A Review of Black Hole and Worm Hole Attack on AODV Routing Protocol in MANET

Ms. Ankita M.Shendurkar[1], Prof. Nitin R.Chopde[2]
[1]ME-CSE (Scholar), G.H.R.C.E.M Department of Computer Science & Amravati University, India
[2]Asst.Professor, G.H.R.C.E.M Department of Computer Science & Amravati University, India

***Abstract*— The wireless mobile Ad-hoc network (MANET) is self-configuring mobile nodes connected through the wireless links with the decentralized networks where the nodes communicate with each other on the basis of mutual trust. For the network design, nature of the MANETs brings a new security challenges. Due to the dynamic infrastructure less nature and decentralized networks, wireless Ad-hoc networks are unprotected and vulnerable to the attack. In black hole attack, by sending false routing reply to the all nodes, malicious node advertises itself as having the shortest path. In Wormhole attack, a pair of attackers creates the tunnels to transfer the data packets from one end to another end by corrupting it. These attacks can affect the performance of the different routing protocol. This paper focuses on the study of the wormhole attack and black hole attack on AODV routing protocol.**

***Keywords*— MANET; AODV Routing Protocol; Black hole and Worm hole attack.**

I. INTRODUCTION

The Mobile Ad-hoc Network (MANET) is a collection of self-configuring formed with the wireless link mobile nodes where each node in MANETs is free to move independently with infrastructure less and decentralized network. A MANET having fundamental characteristics [1], [2], such as open medium, dynamic topology, distributed cooperation, and multi-hop routing. Due to these characteristics, wireless mobile ad-hoc network are vulnerable to the attacks. For the basic functionality of the network, security is the most important concern in the mobile Ad-hoc network. MANETs are vulnerable to various types of attack, such that active and passive attacks. In passive attacks, within the transmission range the attackers attempt to discover valuable information. On the other hand, active attacks, attackers attempt to disrupt the operation of communication [3]. Each node in MANET acts a router that forwards data packets to other nodes. Therefore, there are three types of routing protocol: Proactive Protocols, Reactive Protocols and Hybrid Protocols. Proactive protocols are table-driven that constantly update lists of destinations and routes. Reactive protocols respond on demand. Hybrid protocols combine the features of reactive and proactive protocols. In wormhole attack, pair of attackers creates the tunnels to transfer the data Packets and reply them into the network. This attack has a tremendous effect on wireless networks, especially against routing protocols. In type of two ended wormhole, Wormhole attacker records packets at one end in the network and tunnels them to other end-point in the network. One end tunnels the packet via wormhole link and other end on receiving the packets and replies them to the local area [4]. In black hole attack, a malicious node acts as black hole to attract all the traffic in the network, where incoming traffic is silently dropped without informing the source that the data did not reach to the intended destination. This paper presents the study of wormhole attack and black hole attack over mobile AD-hoc networks and analysis its impact on data communication when using a reactive routing protocol. Ad-hoc on demand Distance Vector (AODV) is reactive routing protocol [5]. The important feature of AODV is the maintenance of time based states. This means that routing entry which is not used recently is expired. The intermediate nodes store the route information in the form of route table [4]. The rest of the paper is structures as follows. In Section II, we will discuss various kinds of existing attacks on MANETs and their detection methods as part of related work. In section III, we will discuss the Ad-hoc on demand Distance Vector (AODV) [routing protocol]. In section IV and V, we discuss the black hole attack and wormhole attack over the AODV routing protocol in MANETs. In this we analyse the effect of black

hole attack and wormhole attack over the AODV routing protocol. In section VI, presents the conclusion of the paper is presented.

