A Study on MAC Address Spoofing Attack Detection Structure in Wireless Sensor Network Environment

Sungmo Jung[1], Jong Hyun Kim[2], and Seoksoo Kim[1,*]

[1] Department of Multimedia, Hannam University, Daejeon-city, Korea
[2] Eectronics and Telecommunications Research Institute, Daejeon-city, Korea
sungmoj@gmail.com, jhk@etri.re.kr, sskim0123@naver.com

Abstract. Wireless sensor network applies authentication by registering/managing user IP and MAC addresses. However, the existing methods are vulnerable to MAC address spoofing, in which a malicious user changes a client's MAC address into his own, calling for a new detection method. Therefore, this paper provides a method of detecting MAC address spoofing attacks in real-time by collecting wireless traffic data through AirSensor/AP- and using a MAC Address Index table in TMS.

Keywords: Wireless Sensor Network, MAC Address Spoofing, Spoofing Attack Detection.

1 Introduction

A wired network can be used only when a user receives an IP address and physical port connection from a network administrator. The network administrator applies various authentication and security systems, using the NAC(Network Admission Control) system[1] in order to register/manage user IP and MAC(Media Access Control) addresses[2]. A wired network environment provides DHCP(Dynamic Host Configuration Protocol)[3]–based IP for user convenience. Thus, it employs MAC address registration/authentication systems so as to effectively detect malicious users.

However, the existing wired network environment, using MAC address registration/ authentication methods based on the NAC system, is vulnerable to MAC Spoofing attacks[4] and, particularly, a MAC address can be easily changed in most client systems.

The number of people using a wireless network is sharply increasing, for it requires no physical port connection. But such an environment allows malicious users to easily access the network, posing more serious threats compared to wired networks.

Although a large number of research has been done in order to detect MAC address spoofing attacks in wireless networks, the existing methods including PTD(Personal Trusted Device)-based wireless network management[5] and wireless MAC address spoofing detection[6] are still not sufficient to discover such attacks in advance.

Therefore, this paper provides a method of detecting MAC address spoofing attacks in real-time by collecting wireless traffic data through AirSensor/AP- and using a MAC Address Index table in TMS(Threat Management System).

[*] Corresponding author.

T.-h. Kim et al. (Eds.): ACN 2011, CCIS 199, pp. 31–35, 2011.

2 Related Researches

2.1 MAC Spoofing Attack Method

There is a unique address in the NIC(Network Interface Card), which is called a hardware or MAC address. A MAC address, assigned to a network card manufacturer, is composed of 48 bits. The number is assigned to venders by IEEE[7] and cannot be duplicated. MAC address spoofing attacks avoid NIC-based authentication by changing MAC addresses.

The following is the general scenario of MAC address spoofing attacks.

① A malicious user scans MAC addresses of surrounding clients using wireless networks
② He changes one of the scanned MAC addresses into his MAC address
③ He blocks a client’s wireless network connection through De-Auth[8] attacks
④ He attempts communication with AP using the fake MAC address
⑤ He uses the fake MAC address in order to receive internal network authentication
⑥ He produces SoftAP[9] using other wireless network cards
⑦ A client attempts communication through SoftAP and the malicious user attempts sniffing of the client’s data

The network authentication technology using MAC addresses are most used in private or internal networks. However, the existing wireless network environment is vulnerable to MAC address spoofing attacks, calling for a new detection method.

2.2 WSLAN Vulnerability Diagnostic Tool

There is quite a large number of methods to attack wireless networks but not sufficient number of detection methods. Therefore, wireless vulnerability diagnostic tools use systems that make virtual wireless network attacks in order to find out which part of the network is particularly vulnerable. This paper also uses such system so as to diagnose vulnerability and provide solutions. Diagnostic tools can discover varied vulnerability to EAP START DoS, EAP FAILURE DoS, EAP LogOFF DoS, Fake AP, and so on[11]. The following figure shows how the tools collect scan data for surrounding APs and carry out virtual attacks.

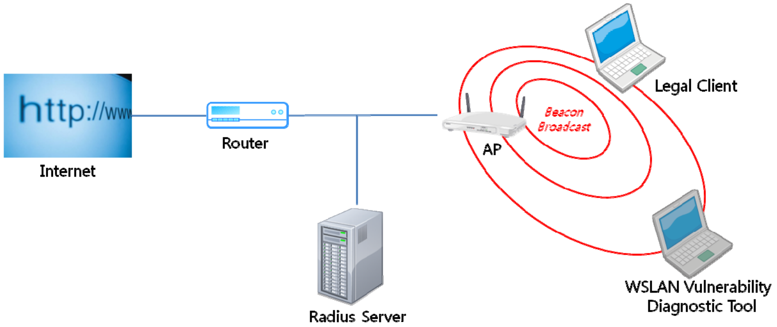

Fig. 1. Structure of WSLAN Vulnerability Diagnostic Tool