Black Hole Attack Deterrence And Exposure Elucidations On AODV Routing Protocol In Manet

Ms. A. Maria stella[1], Ms. J. Jennifer rani [2]
[1]Assistant Professor,Department of Computer Science, Pudukkottai, Tamilnadu, India
[2]M. Phil Scholar, Department of Computer Science, Pudukkottai, Tamilnadu, India

Abstract- *A Mobile ad-hoc Network (MANET) is a self-cultivating infrastructure-less network. AODV (Ad-hoc On-demand Distance Vector) routing protocol is a loop free protocol used in ad-hoc networks. It is conceived such that it can self-start in an environment where all the nodes are mobile in nature. It can also contest a variety of network actions such as mobility, failure of links and much more. The ad-hoc network is swayable to black-hole attack. In a black hole attack, the router drops the packets instead broadcasting them and is a type of denial-of-service attack.*

The proposed work embellishes the AODV routing protocol for detecting a black hole attack more efficiently and hence reducing the delay and communication overhead in the MANET. In the proposed work, the actions of the source node is adapted by broadcasting the repeated RREQ which includes its own sequence number instead of destination sequence number and pre-process RREP () function is also added which makes it more secure than the existing solutions. For this the network simulation 2.35 is used. The results obtained from the proposed methodology shows that the end-to-end delay has been decreased; packet delivery ratio and throughput have been increased.

Keywords- MANET, AODV, Black hole Attack, NS2

I. INTRODUCTION

Mobile ad-hoc network (MANET) has countless properties such as operation elasticity and simple installation. Due to these properties, over the last few years, many researchers have shown their interest in MANET. In Ad-hoc network all nodes are mobile; there is no physical connection while interactive with each other. One of the main features of it is its ability to operate without any central coordinator.

There are many real-world applications of this network, ranging from military to citizen, in search and rescue missions, in the collection of data's, and in virtual classrooms and Conferences. Multi-hop radio conveying results in frequent link breakage due to mobile nodes in the network. It also has a resource constraint like bandwidth, computing power, battery lifetime and many more. As there are various functions that take place in the MANET like packet forwarding and others, the security is one of the essential components.

One of the most popular routing protocols used in MANET is Ad-hoc on-demand distance vector (AODV) routing protocol. As paralleled to others, AODV routing protocol offers numerous benefits such as dynamic in nature, self-starting, and multiple-hops routing. Additionally, it can adapt various functions of MANET such as the change in topology, loop-free, and can automatically reject the inactive routes .Inappropriately, AODV routing protocol is exposed to many attacks. Among them, the black hole attack is one of the most critical attacks in AODV based MANET. This attack occurs by sending false routing information to the target nodes to cause fake route entries of nodes in the routing tables. As a outcome, many replica routes come into existence and cause a bottleneck in the communication channels.

Figure 1: Mobile Ad-Hoc Network.

1.1 Overview of AODV Protocol

AODV routing protocol is an on-demand/reactive protocol. A fresh route is formed when it is needed from source to destination. A source node broadcast route request (RREQ) packet to find a route to the destination node. If RREQ reaches a destination node either by itself or by a fresh route generated by an intermediate node, then it is said to be an honest route.

The renewed route is considered as an authentic entry if a sequence number of the destination node is greater than that of the RREQ sequence number. The route will be noticed if any

links break, and reply with a route error (RERR) packet, this packet is used to notify other contributing nodes in the network.

