IJCSE International Journal of Computer Science and Engineering Open Access
Survey Paper Volume-2, Issue-3 E-ISSN: 2347-2693

A Survey on Security Issue in Mobile Ad-Hoc Network and Solutions

Mayank Kumar[1*] and Tanya Singh[2]

[1*] *Amity Institute of Information Technology, Amity University, India, mkarya21@gmail.com*
[2] *Amity Institute of Information Technology, Amity University, India, tsingh2@amity.edu*

www.ijcseonline.org

Received: 08 Mar 2014 Revised: 14 Mar 2014 Accepted: 22 Mar 2014 Published: 31 Mar 2014

Abstract— Ad hoc networks are temporary networks connection established for a small session, self-configured and organized networks without any fixed infrastructure. In Ad hoc networks, topology is dynamic as nodes communicate the network "on the fly" for a special purpose (such as transferring data between one computer to another). A Mobile Ad hoc network (MANET) is a dynamically arrangement of wireless Mobile nodes, communicate directly or using intermediate nodes without any predefined infrastructures. In the absence of any predefined infrastructures in networks become vulnerable to number of attacks and high level security becomes a major issue. In this survey paper, we first discuss the introduction to Mobile Ad hoc network. The second section discusses weaknesses or vulnerabilities in Mobile Ad hoc network. The third section discusses the types of attack in Mobile Ad hoc network. The fourth section discusses the security goals of Mobile Ad hoc network. Finally the last section discusses the security solutions to prevent the attacks and provide a high level security to Mobile Ad hoc networks.

Index Term— Mobile Ad Hoc Networks, Attacks, Security, Solutions

I. INTRODUCTION

Nowadays, network technology has become very important aspect and has many influences on people's life such as exchanging information smoother and faster than before. The extensive growth of Mobile computing devices includes laptops, Mobiles and all types of digital devices are increasing very fast, has encouraged a revolutionary change in the computing world: Computing will not merely depend on the capability provided by the personal computers, and the concept of universal computing emerges and becomes one of the research booms in the computer science society [1]. There are different types of networks (such as Wi-Fi, APN, Wi-MAX) which helps people to transfer information and data between different devices all around the world. But unfortunately, some people are using these technologies to attack on devices. Therefore security has become major issue to stop attackers and keep the information safe and secure. A Mobile Ad hoc network (MANET) is a dynamically arrangement of wireless Mobile nodes, communicate directly or using intermediate nodes without any predefined infrastructures. This means that there are no fixed infrastructures and routers have ability to move anywhere without any restrictions. Each node of Mobile has a receiver and a transmitter. In other words, this new type of dynamically self organizing networks combines wireless communications with high degree node mobility [3]. In the universal computing environment, respective users utilizes, at the same time, many electronic platforms though which they can access all the required information whenever and wherever they may be [2]. More on, Mobile Ad hoc network nodes can communicate directly with other nodes which they are nearby in their transmission ranges, whereas nodes that are not in their transmission range use intermediate node(s) to communicate therefore this form of wireless networks can be distinguish as MANET. Mobile Ad hoc networks have different types of features as follows [4]:

Firstly, the main features of an Ad hoc network is that there are temporary and do not require any cabling, the communication only requires the Wireless connection between the devices.

Secondly, there is unfaithfulness of wireless link between the nodes. The Ad hoc networks are not faithful for the communication nodes because of limited intensity supply for the wireless nodes.

Thirdly, the rapidly changes in the routing topology due to continuous move and change in the position of nodes. This means that the nodes have the ability to move in or outside the transmission range of the nodes in Mobile Ad hoc network. [Figure 1] Shows Mobile Ad hoc network

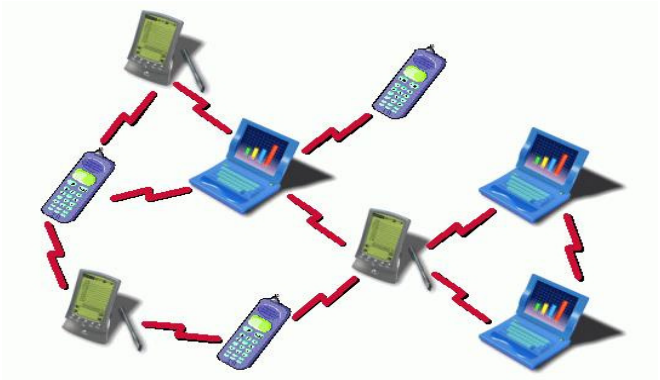

Figure 1: MANET [2]

Corresponding Author: *Mayank Kumar,*

IJCSE © 2014, IJCSE All Rights Reserved

Therefore, because of the features listed above, we need to pay attention to the security issue in the Mobile Ad hoc Network.

