# DEFENDING AGAINST BLACKHOLE ATTACK IN MANET USING AN MULTI PATH BASED APPROACH

Abhimanyu Kumnwar[1], Ashish Sharma[2], Uma Shankar Yadav[3], Umesh Barahdiya[4]

[1,2&3]Research Scholar, NITM, Gwalior India[1,2&3]

[4]Asst. Professor, , NITM, Gwalior India[4]

umesh.barahdia@gmail.com

***Abstract:*** **The most important concern for Mobile Ad-Hoc is the Security. Different types of attacks are applied in MANETs open medium, changing its topology dynamically and lack of central monitoring and management, no clear defense mechanism and cooperative algorithms. One of the major security issues in MANET is Black hole attack. Black Hole is one of these attacks, which Attack against network integrity engrossing all data packets in the network and create link break problem. Where the data packets are do not reach the destination node on account of this attack, data loss will occur. In the study many techniques were introduced by researchers to find the attacks in the MANETs. In this paper we have found an approach to remove black hole attack operations using multipath based AODV. The proposed solution is a Multipath AODV routing protocol, which will be able to detect a black hole node in the network. So this problem and defense mechanisms to remove the intruder that carries out the black hole attack using Multi path AODV Scheme. The work describe here is the simulation of black hole attack in the MANET BASED on demand reactive routing scheme. In this Dissertation, an Ad Hoc Network is to be constructed, and analyze the results from the simulation of the existing and proposed by using the NS-2.**

***Keywords:*** **Black Hole Attack, AODV, Multipath AODV, MANET, Performance Matrices.**

## I. INTRODUCTION

Wireless networks can be basically either infrastructure based networks or infrastructure less networks. The infrastructure based networks uses fixed base stations, which are responsible for coordinating communication between the mobile nodes. The ad hoc networks falls under the class of infrastructure less networks, where the mobile nodes communicate with each other without any fixed infrastructure between them. Due to wireless or infrastructure less network security is the biggest issue. Securing is a highly challenging issue for wireless ad hoc networks. Understanding possible form of attacks is always the first step towards developing good security solutions. Security of communication in MANET is important for secure transmission of information. Absence of any central co-ordination mechanism and shared wireless medium makes MANET more vulnerable to attacks there are a number of attacks that affect MANET. Since the functioning of MANET requires cooperation from the participating nodes in the network, security is a primary concern in MANET. Many applications, especially military and emergency rescue, are based on ad hoc networks, where enforcing security requirements are harder than traditional wired networks. Secure routing is also difficult here because of the absence of centralized administration in the network and each node has to trust other nodes for routing their packets. So the presence of any misbehaving nodes in the network can easily disrupt the network operation and damage the communication within the network. Thus, secure routing is one important aspect that has to be incorporated with ad hoc networks for successful commercialization of such networks, and to support secure applications. Hence, providing secure routing through misbehavior detection and mitigation in MANETs is an important and critical research topic. Security is an essential component for mobile ad hoc network. In order to provide security against attacker, researchers are working specifically on the security challenges in MANETs, and many techniques are proposed for secure routing protocols within the networks. Black hole attack is one of most important security issues in mobile ad hoc networks. It can be seen that Packet Delivery Ratio of standard AODV protocol decreases due to the presence of black hole node in the network and increase the Load. Due to black hole attack related issue solving by using multipath AODV based approach. We have investigated the performance of black hole attack existing and proposed multipath based AODV scheme in this work using network simulator.

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 presents a multipath methodology to prevent a black hole attack, result and lastly discussed conclusion.

## II. OVERVIEW OF AODV ROUTING PROTOCOL

Ad-hoc On Demand Distance Vector Routing Protocol is one of the reactive protocol in which source node initiates data packet to destination node only when requires the route discovery is occur. There are no periodical exchanges of routing information [16].The Protocol consist of two phases:

•Route Discovery

•Route Maintenance.

