International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 04, April-2017

# Survey on Black Hole Attack in Wireless Ad-Hoc Network Using AODV Routing Protocol

Prof. Chirag R. Patel
Computer Engineering
V.V.P. Engineering College, Rajkot
Gujarat, India

Ms. Dhara R. Adhvaryu
Computer Engineering
V.V.P. Engineering College, Rajkot
Gujarat, India

***Abstract*— The Black Hole Attack is one of the customary security attack in wireless mobile ad-hoc networks. The interloper deploy the loophole to carry out their ill-natured behaviors due to route discovery process is essential and unavoidable. Routing protocols, which react as the binding force in these networks, are common prey of the malicious nodes. AODV is widely endorsing network routing protocol for MANET. Black Hole attack is frangibility of on-demand routing protocol such as AODV. This paper will give brief detail about Black hole attack performed on AODV routing protocol with different techniques.**

***Keywords—Ad-hoc Netwrok; Black Hole Attack; MANET;***

## I. INTRODUCTION

### *1. MANET*

Wireless Mobile Ad-hoc Network (MANET) is self configurable and infrastructure less network which is formed of number of mobile nodes which are linked with wireless medium. It's a collection of self-sustaining mobile nodes that can transmit via radio waves. Nodes within the radio range can straightly communicate with each other wirelessly. Following figure shows simple ad-hoc network with 3 nodes [11].

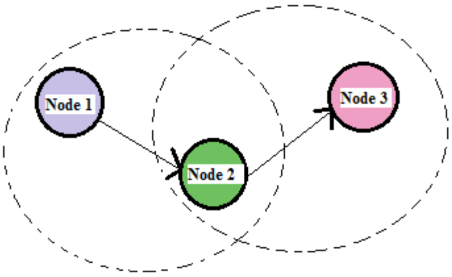

Fig. Example of Mobile Ad-Hoc Netwrok

Here in above figure it describes that Node1 and node 3 are not within the range of each other, while node 2 is a router and can be used to forward packets between node 1 and node 2. There are some characteristics come across the survey such as distributes operation, multi hop routing, dynamic topology, light-weight terminals, shared physical medium are discussed in[10]

## 2 BLACK HOLE ATTACK

### *2.1 AODV Routing Protocol*

AODV routing protocol is an alteration of DSDV protocol for active state. All nodes maintain a routing table which describes detailed information of route for particular destination. At any point, a packet is to be forwarded by a node, it will first inspect with its own routing table to settle on whether a route to the destination is now possible. Assuming this is the case, it utilizes that route to drive the packets to the destination. On the off chance that a route is not accessible or the in advance entered route is inactivated, then the node starts a route discovery course. The routing messages will not describe about whole path it will inform about only particular source and destination. Routing message will contain fresh sequence number which will describe the shortest path towards the destination [1].

### *2.2 Black Hole Attack*

Black hole attack is a sort of Denial of Service (DOS) assault; which, malignant hub drives all packets toward itself by taking favorable circumstances of steering conventions vulnerabilities. In AODV-based MANET, falsie node ensures that the source node would send all packets for it by setting a high number as succession number in RREP packet [14].

In black hole attack, the noxious node sits tight for the neighbors to start a RREQ packet. As the node accept the RREQ packet, it will instantly sends a forge RREP packet with an improve higher freshness number. So, that the source node accepts that node is having the recent route towards the destination. The source node disregards the RREP packet got from different nodes and starts to send the information bundles over malignant node. A vindictive node takes every one of the routes towards itself. It doesn't permit sending any packet anyplace. This attack is known as a black hole as it swallows all items; information packets [2].