The rest of the paper is organized as follows: The second section discusses weaknesses or vulnerabilities in Mobile Ad hoc network. The third section discusses the types of attack in Mobile Ad hoc network. The fourth section discusses the security goals of Mobile Ad hoc network. Finally the last section discusses the security schemes to prevent the attacks and provide a high level security to Mobile Ad hoc networks.

II. VULNERABILITIES OF THE MOBILE AD HOC -NETWORKS

1. Insecure Nature

The Mobile Ad hoc network is insecure by its nature: There is no such restriction for nodes to joining, leaving and moving inside or outside of the network, thus the lack of security makes the Mobile Ad hoc network vulnerable to the attacks. The Mobile Ad hoc network becomes wide open as there is no line of defense such as firewall and gateway before they can perform malicious behavior to the targets [6].

2. Dynamic Topology

Mobile Ad hoc network nodes are independent: They can leave or join any network. As a result the topology changes regularly. It is hard to track the malicious behavior performed by a node in a network. Therefore, threats from these nodes inside the network are more dangerous than that the attacks from the outside attackers and these attacks are hard to detect.

3. Unavailability of Centralized Management

Mobile Ad hoc network do not have any centralized management facility such as a name server, which leads to some vulnerable problems. The unavailability of centralized management machines makes it indeed very hard to detect attacks because it is hard to monitor the traffic in a highly dynamic and large scale Mobile Ad hoc network [7]. This problem affects in turn breakdown and failure in transmitted data. There is no involvement of the nodes in any security operations. A shortage of this type cause directly all operations of Mobile Ad hoc network especially when there is any serious attack faced by any node [5][14][7].

4. Bounded Power Supply

The nodes in Mobile Ad Hoc Network rely fully on the battery as their power supply method, which is bounded kind of power supply. And so, any types of failure in Mobile Ad hoc network instantly cause many problems. But in contrast, the wired network does not need any power supply because it gets its power directly from the electronic power supplier. The first problem occurs is denial-of-service attacks [4]. The second problem is caused by some node suffering from the running off battery power, this behavior is literary a selfish behavior in Mobile Ad hoc network [8].

5. Changeable Scalability

In general wired network scale is predefined when designed and not change such during the use, but Mobile Ad hoc network scale is changing all the time because of mobility of the nodes in Mobile Ad hoc network. There is no method to predict number of nodes in Mobile Ad hoc network. This means that network needs scale up and down at each time in network.

III. ATTACK TYPES IN MOBILE AD HOC NETWORKS

There are numerous types of attacks in the Mobile Ad hoc network, which can be classified as the following two main types [6]:

A. External attacks, in which the attacker aims to propagate fake routing information, cause congestion or disturb nodes from providing services.

B. Internal attacks, in which the attacker wants to participate in the network activities and gain the normal access to the network, by some malicious acting to get the access to the network as a new node, or by directly communicating a current node and using it as a basis to conduct its malicious behaviors.

External attacks are similar to the regular attacks in the long established wired networks in that the attacker is in the closeness but not a trusted node in the network, therefore, this type of attack can be stopped and detected by the security methods such as authentication or firewall, which are relatively traditional security solutions. The security solutions of Mobile Ad hoc network should provide complete protection to the entire protocol stack: [Table 2] [19]

Layer	Security Issues
Application Layer	Detecting and preventing virus, worms, malicious codes, and application abuses
Transport Layer	Authenticating and securing end-to-end communications through data encryption
Network Layer	Protecting the ad hoc routing and forwarding protocols
Link Layer	Protecting the wireless MAC Protocol and providing link-layer security support
Physical Layer	Preventing signal jamming denial-of-service attacks

1. Eavesdropping Attacks

Eavesdropping is known as disclosure attacks, usually done by external or internal nodes and is passive. The attacker's goal of eavesdropping is to analyze broadcast messages and

© 2014, IJCSE All Rights Reserved

obtain some useful information about the network that is secret during the communication [9].

2. Denial of Service (DoS)
The second type of attack is denial of service; in this attackers try to attack at the availability of services of the entire Mobile Ad hoc network. The attackers use the battery exhaustion methods and the radio jamming to perform DoS attacks to the Mobile Ad hoc network.

3. Dropping Attacks
In Mobile Ad hoc network nodes those are malicious or selfish nodes deliberately drops all the packets that are not destined for them. In dropping attack, malicious nodes aim to disrupt the connection, whereas selfish nodes aim to preserve their resources. It reduces the network performance by causing data packets to be transmitted again, new routes to the destination is to be discovered.