***Route Discovery:*** The route discovery process is initiated when a source needs a route to a destination and it does not have a route in its routing table. To initiate route discovery, the source floods the network with a RREQ packet specifying the destination for which the route is requested. When a node receives an RREQ packet, it checks to see whether it is the destination or whether it has a route to the destination. If either case is true, the node generates an RREP packet, which is sent back to the source along the reverse path. Each node along the reverse path sets up a forward pointer to the node it received the RREP from. This sets up a forward path from the source to the destination. If the node is not the destination and does not have a route to the destination, it rebroadcasts the RREQ packet. At intermediate nodes duplicate RREQ packets are discarded. When the source node receives the first RREP, it can begin sending data to the destination.

***Route Maintenance*:** When a node detects a broken link while attempting to forward a packet to the next hop, it generates a RERR packet that is sent to all sources using the broken link. The RERR packet erases all routes using the link along the way. If a source receives a RERR packet and a route to the destination is still required, it initiates a new route discovery process. Routes are also deleted from the routing table if they are unused for a certain amount of time. It is performed by the source node and can be subdivided into: i) source node moves: source node initiates a new route discovery process, ii) destination or an intermediate node moves: a route error message (RERR) is sent to the source node. Intermediate nodes receiving a RERR update their routing table by setting the distance of the destination to infinity. If the source node receives a RERR it will initiate a new route discovery. To prevent global broadcast messages AODV introduces a local connectivity management. This is done by periodical exchanges of so called HELLO messages which are small RREP packets containing a node's address and additional information [2-5].

## III. BLACK HOLE PROBLEM IN AODV

In this chapter author are going to report some recent and adoptable solution for preventing and securing the network through the black hole attackers. In this attack, a black hole node tries to send fake RREPs to route requests in order to advertise itself as having the shortest path to the destination. These false RREPs deceive the source to divert the traffic of the network toward the black hole node for either eavesdropping or absorbing traffic to drop the data packets.

The black hole attack has two phases. In the first phase, the malicious node exploits the ad hoc routing protocol such as AODV to advertise itself as having a valid route to a destination node, with the intention of intercepting packets, even though the route is spurious. In the second phase, the attacker node drops the intercepted packets without forwarding them. There is a more subtle form of this attack when an attacker node suppresses or modifies packets originating from some nodes, while leaving the data packets from other nodes unaffected. This makes it difficult for other nodes to detect the malicious node. In this work, however, a defense mechanism has been proposed against a cooperative black hole attack in a MANET that relies on AODV routing protocol.

In Black Hole Attacks is that malicious nodes never send true control messages initially. To carry out a black hole attack, malicious node waits for neighboring nodes to send RREQ messages. When the malicious node receives an RREQ message, without checking its routing table, immediately sends a false RREP message giving a route to destination over itself, assigning a high sequence number to settle in the routing table of the victim node, before other nodes send a true one. Therefore requesting nodes assume that route discovery process is completed and ignore other RREP messages and begin to send packets over malicious node. Malicious node attacks all RREQ messages this way and takes over all routes. Therefore all packets are sent to a point when they are not forwarding anywhere. This is called a black hole attack.

If malicious node masquerades false RREP message as if it comes from another victim node instead of itself, all messages will be forwarded to the victim node. By doing this, victim node will have to process all incoming messages and is subjected to a sleep deprivation attack. Whereas black hole attack affects the whole network. Moreover, the malicious node that Attacks cannot be perceived easily since it does not send false messages. Behavior of failed or overloaded nodes may seem like selfish nodes attacks cannot fabricate a new control message, they cannot form a black hole attack.

