Access Point 기반 무선 네트워크 환경에서의 MAC Address Spoofing 공격 탐지 및 차단 기법

MAC Address Spoofing Attack Detection and Prevention Mechanism with Access Point based IEEE 802.11 Wireless Network

조 제 경* 이 형 우**
Jo, Je-Gyeong Lee, Hyung-Woo

요 약

유무선 네트워크 환경에서는 사용자 I P 주소와 클라이언트 단말의 MAC 주소 정보를 등록/관리하여 인증 등을 수행하고 있다. 하지만 기존의 MAC 주소 등록/관리 방식은 공격자 자신의 MAC 주소 값을 클라이언트의 MAC 주소 값으로 변경하는 MAC Spoofing 공격에 취약하기 때문에 이에 대한 대처 방안이 제시되어야 한다. 무선 네트워크 환경에서 MAC Spoofing 공격을 탐지하기 위해 기존에 제시된 기법은 패킷의 시퀀스 번호 등에 기초하여 MAC 주소 값의 변경 등을 순차적으로 판별하는 기법이었으나 무선 공격에 대한 탐지/차단 기능을 제공하지 못하고 있다. 이에 본 연구에서는 무선 네트워크에서 AirSensor와 AP를 기반으로 무선 트래픽에 대한 정보를 수집하고 W-TMS에 구축된 MAC Address Lookup 테이블을 통해 실시간으로 MAC Spoofing 공격을 탐지하며, 다시 AP를 통해 해당 공격 트래픽을 차단할 수 있는 알고리즘을 제시하였다. 본 연구에서 제시한 탐지 및 차단 알고리즘은 성능평가 결과 MAC Spoofing 공격 시도에 대해서 고성능의 탐지/차단 기능을 수행하였으며 최소한의 무선 트래픽 전송 지연만으로도 무선 MAC Spoofing 공격에 대해 실시간으로 대응한다는 것을 확인할 수 있었다.

Abstract

An authentication procedure on wired and wireless network will be done based on the registration and management process storing both the user's IP address and client device's MAC address information. However, existent MAC address registration/administration mechanisms were weak in MAC Spoofing attack as the attacker can change his/her own MAC address to client's MAC address. Therefore, an advanced mechanism should be proposed to protect the MAC address spoofing attack. But, existing techniques sequentially compare a sequence number on packet with previous one to distinguish the alteration and modification of MAC address. However, they are not sufficient to actively detect and protect the wireless MAC spoofing attack. In this paper, both AirSensor and AP are used in wireless network for collecting the MAC address on wireless packets. And then proposed module is used for detecting and protecting MAC spoofing attack in real time based on MAC Address Lookup table. The proposed mechanism provides enhanced detection/protection performance and it also provides a real time correspondence mechanism on wireless MAC spoofing attack with minimum delay.

☞ KEYWORD : 키워드 추가: SIP, VoIP, 공격탐지, 가상 프록시, 상태 전이도, 메시지 폭주 공격

1. 서 론

유선 네트워크는 IP 주소의 할당과 물리적인 연결포트를 네트워크 관리자로부터 제공받아야만 사용이 가능하다. 또한 유선 네트워크 환경에서의 보안 관리를 위해 네트워크 관리자는 NAC

* 준 회 원 : 한신대학교 컴퓨터정보대학원 석사과정
aiking@hs.ac.kr (제 1저자)
** 종신회원 : 한신대학교 컴퓨터공학부 부교수
hwlee@hs.ac.kr (제 2저자, 교신저자)
[2008/02/1 투고 - 2008/02/16 심사 - 2008/05/02 심사완료]
☆ 본 연구는 지식경제부 및 정보통신연구진흥원의 대학IT연구센터 지원사업의 연구결과로 수행되었음"(IITA-2008-C1090-0801-0016)"

(Network Access Control)[1] 시스템 등을 이용하여 사용자의 IP 주소와 MAC(Media Access Control) 주소 정보를 등록/관리하는 등 다양한 인증 및 보안관리 시스템을 적용하고 있다. 유선 네트워크 환경에서는 사용자의 편의를 위해서 DHCP 기반 유동 IP를 제공한다. 따라서 유선 네트워크 환경에서는 악의적인 공격자를 효율적으로 차단/관리하기 위한 기술로 MAC 주소 정보에 대한 인증/관리 기능을 제공하고 있다.

