A Survey for Black Hole Attack in MANET

Abdullah Mukhtar[1] Arun Kumar[2]
[1,2]Department of Computer Science Engineering
[1,2]Galgotias University, Greater Noida, Uttar Pradesh, India

Abstract— Mobile Ad Hoc Network (MANET) is a major next generation wireless technology which is mostly used in future. MANET is a collection of communication devices or nodes that wish to communicate without any fixed infrastructure and predefine organization of available links. In a MANET mobile node will be increases and moveable, so that attacker will be attack by a malicious node which brings great challenges to the security of Mobile Ad Hoc network. The Black hole attack is one of such security issue in MANET. Our focus is specifically is on ensuring the security against the Black hole attack with the help of the popular routing protocol which is mostly used in MANET.

Key words: MANET, Black hole attack, AODV, Malicious node, RREQ, RREP

I. INTRODUCTION

Mobile Ad hoc networks (MANET) are usually formed by a group of mobile nodes, interconnected via wireless links which agree co- operate and forward each other's packet. So the minimal configuration and quick deployment make adhoc network suitable for emergency situation like natural disaster and connecting soldier on a battle field. These mobile node in Ad hoc network dynamically create routes among themselves and form a own wireless network on the fly. The random and rapid motions of MANET's require that the node always find new routes. These new routes is finding with the help of these routing protocol: Proactive, Reactive and Hybrid touting protocol.

- Proactive routing protocol is a table-driven routing protocol, each node maintains a routing table which is not only contains records of adjacent nodes and reachable node but also the number of hops. If the size of network increases, the overhead also increases.
- Reactive routing protocol is also called On-demand routing protocols. These protocols do not attempt to maintain correct routing information on all nodes at all times. Routing information is collected only when it is needed and route determination depends on sending route queries throughout the network.
- In Hybrid routing protocol, there is tradeoff between proactive and reactive protocol. Proactive protocol have large overhead and less latency while reactive protocols have less overhead and more latency so a hybrid protocol is presented to overcome the shortcoming of both proactive and reactive routing protocol. Hybrid routing protocol is combination of both proactive and reactive protocol.

MANET technology is a dynamic topology such that node can easily join or leave the network at any time .when the mobile adhoc network are being used in mission critical operations, other issues of security also arise. So that provides a ultimate goal to protected communication between mobile node in a hostile environment with the support of these some routing protocol such as AODV (Adhoc on-demand distance vector), DSR (Dynamic source routing), and DSDV (Destination sequenced distance vector).

Inside the Mobile adhoc network every node act as a router to forwarding a packet to the neighbor node and passing to its destination node via multihop with the help of discover a route. Due to the lack of infrastructure they are reveal a lot of attack. These attacks are mainly classified into two parts: passive attack and active attack. In the passive attack the attacker does not disturb the operation of routing protocol instead it try to capture vital information via traffic analysis. But in active attack, it attempts to alter or destroy the data, gain authentication thereby disrupting the functioning of the network. There are so many attack are come under active attack, one of these attack is black hole attack which comes under a active attack. Black hole attack is a denial of services (DOS) attack in mobile adhoc network. A black hole is formed during the weak routing protocol when a malicious node joins the network this problem arises. In this attack a malicious node falsely advertises the shortest path to the destination node during the route discovery and maintenance phase. We briefly discuss about black hole attack in other section.

II. OVERVIEW OF AODV AND BLACK HOLE ATTACK

A. Adhoc on Demand Distance Vector (AODV):

Ad hoc on demand distance vector (AODV) routing protocol[11] is a reactive routing protocol and it is the most popular and widely used routing protocol which is designed for adhoc mobile network. AODV is capable for both unicast and multicast routing. It is an on demand algorithm means that the route is established only when it is desired by the sourced node for transmitting a packet. This process is accomplished with route discovery mechanism which source node S sees its routing table if a valid route entries is found toward the destination D then source node S send the data to a given destination node D , else it initiate a route discovery procedure which source node broadcasting a route request(RREQ) message to the neighbor. When a RREQ is receiving by any intermediate node they finally see its routing table to find a fresh route toward the requested destination in RREQ. If such a route is obtain a route reply (RREP) is unicast toward a source via intermediate node .If intermediate node doesn't obtain a fresh route its update its routing table and send RREQ to these neighbor. This process is repeated until RREQ accomplish the destination node D and they all have successful route from source to destination.

