ISSN:0975-9646

Prevention Of Black hole Attack using AODV Routing Protocol in MANET

Nirali Modi, Vinit Kumar Gupta

Department of computer engineering
Hasmukh Goswami College of Engineering,
Ahmedabad, India

***Abstract*-Wireless networks are getting popular due to their ease of use MANET is a wireless ad hoc network, decentralized network and autonomous system. Each node in MANET is free to moving in and out direction in network .Recently in past few years Security of computer network has been of serious concern. Due to various factors including lack of infrasture, absence already established trust relationship in between the different nodes. The routing protocols are vulnerable to various attacks Denial –of-service (DOS) attacks are namely as black hole, gray hole, worm hole attack. Reactive routing protocols are suitable for this kind of attack. The proposed algorithm used the trust value which is used to identify the malicious node, after identifying the malicious node it will be removed from the neighboring table and we select the another path. This proposed algorithm can offer a secure way transmission between any nodes in network topology. We propose modification to the AODV protocol and justify the solution with implementation and simulation using NS-2.33. Our analysis shows the significant improvement in end-to-end delay, throughput, and packet delivery ratio of AODV in presence of Black hole attack.**

***Keywords*—MANET, Black hole, AODV, RREQ, RREP**

I. INTRODUCTION

Most important concern for network is security in mobile ad hoc network. It is highly adaptable and deployable network. It is a self- configuring infrastructure less network of mobile devices connected by wireless. Radio communication is used by mobile nodes. Basically there are two types of attacks.

Active attack:

Active attack can be external or internal. They can disturb the network's task by alarming the false message or modifying information. Internal attacks are attacker within the network and external network are outside the network by carried out nodes that do not belongs to the network e.g. modification, jamming and message reply.

Passive attack:

Passive attacks are difficult to detect and does not disturb the network's performance or operation e.g. traffic analysis, traffic monitoring.

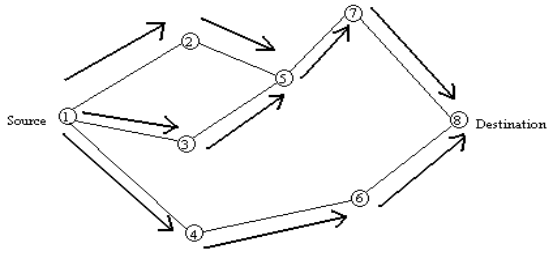
At present, the study of MANET has gained lots of interest of researchers [1]. A Mobile ad hoc network as the name suggest, is self-configurable network of wireless. In MANET, Some mobile hosts are willing to forward packets to neighbors. These type of network have no fixed routers, every node could be router. All nodes are able to moving and can be connected dynamically in an arbitrary manner. The individual terminals are allowed to move freely in the network. In this type of network some pairs of terminals may not be able to communicate directly with each other and have to rely on some other terminals. So that the message are delivered to their destination. Such networks are often referred to as multi hop network. Security in mobile ad hoc network is the most important concern for the basic functionality of network. Availability of network, confidentiality and integrity of the data can be achieved by assuming that security issues have been met. MANET often suffer from security attacks because of the its features like open medium, changing its topology dynamically, lack of central monitoring and management. Security is the cry of the day. In order to provide secure communication and transmission engineer must understand different types of attacks and their effects on the MANETs. Megha Arya et al.[1]worm hole attack, black hole attack, flooding attack, selfish node misbehaving are kind of attacks that a MANET can suffer from . MANET is more open to these kinds of attacks because communication is based on mutual trust between the nodes. There is no central point for network management, no authorization facility, changing topology and limited resources. Routing protocols are usually classified as table driven routing protocols also called proactive protocols which maintain continuous view of the full topology of the network in each node. On- demand protocols are also called reactive protocols which search for a route between source and destination.

The rest of this paper is organized as follows. In section 2, we briefly describe AODV routing protocol. Section 3, discuss about black hole attack, section 4 presents the related work in literature review, section 5 we discuss about our solution to modified black hole AODV algorithm , we conclude in section 6 with future work.