4. Attacks against Routing
Routing is one of the most important part in Mobile Ad hoc network, it the one of the main targets of attackers. Attacks on routing protocols are classified as attacks on protocols and on packet forwarding or delivery [10] [11] [12] [13]. It is very difficult to validate message in constantly changing topology of the Mobile Ad hoc networks. There are some more sophisticated attacks on routing include Wormhole attacks, Rushing attacks and Sybil Attacks [14] [15] [16].

IV. SECURITY GOALS IN MOBILE AD HOC NETWORKS

Before we survey the Mobile Ad hoc network security solutions, first it is necessary to understand the goals on the basic to which we are able to understand that Mobile Ad hoc network is secure or not. First we have to survey that on what basis we want to secure Mobile Ad hoc network. There are several goals and criteria on the basic of which we can judge Mobile Ad hoc networks. Some of these are:

1. Availability
The first criterion is the availability of nodes. Each node should preserve its availability to provide all the services regardless its state of security. This security criterion is mainly challenged at the DoS attacks; this some selfish nodes make network services unavailable.

2. Integrity
When the messages are transferred integrity ensures the identity of the message, so integrity is very important criterion. Integrity depends on [9]:

I. Malicious altering
II. Accidental altering

Malicious altering means that the message can be removed, revised or replayed by attackers with malicious goals. Accidental altering means that the message is lost or its content is changed due to some failures such as transmission error in communication, hardware error or hard disk failure.

3. Confidentiality
Confidentiality is also an important criterion because it prevents the network from the unauthorized access [18]. The secret and confidential information are only accessible to authorized members.

4. Authenticity
Authenticity is mandatory to prove the identity of network users. It assures that users those are participating in communication are genuine and are not imitator.

5. Non-repudiation
Non-repudiation ensures that the receiver or sender cannot deny that have sent or receive fake message. This is helpful if we need to check the work of nodes, if a node found sending improper message means that the node is compromised.

6. Authorization
Authorization is a process of checking whether the user has authorized to access the network or not. It specifies the privileges and permissions and gives authority certificate to authorized user. Authorization is generally used to assign access rights to users at different levels.

V. SECURITY SOLUTIONS IN THE MOBILE AD HOC NETWORKS

The security issues are key concerned of Mobile Ad-hoc network can be solved by using symmetric key algorithms. The symmetric key can be shared between the sender and the receiver. It can be provided by the Key Distribution Center (KDC). This symmetric shared key can be used as an encryption as well as decryption. To understand this, let us look at figure 2 .When User A wants to send a message to User B, User A must encrypt the message by using the same symmetric key for User B. Later on User B will decrypt the message by using the same key. [17] [5].

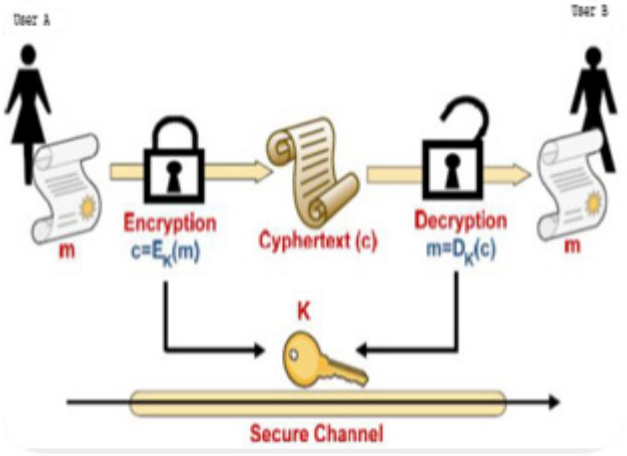

Figure 2 [5]

© 2014, IJCSE All Rights Reserved

By the symmetric key as a skill makes it better to be executed electronically. As the other, the symmetric algorithms can be found as non extensive when the symmetric key is used between more than two nodes .This multiple use of key make the security of node weaker and easy to breakdown. And as solution, it is required to use another technique which is the public key cartography.

