International Journal Of Engineering Research & Management Technology ISSN: 2348-4039

March 2014 Volume 1, Issue 2

Email: editor@ijermt.org Website: ijermt.org

A SURVEY: ON MOBILE AD HOC NETWORKS SECURITY & VULNERABILITIES

Swati shukla **Sunil Kumar Singh**

M-Tech (CSE) Research Scholar **M-Tech Assistant Professor**

Galgotia's University, Greater Noida.

ABSTRACT:

In this paper, we have discussed the security issues and their solutions in the mobile ad hoc network. A mobile ad hoc network is termed as infrastructure less network by wireless links. We basically discuss and analyze the main vulnerabilities in the MANET. In this we have also discussed the security issues of the mobile ad hoc network and also discuss the main attack. Finally we will survey the current security solutions from the MANET.

Keywords: Mobile Ad hoc Network, Security, Intrusion Detection, Secure Routing, Wireless Sensor Network.

I. Introduction:

In the recent years due to the growth of mobile computing devices like laptops, PDAs personal digital assistants have made revolutionary changes in this world. In the ubiquitous computing environment individual users utilize at that instant of same time, several electronic platforms through which they can access all the required information whenever and wherever they may be [1]. A mobile ad hoc network (MANET) is a collection of two or more devices with wireless communication and communicates with each other. A mobile ad hoc network (MANET) is a system of wireless mobile nodes that are self-organized in arbitrary and temporary network topologies [2]. Basically in MANET nodes that are within a radio range can communicate each other directly; whereas nodes that are not in the radio range use intermediate nodes to communicate with other nodes.

In this paper we have also discussed about the vulnerabilities that make the mobile ad hoc network less secure and also the survey of current security solution for MANET. At last we will draw the conclusion for the paper and point out some potential works for future.

II. Security Issues in MANET:

A. Confidentiality: Here confidentiality means, accessing of information only by the authorized user.

B. Availability: Availability means that a node should maintain its ability to provide all the designated services regardless of the security state to it [3]. This security criterion is challenged mainly during the denial-of-services attacks, in which all the nodes in the network can be the target and thus some selfish nodes make some of the network services unavailable, such as the routing protocol or the key management services [4].

C. Authentication: Authentication is essentially assurance those participants in communication are genuine and not impersonators [3]. In order to maintain the security it is very necessary to prove their identities.

D. Integrity: Integrity means that the information which we are receiving is same as it was send by source. Integrity can be compromised mainly in two ways [5].

- Malicious Altering
- Accidental Altering

In malicious altering the information can be altered by malicious node. In accidental altering the information is changed or lost due to accidental node failure.

E. Non-Repudiation: Non-Repudiation means when the information is sent from sender to receiver, the sender or receiver cannot deny that they have even sent or receive the message or information.

F. Authorization: Authorization means to provide security through certificate authority (CA) which ensures that the user is authorized. Basically it provides high level security to the information or messages.

G. Eavesdropping: Eavesdropping means act of secretly listening of the private conversation of others without their consent.

H. Traffic Analysis: Traffic analysis means a security attack occur by extracting information from the analysis of network traffic.

III. Vulnerabilities of the Mobile Ad Hoc Network

Security is more difficult to maintain in mobile ad hoc network than in the traditional wired network. In this section, we will discuss the various vulnerabilities that exist in the mobile ad hoc network.

A. Lack of Boundaries: In this the vulnerabilities generally occurs due to the nature of the MANET, in which node can easily join, leave and move inside the network whenever, wherever. When wireless MANET compared with the wired MANET, in wired MANET the adversaries pass through several medium like firewall and gateway before they can perform malicious behavior to the target [6]. However in the MANET once the adversary is in the radio range of any other nodes, it can join the network automatically. As a result the MANET does not provide the secure boundaries to protect from the threats.

B. Threats from Compromised Nodes inside the Network: Since there is no fixed boundary in MANET, therefore it becomes more vulnerable to link attack. These link attacks take place between the nodes and try to perform malicious behaviors to disrupt their working. Since mobile nodes are free to join or leave the network because of the mobility of the mobile ad hoc network a compromised node can change its attack target and perform malicious behaviors to different node in the network hence it became very difficult to find out the malicious behavior performed by a compromised node which is very much dangerous and even much harder to detect.

C. Lack of Centralized Management: As ad hoc network do not have centralized administrator such as server which leads to some vulnerability problems. In the absence of centralized management system, detection of attacks is very difficult because it is very harder to monitor the traffic in a highly dynamic and large scale ad hoc network [7]. In the MANET benign failure is very common such as path breakage, packet dropping and transmission impairments which happens very frequently, that's why malicious failure will be difficult to detect, when adversaries change their attack pattern and their attack target in different period of time.

