ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 1, Issue 8, October 2012

Performance Evaluation of AODV under Blackhole attack in MANET using NS2 simulator

Ajay Sharma
ME Scholar
IES, IPS Academy Indore

Rajesh Babu Ahirwar
Asst. Professor, ECE Dept.
IES, IPS Academy Indore

Smita Patil
Asso. Professor, ECE Dept.
IES, IPS Academy Indore

***Abstract*—A wireless ad-hoc network is a temporary network set up by wireless mobile nodes moving arbitrary in the place that have no network infrastructure. Basically Wireless or mobile networks are evolved to replace the wired networks from traditional scenario to new paradigm. The mobile ad hoc networks are purely infrastructure less network. Due to this vulnerabilities of the network are unprotected to many attacks. In this paper we are discussing about Black hole attack. In this attack a malicious node advertises itself as having the shortest path to specific node to absorb packet to itself. So to identify the possibility of occurrence of black hole attack we simulate AODV protocol with NS2 tool. We also compare the simulation results of with & without Black hole attack in AODV protocol. Our simulation result are end-to-end delay, packet dropping, throughput of packet dropping ratio are justify that black-hole attack are observed.**

Keywords— Ad hoc Network, Blackhole attack, AODV, MANET.

I. INTRODUCTION

Ad hoc networks are limited capacity networks with no network infrastructure and no dedicated routing devices. Moreover, every node in such networks has to take care of its routing module itself. The main advantage of wireless network is communicating with rest of the world while being mobile. A Mobile Ad-hoc Network (MANET) is a collection of independent mobile users that communicate with available bandwidth and limited power. As the nodes in a MANET are mobile, the network topology may change rapidly [1]. The most important characterizing feature of a MANET is that no one among all has the central role. So there is a big scope of secure algorithm which can serve the best in this mobile scenario.

A MANET can also be known as the mesh network as these communicate with each other randomly and the routes of communication are created as per on-demand. The MANETs do not have to have the fixed infrastructure like a head/base station hence it provides very high flexibility and they communicate quickly and spontaneously. There are several routing protocols of MANET like AODV, DSDV, and DSR. Routing in ad-hoc network involves determining a path from the source to the destination data can be communicated and the delivery of the packets to the destination nodes while nodes in the network are moving freely. Due to this node mobility, a path established by a source may not exist after a short interval of time. To cope with node mobility, nodes need to maintain routes in the network [2]. Routing protocols for ad-hoc networks broadly fall into pro-active, reactive, hybrid and location-based categories depending upon how nodes can establish and maintain paths.

Pro-active routing protocols are table-driven protocols that maintain up-to-date routing table using the routing information learnt from the neighbors on a continuous basis. Routing in such protocols involves selecting a path form the source to the destination, where the source node and each intermediate node selects a next hop, by routing table look up, and forwarding the packet to next hop until destination receives the packet [3]. A drawback of such protocols is the proactive overhead due to route maintenance and frequent route updates to cope with node mobility. Examples of this class include DSDV, WRP.

Reactive routing protocols are demand-driven protocols that find path when necessary. In such protocols, establishing a new route involves a route discovery phase consisting of route request (flooding) and a route reply (by the destination node). Nodes maintain only the active routes until a desired period or until destination becomes inaccessible along every path from the source node. A drawback of such protocols is the delay due to route discovery. Examples of this class include AODV and DSR protocols [3] [4].

Hybrid protocols make use of both reactive and proactive approaches. Example of this type includes TORA, ZRP. Thus mechanism for ensuring packet delivery in Pro Active and Reactive can be apply together in this category [4] [5].

The paper is organized as follows: In section II, AODV routing protocol is discussed.. In section III , Black hole attack is explained. Section IV provides simulation parameters and results. Conclusion and future work is discussed in section V.

II. AODV PROTOCOL

In Ad-hoc On-demand Distance Vector Routing (AODV), a node discovers and maintains a route to the destination as and when necessary [6]. Every node in an Ad-hoc network maintains a routing table, which contains information about the route to a particular destination that is actively communicating with each other. Each entry in the routing table consists of the destination ID, the next hop ID, a hop count, and a sequence number for that destination. The sequence number helps nodes maintain a fresh route to the destination(s) and avoid routing loops. Thus, each node maintains a sequence number for itself and the respective source(s) and destination(s). A node increments its sequence

number if it initiates a new route request or if it detects a link-break with one of its neighbors.