II. Literature survey

MANET is very much popular due to the fact that these networks are dynamic, infrastructure less and scalability. Despite the fact of the popularity of MANET, these networks are very much exposed to attacks [6, 7]. In this section we study the various attacks that are proposed in the recent years working on these areas of attacks over MANETs. In a Black Hole attack, a malicious node sends fake routing information, claiming that it has an optimum route and causes other good nodes to route data packets through the malicious one When the malicious node receives an RREQ message, it immediately sends a false RREP message with a high sequence number and minimum hop count without checking its routing table to make an entry in the routing table of the source node, before other nodes replies to absorb transmitted data from source to that destination and drop them instead of forwarding [8]. In Neighbourhood-based and Routing Recovery Scheme The detection scheme used neighbourhood-based method to detect the black hole attack and then present a routing recovery protocol to build the true path to the destination. Based on the neighbour set information, a method is designed to deal with the black hole attack, which consists of two parts: detection and response. In detection procedure, two major steps are: Step 1- Collect neighbour set information. Step 2-Determine whether there exists a black hole attack. In Response procedure, Source node sends a modify-Route-Entry (MRE) control packet to the Destination node to form a correct path by modifying the routing entries of the intermediate nodes (IM) from source to destination. Advantages of this scheme effectively and efficiently detect black hole attack without introducing much routing control overhead to the network [9]. Wormhole attack which is also known as the tunnelling attack this attack is possible even if the attacker has not compromised any other legitimate nodes and even if all communication provides authenticity and confidentiality. Hence it is one of the most severe and sophisticated attacks. In [10] a path based detection method is proposed, in which every node is not supposed to watch every other node in their neighbourhood, but in the current route path it only observes the next hop. There is no overhead of sending extra control packets for detecting wormhole attack. Many solutions have been proposed to combat on Wormhole attack, one of the solution proposed by **Deng** [11] gives the approach of disabling the reply message by the intermediate. This method avoids the intermediate node to reply which avoid in certain case the Wormhole and implements the secure protocol. The solution proposed in [12] focus on the requirement of a source node to wait unless the arrival of the RREP packet from more than two nodes. When it receives multiple RREPs the source node check that there is any share hops or not. The source node will consider the routed safe if it finds the share hops. Its drawback is the introduction of time delay it has to wait for the arrival of multiple RREPs before it judges the authentication of the node.

III.AODV Routing Protocol

AODV (Ad-hoc on Demand Distance Vector) is a reactive routing protocol [13] and it works as follows. Whenever a node wants to communicate with another node, it looks for an available path to the destination node, in its local routing table. If there is no path exists, then it broadcasts a route request (RREQ) message to its neighbourhood nodes. Any node that receives this message for route discovery looks for a path leading to the respective destination node. Control messages used for the discovery and breakage of route are as follows: Route Request Message (RREQ), Route Reply Message (RREP) and Route Error Message (RERR) Every node in an Ad hoc network maintains a routing table, which contains information about the route to a particular destination. The routing operations of AODV [14] generally consist of two phases: Route discovery and Route maintenance.

Route Discovery: Route discovery is performed through broadcasting RREQ message. Whenever a node needs to send data packets to a destination, it first checks if it has an existing route in the routing table. If not, the source node will initiate a RREQ and broadcast this request to all the neighbours. Then neighbouring nodes will update their routing table according to the received message. When RREQ reaches the destination, a RREP will be generated by the destination node as a response to RREQ. The RREP will be transmitted back to the originator of RREQ in order to inform the route. If an intermediate node has an active route towards destination, it can reply the RREQ with a RREP, which is called Gratuitous Route Reply. The intermediate node will also send an RREP to destination node. The RREP will be sent in reverse route of RREQ if a bidirectional link exists.

Route Maintenance: It is performed with two additional messages: Hello and RRER messages. Each node broadcast Hello messages periodically to inform neighbours about its connectivity. The receiving of Hello message proves that there is an active route towards the originator. Each forwarding node should keep track of its continued connectivity to its active next hops. If a link to the next hop cannot be detected during a period of timeout, a RRER message will be broadcasted to inform the loss of connectivity. On receiving this RRER, usually a local repair will be performed just for maintenance. The expired route will be deleted after the confirmation of its unavailability.

IV. Operation of Black hole attack in AODV

MANETs are vulnerable to various attacks due to the factors described in the introduction section of this literature. These attacks directly pose threat to the important network layers such as physical, data link and network layer which are responsible for routing mechanism of the network, Attacks in network layer can either cause Denial of Service (DoS) by not forwarding the packet or add and modify the routing parameters such as hop count and sequence number in control messages, When the malicious node is chosen as route to the destination, it stops forwarding the data packets. In black hole attack, the malicious node waits for its neighbour to send a RREQ packet. Upon receiving the RREQ packet, the malicious node immediately sends a forged RREP to the source node with a modified higher sequence number. In such a case, the source node assumes that the node is having a fresh route towards destination. The source node discards the RREP packets it receives from other nodes having genuine route and send data packets through malicious node. A malicious node takes all routes towards it and does not allow forwarding any packet. This attack is called black hole as it allows (drops) all data packets [15]. In figure, S and D are assumed to be source and destination nodes respectively. Let M is the malicious node. S being the source node would initiate the route discovery process and broadcasts a RREQ that is received by the nodes B, M and E being the neighbours of node S. Upon receiving the RREQ from the node S, node B and E makes a search to their cache for a fresh route to the destination. Non availability or older entry in their route table causes nodes to rebroadcast the RREQ and this process is continued till the RREQ arrives at node D. But node M claims to have the fresh route to destination and sends RREP packet to the source node S. The reply from the malicious node reaches the source node much earlier than other legitimate nodes, as the malicious nodes does not have to check its routing table. Nodes those have route to the destination would update their route table with the accumulated hop count and the destination sequence number of the destination node and generate a RREP control message. The destination sequence number that determines the freshness of a route is a 32-bit integer associated with every route [16]. The malicious node claims to have a fresher route by including a very high destination sequence number in RREP packet. The source node chooses the path provided by the malicious node and starts sending the data packets, which are dropped by the malicious node.