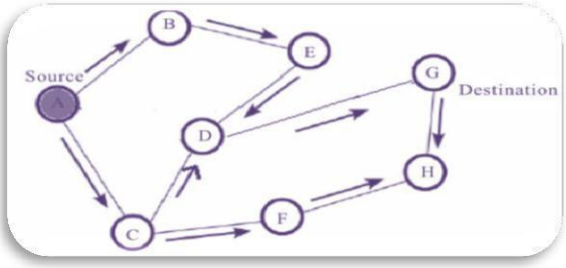

Figure 1.1.2 Propagation of RREQ

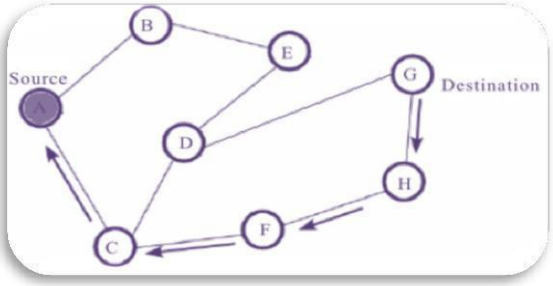

Figure 1.1.3 Route determination from source to destination

1.2 Black Hole Attack

Black hole in the network declaration to the location where an incoming or outgoing packet is mutely discarded (or "dropped"), a source has no information about the data that did not reach its intended recipient. The black hole intruder arrives to the recording group and tries to separate the packets from the multicast. This type of attack cancels one or more of the recipient packets instead of sending them; as a result the packet conveyance rate becomes low.

The black hole node waits to receive a RREQ. It reactions to the RREQ node before the other nodes do, without authenticating its routing list and thereby introducing itself as a fittest path from all the other nodes in the whole network and succeed in purchase all network packets, and can destroy entire network paths and formulate a DOS attack.

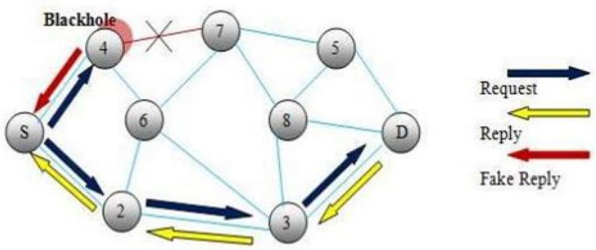

Figure 1.2 black hole attack

II. RELATED WORK

To recognize the black hole attack, several investigates have been conducted, to design methods of intrusion detection systems. Black hole attack is a dangerous active attack on Ad-Hoc networks. Here in this subdivision, the work done in the field of the black hole attack in AODV protocol is discoursed.

In Chavan et al. proposed an amendment in AODV, in which the performance of AODV in presence of black hole node is improved. But here routing overhead is more as compare to unchanged AODV.

Poongodi et al. proposed a confined secure routing architecture against accommodating black hole node in MANET. They have suggested a methodology, in which a novel LSAM protocol is designed to provide a security in MANET. It is shown that the proposed protocol is more secured and efficient. Limitation: It growths the overhead from 1 to 6 % on proposed routing protocol.

In Nishukalia et al. recommended a Modified AODV Routing Mechanism for detecting a multiple Black hole node", here they have used a replica RREQ packet which include source sq. no. instead of destination seq. no. Limitation: In the nonappearance of timer it increases end-to-end delay and also increases the network overhead.

Dhama et al. planned a detection of black hole attack and prevention mechanism for mobile ad-hoc networks. In this paper they introduce a cross layer queue at the transport layer so that when black node is detected or when a link is broken the packets can be defended at conveyance layer queue mean while the nodes will find a new route to the receiver.

In Sharma and Bisen, proposed an uncovering as well as removal of black hole attack in Manet. We have remarked that, there are two mechanisms based intrusion detection drop_ ratio_ analysis and trap_request for detecting and preventing black hole attacks. Limitation: increases network overhead.

III. PROPOSED WORK

In this section, the algorithm to perform the enhanced detection technique for black-hole attack is disclosed:

a) The source node broadcasts the pirated RREQ packet by the whole of its own source sequence number and address instead of destination sequence number and destination address.

b) When an intermediate nodes receives the pirated RREQ packet, the dealer node alternately calls for Pre-process RREP () method and stores all newly created RREP in the routing table new_RREP tab. Each participant in routing table is assigned by source sequence number.

c) It compares RREP dealer sequence number from the new _RREP_ tab and RREQ source sequence number from routing table. If RREP source sequence number is around greater than RREQ source sequence number, the source node discards this position entry in the new_ RREP _ tab, the table is not empty.

