Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IMPACT FACTOR: 6.017

IJCSMC, Vol. 6, Issue. 4, April 2017, pg.380 – 384

Black Hole Attack Analysis in MANET

Gaurav Khedekar[1], Devavrat Kalam[2], Tushar Kuwar[3], Gangaprasad Kawle[4], Sunil P. Khachane[5]

[1,2,3,4,5]Rajiv Gandhi Institute of Technology, Mumbai
[1] khedekar.gaurav@yahoo.in
[2] devavratk96@gmail.com
[3] tushar.kuwar7@gmail.com
[4] 3161prasad@gmail.com
[5] khachnesp@gmail.com

Abstract:- ***We are dealing with (MANET) Mobile ad-hoc network where nodes are mobile that is it moves as well as it communicates with other nodes for receiving and sending information or packets. For communication we are using various routing protocol which are used for making connection between two nodes, out of that we will discuss on AODV (Ad hoc on demand distance vector) routing protocol.***

Because of some loopholes in routing protocols one can attack on nodes such as dropping packets, giving false route etc. AODV finds route during sending packets only. So whenever path is encountered each node stores its path and make route to destination for specific source node. But there is problem known as black hole node. This type of node consumes packets and telling that it will send packets to destination. Here we are dealing with such problem caused by black hole and we will see how, by using sequence number we can avoid black-hole attack.

Keywords:- ***MANET, AODV, DSR, Black hole attack, RREQ, RREP, Sequence number***

I. INTRODUCTION

Mobile ad hoc network (MANET) is nowadays become very famous due to their fixed infrastructure-less quality and dynamic nature. They contain a large number of nodes which are connected and communicated to each other in wireless nature [10].. Due to its wireless nature and lack of any central authority in the background, Mobile ad hoc networks are always vulnerable to some security issues and performance issues.

There is no centralized gateway device to monitor the traffic within network. Since the medium is open for all nodes, both legitimate and malicious nodes can access it. Black hole or sequence number attack is one of the most common attacks made against the reactive routing protocol in MANETs[3].

There are various techniques that are proposed to avoid this attack one of them is watchdog. Watchdog protocol measures the sending time of the next hope node. If the sending time of the next hop neighbour is greater than the packet storing time and exceeds above some defined threshold of the network, then Watchdog knows that system is under black hole attack and it immediately mark this node as a malicious node.

Watchdog doesn't detect the actual reason of the packet loss. Also doesn't distinguish the packet loss due to congestion or due to the presence of a malicious node in the network. Watchdog decreases the network performance in terms of throughput.

II. AODV INTRODUCTION

In MANET previously DSR (distance vector routing) was used, because of DSR disadvantages such as DSR reply includes whole path to the destination, As network size grows route path also increases, data packet's header also increases and also network bandwidth not used fully [7]. In DSR there is more than one entry for one destination. If packet contains path to destination and there are many nodes in between source to destination hence size of packets goes on increasing which is not efficient.

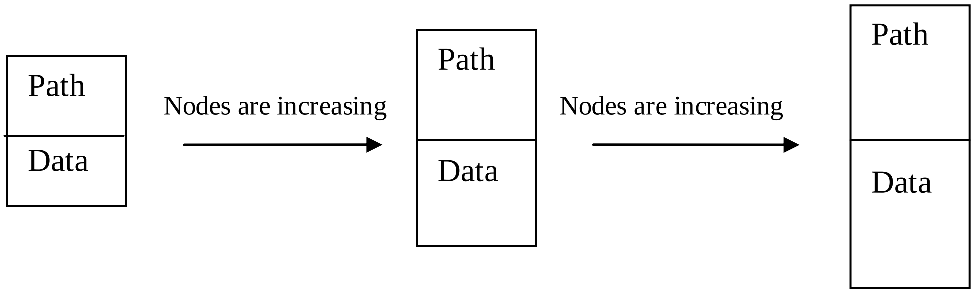


Fig. 1 : Route path increases as nodes are increases in DSR.

After DSR routing protocol AODV is used. AODV is reactive routing protocol. AODV has features such as on demand acquisition system, the routes are created when needed. AODV uses various messages for communication such as RREQ- broadcast to find route, RREP- Used to set forward path, RERR- Used to send error message. In this a routing table entry is expired if not used recently. Destination sequence number used as time stamp, it is used to check information is fresh or not [9].

