A Survey on Black Hole Attack on AODV Protocol in MANET

Rahul Agarwal[1], Dr. Narpat Singh Shekhawat[2]
[1]*Research Scholar, RTU, Kota, Rajasthan, India.*
[2]*Assistant Professor, Dept of CSE, GEC Bikaner, Rajasthan, India.*

Abstract- Mobile Adhoc Network (MANET) is a jumble of mobile nodes with self-framing network that effectively form a impermanent network without infrastructure.Security concern in mobile ad hoc network[5] (MANET) is a propitious research. It has huge numbers of operations typically in the field of Sensor Networks (SN), medical, military and rescue operations. Ad hoc On demand Distance Vector (AODV)[10] is one of the best applicable routing protocol for the MANETs and it is more liable to black hole attack by the malicious nodes. A malicious [7] node wrongly sends the RREP (route reply) that it has a latest route with least hop count to destination and then it dump all the receiving packets. This is called as black hole attack. In this paper, we have studied and discussed the existing solutions to black hole attacks on AODV protocol.

Keywords- MANET, Routing, AODV routing protocol and Black hole attack

I. INTRODUCTION

In Wireless communication network, communication between nodes in the network could be restrained by a central infrastructure, or it could be an infra structure-less which is called Ad hoc Networks. In recent years mobile ad hoc network [5](MANET) has a wide significance on wireless networks. Over wireless medium, ad hoc nodes are deployable anywhere in network, self-constructed, self coordinated, and are free to leave or join network. However, the non-infrastructure network planning gives rise to fussy security issues such as black hole, wormhole, flooding, and Sybil attacks. The detection of malicious[7] attacks in ad hoc networks[5] is important and demanding. MANETs are used at business meetings and conferences to covertly interchange data, at the library to connect the Internet with a laptop, and at hospitals to transfer secret data from a medical device to a doctor's PDA etc.

MANET routing protocols can be categorized as proactive or reactive routing protocols. In proactive (table-driven) routing protocols, each node keeps one or more tables that maintain routing data information to every other node in the network. While in reactive (on-demand) routing protocols, routes are generated whenever a source requires sending data to a destination node which means that source initiates these protocol whenever there is a demand.

Generally there are two methodologies by which manet works namely multi-hop: in this nodes works outside their radio range and peer-to-peer: in this nodes works inside their radio range MANET's attack are divided into active and passive attacks based on their attacking nature. In active attacks, the attacker nodes work by dropping the forwarded data, draining the nodes batteries, altering the connection links, thereby affect the MANET operation. In passive attacks, the attacker nodes do not affect the communication between the nodes rather eavesdrop on the communication between them

II. PRE CONCEPT

AODV [10] is a reactive routing protocol. It uses destination sequence numbers to assure the novelty of routes and in turn make sure of loop freedom. In order to make a route to a destination, a source node broadcasts a route request (RREQ) packet to its neighbor nodes using a new sequence number. The nodes which receive the broadcast packet sets up a reverse route towards the source of the RREQ unless and until it has a fresher one. When the planned destination or in between node that has a fresh route to the destination receives the RREQ, it unicasts a reply message by returning a route reply (RREP) packet along the backtrack maintained at intermediate nodes during the process of route discovery. The process of RREQ and RREP is explained in figure 1.

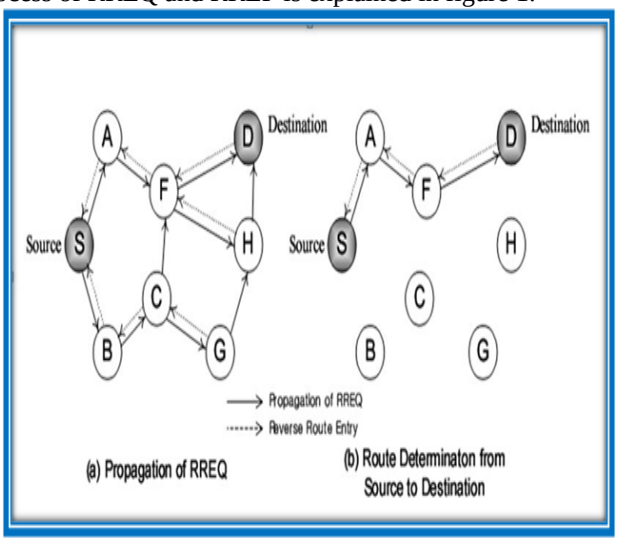

Fig.1:

After this the source node starts its process of sending data packets to the destination through the intermediate nodes that previously responded with an RREP[3]. When an in between node moves along the route, its previous neighbor node will notice route breakage due to the movement and propagate a route error (RERR) message to every responding upstream neighboring nodes. The source node, the destination node, and the intermediate nodes along the active route which deal with data transmission, contain the routing data. This process minimizes the use of network assets, runs well in high mobility conditions and decreases the memory consumptions.