하지만 기존의 NAC 기반 MAC 주소 인증/관리 방식을 이용한 유선 네트워크 환경은 MAC Address Spoofing(이하 MAC Spoofing) 공격에 취약하며 특히 대부분의 클라이언트 시스템에서는 손쉽게 MAC 주소를 수정할 수 있도록 되어 있어 MAC Spoofing에 대한 대처 방안이 시급히 마련되어야 한다.

무선 네트워크는 물리적 연결 포트의 제한이 없다는 특성으로 인하여 사용자가 급증하고 있으나, 기존의 유선 네트워크 보다 더욱더 심각한 문제점을 갖는다. 첫째, Open Authentication 방식의 Access Point를 통해 악의적인 공격자는 손쉽게 내부 네트워크에 접근할 수 있다. 둘째, 악의적인 공격자는 무선 클라이언트에 대한 MAC Spoofing 방식을 통하여 내부 네트워크에 손쉽게 접속할 수가 있다. 셋째, 악의적 공격자는 Soft AP 방식의 Rogue Access Point를 설치하여 일반 사용자에 대한 무선 네트워크 접속 기능을 제공 할 뿐만 아니라 무선 트래픽에 대한 스니핑 공격과 세션 하이재킹 공격 등을 수행할 수 있다.

이에 대응하기 위해 유선 네트워크와 마찬가지로 무선 네트워크 관리자 역시 공격자에 대한 Access Point의 접속을 제한하고 있으나, 기존의 무선 네트워크 기반 NAC 시스템에서는 MAC Spoofing 공격에 대한 탐지 및 차단 기능이 제공되어 있지 않다.

무선 네트워크 환경에서 MAC Spoofing 공격을 탐지하기 위하여 많은 연구가 진행이 되고 있으나 대부분 무선 공격에 대한 탐지를 중심으로 연구가 진행되고 있다. PTD 기반 무선 네트워크 관리 기법[2]에서는 ID, IP 주소 및 MAC 주소를 사전에 등록해 놓고 인증 절차를 통해 무선 네트워크에 대한 접근을 제한하는 방식이다. 하지만 이는 MAC Spoofing 공격에 대해 취약하며 사용자의 편리성이 배제되었다. 무선랜 취약점 진단도구[3]에서는 무선 네트워크에서의 취약점만을 분석하는 방식이며 공격에 대한 탐지 및 차단 기능을 제공하지 못하고 있다. Wireless MAC Spoofing Detect 기법[4]은 기존의 무선 공격 툴인 Wellenreiter, FakeAP, AirJack 등을 이용한 MAC Spoofing 공격 시퀀스를 분석하고 탐지하는 기능을 제공하지만 일반적인 MAC Spoofing 공격에 대해서는 탐지하지 못하며 차단기능을 제공하지 못하고 있다.

따라서 본 연구에서는 무선 네트워크 환경에서 악의적인 공격자에 의한 MAC Spoofing 공격 탐지 및 차단을 위해 AirSensor/AP 기반 무선 트래픽 캡처 및 무선 클라이언트 정보 전송 알고리즘/모듈을 개발하였고, W-TMS(Wireless-Threat Management System)[5]에서는 AirSensor/AP로부터 전달 받은 정보를 이용하여 MAC Spoofing 공격을 탐지/차단하는 알고리즘을 설계/구현하여 안전한 무선 네트워크 환경을 구축할 수 있었다.

2장에서는 무선 네트워크 환경에서의 공격 탐지 및 대응에 대한 기술을 분석하고, 3장에서는 본 연구에서 제안하는 전체적인 구성 및 기법에 대해 설명한다. 4장에서는 실제 구현 및 다른 무선 네트워크 공격 기법과 비교 평가를 수행하였고 5장에서는 본 연구에서의 결과를 제시하였다.

