www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 3 Issue 6 June, 2014 Page No. 6513-6519

Novel Technique to Detect and Isolate Black hole Attack in MANET

Barleen Shinh
Rayat Institute of Engineering and Information Technology, Ropar, Punjab - 143001, India.
Email : engineer_shinh@hotmail.com

Abstract:
The mobile nodes can establish the route from source to destination when they want. In DSR routing protocols many loop hole are there, these loop holes can give arise to different type of active and passive attacks which are triggered by various inside and outside malicious nodes. Among all the type of attacks, black hole attack is the most common of attack which is possible in DSR protocol. Black hole attack is the denial of service attack. Many algorithms had been proposed to prevent this attack. In this paper, we are proposing modifications in traditional DSR protocol to prevent black hole attack.

Keywords: Reactive protocol, worm hole attack, black hole attack

1. Introduction

The network links between nodes are established using either cable media or wireless media. But the networks can be broadly classified into two categories. They are

- Wired Network
- Wireless Network

A wired network connects devices to the network or other network using cables. The most common wired networks use cables connected to Ethernet ports on the network on one end and to a computer or other device on the opposite end. Wired networks provide users with plenty of security and the ability to move lots of data very quickly. A widely adopted family of communication media used in local area network (LAN) technology is collectively known as Ethernet. Wireless Networking is a technology in which two or more computers communicate with each other using standard network protocols but without using cables. The transmission takes place with the help of radio waves at physical level. It is also known as Wi-Fi or WLAN. In this type of network, devices can easily two using radio frequency. The IEEE standard for wireless network is 802.11.

There are two types of Wireless Operating modes. One is Infrastructure and other is Infrastructureless networks. In infrastructure based network, communication takes place only between the wireless nodes and the access points. There is no direct communication between the wireless nodes. The access point is used to control the medium access as well as it acts as a bridge between wireless and wired networks. The infrastructure less network does not need any infrastructure to work. In this network each node can communicate directly with other nodes.

Attacks on Mobile Ad-hoc Network

The attacks in mobile ad-hoc network are done in order to interrupt the communication or to steal the information. The attacks in mobile ad hoc networks can be broadly classified into two distinct categories viz. Active attacks and Passive attacks. An active attack is that attack which any data or information is inserted into the network so that information and operation may harm. It involves modification, fabrication and disruption and affects the operation of the network. Example of active attacks is impersonation, spoofing. A passive attack obtains data exchanged in the network without disturbing the communications operation. The passive attacks are difficult to detection. In its, operations are not affected. The operations supposed to be accomplished by a malicious node ignored and attempting to recover valuable data during listens to the channel. Some of the most common attacks on mobile ad-hoc networks include:

1) Denial of Service Attack

A denial-of-service attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service.. Denial-of-service attacks come in a variety of forms and aim at a variety of services. There are three basic types of attack:

- consumption of scarce, limited, or non-renewable resources
- destruction or alteration of configuration information
- physical destruction or alteration of network components

Denial-of-service attacks are most frequently executed against network connectivity. The goal is to prevent hosts or networks from communicating on the network.

2) Byzantine Attack

In this attack, a compromised intermediate node or a set of compromised intermediate nodes works in collusion and carries out attacks such as creating routing loops, forwarding packets on non-optimal paths and selectively dropping packets which results in disruption or degradation of the routing services. It is hard to detect byzantine failures. The network would seem to be operating normally in the viewpoint of the nodes, though it may actually be showing Byzantine behaviour.

3) Wormhole Attack

It is a network layer attack. In wormhole attack, a malicious node receives packets at one location in the network and tunnels them to another location in the network, where these packets are resent into the network. This tunnel between two colluding attackers is referred to as a wormhole. It could be established through wired link between two colluding attackers or through a single long-range wireless link. In this form of attack the attacker may create a wormhole even for packets not addressed to itself because of broadcast nature of the radio channel.

4) Gray-hole attack

This attack is also known as routing misbehavior attack. It leads to messages dropping. It has two phases. In the first phase a valid route to destination is advertise by nodes itself. In second phase, with a certain probability nodes drops intercepted packets.

