International Journal of Electrical and Electronics Research ISSN 2348-6988 (online)
Vol. 8, Issue 3, pp: (48-53), Month: July - September 2020, Available at: www.researchpublish.com

SOLUTIONS OF SECURITY ISSUES OF BLACK HOLE ATTACK USING MULTIPATH ROUTING SCHEME IN WIRELESS AD HOC NETWORK

[1]Nagendra Singh Tomar, [2]Seema Shukla, [3]Santosh Kumar

[1]Research Scholar, Electronics & Communication Engineering Dept, MITM Bhopal India

[2&3] Professors, Electronics & Communication Engineering Dept, MITM Bhopal India

Meetnagendra.tomars@gmail.com

Abstract: **In this work, the performance of multipath routing under security attack is studied and evaluates the quality of services matrices with this scheme in random network topologies. Because Multipath routing is vulnerable to security attacks, a scheme called Statistical Analysis of Multipath is proposed to detect such type of attacks and to identify malicious nodes. Additional security services or systems nor security enhancement of routing protocols is needed in the proposed scheme. The Black Hole Attack is the major risks in the Ad Hoc Network as an attacker makes faulty route by responding fake network information to the information source, and intercepts data through faulty route they made. The work describe here is the simulation of black hole attack in the MANET using 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: **MANET, AODV, security Attack, multipath AODV Performance Metrics, NS-2.**

I. INTRODUCTION

A mobile ad-hoc network is a collection of wireless mobile nodes, in which all nodes are connected to each other with the help of wireless medium. It does not require any fixed infrastructure it means this is an infrastructure less network. There are many features of this mobile ad hoc network that make it different from other networks such as each node has autonomous behavior. Centralized firewall is absent. Network topology is dynamic in nature and does not require infrastructure to deploy it anywhere. Because of all these features of MANET, it attracts the attention of network researchers, but due to the lack of infrastructure and dynamic topology, some major problems and challenges of this network are also available which limit the performance and security of MANET.

Security attacks are an important issue in this network that has emerged as an important research area. Being a dynamic topology and wireless medium, it faces various types of attacks, understanding and resolving security attacks responsible for MANET is a concern. MANETs suffer from many types of security attacks and threats such as: denial of service, flood attack, impersonation attack, selfish node abuse, routing table overflow attack, wormhole attack, black hole attack, etc.

The rest of the paper begins with performance analysis against Black hole Attack using AODV and modified AODV or Multipath AODV routing protocol in MANET, in Section II, III and section IV AODV, Problem Statement, Black Hole Attack, and section V, VI and VII, are carried out to evaluate the effectiveness of the proposed scheme. And section VIII results and discussion and last section discussed about conclusion and References.

II. AODV ROUTING

AODV routing algorithm is designed for MANETs. It is used on demand strategy, means when builds path between desired by every source nodes. It maintains these paths or routes when they are needed by the sources [3, 5]. AODV make routes using a route request or route reply query cycle. If destination node initiates for packets to source node, it does not have a route then broadcasts RREQ packets across the network. Nodes receiving data packet and update information regarding network nodes for the source node and set up backwards paths in the route tables. As long as the route remains active means data packets periodically travelling from the source to destination. Once the primary nodes stop sending data packets, if the links will time out and eventually to be deleted from the mediate node routing tables. If a link break occurs while acknowledge RERR message to the primary node to inform it of the now unreachable destination [1, 3, 6]. AODV routing protocol offers a quick adaptation to dynamic link conditions, low processing and memory overhead and low network utilization. It avoids problems associated with classical distance vector.

III. PROBLEM STATEMENT

In this thesis, the author addresses the problem of security in mobile ad hoc, which has become an important concern. MANET has various types of attacks at the time of transmission and communication. The author has studied several research papers and discussed the problem statement of black hole attack in this thesis and discovered that the attack is caused by malicious nodes. This attack also causes the problem of a link failure and a large number of data packets may fall, increasing control overhead and delays.

IV. BLACK HOLE ATTACK

In this section black hole attack is discussed in detail and how it affects the network. In this attack, a black hole node tries to send a fake RREP for a route request, being the shortest route to the destination. These false RREPs deceive the source to divert network traffic toward the black hole node for eavesdropping or absorbed traffic to discard data packets.

There are two stages of black hole attack. In the first phase, the malicious node uses an ad node routing protocol such as AODV to advertise as a valid route to the destination node. Even if the route is suspicious, intended to interrupt the packet. In the second stage, the attacker node drops the intercepted packet without forwarding it. A more subtle form of this attack occurs when an attacker node suppresses or modifies packets originating from certain nodes, while leaving data packets unaffected from other nodes. This makes it difficult for other nodes to detect malicious nodes. In this work, however, a defense mechanism against a collaborative black hole attack in AOD is proposed that relies on the AODV routing protocol.

