Volume 4, Issue 2, February 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Security Requirements in MANETs: A Review

Karamjeet Singh*, Chakshu Goel, Gurpreet Singh

ECE, SBSSTC, Ferozepur

India

Abstract — MANETs are vulnerable to number of attacks or threats. Generally attacks are the threats against MAC, Physical, and network layer. These layers are the most important layers that used for the routing mechanism of the ad hoc network. Black hole attack is one of the most important security problems in Mobile Ad hoc Network. It is the attack that a malicious node impersonates a destination node by sending forged RREP to a source node or initiate node that initiates route discovery, and deprives data traffic from the source node. In this paper, we present a review on number of studies that defines internal & external attacks in MANET.

Keywords— MANETs; Routing; Attacks; Node; Security;

I. INTRODUCTION

A Mobile Ad hoc Network (MANET) is a system of wireless mobile nodes that dynamically self-organize in arbitrary and temporary network topologies. The people and vehicles can thus be Internet worked in areas without an existing communication infrastructure or when the use of such infrastructure requires wireless extension. In the mobile ad hoc network, nodes communicate with all the nodes within their radio ranges whereas nodes which are not in the direct communication range use intermediate node(s) to communicate with each other. In these two situations all the nodes that have participated in the communication automatically form a wireless network this kind of wireless network can be viewed as mobile ad hoc network.

The mobile ad hoc network has the following features

- Unreliability of wireless links between nodes. The limited energy supply for the wireless nodes and the mobility of the nodes .The wireless links between mobile nodes in the network are not consistent for communicating participants.
- Constantly changing topology. Due to the continuous motion of the nodes the topology of the network changes constantly the nodes can move into and out of the radio range of the other nodes in the ad hoc network and the routing information will be changing all the time because of the movement of the nodes.
- The Lack of incorporation of security features in statically configured wireless routing protocol not meant for ad hoc environments. Because topology of the ad hoc networks is changing it is necessary for each pair of adjacent nodes to incorporate in routing issue to prevent some kind of attacks that try to make use of vulnerabilities in the configured routing protocol.

Because of these features, the mobile ad hoc networks are prone to suffer from the malicious behaviours. Therefore, we need to pay attention to the security issues in the mobile ad hoc networks. Security has become a primary concern in order to provide protected communication between mobile nodes. Unlike the wire line networks the unique characteristics of mobile ad hoc networks pose a number of nontrivial challenges to security design, such as shared wireless medium, open peer-to-peer network architecture, stringent resource constraints and highly dynamic network topology. These challenges make a case for building multi-defence security solutions that achieve both broad protection and desirable network performance. We focus on the fundamental security problem of protecting the multi-hop network connectivity between mobile nodes in a MANET.

The features of MANETs and the problems/issues are summarized as follows:

Wireless medium: Mobile nodes communicate with each other through wireless medium, which means one transmission can cover all audiences within the transmission range. This broadcast nature is also referred as the Wireless Multicast Advantage (WMA). This is an advantage for broadcast or multicast traffics, however, for unicast traffic, because of the broadcast nature; the nodes within same transmission/interference range have to compete with each other for the network channel. For data access applications which follow the Client/Server model, unicast is the mostly used communication style. If there are multiple data access sessions going on simultaneously, users may encounter increased communication delay or even packet losses due to the competition and interferences from other sessions.

Multi-hop routes: In MANETs, multi-hop routes are used when a node communicates with the nodes that are out of its immediate transmission range. As analyzed by Li etc., the optimal throughput for a multi-hop communication is about 1/3 of the throughput of a single hop communication, as a forwarding node cannot transmit and receive at the same time,

and the upstream and downstream nodes of the forwarding node cannot transmit at the same time because the packets would conflict at the forwarding node. Their results measured on real hardware show that the throughput drops while the number of hops covered gets increased. For data access, the indication is that as the number of hops between a client and a server increases, the throughput will decrease and the response delay will increase accordingly.

Dynamic topologies: Network topology may change for MANETs due to node mobility, exhausted power, and interferences etc. Changing of network topologies may break existing routes and cause extra overhead for establishing new routes. For data access applications, if the route to the server is broken, the client/server communication will be delayed if a new route needs to be established, or even get dropped if the new route cannot get established in time. This delay or disconnection has more chances to happen if there are more forwarding nodes involved in the client/server communication path.

