A Reliable Analysis in MANET using AODV Protocol with Black Hole Attack

Kumari Parveen [1], Aggarwal Gaurav [2] , Singh Sugandha [3]

[1] Research Scholar (CSE), Jagannath University,Jhajjar

[2]Professor & Head Department of CSE, ,Jagannath University Jhajjar,

[3]Prof. (CSE), G.H. Raisoni College Of Engineering, Nagpur.

Abstract - Mobile Ad hoc network is a wireless network in which all nodes set the routes among themselves to form a better network for communication. In this paper, the performance of MANET is analysed using AODV protocol and that performance compared with the blackhole approach in terms of PDR(Packet Delivery Ratio) and PDR is more in AODV than blackhole attack. So the security and communication is better in AODV which also provides the less energy consumption. NS-2 simulator is used for simulation and to plot the graphs.

Keywords: MANET, AODV, Blackhole, NS-2

1. Introduction

MANET is the network which is formed without wires. It is also called a self organized or infra-structure less network[3]. This network consists of only the nodes and there is no central node in the network which guides other nodes for communication. These nodes acts as routers and communicate with each other. The main purpose of this network is to deliver the correct messages between the nodes within the time[4]. A routing protocol is also required to establish a route between the nodes. A black hole is a malicious node which creates the problem for the transferring data packets[9]. A black hole attack is referred to the malicious node which dropped all packets in itself just like a hole without informing the sender about the failed delivery. In this paper, routing protocol AODV is used to compare the performance in the form of PDR of the protocol with black hole attack. The paper is summarized as: section 2, explains the AODV[1]. Section 3, describe black hole. Section 4, describes the evaluation and simulation of result and section 5 concludes the paper.

2. Ad hoc On Demand Distance Vector (AODV)

AODV is used to establish and maintain an ad hoc network between mobile nodes with multi-hop routes. . AODV is reactive that means a route is only requested according to the requirement but not maintained[1] while DV (Distance Vector) is proactive. AODV works on RREQ (Route Request) and RREP (Route Reply) messages[2]. RREQ message is broadcasted when a node wants to find a route to another node. RREQ generates through the network until it reaches the destination and then the route is made available by uni-casting a RREP back to the source. As a RREQ message is received by a node, then the route reply is uni-casted back by using the same path which is used by route request.

2.1 Functions Performed by AODV:

a) Route Management Table - The informations which are kept by this table for each route is IP address of the destination node, Sequence number of the destination node, Number of hops to destination, The next hop that is the neighbour node

which forward the packets to destination, Route lifetime means the valid time of the route, The active neighbour nodes which use the route entry, Request buffer makes sure that a request should be processed only once.

b) Route Discovery - A RREQ is broadcasted when the node requires a route to the destination but no route is available, then there is two possibilities either the RREP is received within the limited time or it is considered that no route is exist. The node again sends RREQ and a temporary reverse route is created by the node. In routing table, the source IP address with the next hop equal to IP address field of neighbouring node that broadcast RREQ [5].

When RREQ reaches to a node that may be the destination node or another node with a valid route to destination, a RREP is generated and send back to requesting node. When this RREP is forwarded, a route is created to destination and then RREP reaches to source node, where a route from the source to destination is already exist.

c) Route Maintenance - When a route is no longer from a node to the neighbour node, then the routing entry will be removed and link failure message is sent. AODV has a active neighbour list which keeps the record of neighbouring nodes with their particular routes. The nodes which receives the link failure message will repeat this procedure. The affected sources also receive this message that may either stop data sending or requesting for new route by sending a new RREQ.

3. Black Hole

Black hole is that place in network where the transferred data is dropped without informing the se. Black holes are the invisible places which are only noticed by tracking the lost traffic[5]. It has a null (black hole) route that goes nowhere , its only work is to drop the matching packets(known as filtering process) at routing level using routing protocol to implement this filter process on all routes at a time. Null routes have the no impact on the performance of routing protocol.

3.1 Attack of Black Hole

The attack on the incoming or outgoing traffic made by that particular node which exist at the place of black hole in the network is known as black hole attack[6]. That node creates the problem for route discovery packets as per requirement of on demand protocols but in AODV protocol, intermediate nodes have the responsibility to find the new path to the destination for sending the discovery packets to the neighbour node but the malicious node do not use the process of fresh path, it sends the false information of no route is available to the sender although there is a fresh route available for the destination.