d) If new_RREP_tab is not empty, it will associate the dealer sequence number in pirated RREQ packet it received by the whole of the sequence number of the source described in the table.

e) As the source node sends its own sequence number, it will be more indisputable that it will be the fresh one. The intermediate node will have the source sequence less than the described in pirated RREQ packet. So it will not reply mutually RREP packet.

f) But, if in the network there reside any black hole node previously it advertises itself as having the shortest path with highest source sequence number and will reply with the RREP packet.

g) The source node will then detect the black hole nodes exist in the network.

Pseudo code of proposed method

Notations:

P: Packet

SN: Source_node

DN: Destination_node

IN: Intermediate_node

RREQ: Route_request

RREP: Route_reply

HC: Hop count

Hdr: Header

Src: Source

Sq. N.: Sequence Number

Drp: Drop

Rcv_time: receiving RREP time.

wait_RREP_time: Waiting time for RREP at source Node.

storeEntry: routing table entry for storing RREP_Entry. new_RREP_tab: new routing table for storing routing table entry.

Step: 1- // Incoming packets //

// There are four types of controls packets in AODV //

Switch (AODVTYPE_P)

{

Handler( )

}

If (AODVTYPE_P_RREQ)

{

// if I am the source or previously seen it
// Do (“Drp_P”);}

Step: 2- // BlackHole node gets RREQ packet for

Establishing a fake route to destination //

BlackholeAODV:: recvRequest (packet *p) {

Structhdr_ip *ip = HDR_IP(P);

Structhdr_AODV_request *rq =

HDR_AODV_request(p);

BlackholeAODV_rt_entry *rt; }

Step: 3- // BlackHole node creates a RREP packet immediately to respond this route request packet // Send reply (rq ->rq_src)

Sq N = max [SqN(u_int32), rq->dst_Sq N >rq_Src_Sq N]; //Comparing of Seq.No.

Step: 4- // when source node got RREPpacket from malicious blackhole node //

```
Preprocess_ RREP_RecvReply (packet p)

{

RrepHeaderRREP_Entry;

P_>RemoveHeader (RREP_Entry);

Rcv_time = receive RREP;

Set_time = Rcv_time + wait_RREP;

storeEntry.add(RREP_Entry);

Step: 5 //Store new_RREP tab entry//

While(Rcv_time<= Set_time)

{

new_RREP_tab.add(storeEntry);

}

Step: 6 // If new_RREP_tab is not empty// While (new_RREP_tab is not Empty) {

If (RREP.Src_ SqN.storeEntry-RT.Src_Sq N)

>(RREQ.Src_Sq N)

{ //Blacklist the node(Node is attacker)//

new_RREP_tab.DeleteRout(RREP_Src_SqN.storeEntry)

}

}

RecvReply (Packet) of AODV.

}

Step: 7 End
```

IV. EXPERIMENTAL RESULTS

i. Presence of black hole attack

In the second simulation module, we add the black-hole attacker Node 11. The attacker nodes drop/swallow every node that comes through it.

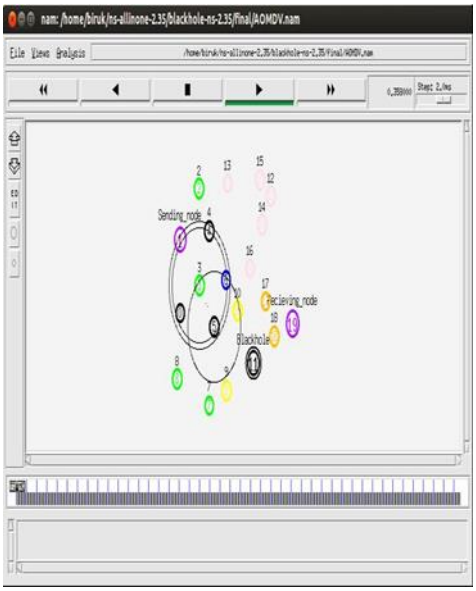

Figure 4.1: Presence of black hole attack

ii. Scenario-based Experiments for Presentation Evaluation of MANET Routing Protocols

In this segment, we define a set of experimentations directed to analyse the performance of the AODV routing protocol in a battlefield scenario.