In section 2 we will do literature survey and in section 3 we will introduce black hole attack.

2. Review of Literature

In this paper [1]Mohammad Al-Shurman et. al [2004], proposed two solutions to black hole attacks prevalent in mobile ad-hoc network. The first solution is to find multiple paths to send data from source to destination. The source sends ping packets along these different routes with different packet Id's and sequence number. The source checks the RREP's from different routes and try to find a secure route having a hop that is shared in more than one route to the destination. This method ensures secure route to destination but at the expense of the time delay caused due to waiting for another RREP from an alternate route. The second method explores the possibility of using the sequence number for identifying the fake replies from genuine replies. In this, two additional tables are used to record sequence number of last sent packet and last received packet. These tables are updated whenever a packet is sent or received and the destination node sends RREP packet along with last packet sequence number. This solution ensures faster delivery of packets. First solution is more secure but delay is large while the second solution is quick in delivering the packets but a malicious node can listen to the channel and can update its tables for the last sequence number. In paper [2] Jeroen Hoebeke et. al [2005], discussed about application of mobile ad-hoc networks and the challenges being faced while using them. In this paper, a complete introduction has been given about the wireless networks. Moreover this paper provides an insight into the potential applications of ad-hoc networks and discusses the technological challenges being faced by network and protocol designers. Most prominent of the challenges are routing, resource and service discovery and security. Different attacks pertaining to security are deletion, fabrication, replication and redirection of data packets. But despite challenges, mobile ad-hoc network opens a new business opportunity for service providers. In paper [3] Giovanni Vigna et. Al [2005], demonstrated an effective intrusion detection tool that can be used to for detecting attacks in mobile ad-hoc network while using limited amount of resources. The tool monitors network packets to detect attacks within its range. This tool is based on State Transition Analysis Technique (STAT). AODVSTAT sensors can be used in standalone mode to detect attacks in neighborhood only or distributed mode, in which update messages are exchanged between sensors to detect attacks in distributed manner. This scheme works well for detecting both single hop as well as distributed attacks in mobile ad-hoc networks while imposing a very small overhead on nodes. In paper [4] Mehdi Medadian et. al [2009], proposed a novel approach for countering the black hole attack. The approach is based on using negotiations with neighbors who claim to have a route to destination. In this approach, any node uses a set of rules to decide the honesty of the reply's sender. During packet transferring, the activities of a node are logged by its neighbors. These neighbors send their opinion about a node. When a node receives replies from all neighbors, it is able to decide whether the replier is a malicious node or a legitimate node. The opinion send by neighbors is based on the number of packets sent to a particular node and number of packets forwarded by it. The method yields better percentage of packets received in presence of cooperative black hole attack. In paper [4] Payal N. Raj and Prashant B. Swadas [2009], proposed DPRAODV (detection, prevention and reactive AODV) to prevent the black hole attack by informing the other nodes about the malicious node. As the value of RREP sequence number is found to be higher than the threshold value, the node is suspected to be malicious and it adds the node to the black list. As the node detected an anomaly, it sends a new control packet, ALARM to its neighbors. The ALARM packet has the black list node as a parameter so that, the neighboring nodes know that RREP packet from the node is to be discarded. Further, if any node receives the RREP packet, it looks over the list, if the reply is from the blacklisted node; no processing is done for the same. The threshold value is the average of the difference of destination sequence number in each time slot between the sequence number in the routing table and the RREP packet. The purposed solution not only detects the black hole attack, but tries to prevent it further, by updating threshold which reflects the real changing environment. Other nodes are also updated about the malicious act by an ALARM packet, and they react to it by isolating the malicious node from network. In paper [5] **Songbai Lu et. al [2009],** proposed a method that is effective and secure against the black hole attack in mobile ad-hoc network. This method is works on the basis of direct verification of the destination node using random number exchange. In this method, the source node sends verification packet SRREQ (Secure Route Request) to destination node along opposite direction route of RREP (Route Reply) received while the verification packet contains random number. This packet is forwarded using different routing paths. At the destination end, upon receiving two or more SRREQ (Secure Route Request) packets, their contents are checked. If content are same, verification confirm packet SRREP (Secure Route Reply) is sent to source along different routing paths. On the source end, upon receiving two or more SRREP (Secure Route Reply) packets, their contents are checked for match. If they match, the route is added to the routing table and warning message regarding malicious nodes, is propagated throughout the network. This scheme can effectively prevent black hole attack and also maintain a high routing efficiency. In paper [5]Harris Simaremare and Riri Fitri Sari [2011], proposed two different approaches viz. AODV-UI (based on reverse request method) and PHR-AODV (Path Hoping on Reverse AODV) and subjected these approaches to various attacks faced by mobile ad-hoc networks. These approaches aim at improving performance as well as security and various metrics viz. packet delivery ratio, end to end delay and packet lost, are used. AODV-UI method works like AODV but with an exception that if one route is lost, route discovery process is not started. Rather the alternate route found earlier in route discovery is selected. This enhances the performance as there is no need to search for routes again and again. PHR-AODV method determines multipath for sending data to destination and checks whether the path is broken or not. If broken, path is deleted from the list and new path is selected. AODV-UI performs better in terms of packets lost, end to end delay and packet delivery ratio. But in presence of black hole nodes, PHR-AODV performs better. In this paper [6] Priyanka Goyal et. Al [2011], describes the elementary problems of ad hoc network by providing its background. The most common challenges involved are limited bandwidth, less computational and battery power and security. It presents an overview of the routing protocols being used and their issues. Moreover desired security goals such as availability, confidentiality, integrity, authorization etc. have been discussed. The general trend is towards mesh architecture and improvements to be made to capacity and bandwidth. Thus it ensures smaller, cheaper and more capable ad-hoc networks.