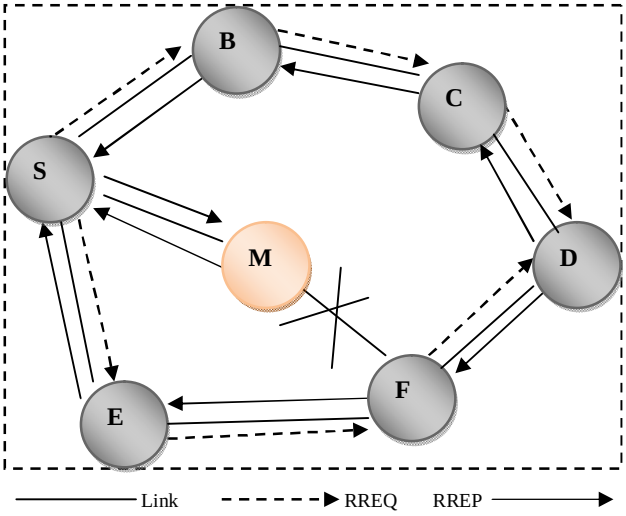

Fig: Black hole attack on AODV in MANET.

V. Operation of Wormhole attack in AODV

Wormhole attack is a kind of replay attack that is particularly challenging in MANET to defend against. Even if, the routing information is confidential, encrypted or authenticated, it can be very effective and damaging. An attacker can tunnel a request packet RREQ directly to the destination node without increasing the hop-count value. Thus it prevents any other routes from being discovered. It may badly disrupt communication as AODV would be unable to find routes longer than one or two hops. It is easy for the attacker to make the tunneled packet arrive with better metric than a normal multi-hop route for tunneled distances longer than the typical transmission range of a single hop. Malicious nodes can retransmit eavesdropped messages again in a channel that is exclusively available to attacker. The wormhole attack can be merged with the message dropping attack to prevent the destination node from receiving packets. Wormhole attack [17] commonly involves two remote malicious nodes shown as X and Y in Figure. X and Y both are connected via a wormhole link and they target to attack the source node S. During path discovery process, S broadcasts RREQ to a destination node D. Thus, A and C, neighbors of S, receive RREQ and forward RREQ to their neighbors. Now the malicious node X that receives RREQ forwarded by A. It records and tunnels the RREQ via the high-speed wormhole link to its partner Y. Malicious node Y forwards RREQ to its neighbor B. Finally, B forwards it to destination D. Thus, RREQ is forwarded via S-A-X-Y-B-D. On the other hand, other RREQ packet is also forwarded through the path S-C-D-E-F-G-D. However, as X and Y are connected via a high speed bus, RREQ from S-A-X-Y-B-D reaches fist to D. Therefore, destination D ignores the RREQ that reaches later and chooses D-B-A-S to unicast an RREP packet to the source node S. As a result, S chooses S-A-B-D route to send data that indeed passes through X and Y malicious nodes that are very well placed compared to other nodes in the network. Thus, a wormhole attack is not that difficult to set up, but still can be immensely harmful for a MANET. Moreover, finding better techniques for detection of wormhole attacks and securing AODV against them still remains a big challenge in Mobile Ad-hoc Networks.

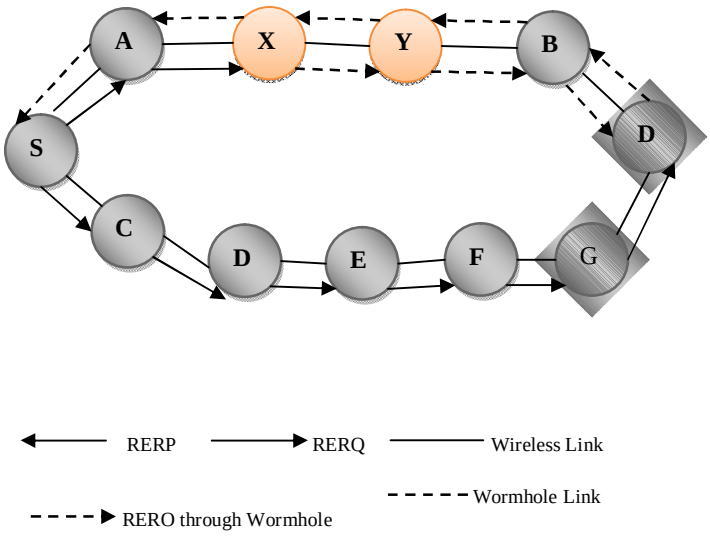

Fig: wormhole attack on AODV in MANET [17].

