Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 5, May 2014, pg.1022 – 1024

RESEARCH ARTICLE

Security Issues in Mobile Ad Hoc Networks

Mali Basaveshwar Laxman
Scholar of Singhania University, India
Basu_mali@rediffmail.com

Abstract— *In this paper, we discuss security issues and their current solutions in the mobile ad hoc network. Owe to the vulnerable nature of the mobile ad hoc network, there are numerous security threats that disturb the development of it. We first analyse the main vulnerabilities in the mobile ad hoc networks, which have made it much easier to suffer from attacks than the traditional wired network. Then we discuss the security criteria of the mobile ad hoc network and present the main attack types that exist in it. Finally we survey the current security solutions for the mobile ad hoc network.*

Keywords—***Mobile Ad Hoc Network, Security, Intrusion Detection, Secure Routing***

I. INTRODUCTION

This In recent years, the explosive growth of mobile computing devices, which mainly include laptops, personal digital assistants (PDAs) and handheld digital devices, has impelled a revolutionary change in the computing world: computing will not merely rely on the capability provided by the personal computers, and the concept of ubiquitous computing emerges and becomes one of the research hotspots in the computer science society [1]. In the ubiquitous computing environment, individual users utilize, at the same time, several electronic platforms through which they can access all the required information whenever and wherever they may be [2]. The nature of the ubiquitous computing has made it necessary to adopt wireless network as the interconnection method: it is not possible for the ubiquitous devices to get wired network link whenever and wherever they need to connect with other ubiquitous devices. The Mobile Ad Hoc Network is one of the wireless networks that have attracted most concentrations from many researchers.

A Mobile Ad hoc NETwork (MANET) is a system of wireless mobile nodes that dynamically self-organize in arbitrary and temporary network topologies. People and vehicles can thus be internetworked in areas without a pre-existing communication infrastructure or when the use of such infrastructure requires wireless extension [3]. In the mobile ad hoc network, nodes can directly communicate with all the other nodes within their radio ranges; whereas nodes that 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, therefore this kind of wireless network can be viewed as mobile ad hoc network.

The mobile ad hoc network has the following typical features [4]:

1. Unreliability of wireless links between nodes. Because of the limited energy supply for the wireless nodes and the mobility of the nodes, the wireless links between mobile nodes in the ad hoc network are not consistent for the communication participants.
2. Constantly changing topology. Due to the continuous motion of nodes, the topology of the mobile ad hoc network changes constantly: the nodes can continuously 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.

3. Lack of incorporation of security features in statically configured wireless routing protocol not meant for ad hoc environments. Because the topology of the ad hoc networks is changing constantly, it is necessary for each pair of adjacent nodes to incorporate in the routing issue so as to prevent some kind of potential attacks that try to make use of vulnerabilities in the statically configured routing protocol.
4. Because of the features listed above, the mobile ad hoc networks are more prone to suffer from the malicious behaviours than the traditional wired networks. Therefore, we need to pay more attention to the security issues in the mobile ad hoc networks.

II. VULNERABILITIES OF THE MOBILE AD HOC NETWORKS

Because mobile ad hoc networks have far more vulnerabilities than the traditional wired networks, security is much more difficult to maintain in the mobile ad hoc network than in the wired network. In this section, we discuss the various vulnerabilities that exist in the mobile ad hoc networks.

A. *Lack of Secure Boundaries*

Lack of secure boundaries makes the mobile ad hoc network susceptible to the attacks. The mobile ad hoc network suffers from all-weather attacks, which can come from any node that is in the radio range of any node in the network, at any time, and target to any other node(s) in the network. To make matters worse, there are various link attacks that can jeopardize the mobile ad hoc network, which make it even harder for the nodes in the network to resist the attacks. The attacks mainly include passive eavesdropping, active interfering and leakage of secret information, data tampering, message replay, message contamination, and denial of service [4].

A. Threats from Compromised nodes Inside the Network

In the previous subsection, we mainly discuss the vulnerability that there is no clear secure boundaries in the mobile ad hoc network, which may cause the occurrences of various link attacks. These link attacks place their emphasis on the links between the nodes, and try to perform some malicious behaviors to make destruction to the links. However, there are some other attacks that aim to gain the control over the nodes themselves by some unrighteous means and then use the compromised nodes to execute further malicious actions. This vulnerability can be viewed as the threats that come from the compromised nodes inside the network.

B. Lack of Centralized Management Facility

Ad hoc networks do not have a centralized piece of management machinery such as a name server, which lead to some vulnerable problems.

C. Scalability

Finally, we need to address the scalability problem when we discuss the vulnerabilities in the mobile ad hoc network [4]. Unlike the traditional wired network in that its scale is generally predefined when it is designed and will not change much during the use, the scale of the ad hoc network keeps changing all the time: because of the mobility of the nodes in the mobile ad hoc network, you can hardly predict how many nodes there will be in the network in the future. As a result, the protocols and services that are applied to the ad hoc network such as routing protocol and key management service should be compatible to the continuously changing scale of the ad hoc network, which may range from decades of nodes to hundreds of nodes, or even thousands of nodes. In other words, these protocols and services need to scale up and down efficiently.

III. SECURITY SOLUTIONS TO THE MOBILE AD HOC NETWORKS

In this section, we survey some security schemes that can be useful to protect the mobile ad hoc network from malicious behaviours.

A. Security Criteria

Before we survey the solutions that can help secure the mobile ad hoc network, we think it necessary to find out how we can judge if a mobile ad hoc network is secure or not, or in other words, what should be covered in the security criteria for the mobile ad hoc network when we want to inspect the security state of the mobile ad hoc network. In the following, we briefly introduce the widely-used criteria to evaluate if the mobile ad hoc network is secure.

1. *Availability*
   The term Availability means that a node should maintain its ability to provide all the designed services regardless of the security state of it [4]. This security criterion is challenged mainly during the denial-of-service attacks, in which all the nodes in the network can be the attack target and thus some selfish nodes make some of the network services unavailable, such as the routing protocol or the key management service [5].
2. *Integrity*
   Integrity guarantees the identity of the messages when they are transmitted. Integrity can be compromised mainly in two ways [9]:
   I. Malicious altering
   II. Accidental altering
3. *Confidentiality*
   Confidentiality means that certain information is only accessible to those who have been authorized to access it. In other words, in order to maintain the confidentiality of some confidential information, we need to keep them secret from all entities that do not have the privilege to access them

3.2 Attack Types in Mobile Ad Hoc Networks:

There are numerous kinds of attacks in the mobile ad hoc network, almost all of which can be classified as the following two types [6]:

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

2. Internal attacks, in which the adversary wants to gain the normal access to the network and participate the network activities, either by some malicious impersonation to get the access to the network as a new node, or by directly compromising a current node and using it as a basis to conduct its malicious behaviours.

IV. CONCLUSIONS

In this survey paper, we try to inspect the security issues in the mobile ad hoc networks, which may be a main disturbance to the operation of it. Due to the mobility and open media nature, the mobile ad hoc networks are much more prone to all kind of security risks, such as information disclosure, intrusion, or even denial of service. As a result, the security needs in the mobile ad hoc networks are much higher than those in the traditional wired networks.

REFERENCES

[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*, September 1991.

[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.