Ad-Hoc On-Demand Distance Vector (AODV) is a dynamic protocol which actuates on demand routing algorithm and multi-hop routing between participating mobile nodes wishing to establish and maintain an ad hoc network. 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. To establish a path to the destination, a source node broadcasts a route request (RREQ) packet [6] [7]. The RREQ packet contains the source ID, the destination ID, sequence number of the source, and the latest sequence number of the destination node that is known to the source node. When a node receives a RREQ packet, it makes an entry for the route request in the route-request cache, and stores the address of the node from which it received the request as the next hop towards the source in its routing table. If receiving node is the destination or it has a fresh route to that destination1, then it responds with a route reply (RREP). Otherwise, it rebroadcasts the RREQ to its neighbors. When a node receives a RREP, it stores the address of the node from which it received RREP as the next hop towards the destination in its routing table and unicast the RREP to the next hop towards the source node. Once the source receives the RREP packet, it starts transmitting data packets along the path traced by the RREP packet. Due to the node mobility, path(s) established by a source node may break. When a node detects a path-break, it drops the packet for the destination and generates a route error (RERR) packet for the destination and sends the RERR to the source. Upon receiving a RERR, the source node buffers data packets for the destination and tries to re-establish a path to the destination. This is illustrated in figure 1.

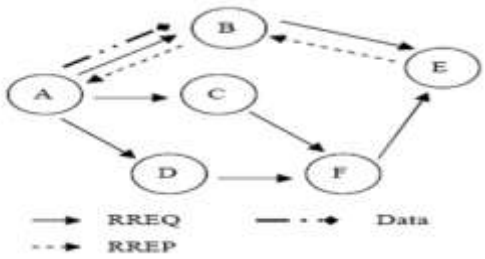

Fig 1: RREQ and RREP propagation from A to E

III. BLACK HOLE ATTACK

The Black Hole attack is a powerful attack in MANET. In this Malicious Node attract all traffic by claiming the route to the destination which then absorbs the packets without forwarding them to the destination. Co-operative Black hole means the malicious nodes act in a group.

The attacker injects falsified routing packets to attract traffic. The attacker intercepts or drops control as well as data packets to deny services to authentic nodes. This attack can be prevented by establishing routes free of such nodes or by removing them from existing routes [8]. In the following illustrated fig. 2, imagine a malicious node 'M'. When node 'A' broadcasts a RREQ packet; nodes 'B' 'D' and 'M' receive it. Node 'M', being a malicious node, does not check up with its routing table for the requested route to node 'E'. Hence, it immediately sends back a RREP packet, claiming a route to the destination. Node 'A' receives the RREP from 'M' ahead of the RREP from 'B' and 'D'.

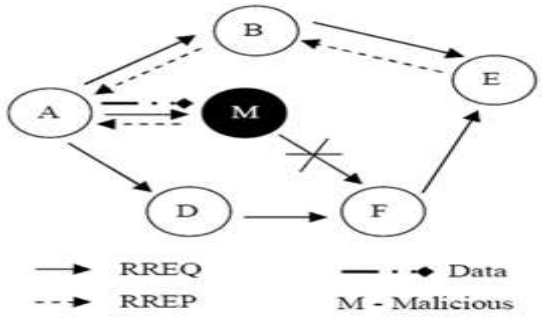

Fig 2: Black Hole Attack

Node 'A' assumes that the route through 'M' is the shortest route and sends any packet to the destination through it. When the node 'A' sends data to 'M', it absorbs all the data and thus behaves like a 'Black hole'. Researchers have proposed solutions to identify a single black hole node. However in that solution next-hop also behaves as a malicious node they cannot identify it.

IV. SIMULATION & RESSULT

The Routing protocols AODV is under the analysis for this paper. The Linux UBUNTU OS 12.04 LTS is used to run the Simulation Software NS2 (Network Simulator 2) version 2.35 for the performance evaluation. The performance is observed at various pause time and intervals with the number of nodes. In this situation 45 nodes will be simulated which move randomly 4500m X 3200 m range. There are modifications done to the original AODV.CC and AODV.H files of the NS2 to simulate the Black Hole behavior.

