ISSN:0975-9646

Survey on Security Issues in Mobile Ad Hoc Networks

Devesh Kumar Pal, Dr. Pallavi Murghai Goel

School of Computing Science
Galgotias University[1]
Greater Noida, India

***Abstract*- In this paper, we discuss security issues and their current solutions in the mobile ad hoc network. Ad hoc networks are a new wireless network for mobile hosts. Owe to the vulnerable nature of the mobile ad hoc network, there are many security threats that effected the development of wireless network. We evaluate the accessible in the mobile ad hoc networks and find out attacks than the conventional wired node to node connected network. Then we discuss the current security criteria and main attack types in the mobile ad hoc network. Finally we evaluate the present security solutions in mobile ad hoc network.**

***Keywords*- MANET, vulnerabilities, Security, solution, Attacks, Routing.**

I. INTRODUCTION

In the modern era, we have the mobile computing devices, which devices are interconnected to various other wireless network, has the large change in the computing world: computing will not merely rely on the capability provided by the personal computers, and the concept of universal computing issue and becomes one of the research host in the computer science society [1]. In the universal computing environment, particular users utilize, at the same time, several electronic platforms are connected and communicated and access all the required information through the wireless network [2]. The nature of the universal computing has kept wireless network as the interconnection method: it is not possible for the global devices to get wired network link whenever and wherever they need to connect with other global devices. The Mobile Ad Hoc Network is one of the wireless networks that have attracted most centralization from many researchers.

A mobile ad hoc network (MANET) is a wireless mobile node that frequently organizes in personal and temporary network in different way. In the mobile ad hoc network, nodes can easily communicate with all the other nodes within their frequency ranges [3].

Changeableness of wireless connections between nodes. Because the limited energy provide for the wireless nodes and the mobility of the nodes, the wireless connection between mobile nodes in the ad hoc network are not regular for the communication participants. The nodes can regularly move into and out of the frequency range of the other nodes in the ad hoc network, and the routing information will be converting all the time because of the action of the nodes.

Lack of incorporation of security features in statically configured wireless routing protocol not meant for ad hoc environments. Because the interconnection of the ad hoc networks is changing regularly, it is compulsory for each pair of border 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.

Because of the features listed above, the mobile ad hoc networks are suffered from the spiteful behaviors than the traditional wired connection networks. Therefore, we want to pay more attention to the security issues in the mobile ad hoc networks.

The rest of the paper is organized as follows: In Section II, we discuss the main vulnerabilities that make the mobile ad hoc networks not secure. In Section III, we analyze the current security solutions for the mobile ad hoc networks and analyze the feasibility of them. In Section IV, we discuss the conclusion for the paper and point out some possible works in the future.

II. VULNERABILITIES OF THE MOBILE AD HOC NETWORKS

Because mobile ad hoc networks have far more weakness than the traditional wired connection networks, security is a type of difficult to maintain in the mobile ad hoc network than in the wired connection network. In this section, we discuss the different type weakness that exists in the mobile ad hoc networks.

A. Lack of adjacent node

The meaning of this vulnerability is clear: there is not such a clear adjacent in the mobile ad hoc network, which can be compared with the secure connection of defense in the conventional wired network. This vulnerability arise from the society of the mobile ad hoc network: frequently to connect, leave and move content the network [6]. However, in the mobile ad hoc network, there is no need for any clear physical access to visit the network: once the adversary is in the frequency range of any other nodes in the mobile ad hoc network, it can interconnect with those nodes in its range and thus connect the network automatically.

Lack of adjacent node makes the mobile ad hoc network prone to the attacks. The mobile ad hoc network suffers from all-climates attacks, which can come from any node that is in the frequency range of many nodes in the network, many time, and target to various nodes in the network. To make matters damage, there are various link attacks that can destroy the mobile ad hoc network, which

prepare for the nodes in the network to check the attacks. The attacks mainly include active interfering, passive bug, leakage the information, data tampering, message replay, message pollution, and rejected services [4].

B. ***Lack of Centralized Management Facility***

Mobile ad hoc network doesn't have a centralized monitor server. Firstly the absence of management makes the detection of attacks hardly because it is not easy to monitor the traffic in a highly dynamic and large scale ad-hoc network [7]. Lack of centralized management will block trust management for nodes.

Second, shortage of centralized management machinery will block the secure management for the nodes in the ad hoc network [4].

Third, some algorithms in the mobile ad hoc network rely on the cooperative participation of all nodes and the infrastructure. Because there is no centralized rule provide for the decision-making in mobile ad hoc network, if it is decentralized, the competitor can make use of this vulnerability and perform some attacks that can break the cooperative algorithm [6].

C. ***Restricted Power Supply***

It is common that the nodes in the ad hoc network will reply on battery as their power supply method.

