Comparison of Performance of AODV Protocol under Black hole Attack on MANET

Shaba Praveen khan
Department of Computer Science and Engineering,
M ITM, Indore
Indore, India

Vinit Gupta
Department of Electronics Engineering
M ITM, Indore
Indore, India

Abstract

A mobile ad-hoc network (MANET) is a self-configuring infrastructure less network of mobile nodes. Since the nodes communicate with each other without an infrastructure, they provide the connectivity by forwarding packets over themselves. These nodes which communicate with each other are suspected to have the malicious behaviour. On of such type of attack is Black Hole Attack In this Attack a malicious node advertises itself as it is having the optimal route to the destination and this malicious node absorbs all data packets in itself, similar to a hole which sucks in everything in. As these data packets do not reach the desired destination the large amount of data is dropped hence data loss occurs.

In this paper the Black-Hole attack is simulated in the MANET using the AODV routing protocol in terms of throughput, End-to-End delay, packet delivery ratio and the analysis have been done with or without black hole attack .

Keywords- AODV; MANET; BLACK-HOLE; Malicious node.

1. Introduction

MANET is formed with wireless mobile nodes without pre-established infrastructure[1,2]. Some packets can be delivered from a source node to a destination node by way of various intermediate nodes, thereby maintaining network connectivity and applicability of MANET depends heavily on cooperation between nodes in such a dynamic environment . To support this connectivity, nodes use some routing protocols such as AODV (Ad-hoc On-Demand Distance Vector) [3], DSR
(Dynamic Source Routing) [4] and DSDV (Destination-Sequenced Distance-Vector)[5]. The security issues of MANETs are more challenging in a multicasting environment with multiple senders and receivers. However, in hostile environments, some nodes may deny to do so, either for saving their own resources or for intentionally disrupting regular communications. This type of misbehavior is generally referred to as black hole attack, which is considered as one of the most destructive attacks that leads to the network collapse [6].

2. AODV

Ad-hoc On-Demand Distance Vector (AODV) [7] Routing Protocol is used for finding a path to the destination in an ad-hoc network. To find the path to the destination all mobile nodes work in cooperation using the routing control messages. It employs destination sequence number to identify the most recent path. The major difference between AODV and other on-demand routing protocol is that it uses a destination sequence number (DestSeqNum) to determine an up-to-date path to the destination [8, 11].

Simple Hello messages are communicated in-order to detect and manage the neighbouring nodes. During the transmission of the HELLO message the active nodes periodically broadcasts the messages so that the neighbouring nodes responds accordingly [9].

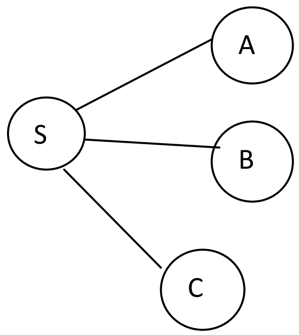

Figure.1 HELLO massage broadcast

When a source node desires a route to a destination for which it does not already have a route, it broadcasts a route request (RREQ) packet across the network. A node receiving the RREQ may send a route reply (RREP) if it is either the destination or if it has a route to the destination with corresponding sequence number greater than or equal to that contained in the RREQ. Once the source node receives the RREP, it may begin to forward data packets to the destination. If the source later receives a RREP containing a greater sequence number or contains the same sequence number with a smaller hop count, it may update its routing information for that destination and begin using the better route[10].

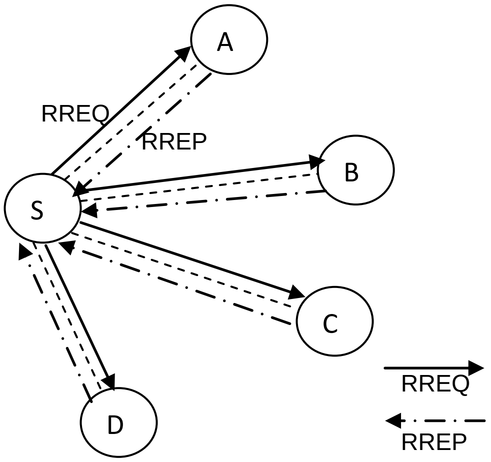

Figure 2. AODV RouteRequest (RREQ) and RouteReply(RREP) massage

When a path breaks between two nodes, both the nodes initiate RouteError message to inform their end nodes about the link break. The end nodes delete the corresponding entries from their tables.

3. Black Hole Aattack

The Black Hole attack is a kind of Denial of Service (DOS) attack. In this attack a Malicious Node falsely advertises good path (shortest path or most stable path) to the destination node during the path finding process (in on-demand routing protocol) or in the route update massage (in table-driven routing protocol). The intention of the malicious node could be to hinder the path-finding process or to intercept all data packets being sent to the destination node concerned [11].