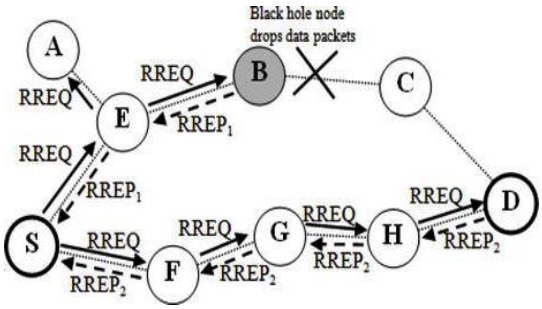

Figure 1: Black hole attack link break

Among black hole attacks is that malicious nodes do not initially send actual control messages. For a black hole attack, the malicious node waits for the neighboring node to send the RREQ message. When a malicious node receives an RREQ message, without checking its routing table, immediately sends an incorrect RREP message that routes to the destination, a higher serial number for the victim node to settle in the routing table Specifies, do not correct before sending to your node. Therefore requesting the nodes assumes that the route discovery process is complete and ignores other RREP messages and starts sending packets to the malicious node. The malicious node attacks all RREQ messages in this way and occupies all routes. Therefore all packets are sent at a point when they are not forwarding anywhere. This is called a black hole attack.

The malicious node messages the wrong RREP message as if it comes from another victim node instead of itself; all messages will be sent to the victim node. By doing this, the victim node intercepts all incoming messages. This causes the

attack link brake problem as shown in the figure above. Black hole attack affects the entire network. This degrades the performance of the network. Problems such as packet loss and delay increase. After launching a black hole attack, the attacker has unauthorized access to the given network. Following are the symptoms that can be seen in the network due to black hole:

•Decrease in Network utility.

•Increase the Traffic Load.

•Increase the Packet Loss.

•Increase Delay.

V. SOLUTION MODEL

In this solution, the sender node needs to verify the authenticity of the RREP packet initiating node using network redistribution. Since any packet can be transported to the destination through multiple redundant paths, the idea of this solution is to wait for the RREP packet to arrive from more than two nodes. During this time the sending node will buffer its packet until a secure route is identified. Once a secure route is identified, these buffer packets will be transmitted. When an RREP arrives at the source, it will take all routes to the destination and wait for another RREP. If it has not received the packet, it follows another path and sends the packet and also checks whether the received packet was received before the same original source. In this solution each node requires two tables; The first table has to hold the sequence number for the last packet sent and the second table has to forward the information of nodes. The sender delivers RREQ packets to its neighbors. Once this RREQ reaches the destination, it will initialize the source to RREP, and this RREP will contain the last packet-sequence-numbers received from this source. When an intermediate node has a route to the destination and receives RREQ, it will respond to the sender with RREP.

For the past few years, the subject of the attack has been a main area of research. In this work, we have found a way to find and solve a black hole attack. We prevented the problem of black hole attack by using the algorithm below and efficient data transmission. Some modifications have been made to the AODV routing scheme that minimizes packet loss. A new protocol known as the multi-path scheme is proposed based on an alternative path to avoid a black-hole attack. The proposal technique is used to detect and isolate malicious nodes from the network. The proposed technique is an improvement over existing technology.

Multipath AODV or Modified AODV: Multiple root discovery procedures are used in this scheme, by which multiple routes are discovered. Continuous route breakdown causes intermediate nodes to fall packets because there is no alternate route available to the destination. Therefore, this scheme provides an alternative route for data transfer.

Modification in Ad hoc on demand distance vector routing Source Code

We have modified the code below to correct the black hole attack:

•In AODV main file should change “finding route to the destination” to “finding multiple routes” to the destination.

•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. The receive reply method should be modified to accept the multiple route reply to create the multiple forward routes.

•The receive reply method should be modified to forward RREP packet to every reverse route. 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. 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 set of the route selector counter should be added for every node in case of one source may have to transmit to more than one destination. The route selector counter is for the source node to switch from the best route to the second route in the next transmission and switch back in the Next Transmission.

VI. SIMULATION PARAMETERS

Simulation Parameters is given below:

PARAMETERS	VALUE
Number of nodes	10 to 100
Simulation Time	200
Area	800x800m^2
Maximum Speed	10m/s
Traffic Source	CBR
Pause Time	1.0
Packet Size	512 byte
Maximum No. of Connection	10
Mobility model used	Random waypoint Model
Examine	AODV, Multi-Path AODV (With Black hole Attack)

VII. PERFORMANCE METRICES

In this section present the definition of metrics and how to calculate these mention parameters. A performance metrics is that when the value of information is computed using mathematical methods, it shows that even performance metrics professionals choose measures the value shows the performance of Routing Protocol is as follows:

•**Packet Delivery Ratio:** This is the Ratio 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 Ratio.