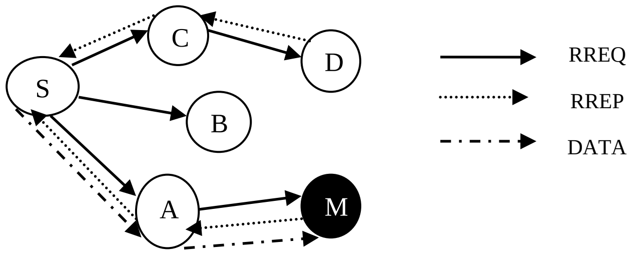

Fig. Black Hole Attack In Manet

## II. RELATED WORK

As per author[2] proposed DPRAODV (detection, prevention and reactive AODV) to prevent the black hole attack by informing the other nodes about the malicious node. As the value of RREP sequence number is found to be higher than the threshold value, the node is suspected to be malicious and it adds the node to the black list. As the node detected an anomaly, it sends a new control packet, ALARM to its neighbors. The ALARM packet has the black list node as a parameter so that, the neighboring nodes know that RREP packet from the node is to be discarded. Further, if any node receives the RREP packet, it looks over the list, if the reply is from the blacklisted node; no processing is done for the same. The threshold value is the average of the difference of destination sequence number in each time slot between the sequence number in the routing table and the RREP packet. The purposed solution not only detects the black hole attack, but tries to prevent it further, by updating threshold which reflects the real changing environment. Other nodes are also updated about the malicious act by an ALARM packet, and they react to it by isolating the malicious node from network. As per author [3] proposed two different approaches viz. AODV-UI (based on reverse request method) and PHR-AODV (Path Hoping on Reverse AODV) and subjected these approaches to various attacks faced by mobile ad-hoc networks. These approaches aim at improving performance as well as security and various metrics viz. packet delivery ratio, end to end delay and packet lost, are used. AODV-UI method works like AODV but with an exception that if one route is lost, route discovery process is not started. Rather the alternate route found earlier in route discovery is selected. This enhances the performance as there is no need to search for routes again and again. PHR-AODV method determines multipath for sending data to destination and checks whether the path is broken or not. If broken, path is deleted from the list and new path is selected. AODV-UI performs better in terms of packets lost, end to end delay and packet delivery ratio. But in presence of black hole nodes, PHR-AODV performs better.Maintaining the Integrity of the Specifications. As per author [4] discussed security concerns in routing protocols in MANET (Mobile Ad hoc Network). In this paper, elaborate study has been done on the various attacks encountered in mobile ad hoc network and the protocols used for this type of network. The various routing protocols used can be broadly classified into proactive and reactive routing protocols. The attacks associated with ad hoc routing protocols can be dynamic topology of ad hoc networks, noise and signal interference with wireless channel, and implicit trust relationships between neighbors. Cryptography, authentication, digital signatures can be used to prevent malicious attacks. Moreover intrusion detection systems and cooperation enforcement mechanisms can be used for this purpose. This paper provides an insight into the various attacks and the counter mechanisms employed against the malicious attacks. As per author [5], proposed a novel method to defend mobile ad-hoc network against cooperative black hole attack using AODV (Ad hoc On Demand Distance Vector) routing protocol. The method used ensures reasonable throughput level in the network. The proposed algorithm uses DRI (Data Routing Information) table and cross checking mechanism to ensure security against black hole attack. The experimental results show that the proposed scheme improves the packet delivery ratio and can further be enhanced to defend mobile ad-hoc network against resource consumption attack. As per author [6] proposed a method to detect and mitigate malicious nodes from mobile ad-hoc network. The detection and mitigation of malicious nodes from the network is based on trust factor being calculated by every node for its neighboring nodes. This trust value is calculated by a ratio between the number of packet received by the node and number of packets dropped by it. Each node has a certain trust value. A threshold value is specified below which a node would be considered malicious and as a result the node will be deleted from the reliable routes and information regarding the malicious node is broadcasted throughout the network. This method works far better than pure AODV (Ad hoc On Demand Distance Vector) and ensures efficient packet delivery even in the presence of malicious nodes. As per author [7], proposed a novel approach for detecting cooperative black hole nodes in the network and propagating information regarding malicious nodes throughout the network. For experimentation, three different scenarios are tested. In first, no malicious node is present, so the route is considered reliable for sending data. In second case, two cooperating malicious nodes are detected and information regarding them is propagated throughout the network. In third case, on finding a node to be reliable, information regarding its reliability is spread through the network. The proposed network works well in all scenarios and achieves success against black hole attack. Thus it ensures reliable route