International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 06 | June-2016 www.irjet.net p-ISSN: 2395-0072

Attacks on Ad hoc On-Demand Distance Vector Routing in MANET

Geetika Sharma[1], Anupam Mittal[2], Ruchi Aggarwal[3]

[1] *Geetika Sharma,* Department of Computer Sci. & Engineering, Chandigarh University, Mohali, India
[2]*Anupam Mittal,* Department of Computer Sci. & Engineering, Chandigarh University, Mohali, India
[3] *Ruchi Aggarwal,* Department of Computer Sci. & Engineering, Chandigarh University, Mohali, India

---

Abstract: *A Mobile Ad-Hoc Network is a self-configured collection of mobile nodes in which there is no need of predefined infrastructure. In this network nodes can arbitrarily change their geographic locations. MANET is more vulnerable to cyber attacks than wired networks because of no any central coordination mechanism. The Black hole attack at network layer is the most attention seeking attack in AODV routing protocol as compared to other protocols. This paper presents a review of Black hole attack in AODV routing protocol.*

Keywords: MANET, AODV, Security, Black hole Attack, Worm Hole Attack,Grey Hole Attack, Detection and Prevention Techniques.

INTRODUCTION

The Mobile Ad-hoc Network (MANET) is a collection of selfconfiguring 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.

AODV Routing Protocols

The AODV routing protocol is an adaptation of the DSDV protocol for dynamic link conditions. Every node in an ad hoc network maintains a routing table, which contains information about the route to a particular destination. Whenever a packet is to be sent by a node, it first checks with its routing table to determine whether a route to the destination is already available. If so, it uses that route to send the packets to the destination. If a route is not available or the previously entered route is inactivated, then the node initiates a route discovery process. A RREQ (Route REQuest) packet is broadcasted by the node. Every node that receives the RREQ packet first checks if it is the destination for that packet and if so, it sends back an RREP (Route Reply) packet. If it is not the destination, then it checks with its routing table to determine if it has got a route to the destination. If not, it relays the RREQ packet by broadcasting it to its neighbors. If its routing table does contain an entry to the destination, then the next step is the comparison of the 'Destination Sequence' number in its routing table to that present in the RREQ packet. This Destination Sequence number is the sequence number of the last sent packet from the destination to the source. If the destination sequence number present in the routing table is lesser than or equal to the one contained in the RREQ packet, then the node relays the request further to its neighbors. If the number in the routing table is higher than the number in the packet, it denotes that the route is a 'fresh route' and packets can be sent through this route. This intermediate node then sends a RREP packet to the node through which it received the RREQ packet. The RREP packet gets relayed back to the source through the reverse route. The source node then updates its routing table and sends its packet through this route. During the operation, if any node identifies a link failure it sends a RERR (Route ERRor) packet to all other nodes that uses this link for their communication to other nodes.

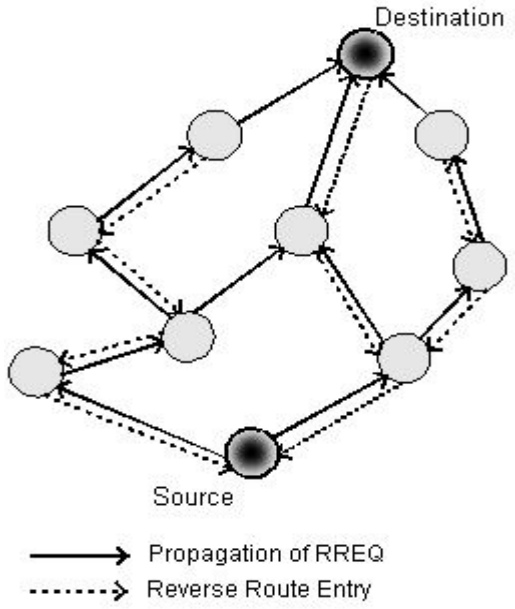

Fig. 1a- Propagation of RREQ.