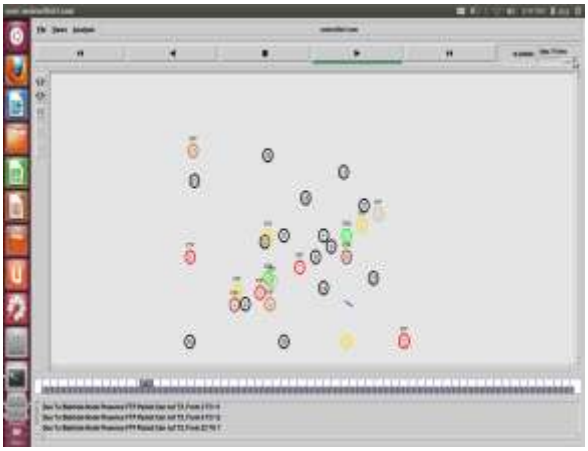

Fig 3: Simulation of AODV without black-hole attack

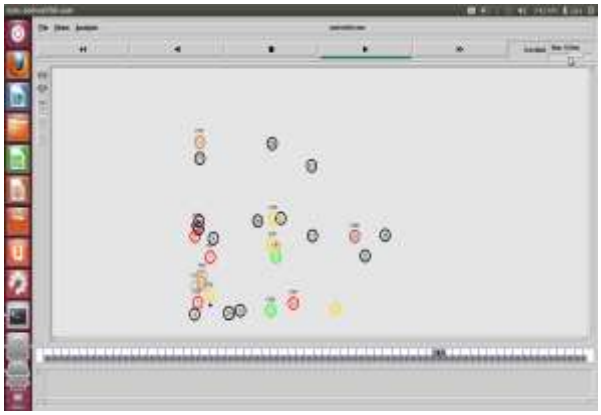

Fig. 4: Simulation of AODV without black-hole attack

The simulation parameters are shown in Table 1

Table 1: Simulation Parameters

Parameters	Ns-2
Examined Protocol	AODV
Simulation time	100 seconds
Number of Nodes	35
Transmission Range	250m
Movement Model	Random way point
Propagation model	Tow-Ray Ground Reflection
Traffic Type	CBR(UDP)
Payload size	512 bytes
Maximum speed	50m/s
Malicious nodes	1

The result of the simulation were analysed that packets are dropped and the performance is decreased to very low level. The performance throughput graph is plotted on the trace graph and the performance is analysed from this graph. The performance is hampered by the attack and the packet drop is pretty high as all the packets have been absorbed by the black hole node and are dropped. The node from which the data came is reported by the blackhole that the data have been successfully delivered or forwarded.

The following metrics are used to evaluate our protocol

Throughput:

Throughput of dropped packets can be tested with respect to simulation time. The graph shown that packet drop is in random fashion with respect to time.

Average End-to-End Delay:

End to end delay can be defined as the time a packet takes to travel from source to destination. In graph the end to end delay measured from source node with respect to time and delay as per the packet need to be delivered from source to destination. Average End-to-End Delay is the average of the end-to-end delays taken over all received packets.

Packet Drop:

Packet drop can be tested among per unit time and cumulative sum of number of dropped packets per unit time. It shows that as we increase time the packet drop effect shown significantly.

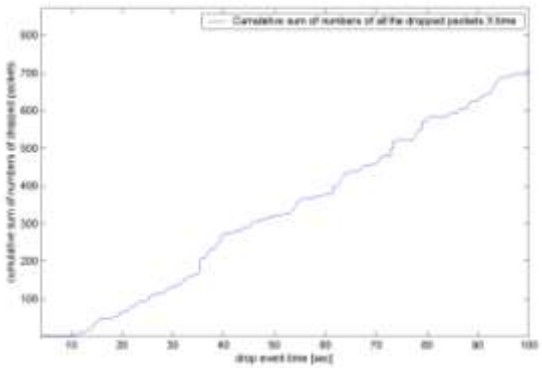

Fig 5: Average packet dropping ratio without Black Hole Attack

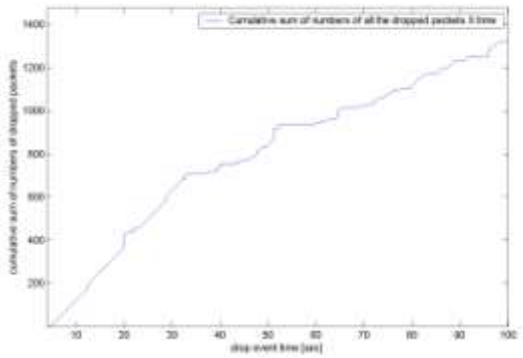

Fig 6 Average packet dropping ratio without Black Hole Attack

Fig 5 and Fig 6 shows the effect of packets dropped for AODV protocol when node mobility is increased. The result shows the cases, without black hole and with black hole attack on AODV. It has been measured that packets dropping are increased with black hole nodes in the Ad hoc network on AODV routing protocol as compared to without black-hole nodes.