Therefore, the lack of centralized management machinery will impede the trust manage for the nodes in the ad hoc network [3]. In the MANET all the nodes cooperate in the network operations while no security association (SA2) can be assumed for all the network nodes. Thus it is not practical to perform a priori classification and a result the usual practice of establishing a line of defenses which distinguishes nodes as trusted and non-trusted cannot be achieved in the MANET.

D. Restricted Power Supply: As we already know, due to the mobility of nodes in the ad hoc network, it is common that nodes in the ad hoc network will reply on battery as their power supply method while nodes in the wired network don not have to consider about the power supply problem because they can get electric power supply from the outlet. Nodes in the MANET need to consider the restricted battery power which will cause several problems. One of these problems is denial-of-service attack [3]. Therefore the adversary knows that the target node is battery restricted, it can continuously send additional packets to the target and ask it routing those additional packets.

IV. Security Attacks

Security in the wireless ad hoc network is a challenging issue. Understanding the attack is always the first step for developing good security solution. Detailed analysis of ad hoc network security issues is very necessary. We will summarize only the main directions of security in ad hoc networks. Active attack involves actions like:

- Modification
- Deletion of exchange data
- Replication

Active attacks can be easily performed against an ad hoc network. These attacks grouped as:

- Impersonation
- Denial-of-services(DoS)
- Disclosure attack

Secure routing protocols helps to cope with malicious nodes that can disrupt the functioning of routing information by fabricating false routing information and by impersonating other nodes. In the brought up also a new type of attack called wormhole attack, cooperation enforcing a basic requirement for keeping an MANET operational is to enforce ad hoc nodes contribution to basic network functions are carried out by the nodes. This difference is the main of the security problem that are specific to ad hoc network. As dedicated nodes to a classical network, the nodes of an ad hoc network can't be trusted for the correct execution of critical network function for e.g. Routing is vulnerable in ad hoc network because each node acts as a router. Forwarding mechanism is cooperative as well. The nodes which do not cooperate is called misbehaving node. Misbehavior can be caused by nodes that are malicious or selfish.
A malicious node does not cooperate because it wants to damage network by dropping packet.

V. Types of Attacks in MANET

In the mobile ad hoc networks the attacks are classified as the following two types [6]:

A. External Attacks: External attack is defined as, in which the attackers disrupt the whole network by causing congestion, which propagates fake routing information or disturbs nodes from providing services.

B. Internal Attacks: Internal attacks is defined as, in which adversary wants to gain the normal access to the network and then participate in the network activities, by some malicious action to get the access to the network as a new access to the network as a new node or by compromising node and then causing malicious behavior.
The external attack is similar to the normal attack in the wired network. This type of attack can be detected and prevented by some security methods such as authentication or firewall. But internal attack are far more dangerous than the external attack: because the compromised nodes are the benign users of the ad hoc

network, they can easily pass the authentication and get protection and then adversaries make use of them to gain normal access to the services. And can disrupt the network badly. So we have to pay more attention to the internal attacks in the mobile ad hoc network. We discuss the main attack types that emerge in the MANETs.

C. Denial-of-Service Attack: Denial-of-Service Attack basically disrupts all the services of the ad hoc network. The mobile ad hoc network is more vulnerable because of the interference-prone radio channel and limited battery power. The attacker uses the radio jamming and battery exhaustion method to conduct denial-of-service attack.

D. Impersonation: Impersonation attack is a threat to the security of mobile ad hoc network [3]. If no proper steps are taken the adversary will capture all the nodes in the network and make them look like benign nodes. Therefore in this way compromised nodes can join the network as the normal node and conduct the malicious behavior.

E. Eavesdropping: Eavesdropping means act of secretly listening of the private conversation of others without their consent. The main goal of eavesdropping is to obtain confidential information that should kept secret during communication.

F. Attacks against Routing: Routing is one of the most important services in the network. In routing attackers easily conduct malicious behaviors. In mobile ad hoc network attacks against routing are generally classified into two categories: attacks on routing protocols and attacks on packet forwarding/delivery [6].
There are some attacks against routing that have been studied and well known [7] [8] [9] [10].

- Impersonating another node to spoof of route message.
- Suppressing route error to mislead other.
- Flooding route discovery excessively as a denial-of-service attack.
- Modifying a route reply message to inject a false route.
- Generate bogus route error to disrupt a working route.
- Advertising a false route metric to misrepresent the topology.
  Because of the mobility and constantly changing topology of the mobile ad hoc network it is difficult to validate the entire route message [6]. There are some routing attacks like wormhole attack [11], rushing attacks [12], and Sybil attack [13].

