International Journal of Engineering Research in Electronic and Communication Engineering (IJERECE) Vol 2, Issue 11, November 2015

Effect of Black Hole attack on MANET routing protocols

[1] Akshata Prabhu[2] Shobha Krishnan
[1][2] Department of Electronics & Telecommunication
Vivekanand Education Society's Institute of Technology, Chembur, Mumbai
[1]Akshata.n.prabhu@gmail.com [2] shobha.krishnan@ves.ac.in

***Abstract:*— Mobile ad hoc networks are the extension of wireless networks. They play an important role in military applications, home applications etc. these networks are threatened by various security attacks such as Modification, Fabrication attack, Denial of Service attack, Sybil attack, Worm hole attack, Sleep Deprivation attack, Routing table Overflow etc. Black hole attack is an active attack on mobile ad hoc network. Due to its nature , the attacker makes the source node send all data packets to a Black-hole node that ends up dropping all the packets. In this paper an effect of black hole attack on Ad hoc on-demand distance vector routing protocol (AODV) and Ad hoc on-demand Multi path distance vector routing protocol (AOMDV) routing protocols will be studied. Effect of attack on parameters like dropped packets, throughput and end to end delay is analyzed.**

***Keywords*— Mobile ad hoc networks, Black hole attack, AODV, AOMDV**

I. INTRODUCTION

A Mobile Ad-Hoc Network (MANET) is a collection of wireless mobile nodes forming a temporary network without using centralized access points, infrastructure or centralized administration .All nodes having routing capabilities and forward data packets to other nodes in multi-hop transmission. Nodes can enter or leave the network at any time and may be mobile, so that network topology continuously changes. MANETs can be used in wide range of future applications as it has capability to establish networks at anytime, anywhere without the aid of established infrastructure. They have many potential applications, especially, in military and rescue areas such as connecting soldiers on the battlefield or establishing a new network in place of network which collapsed after a disaster like earthquake.

The nodes provide connectivity by forwarding packets over themselves in the network. To support this connectivity, nodes use various routing protocols such as AODV (Ad-hoc On-Demand Distance Vector), DSR (Dynamic Source Routing) etc.

As wireless ad-hoc networks lack infrastructure, they are exposed to lot of attacks. One of these attacks is the Black hole attack. In black hole attack, a malicious node absorbs all data packets in itself. In this way, all the packets are dropped. A malicious node dropping all the traffic in the network makes use of the vulnerabilities of the route discovery packets of on demand protocols, such as AODV. In route discovery process of AODV, intermediate nodes are responsible to find a fresh path to destination, sending discovery packets to the neighboring nodes.

Malicious nodes do not use this process and instead, they immediately respond to the source node with false information as though it has fresh enough path to the destination. Therefore source node sends its data packets via the malicious node to destination assuming it is a true path. The effect of black hole attack on two major routing protocols AODV and AOMDV is discussed.

II. MOBILE AD HOC NETWORK

A MANET is a self configuring network that does not require any pre-existent infrastructure, which minimizes their deployment time as well as cost. As each node in this network is free to move which makes the network to change its topology continuously. These infrastructure-less mobile nodes in ad hoc networks dynamically create routes among themselves to form own wireless network as shown in Figure 2.1.

Figure 2.1 Mobile Ad hoc Network

MANET is a dynamic wireless network formed by a set of mobile hosts which communicate among themselves by means of air without any pre-existing infrastructure.[1] Each node in the MANET can act as a router as well as host. In order to maintain connectivity in a mobile ad-hoc network all participating nodes have to perform routing of network traffic

III. ROUTING PROTOCOLS IN MAGNET

A routing protocol is used to discover routes between nodes in order to have communication within the network. The primary goal of such ad-hoc network routing protocol is to establish correct and efficient route between a pair of nodes so that messages may be delivered in a timely manner. Route construction should be done with a minimum of overhead and bandwidth consumption. The two major classifications of MANET routing protocols are unipath and multipath routing protocols

A. Unipath routing protocol

The unipath routing protocols discover a single route between a pair of source and destination. A new route discovery is required in response to every route break which leads high overhead and latency. The two components of unipath routing protocols are i) Route Discovery: finding a route between a source and destination. ii) Route Maintenance: repairing a broken route or finding a new route in the presence of a route failure.[2] AODV is the most widely used unipath protocol.

