International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 11, November-2014

A Review on Detecting and Mitigating Techniques of Black-Hole Attack from Aodv in Manet

Ankita Shukla
Department Of Computer Science & Engineering
Amity University, Lucknow

***Abstract*—A mobile ad hoc network (MANET) is a collection of autonomous nodes that communicate with each other by forming a multi-hop radio network and maintaining connections in a decentralized manner. One of the most critical problems in MANETs is the security vulnerabilities of the routing protocols. Most of the routing protocols for MANETs are vulnerable to various types of attack. Ad hoc On-demand distance vector routing (AODV) is a very popular routing algorithm. However, it is vulnerable to the well-known Black Hole Attack, wherein a malicious node falsely advertises good paths to a destination node during the route discovery process. This attack becomes more severe when a group of malicious nodes cooperate with each other. This paper analyses the impact of black hole attack on AODV.**

Keywords: Mobile ad-hoc network (manet), AODV, Black hole attack, Packet dropping, Malicious node.

I.INTRODUCTION

MANET is a group of mobile hosts that do not require involvement of any offered infrastructure or a base station. Instead of using physical cables, these wireless networks use radio frequencies to send and receive data packets.

Data transfer among nodes is realized by using multiple hops. These *Ad hoc* networks basically communicate via trust and cooperation among nodes.

MANET routing Protocols are divided into three categories: Proactive (table -driven), Reactive (on-demand) and Hybrid.

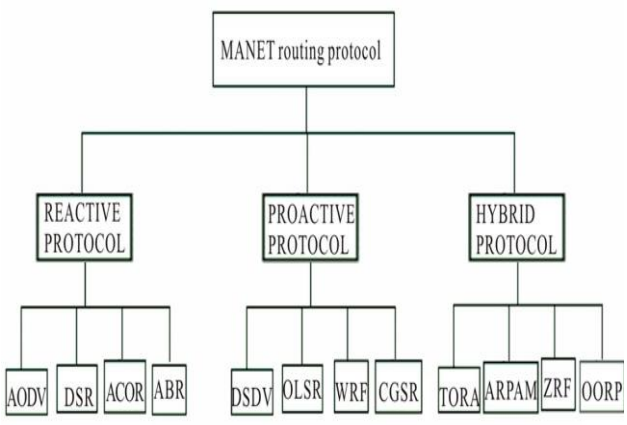


Fig.1. Classification of MANET routing protocol

Various factors like lack of centralized authority, power depletion, limited bandwidth and existence of a dynamic topology several attacks can be launched on an ad hoc network. These attacks can be categorized as:

Active and Passive attacks: In Active attacks, attacker actively participates in disrupting the normal operation of the network services by acting as an internal node in the network[1]. In passive attacks, the attacker does not actively participate in bringing the network down. It, however, listens to the network in order to know and understand, how the nodes are communicating with each other and how they are located in the network. Before the attacker launches an attack against the network, it already has ample information about the network so that it can easily hijack and inject attack in the network [1].

One of the most popular attacks is the Black Hole Attack which is going to be the focus of this review paper. In Black hole Attack, a malicious node uses its routing protocol primarily to advertise itself as having the best path to the destination node. Consequently the data packet transits through it and gets dropped thereby failing the network.

II. AODV OVERVIEW

AODV is a collaborative protocol, allowing nodes to share information about each other. Sequence Numbers are used by AODV to identify fresher routing information. Each node has to maintain its sequence number, incrementing it before sending either a new RREQ or RREP messages. AODV [2, 3, 4] is perhaps the most well-known reactive routing protocol for a MANET [5].

As AODV is reactive protocol, it does not give whole network topology view to nodes.
When source node requires transfer of a data packet to destination node it broadcasts a route request messages (RREQ) to all its neighbors. Then the neighbors also generate RREQ messages to all their neighbors to find the best, shortest and fresher route to destination node. As Destination node is reached, it Unicast a Route Reply messages RREP to the source node.

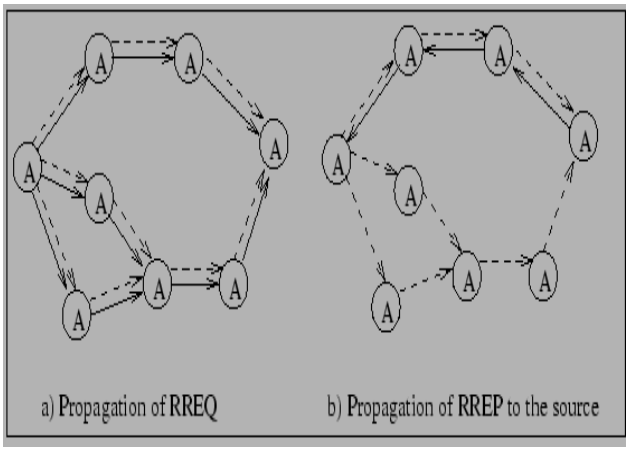


Fig.2. RREQ and RREP functioning in AODV

III.BLACKHOLE ATTACK

Black Hole Attack is basically a kind of DoS attack. It mainly takes over the command through the whole network and fails it .In AODV, *Black Hole* attack forges the sequence number and hop count of a routing message to forcibly acquire the route, and then eavesdrop on or drop all data packets that pass.

