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

PERFORMANCE ANALYSIS OF ENHANCED NETWORK PERFORMANCE UNDER THE BLACK HOLE ATTACK IN MANET

Bhavesh Batra*, Sadhna Rai & Monal Jain*****
Computer Science Engineering, Swami Vivekanand University, Sagar, Madhya Pradesh

Abstract:

Black hole Attack is one of the promising and severe security attacks in mobile ad hoc networks which block the communication of secret data during packet delivery. Black hole attack directly attacks the node's data traffic on the path and with intent packet drops. In this paper approach to focus on analyzing and improving the security of AODV, which is one of the popular AODV routing protocol for MANET. Our aim is on ensuring the security against Black hole attack. In this work to enhance the performance of Ad hoc On-demand Multipath Distance Vector routing protocol against Black hole attack in MANETs to a delay-aware multi-path protocol. The focus area is to improve the QoS in MANETs by creating a protocol. The solution is capable of detecting & removing Black hole node in the MANET at the beginning. Also the objective of this paper is to provide a simulation study that illustrates the effects of Black hole attack on network performance.

Key Words: Black Hole Attack, AODV, Improved AODV, MANET & NS-2.31

1. Introduction:

Mobile ad hoc networks (MANETs) are extensively used in military and civilian applications. The dynamic topology of MANETs allows nodes to join and leave the network at any point of time. This generic characteristic of MANET has rendered it vulnerable to security attacks. In this paper, we address the problem of coordinated attack by multiple black holes acting in group. We present a technique to identify multiple black holes cooperating with each other and a solution to discover a safe route avoiding cooperative black hole attack. A black-hole attack in the Mobile Ad-hoc Network (MANET) is an attack occurs due to malicious nodes, which attracts the data packets by falsely advertising a fresh route to the destination. In this paper, we present an Ad-hoc On-demand Distance Vector (AODV) routing protocol for the prevention of black-hole attack in MANETs.

In the rest of this paper, we summarizes the basic operation of AODV protocol and Black hole attack and describe some methods that have proposed for detecting or preventing these attacks and provides a comparison for the methods and finally, we conclude the paper.

2. AD HOC ON-Demand Distance Vector:

Ad hoc On Demand Distance Vector (AODV) [1] routing algorithm is a routing protocol designed for ad hoc mobile networks. 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.[3,5] AODV builds routes using a route request / route reply query cycle. 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. Nodes receiving this packet update their information for the source node and set up backwards pointers to the source node in the route tables. As long as the route remains active, it will continue to be maintained. A route is considered active as long as there are data packets periodically travelling from the source to the destination along that path. Once the source stops sending data packets, the links will time out and eventually be deleted from the intermediate node routing tables. If a link break occurs while the route

is active, the node upstream of the break propagates a route error (RERR) message to the source node to inform it of the now unreachable destination(s). After receiving the RERR, if the source node still desires the route, it can reinitiate route discovery. If it possesses a route towards the destination with greater sequence number than that in the RREQ packet, it unicasts a RREP (Route Reply) packet back to its neighbor from which it received the RREQ packet. Otherwise, it sets up the reverse path and then rebroadcasts the RREQ packet. Duplicate RREQ packets received by one node are silently dropped. This way, the RREQ packet is flooded in a controlled manner in the network. The RREQ packet will eventually arrives at the destination itself or a node that can provide a fresh route to the destination, which will generate the RREP packet. As the RREP packet is propagated along the reverse path to the source, the inter-mediate nodes update their routing tables.

3. Black Hole Attack:

In an ad-hoc network that uses the AODV protocol, a Black Hole node absorbs the network traffic and drops all packets. To explain the Black Hole Attack we added a malicious node that exhibits Black Hole behavior in the scenario. In this attack, a malicious node advertises that it has the best path to the destination node during the route discovery process. Whenever it receives the RREQ message, it immediately sends out a fake RREP to the source node. The source node first receives the RREP from the malicious node ahead of other RREPs. However, when the source node starts sending the data packet to the destination by using this route, the malicious node drops all packets instead of forwarding. We simulated the Black Hole attack in wireless ad-hoc networks and evaluated its damage in the network. Damage network means path break by using malicious node and solve out this problem by using Improved AODV.