AODV is capable of both unicast and multicast routing. It is an on demand algorithm, meaning that it builds routes between nodes only as desired by source nodes. It maintains these routes as long as they are needed by the sources. Additionally, AODV forms trees which connect multicast group members. The trees are composed of the group members and the nodes needed to connect the members. AODV uses sequence numbers to ensure the freshness of routes. It is loop-free, self-starting, and scales to large numbers of mobile nodes.

B. Multipath routing protocol

The multipath routing protocols discover multiple routes between a pair of source and destination in order to have load balancing to satisfy Quality of Service (QoS) requirements. The three main components of multipath routing protocols are i) Route Discovery: finding multiple nodes disjoint, links disjoint, or non-disjoint routes between a source and destination. ii) Traffic Allocation: Once the route discovery is over, the source node has selected a set of paths to the Destination and then begins sending data to the destination along the paths. iii) Path Maintenance: regenerating paths after initial path discovery in order to avoid link/node failures that happened over time and node mobility.[2] AOMDV is the most widely used multipath protocol.

AOMDV protocol is an extension to AODV protocol for computing multiple loop-free and link disjoint paths. The routing entries for each destination contain a list of next-hops along with the corresponding hop counts. All next hops have the same sequence number. This helps in keeping track of the route. For each destination, a node maintains the advertised hop count, which is defined as the maximum hop count, for all the paths, which is used for sending route advertisements of the destination. Each duplicate route advertisement received by the node defines an alternate path to the destination. [3]

Loop freedom is assured for a node by accepting alternate paths to destination if it has less hop count than the advertised hop count for that destination. Because the maximum hop count is used, the advertised hop count therefore does not change for the same sequence number. When a route advertisement is received for a destination with greater sequence number, the next hop list and the advertised hop count are reinitialized. [3] Figure 3.1 shows an example for loop situation. Here node D is the destination node.

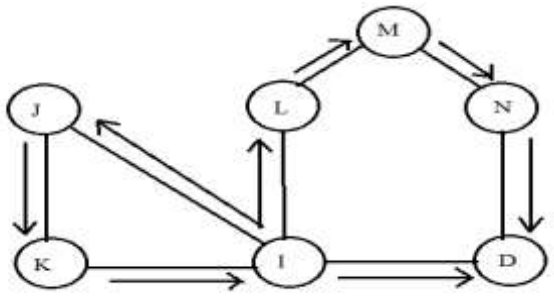

Figure 3.1 Example of routing loop scenario [4]

Node J has a three hop path to D via K (J-K-I-D). Node L also has a three hop path to D via M (J-M-N-D). Suppose I obtains a four hop path to D from L. In this case, I cannot ascertain whether or not L is an upstream node because J can also provide a four hop path to D. Therefore, accepting a longer path after having advertised a shorter path to neighbors may cause a routing loop.

IV. SECURITY ATTACKS IN MANET

Attacks in MANETs generally have two purpose and they are first is not to forward the packet or change the parameters of routing messages and to exhaust the battery of nodes by make them traversing the wrong packet in wrong direction and they also change the parameters of the packets such as sequence numbers and by using mechanism like authentication or cryptography as a preventive approach and can be used against attackers. [7] By means of these mechanisms we can only prevent attacks from outside but not from inside any node inside by using this information can cause hazards in
the network.

A. Black hole attack in MANET

In black hole attack, a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to intercept. This hostile node advertises its availability of fresh routes irrespective of checking its routing table. In this way attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it.

In protocol based on flooding, the malicious node reply will be received by the requesting node before the reception of reply from actual node; hence a malicious and forged route is created. When this route is establish, now it's up to the node whether to drop all the packets or forward it to the unknown address.