The blue circles in figures 4.1, 4.1.1 and 4.1.2 represent the “optimal points” which corresponds to the highest PDF, lowest end-to-end delay and the lowest normalized routing load. It is found that for 60 nodes we complete this optimal point.

Ns-2 is an open source discrete event simulator used by the research community for research in networking. It has support for both wired and wireless networks and can simulate several network protocols such as TCP, UDP, multicast routing, etc. NS-2 can produce a detailed trace file and an animation file for each ad hoc network simulation that is very suitable for analysing the routing behaviour.

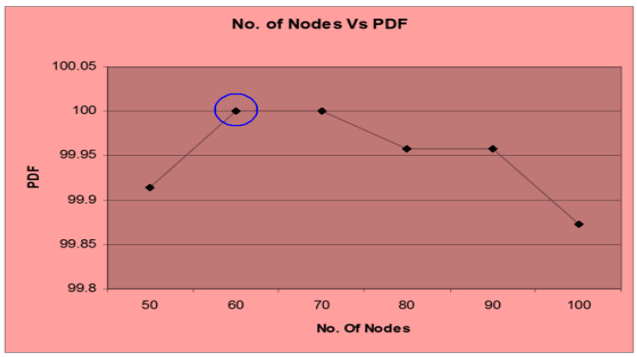

Figure 4.1 Effect of varying the number of nodes on the pause time

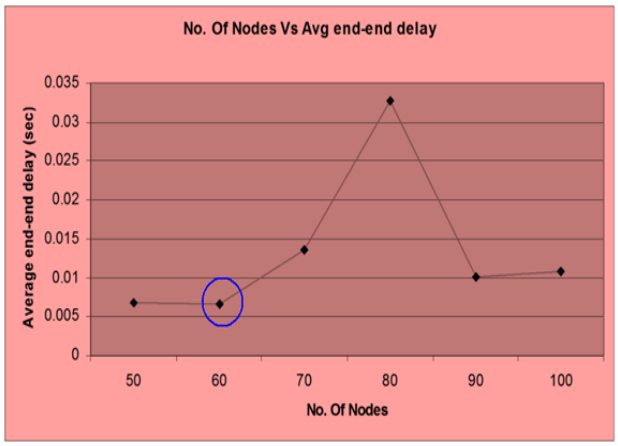

Figure 4.1.1: Effect of varying the number of nodes on the Average end-end delay

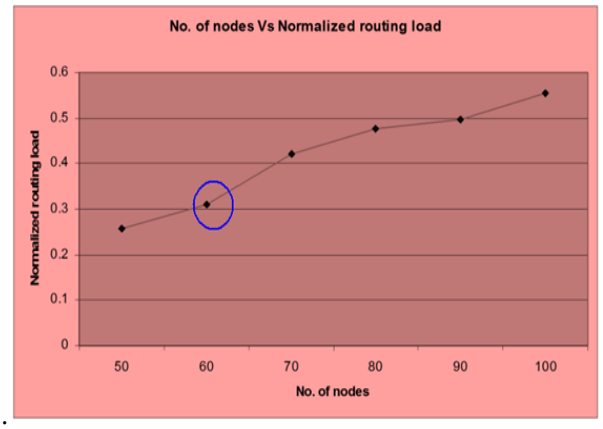

Figure 4.1.2 Effect of varying the number of nodes on the Normalized Routing Load.

V. CONCLUSION

In this paper, the performance of AODV, Black Hole AODV routing protocols is analysed. The scenarios simulated are with varying number of nodes such as 10, 20, 30, and 40 and with queue length 150. Along with this the nodes mobility speed has been varied between 0-10 m/s, on the basis of three parameters i.e. Packet delivery ratio, average throughput, and average End-to-End delay.