In AODV the nodes participating in the communication can be classified as source node, an intermediate node or a destination node. With each role, the behaviour of a node actually varies. When a source node wants to connect to a destination node, first it checks in the existing route table, as to whether a fresh route to that destination is available or not. If a fresh enough route is available, it uses the same. Otherwise the node initiates a Route Discovery by broadcasting a RREQ control message to all of its neighbours. This RREQ message will further be forwarded (again broadcasted) by the intermediate nodes to their neighbours. This process will continue until the destination node or an intermediate node having a fresh route to the destination. At this stage eventually, a RREP control message is generated. Thus, a source node after sending a RREQ waits for RREPs to be received [3].

AODV has advantages such as, there is no central administration. Overhead of message is small, loop free and avoid count to infinity by usage of sequence number, perform better with static traffic with the source and destination pairs is relatively small for each host [1].

AODV has disadvantages such as, intermediate nodes leads to inconsistent routes if the source sequence number is very old and intermediate node have a higher but not the latest sequence number there by having stale entries. Multiple route reply packets in response to a single route request packet can lead to heavy control overhead. The periodic beaconing lead to unnecessary bandwidth consumption [1].

III.BLACK HOLE ATTACK

Black hole attack is an attack in which malicious node uses its routing protocol to advertise itself for having the shortest path with minimum hops to the destination node whose data packet it wants to take away [2].

Consider following scenario, A wants to send data to E and M is a malicious node. If A doesn't know route to node E. It starts with route discovery. In this A will send RREQ to its neighbour. RREQ format is like <source_ip_address, source_sequence_number, broadcast_id, destination_ip_address, destination_sequence_number, hop_count>. Refer figure 2.

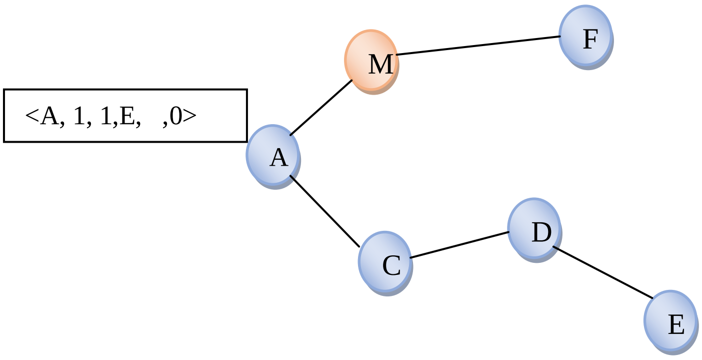


Fig. 2 : A starts RREQ

This route request broadcasted in the network. In this example it goes to C, D, E, M, F as shown. Whoever gets RREQ packets checks in its routing table for particular destination mentioned in the RREQ packet. If destination is present then it will send RREP. When packet reaches to destination it will send RREP packet along with its sequence number also at each node hop count gets increased by one. So source gets total hop count. Refer figure 3.

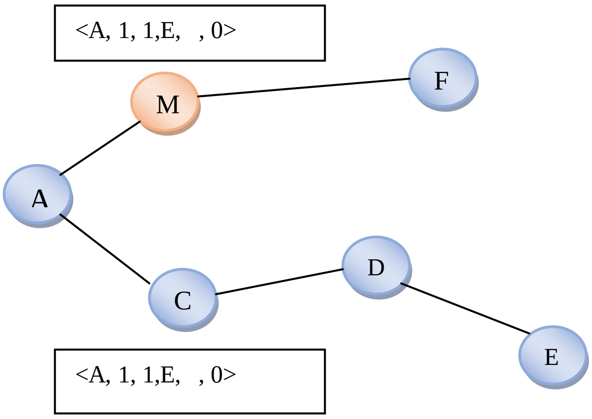


Fig. 3 : Broadcasting of RREQ in network by node A

Node C will check if it has a fresh route to node A. If not C will create an entry in its routing table for A. If C has route to E already then C will reply with RREP packet otherwise it will flood RREQ it again. Refer figure 4.

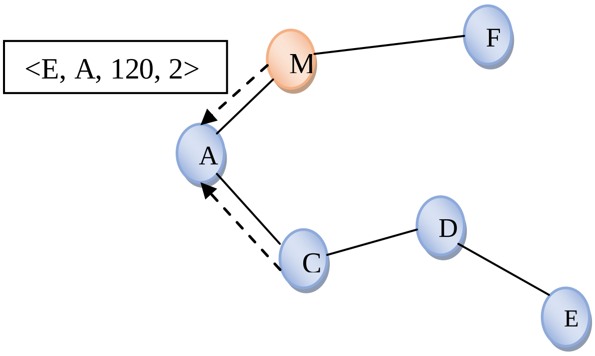


Fig. 4 : Fake reply from black-hole node M

Malicious node M will sends false RREP saying that I have shorter route to the destination. Node M creates RREP packet with less hop count. M is saying node E is reachable from me with hop count of 1. So from A it will be 2 hops. Refer figure 3.Now whenever A gets request to send packet to E. It will check for routing table entry, selects entry with high sequence number present that shows entry is fresh enough to use. This way black hole works in MANET.