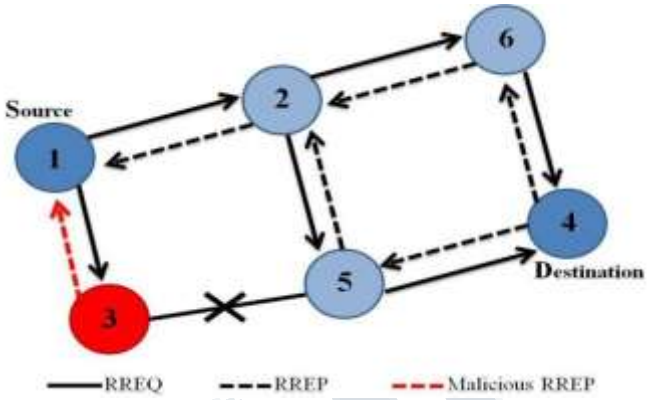

Figure 4.1Black hole attack [5]

The method how malicious node fits in the data routes varies. The above figure 4.1 shows how Black Hole problem arises, here node "N1" want to send data packets to node "N4" and initiate the route discovery process. So if node "N3" is a malicious node then it will claim that it has active route to the specified destination as soon as it receives RREQ packets. It will then send the response to node "N1" before any other node. In this way node "N1" will think that this is the active route and thus active route discovery is complete. Node "N1" will ignore all other replies and will start seeding data packets to node "N3". [8] In this way all the data packet will be lost consumed or lost

V. IMPLEMENTATION AND METHODOLOGY

To evaluate the effects of the Black Hole attacks in the Mobile Ad-hoc Networks Network Simulator-2 is used. NS-2 is an event driven network simulator program, developed at the University of California Berkley, which includes many network objects such as protocols, applications and traffic source behavior.

NS-2 is freely distributed. It is used as a network simulation tool for hypothesis testing.NS-2 provides faithful implementation of network routing protocols. The implementation of protocol is done using C++ language in the backend and TCL language in the frontend on the Ubuntu Linux 14.04 operating system.[9] The block diagram for implementation is as shown in Figure 5.1

.

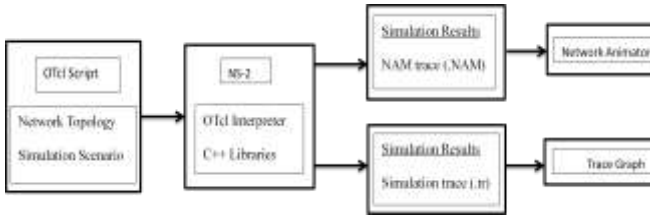

Figure 5.1 Block diagram for implementation

The user writes in TCL scripts which are interpreted by network simulator and give two output files. They are NAM and tr files. NAM is for visual animation of output and tr is large trace file consists of simulation results.

In this paper, an empirical study is done by simulation and analysis of Black hole attack on AODV and AOMDV routing protocol. The simulation work will be done in NS2 environment. Initially, simulation results for AODV and AOMDV without Black hole attack have been checked. Various scenarios are created. Based on the simulation results, QoS metrics such as Throughput, Delay and dropped packets are calculated. To analyze protocols various contexts are created by varying number of malicious nodes.

VI. SIMULATION AND RESULTS

In this section, the simulation environment and the simulation parameters are discussed. Simulation is done using Network simulator-2.34

The total number of nodes is 30. The number of attackers have been varied from 1 to 5.We have used constant bit rate connections with packet length of 250 kb. Each node independently repeats the behavior.[10]

Parameters	Values
Number of nodes	30
Traffic model	CBR
Routing protocol	AODV, AOMDV
Simulation time	100s
Number of sources	1

Table 1 Simulation Parameters

A.Throughput

. Throughput is the number of bits received over the time difference between the first and the last received packets. [11]

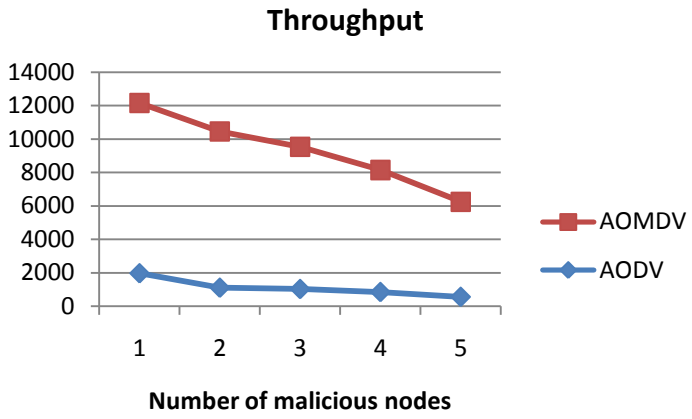

Figure 6.1 Throughput versus number of malicious nodes

It can be seen from the above graph that as the number of malicious nodes goes on increasing the throughput goes on decreasing. More the number of malicious nodes less is the throughput. The effect of attack on AOMDV is less as compared to that of AODV.