3. Black Hole Attack

DSR (Dynamic Source Routing) protocol is an important on-demand routing protocol that creates routes only when desired by the source node. When a node requires a route to a destination, it broadcasts a route request (RREQ) packet to its neighbors, which then forward thee request to their neighbors adding its destination address until either the destination or an intermediate node with a “fresh enough” route to the destination is located. In this process the intermediate node can reply to the RREQ (Route Request) packet only if it has a fresh enough route to the destination. Once the RREQ (Route Request) reaches the destination or an intermediate node with a fresh enough route, the destination or intermediate node responds by unicasting a route reply (RREP) packet back to the neighbor from which it first received the RREQ (Route Request). After selecting and establishing a route, it is maintained by a route maintenance procedure until either the destination becomes inaccessible along every path from the source or the route is no longer desired. A RERR (Route Error) message is used to notify other nodes that the loss of that link has occurred. A black hole problem means that a malicious node utilizes the routing protocol to claim itself of being the shortest path to the destination node, but drops the routing packets but does not forward packets to its neighbors. Imagine a malicious node ‘M’. When node ‘A’ broadcasts a RREQ packet, nodes ‘B’ ‘D’ and ‘M’ receive it. Node ‘M’, being a malicious 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 a route to the destination. Node ‘A’ receives the RREP from ‘M’ ahead of the RREP from ‘B’ and ‘D’. Node ‘A’ assumes that the route through ‘M’ is the shortest route and sends any packet to the destination through it. When the node ‘A’ sends data to ‘M’, it absorbs all the data and thus behaves like a ‘Black hole’.