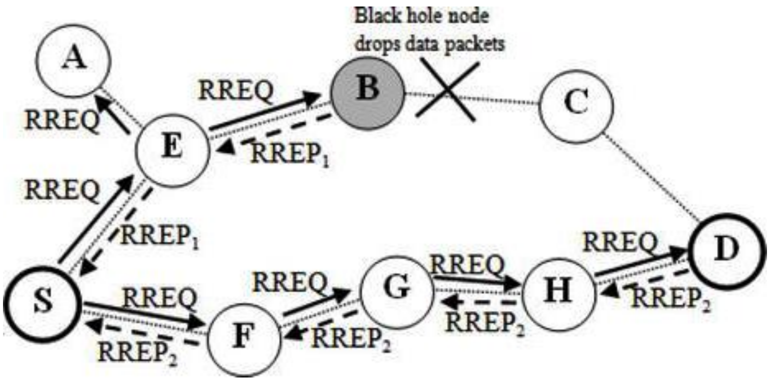

**Figure 1: Due to attack link break Shown**

For example, in Figure 1, source node S wants to send data packets to destination node D and initiates the route detection process. Suppose that device E is a malicious device and it claims that it has a route to the destination whenever it receives route request packets, and straight away sends the reaction to node S. If the reply from the malicious node E influences firstly to node S, then node S considers that route detection is finished, than S ignores all other replies and starts to send data packets to node E. As an outcome, all packets through the malicious node is consumed or lost.

## IV. MULTIPATH AODV ROUTING PROTOCOL

AODV is a reactive routing protocol that does not require maintenance of routes to destination nodes that are not in active communication. Instead, it allows mobile nodes to quickly obtain routes to new destination nodes. Every mobile node maintains a routing table that stores the next hop node information for a route to the destination node. When a source node wishes to route a packet to a destination node, it uses the specified route if a fresh enough route to the destination node is available in its routing table. If such a route is not available in its cache, the node initiates a route discovery process by broadcasting a Route Request (RREQ) message to its neighbors. On receiving a RREQ message, the intermediate nodes update their routing tables for a reverse route to the source node. All the receiving nodes that do not have a route to the destination node broadcast the RREQ packet to their neighbors. Intermediate nodes increment the hop count before forwarding the RREQ. A Route Reply (RREP) message is sent back to the source node when the RREQ query reaches either the destination node itself or any other intermediate node that has a current route to the destination. As the RREP propagates to the source node, the forward route to the destination is updated by the intermediate nodes receiving a RREP. The RREP message is a unicast message to the source node. AODV uses sequence numbers to determine the freshness of routing information and to guarantee loop-free routes. In case of multiple routes, a node selects the route with the highest sequence number. If multiple routes have the same sequence number, then the node chooses the route with the shortest hop count. Timers are used to keep the route entries fresh. When a link break occurs, Route Error (RERR) packets are propagated along the reverse path to the source invalidating all broken entries in the routing table of the intermediate nodes. AODV also uses periodic hello messages to maintain the connectivity of neighboring nodes. In this algorithm used Multiple Route Discovery Procedure is the process by which multiple paths are discovered. One observation of AODV is that, though the source actually discovers multiple paths during the route discovery process, it chooses only the best route and discards the rest. Also, frequent route breaks cause the intermediate nodes to drop packets because no alternate path to the destination is available. This reduces the overall throughput and the packet delivery ratio by using this methodology to efficient data delivered and solve out link break problem.

**SOLUTION MODEL**: In the study many techniques were introduced by researchers to find the attacks in the MANETs. Black Hole is one of these attacks, which Attack against network integrity all data packets in the network and create link break problem. Where the data packets are do not reach the destination node on account of this attack, data loss will occur.

In this work we have found an approach to remove black hole attack operations using multipath based AODV, which will be able to detect a black hole node in the network.

First we modified the AODV to multipath based protocols, in this modified approach, when primary path is fail due to attack, start the route discovery process for search path and efficient data transmission and reduced delay and packet loss used this modification in existing AODV routing scheme. And have followed the following steps:

Step 1: create a new type of object called multiple route entry. The objective of multiple route entry is to keep the routes to the same destination.

Step 2: In AODV file should change “finding route to the destination” to “finding multiple routes” to the destination.

Step 3: The receive request method should be modified to receive the RREQ with the same ID as previous one in order to create the multiple reverse routes. Store the entire Route Replies destination ID and Node ID

Step 4: The receive reply method should be modified to accept the multiple route reply to create the multiple forward routes. Sort the contents of Table entries according to the Destination ID. Select the Node ID among Routing table entries.

Step 5: The receive error method should be modified to check if the node still has another active route to the destination. If the node still has another active route to the destination, the node no needs to forward the RERR packet.