B. End to end delay

This is the average delay between the sending of packets by the source and its receipt by the receiver. It means it is the difference between the receiving time and sending time. This includes all the possible delays caused by buffering during data acquisition, route discovery, queuing, processing at intermediate nodes, retransmission delays, propagation time, etc.

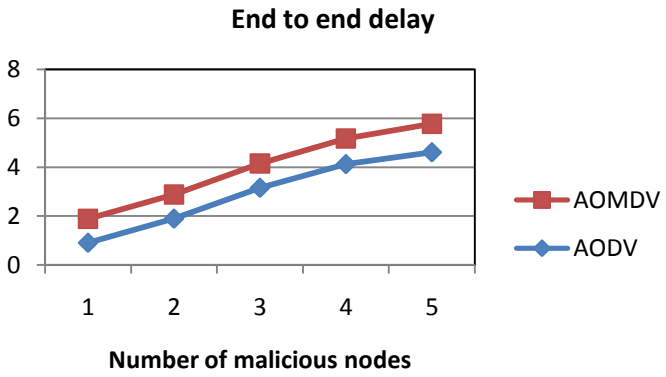

Figure 6.2 End to end delay versus number of malicious nodes.

From the above graph it can be seen that as the number of malicious nodes increases the delay between the

packets will increase i.e time taken by the packet to travel from source to destination will increase. The effect of black hole attack on AODV is more as compared to AOMDV as there are multiple paths in AOMDV.

C. Dropped packets

They are the number of packets which are dropped in the network due to collision.

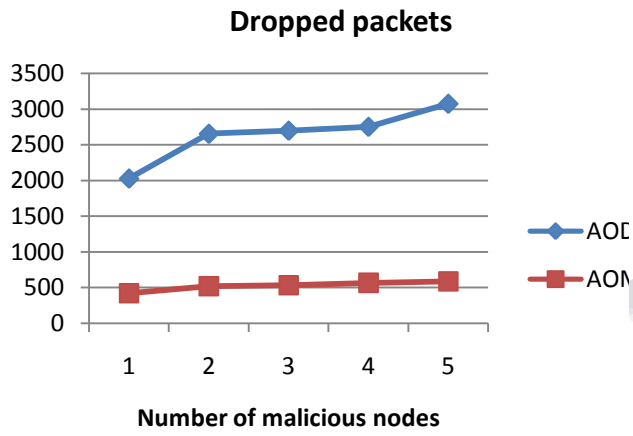

Figure 6.3 Number of malicious nodes versus dropped packets

It can be seen from the above graph that as the number of malicious nodes increases the dropped packets increases. More the number of attackers, more are the dropped packets.

VII. ANALYSIS

Comparison graphs have been made for AODV without attack, AODV with attack, AOMDV without attack and AOMDV with attack.

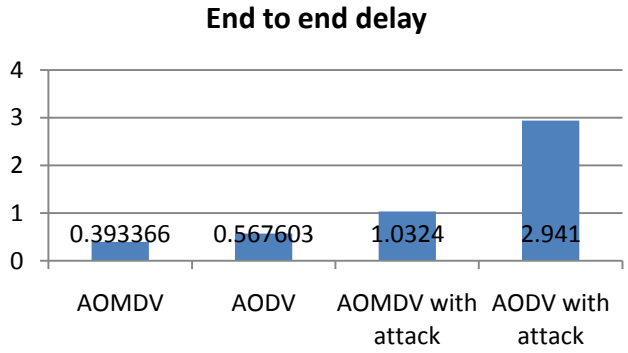

Figure 7.1 End to end delay

The above graph shows the variation in delay as per the changes made in the scenarios. The delay is minimum for AOMDV without attack and delay is maximum for AODV with attack. The impact of attack on AODV is more as compared to that of AOMDV.