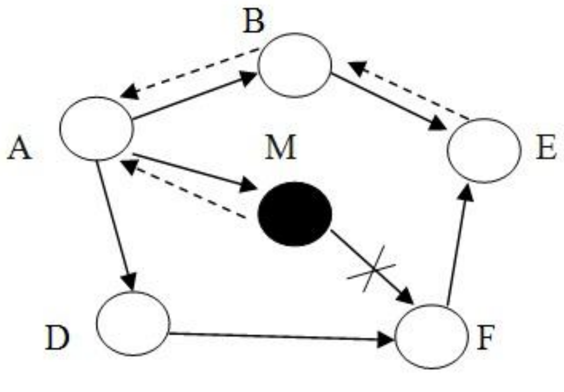


Fig. 1.1 Black Hole Attack

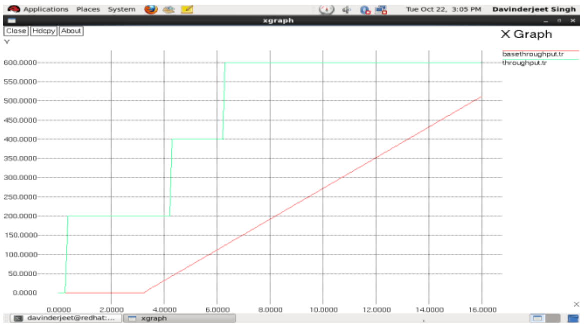
In DSR, the sequence number is used to determine the freshness of routing information contained in the message from the originating node and address is added to find out multiple source paths. When generating RREP (Route Request) message, a destination node compares its current sequence number, and the sequence number in the RREQ

(Route Request) packet plus one, and then selects the larger one as RREPs (Route Request) sequence number. Upon receiving a number of RREP (Route Request), the source node selects the one with greatest sequence number in order to construct a route. But, in the presence of black hole when a source node broadcasts the RREQ (Route Request) message for any destination, the black hole node immediately responds with an RREP (Route Request) message that includes the highest sequence number and this message is perceived as if it is coming from the destination or from a node which has a fresh enough route to the destination. The source then starts to send out its packets to the black hole trusting that these packets will reach the destination. Thus the black hole will attract all the packets from the source and instead of forwarding those packets to the destination it will simply discard those. Thus the packets attracted by the black hole node will not reach the destination.

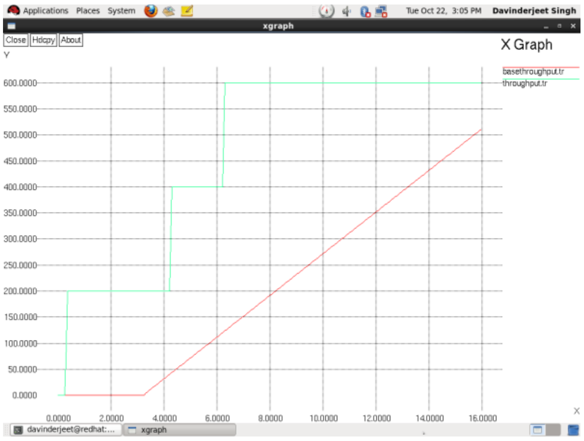
4. Proposed Method

In proposed work, firstly we deploy the mobile ad hoc network with infinite number of mobile nodes. All the mobile nodes are randomly deployed into the fixed area. The source and destination are selected for route establishment. For the route establishment source node flood the route request packet in the network and route reply packets are send back to the source by the adjacent nodes. The route is established between source and destination on the basis of hop counts and sequence numbers. The malicious node exists in the route which is selected between source and destination. The malicious node will be responsible for triggering the selective packet drop attack. The proposed mythology will detect the malicious node and isolate, it from the network. The methodology is based on the throughput of the network. When the throughput of the network, will degrades to certain threshold value, nodes in the network will go to monitor mode and detect the malicious node. The proposed methodology will be implemented in network simulator version 2.

5. Results



Graph 1: Delay Graph



Graph 2: Throughput Graph

Graph 1 shows the change in end-to-end delay after the deployment of the proposed method. In the conventional method, the delay starts increasing when there is presence of a black hole node in the network whereas in absence of black hole nodes, the delay is almost zero as all packets arrive at their destination in a timely manner. the change in throughput achieved using the proposed method. As the delay in the network is at a minimum due to isolation of black hole nodes, the throughput increases as more and more packets are delivered to their destinations. Green line represents the throughput in the new scenario and red line represents the throughput in conventional method.

Conclusion

In this paper, we conclude that black hole attack one of dangerous attack of the network. Due to this attack packet loss may occur and delay increase. The main objective of the paper is to isolate black hole attack so that packet loss and through of the network increase. Experimental results show that proposed method is far better than existing method as it has less time delay and less packet loss as compare to the existing technique.

