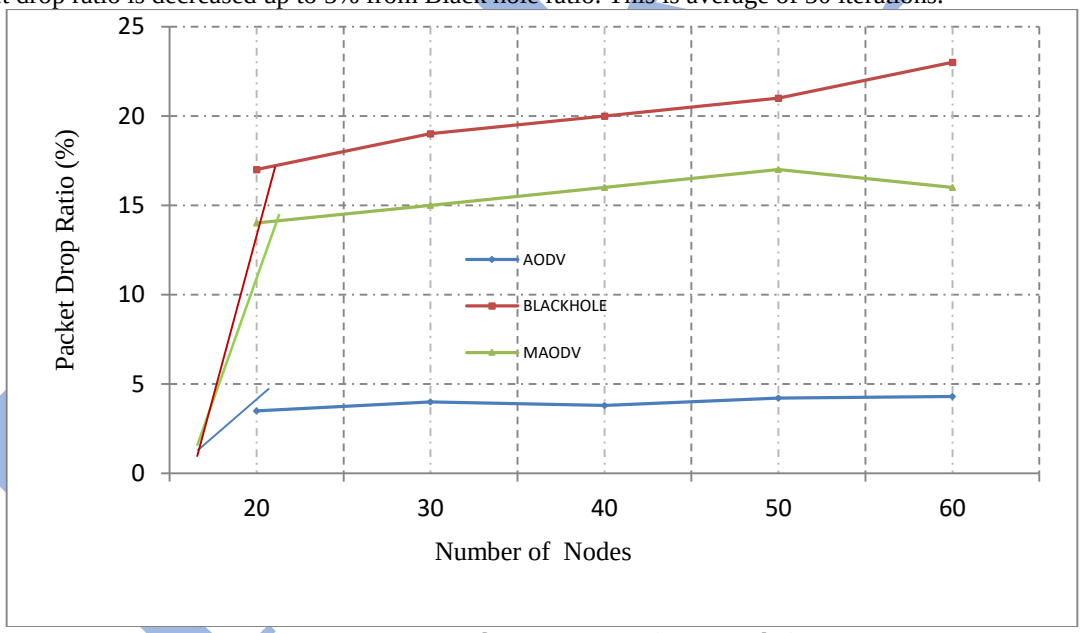


Fig.2 PDR in Random Way Point (20-60 nodes)

From figure 2, it is clearly shown that Packet Drop Ratio with Black Hole attack (shown by red line) is increased by 13% to 19% with respect to the normal AODV (shown by blue line). When we implemented the MAODV (green line), the packet drop ratio is decreased up to 9% from Black hole ratio. This is average of 50 iterations.

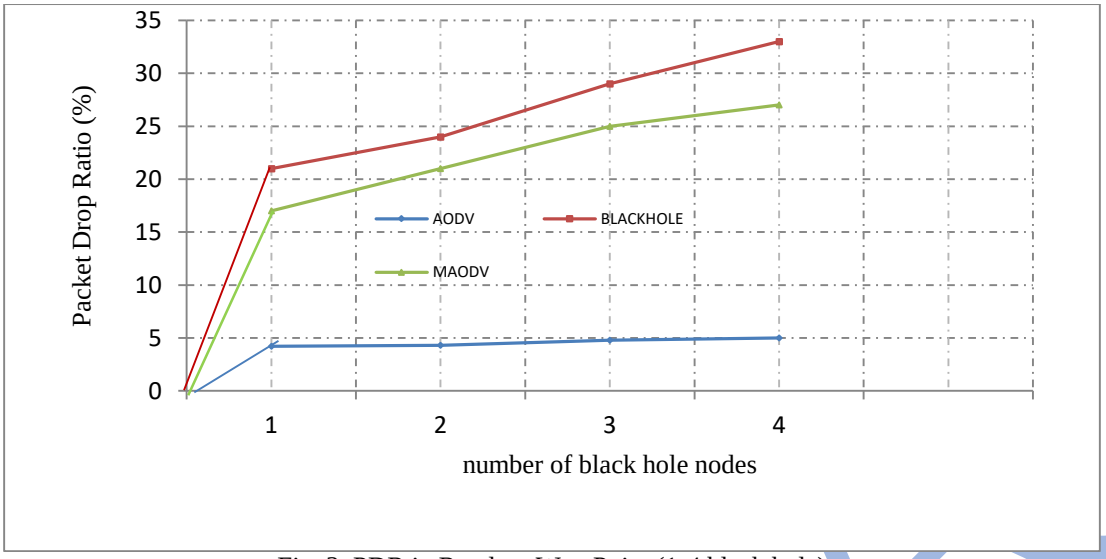


Fig. 3 PDR in Random Way Point (1-4 black hole)