The malicious node is the part of the network will also going to receive the RREQ packets from the transmitting node. Since these Black Hole node respond to the RREQ packets it immediately sends out the RREP packets to the transmitting node. When the RREP messages are received the node starts transmitting the data packets. On receiving the data packets the Black Hole node simply drops the packets instead of forwarding to the required destination.

A malicious node M can carry out many attacks against AODV. When source node S broadcasts a RREQ packet, nodes A, B, C and 'M' receive it. Node 'M', being a malicious node, does not check up with its routing table for the requested route to node B. Hence, it immediately sends back a RREP packet, claiming a route to the destination. Node S receives the RREP from 'M' ahead of the RREP from A, B and C. Node S assumes that the route through 'M' is the shortest route and sends all packets to node 'M'. When the node S sends data to 'M', it absorbs all the data without forwarding data to destination and thus behaves like a 'Black hole'.

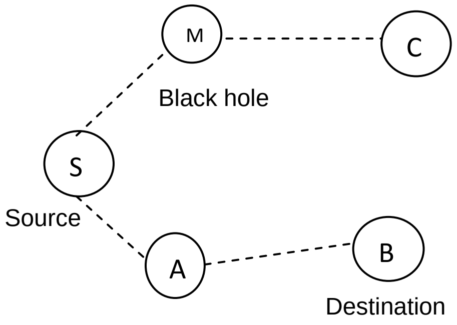

Figure 3. Black hole attack

4. Simulation of black Hole attack

The Routing protocol AODV is under the analysis for this paper. The Linux UBUNTU OS10.10 is used to run the Simulating Software NS2 (Network Simulator 2) version 2.34 for the performance evaluation. The performance is observed at various pause time and intervals with the number of nodes. In this situation 30 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 behaviour.

Table 1. Simulation parameter

Examined Protocol	AODV
Simulation time	100 seconds
Number of Nodes	30
Transmission Range	250m
Movement Model	Random way point
Propagation model	Tow-Ray Ground Reflection
Traffic Type	CBR(UDP)
Payload size	512 bytes
Maximum speed	20m/s
Malicious nodes	1

5. Results

The result of the simulation were analysed for various time span, the performance of the AODV goes down to 40% - 60%. This means packets are dropped and the performance of the network decreased to very high level. The performance graphs is plotted on the trace graph and the performance is analysed from this though graphs.

Throughput:

It indicates the fraction of channel capacity used for successful data transmission.

Average End-to-End Delay:

End-to-End Delay can be defined as the time a packet takes to travel from source to destination. Average End-to-End Delay is the average of the end-to-end delays taken over all received packets.

Node Mobility:

Node mobility indicates the mobility speed of nodes.

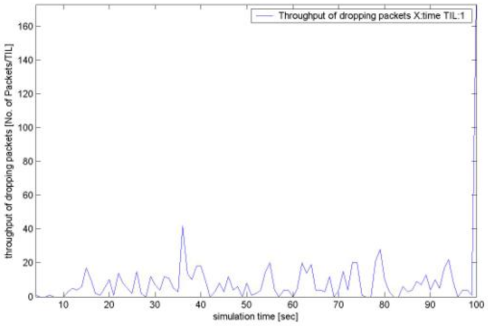

Figure 4. Throughput of dropping packets without Black hole attack

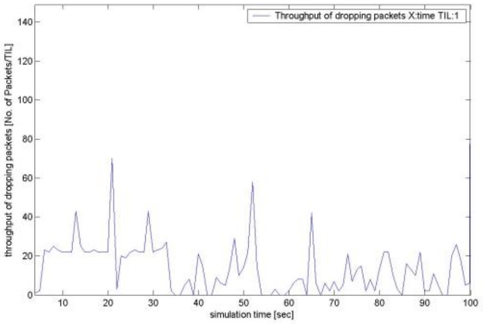

Figure 5. Throughput of dropping packets with Black hole attack

Figure 4 and 5 shows the effect of throughput 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 throughput decreases with black hole nodes in the Ad hoc network on AODV routing protocol as compared to without blackhole nodes.

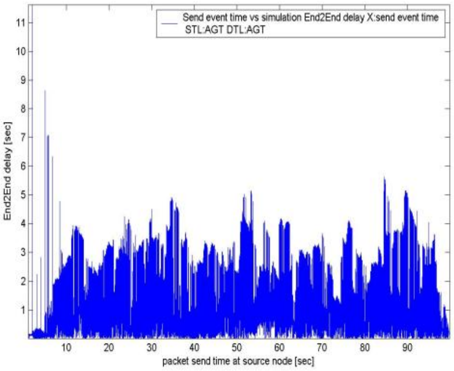

Figure 6. End-to-End Delay without Black Hole Attack

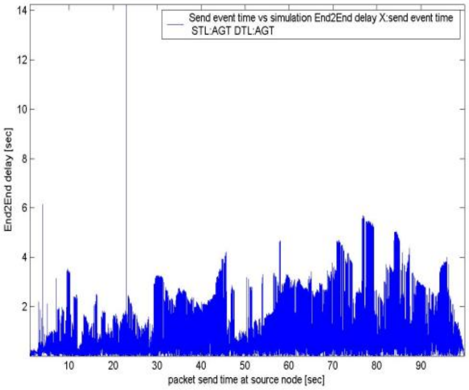

Figure 7. End-to-End Delay with Black Hole Attack

From the figure 6 to 7 it can be observed that, there is slight increase in the average end-to-end delay without the effect of black hole, as compared to the effect of black hole 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