In a black hole attack, a malicious[7] node consumes the network traffic and dump all packets. After a malicious node gets a RREQ packet from any other node, it suddenly sends a fake RREP. It does this without checking its routing table. It also sends a high sequence number and hop count as low as 2 to bluff its neighbors that it has the shortest route available to the destination. The source node receive reply from malacious node before it can get any other replies from other nodes. Malicious node is selected for high sequence number.

When the black node receive the information packet routed by source node, it start dropping the packets instead ofroutingthe packets to the destination node. A malicious[7] node initiates a blackhole attack in which all packets are sent to a point where they are dumped which is also called as denial of service (DoS) attack. A node cannot detect whether the neighboring node is malicious or not. A black hole attack has a wide impact on the network performance [2]. The process of black hole attack is explained in figure 2.

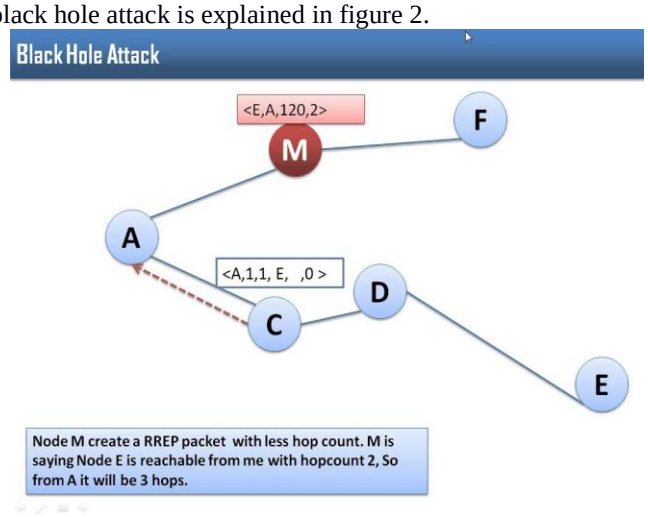

Fig.2

Attacks: Nowadays, most research on manet routing protocols, has assumed trusted environment but it does not work because ad-hoc network[5] mostly run in untrusted environment. Therefore, these protocols are susceptible to different types of networking attacks. There are two categories of attack, called external attacks and internal attacks. Authorized node perform internal attack in the network, where as external attacks are performed by the node that they are not authorized to take part in the network. Another type of attacks cane be network layer attacks and some network layer attacks are Wormhole attack, Byzantine attack, Rushing attack, Resource consumption attack, Black hole attack. Nodes can also be categorized into two groups a) Selfish node [7]: These nodes aim is to save its resources to maximum. b) Malicious node [7]: These nodes try to participate in the conversation more and more by distrupting other nodes and do harm to conversation.

III. RELATED WORK

Authors in reference number eight have proposed a solution that was designed upon a Fidelity Table[8] in which node which are participating are associated with a fidelity level that decides the reliability of the node. An obvious fidelity[8] level is attached to every node and based on the node's behavior, there level is renewed. When a RREP is received by source node, it halts to receive more route replies from intermediates nodes. After this, the node with the highest fidelity level with which its send data to destination node, is selected by source node. An ACK is sent by destination node as an acknowledgment. There exists trusted participation of the node in the network. Fidelity level [8] updation of node relies on this trusted participation. Whenever the source node receives the acknowledgement it increases the fidelity level and does opposite in reverse case. If node's fidelity level reaches zero then it is marked as malicious and in turn it is removed from the network. The main drawback of this solution is the high end-to-end delay.

Authentication Routing for Ad-hoc Network (ARAN)[9]. This protocol uses cryptographic credential to avoid and discover many attacks which are faced by many routing protocols. Ad hoc environment needs authentication, message integrity, confidentiality, privacy as a minimum requirement. This protocol covers all these factors. ARAN[9] guarantees end-to-end authentication. It consists of a basic certification operation succeed by a route instantiation operation. So, the routing messages are authenticated end-to-end and only valid nodes take part at each hop between source and destination.