In this research, the proposed mechanism handles the black hole nodes attack in MANET. To tackle the black hole nodes attack, it assume that the source node is an intelligent node which uses the sequence number concept to detect the intruder nodes in

MANET and use timer and RREP(). In previous work, the source sequence number was used by the source node to detect the black hole attack without the timer. In the absence of time, the source node will not know that how much time it will take to detect the black hole node. After the black hole attack has overcome and route resuming is done, it is observed that:-

1. Packet delivery ratio is far better than that of AODV with black hole (malicious node)

2. The throughput of the network increases.

3. End-to-End delay decreases.

FUTURE WORK

The number of routing protocol provides different types of services to nodes in the presence of different scenario of the network. Every protocol shows different characteristics in the environment of mobile ad hoc network. In future work the stability of routing protocol in presence of multiple black hole node needs to be studied, and should identify which type of protocol gives the best performance if the size of network will increase sustainably and also found out the simulation result in presence of different scenario in large size of the network with cooperative black hole nodes and number of mobile nodes.

REFERENCES

[1] Sina Shahabi, Mahdieh Ghazvini1, Mehdi Bakhtiarian3, “A modified algorithm to improve security and performance of AODV protocol against black hole attack”, Springer Science Business Media New York 2015.

[2] A. A. Chavan, Prof. D.S.Kuruleb, Prof. P.U.Derec. “Performance Analysis of AODV and DSDV Routing Protocol in MANET and Modifications in AODV against Black Hole Attack” . 7th International Conference on Communication, Computing and Virtualization 2016, Published by Elsevier B.V.

[3] Jamali, S.B.S. (2015). “A survey over black hole attack detection in mobile ad hoc network”. International Journal of Computer Science and Network Security (IJCSNS), 15, 44

[4] N Vetrivelan, Dr. A V Reddy ―Performance Analysis of Three Routing Protocols form Varying MANET Size‖ Proceedings of the International Multi Conference of Engineers and Computer Scientists 2008 Vol II IMECS 2008, 19-21 March, 2008, Hong Kong.

[5] Abdul Hadi Abd Rahman and Zuriati Ahmad Zukarnain, ―Performance Comparison of AODV, DSDV and I-DSDV Routing Protocols in Mobile Ad Hoc Networks‖ , European Journal of Scientific Research, ISSN 1450-216X Vol.31 No.4, pp.566-576, 2009.

[6] Mohamed A. Abdelshafy and Peter J.B. King. Resisting black hole attacks on MANETs. In 13th IEEE Consumer Communications and Networking Conference (CCNC), pages 1–6, Las Vegas, USA, Jan 2016.

[7] Nital Mistry, Devesh C Jinwala, and Mukesh Zaveri. Improving AODV protocol against black hole attacks . In International Multi Conference of Engineers and Computer Scientists (IMECS), pages 1–5, Hong Kong, China, March 2010.

[8] Xin Li, Zhiping Jia, Peng Zhang, and Haiyang Wang. A trust-based multipath routing framework for mobile ad hoc networks. In 7th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD), volume 2, pages 773–777,Aug 2010.

[9] Rajdipsinh Vaghela, Divyesh Yogan and , and Monika Changela. A survey on approaches towards the black hole attack in MANET. Indian Journal of Research, 1(12):58–61, 2012.

[10] Tarek M. Mahmoud, Abdelmgeid A. Aly, and Omar Makram. A modified AODV routing protocol to avoid black hole attack in MANETs, International Journal of Computer Applications, 109(6):27–33, January 2015.

[11] Cho, J.-H. and I.-R. Chen, Modeling and analysis of intrusion detection integrated with batch rekeying for dynamic group communication systems in mobile ad hoc networks. Wireless Networks, 2010. 16(4): p. 1157-1173.

[12] Mutlu, S. and G. Yilmaz, A distributed cooperative trust based intrusion detection framework for MANETs, in The Seventh International Conference on Networking and Services2011.