Limited resources: In MANETs, the mobile nodes usually have restricted power supply, limited computing capability, and limited storage space. Due to this fact, data accesses applications shall be able to function properly with least resource possible. That is, data access applications need to be energy-efficient and light-weight (not computing-hungry or memory-hungry).

II. SECURITY REQUIREMENTS & ISSUES IN MANETS

A. Security Requirements in MANETs

Mobile wireless networks are generally more prone to physical security threats than are fixed wired networks. Existing link level security techniques (e.g. encryption) are often applied within wireless networks to reduce these type of threats. Absent link-level encryption, at the network layer, the major issue is one of inter-router authentication prior to the exchange of information regarding network control. Several levels of authentication ranging from no security and simple key approaches to fully public key infrastructure-based authentication mechanisms will be explored by the group. As the working groups efforts, a number of optional authentication modes may be standardized for use in MANETs. Some of the Security requirements in MANETs are:

- Availability
- Authorization and Key Management
- Data Confidentiality
- Data Integrity
- Non-repudiation

B. Security Issues in MANETs

Due to the fact that MANET is a group of nodes that form a temporary network without centralized administration, the nodes have to communicate with each other based on unconditional trust. This characteristic leads to the consequence that MANET is more susceptible to be attacked by inside the network while comparing to other type of networks. Practically, MANET could be attacked by several ways using multiple methods; before going to deeper investigation, it is necessary to classify security attacks within the context of MANET. The classification can be based on the behaviour of the attack (Passive vs. Active), the source of the attacks (Internal vs. External), the number of the attackers (Single vs. Multiple) and the processing capacity of the attackers (Wired vs. Mobile) [8]. We choose these attack classifications because they are applicable to the collaborative attacks we are categorizing. We illustrate further on the latter two as the collaborative nature of the attack could take any of the methods.

Passive vs. Active attack

Typically, passive attacks aim to steal valuable information in at least two communicating nodes or even in the whole network. There are many variations of passive attacks, but in MANET, there exist two types: eavesdropping and traffic analysis. Practically, depending on situations, passive attacks can be considered as legitimate or illegitimate actions. If the purpose is benign, for example, if the administrator wants to use some tools to probe the network traffic, in order to troubleshoot or account the network then it is legitimate. On the contrary, if the purpose is malicious, one attacker can steal valuable information by probing the network traffic such as credit card information, credential email, and then use the information to illegally withdraw money from bank accounts or blackmail the victims. Roughly speaking, passive attacks do not intend to disrupt the operation of the particular network, but active attacks are able to alter the normal network operation.

Internal vs. External attack

As the name implies, external attacks are launched by attackers who physically stay on outside of the attacked network. These attacks usually aim to deny access to specific function in the network (i.e. http traffic), or to cause network congestion or even to disrupt the whole network. While external attacks would be difficult to be launched if the network was properly configured and protected, the internal attacks are much tougher to defend against. One of the reasons is because we tend to protect the network from being attacked by outsiders rather than insiders. Also because of the fact that an external attack can easily be traced compared to the internal attack.

An external attack can become an internal attack and the consequence of the attack would be more serious. Therefore, there exist two types of internal attacker nodes, one is the compromised node, which was discussed above, and the other one is the misbehaving node, which is authorized to access the system resources but fail to use them according to the way it should be used. The detection of the Attacks caused by these internal misbehaving nodes are difficult, for example,

selfish attack in which the node is unwilling to consume battery power, CPU cycles or network bandwidth to forward uninterested packets, even though it expects other nodes to forward packets for it.

III. EXISTING TECHNIQUES

H. Deng [4] proposed the method for detecting the single black hole node in MANET. In this method, the intermediate nodes send RREP message along with the next hop information. After getting this information, the source node sends further request to next hop node to verify that it has the route to the intermediate node or not. If the route exists, the intermediate node is trusted and source node will send data packets via that trusted node. If not, the reply message from intermediate node will be discarded and alarm message is broadcasted and isolate the detected node from network. By using this method, the routing overhead and end to end delay will be increased. If black hole nodes work as a group in an attempt to drop packets then this method is not efficient.