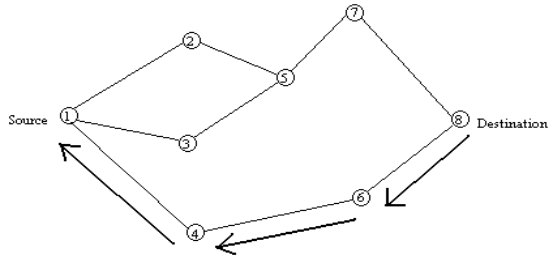
II. AN OVERVIEW OF AODV ROUTING PROTOCOL

AODV routing protocol is based on DSDV and DSR algorithm and is a state –of – the – art routing protocol that adopts a purely reactive strategy. It sets up a route on demand at the start of communication and use it till it breaks after which a new route setup is initiated [2]. This protocol is composed of two mechanism (1) Route discovery (2) Route maintenance. AODV use Route Request (RREQ), Route Reply (RREP) control messages in Route discovery phase and Route error (RERR) control messages in Route maintenance phase. The header information of this control message can be seen in detail in [3].

The nodes participating in the communication are classified as source node, an intermediate node or a destination node with each role, the behavior of a node actually varies. When a source node wants to connect a destination node, first it checks in the existing route table as to whether a fresh route to that destination is available or not. It uses the same otherwise the node initiates a Route discovery by broadcasting a RREQ message to all of its neighbors. This RREQ message will further be forwarded by the intermediate nodes to their neighbors. This process will continue until the destination node or an intermediate node having a fresh route to the destination. At this stage, RREP control message is generated, a source node after sending a RREQ waits for RREPs to be receive. Fig 1 shows the control messages.



(a) Propogation of Route Request (RREQ) Packet



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

Figure 1: AODV control message [3]

III. BLACK HOLE ATTACK

Routing protocols are exposed to a variety of attacks. Black hole attack is one such attack and kind of DOS. In which a malicious (fake) node makes use of the vulnerabilities of the route discovery packets of routing protocols to advertise it as having the shortest path and higher sequence number to the node whose packets it wants to intercept [3]. This attack aims at modifying the routing protocol so that traffic flows through a specific node controlled by the attacker. During route discovery phase, the source node sends the RREQ packet to the intended destination. Malicious nodes respond immediately to the source nodes as these nodes do not refer the routing table. The source node assumes that the route discovery phase is complete ignores other RREP message from other nodes and selects the path through the malicious node to route the data packets. The malicious node does this by assigning a high sequence number to reply packet.

As an example, consider the following figure 2, the malicious node "1" first detects the active route in between the sender 3 and sender 1. The malicious node "1" then send RREP which contains the spoofed destination address including small hop count, large sequence number than normal to node 2. This node "3" forwards this RREP to sender node "1".Now this route is used by sender to send the data and in this way data will arrive at malicious node. These data will then be dropped. In this way sender and destination node will be in no position any more to communicate in state of black hole attack [1].

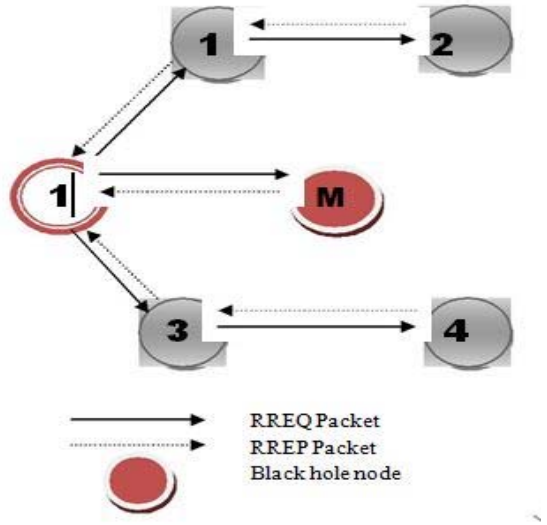


Figure 2: Black hole attack [1]

IV. RELATED WORK

We survey following paper to prevent the black hole attack.