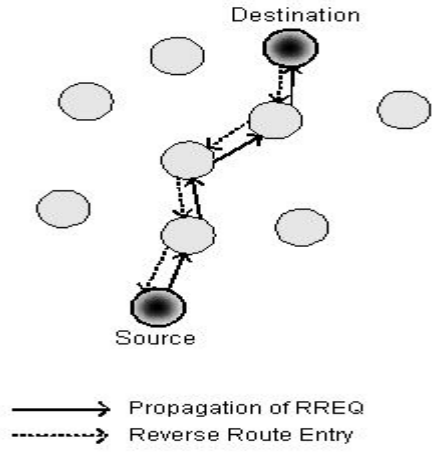

Fig. 1b- Propagation of RREP

BLACK HOLE ATTACK IN AODV

In Black hole attack a malicious node advertises about the shortest path to the node whose packets it wants to intercept [5].In following figure, imagine, M is malicious node. When node A broadcasts a RREQ packet, nodes B, D and M receive it. Node M, being a malicious node, this node does not check up with its routing table for the requested route to node E. Hence, it immediately sends back a RREP packet, claiming that it has a route to the destination.

Internal Black hole attack This type of black hole attack has an internal malicious node which fits in between the routes of given source and destination, when it gets the chance this malicious node makes itself an active data route element. Now this node is capable of conducting attack with the start of data transmission. This is an internal attack because node itself belongs to the data route.

External black hole attack External attack physically stays outside of the network and denies access to network. External attack can become a kind of internal attack when it take a control of internal malicious node and control it to attack other nodes in MANET.

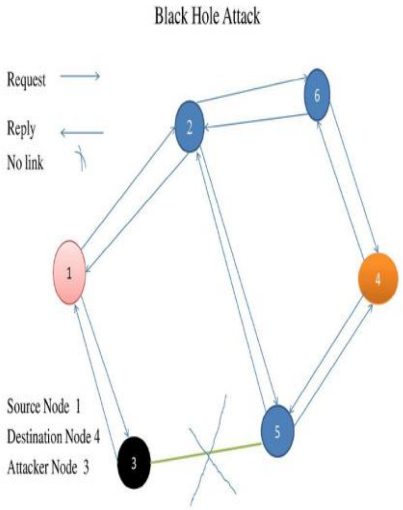

Fig. 1c- Black Hole Attack

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.

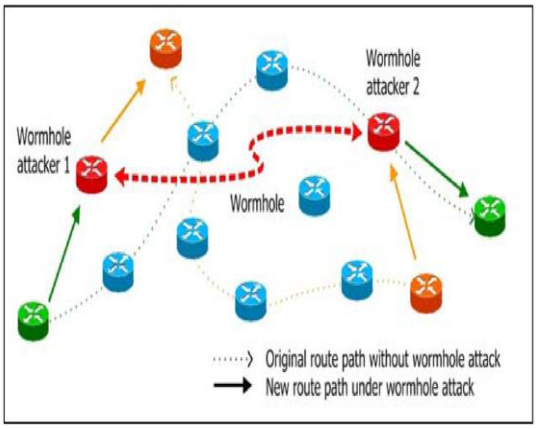

Fig. 1d- Worm Hole Attack

GRAY HOLE ATTACK

Gray hole attack is bit similar to black hole attack with a small variation where the malicious node does node drop the whole packets instead it will drop some selective packets. In Gray hole [2] attack, a node which is member of the network, gets RREQ packets and create a route to destination. After creating the route, it drops some of data packets. Gray hole attack is very difficult to detect because malicious node do not drop data packets regularly but instead it will drop the data packets occasionally. Therefore sometimes node will act normal node and sometime node switch to malicious node.