Public key cryptography: there are two important keys in public key cryptography, pubic key and private key. The pubic key is usually provided among group of users while the private key is kept safe and secretly. This implies that no one apart from the authentic users knows about this key. Figure 3 [5]:

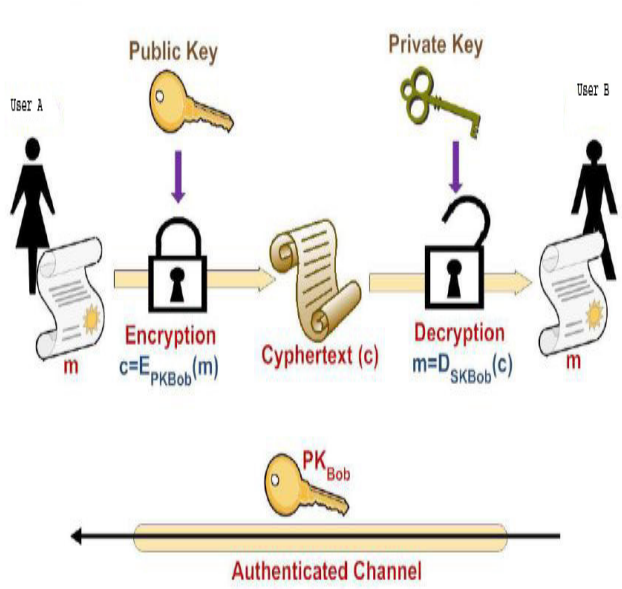

Figure 3 [5]

VI. CONCLUSION

In this survey paper, we try to survey the security issues in the mobile ad hoc networks, which may be a main issue to the operation of Mobile Ad hoc Network. Due to the insecure nature and dynamic topology, the mobile ad hoc networks are less secure to all types of security risks, such as information disclosure or denial of service. As a result, the security needs in the mobile ad hoc networks are much higher than those in the regular wired networks.

First we briefly introduced the basic features of the mobile ad hoc network. Then we discuss about the vulnerabilities of Mobile Ad hoc network that includes: Unreliability of nodes, dynamic topology, unavailability of centralized management facility, bounded power supply and changeable scalability. Then we discuss about the attacks on Mobile Ad hoc networks: Internal or external. Here we find that there are numerous kinds of attack that an attacker used to access the network and important information and messages. Then we review what could the security goals for a Mobile Ad hoc networks. The main security criterions we survey are: Availability, Integrity, Confidentiality, Authenticity, Nonrepudiation and Authorization. Then we discuss two main security solutions algorithms: symmetric key algorithms and Public key cryptography. We discuss that how we can make our network secure from unauthorized access and other issues. During the survey, we also find some points that can be further explored in future such as Intrusion Detection Technique (IDT) a security schemes in Mobile Ad hoc networks and we further improve security solutions in Mobile Ad hoc Networks. We will try to explore deeper in this research area.

REFERENCE

[1]. Marco Conti, Body, Personal and Local Ad Hoc Wireless Networks, in Book The Handbook of Ad Hoc Wireless Networks (Chapter 1), CRC Press LLC, 2003.
[2]. M. Weiser, The Computer for the Twenty-First Century, Scientific American, September1991.
[3]. [3] 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.
[4]. 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.
[5]. Lidong Zhou and Zygmunt J. Hass, Securing Ad Hoc Networks, IEEE Networks Special Issue on Network Security, November/December 1999.
[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]. Panagiotis Papadimitraos and Zygmunt J. Hass, Securing Mobile Ad Hoc Networks, in Book The Handbook of Ad Hoc Wireless Networks (Chapter 31), CRC Press LLC, 2003.
[8]. Yi-an Huang and Wenke Lee, A Cooperative Intrusion Detection System for Ad Hoc Networks, in Proceedings of the 1st ACM Workshop on Security of Ad hoc and Sensor Networks, Fairfax, Virginia, 2003, pp. 135 – 147.
[9]. Data Integrity, from Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/Data_integrity.
[10]. 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.
[11]. Y. Hu, A. Perrig and D. Johnson, Ariadne: A Secure On-demand Routing Protocol for Ad Hoc Networks, in Proc. of ACM MOBICOM'02, 2002.
[12]. 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.
[13]. 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.
[14]. 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.
[15]. Y. Hu, A. Perrig and D. Johnson, Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols,

 © 2014, IJCSE All Rights Reserved

in Proceedings of ACM MobiCom Workshop - WiSe'03, 2003.

[16]. 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.

[17]. Intrusion-detection system, from Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/Intrusion-detection_system.

[18]. Y. Zhang and W. Lee, Intrusion Detection in Wireless Ad-hoc Networks, in Proceedings of the 6th International Conference on Mobile Computing and Networking (MobiCom 2000), pages 275–283, Boston, Massachusetts, August 2000.

[19]. Jim Parker, Anand Patwardhan, and Anupam Joshi, Detecting Wireless Misbehavior through Cross-layer Analysis, in Proceedings of the IEEE Consumer Communications and Networking Conference Special Sessions (CCNC'2006), Las Vegas, Nevada, 2006.

© 2014, IJCSE All Rights Reserved