A.Detection/removal of cooperative Black hole attack in MANET" [4]

In this paper, the authors proposed method can be used to find the short and secured routes and prevent the black hole nodes in MANET by checking whether there is large difference between the sequence number of source node or intermediate node who has sent back RREP packets or not . Generally the first route reply will be from the malicious node with high destination sequence number, which is stored in the RR-table as a first route entry then compare the first destination sequence number with the source node sequence number, if there exists much more difference between them, it means that node is the malicious node then immediately remove that entry from the RR-table.

B. Analysis of black hole and gray hole attack on RP-AODV in MANET"[5]

In this paper, the author presents a technique to find the chain of cooperating malicious node which drops a fraction of packet. Instead of sending a total data traffic at a time divide the total traffic into small sized blocks. So that malicious node can be detected and removed in between the transmission of two such blocks by ensuring an end to end checking. Source node sends a prelude message to destination node before start of sending any block to alert it about incoming data block. Flow of traffic is monitored. At the end of transmission, destination node sends an acknowledgement via postlude message containing the no

of data packets. Source node uses this information to check whether the data loss during transmission is within the tolerable range.

C. Mitigating routing misbehavior in self-organizing MANET using K-neighborhood local reputation system [6]

S. Neelavathy Pari et al presents a novel reputation based mechanism to detect the misbehaving nodes (NRMDM). This system adopts the local value of its K-hop neighborhood and the value is exchanged in K-hop neighborhood. This method helps to fully learn the experiences from its neighbor which helps from its neighbor to improve the ability to judge and improve itself. NRMDM contains for module .monitor module listens or monitors when the node sends a packet to the next node, it caches the packet to the next node, it caches the packet simultaneously or not. Reputation system module composed of node ID, direct reputation, indirect reputation and alarm count and flag. Path manager module selects the path from source to destination.

D. Destination based group black hole attack detection in MANET [7]

Avnesh Kumar et al proposed destination based scheme it contains the three steps.

1 .store the RREP packet on previous node.

2. Check 2 hop distance of suspected node.

3. Rejection of RREP packet to identifying a suspected node.

The common neighbor of previous node and suspected node checks the two hop distance node for reach ability to destination. To do so first it stores the RREP packet at previous node and attaches one hop distance of suspected node. In this paper , when RREP message replies to previous node, it should also attach the one hop distance node of replying node (suspected node) otherwise previous node will reject the RREP message in other case when there is no malicious node present in network, data packets successfully travels between source node to destination node.

E. The impact of packet drop attack and solution on overall performance of AODV in MANET [8]

In this paper the author presents the solution to packet drop attack and improves the performance of network. In this approach the trusted list is introduced instead of black list. As the packet drop is minor attack as proved to reduce re-analysis overhead analyzed node is or detection overhead added to trusted list. So it is skip that node's analysis in future. Hence it is reduce the calculation/ analysis or detection overhead for already analyzed trusted list to some extent trusted list is local to every node maintained as data structure in local RAM buffer. Direct reputation method using two counters.

F. Dynamic trust based method to mitigate black hole attack in MANET [9]

N. bhalaji et al presents the trust model. Here each node calculates trust value and association status for all its neighboring nodes through monitoring its behavior in the network. Then this trust model is integrated into the DSR protocol which is the common on demand routing protocol used in MANET. The security problems in the ad hoc network are analyzed and a trust based association security. To detect malicious node, each node maintains an association table. Association table is used to store the association status of any node with its neighbors. Association table has two fields first identifier of its entire neighboring node and second its relationship status with the neighbor node.

V. THE PROPOSED SOLUTION

The solution that we have proposed here is that we develop black hole AODV which allows some degree of node maliciousness to give an motivation to selfish nodes to state its malicious behavior to its neighbors which decreases searching time of misbehaving nodes. In proposed model the trust among nodes is represented by trust score. The trust calculation is based on packets loss rate if data packet is successfully transmitted then node trust value is incremented by 1, otherwise it becomes zero.

Step 1:

Add Black hole attack in AODV

Step 2:

Initially trust value 1 is assigned to all nodes in the network.

Step 3:

Source node broadcast request RREQ to all its neighbouring node using sendRequest( ) function. In this function hop count is initialized. Scheduler class is raised to run the simulation.