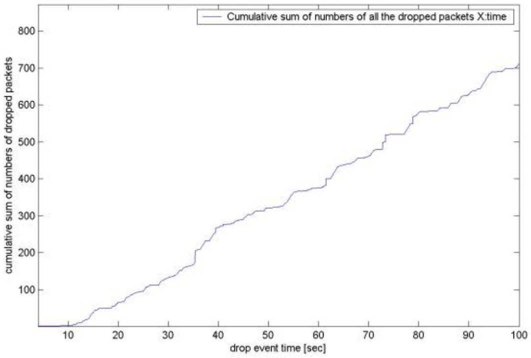

Figure 8. Average packet dropping ratio without Black Hole Attack

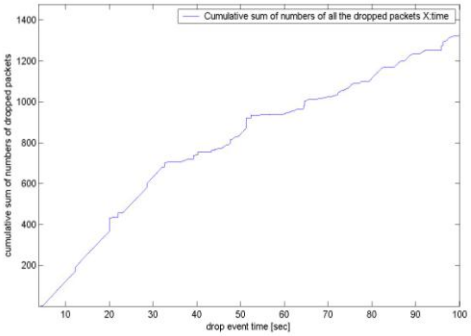

Figure 9. Average Packet dropping Ratio With black hole attack

It is observed from the figure 8 that, average packet dropping ration between the nodes is less without the black hole attack, as compared to the Average Packet dropping ratio between the nodes with the effect of black hole attack in figure 9. This is due to the malicious nodes, which drop all incoming packets so that the packet dropping ratio is increase.

6. Conclusion

MANET nodes are highly mobile, and this mobility produces network security problems. In Black hole attack all network traffics are redirected to a specific node or from the malicious node causing serious damage to networks and nodes as shown in the result of the simulation. In this paper the effect of packet delivery ratio, Throughput and End-to-End Delay has been detected with respect to the variable node mobility. There is deduction in Packet Delivery Ratio, Throughput and slight increase End-to-End Delay, as shown in fig. 4-9. The detection of Cooperative Black holes in ad hoc networks is still considered to be a challenging task, but prevention of the Black Hole Node is another future work

References

[1] D. D. Perkins, H. D. Hughes and C. B. Owen, "Factors Affecting the Performance of Ad Hoc Networks," Proceedings of the IEEE International Conference on Communications (ICC), 2002, pp.2048-2052.

[2]I. Chlamtac, M. Conti and J. J.-N. Liu, "Mobile Ad hoc networking imperatives and challenges" Ad Hoc Networks, Vol 1, 2003, pp.13-64.

[3]C. E. Perkins and E. M. Royer, "Ad hoc On-DemandDistance Vector Routing (AODV) ", IETF RFC 3561, 2003.

[4]D. B. Johnson, D. A. Maltz, and J. Broch, "DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks", Ad Hoc Networking,Addison-Wesley, 2001 pp. 139-172

[5] C.E. Perkins and P. Bhagwat″ Highly Dynamic Destination-Sequenced Distance Vector Routing(DSDV) for Mobile Computers″, ACMSIGCOMM Conferenc on Communications Architectures,Protocols and Applications, 1994, Vol. 24, pp. 234-244.

[6] S. Djahel, F Na¨ıt-abdesselam, Z. Zhang" Mitigating Packet Dropping Problem in Mobile Ad Hoc Networks: Proposals and Challenges" *IEEE COMMUNICATIONS SURVEYS & TUTORIALS, ACCEPTED FOR PUBLICATION*, 6 June 2010.

[7] C. Perkins, "(RFC) Request for Comments – 3561", Category: Experimental, Network, Working Group, July 2003.

[8] C. E. Parkins and E. M. Royer. "Ad hoc On-Demand Distance ", *Proceeding of IEEE workshop on mobile computin System and Applications 1999, pp,90-100,* Ferbary*1999.*

[9] M. Rastogi, K. K. Ahirwar, A. Bansal H. "Traffic Generator Based Performance Evaluation of Proactive and Reactive Protocols of Mobile Ad-Hoc Networks" International Journal of Scientific & Technology Research Vol. 1, Issue 4, MAY 2012.

[10] http://moment.cs.ucsb.edu/AODV/

[11] C. Siva Ram Moorthy, B. S. Manoj: Ad hoc Wireless Networks Architectures and Protocols, Prentice Hall, 2004.