IJETST- Volume||01||Issue||04||Pages 540-545||June||ISSN 2348-9480 2014

Open access Journal International journal of Emerging Trends in Science and Technology

Detection and Isolation of Multiple Black Hole Attack Using Modified DSR

Authors

Barleen Shinh, Manwinder Singh

Rayat Institute of Engineering and Information Technology
Rail Majra Distt. Nawanshar,
Punjab 143001

Abstract

Mobile Ad hoc Network is a robust infrastructure less wireless network. It can be formed either by mobile nodes or by both fixed and mobile nodes. Nodes are randomly connected with each other and forming arbitrary topology. MANET is susceptible to various routing attacks which hinder the security of the network. The routing attack addressed in this paper is the black hole attack in DSR protocol of MANET. In the Black hole attack a malicious node advertises itself as the best shortest route to the destination. This paper describes a strategy to detect and isolate the multiple black hole attack in MANETs.

Keywords : *MANET, Black hole attack, DSR*

1. Introduction

MANET is a Mobile Adhoc Network in which the nodes get connected with each other without an access point. They can function as both routers and hosts. Messages are exchanged and relayed between nodes. Routing algorithms are utilized for forwarding packets between indirect nodes i.e not in direct range with aid of intermediate nodes. MANET is further classified as single hop and multi hop network, thereby extending the coverage of the network to extended ranges. Single hop networks have nodes in direct communication mode with each other, whereas Multi hop networks have indirect communication between nodes through intermediate nodes. Mobile Ad hoc Network is multi-hop wireless distributed network which is self organizing in nature. The primary objective of routing protocol is to discover the route. In MANET, routing protocol undertakes to setup and maintain routes between nodes. In such cases, the ability to confidentially communicate secret information in the presence of attacker is very strenuous. Security is a prime concern for mobile Ad-hoc networking (MANET) because wireless mobile ad-hoc links makes the network available to neighboring nodes which posses vulnerability to various active and passive attacks if malicious node is present in the network. Though many trust management schemes have been used for detecting external attacks from outside and various securities related MANET routing protocols for preventing internal attacks are

created within the MANET but Black hole attack is still the most prominent form of vulnerability in which the malicious node pretends to be the best shortest path to the destination.

1.1 Overview of DSR

DSR is a reactive routing protocol for ad hoc wireless networks. It also has on-demand features like AODV but it's not table-driven. It is based on source routing. The Dynamic Source Routing protocol (DSR) is a simple designed specifically for use in multi-hop wireless ad hoc networks of mobile nodes and efficient routing protocol. DSR allows the network to be fully self-organizing and self-configuring. Dynamic Source Routing protocol allows finding a source route across multiple networks nodes to dynamically. In this each data packet carries in its header completely, nodes list of nodes through which the packet must pass dynamically ordered, allowing loop-free packet routing and the need for up-to-date routing information in the intermediate nodes avoiding through which the packet is forwarded. DSR uses the sequence number to determine the fresh route information contained in the message from the source node. DSR follow two processes ROUTE DISCOVERY and ROUTE MAINTENCE and three control messages: RREQ, RREP, RERR .

in Route Discovery if a source node wants to discover a route to another node it check its route cache if and if no route is found or is expired, it broadcasts a new route request packet containing unique ID of the destination address. When the intermediate node receives the RREQ packet from the source node it replies through a RREP message and adding its own address in the RREP packet. The message is further broadcasted until the required destination node is found. When the source node finally receives the RREP it updates its caches and the data is transmitted to the destination node through new route.

Route Maintenance:

In route maintenance process the transmitting node needs to keep the information of the route whether its working or expired during transmission of data. If the link failure occurs in the path, then it generates a route error message and the broken link is repaired. All the neighboring nodes are updated with Route Error message.

1.2 Attacks in MANETS

The attacks in MANETs are classified into internal and external attacks. These are discussed in brief in succeeding paragraphs.