Step 4:

Neighboring node receives the request then it will check whether it is destination or not. If it is Destination then it will send reply by using sendReply( ) function otherwise forward request to its neighbouring node. This will check in recvRequest () function.

Step 5:

After confirming that it is not destination, it will further forward request to all its neighbouring node function. Hop count is increased at each node.

Step 6:

If it is destination then it will send reply using sendReply() function. Trust value is increment by 1 and assigned to all nodes in the path from destination to source node. Now, Source becomes destination for the current node.

Step 7:

After receiving the reply then the decision will take whether the index node is destination or not using recvReply( ) function. If it is not destination then it will forward reply.

Step 8:

In Source to destination, if any malicious node is present then it assigns Trust=0. So this path is not taken.

Step 9:

END

The main advantage of modifying the AODV protocol is (1). Malicious node is identified at initial stage, so immediately removed from neighboring table's entry (2)

packet delivery ratio is increased.(3) throughput also increased (4) with no delay the malicious nodes are easily identified.

Table 1: comparison of PDF of normal AODV, black hole AODV and modified AODV

Nodes	Normal AODV	Black hole attack with AODV	Modified Black hole AODV
20	0.9910	36.72	98.81
30	0.9930	33.55	99.22
40	0.9904	35.85	99.04
50	0.9946	41.60	99.33
60	0.9891	50.15	98.81

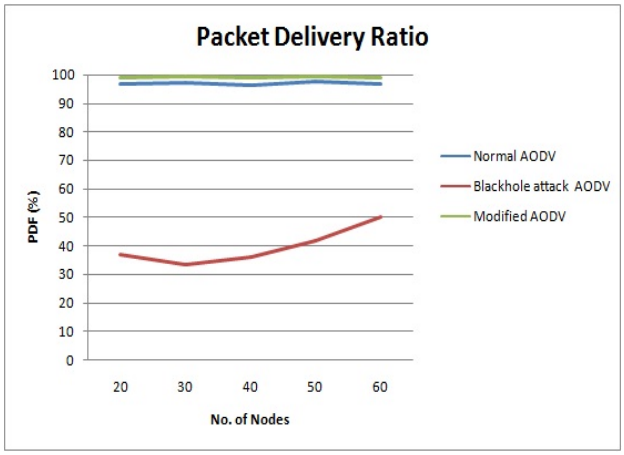


Figure 3: Black hole PDR

Table 2: comparison of Delay of normal AODV, black hole AODV and modified AODV

Nodes	Normal AODV	Black hole attack with AODV	Modified Black hole AODV
20	22.4009	10.45	28.01
30	19.7989	9.45	20.0655
40	31.6295	11.40	29.81
50	18.1787	9.16	21.45
60	30.9652	8.11	39.45

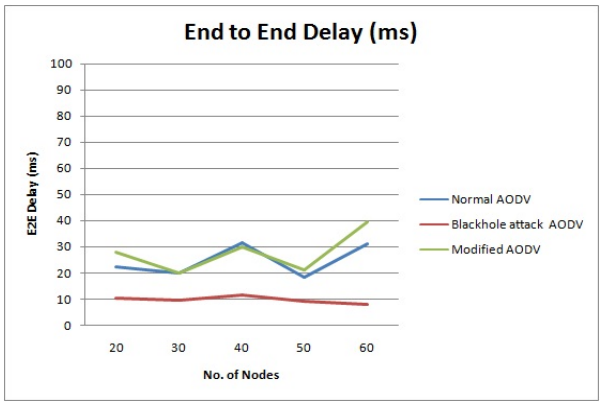


Figure 4: Black hole delay

Table 3: comparison of Throughput of normal AODV, black hole AODV and modified AODV

Nodes	Normal AODV	Black hole attack with AODV	Modified Black hole AODV
20	112.86	42.16	113.72
30	111.74	38.34	113.52
40	113.62	41.09	113.55
50	113.51	47.49	113.52
60	112.69	58.23	113.55

