AODV Routing Protocol under BlackHole Attack

Sai Swaroop Madugula, Anil Thota, Anil Govinda Reddy Mallidi.

Abstract: **With the advancement of Internet, the number of attack vectors on computer networks are rapidly increasing, the existing systems are typically focused on detecting and preventing one or two attacks but not on many different levels of attacks. The Ad Hoc on Demand Distance Vector Routing Protocol (AODV), which is an enhanced model of DSDV algorithm as well as minimizes the number of broadcasts by creating routes on-demand, is now a widely used on-demand routing in "MANET".**

Keywords—Ad-hoc networks, MANET, Network security, AODV , Black hole attack.

I. INTRODUCTION

The adverse attacks on computer networks are rapidly increasing. Most existing security solutions are not optimal to protect the existing systems.As the core device, routers are responsible for connecting different networks and forwarding data packets. In addition to dedicated router device, end nodes in networks such as ad hoc networks also perform as routers. The router as the core part is also vulnerable because of its critical role it plays. Generally, the TrsustRas data plane, control plane and management plane, the attacks can be categorized into their planes 1) unauthorized access to network resources, such as IP address spoofing; 2) Data-plane attacks to prevent data packets from being successfully delivered, such as Black Hole and Jellyfish; 3) Control-plane attacks to disturb or disrupt network operations, such as routing spoofing. The Implementation of cryptographic authentication mechanisms is used to prevent these sorts of attacks. These sorts of attacks are mostly successful because the authentication entities are always trusted because intruders cannot get authenticated, However emerging attack vectors such as persistent threats and social engineering attacks break up the foundation on which authentication is built upon by manipulating the compromised router systems through which intruders can bypass cryptographic mechanisms which is followed by more internal attacks until the entire system can be compromised, the trust management system comes to the rescue upon these kind of scenarios, it is introduced as second wall next to fire wall to provide extra protection which bypasses the firewall.

II. OVERVIEW OF AODV PROTOCOL

The Ad Hoc on Demand Distance Vector Routing Protocol (AODV), which is an enhanced model of DSDV algorithm as well as minimizes the number of broadcast by creating routes on-demand, is now a widely used on-demand routing in "MANET" [2]. MANET is regarded as a collection of mobile nodes that perform cooperation and communication with each other without relying on any pre-established infrastructure or centralized access points. As mobile nodes of MANET can communicate with each other without pre-existing infrastructure in many situations, it is widely applied in battlefields and the rescue scene of earthquake and flooding.

AODV mainly consists of two phases: route discovery and route maintenance phase. It defines four different types of control message, RREQ (Route Request), RREP(Route Reply), RRER (Route Error), and RREPBACK (Route Reply Acknowledgement) used in the route Discovery and route maintenance [3]. When the source hopes to send data to the destination but cannot find available route, it generates a RREQ packet and broadcasts it to its neighbors. The route discovery phase initiates. The node received the RREQ packet needs to establish a temporary reverse route to the previous node and then queries its routing table to see if there is any valid route to the destination. If there is, the node sends RREP to the source, otherwise, continues to broadcast the RREQ packet. The destination sends RREP packet when receives the RREQ packet. After receiving the RREQ packet, the source can create a route to the destination.

III. BLACK HOLE ATTACK

In computer networking, a packet drop attack or Black Hole attack is a type of denial-of-service attack in which a router that is supposed to relay packets instead discards them. This usually occurs from a router becoming compromised from several different causes. One cause mentioned in research is through a denial-of-service attack on the router using a known DDoS tool.Because packets are routinely dropped from a lossy network, the packet drop attack is very hard to detect and prevent.

The malicious router can also accomplish this attack selectively, e.g. by dropping packets for a network destination, at a certain time of the day, a packet every *n* packets or every *t* seconds, or a randomly selected portion of the packets. This is rather called a greyhound attack. If the malicious router attempts to drop all packets that come in, the attack can be discovered quickly through common networking tools such as traceroute. Also, when other routers notice that the compromised router is dropping all traffic, they will generally begin to remove that router from their forwarding tables and eventually no traffic will flow to the attack. However, if the malicious router begins dropping packets on a specific period or over every *n* packets, it is often harder to detect because some traffic still flows across the network.