2. 관련연구

2.1 MAC Spoofing 공격 기법

네트워크 인터페이스 카드(NIC)에는 고유의 주소가 존재한다. 이를 하드웨어 주소 또는 MAC 주소라고 한다. MAC 주소는 네트워크 카드를 제

조하는 회사마다 할당되는 고유번호이며 총 48비트로 구성된다. 이것은 IEEE[6]에서 벤더에 할당한 고유 번호이기 때문에 중복되는 경우가 없으며 클라이언트 인증을 위한 기술로 사용되고 있다. NIC 기반 인증 기술을 회피하기 위해 MAC Spoofing 공격 기법이 등장하였으며 이는 자신의 MAC 주소를 인증 받은 MAC 주소로 바꾸는 것이다. 일반적인 MAC Spoofing 공격 시나리오는 다음과 같다.

① 공격자는 무선 네트워크 환경에서 주변 클라이언트의 MAC 주소를 스캔한다.

② 스캔한 MAC 주소 중 하나를 자신의 MAC 주소로 변경한다.

③ 클라이언트에 DeAuth 공격을 통해 클라이언트의 무선 네트워크 접속을 막는다.

④ 공격자의 변경된 MAC 주소 값을 이용하여 AP와 통신을 시도한다.

⑤ 공격자는 변경된 MAC 주소를 이용하여 내부 네트워크를 인증 받은 상태로 위장하여 공격할 수 있다.

⑥ 공격자는 다른 무선 네트워크 카드를 이용해서 SoftAP를 생성한다.

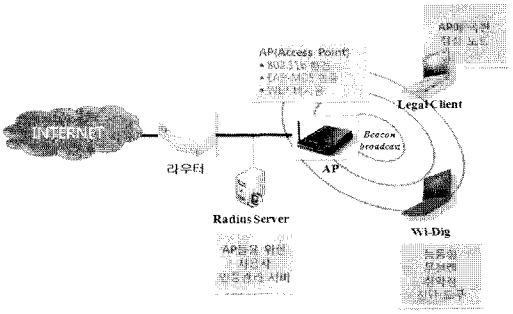
⑦ 이제 클라이언트는 SoftAP를 통해 통신하게 되며 공격자는 클라이언트의 데이터를 스니핑 할 수 있다.

MAC 주소를 이용한 네트워크 인증 기술은 사설망이나 내부 네트워크 환경에서 많이 사용되고 있다. 하지만 기존의 무선 네트워크 환경은 MAC Spoofing 공격에 취약하며 이를 탐지하고 차단하기 위한 모듈 및 시스템이 개발되어야 한다.

2.2 무선랜 취약점 진단 도구

현재 무선 네트워크를 사용하는데 있어서 상당히 많은 공격 기법들이 나와 있다. 하지만 이에 대한 대처 방안은 미흡한 상황이다. 이러한 이유로 무선랜 취약점 진단도구[3]에서는 무선 네트워크를 가상적으로 공격하여 해당 시스템의 취약점을 분석할 수 있는 시스템을 개발하여 무선 네트워크 구성에 어떠한 부분이 문제가 되는지 분석하는 역할을 수행한다.

EAP START DoS, EAP FAILURE DoS, EAP LogOFF DoS, Fake AP 등 다양한 공격에 대한 취약점 분석 기능을 가지고 있으며 이를 이용하여 무선 네트워크 환경의 문제점을 진단하고 그에 대한 해결 방안을 제시한다. [그림 1]에 의하면 무선랜 취약점 도구가 주변 Access Point에 대하여 스캔을 통하여 정보를 수집한 다음 EAP START DoS, EAP FAILURE DoS, EAP LogOFF DoS, Fake AP 등의 가상의 공격을 수행하여 무선랜 환경의 취약점을 알려주는 역할을 수행한다.