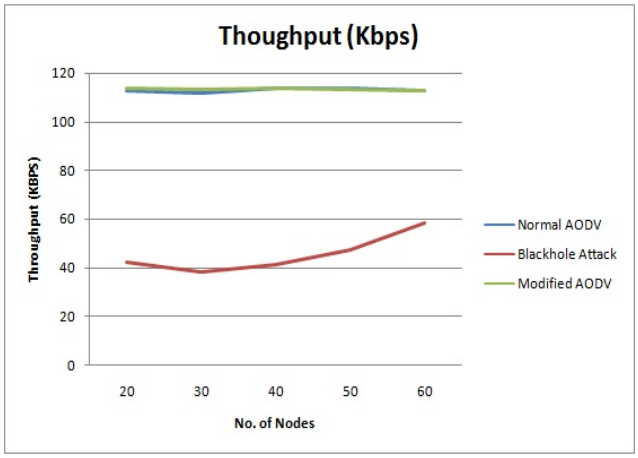


Figure 5: Black hole Throughput

VI. CONCLUSION

In this paper we have mentioned the AODV protocol and Black hole attack in MANET. We have proposed a feasible solution for Black hole attack that can be implemented on the AODV protocol. The proposed method can be used to find the malicious node. Based on the trust value of node we define which path is most suitable for routing the packet and Untrusted node can easily remove or ignored. As future work, we intend to develop simulation to analyze the performance of proposed solution based on the security parameters like packet overhead, memory usage, and mobility.

REFERENCES

[1] Inrich chalamtac, Maco conti, jennifer “mobile ad hoc networking:imperatives and challenges”school of engineering, university of texas at dallas, USA

[2] Amit N. thakare, Mrs. M.Y.Joshi, “ Performance Analsis of AODV and DSR Routing Protocol in Mobile Ad Hoc Network “, IJCA special issue on “ Mobile ad hoc networks”, 2010.

[3] C. perkins “(RFC) request for comments- 3561” category:experimental, networking working group , july.

[4] Sukla Banerjee, “ Deteciton / Removal of cooperative Black and Gray hole attack in Mobile Ad-Hoc Networks “, proceedings of the world congress on engineering and computer science.

[5] Nisha, samrajit kaur, “Analysis of black hole and gray hole attack on RP-AODV in MANET” International journal of engineering research and technology -2012.

[6] S Neelavathy Pari, D. Shridharan ,” Mitigating Routing Misbehavior in Self Organizing Mobile Ad hoc Network using K-neighborhood Local Reputation System” IEEE International Conference on recent trends in information technology.

[7] Avenash Kumar, Meenu Chawla," Destination based group Gray hole ackttack detection in MANET through AODV", IJCSI international journal of computer science issue, vol-9 , issue 4, No 1, july 2012.

[8] Ashok M. Kanthe , Ramjee Prasad, Dina Simunic,"The Impact of Packet Drop Attack and Solution on Overall Performance of AODV in Mobile Ad-Hoc Networks", international journal of recent technology and engineering (IJRTE) ISSN: 2249-8958, volume-2, issue-2, December 2012.

[9] N.Bhalaji, A.shanmugan, " Dynamic Trust Based method to Mitigate Gray hole attack in Mobile Ad Hoc Networks", International Conference on Communication Technology and system design 2011.

[10] Senith dokurar, v.m erten"performance analysis of ad-hoc networks under black hole attack"international journal of advanced research in computer science and software engineering volume-3, april 2012

[11] Rutvij h. javeri, sankita j.patel, devesh c.jinwala,"Dos attacks in MANET A survey " second international conference on advanced computing and communication technology 2012.

[12] A. anna lakshmi, k.r.valluvan" A survey of algorithm for defending MANETs against the DOS attacks", international journal of advanced research in computer science and software engineering september 2012.

[13] N. bhalaji, A. shanmugan,"Association between nodes to combat black hole attack in DSR based MANET" IEEE 2009.

[14] G.S. Mamatha, Dr. S.C.sharma,"Network layer attack and defence mechanisms in MANETs- A survey" international journal of computer applications , november 2010.

[15] Rutvij H. jhaveri, sankita j.patel and devesh c. jinwala" A novel approach for Gray hole and black hole attacks in MANET" second international conference on advanced computing and communication technologies 2012.