The packet drop attack can be frequently deployed to attack wireless ad hoc networks. Because wireless networks have a much different architecture than that of a typical wired network, a host can broadcast that it has the shortest path towards a destination. By doing this, all traffic will be directed to the host that has been compromised, and the host is able to drop packets at will. Also, over a mobile ad hoc network, hosts are specifically vulnerable to collaborative attacks where multiple hosts will become compromised and deceive the other hosts on the network.

IV. METHODOLOGY

Here we try to understand and measure the performance of AODV under malicious blackhole node attack in wireless Ad-hoc networks. We use 10 nodes which implements AODV protocol to transfer packets from source to destination and simulate a Black Hole attack on the same. Using a Network Simulator(NS-2), we simulated malicious nodes attack on to 10 nodes. Below are various malicious attacks that are simulated.

1) Single Malicious Node
2) Multiple Malicious Nodes.

Below are the screens of the network simulator for above mentioned attack types.

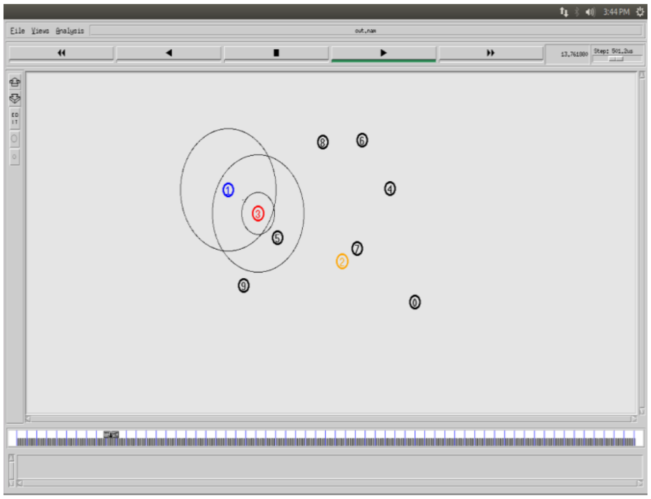

Figure.1 Single Malicious Node

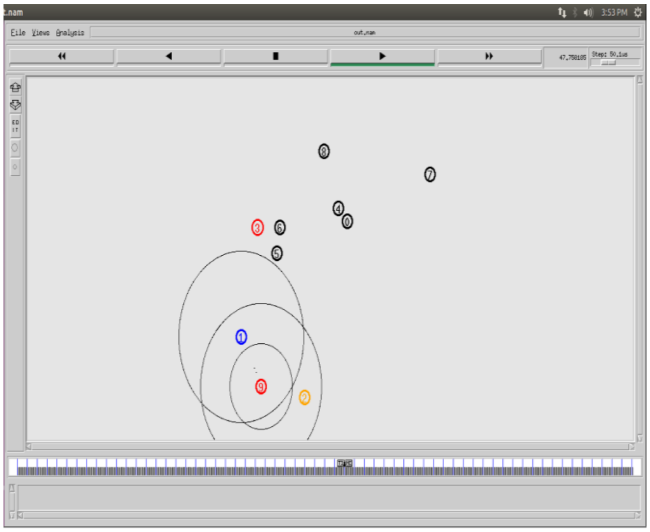

Figure.2 Multiple Malicious Nodes

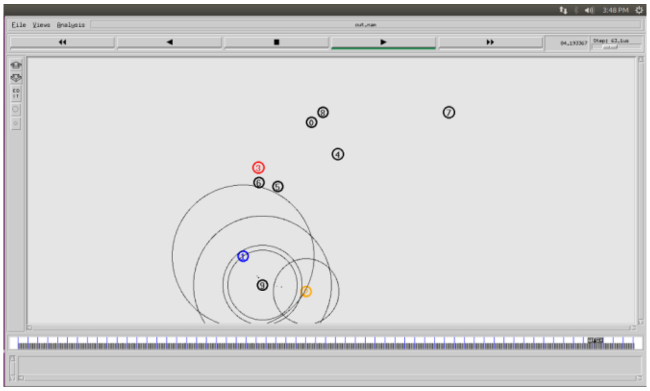

Figure.3 Singe Malicious Node Out of Range Delivery(S/D)

V.SIMULATION RESULTS

An Ad-hoc network topology with 10 nodes is built and with addition of two malicious nodes and the Ad-hoc On-Demand Distance Vector (AODV) routing protocol is employed. We use and modify an existing wireless networksimulator in NS2 for the simulation tests. The simulation time is 100s.

