Security and Cost based Comparative Analysis of Prevention Methods of Black Hole Attack in MANET

S. Sathyapriya[1] M. Reehanaparveen[2]
[1]Assistant Professor [2]Research Scholar (M. Phil)
[1,2]Department of Computer Science
[1,2]Sankara College of Science and Commerce, Coimbatore, India

Abstract— Mobile ad hoc network (MANET) is a self-organizing network. It formed a network by using mobile nodes without any pre-defined structure. MANET has dynamic topology which allows nodes to join and leave the network at any point of time. Security is an important parameter in mobile ad hoc network (MANET) because of its built-in Vulnerabilities. These are temperament of MANET structure that cannot be removed. As a result, attacks with malicious intent have been and will be devised to exploit these susceptibilities and to cripple MANET operation. The black hole attack at network layer is the most concentration seeking attack in ad hoc networks. Prevention methods are very important to detect and prevent the different attacks in MANET. But securable and cost effective prevention methods are play vital role in MANET. This paper analyze the various prevention methods of black bole attack and present the report based on secured and low cost prevention methods for black hole attack.

Key words: Black Hole Attack, MANET

I. INTRODUCTION

A MANET is a collection of mobile nodes that organize themselves into a network without any predefined infrastructure or centralized operation management [1]. Dynamic network topology, Fluctuating link bandwidth, multi-hop routing, self-organization, self-adaptive and self-configurable make it an attractive option for broad area of networking, particularly in military tactical, personal area, instant conferences and disaster area networks [2,3 and 4]. Additionally to features, energy constrained operation and limited physical security cause MANET be vulnerable to security attacks. Therefore providing security service in MANET is challenging that has attracted several researchers in this field [5, 6 and 7].

Several kinds of applications of MANET are emergency services, vehicle to vehicle communication, military battlefields and sensor networks. These wireless links makes the MANETs more susceptible to attacks, which make it easier for the attacker to go inside the network and get access to the ongoing communication. Black hole attack is one category of attack of MANET suffers from. In black hole attack, a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to intercept. Different kinds of attack prevention methods are available. Many researchers proposed various kinds of prevention methods for black hole attack. In this paper a different kind of survey is proposed. This paper produce a review report about prevention methods of black hole attacks based on two parameters one is security and another one is cost effective.

Black hole attack is a type of attacks in the MANET. It causes severe security problem in the network. In black hole attack [8][9] a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to intercept. This hostile node advertises its availability of fresh routes irrespective of checking its routing table. In this way attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it [10]. In protocol based on flooding, the malicious node reply will be received by the requesting node before the reception of reply from actual node; hence a malicious and forged route is created. When this route is establish, now it's up to the node whether to drop all the packets or forward it to the unknown address [11].

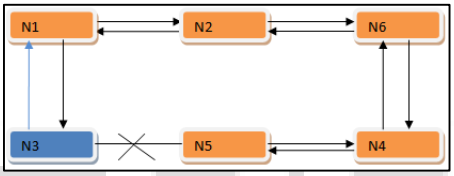

Fig. 1: Black Hole Attack problem

The method how malicious node fits in the data routes varies. Figure 1 shows how Black Hole problem arises, here node "N1" want to send data packets to node "N4" and initiate the route discovery process. So if node "N3" is a malicious node then it will claim that it has active route to the specified destination as soon as it receives RREQ packets. It will then send the response to node "N1" before any other node. In this way node "N1" will think that this is the active route and thus active route discovery is complete. Node "N1" will ignore all other replies and will start seeding data packets to node "N3". In this way all the data packet will be lost consumed or lost. Black hole Attacks are classified into two categories:

A. Single Black Hole Attack [11, 12]

In Single Black Hole Attack only one node acts as malicious node within a zone. It is also known as Black Hole Attack with single malicious node.

B. Collaborative Black Hole Attack [13, 14]

In Collaborative Black Hole Attack multiple nodes in a group act as malicious node. It is also known as Black Hole Attack with multiple malicious nodes.

II. SECURITY ISSUES IN MANET

Security in MANET is the most important concern for the basic functionality of network. Availability of network services, confidentiality and integrity of the data can be achieved by assuring that security issues have been met. MANET often suffer from security attacks because of the its features like open medium, changing its topology

dynamically, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism. These factors have changed the battle field situation for the MANET against the security threats.