•**End-to-end delay:** The packet end-to-end delay is the time of generation of a packet by the source up to the destination reception. It refers to the time taken for a packet to be transmitted across a network from source to destination.

VIII. SIMULATION MODEL

In this task a wireless scenario is configured with the same set with 10 to 100 nodes. These nodes run within the area 800mX800m, the range of which is defined as in this example. At the beginning of a wireless simulation, the types of each of these network components have to be defined. The type of antenna, routing protocol used by mobile nodes, are some of the other parameters that have been defined. In the thesis, the black hole attack is simulated and evaluated in a wireless ad-hoc network. The simulation is performed in NS-2 which has network protocols for simulation of networks of different nodes. To evaluate the network in existence of a malicious node, a black hole node is created with the help of an agent. A tcl script is created for the implementation, including the creation of nodes, the relationships between nodes, setting the topography region in which nodes are located according to the x axis and the y axis. The simulation is run for 200 seconds. Routing algorithms have been used to route between source and destination AODVs. The author considered the case of continuous mobility (no holds barred). To change the node dynamics and fixed simulation time.

IX. RESULT AND DISCUSSION

In this thesis malicious nodes with a variation of nodes are analyzed with black holes. And its results are presented in this section. The above data obtained indicate that malicious nodes cause significant degradation in network performance. Simulations have used malicious nodes in a network, comparing them with the normal functioning of AODV. And also presents the performance of the proposed solution which is concluded by taking into account scenarios with attacks. In both cases the diagram below analyzes the effect of network performance with the variation of nodes using the graphical method.

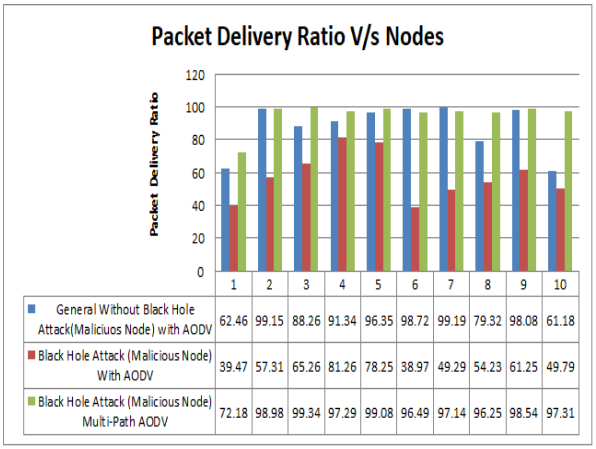

Figure 2: PDF with variations of nodes

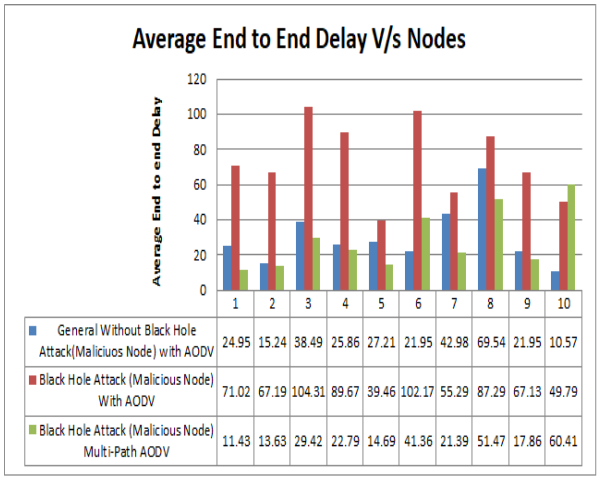

Figure 3: Average End to end Delay with variations of nodes

The figures show a delay with PDRs above 3 and 4 with variation of nodes. Both are very important matrices of networks. In which data packets between nodes are successfully transmitted between 10 and 100 nodes. Network performance is tested with the help of three scenarios. In the first scenario we found a PDR with normal AODV, in the second scenario we implemented a black hole attack with the help of a malicious node and also tested the PDR for the second scenario. In the second scenario, we saw that the attack reduced network performance. We have assumed that such a situation arises when the link break problem arises due to the attack, which increases the loss of packets. Because it follows a single path and there is no other method for data transmission. To solve this problem in the third scenario we have used multi-path AODV and with its help started the data transmission for another route. Multi-paths control packet loss and enhance network performance with the help of AODV.