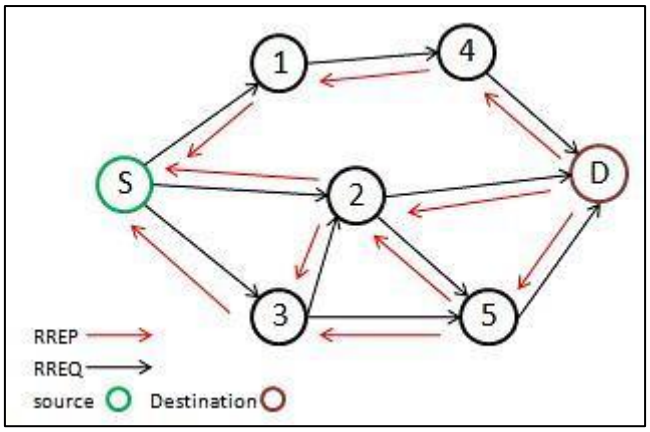

Fig. 1: Route Discovery Process under AODV

B. Black Hole Attack:

Routing protocol has exposed variety of attack. Black hole attack[2][7][11] is denial of services (DOS) attack in Manet. Black hole attack is a kind of active attack in which the malicious node takes the benefits of the vulnerabilities of routing protocol. In this attack a malicious node falsely advertises the shortest path to the destination node during the route discovery and maintenance phase to sending a fake RREP packet to the source node. When the source node receive his RREP packet its start sending a data packet to the malicious node and this malicious node absorb all these data packet and drops them fully or sometimes partially. When another RREP packet is reaches from another route to the source node then they discard that RREP packet. So that source and destination node will not be able to communicate with each other. Black hole attack has two types:-

1) Single Black Hole Attack:

Its very simple form of black hole attack because in this attack only on -e malicious node is used to carry out the attack. That malicious node advertise itself as a node of shortest path to the destination and when the packet arrived at it this node simply discard the all packet which is sending from the source node to the destination.

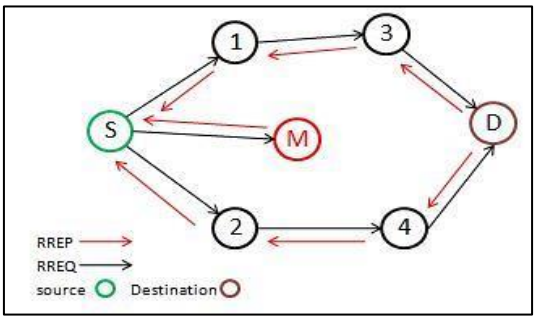

Fig. 2: Single Black Hole Attack

2) Cooperative Black Hole Attack:

In this black hole attack there are more than one malicious node and this malicious node has also send a fake RREP packet to the source node that has initiated a route discovery in order to show itself as a destination node or an intermediate node to the actual destination node. This malicious absorb, drop and then lost the entire packet which is sending from the source node. In sometime these malicious has co operate with each other with the same aim of dropping packets these are known as cooperative black hole node[13] and these type of attack is known as cooperative black hole attack.