Step 6: Route resolve method for source node should be set to switch from one active path to another active path and switch back in next transmission. The multiple paths will be used to transmit the data packet.

## V. SIMULATION PARAMETERS

Simulation Parameters is as follows:

| Serial No. | PARAMETERS | VALUE |
|---|---|---|
| **1.** | **Number of nodes** | 10,20,30,40,50,60,70,80,90,100 |
| **2.** | **Simulation Time** | 200 |
| **3.** | **Area** | 800x800m$^2$ |
| **4.** | **Maximum Speed** | 10m/s |
| **5.** | **Traffic Source** | CBR |
| **6.** | **Pause Time** | 1.0 |
| **7.** | **Packet Size** | 512 byte |
| **8.** | **Maximum No. of Connection** | 5 |
| **9.** | **Mobility model used** | Random waypoint Model |
| **10.** | **MAC Protocol** | MAC/802.11 |
| **11** | **Protocol** | AODV, Multipath AODV<br>(With and Without Attack) |

## VI. PERFORMANCE METRICS

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].

***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.

## VII. SIMULATION MODEL

In this section discussed the simulation model of different number of parameters used in network scenario. And have given all the parameters and its value in below section, which have used in our work. For the evaluation of the network in the existence of a malicious node, the black hole node is created with the help of an agent. A tcl script is created for the implementation ,which consist of the creation of the nodes, connection between the nodes, setting the topography area in which the nodes are located according to the x axis and y axis. The simulation is run for 200 seconds. The simulation process was carried out for 10 to 100 numbers of nodes. The nodes were randomly distributed in the simulation in the area of 800x800 m2 rand function of network. To create path between source and destination AODV on demand Routing Algorithm was used. The author considered mobility of nodes, and have also found PDF and LOAD with node variations.

## VIII. SIMULATION RESULT AND DISCUSSION

In this work detailed about the malicious black hole attack. And we have found the results with variation of nodes. In above figure explain that a malicious node can bring a significant drop in the performance of the network. To study this, simulations have carried out using malicious nodes in a network, to compare it with the normal working of AODV. And also present the performance of the proposed solution that is two types of scenarios are taken into Consideration based on attacks and without attacks. In both cases there is an analysis of the effect of network performance with the variation of nodes discussed below using the graphical method.