The black hole attack has resulted in a link break problem. The network is delayed due to the link break problem. Here in this packet the AODV is transmitted between the source and the destination using modified routing approaches. But the delay is very large due to the black hole attack. And our proposed scheme has solved this delay coordination problem to a great extent. In this, data are available to the source within a certain time by looking for multiple routes to a host behind an alternative route plan with the intention of avoiding a delay. And finally it is seen that the modified AODV or multi-path approach. Has solved the attack problem to a great extent and enhanced network performance.

X. CONCLUSION AND FUTURE SCOPE

The simulation results prove that our proposed multi-technique technique is successful in detecting malicious nodes, as this condition receives multiple answers from the packet. The proposed technique provides a high packet delivery ratio and low delay because only reliable nodes communicate in the network after malicious nodes are detected. And the technique we propose has proved to be better given the performance matrices represented by graphs in the previous chapter, making it clear that multiple routing is capable of improving the reliability of wireless networks. This system

provides better fault tolerance against black hole attack. We have proposed our multi-Path Routing scheme to overcome the solution of the existing problem. Its high packet delivery friction and low delay are major achievements. Finally it is concluded that the proposed approach provides better results than the existing scheme.

In this proposed algorithm the researcher also considers the complexity of time and space and tries to reduce it. And with this the idea is to present a plan to implement our proposed system for detection and prevention of other attacks (eg, wormhole attack) with necessary modification in future.

REFERENCES

[1] Taku Noguchi and Takaya Yamanmoto "Black Hole Attack Prevention Method Using Dynamic Threshold in Mobile Ad Hoc Networks" Conference on Computer Science and Information Systems 2017 PP- 797-802.

[2] 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 PP-978-990.

[3] Mohamed A. Abdelshafy and Peter J. B. King "Resisting Black hole Attacks on MANETs" 13th IEEE Annual Consumer Communications & Networking Conference (CCNC) 2016 PP-1-7.

[4] Arathy K Sa and Sminesh C Na "A Novel Approach for Detection of Single and Collaborative Black Hole Attacks in MANET" Global Colloquium in Recent Advancement and Effectual Researches in Engineering, Science and Technology (RAEREST 2016) PP-264-271.

[5] Shruti Singh, Abhishek Bajpai and Suryambika "A Survey on Black Hole Attack in MANET" International Conference on Recent Cognizance in Wireless Communication & Image Processing, Proceeding Springer India 2016 PP-933-941.

[6] Muhammad Imran1, Farrukh Aslam Khan1, Haider Abbas and Mohsin Iftikhar "Detection and Prevention of Black Hole Attacks in Mobile Ad hoc Networks" ADHOC-NOW Workshops 2014, LNCS 8629, 2015 PP-111-122.

[7] Heta Changela and Amit Lathigara "Algorithm to Detect and Overcome the Black Hole Attack in MANETs" International Journal of Computer Applications (0975 – 8887) Volume 124 – No.8, August 2015 PP-22-26.

[8] Nilima H Masulkar, Archana A Nikose "An Improved Multipath AODV Protocol Based On Minimum Interference" International Conference on Advances in Engineering & Technology – 2014 (ICAET-2014) PP-1-8.

[9] MohanV.PawarandJ.Anuradha "Network security and types of attacks in network," Computer Science, vol. 48, 2015 PP-503–506.

[10] Vimal Kumar and Rakesh Kumar "An adaptive approach for detection of black hole attack in mobile adhoc network," Computer Science, vol. 48, 2015 PP-472-479.

[11] 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 PP: 529-533.

[12] 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 PP: 207-212.

[13] C. K. Nagpal , Chirag Kumar , Bharat Bhushan and Shailender Gupta "A Study of Black Hole Attack on MANET Performance" I.J.Modern Education and Computer Science, 2012, 8, PP: 47-53.

[14] Bindra, G.S., Kapoor A., Narang A., Agrawal A.: Detection and Removal of Co-operative Blackhole and Grayhole Attacks in MANETs, IEEE Conference on System Engineering and Technology (ICSET), 11-12 Sept. 2012, PP:1-5.

[15] F. H. Tseng, L. Chou, H.C. Chao: A survey of black hole attacks in wireless mobile ad hoc networks, International journal on Humancentric Computing and Information Sciences, 22 Nov 2011, PP:1-16.

[16] N.Jaisankar and R.Saravanan "An Extended AODV Protocol for Multipath Routing in MANETs" IACSIT International Journal of Engineering and Technology, Vol.2, No.4, August 2010 PP: 394-400.

[17] Elizabeth M. Royer, and Chai-Keong Toh, "A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks," IEEE Personal Communications, 1999 PP:46-55.

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