ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 3, May 2013

EFFECTS OF BLACK HOLE ATTACKS IN AODV: A REVIEW STUDY

Er.AshuBansal, Er. Dinesh Kumar

M.Tech.*, Dept. of Computer Science & Engineering, PTU-GZS Campus, Bathinda, India

Assistant Professor, Dept. of Computer Science & Engineering, PTU-GZSCampus, Bathinda, India

ABSTRACT: An ad hoc network is a collection of mobile nodes that dynamically form a temporary network and are infrastructure less. A black hole is a malicious node that incorrectly replies the route requests that it has a fresh route to destination and then it drops all the receiving packets. So, a black hole attack is one kind of routing disturbing attack, and can bring damage to the network. The damage becomes more serious if group of malicious nodes comes together. This type of attack is known as co-operative black hole attack.Performance of the Black Hole ADOV protocol has been analyzed by varying the number of mobile nodes and black hole nodes. The protocol is analyzed on various performance metrics like packet loss, and throughout of network.

Keyword: Ad hoc network, black hole attack, MANET.

I.INTRODUCTION

Mobile ad hoc network (MANET) is a collection of mobile hosts without the required intervention of any existing infrastructure or centralized access point such as a base station.Nodes within each other's radio range communicate directly via wireless links, while those that are far apart use other nodes as relays. Nodes usually share the same physical media; they transmit and acquire signals at the same frequency band. However, due to their inherent characteristics of dynamic topology and lack of centralized management security, MANET is vulnerable to various kinds of attacks. As a result, an attacker can take advantage of flaws in routing protocols to carry out various attacks.

Security Issues: Security is much more difficult to maintain in Ad-hoc network as compare to wired network. Here, followings are the various vulnerabilities that exist in wireless ad hoc network:
Open Medium - Eavesdropping is easier than in wired network as there is no centralized medium.
Dynamically Changing Network Topology – Mobile Nodes comes and goes from the network. They dynamically change their topology. This allows any malicious node to join the network without being detected.
Cooperative Algorithms - The routing algorithm of MANETs requires mutual trust between the neighbor nodes which violates the principles of Network Security.
Lack of Centralized Monitoring – There is absence of any centralized infrastructure that prohibits any monitoring agent in the system.
Lack of Clear Line of Defense - The only use of I line of defense attack prevention may not secure. Experience of security research in wired world has taught us that we need to deploy layered security mechanisms because security is a process that is as secure as its weakest link. In addition to prevention, we need two lines of defense detection and response.

Realizing security in ad hoc environments is exceedingly difficult since many different types of ad hoc networks exist. Any variation is possible ranging from predominantly static sensor networks to highly mobile vehicular network scenarios. So, it is necessary to design specialized security solutions adapted to the underlying ad hoc network. Not only the network architecture has to face security threats, also the services and protocols used within the network have to withstand many different attacks.

II.INTERNAL BLACK HOLE ATTACK

As its name implies that, it is present in the network internally. Here the internal malicious node fits in between the routes of source and destination. As its present internally so this node make itself an active data route element. At this stage it is now capable of conducting attack with the start of data transmission. This is called an internal attack because here node

ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 3, May 2013

itself belongs to the network internally. Internal attack is more severe to attack because here malicious node present inside the network actively.

III.EXTERNAL BLACK HOLE ATTACK

External attacks physically stay outside of the network and deny access to network traffic or creating congestion in network or by disrupting the entire network. External attack can become a kind of internal attack when it take control of internal malicious node and control it to attack other nodes in MANET.

External black hole attack can be summarized in following points:

1. Malicious node detects the active route and notes the destination address.
2. Malicious node sends a route reply packet (RREP) including the destination address field spoofed to an unknown destination address. Hop count value is set to lowest values and the sequence number is set to the highest value.
3. Malicious node send RREP to the nearest available node which belongs to the active route. This can also be send directly to the data source node if route is available.
4. The RREP received by the nearest available node to the malicious node will relayed via the established inverse route to the data of source node. The new information received in the route reply will allow the source node to update its routing table.
5. New route selected by source node for selecting data. The malicious node will drop now all the data to which it belong in the route.

IV.ADOV PROTOCOL

An Ad-hoc network maintains a routing table, which contains routing information. Whenever a packet is to be sent by a node, it first checks with its routing table to determine whether a route to the destination is already available. If so, it uses that route to send the packets to the destination. If a route is not available or the previously entered route is inactivated, then the node initiates a route discovery process. A RREQ (Route Request) packet is broadcasted by the node. Every node that receives the RREQ packet first checks if it is the destination for that packet and if so, it sends back an RREP (Route Reply) packet. If it is not the destination, then it checks with its routing table to determine if it has got a route to the destination. If not, it relays the RREQ packet by broadcasting it to its neighbors.

An important feature of AODV is the maintenance of time-based states in each node: a routing entry not recently used is expired. In case of a route is broken the neighbors can be notified. Route discovery is based on query and reply cycles, and route information is stored in all intermediate nodes along the route in the form of route table entries. The following control packets are used: routing request message (RREQ) is broadcasted by a node requiring a route to another node, routing reply message (RREP) is unicast back to the source of RREQ, and route error message (RERR) is sent to notify other nodes of the loss of the link. HELLO messages are used for detecting and monitoring links to neighbors.