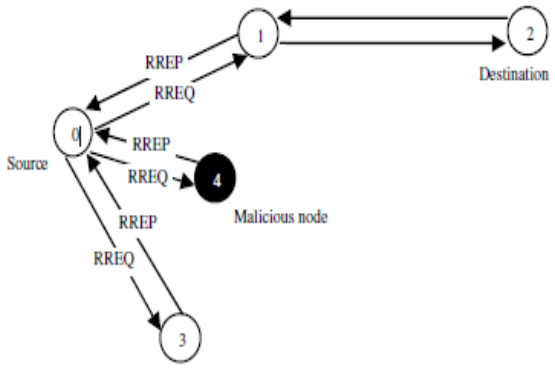

Figure: Black Hole Attack

Method to Add a Malicious Node:

The main setback of black hole attack is to hinder the communication from source to destination. To add malicious nodes in AODV the following procedure has been implemented [24].

First we need to modify aodv.cc and aodv.h files:

In aodv.h:

bool malicious;

In aodv.cc:

malicious = false;
if(strcmp(argv[1], "malicious") == 0) {
malicious = true;
return TCL_OK; }

Next we need to modify the TCL file to set a malicious node:

$ns at 0.0 "[$mnode_(i) set ragent_] malicious"
if (malicious == true) {
drop (p,DROP_RTR_ROUTE_LOOP); }

Algorithmic Approach to Avoid Black Hole Attack in MANETs:

The solution that we propose here, basically, only modifies the working of the source node without altering intermediate and destination nodes. In this method two main things are added namely Data Routing Information table and cross checking.

Step1: Source node broadcasts RREQ to neighbors
Step2: Source node receives RREP from neighbors
Step3: Source node selects shortest and next shortest path based on the number of hops
Step4: Source node checks its routing table for single hop neighboring nodes only
Step5: If the neighbor node is in its routing table then route data packet else the node is malicious and sends false packets to that node
Step 6: Invoke the route discovery Inform all the neighboring nodes about the stranger
Step 7: Add the status of stranger to the routing table of source node
Step 8: Again send packet to neighboring node
Step 9: If step 5 repeats then broadcast the malicious node as black hole
Step 10: Update the routing table of source node after every broadcast
Step 11: Repeat step 4 to 10 until packet reaches the destination node correctly
Neighboring nodes even from an actual destination node. In an Improved AODV routing protocol used multiple path in routing protocol establishes multiple paths and data send using alternative path data transfer continuously.

4. Simulation Parameters:

Simulation Parameters is as follows

Parameter	Value
Routing Protocol	Blackhole AODV, AODV, Im AODV
Traffic Type	CBR
Simulation Time	100 sec.
Number Of Nodes	50
Pause Time	1.0s
Maximum Connection	10
Maximum Speed	10 to 50 m/s
Transmission Rate	2.0 Mbps
Area of Networks	800m X 500m

5. Performance Metrics:

Protocols can be compared by evaluating various performance metrics as shown below:

Packet Delivery Ratio (Fraction): It is calculated by dividing the number of packet received by destination through the number packet originated from source.

$$PDF = (Pr/Ps)$$

Where Pr is total Packet received and Ps is the total Packet sent.

Average End-To End Delay: It is defined as the time taken for a data packet to be transmitted across an MANET from source to destination.

$$D = (Tr - Ts)$$

Where Tr is receive Time and Ts is sent Time.

Normalized Routing Overhead: It can also be defined as the ratio of routed packets to data transmissions in a single simulation. It is the routing overload per unit data delivered successfully to the destination node

6. Simulation Model:

In this section, The Simulation environment consists of an area of 800x500, where randomly 50 mobile nodes are placed. A source and a destination are 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 with varying speed. Data rate of 2Mbps is used [6, 9].

7. Simulation Result and Discussion:

In the section, by using ns-2 simulator the check the performance of under black hole attacks using ns-2. The simulation results shown above explain that a single malicious node can bring a significant drop in the performance of the network. But when multiple malicious nodes launch an attack on the network, its functioning is rendered almost useless. To study this, simulation was carried out using multiple malicious nodes in a network.

The graphs show that with black hole more packets reaching the destination are lost. Figure shows the effect of black hole on received packets after deleting the black hole using the alternative path and the effect of using random routes to secure the packets with increased packet received. In an Improved or modified AODV. In this paper focus on reduced the data loss and solve out the link failure problem this link failure problem create by using black hole attack. By using alternative path discard the malicious node of the wireless network so also packet received in maximum in improved AODV. The overall performance by using x graph with varying maximum speed.

The network metrics like as packet delivery fraction, average end to end delay and network load shown the result by using x graph in below.