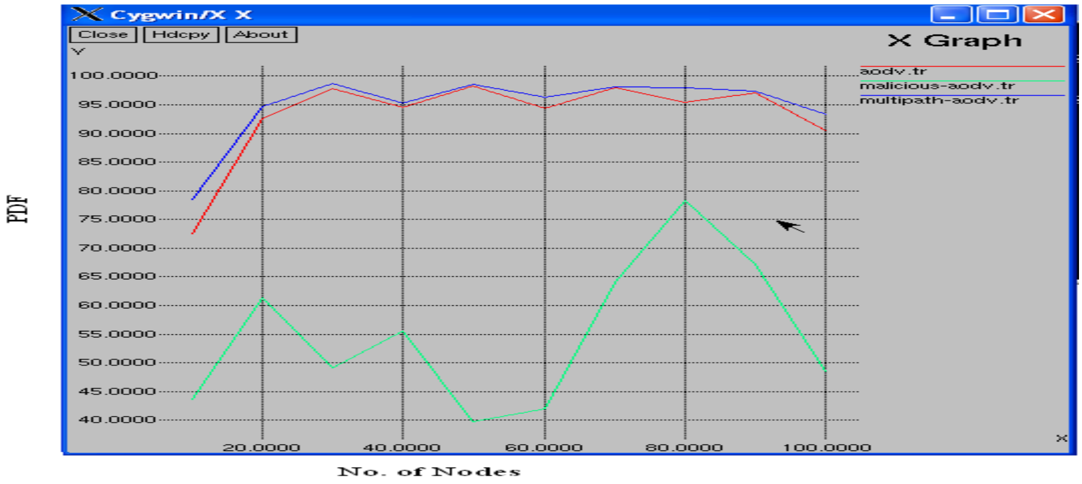

**Figure 2: PDF with variation of nodes**

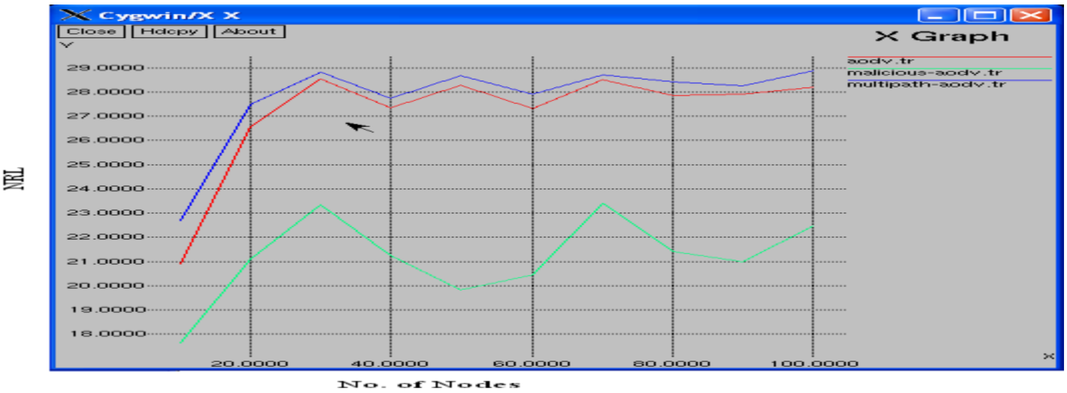

**Figure 3: NRL with variation of nodes**

As a result, a variation in value of PDF and load is seen. Here, in this case, all the packets send by the sender does not reaches the destination at that time. That leads to more dropping of packets. To compare it with the normal working of AODV, a reading for AODV without presence of malicious nodes is included. Single path AODV initiates a new route discovery when it detects one path failure to the destination, whereas in multipath it creates a fresh route in case all the existing routes fail or expire. It also reduces the number of similar routes between source and destination nodes. And we have observed that the proposed multipath methodology becomes better compare than existing or traditional routing scheme in terms of PDF and Load.

## IX. CONCLUSION

This algorithm is equally applicable to other reactive protocols. The proposed methodology is based on simple acknowledgement based scheme to detect the black-hole nodes in MANET. This approach can be incorporated with any existing on demand routing protocols. Due to solve out packet loss and link breakage problem used alternative path scheme our work. Simulation results show the difference between the number of packets lost in the network with and without a Black Hole Attack. This also shows that Black Hole Attack affects the overall network connectivity and the data loss occurs in the network. The finally concluded after the Experimental results show that the proposed algorithm achieves a very good rise in Packet Delivery Ratio and Decrease the Load.

## 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] Karthik Pai B.H1, Dr.Nagesh H.R2, Dr.Niranjan N.Chiplunkar3, Sharath Kumar4 "A Study of Behaviour And Performance Analysis Of Wormhole Attack In Mobile Ad-Hoc Networks" International Journal of Innovative Research in Computer and Communication Engineering Vol. 2, Issue 4, April 2014 PP 3782-3787.

[3] Akansha Shrivastava and Rajni Dubey "Wormhole Attack in Mobile Ad-hoc Network: A Survey" International Journal of Security and Its Applications Vol.9, No.7 (2015), pp.293-298.

[4] Priyanka Goyal, Sahil Batra & Ajit Singh "A Literature Review of Security Attack in Mobile Ad-hoc Networks" International Journal of Computer Applications (0975 – 8887) Volume 9– No.12, November 2010 PP 11-15.

[5] H. A. Esmaili, M. R. Khalili Shoja & Hossein gharaee " Performance Analysis of AODV under Black Hole Attack through Use of OPNET Simulator" World of Computer Science and Information Technology Journal (WCSIT) ISSN: 2221-0741 Vol. 1, No. 2, PP 49-52, 2011.

[6] Dipesh Chouhan1, Sujeet Mishra2 "A Literature Survey on Wormhole Attacks in MANET" International Journal of Technology Research and Management Vol 3 Issue 3 March 2016 PP 1-5.