Deng [4] have put forward a remedy against black hole attack by revising the AODV[10] protocol. In this the algorithm prevents malicious node from announcing fake route. To verify whether there are any malicious nodes in the route announced, every hope must include the network address of the consequent hop in RREP message. As soon as the RREP [4] message is received by the source node, it collects the information of the consequent hop. After this it sends request to consequent hop in the route. This is done to check the presence of the consequent hope node and the routing metric value (i.e. the hop count) with the consequent hop node. The

consequent hop node of the neighbour node replies the Further reply packet back to the source node to affirm the route data. In the process if route contains any malicious node then the source node will not receive any further reply and that route will be deleted from the routing table. However, this explanation is sensitive to cooperative black hole attacks. The consequent hop node can reply to the source node with wrong routing information, if both neighbour node and the consequent hop node are black hole nodes

Seryvuth Tan[3] proposed a solution against black hole attack using cryptography. It uses public key cryptography and session key to establish a valid session between sender and destination. Sender sends its public key encrypted by destination public key to destination during RREQ[3] which is received by intermediate node, black node and destination node. Intermediate node forwards it to other node. Black node will be unable to decrypt the encrypted packet. So it does not get public key of source. Black node sends RREP back to source with low hop count and high destination sequence number. And at last destination node decrypt encrypted packet and gets source's public key. Then it generates session key and encrypt session key and its IP address with source's public key.

Upon receiving the packet from destination node, the source node obtains the source and destination IP address from Route Reply (RREP).The source node decrypts the encrypted packet by using the source private key for session key and destination IP address. The source node does not receive any encryption packet from black node.

A new solution which used cryptography and DNA based mechanism was proposed by authors in reference number two. The suggested protocol uses Hybrid DNA-based Cryptography (HDC) to establish communication among the nodes which is cryptographically safe. HDC[2] is one of the promised methodologies for delicate wireless ad hoc network. It requires less computational power, bandwidth and memory. In [1] the authors have proposed a new innovative method based cryptographic mechanisms know as pseudo symmetric DNA. This technique is mainly used to achieve data integrity and confidentiality.

A pair of secret key and public key is generated by a node A (sender node). After this node A distribute the public key to node B (destination node) using PKI or third trusted party. Similarly node B does the same procedure. Node A can authenticate Node B if both the nodes are 1 hop apart by issuing a signed certificate with its DNA private key. Here certificate is a proof of node ID and DNA public key with S signature. If any of the intermediate nodes 'x' holds source DNA public key and then that node A can read and trust that node by bind it along its DNA public key. Finally, A three-way handshake is used based on the key information and certificates availability in the PKI [3] for creating private keys. These keys are created for N-hop one to one intermediate nodes

IV. References

[1]. Babu, E. Suresh, C. Naga Raju, and Munaga HM Krishna Prasad. *Inspired Pseudo Biotic DNA Based Cryptographic Mechanism Against Adaptive Cryptographic Attacks*, International Journal of Network Security, Vol.18, No.2, PP.291-303, Mar. 2016.

[2]. E.Suresh Babu , C Nagaraju, MHM Krishna Prasad, 4th International Conference on Eco-friendly Computing and Communication Systems, pages 341-347, ICECCS 2015

[3]. Seryvuth Tan, Phearin Sok, Keecheon Kim,*Using Cryptographic Technique for Securing Route Discovery and Data Transmission from BlackHole Attack on AODV-based MANET*, International Journal of Networked and Distributed Computing, Vol. 2, No. 2 (April 2014), 100-107.

[4]. Deng H., Li W. and Agrawal D.P., *Routing security in wireless ad hoc networks*, Communications Magazine, IEEE, vol.40, no.10, pp. 70- 75, October 2012.

[5]. Mohammad Abu Obaida, Shahnewaz Ahmed Faisal, Md. Abu Horaira, Tanay Kumar Roy, *AODV Robust (AODVR): An Analytic Approach to Shield Ad-hoc Networks from Black Holes*, International Journal of Advanced Computer Sciences and Applications, Vol: 2 Issue: 8 Pages: 97-102, 2011.

[6]. Madhusudhananagakumar KS, G. Aghila, *A Survey on Black Hole Attacks on AODV Protocol in MANET*, International Journal of Computer Applications (0975 – 8887) Volume 34– No.7, November 2011

[7]. Praveen Joshi, *Security issues in routing protocols in MANETs at network layer*, Procedia Computer Science 3 (2011) 954–960, World Conference on Information Technology 2010.

[8]. L. Tamilselvan and V. Sankaranarayanan, *Prevention of blackhole attack in MANET*, 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, pages 21–21, Aug 2007.

[9]. K. Sanzgiri and et al, *Authenticated routing for ad hoc networks*, IEEE Journal On Selected Areas In Communications, 23:598–610, 2005.

[10]. C. E. Perkins, E. M. B. Royer and S. R. Das, *Ad-hoc On-Demand Distance Vector (AODV) Routing*, Mobile Adhoc Networking Working Group, Internet Draft, draftietf-manetaodv- 00.txt, (Feb, 2003).