VI. SOLUTIONS OF SECURITY ISSUES IN MANET:

A. Hash: The hash of messages is a set of bits obtained after applying specific algorithm.

B. MAC: Combination of hash and security key.

C. Encryption: Public key and private key encryption.

D. SSL: SSL is a protocol in between HTTP and TCP for secure transactions.

E. Check sum: Check sum and parity are the primitive methods check message integrity.

F. IPSec: IPSec is a method for message integrity check.

G. CHAP: CHAP is a method for authentication of point to point communication.

H. RADIUS: RADIUS is a service for sending the message that the client stands authenticated.

I. AAA: AAA is a strategy for authentication.

J. There are two main techniques in the MANET for security purpose:

a. Intrusion detection techniques: Intrusion detection is not a new concept in the network research. According to the definition in the Wikipedia, an Intrusion Detection System (or IDS) generally detects unwanted manipulations to systems [14]. Although there are some differences between the traditional and the mobile ad hoc network, intrusion detection technique, which was developed first in the wired network and has become a very important security solution for the wired network, has also gained some attentions from the researchers when they explore the security solution for the mobile ad hoc network.

b. Secure Routing Techniques in Mobile Ad Hoc Network

There are many kinds of attacks against the routing layer in the mobile ad hoc networks, some of which are more sophisticated and harder to detect than others, such as Wormhole attacks and Rush attacks.

VII. CONCLUSION

In this survey paper, we try to discuss the security issues in the mobile ad hoc networks. Due to the mobility and open media nature, the mobile ad hoc network suffers from all kinds of security risks such as denial-of-services, intrusion or even information disclosure. Therefore, as a result the security in mobile ad hoc network is much higher than in the traditional wired networks.

Firstly we have briefly introduced the basics of mobile ad hoc network; there is an increasing need for the network users to get connection with the world, which inspires the emergence of the mobile ad hoc network. As mobile ad hoc network has provide us much convenience, so there are also increasing security threats for the mobile ad hoc network which need to gain more attention.

We have also discussed some dangerous vulnerability in the mobile ad hoc networks. This basically caused by the characteristics of mobile ad hoc networks such as mobility, constantly changing topology and limited battery power. Due to these vulnerabilities made it necessary to find effective security solution to protect the mobile ad hoc network from security risks.

And then finally we introduce some current solutions for the mobile ad hoc networks. We have also discussed about the main attack types that affect the mobile ad hoc networks. At the end, we discuss several security techniques that can help to protect the mobile ad hoc networks from external and internal security threats.

During the survey, we also find some points that can be explored in the future such as intrusion detection techniques can get further improved.

VIII. REFERENCES

1. M. Weiser, The Computer for the Twenty-First Century, Scientific American, September 1991.
2. M.S. Corson, J.P. Maker, and J.H. Cernicione, Internet-based Mobile Ad Hoc Networking, IEEE Internet Computing, pages 63–70, July-August 1999.
3. Amitabh Mishra and Ketan M. Nadkarni, Security in Wireless Ad Hoc Networks, in Book The Handbook of Ad Hoc Wireless Networks (Chapter 30), CRC Press LLC, 2003.
4. Lidong Zhou and Zygmunt J. Hass, Securing Ad Hoc Networks, IEEE Networks Special Issue on Network Security, November/December 1999.
5. Data Integrity, from Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/Data_integrity.
6. Yongguang Zhang and Wenke Lee, Security in Mobile Ad-Hoc Networks, in Book Ad Hoc Networks Technologies and Protocols (Chapter 9), Springer, 2005.
7. P. Papadimitratos and Z. J. Hass, Secure Routing for Mobile Ad Hoc Networks, in Proceedings of SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS), San Antonio, TX, January 2002.
8. Y. Hu, A. Perrig and D. Johnson, Ariadne: A Secure On-demand Routing Protocol for Ad Hoc Networks, in Proceedings of ACM MOBICOM'02, 2002.
9. K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer, A Secure Routing Protocol for Ad Hoc Networks, in Proceedings of ICNP'02, 2002.
10. Y. Hu, D. Johnson, and A. Perrig, SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks, Ad Hoc Networks, 1 (1): 175–192, July 2003.
11. Y. Hu, A. Perrig and D. Johnson, Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks, in Proceedings of IEEE INFOCOM'03, 2003.
12. Y. Hu, A. Perrig and D. Johnson, Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols, in Proceedings of ACM MobiCom Workshop - WiSe'03, 2003.
13. J. R. Douceur, The Sybil Attack, in Proceedings of the 1st International Workshop on Peer-to-Peer Systems (IPTPS'02), pages 251–260, March 2002, LNCS 2429.
14. Intrusion-detection system, from Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/Intrusion detection_system.