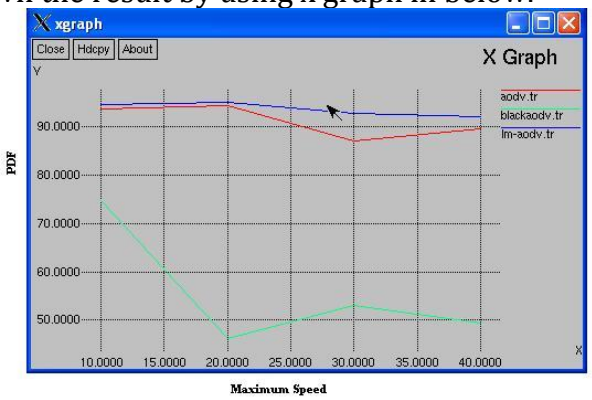

Figure 1: PDF V/s Maximum Speed

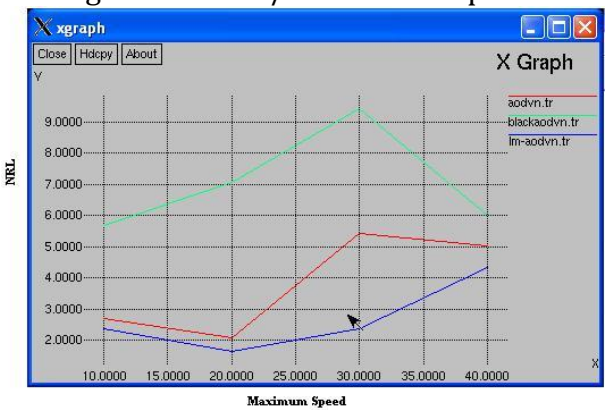

Figure 2: NRL V/s Maximum Speed

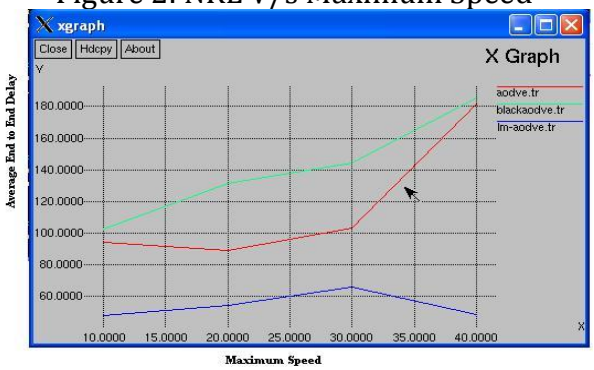

Figure 3: Average Delay V/s Maximum Speed

8. Conclusion & Future Work:

In this work, we have analyzed the effect of black hole attack in the performance of AODV protocol. The simulation has been done using the network simulator. The simulation results show 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. In this paper find out the simulation detection Black hole attack using multiple path algorithm and 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. In future work, we intend to simulate and analyze the effect of the black hole attack in other routing protocols and we intend to perform the solution for the black hole attack and compare its performance with the AODV protocol.

9. 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. Mohan Kumar S B and Nirmal Kumar S Benni "Cryptographic Approach to Overcome Black Hole Attack in MANETs" International Journal of Innovations in Engineering and Technology (IJIET) Vol. 2 Issue 3 June 2013.
4. Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon and Kendall Nygard. "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks". Department of Computer Science, IACC 258 North Dakota State Universities, Fargo, ND 58105.
5. 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
6. 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
7. 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
8. 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

9. 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
10. 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.
11. 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.
12. 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)
13. "Garima Gupta1 and Atul Mishra2SIMULATION BASED STUDY OF COOPERATIVE BLACK HOLE ATTACK RESOLUTION USING CROSSCHECKING ALGORITHM" International Journal on AdHoc Networking Systems (IJANS) Vol. 5, No. 2, April 2015.
14. Xiaoxia Qi1,2, Qijin Wang1 and Fan Jiang 2 "Multi-path Routing Improved Protocol in AODV Based on Nodes Energy" International Journal of Future Generation Communication and Networking Vol. 8, No. 1 (2015).
15. Hoda Rafiee Pour1, Marjan Kuchaki Rafsanjani2,and Hamid Saadat3 A New Zone Disjoint Multi Path Routing Algorithm to Increase Fault-Tolerant in Mobile Ad Hoc Networks" Applied Mathematics & Information Sciences An International Journal. Appl. Math. Inf. Sci. **9**, No. 1, 433-444 (2015)
16. Network Simulator Official Site for Package Distribution, web reference, http://www.isi.edu/nsnam/ns