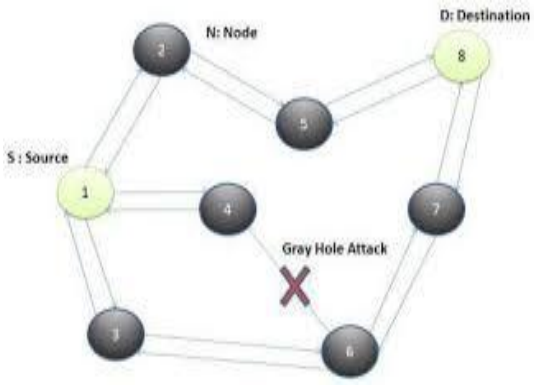

Fig. 1e- Grey Hole Attack

IV. LITERATURE SURVEY

In this section, we review different methods for the detection and prevention of various attacks in AODV based mobile ad-hoc networks.

DPRAODV(Detection,Prevention and Reactive AODV) scheme : In this paper authors proposed have proposed the method DPRAODV[15] (A dynamic learning system against black hole attack in AODV based MANET) to prevent security of black hole by informing other nodes in the network. In normal AODV, the node that receives the RREP packet first checks the value of sequence number in its routing table. If its sequence number is higher than the one in routing table, this RREP packet is accepted. In this solution, it has an addition check whether the RREP sequence number is higher than the threshold value. If it is higher than the threshold value, then the node is considered to be malicious node and it adds to the black list.

ABM (Anti-Blackhole Mechanism) scheme :This paper attempts to detect and separate malicious nodes, which selectively perform black hole attacks by deploying IDSs in MANETs (mobile ad hoc networks). All IDS nodes perform an ABM (Anti-Blackhole Mechanism), which estimates the suspicious value of a node, according to the amount of abnormal difference between RREQs and RREPs transmitted from the node.

Honeypot based detection scheme :Athors propose a novel strategy by employing mobile honeypot agents that utilize their topological knowledge and detect such spurious route advertisements. They are deployed as roaming software agents that tour the network and lure attackers by sending route request advertisements. We collect valuable information on attacker's strategy from the intrusion logs gathered at a given honeypot[9] Drawbacks: proposed algorithm is for WMN not for MANET.as it is proactive mechanism, it will generate lots of traffic. honey pot has lack of centralized authority control.

ERDA (Enhance Route Discovery for AODV) scheme Have designed an ERDA solution to improve AODV protocol with minimum modification to the existing route discovery mechanism recvReply() function. a method called ERDA (Enhance Route Discovery for AODV). The proposed method is able to mitigate the a foresaid problem by introducing new conditions in the routing table update process and also by adding simple maliciousnode detection and isolation process to the AODV route discovery mechanism.

Cryptographic based technique : This paper focuse that many investigations have been done in order to improve the security in MANETs, most of which are relied on cryptographic based techniques in order to guarantee some properties such as data integrity and availability. These techniques cannot prevent a malicious node from dropping packets supposed to be relayed.

Time-based Threshold Detection Scheme :propose algorithm enhancement of the original AODV routing protocol. In this, one timer is set into the Timer Expired Table which is collect the request of other node after receiving the first node's request. Collect Rout Reply Table includes the packet sequence number and received time. After that counting the timeout value using arriving time and based on threshold value take decision for the route.

Effective Filtering Technique[8] :In this technique author proposed a new mechanism to prevent RREQ flooding attack; this technique can detect the malicious nodes and attacker nodes, which are disturbing the network communication. In this technique there are two thresholds RATE_LIMIT and BLACKLIST_LIMIT, which are used to limit the RREQ message. RATE_LIMIT parameter indicates no. of RREQ that can be known and managed. Here each node monitors the RREQ and maintain a count table for RREQ received.

Anonymous Secure Routing protocol Technique[9]: In this technique presented anonymous communication. In this paper, three main components are used: white listing threshold, blacklist threshold and transmission threshold. This component displays the threshold limit of request packets sent by the neighboring performance analysis of flooding Attack. In RREQ flooding attack the invader selects numerous IP addresses which are not present in the network or choose arbitrary IP addresses dependent on information about range of the IP address in the network. Exhausting neighborhood suppression method, a single threshold is established for all neighboring node. In Data flooding attack the invader node first sets up the path to all the nodes and send useless packet.