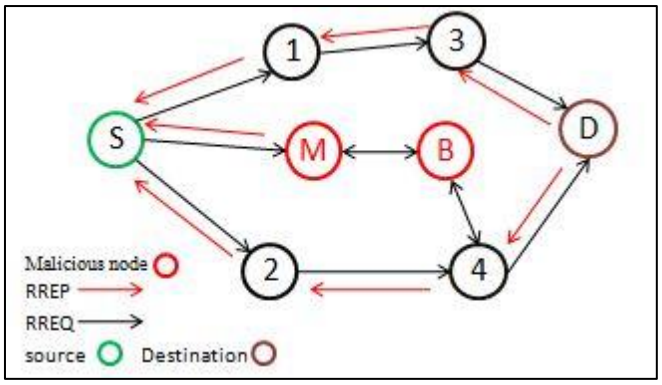

Fig. 3: Cooperative Black Hole Attack

In the fig 3 source node S wishes to transmit a data packet to the destination, it first broadcast the RREQ packet to the neighboring nodes. The (Black hole node) malicious nodes being part of the network, also receive the RREQ packet. The RREP packet from the malicious node M reaches to the source node, it start sending data to this malicious node M and another RREP packet which is reached later from different route they discard it. This malicious node M drop or absorb all data packets which is sending from the source to destination .This situation is follow only when single malicious node has occur in the network. But when multiple black hole nodes are acting in coordination with each other first black hole M refer to its partner B as next hop, the source node S send further request (frq) to B through a different route (S, 2, 4 , B) other than via M. Node S ask B if he is having route to M and route to destination node D. Because B is co operating with M its further reply is 'yes 'for both questions. Source node S start sending packet assuming route (S,M,B) is secure but the packet are drop by node M.

III. LITERATURE SURVEY

Hongmei Deng, Wei Li and Dharma P. Agarwal proposed a solution[10] to the black hole problem. In this solution the black hole problem is to disable the ability to reply in a message of an intermediate, so all reply messages should be sent out only by the destination node using this method the intermediate node cannot reply, so in some sense we avoid the black hole problem and implement a secured AODV protocol. But in the solution there are two associate disadvantages one is delay is greatly increased and another is malicious node can take further action such as fabricate a reply message on behalf of the destination node. So they are proposed another solution using one more route to the intermediate node that replays the RREQ message to check whether the route from the intermediate node to the destination node exists or not. If it exists we can trust the intermediate node and send out the data packet .if not then source node just discard the reply message from the intermediate node and send out alarm message to the network and isolate the node from the network.

Hesiri weerasinghe proposed algorithm[1] for defending against a cooperation black hole by introducing two concepts: data routing information (DRI) table and cross checking .In DRI each node is maintain DRI table with assigning two bit 1 and 0. 1 is stand for true and 0 is false , first one bit "from" stand for the information on routing data

packet from the node and second bit "through" stand for information on routing data packet through the node

While in cross checking using further request (FREQ) and further reply (FREP). If the secure node does not have a route entry to the destination, it will broadcast a RREQ message to discover a secure route to the destination. If destination replies, all intermediate nodes update and insert routing entry for that destination to as a trust destination. Source node also trust on destination and they will start to send to send data along that path and source node updates our DRI table for this path.

Soufine Djahel, Farid Nait-Abdesselam and Ashfaq Khokhar proposed solution[4] to deal with the cooperative black hole attack an acknowledgement based scheme to mitigate the loss of topology information due to the dropping of topology control (TC) message by attackers. In addition to the original control message of OLSR are Hello and TC messages. They introduce another two type of control packets, which are called 3*hop_ACK* and *HELLO_rep*. The 3*hop_ACK* message is used by a node to acknowledge its reception of a TC message from the neighbors 3 hops away, and the HELLO_*rep* message is used by a node to advertise its 2 hop neighbors to a requesting multi point relay (MPR) node. For the request, they use one of the unused bits in the HELLO message to indicate whether the sender's MPR nodes should generate *HELLO_rep* packet or not.

Ms. Gayatri Wahane and Ms. Savita Lonare has proposed scheme[5] for detecting as well as defending against co-operation black hole attack is identified and presented by an algorithm to the modification of AODV routing protocol with two types. First is maintenance of routing information table(RIT) and reliability checking of a node. In RIT every node maintains three bit information. In these three bit the first two bit is discuss earlier but the last one bit is represented by "through any trustful node". This last bit is set if any trustful node has routed data packet through the node. But in reliability checking of node is based on a intermediate node that generate the RREP has to provide the information about Next hopping node (NHN) and RIT entry for the NHN. Source node will check its own RIT to see whether IN is unreliable and source node send Additional request(ARq) message to next hop node.