Behavior of Black Hole Attack is depicted in following figure:

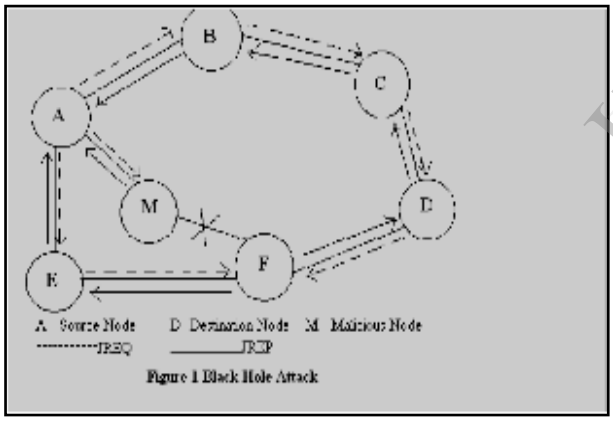


Fig.3. Black Hole attack effect

In above figure, A is plays a source node role , D is Destination node and M is playing a malicious node character. In this situation, malicious (fake) node M make use of the vulnerabilities of the route discovery packets of routing protocols to advertise itself as having the shortest path and a higher sequence number to the node A, whose packets it wants to intercept. Now A upon finding the shortest path to destination, without knowing that M is faulty node, transmits packet to M. M then receives the packet and retains it. As a result, the source and the destination nodes are unable to communicate with each other. Consequently the network's capability for handling packets slows down and power depletion grows, time exceeds and at the end network fails.

The malicious node always sends RREP as soon as it receives RREQ without performing standard AODV operations, while keeping the Destination Sequence number very high. Since AODV considers RREP having higher value of destination sequence number to be fresh, the RREP sent by the malicious node is treated fresh. Thus, malicious nodes succeed in injecting *Black Hole* attacks [6].

IV. RELATED WORK

Vipin Chand Sharma[7] proposed a method in which two new things, a new routing table RR-Table (Request Reply), a timer WT (Waiting Time) are added to the data structure of AODV protocol. In this method first Source Node sends a route request to all nodes within a specified time period .All route reply messages are stored into new routing table RR-Table (Request Reply). Then it compares the first destination sequence number with the source node sequence number. If there is a high difference between them then the node is considered to be a malicious node. Then that entry is removed from the RR-Table. This is how a malicious node is identified and removed from the RR-Table. The operation of the proposed method is same as the original AODV, once the malicious node has been detected.

Jaydip Sen[8] proposed a mechanism to remove cooperative Blackhole Attack from AODV . According to this mechanism AODV is modified by introducing two new concepts, (i) Data Routing Information (DRI) table and (ii) Cross Checking. In the proposed scheme, two bits of additional information are sent by the nodes that respond to the RREQ message of a source node during route discovery process. Each node maintains an additional data routing information (DRI) table. In the DRI table, the bit 1 stands for 'true' and the bit 0 stands for 'false'. The first bit 'From' stands for the information on routing data packet *from* the node (in the *Node* filed), while the second bit 'Through' stands for information on routing data packet *through* the node (in the *Node* field). So if the node is a malicious node it always shows 1,1 for both bit by which it can easily be verified after two or three step of cross checking by neighboring nodes.

Nirali Modi[9] proposed another method in which a Black hole AODV is developed that allows some degree of node maliciousness so as to give motivation to selfish nodes to state its malicious behavior to its neighbors for decreasing searching time of misbehaving nodes. In this model the trust among nodes is represented by a 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. Initially trust score of all nodes is 1. Then source send RREQ function () to all nodes. If neighboring node is the destination then it will send RREP message otherwise it forwards the RREQ Message. After that if the destination node is reached it will send REVERSE ROUTE REPLY function (). After receiving the reply then the decision will be taken whether the index node is destination or not using recvReply( ) function. If it is not destination then it will forward reply. In

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

Neelam Khemariya[10] proposed an algorithm to mitigate the effect of Black Hole Attack from AODV protocol. The beauty of the proposed algorithm is that it works in both the cases when there is no communication (i.e., a node is idle) and when a node is communicating (node is not idle). Firstly if communication interval time (CI) is greater than set threshold value (Th) the node is idle. Now the node sees the entries of the recent paths stored in its route cache and then sends RREQ packets to them and waits for the reply. Based on the reply it stores the entries in terms of the DSN in decreasing order and then calls the Black hole detection procedure. In Black Hole detection procedure if DSN is higher than other nodes sequence number then it is removed from node's entry. When a Node is not idle, then simply the Black Hole Detection procedure is invoked.