MANETs are very flexible for the nodes i.e. nodes can freely join and leave the network. There is no main body that keeps watching on the nodes entering and leaving the network. All these weaknesses of MANETs make it vulnerable to attacks and these are discussed below.

- Non secure boundaries: MANET is vulnerable to different kind of attacks due to no clear secure boundary. The nature of MANET, nodes have the freedom to join and leave inside the network. Node can join a network automatically if the network is in the radio range of the node, thus it can communicate with other nodes in the network. Due to no secure boundaries, MANET is more susceptible to attacks. The attacks may be passive or active, leakage of information, false message reply, denial of service or changing the data integrity. There is no protection against attacks like firewalls or access control, which may result the vulnerability of MANET to attacks [15].
- Availability ensures the survivability of network services despite denial of service attacks. It assures that the services of the system are available at all times and are not denied to authorize users. A denial of service attack could be launched at any layer of an ad hoc network.
- Confidentiality ensures that certain information is never disclosed to unauthorized entities. In MANETs, this is more difficult to achieve because intermediates nodes (that act as routers)receive the packets for other recipients, so they can easily eavesdrop the information being routed.
- Integrity guarantees that a message being transferred is never corrupted. And Message being transmitted is never altered. A message could be corrupted because of benign failures, such as radio propagation impairment, or because of malicious attacks on the network.
- Authentication Assure that an entity of concern or the origin of a communication is what it claims to be or from. It enables a node to ensure the identity of the peer node it is communicating with. Without authentication, an adversary could masquerade a node, thus gaining unauthorized access to resource and sensitive information and interfering with the operation of other nodes. Scalability and cost is the most important security issues.

III. VARIOUS PREVENTION METHOD FOR BLACK HOLE ATTACK BASED ON VARIOUS PARAMETERS

According to the various parameters in security issues in MANET. This paper reviews the various methods and produces a table. Table 1.1 contains the analysis of various prevention methods based on high security, low cost, collusive attack, and communication overhead.

In this review only one method Mechanism for controlling cooperative back hole attack is produce very high communication overhead is proposed by Jaydip Sen et.al 2011. Sun, Guan, Chen and Pooch, 2003 proposed neighborhood-based approach. This method provides medium communication overhead. Johnson, and A. Perrig, 2002, The Secure Efficient Ad hoc Distance vector routing protocol (SEAD) ,this method also provides medium communication overhead. Multipath ADOV routing protocol and DPRAODV (Detection, Prevention and Reactive AODV) method s provides the high communication overhead. Selfish behavior control mechanism, Further Request and Reply and Shared Awareness Ad hoc Routing (SAR) provides low communication overhead.

IV. CONCLUSION AND FUTURE WORK

Ad hoc networks are an increasingly promising area of research with lots of practical application. However MANET are extremely vulnerable to Attack due to their dynamically changing topology, absence of conventional security infrastructure and open medium of communication, which unlike their wired. This paper has consolidated various works related to prevention against black hole attack methods in MANETs. A comparative study between them was then conducted to highlight their respective effectiveness and limitations. For future work, develop a more complex black hole attack scenario.

REFERENCES

[1] S. K. Alampalayam and F. E. Natsheh, "Multivariate Fuzzy Analysis for Mobile Ad hoc Network Threat Detection", International Journal of Business Data Communications and Networking , Volume 4, Issue 3, 2008.
[2] P. Vinayakray-Jani, "Security within ad hoc networks," presented at First PAMPAS Workshop, London, UK, pp. 66-67., 2002.
[3] K. Wrona, "Distributed security: Ad hoc networks & beyond," presented at First PAMPAS Workshop, London, UK, pp. 70-71.2002.
[4] F. Stajano and R. Anderson, "The resurrecting duckling: Security issues for ad hoc wireless networks," in Proceedings of International workshop on Security Protocols, pp. 172-194., 1999.
[5] Y. Zhang, W. Lee, and Y. Huang, "Intrusion detection techniques for mobile wireless networks," Wireless Networks, vol. 9 no. 5, pp. 545-556., 2003.
[6] D. E. Denning, "An intrusion-detection model," IEEE Transactions on Software Engineering, vol. SE-13, no. 2, pp. 222-232, February 1987.
[7] J. P. Anderson, Computer Security Threat Monitoring and Surveillance. Fort Washington: James P. Anderson Co., 1980.
[8] E. A .Mary Anita and V. Vasudevan, "Black Hole Attack Preventionin Multicast Routing Protocols for mobile Adhoc networks using Certificate Chaining", International Journal of Computer Applications (0975 – 8887) Vol. 1, Issue 12, pp. 21-28, 2010
[9] Umang S, Reddy BVR, Hoda MN, " Enhanced Intrusion Detection System for Malicious Node Detection in Ad Hoc Routing Protocols using Minimal Energy Consumption", IET Communications Vol.4, Issue17, pp2084–2094. doi: 10.1049/ietcom. 2009.
[10] K. Biswas and Md. Liaqat Ali, "Security threats in Mobile Ad-Hoc Network", Master Thesis, Blekinge Institute of Technology" Sweden, 22nd March 2007.
[11] N. Bhalaji and A. Shanmugam, "A Trust Based Model