Suparna biswas, tanumoy nag and sarmishta neogy proposed [11] a solution to prevention of black hole to average value for following parameters- rank, velocity, and battery power for selected a higher trust value among all the available routes. These trust values of all routes are compared and the route having highest average trust is selected for packet transmission. If the packet transmission through is selected for transmission destination node send a acknowledge to source node which in turn increment the rank and decrements battery power of each of the node in that route.

IV. Conclusion and Future Work

In MANET, security is major challenges for detection and prevention the malicious node for attacker. So here we can see that attacker will be attack through a some malicious node and this attack has comes under a black hole attack and this malicious node send a fake RREP packet with higher sequence number and some other technique. So we can detect and prevent this black hole in some various techniques such as route discovery process, cross checking and DRI and some other way. This can be possible with the help of AODV routing protocol. Detection and prevention arises some defect which is packet delivery is low and consume a more time. future work is focused on to designed algorithm for minimum delay and reduce packet dropping ratio and increase packet delivery ratio

References

[1] Hesiri Weerasinghe and Huirong Fu, "Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation", International Journal of Software Engineering and its Application, Vol.2, Issue 3, July 2008.

[2] Yibeltal Fantahun Alem and Zhao Cheng Xuan , "Preventing Black Hole Attack in Mobile Ad-hoc Networks Using Anomaly Detection",2nd International Conference on Future Computer and Communication , volume 3, 2010

[3] Jaydip Sen , Sripad Koilakonda and Arijit Ukil "A Mechanism for Detection of Cooperative Black Hole Attack in Mobile Ad Hoc Networks", Second International Conference on Intelligent Systems, Modeling and Simulation, pp 338-343 , Jan 2011

[4] Soufine Djahel, Farid Nait-Abdesselam and Ashfaq Khokhar "An Acknowledgment-Based Scheme to Defend Against Cooperative Black Hole Attacks in Optimized Link State Routing Protocol", IEEE Communications Society, 978-1-4244-2075-9/08/ © ICC 2008 IEEE

[5] Ms. Gayatri Wahane and Ms. Savita Lonare " Technique for Detction of Cooperative Black Hole Attack in MANET", 4th ICCCNT ,IEEE- 31661 July 4-6, 2013, Tiruchengode, India

[6] Namrata Marium Chacko, Shini sam and P.Getzi Jeba Leelipushpam "A survey on various privacy and security features adopted in MANETs routing Protocol", International Multi-Conference on Kottayam,IEEE, pp 508 – 513, 22-23 March 2013

[7] Kishor Jyoti Sarma, Rupam Sharma and Rajdeep Das "A Survey of Black Hole Attack Detection in Manet", 978-1-4799-2900-9/14/ ©2014 IEEE

[8] Harsh Pratap Singh and Rashmi Singh "A Mechanism for Disco very and Prevention of Cooperative Black hole attack in Mobile Ad hoc Network Using AODV Protocol", Electronics and Communication Systems (ICECS),International Conference on Coimbatore ,IEEE, 13-14 Feb. 2014

[9] Kriti Chadha and Dr. Sushma Jain "Impact Of Black Hole And Gray Hole Attack In AODV Protocol", IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2014), May 09-11, 2014, Jaipur, India

[10] Hongmei Deng,Wei Li,and dharma P. Agrawal "Routing security in wireless Adhoc networks", IEEE communications magazine ,October 2002

[11] Suparna Biswas, Tanumoy Nag and Sarmistha Neogy "Trust Based Energy Efficient Detection and Avoidance of Black Hole Attack to Ensure Secure Routing in MANET",Applications and

innovations in mobile computing (AIMoC),IEEE, Feb. 27 2014-March 1 2014, Kolkata, India

[12] Mangesh kumar S. Shegokar and R. R. Tuteja "Survey on Classified Ad-hoc Routing Protocols in MANET", International Journal of Science and Research (IJSR), Volume 3 Issue 4, April 2014

[13] Ankur mishra, Ranjeet Jaiswal and Sanjay Sharma "A Novel Approach for Detecting and Eliminating Cooperative Black Hole Attack using Advanced DRI Table in Ad hoc Network", 3rd IEEE International Advance Computing Conference (IACC) , 2013

