An Efficient Scheme for Detection and Prevention of Black Hole Attack using Multipath AODV in Mobile ad-hoc Network

Jagrati Chaturvedi[1], Ramnaresh Sharma[2]
[1]*Research Scholar, Computer Science & Engineering Dept, MPCT Gwalior*
[2]*Professors, Computer Science & Engineering Dept, MPCT Gwalior*

***Abstract* - In the study many techniques were introduced by researchers to find the attacks in the MANETs. In this work 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. This 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 analyse the results from the simulation of the existing and proposed by using the NS-2.**

***Index Terms* - MANET, AODV, security Attack, multipath AODV Performance Metrics, NS-2.**

I.INTRODUCTION

Wireless networks are basically infrastructural networks, which are responsible for coordinating communication between mobile nodes. Ad hoc networks fall under the category of infrastructural networks, where mobile nodes communicate between each other with no fixed infrastructure. Low network security is the biggest issue due to wireless or infrastructure.

Currently wireless networks have grown significantly in the field of telecommunication networks. Wireless networks have the main characteristic of providing access of information without considering the geographical and the topological attributes of a user. Over the past few years, the wireless network has almost exploded due to the rapid development of the Internet, and also the growth of small mobile devices as an instrument of communication and data exchange.

Researchers are particularly working on security challenges in MANETs, and several techniques have been proposed for secure routing protocols within networks. The Black Hole attack is one of the most important security issues in mobile ad hoc networks. It can be seen that the packet distribution ratio of the standard AODV protocol decreases due to the presence of black hole nodes in the network and increasing load. Causes to solve the problem related to black hole attack using multidimensional AODV based approach. We have investigated the black hole attack performance of existing and proposed multipath based AODV schemes in this thesis using network simulator.

The rest of the paper begins with performance analysis of AODV & Multipath AODV routing protocol in MANET in Section II, III and section IV solution mode; Simulation Parameters, simulation model and performance metrics in section V, VI and VII, are carried out to evaluate the effectiveness of the proposed scheme. And section VIII display the simulation graph with discussion and last section discussed about conclusion and References.

II AODV ROUTING

In November 2001 the MANET Working Group for routing of the IETF community has published the first version of the AODV Routing Protocol. AODV belongs to the class of Distance Vector Routing Protocols. In a DV every node knows its neighbors and the costs to reach them. A node maintains its own routing table, storing all nodes in the network, the distance and the next hop to them. If a node is not reachable the distance to it is set to infinity. Every node sends its neighbors periodically its whole routing table. So they can check if there is a useful route to another node using this neighbor as next hop.

When a link breaks a Count-To- Infinity could happen. AODV is an 'on demand routing protocol' with small delay. That means that routes are only established when needed [3, 25, and 31].

AODV is a reactive routing protocol used to find a route between a source and a destination and allows mobile nodes to obtain new routes for new destinations in order to establish an ad hoc network. In this order several messages are exchanged, different types of link are established, and many information can be shared between the participant's nodes. In AODV protocol we find hello message and three others significant type of messages, route request RREQ, route reply RREP and route error RERR. The Hello messages are used to monitor and detect links to neighbors, every node send periodically a broadcast to neighbors advertising it existent ,if a node fails to receive an hello message from neighbor a link down is declared. In order to communicate every node must create routes to the destinations, to achieve that the source node send a request message RREQ to collect information about the route state; if the source receives the RREP message the route up is declared and data can be sent and if many RREP are received by the source the shortest route will be chosen. Any nodes have a routing table so if a route is not used for some period of time the node drop the route from its routing table and if data is sent and a the route down is detected another message (Route Error RERR) will be sent to the source to inform that data not received.