From figure 3, it is clearly shown that Packet Drop Ratio with Black Hole attack (shown by red line) is increased by 17% to 28% with respect to the normal AODV (shown by blue line). When we implemented the MAODV (green line), the packet drop ratio is decreased up to 7% from Black hole ratio. This is average of 50 iterations.

Throughput Analysis

We analyzed the throughput for every 200 seconds. Following graphs have been found after the simulation.

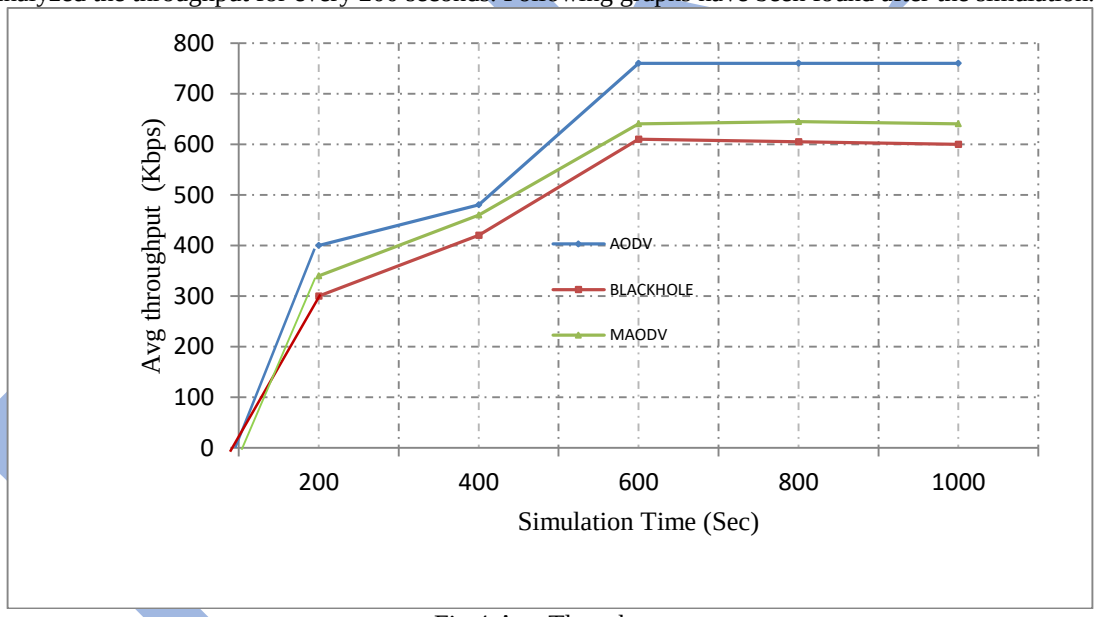


Fig 4 Avg Thoughput

Throughput has been reduced significantly as it is clearly shown by the graph. It is clear from these graphs throughput has been reduced up to 100 Kbps. This is average of 50 iterations. The mitigation scheme reduced the impact of attack with respect to throughput. Throughput reduction is almost same in the entire scenario.

VI. CONCLUSION AND FUTURE WORK

Mobile ad- hoc networks (MANET) which are recently being discussed in great extent. Security is the major issue to implement the MANET. In this paper work, we study the security requirements and challenges to implement the security measure in the MANET. Different types of attacks and available solutions are also discussed. We discuss some technologies which are used in the different solutions. However confidentiality is not required in the MANET because generally packets on the network do not contain any confidential data. Even though many cryptographic algorithms are implemented but some attacks do not bother about that. In this type of attack, the attackers silently drop the packet. Black hole and Gray hole attacks fall in this category.