The first problem that may be caused by the restricted power supply is rejection-of-service attacks [4]. Since the competitor knows that the target node is battery-restricted. the battery power of the target node will be disabled by these usefulness tasks, and the target node will be out of order to all the resume service requests since it has execute out of power back up. It is keep the cluster-based intrusion detection method let us consider an example [8].

A cluster of nearest MANET nodes can randomly and truly elect a monitoring node that will focus on the abnormal behaviors in the network traffic for the entire cluster.

D. ***Scalability***

In this paper scalability is the most important problem when we discuss the vulnerabilities in the mobile ad hoc network [4]. unrelated the conventional wired network in that its scale is generally predefined when it is described and will not change much during the use, the scale of the ad hoc network constantly changes with the time: because of the mobility of the nodes in the mobile ad hoc network, you can difficulty predict how many nodes there will be in the network in the future.

III. SECURITY SOLUTIONS TO THE MOBILE AD HOC NETWORKS

We have observed several vulnerabilities that capability makes the mobile ad hoc networks unsure in the previous section. However, it is achieved greatest goal to secure the mobile ad hoc network if we merely know the existing vulnerabilities in it. As a result, we need to obtain some security solutions to the mobile ad hoc network. In this section, we survey some security schemes that can be useful to protect the mobile ad hoc network from spiteful behaviors.

A. ***Security Criteria***

Previous we discuss the solutions that can help sure and safe the mobile ad hoc network, we think it is mandatory to find out how we can judge if a mobile ad hoc network is safe 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 given sections, we briefly discuss the widely-used criteria to calculate if the mobile ad hoc network is confident.

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 faced mainly during the rejection-of-service attacks, in which all the nodes in the network cannot be available the attack target and thus some greedy nodes make some of the network services , such as the routing protocol or other key management service [5].

2. Integrity

Integrity defines the identity of the messages when they are forwarded. Integrity can be compromised mainly in two ways [9]:

Spiteful altering
Accidental altering

A message can be removed, resume or revised by an competitor with spiteful goal, which is regarded as spiteful altering; on the contradictory, if the message is discard or its content is changed due to some benign failures, which may be sending errors in communication or hardware errors such as hard disk failure, then it is categorized as accidental altering.

3. Confidentiality

Confidentiality define the certain information is only accessible by authorized users. In other words, in order to maintain the confidentiality of some confidential information, we need to keep them privacy from all entities that do not have the freedom to access them.

4. Authenticity

Authenticity is essentially assurance that participants in communication are genuine and not impersonators [4]. It is necessary for the communication participants to prove their identities as what they have claimed using some techniques so as to ensure the authenticity. If there is no confirmed mechanism, the competitor could masquerade a liberal node and thus get access to confidential sources, or even generate some fake messages to disturb the network operations.

5. No repudiation

No repudiation confirmed that the sender and the receiver of a message cannot reject that they have ever sent or received such a message. This is useful mainly when we need to victimized if a node with some abnormal behavior is compromised or not: if a node recognizes that the message it has received is incorrect, it can then use the incorrect message as an corroboration to notify other nodes

that the node sending out the impolite message should have been compromised.

6. Authorization

Authorization define an entity is issued a license, which specifies the advantage and permissions it has and cannot be prevented, by the licenses authority. Authorization is generally used to assign different access gadget to different level of users. For instance, we need to confirm that network management function is only accessible by the network management. Therefore there should be an authorization process before the network management accesses the network management functions.

7. Anonymity

Anonymity means that all the information that can be used to define the holder or the current user of the node should default be kept confidentially and not be interrupted by the node itself or the system software. This standard is closely related to confidentially secure, in which we should try to cover the privacy of the nodes from subjective disclosure to any other entities.

B. ***Attack Types in Mobile Ad Hoc Networks***

There are several kinds of attacks in the mobile ad hoc network, there are classified the following two types [5]:

(i). External attacks, in which the attacker target to reason of congestion, generate entrusted routing information or disturb nodes from providing services.

(ii). Internal attacks, in which the competitor wants to collect the normal access to the network and attempt the network activities, either by some spiteful imitation to get the access to the network as a new node, or easily compromising with current node and using it as a basis to conduct its spiteful behaviors.

1. Denial of Service (DoS)

The first attack is denial of service, which aims to sure the availability of certain node or even the services of the entire ad hoc networks. In the conventional wired network, the DoS attacks are taken out by some kind of network traffic to the target so as to disable the processing power of the target and make the services provided by the target become unavailable. The mobile ad hoc networks are more vulnerable than the wired networks because of the interference-prone radio channel and the limited battery power. During practice, the attackers Often use the radio jamming and battery consumption methods to conduct DoS attacks to the mobile ad hoc networks, which well correspond to the two vulnerabilities.