The important thing in this approach is that the RREQ packets are sent in Fibonacci series pattern till the Flow count Threshold (Fth) is not reached.

Vipin Khandelwal[11] proposed an algorithm in which three new terms are used : Waiting_REP_ time T,Store entry, new RREP table. First of all waiting time't' has already been set for source node then it sends RREQ message to all nodes. After receiving Reply source node it checks that REPLY messages arrived within time or not. If not it will not be saved into new RREP table. The Black Hole Detection Procedure starts on New RREP table in which comparison between Destination Sequence number from new RREP tab and Source Sequence Number has been done.

If destination sequence number is much higher than source sequence number, the source node discards this route entry in the new _ RREP _tab routing table. Source node performs this process for all RREP that are stored in a new_ RREP_tab until new_RREP_tab table is not empty.

V.SIMULATION PARAMETERS

As we know that AODV gets affected by *Black hole* attack, so here a simulation is done using OmNet++ to analyze the AODV routing performance under the influence of a *Black Hole* attack, by varying the node mobility speed.

SIMULATION PARAMETERS

Simulator	OMNET++
Transmission Range	300m
Traffic	Constant Bit Rate (CBR)
Routing Protocol	AODV
No.of Malicious Nodes	1
No. of Mobile Nodes	20 to 60
Pause time	30s
Packet Size	512 bytes

Table.1. parameters for simulation

The parameters which are used to evaluate the performance are:

1.) *Packet Delivery Ratio:* It is the ratio between the number of packets send by the source and the number of packets received by the destination.

2.) *Average End-to-End Delay*: This is the average delay between the sending of the data packet by the source and its corresponding receiver. It includes all the delays caused during route acquisition, buffering and processing at intermediate nodes, retransmission delays in milliseconds.

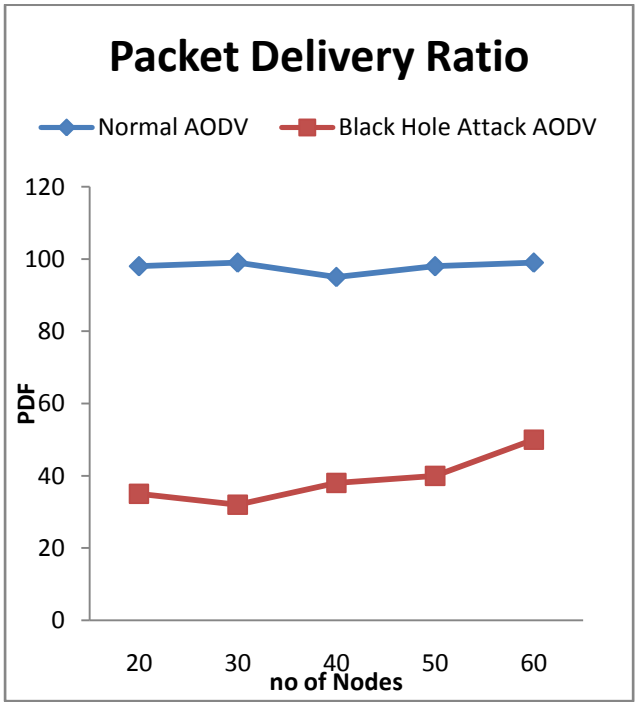
3.) *Throughput:* Also known as normalized throughput. It is the ratio of overall the number of packets received by the CBR sink to the number of packets sent by the CBR source.

VI.SIMULATION RESULTS

Results are shown in both cases : Normal AODV and Black hole Attack AODV . Due to this graph performance analysis can be measured . By this when a malicious node attack AODV, performance automatically reduced.

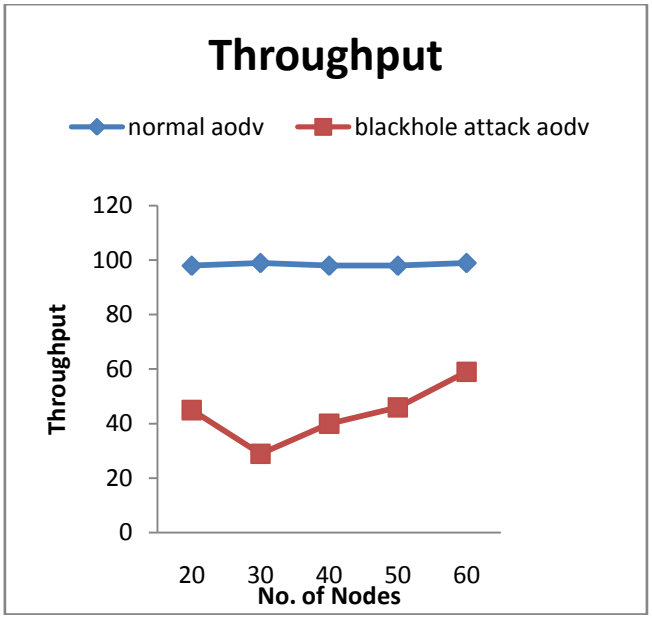
Malicious node is identified. Packet delivery Ratio is decreased, end to end delay also noticed and throughput also decreased.

