International Journal of Engineering Research and Modern Education (IJERME)
ISSN (Online): 2455 - 4200
(www.rdmodernresearch.com) Volume I, Issue I, 2016

PERFORMANCE STUDY OF IMPROVED AODV AGAINST BLACK HOLE ATTACK IN WIRELESS ENVIRONMENT

Piyush Khemariya*, Upendra Kumar Purohit & Umesh Barahdiya*****

Electronics and Communication Engineering, Nagaji Institute of Technology and Management, Gwalior, Madhya Pradesh

Abstract:

In this paper author analyzed the effect of black hole attack using AODV routing protocol. The simulation has been done using the network simulator .The performance metrics like average end to end delay, packet delivery ratio and routing overhead has been detected and analyzed with the variable node mobility. The simulation results shown in the result section that when the black hole node exists in the network, it can be affected and decreased the performance of AODV routing protocol. So, the detection and prevention of black hole attack in the network exists as a challenging task, implement alternative path in AODV, And Author performs the solution for the black hole attack and compares its performance with the AODV protocol.

Key Words: Black Hole Attack, AODV, Multipath AODV, MANET & Performance Matrices

1. Introduction:

Mobile ad-hoc network is a kind of wireless and is a self configuring network of mobile nodes connected by wireless link. The nodes are free to move independently and randomly bit capability of changing its link to other devices frequently. They should be capable to ensure that the packet is being transferred from source to destination. Mobile Ad-hoc network also capable of handling topology changes and functions in nodes through network reconfiguration. The mobile Ad-hoc networks are very flexible and suitable for many types of applications as they allow the establishment of temporary communication without any pre existing infrastructure. Ad-hoc network requires no centralized or fixed infrastructure such as base station or access points and can be quickly and inexpensively setup is needed in wireless network.

As wireless ad-hoc networks lack an infrastructure, they are exposed to a lot of attacks. One of these attacks is the Black Hole attack. In the Black Hole attack, a malicious node absorbs all data packets in itself, similar to a hole which sucks in everything in. In this way, all packets in the network are dropped. A malicious node dropping all the traffic in the network makes use of the vulnerabilities of the route discovery packets of the on demand protocols, such as AODV. In route discovery process of AODV protocol, intermediate nodes are responsible to find a fresh path to the destination, sending discovery packets to the neighbor 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 the destination assuming it is a true path. Black Hole attack may occur due to a malicious node which is deliberately misbehaving, as well as a damaged node interface. In any case, nodes in the network will constantly try to find a route for the destination.

The rest of the paper is organized as follows. In Section 2, we introduce overview of overview of AODV, Section 3 black hole attack and Next Sections; we present a methodology to prevent a black hole attack. Finally, we conclude result, conclusion and discuss future work.

2. Overview of AODV Routing Protocol:

AODV is one of the most common ad-hoc routing protocols used for mobile ad-hoc networks. As its name indicates AODV is an on-demand routing protocol that discovers a route only when there is a demand from mobile nodes in the network.

In an ad-hoc network that uses AODV as a routing protocol, a mobile node that wishes to communicate with other node first broadcasts an RREQ (Route Request) message to find a fresh route to a desired destination node. This process is called route discovery. Every neighboring node that receives RREQ broadcast first saves the path the RREQ was transmitted along to its routing table. It subsequently checks its routing table to see if it has a fresh enough route to the destination node provided in the RREQ message. The freshness of a route is indicated by a destination sequence number that is attached to it. If a node finds a fresh enough route, it unicasts an RREP (Route Reply) message back along the saved path to the source node or it re-broadcasts the RREQ message otherwise. The same process continues until an RREP message from the destination node or an intermediate node that has fresh route to the destination node is received by the source node.