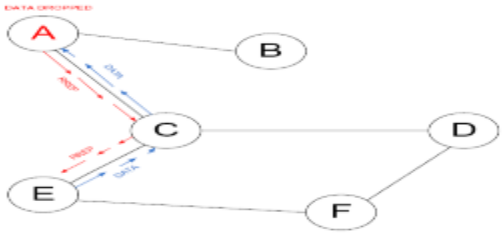

Figure 1: Black hole attack specification

In AODV black hole attack the malicious node “A” first detect the active route in between the sender “E” and destination node “D”. The malicious node “A” then send the RREP which contains the spoofed destination address including small hop count and large sequence number than normal to node “C”. This node “C” forwards this RREP to the sender node “E”. Now this route is used by the sender to send the data and in this way data will arrive at the 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.

ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 3, May 2013

An attacker node selectively drops RREQ/RREP packets. In this case in which the intruder drops packets by sending "Fake RREP" to the source node. In AODV after receiving a RREQ message, an inside attacker may forge a RREP message as if it had a fresh route to the destination node. In order to suppress other legitimate RREP messages that the source node receives from other nodes, the attacker forges a faked RREP message by increasing the destination sequence number. An attacker may disrupt the route between the victim nodes to a given destination, or invade in the route between by suppressing other alternative routes. These kinds of nodes are known as Black Hole nodes.
In figure below Node A which is a malicious node, can forge a RREP message to the source node S When source node S receives faked RREP message from node A, it updates its route to the destination node through attacking node. When node A receives the data packets it drops the packets as shown in fig below.
This attack drops the data packets in the network. Thus the packets in the network from source never reach the destination. A Black Holeattack forges the sequence number and hop count of a routing message to forcibly

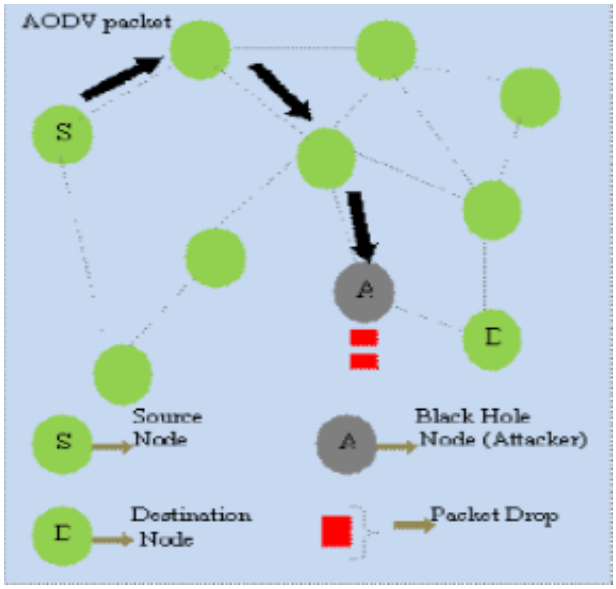

Figure 2. Black hole attack packet dropping

acquire the route, and then eavesdrop or drop all data packets that pass. A malicious node impersonates a destination node by sending a spoofed RREP to a source node that initiated a route discovery.

1. A Black Holenode has following two properties.

The node exploits the ad hoc routing protocol andadvertises itself as having a valid route to a destination,even though the route is Fake, with the intention ofintercepting packets.

2. The node consumes the intercepted packets.

The malicious node always sends RREP as soon as itreceives RREQ without performing standard AODVoperations, while keeping the Destination Sequencenumber very high. Since AODV considers RREPhaving higher value of destination sequence number tobe fresh, the RREP sent by the malicious node is treatedfresh. Thus, malicious nodes succeed in injecting BlackHoleattack.

V.CONCLUSION

The paper here mainly describes the major aspects of black hole attack in MANET such as how it is defined, its classification and how packets are dropped in the network. Future scope of paper is how to deal with black hole attack with zero packet loss.

REFERENCES

[1] AnuBala, Jagpreet Singh and MunishBansal "Performance Analysis of MANET under Blackhole Attack" First International Conference on Network and Communication 2009
[2] Mohammad Al-Shurman and Seong-Moo Yoon and Seungjin Park, "Black Hole Attack in Mobile Ad Hoc Networks"

ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 3, May 2013

[3] Dokurer .S, Y. M. Erten , Can ErkinAcar "Performance analysis of ad-hoc networks under black hole attacks", Turkey
[4] Dr. A.A.Gurjar, A.A.Dande "Black Hole Attack in MANET's", IJIEASR 2013.
[5] H. M. Deng, W. Li and Dharma P. Agarwal, Routing Security in Wireless Ad Hoc Networks. University ofCincinnati, IEEE Communication Magazine,Vol.40, no.10, October 2002.
[6] Payal N. Raj and Prashant B. Swadas,"DPRAODV: A dynamic learning system against black hole attack in AODV based Manet", International Journal of Computer Science Issues (IJCSI), Vol. 2, Issue 3, pp: 54-59, 2009
[7] S. Marti, T. J. Giuli, K. Lai, and M. Baker.Mitigating routing misbehavior in mobile ad hoc networks. In mobile Computing and Networking (MOBICOM), pages 255–265, 2000. Available on: citeseer.ist.psu.edu/marti00mitigating.html.
[8] S. Buchegger and J. Y. Le Boudec. A robust reputation system for mobile adhocnetworks.Technical Report IC/2003/50, EPFL-DI-ICA, July 2003.