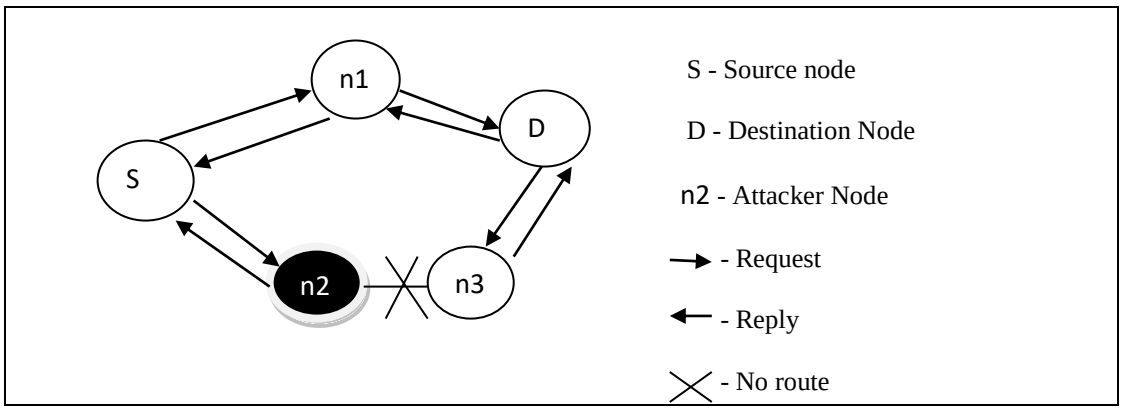

Figure 1. Black Hole Attack

4. Evaluation and Simulation of Result

Comparison of basic AODV protocol with AODV under blackhole is evaluated and simulated by NS-2 and the performance is shown by graph.

Simulation Parameters Table :

Topology	500 m × 500m
Number of Nodes	8,16,24,32
Antenna Type	Omni Antenna
Simulation time(s)	100 s
Initial Energy(Joule)	100 joule
MAC Type	Mac/802_11
Simulated Routing Protocol	AODV
Performed Evaluation Metrics	Packet Delivery Ratio

4.1 Packet Delivery Ratio

The ratio between the number of packets originated by the source and the number of packets received at the destination[8]. As shown in figure 2, more packets are delivered in basic AODV as compared to black hole attack. So the performance is better in AODV than black hole attack.

Figure 2. Network nodes Vs. Packet Delivery Ratio

5. Conclusion

In this paper, a reliable analysis of performance in MANET between basic AODV and with black hole is evaluated and it is cleared that the performance is better as packet delivery ratio in basic AODV as compared to the black hole attack. So the communication is more reliable in MANET with AODV protocol.

References

[1] Singh, S., Rajpal, N., Sharma, A.: Address allocation for MANET merge and partition using cluster based routing. http://www.springerplus.com/content/3/1/605.

[2] Parveen Kumari, Gaurav Aggarwal, and Sugandha Singh," Clustering in Mobile Adhoc Network:WCA Algorithm" in proceedings of J. Hemanth et al. (Eds.): ICICI 2018, LNDECT 26, pp. 525–533, 2019. https://doi.org/10.1007/978-3-030-03146-6_58.

[3] Parveen Kumari, Sugandha Singh, and Gaurav Aggarwal," Energy Efficiency Analysis of Cluster Based Routing in MANET" S. Balaji et al. (Eds.): ICICV 2019, LNDECT 33, pp. 460–469, 2020. https://doi.org/10.1007/978-3-030-28364-3_46.

[4] Parveen Kumari, Gaurav Aggarwal and Sugandha Singh," Swarm optimized energy efficient clusters for MANET", published In JETIR (www.JETIR.org) ISSN UGC Approved (Journal No: 63975) & 5.87 Impact Factor Published in Volume 6 Issue 6 , June 2019 | Date of Publication: 2019-06-07. http://doi.one/10.1729/journal.23261.

[5] S. Mehta, M.Sharma,"Analysis of Black Hole and Wormhole Attack using AODV Protocol"International Journal of Research in Management, Science & Technology (E-ISSN: 2321-3264) Vol. 1; No. 1, June 2013.

[6] Dokurer, Semih, "Simulation of Black Hole Attack In Wireless Adhoc Networks", September 2006.

[7] D. Koshti,"Comparative study of Techniques used for detection of Selfish Nodes in Mobile Ad hoc Networks", International Journal of soft Computing and Engineering (IJSCE) ISSN: 2231-2307,2011.

[8] A. Mishra,"Security and Quality of Services in Ad hoc Wireless Networks", 2008.

[9] Li Zhao, "MARS: Misbehavior Detection in Ad hoc Networks", Global Telecommunication Conference, 2007. GLOBECOM'07. IEEE, 26-30 Nov. 2007,941- 945.