Figure: Propagation of RREQ in AODV

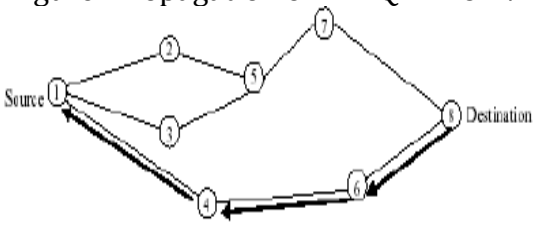

Figure: Path taken by the RREP in AODV

3. Black Hole Problem in AODV:

Routing protocols are exposed to a variety of attacks. Black hole attack is one such attack and a kind of Denial Of Service (DoS) in which a malicious node makes use of the vulnerabilities of the route discovery packets of the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept [10][11]. This attack aims at modifying the routing protocol so that traffic flows through a specific node controlled by the attacker. During the Route Discovery process, the source node sends RREQ packets to the intermediate nodes to find path to the intended destination. Malicious nodes respond immediately to the source node as these nodes do not refer the routing table. The source node assumes that the route discovery process is complete, ignores other RREP messages from other nodes and selects the path through the malicious node to route the data packets. The malicious node does this by assigning a high sequence number to the reply packet. The attacker now drops the received messages instead of relaying them as the protocol requires.

For example, let's consider the scenario in Figure. In this scenario, the node 'S' is the source node, 'D' is the destination node and 'M' is assumed the malicious node. When 'S' want to send the data packets to 'D', it starts the route discovery process by

broadcasting RREQ message to the Neighboring nodes. So, the node 'C', 'E' and 'F' receive this message. Since M is a malicious node, it immediately sends out a RREP message to 'S' with high sequence number. 'S' assumes that it is the freshest route, ignores all other RREPs and sends any packets to the destination over it. However, the node 'M' drops all data packets instead of sending to intended destination.

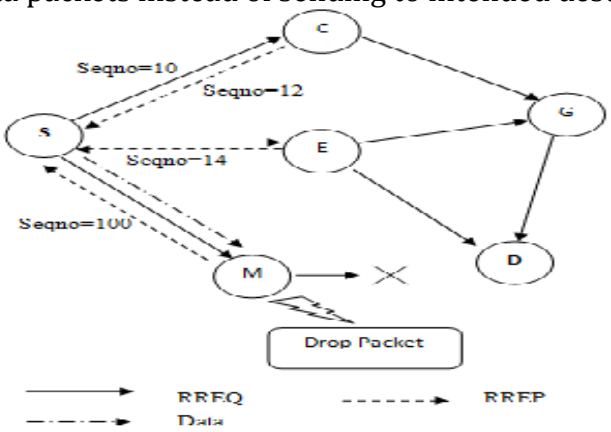

Figure: Black hole attack

4. Improved AODV Routing Protocol:

In AODV routing protocol is not resetting a new alternative routing path during expire time, because it must maintain it until disconnecting nodes. So, we proposed improved AODV routing protocol for reset a new multiple routing path during sending packet. In order to minimize the route break recovery overhead. This scheme provides multiple routes on the intermediate nodes on the primary path to destination along with source node. The primary path is failed due to the attack and packet loss continuously the alternate path received by the source node after initiating the route discovery. So improved AODV routing protocol is best for reduced packet loss. so we used in this work focus on this methodology.

5. Related Works:

The main goal is to improve the performance and throughput of existing on-demand routing protocols. The most common on-demand routing protocols are AODV protocol. So from them, I select AODV protocol to implement our propose scheme because AODV is an efficient routing protocol which removes any unnecessary information quickly, and does not create traffic unless necessary.

In this work we compared the performance of AODV and black hole AODV and their description in above section in briefly. By using AODV routing scheme we follow these steps. Main focus on route discovery process. Route discovery is a vulnerability of on-demand ad-hoc routing protocols, especially AODV, which an adversary can exploit to perform a black hole attack on mobile ad- hoc networks. A malicious node in the network receiving an RREQ message replies to source nodes by sending a fake RREP message that contains desirable parameters to be chosen for packet delivery to destination nodes. After promising (by sending a fake RREP to confirm it has a path to a destination node) to source nodes that it will forward data, a malicious node starts to drop all the network traffic it receives from source nodes. This deliberate dropping of packets by a malicious node is what we call a black hole attack [5]. A malicious node sends RREP messages without checking its routing table for a fresh route to a destination. Above, An RREQ broadcast from node 0 is received by neighboring nodes. However, malicious node sends an RREP message immediately without even having a route to destination node. An RREP message from a malicious node [6] is the first to

arrive at a source node. Hence, a source node updates its routing table for the new route to the particular destination node and discards any RREP message from other neighboring nodes even from an actual destination node. Once a source node saves a route, it starts sending buffered data packets to a malicious node hoping they will be forwarded to a destination node. Nevertheless, a malicious node (performing a black hole attack) drops all data packets rather than forwarding them on.