from source to destination. But the algorithm requires improvements in end-to-end delay as well as routing overhead. As per author [8], presented a couple of solutions that can be used as a strategy against the black hole attack in MANET (Mobile Ad hoc Network). First solution is to have multiple routes to destination and unicast ping packet to destination using multiple routes (assigning different packet ID's and sequence number). Upon checking the replies received from different routes, decision is made regarding the selection of a route for communication. In the second approach, sequence number is used for the verification of legitimate node. Two extra tables are maintained to record sequence number of the forwarded packets and sequence number of the received packets. If there is a mismatch between sequence number of received RREP (Route Reply) and the sequence number of the table, the route discovery process is started while alarming the whole network about the node. The scheme does not add overhead as sequence number itself is included in every packet in base protocol. As per author [9] presented a method to avoid malicious nodes from participating in the information exchange between two nodes and also reducing the network load. This method works on R-AODV (Reverse AODV), which states that a , a PEAK value is calculated by intermediate node using parameters viz. routing table sequence number, RREP sequence number and number of replies during a time interval. Maximum possible value acceptable as a sequence number is the PEAK value and if a RREP packet received has a sequence number higher than the PEAK value, the packet is simply discarded. In this way, only genuine RREP are received at the source. Thus it reduces the network traffic. This method increases the packet delivery ratio with acceptable routing overhead. As per author [10] Black hole attack is a common security issue encountered in Mobile Adhoc Network (MANET) routing protocol. In this paper a trust value for each node has been obtained depending upon the packet forwarding ability of the node. A rank is generated based on this trust value. In the route discovery step of the AODV routing protocol a path is chosen in such a way that more trusted nodes are involved. Also a node can be excluded which is not trusted from the route. Thus the packet is transferred through a more trusted path rather than the shortest path. Results of simulation through the use of OMNeT++ simulation software shows that higher threshold values gives less packet drops providing more reliable communication. As per author [12] Mobile ad hoc networks (MANETs) are established frequently when needed as of their improved nature. Wireless medium is accessible to malicious and legitimate users which makes the network much vulnerable to different internal and external attacks. Routing protocols for MANET are responsible for mobility of wireless networks and these are the common target of these threats. Ad hoc On-demand Distance Vector (AODV) is commonly employed and an efficient routing protocol. Black hole attack is a common active and internal attack which can misdirects the routing in reactive protocols. In this paper, a solution is proposed to avoid Black hole attack in AODV. Proposed solution uses a route legitimacy value attached with RREP which ensures that the route is free from black hole node. As per author [13] Security is an essential component for mobile ad hoc network (MANET). 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. Our proposed work presents a more efficient solution for detecting a black hole attack with less communication cost in the MANET, which is particularly vulnerable compared to infrastructure-based networks due to its mobility and shared broadcast nature. As an adversary can successfully deploy black hole attack in the network. It can be seen that proposed work is more secure than the existing solutions. We also compared its performance to standard AODV routing protocol. The experimental results show that the proposed approach is better than standard AODV. As per author **[14]** Mobile Ad hoc Network (MANET) is a self-configurable, self-maintenance network with wireless, mobile nodes. Special features of MANET like dynamic topology, hop-by-hop communications and open network boundary, made security highly challengeable in this network. From security aspect, routing protocols are highly vulnerable against a wide range of attacks like black hole. In black hole attack malicious node injects fault routing information to the network and leads all data packets toward it-self. In this paper, we proposed an approach to detect and eliminate cooperative malicious nodes in MANET with AODV routing protocol. A data control packet is used in order to check the nodes in selected path; also, by using an Extended Data Routing Information table, all malicious nodes in selected path are detected, then, eliminated from network. For evaluation, our approach and a previous work have been implemented using Opnet14 in different scenarios. Referring to simulation results, the proposed approach decreases packet overhead and delay of security mechanism with no false positive detection. In addition, network throughput is improved by using the proposed approach.