In this paper, we worked on black hole attack which is the most common attack. We have analyzed the behavior of the black hole attack. In this paper we have analyzed the black hole attack using ns2 with scenario random way point. Random Way Point where the direction of the mobile in random with high speed. We have analyzed the effect of attack regarding throughput and packet drop ratio. Further, we have also performed the comparative analysis which gives the clear picture of the impact of the attack in this scenario. We have also evaluated a mitigation scheme which tries to avoid the occurrence of black hole attack.

An ample amount of paper has been carried out for the improvement towards the security of the MANET but still there are some issues to resolve. To perform a paper within a given time is never easy, as time increases the pressure on researchers to perform. Because of the time constraint, this paper focused only on the single attack. In future we would like to perform following tasks regarding black hole attacks:

- The co-operative black hole can be implemented and evaluated.
- The mitigation scheme can also be implemented with variable destination sequence no.
- The effect of the black hole attack can be evaluated with some other protocol like DSR and other MANET routing protocol.

REFERENCES

[1] C. Perkins, "Ad Hoc Networks", Addison-Wesley, 2001.
[2] S.Ci. et al.,"Self-Regulating Network Utilization in Mobile Ad-Hoc Wireless Networks", IEEE Trans. Vehic. Tech., vol. 55, no. 4, July 2006, pp. 1302–10.
[3] M. Zapata et al., "Secure Ad Hoc On-Demand Distance Vector (SAODV). Internet Draft", 2002.
[4] Y. Hu, A. Perrig, and D. Johnson, Ariadne, "A Secure On-Demand Routing for Ad Hoc Networks", Proc. of MobiCom 2002, Atlanta, 2002.
[5] Th. Clausen et al., "Optimized Link State Routing Protocol", IETF Internet draft, draft-ietf-manet-olsr-11.txt, July 2003. Routers," IEEE Commun. Lett., vol. 9, no. 4, Apr. 2005, pp. 363–65.
[6] M. G. Zapata and N. Asokan, "Securing Ad-Hoc Routing Protocols", Proc. 2002 ACM Workshop, Wireless Sec., Sept. 2002, pp. 1–10.
[7] K. Sanzgiri et al., "A Secure Routing Protocol for Ad Hoc Networks", Proc. 2002 IEEE Intl. Conf. Network Protocols, Nov. 2002.
[8] Y-C.Hu, A.Perrig, and D.B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," Proc. MobiCom02, Atlanta, GA, Sept. 23–28, 2002.
[9] C. E. Perkins, E.M.B. Royer and S. R. Das, "Ad Hoc On-Demand Distance Vector (AODV) routing", RFC 3561, July 2003.
[10] Ms.Nidhi Sharma et.al., "The Black-hole node attack in MANET", 978-0-7695-4640-7/12 2012 IEEE.
[11] Fidel Thachil,et.al., "A trust based approach for AODV protocol to mitigate black hole attack in MANET", 978-0-7695-4817-3/12 2012 IEEE.
[12] Rutvij H. Jhaveri et.al., "Improving Route Discovery for AODV to Prevent Blackhole and Grayhole Attacks in MANETs", INFOCOMP, vol. 11 no. 1, p. 01-12, March of 2012.
[13] Rutvij H. Jhaveri et.al., "MR-AODV: A Solution to Mitigate Blackhole and Grayhole Attacks in AODV Based MANETs", 978-0-7695-4941- 5/12 2013 IEEE.
[14] Seryvuth Tan and Keecheon Kim "Secure Route Discovery for Preventing Black Hole Attacks on AODV-based MANETs"978-0-7695-5088-6/13© 2013 IEEE.
[15] Gayatri Wahane, Ashok M. Kanthe and Dina Simunic "Detection of Cooperative Black Hole Attack using Crosschecking with TrueLink in MANET" 978-1-4799-3975-6/14/$31.00 ©2014 IEEE.
[16] Apurva jain and Anshul Shrotriva "Investigating the Effects of Black Hole Attack in MANET under Shadowing Model with Different Traffic conditions" IEEE International Conference on Computer, Communication and Control (IC4-2015).
[17] Manju and Kapil Kaswan "To study the impact of Black protocols" International Journal of Advanced Research in Computer and Communication Engineering (ISO 3297:2007, vol. 6, 2017).

