A STUDY ON BLACKHOLE ATTACKS IN ADHOC NETWORKS

JOY JEBA MERLINE.S [1], *GEETHA PRIYA.S* [2], SHINU P.S[3],ROSHINI .R[4],SANTHIYA.G[5]

[1] *JOY JEBA MERLINE.S, ASSISTANT PROFESSOR, VLB JANAKIAMMAL COLLEGE OF ARTS AND SCIENCE, TAMIL NADU, INDIA*
[2] *GEETHA PRIYA.S, ASSISTANT PROFESSOR, VLB JANAKIAMMAL COLLEGE OF ARTS AND SCIENCE, TAMIL NADU, INDIA*
[3] *SHINU P.S, STUDENT, VLB JANAKIAMMAL COLLEGE OF ARTS AND SCIENCE, TAMIL NADU, INDIA*
[4] *ROSHINI .R, STUDENT, VLB JANAKIAMMAL COLLEGE OF ARTS AND SCIENCE, TAMIL NADU, INDIA*
[5] *SANTHIYA.G, STUDENT, SRI KRISHNA COLLEGE OF ARTS AND SCIENCE, TAMIL NADU, INDIA*

ABSTRACT

A Mobile ad-hoc network (MANET) is a latest and emerging research topic among researchers. It is a continuously self-configuring, infrastructure-less network of mobile devices connected wirelessly. The MANET is mainly popular for the flexibility and independence of network infrastructure. Unique characteristic include dynamic network topology, limited power and limited bandwidth for communication. The general routing protocols used in ad-hoc network are AODV (ad-hoc on demand distance vector) protocol. AODV protocol is threatened by "Black Hole" attack. Black holes is a kind of denial of services in which places in the network where incoming or outgoing traffic is silently discarded , without informing the source that the data did not reach its intended recipient. In this, attack a malicious node advertises itself as having the4 shortest path to the destination node. To struggle with black hole attack so many solutions provided by researchers. In this article we study the routing security issue of MANET and analyze in detail about the "Black hole" attack.

Keyword: - ***MANETs (Mobile ad hoc networks), Black hole attack, RREP, AODV, security.***

1. INTRODUCTION

A mobile ad hoc network (MANET) is a collection of mobile devices that can communicate each other without the use of a predefined infrastructure or centralized administration. Nodes can communicate directly however, nodes present outside on each other's range have to rely on some other nodes to transmit messages [1]. Due to the mobility nature of nodes, the network topology changes rapidly and randomly changed over time.

MANETs have many budding applications, like Sensor Networks, Medical Service, Personal Area Network, especially in military and res-cue operations such as connecting soldiers in the battlefield or creating a temporary network in place of one, which collapsed after a disaster like tsunami [2].

Limited bandwidth and limited battery power is another characteristic of a MANET. It makes routing in a MANET an even more challenging task. Therefore providing routing service with minimum cost in terms of bandwidth and battery power is focused by the MANET. There are a variety of attacks that target the weakness of MANET. For example, routing messages are an essential component of mobile network communications, as each packet needs to be passed quickly through intermediate nodes, which the packet must traverse from a source to the destination.

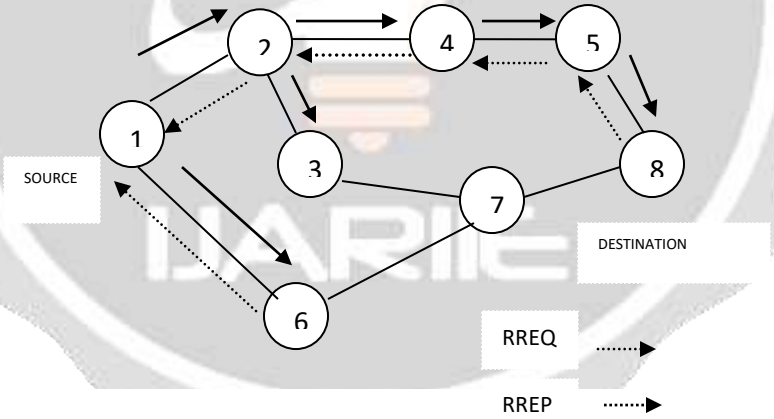
Malicious routing attacks can target the routing discovery or maintenance phase by not following the specifications of the routing protocols. There are also attacks that target some particular routing protocols, such as DSR, or AODV [3] [4].The primary goal of such an ad hoc network routing protocols are correct and efficient route establishment between a pair of nodes so that messages can be delivered in a timely manner[5].