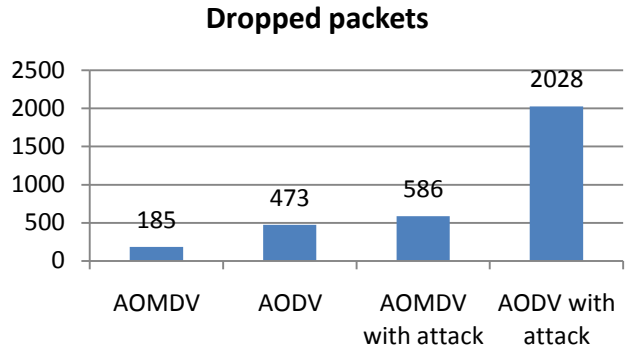

Figure 7.2 Dropped packets

The above graph shows the variation in dropped packets as per the changes made in the scenarios. The number of dropped packets is minimum for AOMDV without attack and dropped packets are maximum for AODV with attack. The impact of attack on AODV is more as compared to that of AOMDV.

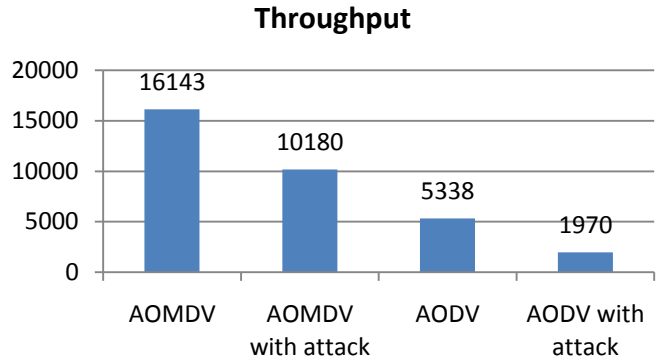

Figure 7.3 Throughput

The above graph shows the variation in throughput as per the changes made in the scenarios. The throughput is minimum for AODV with attack and throughput is maximum for AOMDV. The impact of attack on AODV is more as compared to that of AOMDV

VIII. CONCULSION AND FUTURE SCOPE

MANET has the ability to deploy a network where a traditional network infrastructure cannot possibly be

deployed. Security of MANETs is one of the important features for its deployment. In this paper we have studied the effect of black hole attack on the routing protocols AODV and AOMDV. We observed that the effect of attack was more on AODV as compared to AOMDV.

As a future work, ways has to be developed to find secured routes and prevent the black hole nodes in the MANET. This can be done by identifying the sequence number of the nodes.

REFERENCES

[1] Aditya Bakshi,A.K.Sharma,Atul Mishra ,"Significance of Mobile AD-HOC Networks (MANETS)," International Journal of Innovative Technology and Exploring Engineering (IJITEE),Volume-2,Issue-4,March 3013

[2] P.Periyasamy, Dr.E.Karthikeyan, "Performance Evaluation Of AOMDV Protocol Based On Various Scenario And Traffic Patterns," International Journal of Computer Science, Engineering and Applications (IJCSEA) Vol.1, No.6, December 2011

[3] R.Balakrishna, U.Rajeswar Rao, N.Geethanjali N, "Performance Issues Of AODV and AOMDV for MANETs", International Journal of Computer Science and Information Technologies" Vol.1,2010

[4] Mahesh K., Samir R. Das, "Ad-hoc on demand multipath distance vector routing." Wireless communication and Mobile Computing , Published online.

[5] Fan-Hsun Tseng, Li-Der, Han Chieh Chao, "A survey of black hole attacks in wireless mobile ad hoc networks", Human-centric Computing and Information Sciences.

[6] http://www.niksula.hut.fi/~janski/iwork/

[7] Ms nidhi Sharma, Mr Alok Sharma Das, "The black hole-node attack in MANET " 2012 Second International Conference on Advanced Computing and Communication Technologies.

[8] HimaniYadav,RakeshKumar,"Identification and Removal of Black Hole Attack for Secure Communication in MANETs", International Journal of computer science and Telecommunivation,Volume3,Issue 9,September 2012

[9] Atul Guptal, Vivek Damri,Vipan Chand Sharma "International Journal of computer Science and Software Engineering ", ISSN: 2277-128X, Volume 3, Issue 6, June 2013

[10] Pooja Jaiswal, Dr. Rakesh Kumar, "International Journal of computer Networks and Wireless Communications", ISSN: 2250-3301, Volume 2, No 5,October 2012

[11] Vasanthavalli.S , R.Bhargava Rama Gowd, "Pursue of Black hole attack and prevention using AODV on MANET " International journal of Innovative Research In Science, Engineering and Technology.

[12] http://www.isi.edu/nsnam/ns/tutorial/