VI. Conclusions

As there is increasing threats of attacks on the mobile network, MANETs must have a secure way of transmission and communication and this quite challenging and vital issue In this paper we study the black hole and wormhole attack on routing protocol AODV in MANETs. In this section the black hole attack is more effective in MANETs as compared to the wormhole attack. This is due to the fact that in black hole attack the attacker forcefully makes himself an intermediate node on a selected route. Due to this the attacker is almost always able to launch an attack during the communication process. On the other hand, in case of wormhole attack the effect of attack is not always very high and highly depends on the position of both the colluding attackers.

ACKNOWEDGEMENT

I would like to thank to all the people those who have help me to give the knowledge about these research papers and I thankful to my guide with whose guidance I would have completed my research paper and make it to published, finally I like to thank to all the website and IEEE paper which I have gone through and have refer to create my review paper successful.

REFERENCES

[1] J. Gronkvist, A. Hansson, and M. Skold, "*Evaluation of a Specification-Based Intrusion Detection System for AODV*". 2007.

[2] S. Kurosawa, H. Nakayama, and N. Kato, "*Detecting black hole attack on AODV based mobile ad-hoc networks by dynamic learning method*," International Journal of Network Security, pp. 338–346, 2007.

[3] West off, D., Paul K, "Context Aware Detection of Selfish Nodes in DSR based Ad Hoc Networks", IEEE GLOBECOM. Taipei, Taiwan, pp. 178-182, 2002.

[4] Gurpreet Kaur, Er. Sandeep Kaur Dhanda, "*Analyzing the effect of Wormhole Attack on Routing Protocol in Wireless Sensor Network"*, International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 8, August 2013

[5] C.E. Perkins and E.M. Royer. "*Ad-hoc on-demand distance vector routing*". In Second IEEE Workshop on Mobile Computing System and Application, WMCSA 99, pages 90 –100, Feb. 1999

[6] Y.F.Alem, Z.C.Xuan, "*Preventing Wormhole Attack in Mobile Ad-hoc Networks Using Anomaly Detection"*, 2nd International Conference on Future Computer and Communication (ICFCC 2010), Vol. 3, pp. 672-676, May, 2010.

[7]. M.Parsons, P.Ebinger, "*Performance Evaluation of the Impact of Attacks on mobile Ad-Hoc Networks*" April. 10, 2010.

[8] M Al-Shurman, S-M Yoo and S. Park, "*Black Hole Attack in Mobile Ad Hoc Networks*", ACM Southeast Regional Conf, 2004.

[9] Y.-C. Hu, D. B. Johnson, and A. Perrig, "*Secure efficient distance vector routing for mobile wireless ad-hoc networks*," Proceedings of the Fourth IEEE Workshop on Mobile Computing Systems and Applications, 2002.

[10] C.Jiwen, Y.Ping, C.Jialin, W.Zhiyang, L.Ning, " *An Adaptive Approach to Detecting Black and Gray Hole Attacks in Ad Hoc Network*",24th IEEE International Conference on Advance Information Networking and Application (AINA 2010), pp. 775-780, April,2010.

[11] J. W. Creswell," *Research Design: Qualitative, Quantitative and Mixed Methods Approach*", 2nd Ed, Sage Publications Inc, California, July 2002.

[12] P.A.R Kumar, S.Selvakumar, "*Distribute Denial-of-Service (DDoS) Threat in Collaborative Environment A survey of DDoS Attack Tools and Traceback Mechanism"*,

IEEE International Advance Computing Conference (IACC 2009), pp. 1275-1280, March, 2009.

[13] Kamini, Rakesh K "*VANET Parameters and Applications: A Review"*, Global Journal of Computer Science and Technology, September 2010.

[14] C.E. Perkins and E.M. Royer *"Ad-Hoc on-Demand Distance Vector Routing,"* Proc. of IEEE Workshop Mobile Computing Systems and Applications, pp 90-100, 1999.

[15] Dokurer, Semih "*Simulation of Black hole attack in wireless Ad-Hoc networks*", Master's thesis, Atihm University, September 2006.

[16] Santoshi Kurosawal, hidehisa, Nakayama, Nei Kato, Abbas, Jamalipour and Yoshiaki, Nemoto. "*Detecting Black hole Attack on AODV based Mobile Ad Hoc Networks by Dynamic Learning Method*" in International Journal of Network Security, Vol.5, No.3, pp.338-346, Nov.2007.

[17] Rashid Hafeez Khokhar, Md Asri Ngadi and Satira Mandala, *"A Review of Current Routing Attacks in Mobile Ad Hoc Networks"*, International Journal of Computer Science and Security, pp. 18-29, Volume-2 Issue-3, 2009.