III PROBLEM STATEMENT

Due to their nature that is the dynamic topology caused by the node mobility, create the issue of link stability or link break problem to solve this problem need new requirements on the routing protocol. Through some papers in the previous chapter, the author comes to know about several security challenges in MANET, one of them is black hole attack. The literature found that this attack is caused by malicious nodes. Malicious nodes have a detrimental effect on the network. Density plays an important role to mitigate the effects of a security attack. In addition, this work focuses on addressing the performance issue in MANET. This is not very effective due to improper selection of malicious nodes. A black-hole attack in a mobile ad-hoc network is caused by malicious nodes, which attract data packets by incorrectly advertising a fresh route to the destination. Therefore, some improvement on this proposed methodology is needed to provide security in MANET.

IV HOW BLACK HOLE WORKS

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.

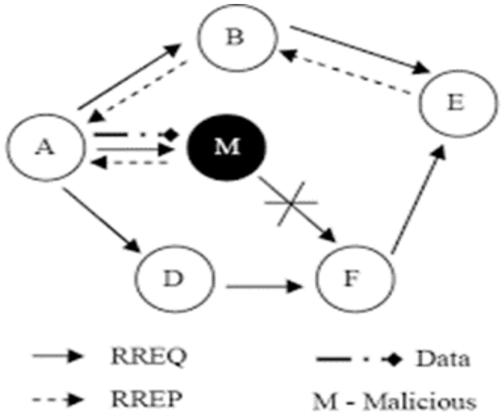

Figure: 1 black hole attack link break

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 neighbouring 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 MULTI PATH AODV

In this work, 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.

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.

V SIMULATION PARAMETERS

Simulation Parameters is given below:

PARAMETERS	VALUE
Simulator	NS-2
Routing protocol	AODV, Black hole AODV, Im- Aodv
Number of Nodes	10 to 50
Area	1000mX1000m
Packet size	512byte
Simulation time	500s
Pause time	1.0
Traffic type	CBR-UDP
Mac protocol	IEEE/MAC_802.11
Speed	10 m/s

VI PERFORMANCE METRICES

It is the value of information calculated using mathematical methods, indicating that the performance metric measures the value, and shows the display using the following metrics:

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.

VII SIMULATION MODEL

In this task a wireless scenario is configured with the same set with 50 nodes. These nodes run within the area 1000mX1000m, 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 500 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.

VIII RESULTS AND DISCUSSION

In this section simulate the performance under the black hole effect in the on demand AODV routing scheme by using network simulator version 2 and display the variations of mobility parameters. The impact variation of Ad Hoc On-Demand instance Vector routing. These section covers the avoid black hole attack problem using alternate path AODV scheme. The find the overall results and its compared existing and modified approaches.

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.

Black hole attack is one of the most important issues in the network. It can be seen that the packet delivery ratio of the standard AODV protocol decreases due to the presence of a black hole node in the network and the delay is larger. However, when the state of the network changes. Then some differences can also be seen in this approach. The difference between the number of packets received by the node and the number of packets forwarded by it is significant. Finally, experimental results show that the proposed algorithm achieves an increase in packet distribution ratio and also reduces delay significantly. .The X-axis of the graph represents the No. of Nodes and the Y-axis represents Packet delivery ratio and End-to-End Delay. While comparing these two protocol AODV and Multipath AODV.