Mohammad Al-Shurman [15] proposed the two methods to avoid the black hole attacks. According to the first solution, the source node verifies the validity of the route by finding more than one route to the destination. It waits for RREP packets to arrive from more than two nodes. When the source node receives RREP packets and the routes to destination have shared hops then the source node can then recognize the safe route. This method causes routing delay. The second solution is to store the last packet sent sequence number and the last packet received sequence number in a table. When node receives reply message from another node it checks the last sent and received sequence number. If there is any mismatch, then the ALARM packet is broadcasted which indicates the existence black hole node. This mechanism is reliable and faster having no overhead.

Latha Tamilselvan [9] proposed the solution in which the source node waits for the responses including the next hop details from other neighbouring nodes for a predefined time value. After the timeout value, it first checks in the CRRT (Collect Route Reply Table), whether there is any repeated next-hop-node or not. If any repeated next-hop node is present in the return paths, it assumes the paths are correct or the chance of malicious paths is very less. The solution adds a delay and the process of finding repeated next hop is an additional overhead.

Maha Abdelhaq, Sami Serhan, Raed Alsaqour and Rosilah Hassan [12] provide an improvement over the solution in which the used method is Source Intrusion Detection (SID) method. This mechanism is good for small scale MANET but when this mechanism is applied in a large scale MANET and the distance between the source node and the intermediate node is long then the above solution is not sufficient. Secondly, if the distance between the source node and the intermediate node is long then the delay in the discovery period of the route will be high, which causes an overall network performance degradation. In order to mitigate the drawbacks in SID security routing mechanism, a new mechanism called Local Intrusion Detection (LID) security routing mechanism is proposed to allow the detection of the attacker to be locally; which means that when the suspected intermediate node unicast the RREP towards the source node, the previous node to the intermediate node performs the process of detection and not the source node.

Yiebeltal Fantahun Alem, Zhao Chenh Xuan [13] proposed an Intrusion Detection using Anomaly Detection (IDAD) technique to prevent the black hole attack. IDAD assumes every activities of a user or a system can be monitored and anomaly activities of an intruder can be identified by normal activities. So by identifying anomaly activities of an adversary there is a possiblility to detect a possible intrusion and isolate the adversary. To do so an IDAD needs to be provided with a pre-collected set of anomaly activities that is audit data. Once audit data is collected and is given to the IDAD system, the IDAD system can compare the every activity of a host with the audit data on a fly. If any activity of a host (node) resembles with the activities listed in the audit data then this IDAD system isolates the particular node by forbidding further interaction. It minimizes the extra routing packets which in turn minimizes the network overhead and facilitates faster communication.

DRI Table and Cross Checking [16] Scheme is used to identify the cooperative black hole nodes. Each node maintains the extra DRI table with two entries "From" and "Through", where 1 represents for true and 0 for false. These entries stand for the information on routing data packet from and through the nodes. In this solution, the Intermediate node replies the next hop information and DRI entry about next hop node along with RREP packet. The source node then checks the reliability of intermediate nodes by using cross checking scheme via alternate paths by using DRI table information. It provides 50 % throughput but increases end to end delay and routing overhead.

In the paper [19] a mechanism to detect the multiple black hole nodes has been proposed by modifying AODV protocol. This paper is an enhancement to the AODV protocol by proving more security after detecting the single or multiple black hole nodes in MANET. By using fake RREQ packet and modified RREP packet, the multiple black hole nodes are detected at the initial stage before the actual route discovery process of AODV, which leads to less routing overhead and high PDR.

IV. CONCLUSION

Mobile Ad hoc Networks (MANET) is a self-configuring & infrastructure less network consists of independent mobile nodes that can communicate via wireless medium. In this, each mobile node can move freely in any direction and changes their links to other devices frequently. The Security is an essential part of ad hoc networks. Because of its dynamic topology, the resource constraints with no centralized infrastructure and limited security, this is vulnerable to various attacks and black hole attack is one of them. This attacks the malicious node advertises itself as having the shortest path to the destination and falsely replies to the route requests, and drops all receiving packets. In this paper various mechanisms has been studied to detect the different attacks and concluded that the Security in ad hoc networks is still considered to be a challenging task.

REFERENCES

[1] Kartik Kumar Srivastava, Avinash Tripathi, and Anjnesh Kumar Tiwari, " Secure Data Transmission in MANET Routing Protocol" IJCTA , Int.J.Computer Technology & Applications,Vol 3 (6), 1915-1921 Nov-Dec 2012.

[2] Danai Chasaki and Tilman Wolf, "Evaluation of Path Recording Techniques in Secure MANET".