Internal Attacks

Nodes present in the network and respective link interfaces are attacked in it. These attacks are not easy to isolate as most trusted nodes mislead other nodes in the network by broadcasting wrong routing information.

External Attacks

These types of attacks cause high trafficking in the network, denial of services (DoS), and broadcasting wrong routing information etc. External attacks can be further categorized as passive and active attacks.

Passive Attack

The data transmitted is not changed within the network but unauthorized "listening" to the network traffic or accumulation of data is carried out. Passive attacker does not interrupt with the operation of a routing protocol but puts efforts to gather the vital information from packets. As the normal operation of the network doesn't get affected, this problem can be eased by using powerful encryption algorithms.

Active Attacks

The severity of these types of attacks is seen as prevention of packets exchange between the nodes. Furthermore active attacks can be internal or external. The sources not belonging to the network pose active attacks whereas malicious nodes within the network make internal attacks more severe and difficult to detect. These attacks are able to get unauthorized access to network and make changes such as modification of packets, DoS, congestion etc. Malicious nodes change the routing information by showing itself as having the shortest path to the destination. Black hole attack falls in this category.

2. Review of Literature

[1] Payal N. Raj1 et al, (2009) have proposed black hole attack detection mechanism by employing additional check of RREP sequence number with a prescribed threshold value. This value is periodically updated and RREP sequence number is compared with the threshold value and if greater is added to black list as node is suspected to be malicious. After detection of suspicious nodes, the authors proposed sending of new control packet ALARM to neighboring nodes. This approach comparatively isolated malicious nodes by including threshold comparison parameter. [2] Tien-Ho Chen and Wei-Kuan Shih, (2010) have discussed about importance of mutual authentication for wireless sensor networks .They also discussed about the DES protocol which is the hash-based authentication protocol. This protocol provides the security aligned with the stolen-verifier, masquerade, replay, and guessing attacks. [3] Xianren WuA (2010) studied various routing protocols and compared and categorized protocols based on restricted simulation approaches under dynamic network configurations. Experimental results of packet delivery ratio, delay and throughput are analyzed under effect of traffic patterns, mobility and network density. Different models have been discussed for reducing routing overhead. Simulation done of two protocols of MAC layer by author showed that GTDMA provides low throughput and LTDMA enjoys good performance. He also highlighted in his work that reactive protocols are more prone to traffic increase causing packet delivery ratio to decline. [4] Priyanka Goyal et al, (2011) have discussed about the Mobile ad-hoc network as one of the most promising fields for research and development of wireless network. They brought out that as the popularity of mobile device and wireless networks significantly increased over the past years, wireless ad-hoc networks has now become one of the most vibrant and active field of communication and networks. The authors bring out essential problems of ad hoc network by including the idea, features, category, and vulnerabilities of MANET. This paper presents an overview and the study of the routing protocols. Also include the several challenging issues, emerging application and the future trends of MANET. [5] Fan-Hsun Tseng et al, (2011) have reviewed various schemes of black hole detection in MANET under proactive, reactive and hybrid routing protocols. The proactive protocols show better packet delivery ratio and detection probability but have high routing overhead problems. Reactive protocols reduced routing overhead but failed to maintain efficient delivery of packets resulting in packet loss in initial procedures. The hybrid protocols combine the typical qualities of proactive and reactive protocols. The authors also carried out the study of security mechanisms like time based threshold scheme¸ hash based technique with perspective to black hole attack. [6] Caimu Tang, (2011) has discussed efficient authentication mechanisms for low-power devices. In the proposed scheme the mobile station simply require to overtake one packet for mutual authentication .He used the elliptic-curve-crypto system based trust delegation Mechanism to generated group pass code for mobile station authentication. With the make use of this authentication mechanism many active and passive attacks will be banned including the denial of service attack. The mobile device authenticated with the visiting base station only by the exchange of one packet. The author proposed mechanism that requires less computations and less message exchange as compared to other authentication schemes.