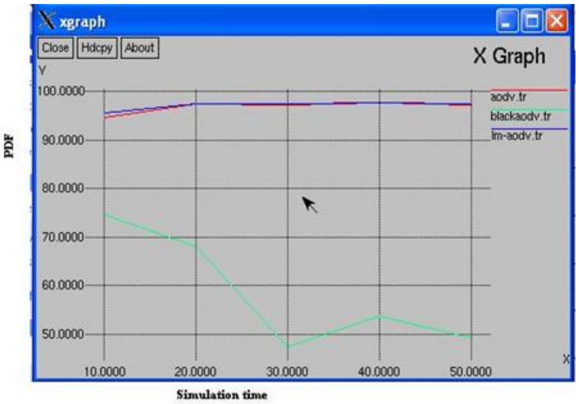

Figure-2 Packet delivery Ratio with variation of nodes

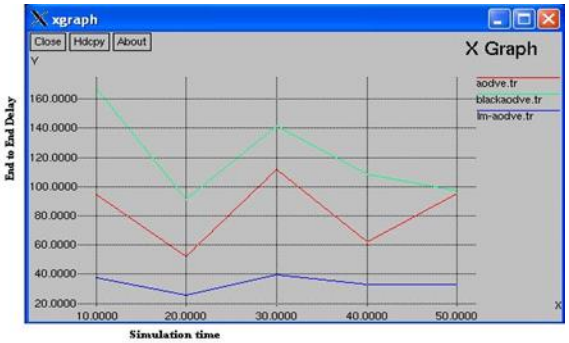

Figure-3 Average End to End Delay with variation of nodes

The figures show a delay with PDRs above 2 and 3 and variation of nodes. Both are very important matrices of networks. In which data packets between nodes are successfully transmitted between 10 to 50 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.

IX CONCLUSION

The Final concluded results after simulating proposed scheme on NS-2 a performance comparison of proposed modified or multipath AODV has been carried out with existing AODV (Normal, Attack and Defence) protocol. Performance evaluation of proposed malicious AODV, existing AODV and Modified or multipath AODV has been carried out using various metrics as Packet Delivery Ratio, End-to-End Delay and Throughput. Proposed protocol gives better performance in terms of security in different conditions like varying network size, varying pause time, varying number of nodes and varying speed using simulations. I can be seen in terms of Packet Delivery Ratio, delay, load and Throughput in various Graphs. These simulation metrics are shown by the previous section of simulation results and discussion.

FUTURE SCOPE: Security is such an important feature that it can determine the success and widespread deployment of MANET. In this thesis we have worked on the black hole attack and related issues. A black hole attack is a type of denial-of-service attack accomplished by dropping maximum the packets. In future work author have suggested new complex and efficient protocols are being proposed. As the secure protocols surveyed here are being maintained and improved by the developers and researchers. As no scheme is capable enough to avoid all type of attacks, sometimes assumptions are made for different scenarios. Therefore, we can work on this proposed scheme to avoid other types of attacks in future.

REFERENCE

[1] Elizabeth M. Royer, and Chai Keong Toh, “A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks,” IEEE Personal Communications, April 1999, Page: 46-55.

[2] L. Wang, Y. Shu, M. Dong, L. Zhang and O. Yang, “Adaptive Multipath Source Routing in Ad hoc Networks”, IEEE ICC 2001, vol.3, June 2001, Page: 867-871.

[3] Amitabh, M. and Ketan, M.N. “Security in wireless Ad hoc networks”, The handbook of ad hoc wireless networks, CRC press, 2003 Page: 499-549.

[4] N. Jaisankar, N. Saravanan, and K. D. Swamy, “A Novel Security Approach for Detecting Black Hole Attack in MANET”, Proc. Business Administration and Information Processing Heidelberg, 2010, Page: 217-223.

[5] V. Palanisamy, P. Annadurai and S. Vijayalakshmi, “Impact of black hole attack on multicast in ad hoc network”, Computational Intelligence and Computing Research, 2010 IEEE International Conference on 28-29 Dec. 2010.

[6] Ming-Yang Su, Kun-Lin Chiang and Wei-Cheng Liao “Mitigation of Black-Hole Nodes in Mobile Ad Hoc Networks” Proceedings of IEEE International Symposium on Parallel and Distributed Processing with Applications, 2010, Page: 162-167.

[7] S. Jain, M. Jain and H. Kandwal “Advanced Algorithm for Detection and Prevention of Cooperative Black and Gray Hole Attacks in Mobile Ad Hoc Networks” J. Computer Applications, vol. 1, 2010 Page: 37-42.

[8] Ajay Jangra, Nitin Goel, Priyanka and Komal, “Security Aspects in Mobile Ad Hoc Network (MANETs): A Big Picture” International Journal of Electronics Engineering, 2(1), 2010, Page: 189-196.

[9] Ming-Yang Su and Kun-Lin Chiang, “Wei-Cheng Liao. Mitigation of Black Hole Nodes in Mobile Ad Hoc Networks” In: Proceedings of IEEE International Symposium on Parallel and Distributed Processing with Applications, 2010, Page: 162-167.