References

[1] Bo Yang, Ryo Yamomoto, Yoshiaki Tanaka (2012), *"Historical Evidence Based Trust Management Strategy against Black Hole Attack in Mobile Ad-Hoc Networks"* ICACT February 19~22, 2012.

[2] Seung Yi, Robin Kravets (2002), *"Key Management for Heterogeneous Ad Hoc Wireless Networks."* 10th IEEE International Conference on Network Protocols (ICNP'02), 1092-1648.

[3] Dokurer, S. Ert, Y.M, Acar, C.E (2007), *"Performance Analysis of Ad-Hoc Networks under Black Hole Attack."* Proceedings IEEE, pp. 148-153, 2007.

[4] Hothefa Sh. Jassim, Salman Yussof (2009), *"A Routing Protocol based on Trusted and Shortest Path Selection for Mobile Ad-Hoc Networks"* IEEE 9th Malaysia International Conference on Communications 2009.

[5] Pradeep Kyasanur (2005), "Selfish MAC layer Misbehavior in wireless networks" IEEE on Mobile Computing 2005.

[6] J.H. Cho, A. Swami, I.R. Chen (2011), *"A survey of Trust Management in Mobile Ad-Hoc Networks"* IEEE Communication Surveys and Tutorials 13 (4) 2011, 562-583.

[7] Priyanka Goyal, Vintra Parmar and Rahul Rishi (2011), *" MANET: Vulnerabilities, Challenges, Attacks, Application"* IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011 ISSN 2230-7893 2011.

[8] Radha Krishna Brar, Jyotsna Kumar, Moirangthem Marjit Singh, *"Qos of MANET through Trust Based AODV protocol by Exclusion of Black Hole Attack"* International Conference on Computational Intelligence Modelling Technology Applications, CIMTA, 2013.

[9] Tien-Ho Chen and Wei-Kuan, Shih (2010), *"A Robust Mutual Authentication Protocol for Wireless Sensor Networks"* ETRI Journal, Volume 32, Number 5, October 2010.

[10] M.E.G, Moe, B.E. Helvik, S.J. Knapskog (2008), *"Trust Based Secure Mobile Ad-hoc Networks routing using HMMs"* Proceedings ACM Symposium on Qos and Security for Mobile Ad-hoc Network, Vancouver, British Columbia, Canada, 27-28 October 2008, pp. 83-90.

[11] J. Golbeck (2008), *"Computing with Social Trust for Human-Computer Interaction series"* Springer 2009.

[12] Caimu Tang, Dapeng Oilver (2011), *"An Efficient Mobile Authentication Scheme for Wireless Networks."* IEEE 2011.

[13] Durgesh Wadbude, Vineet Richariya (2012), *"An Efficient Secure AODV Routing Protocol in MANET"* International Journal of Engineering and Innovative Technology (IJEIT) ISSN: 2277-3754 Volume 1, Issue 4, April 2012.

[14] Jacek Cicho, Rafał Kapelko, Jakub Lemiesz, and Marcin Zawada (2010), *"On Alarm Protocol in Wireless Sensor Networks"* IEEE 2010.

[15] S. Sharmila and G. Umamaheswari (2012), *" Defensive Mechanism of Selective Packet Forward Attack in Wireless Sensor Networks"* In International Journal of Computer Applications (0975 – 8887) Volume 39– No.4, February 2012.

[16] Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt and Piet Demeester (2005), *“An Overview of Mobile Ad Hoc Networks: Applications and Challenges”* IJSER 2005.

[17] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei (2006), *“A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks”* Springer 2006.

[18] Sevil Şen, John A. Clark, Juan E. Tapiador (2010), *“Security Threats in Mobile Ad Hoc Networks.”* IEEE 2010.

[19] Giovanni Vigna, Sumit Gwalani, Kavitha Srinivasan, Elizabeth M. Belding-Royer Richard, A. Kemmerer (2004), *“An Intrusion Detection Tool for AODV-based Ad hocWireless Networks”* 2004.

[20] Jin-Hee Cho and Ing-Ray Chan (2013), *“On Tradeoff between Altruism and Selfishness in MANET Trust Management”* Elsevier 2013.