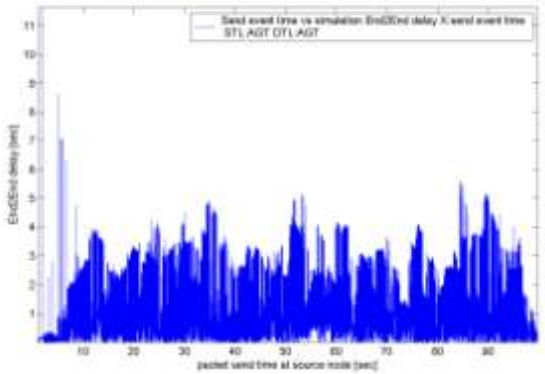

Fig 7: End-to-End Delay without Black Hole Attack

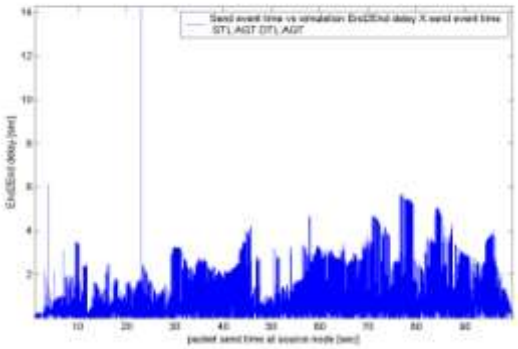

Fig 8: End-to-End Delay with Black Hole Attack

From the Fig 7 & Fig 8 it can be observed that, there is slight decrease in the average end-to-end delay without the effect of blackhole, as compared to the effect of blackhole attack, This is due to the immediate reply from the malicious node i.e. the nature of malicious node here is it would not check its routing table.

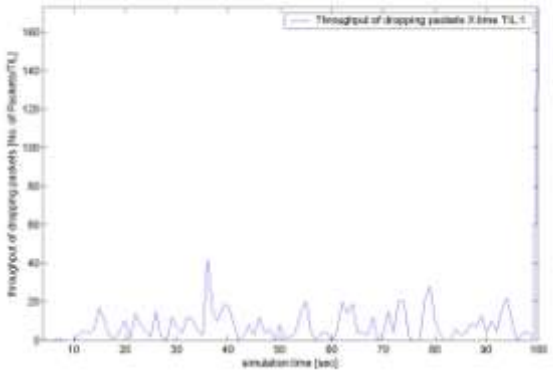

Fig 9: Throughput of dropping packets without Black hole attack

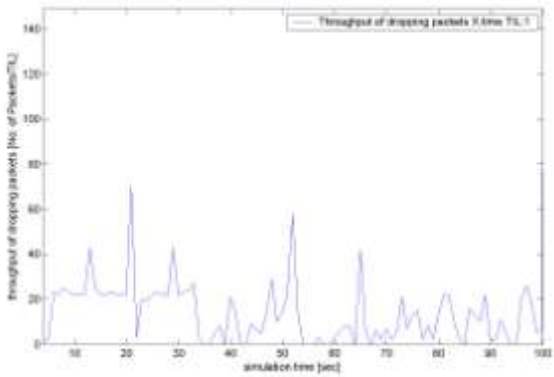

Fig. 10: Throughput of dropping packets with Black hole attack

It is observed from the Fig 9 & Fig 10 that, throughput of dropping packets between the nodes is more without the blackhole attack, as compared to the throughput of dropping packets between the nodes with the effect of blackhole attack. This is due to the malicious nodes provides the path with fewer number of nodes, or smaller path.

V. CONCLUSION & FUTURE WORK

This paper has described the performance evaluation of Ad hoc on demand distance vector routing protocol (AODV) under black hole attack. The simulation has been done using NS2 (Network Simulator 2) version 2,35 and the simulation result occurred at various levels of pause time with respect to average end to end delay, throughput, packet drop etc. The packet dropping clearly shows that Black hole attack has occurred. Simulation results show that the throughput is decreased with black-hole attack as compared to without black-hole attack. The future work can be done under blackhole attack by simulating this work with respect to risk mitigation, reputation index, node cooperation and trust across MANET nodes.

REFERENCES

[1] S. Corson and J. Macker, "RFC 2501Mobile Ad Hoc Networking(MANET): Routing Protocol Performance Issues and Evaluation Consideration ,"1999.

[2] Constantine Manikopoulos and Li Ling "Architecture of the Mobile Ad-hoc Network Security (MANS) System" CONEX Laboratory, NJWINS Center.

[3] Hsu J.,Bhatia S., Takai M.,bagrodia R. and Acriche M.J.,(2003),"performance of mobile Ad Hoc Networking routing protocols in realistic scenarios", proceeding of IEEE conference on military communications, Vol. 2,pp. 1268-1273.

[4] Hongmei Deng, Wei Li, and Dharma P. Agarwal, "Routing Security in Wireless Ad Hoc Networks", University of Cincinnati, IEEE Communications magazine, October 2002..

[5] V. Karpijoki, "Security in Ad Hoc Networks", Seminar on Net Work Security, HUT TML 2000.

[6] C.E. Perkins, S.R. Das, and E. Royer, "Ad-Hoc on Demand Distance Vector (AODV)", March 2000, http://www.ietf.org/internet-drafts/draft-ietf-manet-aodv- 05.txt

[7] Lidong zhou, Zygmunt J. Haas, "Securing Ad Hoc Networks", IEEE network, special issue, November/December 1999.

[8] D.Djen, L. Khelladi, and A.N. Badache, "A survey of of Security issues in Mobile Ad Hoc Network," Communication Surveys & Tutorials , IEEE, vol. 7 no. 4,2005,pp. 2-28.