[3] Vineetha S. H. and Shebin Kurian, " Performance Analysis of Cluster Based Secure Multicast Key Management in MANET" **I**nternational **J**ournal of **C**omputer **S**cience and **T**elecommunications, Volume 4, Issue 4, April 2013.

[4] Hongmei Deng, Wei Li, and Dharma P.Agarwal, "Routing Security in Wireless Ad Hoc Network", IEEE Communications Magazine, Volume 40, Number 10, 2002, pp 70-75.

[5] Merin Francis, M. Sangeetha, and Dr. A. Sabari, "A Survey of Key Management Technique for Secure and Reliable Data Transmission in MANET" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 1, January 2013, ISSN: 2277 128X.

[6] J. Liebeherr, J. Wang, and G. Zhang. Programming overlay networks with overlay sockets. In Proc. 5th COST 264 Workshop on Networked Group Communications (NGC 2003), LNCS 2816, pages 242–253, Sep. 2003.

[7] H. Lundgren, E. Nordstrom, and C. Tschudin. Coping with communication grayzones in IEEE 802.11b. In Proc. of 5th ACM International Workshop on Wireless Mobile Multimedia (WoWMoM 2002), Sep. 2002.

[8] H. Luo, J. Kong, P. Zerfos, S. Lu, and L. Zhang. Ursa: Ubiquitous and robust access control for mobile ad hoc networks. ACM/IEEE Transactions on Networking, 2005. To appear.

[9] LathaTamilselvan and V Sankarnarayana, " Prevention of Black Hole Attack in MANET", Journal of Networks, Volume 3, Number 5, 2008, pp 13-20.

[10] C. E. Perkins and E. M. Royer. Ad-hoc on-demand distance vector routing. In Proc. 2nd IEEE Workshop on Mobile Computing Systems and Applications, pages 90–100, Feb. 1999.

[11] K. Lakshmi et al. "Modified AODV Protocol Against Black hole Attacks in MANET" International Journal of Engineering and Technology Vol.2 (6), 2010, 444-449.

[12] Maha Abdelhaq, Sami Serhan, Raed Alsaqour and Rosilah Hassan "A local Intrusion Detection Routing Security over MANET Network", IEEE, July 2011, Bandung, Indonesia.

[13] Yiebeltal Fantahun Alem, Zhao Chenh Xuan, " Preventing Black Hole Attack in Mobile Ad-hoc Networks Using Anamoly Detection",2nd International Conference on Future Computer and Communication, IEEE, Volume 3, 2010.

[14] S.Marti, T.J.Giuli, K.lai and M.bakery "Mitigating routing misbehaviour in mobile ad hoc networks", 6th MobiCom, Boston, Massachusetts, August 2000.

[15] Mohammad Al-Shurman, Seong-Moo Yoon and Seungjin park, "Black Hole Attack in Mobile Ad Hoc Networks", ACM Southeast Regional Conference, Proceedings of the 42nd annual southeast regional conference , 2004, pp 96-97.

[16] J.Sen, S.Koilakonda and A.Ukil, "A mechanism for detection of cooperative black hole attack in mobile ad hoc networks", Second International Conference on Intelligent System, Modeling and Simulation ,Innovation lab, Tata consultancy services ltd. , Kolkata, 25-27January 2011.

[17] Rakesh Kumar Sahu, Dr. Narendra S. Chaudhari, "Efficient Techniques to Detect the Various Attacks in Ad-Hoc Network", November 2002**.**

[18] Sanjay Ramaswamy, Huirong Fu, John Dixon "Prevention Of Cooperative Black Hole Attack In Wireless Ad Hoc Network", Department of Computer Science, IACC 258, North Dakota State University, Fargo, ND 58105.

[19] Nishu Kalia, Kundan Munjal, "Multiple Black Hole Node Attack Detection Scheme In MANET By Modifying AODV Protocol" , International Journal of Engineering and Advanced Technology (IJEAT), Volume-2, Issue-3, February 2013.

[20] H. Rangarajan "Robust loop-free on-demand routing in Ad-hoc networks" PhD dissertation, University of California, USA, June 2006.

[21] Ranjeet Singh, and Prof. Harwant Singh Arri, "COMPARISON OF AAMRP AND IODMRP USING SBPGP" International Journal of Computer Science and Management Research, Vol 2 Issue 3 March 2013.ISSN 2278-733X.