[7] Saurabh Upadhyay1 and Aruna Bajpai2 "Avoiding Wormhole Attack in MANET using Statistical Analysis Approach" International Journal on Cryptography and Information Security(IJCIS),Vol.2, No.1,March 2012 PP 15-23.

[8] Moutushi singh & rupayan das "A Survey of Different Techniques for Detectionof Wormhole Attack in Wireless Sensor Network" International Journal of Scientific & Engineering Research Volume 3, Issue 10, October-2012 PP 1-6.

[9] Shang-Ming Jen 1, Chi-Sung Laih 1 and Wen-Chung Kuo 2,* "A Hop-Count Analysis Scheme for Avoiding Wormhole Attacks in MANET" PP 5022-5039. www.mdpi.com/journal/sensors.

[10] Swati Bhagat & Trishna Panse "A Review on Detection and Prevention of Wormhole Attack in Wireless Sensor Network" International Journal of Computer Applications (0975 – 8887) Volume 127 – No.13, October 2015 PP 1-4.

[11] R. H. Jhaveri, "MR-AODV: A Solution to Mitigate Blackhole and Grayhole Attacks in AODV Based MANETs," Third International Conference in Advanced Computing and Communication Technologies (ACCT), 2013, Page: 254-260.

[12] N. Kalia, and K. Munjal, "Multiple Black Hole Node Attack Detection Scheme in MANET by Modifying AODV Protocol" International Journal of Engineering and Advanced Technology (IJEAT), Vol. 2, No. 3,2013, Page: 529-533.

[13] K. S. Chavda, and A. V. Nimavat, "Removal of Black Hole Attack in AODV Routing Protocol of Manet", Proc. IEEE conference on computer networks, Tiruchengode, India, 2013, Page: 207-212.

[14] Pranjul Sarathe and Neeraj Shrivastava "A Review on Different Methods to Prevent Black Hole Attack in MANET" International Journal of Computer Sciences and Engineering Vol.-6, Issue-6, June 2018, Page: 1149-1156.

[15] Nigahat and Dr. Dinesh Kumar "A Review on black hole attack in mobile ad hoc networks" International Journal of Engineering Sciences & Research Technology March, 2017 Page:556-561.

[16] Lokesh Baghel, Prakash Mishra, Makrand Samvatsar and Upendra Singh "Detection of Black hole Attack in Mobile Ad hoc Network using Adaptive Approach" International Conference on Electronics, Communication and Aerospace Technology ICECA 2017 978-1-5090-5686.

[17] Dr. T.Sivaraman "Link Based Bandwidth Aware Multipath Routing Protocol in MANET". International Journal of Engineering Science Invention Page NCIOT-2018 Page: 70-76

[18] G. Stephanie Vianna, T. Vishnu Priya and M. Sathya "Trust based approach to overcome black hole attack in MANET" International Journal of Pure and Applied Mathematics Volume 118 No. 22 2018, Page: 1763-1769.

[19] Sandeep Lalasaheb Dhende, Dr. S. D. Shirbahadurkar, Dr. S. S. Musale and Shridhar K Galande "A Survey on Black Hole Attack in Mobile Ad Hoc Networks" 4th Int'l Conf. on Recent Advances in Information Technology RAIT-2018, 978-1-5386-3039.

[20] Layth A. Khalil A, Dulaimi1 R. Badlishah Ahmad, Naimah Yaakob, Mohd Hafiz Yusoff and Mohamed Elshaikh " Black hole attack behavioral analysis general network scalability" Indonesian Journal of Electrical Engineering and Computer Science Vol. 13, No. 2, February 2019, Page: 677-682.

[21] Taku Noguchi and Takaya Yamamoto "Black Hole Attack Prevention Method Using Dynamic Threshold in Mobile Ad Hoc Networks" Computer Science and Information Systems ACSIS, Vol. 11, Page: 797–802.

[22] Network Simulator Official Site for Package Distribution, web reference, http://www.isi.edu/nsnam/ns.