In an Improved AODV routing protocol used multiple path in routing protocol establishes multiple transmission paths between source nodes and destination node, which can not only transmit data in parallel, but also one as main path and others as backup paths for solve out link break problem and data send continuously without interruption.

6. Simulation Parameters:

Simulation Parameters is as follows

Parameter	Value
Routing Protocol	AODV, Blackhoe AODV, Im AODV
Traffic Type	CBR
Simulation Time	100 to 400s.
Number Of Nodes	50
Pause Time	1.0 s
Maximum Connection	20
Maximum Speed	10 m/s
Transmission Rate	2.0 Mbps
Area of Networks	1200m X 500m

7. Performance Metrices:

In this section, we discuss of performance metrics for the protocols:

Packet Delivery Fraction: This is the fraction of number of packets received at the destination to the number of packets sent from the source multiply by 100. In other words, fraction of successfully received packets, which survive while finding their destination, is called as packet delivery fraction [3, 10].

End-to-End Delay: It is the ratio of time difference between every CBR packet sent and received to the total time difference over the total number of CBR packets.

Normalized Routing Load: Normalized routing load is the ratio of the number of control packets propagated by every node in the network and the number of data packets received by the destination nodes.

Packet loss (%): Packet loss is the failure of one or more transmitted packets to arrive at their destination.

8. Simulation Model:

In this section, The Simulation environment consists of an area of 1200x500, where randomly 50 mobile nodes are placed. A source and a destination is selected randomly. Data sources generate data according to Constant bit rate traffic pattern. Source destination pairs are spread randomly over the network. A packet size of 512 bytes is used. Mobility pattern of the mobile nodes is generated using Random waypoint model. By observing the performance of the network under mobility we can test the stability of design in real time scenario. Rate of 2Mbps is used [6, 9].

9. Simulation Result and Discussion:

In the section, we analyzed the performance of under black hole attack using ns-2. The overall performance metrics gives in above. In random simulation environment, the first step is to determine the network delay on network performance with and

without attack. Results are analyzed carefully by obtaining from NS-2 simulation. Its simulate a network of 50 mobile nodes. There is no prevention is applied, and then attacks will occurs. The false node is choose randomly in simulation test, and increases delay in network. The graphs show that with no black hole we get a maximum value of throughput and almost minimum delay. In this case all the packets send by the sender reaches the destination accurately i.e. there is minimum packet loss. So PDF is maximum in improved aodv.The overall results shown in below by using xgraph with Varying Simulation time.