## III. CONCLUSION

Mobile Ad hoc Network (MANET) is a kind of Ad hoc network with mobile, wireless nodes. Its special characteristics like open network boundary, dynamic topology and wireless communications made security highly challengeable. Black Hole Attack disturbs normal network functionality by sending forged reply to the source node claims that it has fresh sequence number and shortest path towards destination [1].

In cooperative black hole attack, malicious node works together to defeat security mechanism. This approach detects and prevents cooperative malicious nodes in AODV-based MANET. A table is maintained in which ID's of all malicious node is maintained in order to reduce security mechanism. Our approach generates the safe path.

As future scope, the proposed security approach will detect and prevent all malicious nodes in network; either they work cooperatively or not.

## IV. REFERENCES

[1] Junhai Luo, Mingyu Fan, D. Ya, “Black Hole Attack Prevention Based on Authentication Mechanism”, ICCS, 2008.

[2] P. N. Raj and P. B. Swadas, “DPRAODV: A Dynamic Learning System against Black Hole Attack in AODV based MANET,” *IJCSI.*

[3] H. Simaremare and R. F. Sari, “Performance Evaluation of AODV variants on DDOS, Black hole and Malicious Attacks,” *International Journal of Computer Science and Network Security*, vol. 11, no. 6, pp. 277-287, 2011.

[4] P. Joshi, “Security Isues in Routing Protocols in MANET's at Network Layer,” *Procedia Computer Science*, no. 3, pp. 954-960, 2011.

[5] J. Sen, S. Koilakinda and A. Ukil, “A mechanism for Detection of Cooperative Black Hole Attack in Mobile Adhoc Network,” *International conference on Inteligent Systems, Modellingand Simulation*, pp. 338-343, 2011.

[6] F. Thachil and K. Shet, “A Trust Based Approach for AODV Protocol to mitigate Black Hole Attack in MANET,” *International conference on Computing Sciences*, pp. 281-285, 2012.

[7] K. Munjal, S. Verma and A. Bakshi, “Cooperative Black Hole Node Detection by Modifying AODV,” *International Journal of Management, IT and Engineering*, vol. 2, no. 8, pp. 484-501, 2012.

[8] N. Sharma and A. Sharma, “The Black Hole Node Attack in MANET,” *IEEE Second International conference on Advanced Computing and Communcation Technologies*, pp. 546-550, 2012.

[9] R. H. Jhaveri, S. J. Patel and D. C. Jinwala, “A Novel Approach for Gray Hole and Black Hole Attacks in Mobile Adhoc Nework,” *IEEE 2nd International conference on Advanced Computing and Communiaction Technologies*, pp. 556-560, 2012.

[10] Radha Krishna Bar, Jyotsna Kumar Mandal, M.M.Singh, “QoS of MANet Through Trust Based AODV Routing Protocol By Exclusion of Black Hole Attack”, International Conference on Computational Intelligence: Modeling Techniques and Applications (IMTA), 2013.

[11] Aarti, Dr. S. S. Tyagi, “Study on MANET: Characteristics, Challenges, Application & Security Attacks”, *ijarcsse*, Vol. 3, ISSN. 2277 128X, 2013.

[12] Ume-Rani Syed, Dr.ArifIqbal Vmar, Fahad Khurshid, “Avoidance of Black Hole Routes in AODV BasedMANET”, international Conference on Open Source Systems and Technologies (iCOSST), 2014.

[13] Vimal Kumar, Rakesh Kumar, “An Adaptive Approach for Detection of Blackhole Attack in Mobile Ad hoc Network”, Elsevier, 2015.

[14] Ali Dorri, “An EDRI-based approach for detecting and eliminating cooperative black hole nodes in MANET”, Springer, March 2016.