to Mitigate Black Hole Attacks in DSR Based Manet", European Journal of Scientific Research, Vol.50 No.1, pp.6-15, 2011
[12] Latha Tamilselvan and Dr. V Sankaranarayanan, "Prevention of Blackhole Attack in MANET", The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, 0-7695-2842-2/07, 2007.
[13] Chang Wu Yu, Tung-Kuang Wu, Rei Heng Cheng, and Shun Chao Chang, "A Distributed and Cooperative Black Hole Node Detection and Elimination Mechanism for Ad Hoc Networks", PAKDD 2007 Workshops, LNAI 4819, pp. 538–549, 2007
[14] Santhosh Krishna B V, Mrs.Vallikannu A.L , "Detecting Malicious Nodes For Secure Routing in MANETS Using Reputation Based Mechanism" International Journal of Scientific & Engineering Research, Vol. 1, Issue 3, ISSN 2229-5518, December-2010.
[15] Y.-C. Hu, D.B. Johnson, and A. Perrig, "SEAD: SecureEfficient Distance Vector Routing for Mobile Wireless Ad hoc Networks," Proc. 4th IEEE Workshop on Mobile Computing Systems and Applications, Callicoon, NY, June 2002, pp. 3-13.
[16] Y.-C. Hu, A. Perrig, and D.B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad hoc Networks," Proc. 8th ACM Int'l. Conf. Mobile Computing and Networking (Mobicom'02), Atlanta, Georgi a, September 2002, pp. 12-23.
[17] Kimaya Sanzgiti, Bridget Dahi ll, Brian Neil Levine, Clay shields, Elizabeth M, Belding-Royer, "A secure Routing Protocol for Ad hoc networks In Proceedings of the 10th IEEE International Conference on Network Protocols (ICNP' 02), 2002
[18] Payal N. Raj, Prashant B. Swadas , DPRAODV: A DYANAMIC LEARNING SYSTEM AGAINST BLACKHOLE ATTACK IN AODV BASED MANET ,IJCSI International Journal of Computer Science Issues, Vol. 2, 2009
[19] B. Sun, Y. Guan, J. Chen and U.W.Pooch,"Detecting black-hole attack in mobile ad hoc networks", Proc. 5th European Personal Mobile Communications Conference , Apr 2003, pp.490-495.
[20] S. Kurosawa, H. Nakayama, N. Kato, A. Jamalipour and Y. Nemoto, "Detecting blackhole attack on AODV-based mobile ad hoc networks by Dynamic Learning Method", Intl Journal of Network Security, vol 5, no.3, Nov. 2007, pp. 338-346.
[21] H. Deng, W. Li and D. P. Agrawal, Routing security in wireless ad hoc networks, IEEE Commun. Mag., 40(10): 70-75, October 2002.
[22] S. Marti, T. J. Giuli, K. Lai and M. Baker, Mitigating routing misbehavior in mobile ad hoc networks, In Proc. 6th annual international conference on Mobile computing and networking (MOBICOM '00),Boston, Massachusetts, USA, August 2000.
[23] Buchegger and Jean-Yves Le Boudec. Coping with False Accusations in Misbehavior Reputation Systems for Mobile Ad Hoc Networks. EPFL Technical Report Number IC/2003/31, 2003.
[24] Jaydip Sen 1, Sripad Koilakonda 2, Arijit Ukil 3, A Mechanism for Detection of Cooperative Black Hole Attack in Mobile Ad Hoc Networks, In 2011 Second International Conference on Intelligent Systems, Modeling and Simulation.
[25] S. Buchegger and Jean-Yves Le Boudec. Coping with False Accusations in Misbehavior Reputation Systems for Mobile Ad Hoc Networks. EPFL Technical Report Number IC/2003/31, 2003.