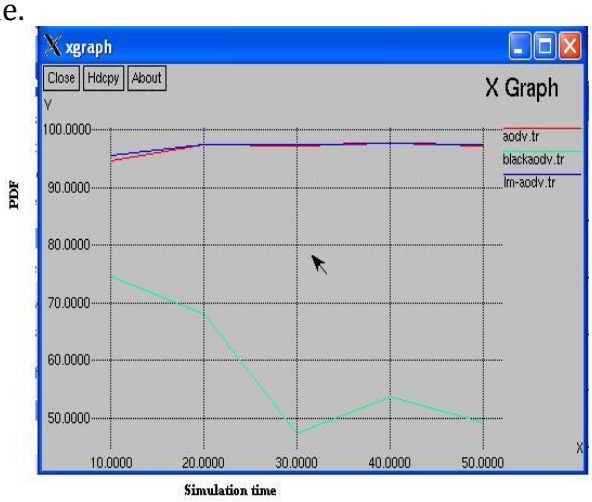

Figure 1: PDF V/s Simulation time

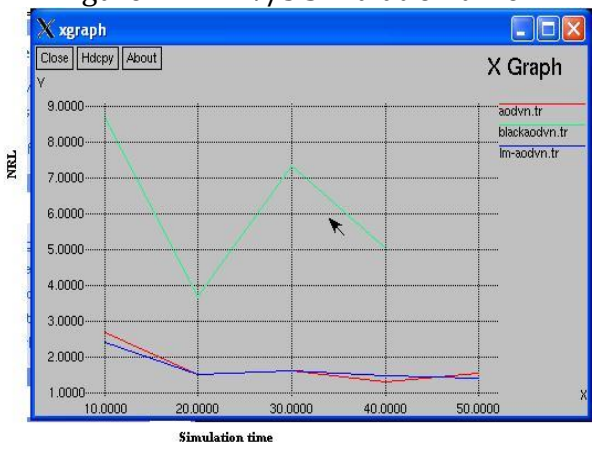

Figure 2: NRL V/s Simulation time

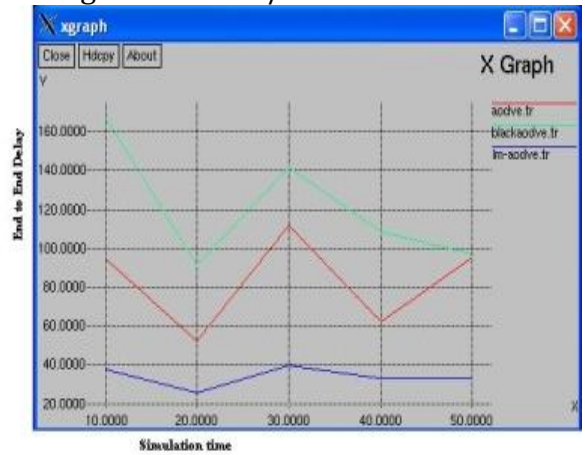

Figure 3: Average Delay V/s Simulation time

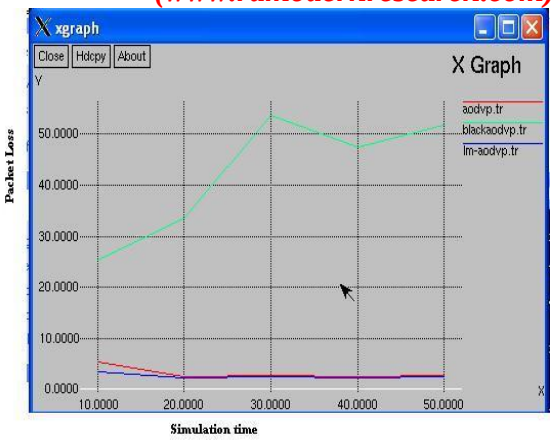

Figure 4: Packet Loss V/s Simulation time

10. Conclusion & Future Work:

In this paper simulations are analyzed having simulated the Black Hole Attack using NS-2 software find out the results in wireless environment. We saw that the packet loss is increased in the ad-hoc network with the affect of black hole attack. The simulation results show the difference between the number of packets lost in the network with and without a Black Hole Attack and improved AODV. This also shows that Black Hole Attack affects the overall network connectivity and the data loss could show the existence of the Black Hole Attack in the network. If the number of Black Hole Nodes is increased then the data loss would also be expected to increase. In future work focus study and detection of black hole attack using AODV and Different routing scheme.