3. Black Hole Attack

In MANET inside and outside attacks are possible, which degrade the performance of the network. In inside attacks a node within the network become malicious node and it launched attacks on network. In outside attacks a malicious node which is outside the network, it become the member of the networks and then launch the attack on network. A

passive outsider eavesdrops on all communication and aims to compromise privacy. Among all attacks discussed so far black hole attack is the most common active type of attacks. Black hole attack is the denial of service attacks which is triggered by the malicious nodes in the network. In the previous works, many techniques have been proposed to isolate black hole attacks from the network. When black hole attack is triggered in the network, throughput of the network reduced and delay increase as steady rate. The black hole attack is even worse if the multiple black hole nodes exist in the network. When multiple black hole nodes exist in the network, all the malicious nodes are responsible for triggering the black hole attack. This type of attack is called multiple black hole attack. In our work, we work on to detect and isolate multiple black hole attack in mobile Ad hoc network.

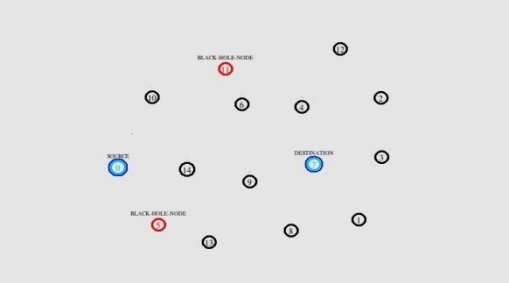
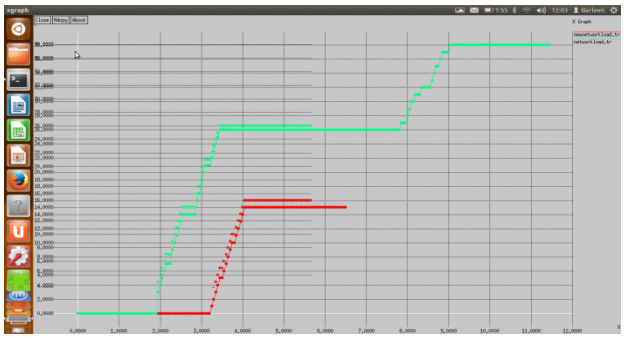


Fig. 1.1 Black Hole Attack

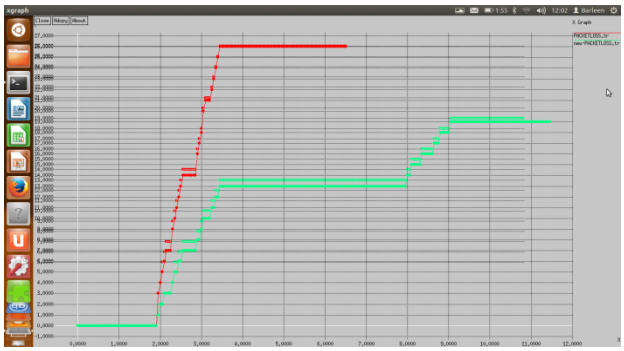
4. Proposed Method

In proposed work, firstly we randomly deploy nodes in the mobile ad hoc network. The source node and destination node are selected and the establishment of route is done. Route request message is broad-casted in the network for establishing the route. Intermediate nodes reply through Route reply message to the source node and further broadcast the route request message to find the required destination node. The source node selects the best path to the destination depending on the minimum hop counts and maximum sequence number. The malicious node is present in the path which advertises itself as the best optimal path to the destination. When multiple black hole nodes exist then it is said to be multiple black hole attack and is responsible for selective packets dropping. The proposed work will detect the black hole node and isolate it from the network. It is based on the packet loss of the network. When number of packets are dropped exceeding particular value and performance of network starts deteriorating then the network will start detecting the malicious node and ultimately inform rest of the nodes present in the network of the black hole nodes, thereby isolating them from the network. The proposed methodology will be implemented in network simulator version 2.

5. Results



Graph 1 Network Load Graph



Graph 1 Packet Loss Graph

Graph 1 shows network load of the network in presence of the black hole attack considerably incremented and enhancing the performance of the network. Green line shows network load under new technique and red line shows performance in old scenario. Graph 2 is showing packet loss comparison in both techniques.