Some results that we are getting through analysis of black hole attack.

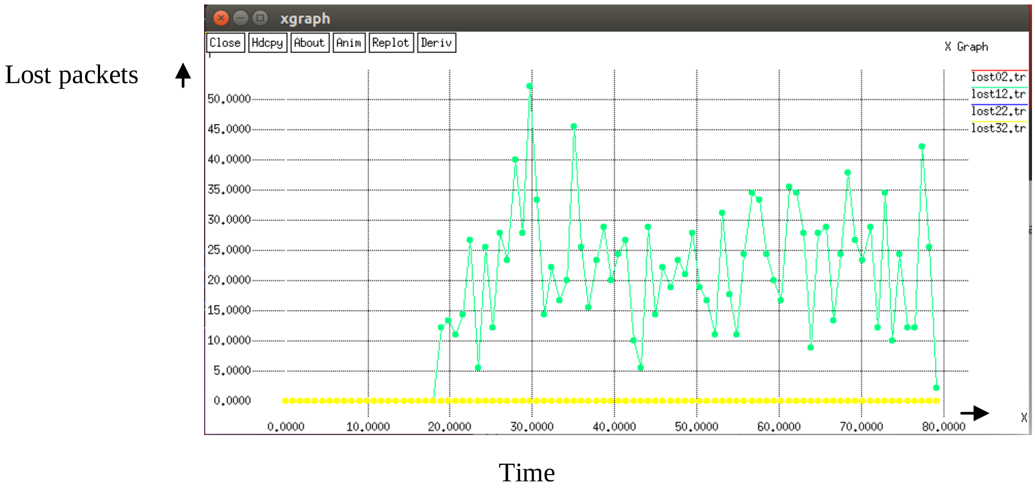


Fig 5. Packet loss between two nodes

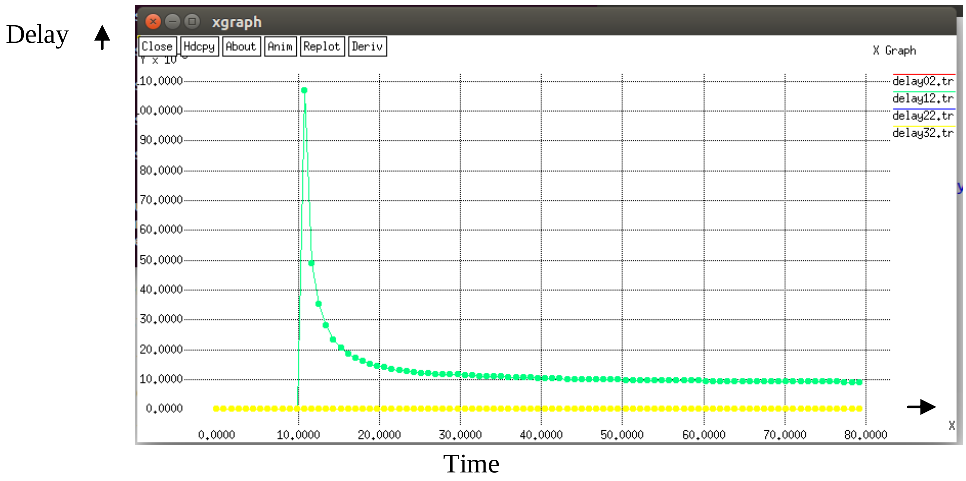
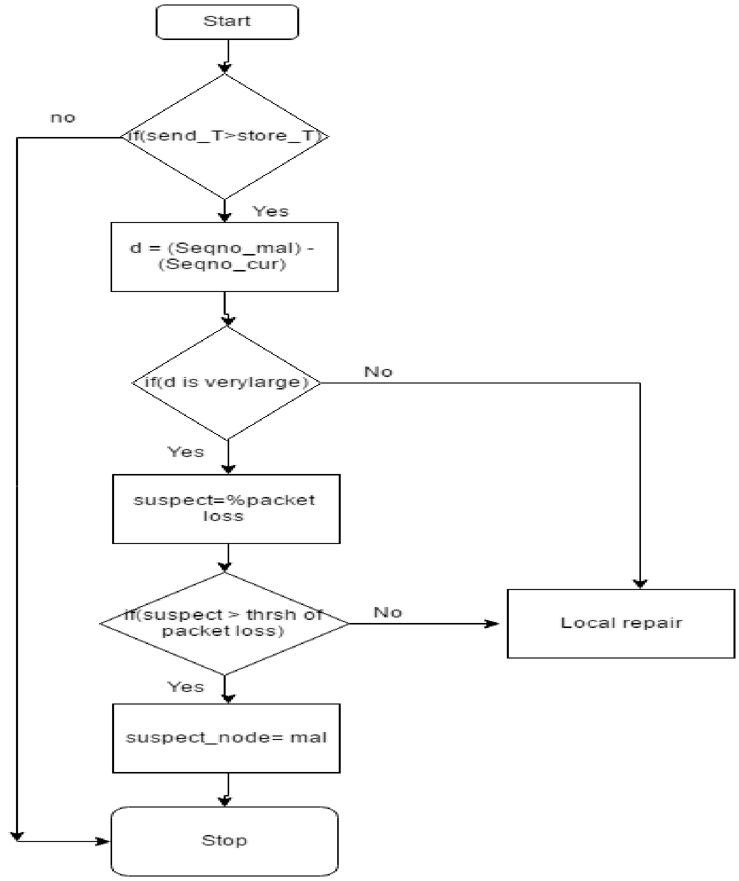