2. OVERVIEW OF AODV ROUTING PROTOCOL

The Ad Hoc On-Demand Distance Vector (AODV) is a routing protocol for MANET and other wireless device. This protocol's algorithm creates routes between nodes when the source nodes request for the routes, giving the network the ability to be flexible to allow nodes to enter and leave the network. Routes remain lively as long as data packets are moving along the paths from the source to the destination. When the source stops sending packets, the path will get time out and will be closed. AODV, when a source node S has to send a data packet to a destination node D and does not have a route to D, it initiate route discovery by spreading a route request (RREQ) to its neighbors. The nodes which are neighbor to the source who receive this RREQ rebroadcast the similar RREQ to their neighbors. It is repeated until the RREQ reaches the destination node. Upon receiving the first arrived RREQ, route reply (RREP) is send to the source node by the destination node through the reverse path where the RREQ will be arrived. The same RREQ which arrive later will be unnoticed by the destination node. In addition, AODV enables the middle nodes to generate and send a RREP to the source node that have sufficiently fresh routes. Whenever the node sends a packet, it first checks with its routing table to conclude whether route to the destination is available earlier. It uses that route to send the packets to the destination. If a route is not present or the previously entered route is inactivated, then the node initiates a route finding process RREQ (Route Request).

3. BLACK HOLE ATTACK ON AODV PROTOCOL

In networking area, black holes refer to the networking places where arriving or departing traffic is silently dropped without notifying the source that the data did not reach its intended recipient. Black hole attack, a malicious node uses its routing protocol for releasing false news, having the shortest way to the packet or to the destination node. This black hole node advertises its easiness of understanding to new routes irrespective of checking its routing table in the attacker node will also have the availability in replying to the route request and thus stop the data packet and get back it (Biswas et al 2007). In this type, a malicious node waits for the Route Request message (RREQ) from the neighbor nodes. When it receives the RREQ message, a false RREP is send with high sequence number to the source node. The source node assumes that the route is new route. However, when the data packet is send by the source node to the destination node by using this route, the malicious node does not relay the packet and absorbs all data packet.



In the above diagram, 6 is the malicious node and 1 and 2 are the source node and destination node respectively. In the beginning, the source node 1 broadcasts RREQ packet to its one step neighbors. Then, on receiving this packet each neighbor node is supposed to rebroadcast it if a route cache towards the destination is unavailable. However, the node 6 disobeys this rule and privileges that it has the shortest path to the destination and sends a RREP packet back to node 1. Consequently, if the RREP packet sent by node 8 which has a new route to 8, reaches the node 1 before the 6ths RREP then everything will work normally. Else, the source node 1 estimates that the route fleeting through the node 6 is the shortest path, and will start transmitting data packets towards 6 which will drop them.

4. SECURUTY THREATS IN MOBILE AD HOC NETWORK

All the Routing protocols are vulnerable to different security attacks. Attacks could be generally divided into two categories as passive attack and active attack.

- Passive attack: The attacker only tries to get the essential information in the network traffic but doesn't affect with the usual operation of the network routing protocols.

- Active attack: The attacker modifies, fabricates, injects, forges or drops the exchanged data, which results in disturbances in the normal network. Some of the actions proposed in connection may include the black hole. Black hole Attack, a type of Denial of Service Attack (Ranjan et al 2015) [7]. Black hole Attack can be a malicious node uses its routing protocol to support itself obtain shortest path towards destination node.

5. SOLUTIONS TO BLACK HOLE ATTACKING MANET

GayatriWahane et.al. [9] Proposed that detection and protection against Black hole attack using secure knowledge algorithm.It provides good performance in terms of energy consumer and minimum packet loss.

Al-Shurman et.al [10] Proposed a solution that a source code is required to wait until a RREP packet arrives from more than two nodes. On receiving multiple RREPs, the source node confirms a shared hop or not. The source node desires that the route is safe, when there is a shared hop. The main drawback of this solution is that time delay is introduced it wait until multiple RREPs arrive.

Hesiri Weerasingh et al [11] concluded that the detecting Black hole Attack on AODV-Based Mobile Ad Hoc Networks by Dynamic Learning Method Black whole AODV compare with the earlier solutions in term of throughput rate and minimum packet loss has high performance.

Lalit Himral et.al [12] have proposed method to find the secured routes and prevent the malicious node in the MANET by inspecting whether there is large variation between the sequence number of source node or intermediate node who has sent back first RREP or not.

Rutvij H. Jhaveri et. al. (Rutvij Wahane et al [13] have proposed a method to mitigate Black hole and Gray whole Attacks in AODV. In this process, in memory PEAK value is allocated. PEAK value is calculated by using the Number of Sent Request and Number of Receive Reply. In this method, malicious node is detected using PEAK value. It maintains malicious node list inside routing table for RREQ and used to inform other nodes inside network about malicious nodes.

XiaoYang Zhang et.al. [14] Discussed a new detection method which checks RREP's sequence number of messages created by the destination. In this method, when intermediate nodes sends RREP packet , source node sends the control message in need of up-to- date SN to the destination node . After receiving, destination node replays with up-to-date SN to the source node. Source node checks whether the intermediate nodes RREP's SN is larger than up-to-date SN, to identify the fake RREP passed by intermediate node. In this method, network creates new packets highly, so it increases network overhead and time delay.