2. Impersonation

Impersonation attack is a severe threat to the security of mobile ad hoc network [4]. As we can see, if there is not such a proper authentication mechanism among the nodes, the contestant can take some nodes in the network and make them look like benign nodes. In this field, the adjusted nodes can join the network as the normal nodes and begin to conduct the spiteful behaviors such as propagate fake routing information and gain inappropriate priority to access some confidential information.

3. Eavesdropping

Eavesdropping is another type of attack that usually occurs in the mobile ad hoc networks. The aim of eavesdropping is to achieve some confidential information that should be kept secret during the conversation. The confidential information may include the area, public key, private key or even passwords of the nodes. Because these data's are very important to the security field of the nodes, they must be kept away from the illegal access.

4. Attacks against Routing

Routing is one of the most important services in the network; therefore it is also one of the main targets to which attackers conduct their spiteful nature. In the mobile ad hoc networks, attacks against routing are simply classified into two categories: attacks on routing protocols and attacks on packet forwarding/delivery [6]. Attacks on routing protocols aim to block the motion of the routing information to the victim even if there are some routes from the victim to other targets. Attacks on packet forwarding try to interrupt the packet delivery along a predefined path. The first main effects brought by the attacks against routing protocols include network division, routing loop, resource removal and route hijack [6]. The second category of attacks against routing is attacks on packet forwarding/delivery, which are not easy to detect and prevented [6]. There are two main attack strategies in this type: one is selfishness, in which the spiteful node selectively drops route messages that are assumed to forward in order to save it own battery power; the other is dismissal-of-service, in which the competitor sends out overwhelming network traffic to the victim to emit its battery power.

C. ***Secure Routing Techniques in Mobile Ad Hoc Network***

As we have discussed in Section III.B.4. there are different kinds of attacks against the routing layer in the mobile ad hoc networks, some of which are more discreetly and harder to detect than others, such as two attack like that Wormhole attacks and Rush attacks.

1. Defense Method against Wormhole Attacks in Mobile Ad Hoc Networks

Wormhole attack is a threatening attack again routing protocols for the mobile ad hoc networks [10] [12]. In the wormhole attack, an attacker records packets (or bits) at one location in the network, tunnels them (possibly selectively) to different location, and resume them there into the network. The resume of the information will make biggest confusion to the routing issue in mobile ad hoc network because the nodes that get the resumed packets cannot differ it from the real routing packets.

2. Defense Mechanism against Rushing Attacks in Mobile Ad Hoc Networks

Rushing attack is a new attack that results in denial-of-service when used against all previous on-demand ad hoc network routing protocols [11]. This attack is also particularly damaging because it can be performed by a relatively weak attacker. The implementation details of rushing attacks are shown in the Figure 4.

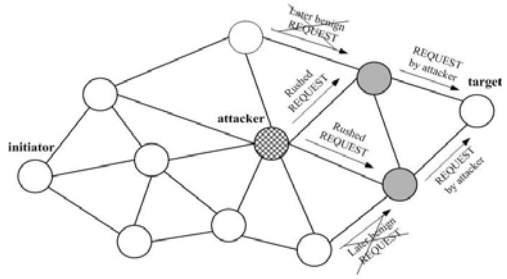

Figure 4. Rush Attack in the Example Ad Hoc Network

*D. **Security Solutions in the Mobile Ad Hoc Networks: Summary***

In this section, we survey the security solutions in the mobile ad hoc networks. First we analyze the vulnerabilities in the mobile ad hoc network and analyze the main security criteria for the mobile ad hoc networks, which should be finding the solutions to the security issues in the mobile ad hoc networks. We noted the various attack types that mainly threaten the mobile ad hoc networks. According to these attack types, we survey secure routing techniques that can partly solve the security problems in the mobile ad hoc networks.

IV. CONCLUSION

In this paper, we analyze try to inspect the security issues in the mobile ad hoc networks, which may be a main disturbance to the operation of it.

We discuss some typical and dangerous vulnerability in the mobile ad hoc networks; these are caused by the characteristics of the mobile ad hoc networks such as mobility, scalability, lack of centralized management facility and limited battery power.

Finally we introduce the current security solutions for the mobile ad hoc networks. We start with the discussion on the security criteria in mobile ad hoc network, which acts as a guidance to the security-related research works in this area and we discuss about the secure routing technique.

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] 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.

[6] Lidong Zhou and Zygmunt J. Hass, Securing Ad Hoc Networks, IEEE Networks Special Issue on Network Security, November/December 1999.

[7] Data Integrity, from Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/Data_integrity.

[8] 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.

[9] 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.

[10] Y. Hu, A. Perrig and D. Johnson, Wormhole Attacks in Wireless Networks, IEEE Journal on Selected Areas in Communications, Vol. 24, No. 2, February 2006.

[11] Yongguang Zhang and Wenke Lee, Security in Mobile Ad-Hoc Networks, in Book Ad Hoc Networks Technologies and Protocols (Chapter 9), Springer, 2005.

[12] 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.