Detection and isolation of malicious nodes which are responsible for selective packet dropping is done with implementation of proposed methodology. The packets are efficiently transmitted from source to the destination. It increases number of packets successfully received by destination and ultimately decreases the packet loss.

Conclusion

In this paper, we conclude that multiple black hole attack is one of the devastating attack done on the network. Due to this attack packet loss may occur and delay increases. The main aim of the paper is to isolate black hole attack so that packet loss of the network decreases and the throughput increases. Experimental results show that proposed modified DSR method is very efficient than existing method as it has low packet loss as compare to the old technique.

References

1. Stallings W., "Data and Computer Communications", Prentice Hall, 7th Ed., 2004
2. Sunil Taneja, Dr. Ashwani Kush, Amandeep Makkar, "End to End Delay Analysis of Prominent On-demand Routing Protocols", IJCST Vol. 2, Issue1, March 2011
3. Abdul Haimid Bashir Mohamed, Thesis, "ANALYSIS And Simulation Of Wireless Ad-Hoc Network Routing Protocols"2004
4. Priyanka goyal, vinit, Rishi, " MANET- A valunarable, challenge, attacks and application", IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011[1]
5. John A. Stankovic , "Wireless Sensor Network" , june 2006
6. Giovanni Vigna Sumit Gwalani Kavitha Srinivasan Elizabeth M. Belding-Royer Richard A. Kemmerer, "An Intrusion Detection Tool forAODV-based Ad hocWireless Networks", 2004
7. Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt and Piet Demeester, "An Overview of Mobile Ad Hoc Networks: Applications and Challenges" ,2005
8. Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei, "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks" ,Springer 2006
9. Sevil Şen, John A. Clark, Juan E. Tapiador, "Security Threats in Mobile Ad Hoc Networks", 2010
10. Rusha Nandy, "Study of Various Attacks in MANET and Elaborative Discussion Of Rushing Attack on DSR with clustering scheme" Int. J. Advanced Networking and Applications Volume: 03, Issue: 01, Pages:1035-1043 (2011)
11. Giovanni Vigna Sumit Gwalani Kavitha Srinivasan Elizabeth M. Belding-Royer Richard A. Kemmerer, "An Intrusion Detection Tool for AODV-based Ad hocWireless Networks", 2004
12. Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt and Piet Demeester, "An Overview of Mobile Ad Hoc Networks: Applications and Challenges" ,2005
13. Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei, "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks" ,Springer 2006
14. Wenjia Li and Anupam Joshi , "Security Issues in Mobile Ad Hoc Networks- A Survey",2005
15. Vinit Garg, Manoj Kr.Shukla, Tanupriya Choudhury, Charu Gupta, "Advance Survey of Mobile Ad-Hoc Network," IJCST Vol. 2, Iss ue 4, Oct . - Dec. 2011
16. Humayun Bakht, " Survey of Routing Protocols for Mobile Ad-hoc Network" , Volume 1 No. 6, October 2011 ISSN-2223-4985 International Journal of Information and Communication Technology Research

17. Tamilselvan, L. Sankaranarayanan, V. "Prevention of Blackhole Attack in MANET", Journal Of Networks,Vol.3,No.5,May2008.
18. Yi-Chun Hu, Adrian Perrig, "A Survey of Secure Wireless Ad Hoc Routing", IEEE Security and Privacy, 1540- 7993/04/$20.00 © 2004 IEEE, May/June 2004.
19. David B. Jhonson ,David A.Maltz and Josh Broch ,DSR: The Dynamic Secure Routing protocol for Multi-Hop Wireless Adhoc Networks.http://www.monarch.cs.cmu.edu .
20. D. Djenouri, L. Khelladi and N. Badache, A Survey of Security Issues in Mobile Ad Hoc and Sensor Networks, IEEE Communication Surveys & Tutorials, Vol. 7, No. 4,4th Quarter 2005.