Trust Estimation Technique[10] A trust estimator is used in every node to estimate the trust level of its neighboring nodes. The trust level is a function of various factors like, ratio of number of packets received intact from the neighbor to the total number of received packets from that node, ratio of the number of packets forwarded successfully by the neighbor to the total number of packets sent to that neighbor average time taken to respond to a route request etc. This technique proposed a distributive approach to identified and prevent the flooding attack.

V. CONCLUSION

There is no fix mechanism to detect or prevent the attacks researcher finds new methods to detect these attack. To detect multiple attack there is one or combinations of two methods are used. As discussed above methods are implementing in AODV or in DSR routing protocol. The proactive based method gives higher packet delivery ratio but it creates more overhead. Whereas, reactive based method gives lower overhead but the packet loss is higher. So hybrid method is solution of that problem. Combining both proactive and reactive method we get the better results.

VI. References

[1] Pradip M. Jawandhiya and Mangesh M. Ghonge, "A Survey of Mobile Adhoc Network Attacks", International Journal of Engineering Science and Technology, Vol. 2(9), pp.- 4063- 4071, 2010.

[2] A. Mishra and K..M.Nadkarni, Security in Wireless Ad -hoc Network, in Book. "The Hand Book of Ad Hoc Wireless Networks" (chapter 30) , 2003.

[3] Robinpreet Kaur & Mritunjay Kumar Rai, " A Novel Review on Routing Protocols in MANETs", Undergraduate Academic Research Journal (UARJ), Volume-1, Issue-1, pp. 103-108, 2012

[4] Siva Ram Murthy and B.S.Manoj, "Ad hoc Wireless Networks"(Chapter 7),2014.

[5] E.M.Royer and C.E.Perkins "Adhoc On-Demand Distance Vector Routing", IEEE, February 1999.

[6] Datuk Prof Ir Ishak Ismail and Mohd Hairil Fitri Ja'afar," Mobile Ad Hoc Network Overview", IEEE, December 2007.

[7] Ruchita Meher and Seema Ladhe," Review Paper on Flooding Attack in MANET", International Journal of Engineering Research and Applications, pp. 39-46,January 2014. [8] Jian-Hua Song, Fan Hong and Yu Zhang, "Effective Filtering Scheme against RREQ Flooding Attack in Mobile Ad Hoc Networks", IEEE, 2006.

[9] Venkat Balakrishnan, Vijay Varadharajan ,and Uday Tupakula" Mitigating Flooding attacks in Mobile Ad-hoc Networks Supporting Anonymous Communications", IEEE, 2007.

[11] Anoosha Prathapani,Lakshmi Santhanam,Dharma P. Agrawal," Detection of blackhole attack in aWireless MeshNetwork using intelligent honeypot agents" Springer Science+Business Media, LLC 2011

[12] Lalit Himral, Vishal Vig, Nagesh Chand, "Preventing AODV Routing Protocol from Black Hole Attack"

International Journal of Engineering Science and Technology (IJEST) Vol. 3 No. 5 May 2011.

[13] Sreedhar. C, Dr. S. Madhusudhana Verma and Dr. N. Kasiviswanath, "POTENTIAL SECURITY ATTACKS ON WIRELESS NETWORKS AN THEIR COUNTERMEASURE", International journal of computer science & information Technology (IJCSIT) Vol.2, No.5, October 2010

[14] Nital Mistry, Devesh C Jinwala, Mukesh Zaveri, "Improving AODV Protocol against Blackhole Attacks", proceedings of the International Multi Conference of Engineers and Computer Scientists 2010 Vol II, IMECS 2010.

[15] Payal N. Raj, Prashant B. Swadas" DPRAODV: A Dyanamic Learning System Against Blackhole Attack In AODV Based Manet." arXiv:0909.2371,2009.

[16] H. Deng, W. Li and D. P. Agrawal, Routing security in wireless ad hoc networks, IEEE Commun. Mag., 40(10): 70-75, October 2002.

[17] Lidong Zhou, and Zygmunt J. Haas, "Securing Ad Hoc Networks," IEEE Network Magazine, vol. 13, no.6, November/December 1999.

[18]http://www.faqs.org/rfcs/rfc3561.html