1. Packet delivery Ratio Analysis



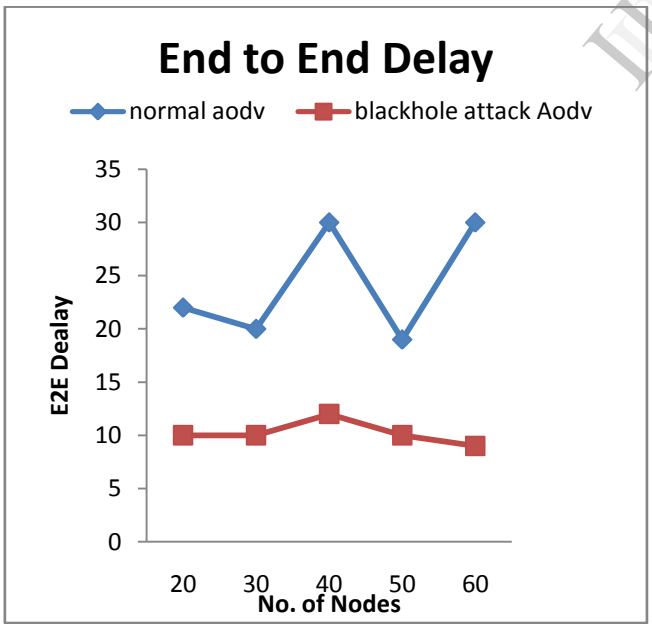
Graph .1. packet delivery ratio with attack and without attack

2. Throughput Analysis



Graph .2. Throughput with attack and without attack

3. End to End Delay Analysis



Graph .3. E2E Delay with attack and without attack

VII.CONCLUSION

In this paper, analysis of Black hole attack has done. Performance of AODV routing protocol has been analyzed into different scenarios like with Black Hole Attack or without Black Hole Attack. A lot of methods proposed to detect and remove black hole nodes from AODV were also discussed. From the graphs illustrated in results we can easily infer that the performance of the normal AODV drops under the presence of black hole attack.

VIII.REFERENCES

1. Harmandeep Singh, Gurpreet Singh and Manpreet Singh, **Performance Evaluation of Mobile Ad Hoc Network Routing Protocols Under Black Hole Attack**, *International Journal of Computer Applications*, Vol. 42(18):1-6, March 2012..
2. C.E. Perkins, E. Beliding-Royer, S. Das**, Ad hoc on-demand distance vector (AODV) routing**, IETF Internet Draft, MANET working group, Jan. 2004.
3. Latha Tamilselvan and Dr. V. Sankaranarayanan, **"Solution to Prevent Rushing Attack in Wireless Mobile Ad hoc Networks",** Ad Hoc and Ubiquitous Computing, December 2006, pp. 42-47.
4. J. Schiller, **"Mobile Communications",** Addison-Wesley, Pearson education August 2003.
5. Davide Cerri and Alessandro Ghioni, **"Securing AODV: The A-SAODV Secure Routing Prototype,"** IEEE Communications Magazine, February 2008
6. Ochola EO and Eloff MM , " **A Review of Black Hole Attack on AODV Routing in MANET**"
7. Vipan Chand Sharma* Atul Gupta Vivek Dimri," **Detection of Black Hole Attack in MANET under AODV Routing Protocol**", Volume 3, Issue 6, June 2013 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering
8. Jaydip Sen, Sripad Koilakonda, Arijit Ukil," **A Mechanism for Detection of Cooperative Black Hole Attack in Mobile Ad Hoc Networks**", IEEE 12/03/2010
9. Nirali Modi, Vinit Kumar Gupta," **Prevention Of Black hole Attack using AODV Routing Protocol in MANET**", Nirali Modi et al, / (IJCSIT) Vol. 5 (3) , 2014, 3254 – 3258
10. Neelam Khemariya, Ajay Khuntetha," **An Efficient Algorithm for Detection of Blackhole Attack in AODV based MANETs**", International Journal of Computer Applications (0975 – 8887) Volume 66– No.18, March 2013
11. Vipin Khandelwal, Dinesh Goyal ,"**BlackHole Attack and Detection Method for AODV Routing Protocol in MANETs**", ***IJARCET)*** Volume 2, Issue 4, April 2013.