11. References:

1. Elizabeth M. Royer, and Chai-Keong Toh, "A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks," IEEE Personal Communications, pp. 46-55, April 1999.
2. Charles E. Perkins, (2001) Ad Hoc Networking, Addison-Wesley, Pearson edu.
3. Hongmei Deng & Wei Li, Dharma P. Agarwal (2002) "Routing security in wireless ad hoc networks", University of Cincinnati, IEEE Communications magazine, Vol. 40, No. 10.
4. IETF MANET Working Group AODV Draft, http://www.ietf.org/internet-drafts/draft-ietf-manet-aodv-08.txt, Dec 2002.
5. M. G. Zapata and N. Asokan, "Securing Ad-Hoc Routing Protocols," Proc. 2002 ACM Wksp. Wireless Sec., Sept. 2002, pp. 1–10.
6. Avoiding Black Hole and Cooperative Black Hole Attacks in Wireless Ad hoc Networks http://www.scribd.com/doc/26788447/Avoiding-Black-Hole-and-Cooperative-Black-Hole-Attacks-in-Wireless-Ad-hoc-Networks
7. N.Shanthi, Dr.Lganesan and Dr.K.Ramar,"Study of Different Attacks on Multicast Mobile Ad-hoc Network", Journal of Theoretical and Applied Information Technology, pp.45-51.
8. Avoiding Black Hole and Cooperative Black Hole Attacks in Wireless Ad hoc Networks http://www.scribd.com/doc/26788447/Avoiding-Black-Hole-and-Cooperative-Black-Hole-Attacks-in-Wireless-Ad-hoc-Networks.
9. Ochola EO & Eloff MM, "A review of black hole attack on AODV routing in MANET".
10. R.E.Kassi, A.Chehab, and Z. Dway, "DAWWSEN: A Defense Mechanism against Wormhole Attacks in Wireless Sensor Networks", in proceeding of the second

International conference on innovations in information Technology (ITT' 05), UAE, September 2005.
11. S. Ci et al., "Self-Regulating Network Utilization in Mobile Ad-Hoc Wireless Networks," IEEE Trans. Vehic. Tech., vol. 55, no. 4, July 2006, pp. 1302–10.
12. B. Wu et al., "A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks," Wireless/Mobile Network Security, Springer, vol. 17, 2006.
13. W. Weichao, B. Bharat, Y. Lu, X. Wu, Wiley Interscience, "Defending agains Wormhole Attacks in Mobile Ad Hoc Networks," Wireless Communication and Mobile Computing, January 2006.
14. Dokurer, S.; Erten Y.M., Acar. C.E., SoutheastCon Journal, "Performance analysis of ad-hoc networks under black hole attacks". Proceedings IEEE Volume, Issue, 22-25 March 2007 Page(s):148 – 153.
15. F. Anjum and P. Mouchtaris, Security for Wireless Ad Hoc networks, Illustrated Edition: illustrated, Wiley-Interscience, 2007.
16. Rashid Hafeez Khokhar, Md Asri Ngadi and Satira Mandala, "A Review of Current Routing Attacks in Mobile Ad Hoc Networks", International Journal of Computer Science and Security, pp. 18-29, Volume-2 Issue-3
17. Rupinder Kaur1 and Parminder Singh2 "REVIEW OF BLACK HOLE AND GREY HOLE ATTACK" The International Journal of Multimedia & Its Applications (IJMA) Vol.6, No.6, December 2014
18. Bhoomika Patel and Khushboo Trivedi "A Review - Prevention and Detection of Black Hole Attack in AODV based on MANET" Bhoomika Patel et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 2816-2818
19. Ashish Sharma 1, Dinesh Bhuriya 2 , Upendra Singh 3 , Sushma Singh 4 "Prevention of Black Hole Attack in AODV Routing Algorithm of MANET Using Trust Based Computing" Ashish Sharma et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (4) , 2014, 5201-5205
20. Ei Ei Khin and Thandar Phyu "IMPACT OF BLACK HOLE ATTACK ON AODV ROUTING PROTOCOL" International Journal of Information Technology, Modeling and Computing (IJITMC) Vol. 2, No.2, May 2014.
21. FIHRI Mohammed, OTMANI Mohamed, EZZATI Abdellah "The Impact of Black-Hole Attack on AODV Protocol" (IJACSA) International Journal of Advanced Computer Science and Applications, Special Issue on Advances in Vehicular Ad Hoc Networking and Applications.
22. Nilima H Masulkar1, Archana A Nikose2 "An Improved Multipath AODV Protocol Based On Minimum Interference" International Conference on Advances in Engineering & Technology – 2014 (ICAET-2014)