Fig 6. Packet delay between two nodes

IV. SOME WAYS TO ESCAPE FROM BLACK HOLE ATTACK

First we have to check sending time of packet is greater than packet storing time or not. If this is the case then there may be congestion in the network. Find difference between sequence number of node which can be black hole and sequence number of current node. If sequence number is large that is towards sequence number of suspected node. We calculate percentage loss of data on suspected node. If packet loss exceeds the threshold value then we labelled that node as malicious node. And spread this information in the network by flooding [4]. Refer figure 7.



V. CONCLUSION

Confidentiality and integrity are major factors for all communications in today's life. There are several attacks to which our communication media is vulnerable to. We have studied one of the most common attacks which occur while transmission of packets i.e. Black hole attack. To avoid such attacks such mechanisms are essential to be implemented to ensure the security of communication.

REFERENCES

[1]. Rahul Sharma1, Naveen Dahiya2, Divya Upadhyay3, An Analysis for Black Hole Attack in AODV Protocol and Its Solution, IJCSMC, vol. 2, Issue. 4, pp.391 – 395, April 2013.

[2]. Tarandeep Kaur, Amarvir Singh, Performance Evaluation of MANET with Black Hole Attack Using Routing Protocols, IJERA, Vol. 3, Issue 4, pp.1324-1328, Jul-Aug 2013.

[3]. Vipan Chand Sharma, Atul Gupta, Vivek Dimri, Detection of Black Hole Attack in MANET under AODV Routing Protocol, Volume 3, Issue 6, June 2013.

[4]. Nidhi Lal, An Effective Approach for Mobile ad hoc Network via I-Watchdog Protocol, International Journal of Artificial Intelligence and Interactive Multimedia, Vol. 3, No.1.

[5]. Mobile Ad-hoc Network (MANET) Properties and Spectrum needs at thenodesG. © Oxford University Press 2007.

[6]. Al-Roubaiey, A.; Sheltami, T.; Mahmoud, A.; Shakshuki, E.; Mouftah, H., "AACK: Adaptive Acknowledgment Intrusion Detection for MANET with Node Detection Enhancement," Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on , vol., no., pp.634,640, 20-23 April 2010.

[7]. Surana, K. A. "Securing Black Hole Attack in Routing Protocol Aodv in Manet with Watchdog Mechanisms." World Re-search Journal of Computer Architecture, ISSN (2012): 2278-8514.

[8]. Aarti, Dr SS. "Tyagi,"Study Of Manet: Characteristics, Challenges, Application And Security Attacks"." International Journal of Advanced Research in Computer Science and Software Engineering 3.5 (2013): 252-257.

[9]. Gandhewar, Nisarg, and Rahila Patel. "Performance Evaluation of AODV protocol in MANET using NS2 Simulator." 2nd National Conference on Information and Communication Technology (NCICT), Proceedings published in International Journal of Computer Applications® (IJCA). 2011.

[10]. Wage, Pratibha, and Channveer Patil. "INTRUSION-DETECTION SYSTEM FOR MANETS: A SECURE EAACK."

[11]. Bhosle, Amol A., Tushar P. Thosar, and Snehal Mehatre. "Black-Hole and Wormhole Attack in Routing Protocol AODV in MANET." International Journal of Computer Science, Engineering and Applications (IJCSEA) Vol 2 (2012).