[10] 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 page: 394-400.

[11] Subhashis Banerjee and Koushik Majumder “A Survey of Blackhole Attacks and Countermeasures in Wireless Mobile Ad-hoc Networks” Springer-Verlag Berlin Heidelberg, SNDS 2012, CCIS 335, Page: 396–407.

[12] Nilima H Masulkar and Archana A Nikose “An Improved Multipath AODV Protocol Based on Minimum Interference” International Conference on Advances in Engineering & Technology – 2014.

[13] Swarnali Hazra and S.K. Setua “Black hole Attack Defending Trusted on Demand Routing in Ad-Hoc Network” Advanced Computing, Networking and Informatics - Volume 2, Smart Innovation, Systems and Technologies 28, Springer International Publishing Switzerland 2014 Page:59-63.

[14] Vimal Kumar and Rakesh Kumar “An Adaptive Approach for Detection of Blackhole Attack in Mobile Ad hoc Network” International Conference on Intelligent Computing, Communication & Convergence Procedia Computer Science, Elsevier, 2015, Page: 472 – 479.

[15] G. Stephanie Vianna, 2T. Vishnu Priya, 3M. Sathya “Trust based approach to overcome black hole attack in MANET” International Journal of Pure and Applied Mathematics Volume 118 No. 22 2018, 1763-1769.

[16] 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.

[17] Vipul Maheshwari and Shrikant Jadhav "Survey on MANET Routing Protocol and Multipath Extension in AODV" International Journal of Applied Information Systems (IJAIS) – ISSN: 2249-0868 Foundation of Computer Science FCS, New York, USA Volume 2– No.4, May 2012.

[18] Versha Matre and Reena karandikar "A Literature Review of Reliable Multipath Routing Techniques" International Journal of Engineering and Computer Science ISSN:2319-7242 Volume 4 Issue 3 March 2015, Page No. 10599-10602.

[19] Nisha P John, Ashly Thomas** " Prevention and Detection of Black Hole Attack in AODV based Mobile Ad-hoc Networks - A Review" International Journal of Scientific and Research Publications, Volume 2, Issue 9, September 2012 PP 1-6.

[20] Tariq A. Murshedi, Xingwei Wang, and Hui Cheng "On-demand Multipath Routing Protocols for Mobile Ad-Hoc Networks: A Comparative Survey" International Journal of Future Computer and Communication, Vol. 5, No. 3, June 2016 PP:148-158.

[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, 2017 Page: 797–802.

[22] 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.

[23] 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.

[24] Noguchi, Taku, and Mayuko Hayakawa. "Black Hole Attack Prevention Method Using Multiple RREPs in Mobile Ad Hoc Networks." IEEE International Conference on Trust, Security and Privacy in Computing and Communications 2018, Page: 539-544.

[25] 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.

[26] Muhammad Salman Pathan1, Jingsha He2, Nafei Zhu3, Zulfiqar Ali Zardari4, Muhammad Qasim Memon5, Aneeka Azmat6 "An Efficient Scheme for Detection and Prevention of Black Hole Attacks in AODV-Based MANETs" (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 10, No. 1, 2019, Page: 243-251.

[27] Md Ibrahim Talukdar , Rosilah Hassan , Md Sharif Hossen ,Khaleel Ahmad ,Faizan Qamar , and Amjed Sid Ahmed "Performance Improvements of AODV by Black Hole Attack Detection Using IDS and Digital Signature" Hindawi Wireless Communications and Mobile Computing Volume 2021 Page: 1-13.

[28] Deshmukh, Sagar R., and P. N. Chatur. "Secure routing to avoid black hole affected routes in MANET." In Colossal Data Analysis and Networking (CDAN), Symposium on, pp. 1-4. IEEE, 2016.

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

[30] L. Yingbin, H. V. Poor, and Y. Lei, "Secrecy Throughput of MANETs under Passive and Active Attacks," Information Theory, IEEE Transactions on, vol. 57, 2011, Page: 6692-6702.

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