Alem, Y.F et.al. [15] Proposed a solution to prevent attacks from the both single and multiple black hole nodes to identify the Intrusion Detection using Anomaly Detection (IDAD). IDAD examines the work of each user and identifies the irregular activities from their normal activities. A review data is collected from set of irregular activities and transmitted to IDAD system. It compares the review data with the activity of each node, nodes with different activity which is out of review data is separated from the network. It minimizes the network overhead and provides faster communication when number of packets decreases.

Payal N. Raj et. Al [16]. varies the actions of AODV to include a method for examining the sequence number of the received RREP. Whenever Source node receives the RREP from its intermediate node, it compares the sequence number of RREP with threshold value to check whether it is greater. If it's so, replying node is suspected to be black hole node. Source nodes add the suspected node to its black list and produce a notification to advertise the black list for its neighbor nodes. The threshold value is calculated with the average of differences between the destination sequence number in the routing table and the destination sequence number in the RREP

within certain amount of time. Source node advertises the black hole to the neighbors so it can be ignored and eliminated by them easily.

6. CONCLUSIONS

At the present scenario MANET has additional features due to which it is accepted globally. MANET has so many features and has some security issues. In this paper we have just provide a list of solutions in MANET on a specific attack that is black hole attack. Many solutions are there which provide better security in case of single malicious node but they are not effective in case of multiple malicious node. Special hardware like GPS may be required for some solutions. A brief introduction is provided for each solution with their improvements and drawbacks in this paper. Future research work researchers have to focus on improving the efficiency of the security scheme as well as minimize the cost to make them suitable for a MANET environment.

7. REFERENCES

[1]. C. Perkins, Ad Hoc Networks, Addison-Wesley, 2001.
[2]. Sheikh R., Singh Chande, M., and Kumar Mishra D. Security issues in MANET: A review. Wireless And Optical
Communications Networks (WOCN), 2010 Seventh International Conference, pages 1–4, 2010.
[3]. M. Zapata, Secure Ad Hoc On-Demand Distance Vector(SAODV). Internet draft, draft-guerrero-manet-saodv-01.txt, 2002.
[4]. Y. Hu, A. Perrig, and D. Johnson, Ariadne: A Secure On-Demand Routing for Ad Hoc Networks. Proc. Of MobiCom 2002, Atlanta, 2002.
[5]. Madhusudhananagakumar K.S., and G. Aghila. A Survey on Black Hole Attacks on AODV Protocol in MANET.International Journal of Computer Applications, 34(7), 2011.
[6]. K. Biswas and Md. Liaqat Ali, "Security threats in Mobile Ad-Hoc Network", Master Thesis, Blekinge Institute of Technology" Sweden, 22nd March 2007.
[7]. Ranjan, Rakesh, Nirnemesh Kumar Singh, and Ajay Singh. "Security issues of black hole attacks in MANET"Computing, Communication & Automation (ICCCA), 2015 International Conference on. IEEE, 2015.
[8] Soufiene Djahel, Farid Naït-abdesselam, and Zonghua Zhang. Mitigating Packet Dropping Problem in Mobile Ad Hoc Networks: Proposals and Challenges. IEEE COMMUNICATIONS SURVEYS and TUTORIALS, 13(4), 2011.
[9]. Wahane, Gayatri, Ashok M. Kanthe, and Dina Simunic. "Detection of cooperative black hole attack using Crosschecking with truelink in MANET." Computational Intelligence and Networking Technologies (ICCCNT), 2013 Fourth International Conference on. IEEE, 2013.
[10]. Mohammad Al-Shurman et. Al" Black Hole Attack in Mobile Ad-Hoc Network" ACMSE'04, Apri l 2-3, 2004,Huntsville, AL, USA .
[11]. Hesiri Weerasinghe , 2011, on Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks Proceedings of the IEEE International Conference on Communications, Jun. 24-28
[12]. Lalit Himral, Vishal Vig, Nagesh Chand, "Preventing AODV Routing Protocol from Black Hole Attack" International Jtheynal of Engineeri ng Science and Technology (IJEST) Vol. 3 No. 5 May 2011.
[13]. Rutvij H. Jhaveri, Sankita J. Patel and Devesh C. Jinwala, "A Novel Approach for Gray Hole and Black Hole Attacks in mobile Ad-hoc Networks ", 2012 Second nternational Conference on Advanced Computing & Communication Technologies.
[14]. XiaoYang Zhang; Sekiya, Y.; Wakahara, Y., "Proposal of a method to detect black hole attack in MANET," Autonomous Decentralized Systems, 2009. ISADS '09. International Symposium on, vol., no., pp.1 - 6, 23 - 25 March 2009.
[15]. Alem, Y.F.; Zhao Cheng Xuan; , "Preventing black hole attack in mobile ad -hoc networks using Anomaly Detection," Future Computer and Communication (ICFCC), 2010 2nd
[16] Payal N. Raj1 and Prashant B. Swadas2, "DPRAODV: A Dynamic Learning System against Blackhole Attack in AODV based MANET", IJCSI International Jtheynal of Computer Science Issues, Vol. 2, 2009.