In this simulation we use NS2 and have take ten mobile nodes including the two malicious infected nodes and measure the performance of AODV routing mechanism under the Black Holeattack.

First, we simulate a normal AODV protocol without any interference of malicious nodes. Then, we calculate the total Packet Delivery Ratio (PDR) over the simulation time.

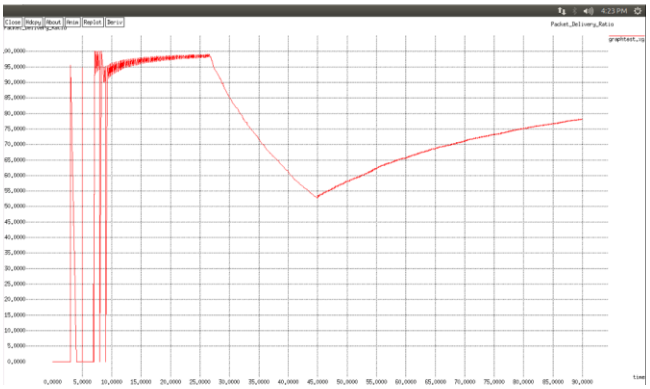

Figure.4 Normal AODV X-Graph

We, then, deploy Black Holeattack that drops all data packets needing to be forwarded, as seen in Figure.5. The same performance metrics are taken and the graph is generated.

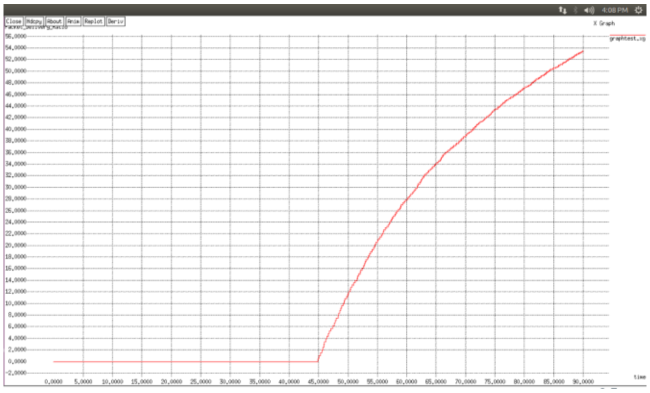

Figure.5 Single Malicious NodeX-Graph(PDR Vs Time)

VI. Conclusion

In our implementation, we have observed the performance of AODV in different scenarios of Blackhole attack. During a single malicious blackhole node attack, we have observed that the packet delivery ratio almost to drops to half. During multiple attacks however, the packet ratio drop to a total zero. We must keep in mind that the range of the node influences the packet delivery ratio very much. AODV protocol works in such a way that it takes a better route among the given two. Therefore, if the destination node is within range of the source node, then the source node will eliminate the need of an intermediate node all together and send the packets directly to the destination node. This way, in some cases, AODV protocol can avoid a blackhole attack.

VII.References

[1] Shuaishuai Tan, Xiaoping Li, and Qingkuan Dong, “TrustR:An Integrated Router Security Framework for Protecting ComputerNetworks” IEEE Commun. Lett., vol. 20, no. 2, pp. 376-379, Feb 2016.

[2] Meeta Singh, Jigyasa Sharma, “Performance analysis of secure and efficient Aodv (SE-AODV) with AODV routing protocol using NS2” January 2015.

[3] Monika Y. Dangore, Santosh S. Sambare “Detecting and Overcoming Blackhole Attack in AODV Protocol.” Pp. 77-82, Nov. 2013.

[4] Yingbin Liang, H. Vincent Poor, Lei Ying “Secrecy Throughput of MANETs Under Passive and Active Attacks.” IEEE Trans. On Info. Th. Vol.57, pp. 6692-6702, Oct 2011.

[5] Jian-Ming Chang ; Po-Chun Tsou ; Isaac Woungang ; Han-Chieh Chao ; Chin-Feng Lai, “Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach” IEEE Sys Journal vol. 9, pp.65-75, January 14.

[6] S. Krco, M. Dupoinov“Improved neighbor detection algorithm for AODV routing protocol“IEEE Commun. Lett., vol.7, pp.584-586, Dec 2003.