(그림 2) 무선랜 취약점 진단 도구의 구성

하지만 이는 무선 네트워크 공격을 통하여 취약점을 진단할 뿐 실제 공격에 대한 대처 및 탐지 기능을 제공하지 못한다는 문제점이 있다. 그리고 시스템 구현에 있어서 커널 2.4 기반의 리눅스와 Airjack 라이브러리가 구동되는 무선 네트워크 카드를 이용해야 한다는 단점이 있다.

2.3 무선 랜 MAC Spoofing 탐지 기법

기존 연구[4]는 무선 네트워크 환경에서 MAC Spoofing 공격을 탐지하기 위한 연구이다. 기존의 Wellenreiter, FakeAP, AirJack과 같은 MAC Spoofing 공격 툴을 이용하여 공격을 시도하고

MAC Spoofing 공격 패킷 덤프를 통하여 MAC 주소나 시퀀스 넘버를 분석하여 공격에 대한 패턴을 추출한다. 이렇게 추출된 패턴은 룰기반 공격 탐지 모듈과 비교하여 MAC Spoofing 공격으로 판단한다. 특히 시퀀스 넘버에 의한 공격 판단은 공격 툴을 이용할 경우 [그림 2]와 같이 시퀀스 값이 1씩 증가하기 때문에 기존 연구[4]에서는 이를 순차적으로 체크하여 시퀀스 값이 증가할 경우 MAC Address Spoofing 공격으로 판단한다.

```
IEEE 802.11
    Type/Subtype: Beacon frame (8)
    Destination address: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
    Source address: 00:02:a5:a5:75:a5 (00:02:a5:a5:75:a5)
    BSS Id: 00:02:a5:a5:75:a5 (00:02:a5:a5:75:a5)
    Fragment number: 0
    Sequence number: 2056
IEEE 802.11 wireless LAN management frame
    Tagged parameters (26 bytes)
        Tag Number: 0 (SSID parameter set)
        Tag interpretation: breathing

IEEE 802.11
    Type/Subtype: Beacon frame (8)
    Destination address: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff)
    Source address: 00:02:a5:a5:75:a5 (00:02:a5:a5:75:a5)
    BSS Id: 00:02:a5:a5:75:a5 (00:02:a5:a5:75:a5)
    Fragment number: 0
    Sequence number: 2057
IEEE 802.11 wireless LAN management frame
    Tagged parameters (26 bytes)
        Tag Number: 0 (SSID parameter set)
        Tag interpretation: breathing
```

(그림 3) Seq 값 증가에 따른 MAC Spoofing 탐지

하지만 기존 기법은 공격자가 자신의 무선 NIC를 이용하여 무선 트래픽에 대한 스니핑을 통하여 얻어진 클라이언트 MAC 주소로 바꿀 경우 실시간 탐지를 할 수 없다는 단점이 있다. 따라서 기존 연구는 무선 네트워크 공격의 일부분만을 고려한 것이며 이를 보완하기 위해 MAC 주소가 실시간으로 변경되는 것을 탐지해야만 한다.

2.4 해결 방안

기존의 연구들[2,3,4]은 무선 네트워크 환경에서의 MAC Spoofing 공격에 실시간으로 대응하지 못하고 있다. 따라서 본 연구에서는 실시간 MAC Spoofing 공격 탐지/차단을 위한 알고리즘과 구체적 모듈 설계 및 구현 결과를 제시하였다.

MAC Spoofing 공격을 탐지하고 차단하기 위해서는 (1) Access Point에서의 무선 네트워크 트래픽 정보 수집 및 W-TMS로의 전송 기술이 필요하며 (2) MAC Spoofing 공격에 대한 오탐지률을 줄이기 위하여 AirSensor 기반 무선 트래픽 캡쳐 및 분석 모듈을 이용하여 지속적인 MAC 주소에 대한 정보를 갱신하였다. (3) AP와 AirSensor로부터 전송된 무선 트래픽과 클라이언트에 대한 정보를 W-TMS가 수신하여 MAC 주소와 IP 주소, 시간에 대하여 MAC Spoofing 공격 탐지를 수행하며 탐지된 공격에 대하여 Access Point에 차단을 위한 기능을 수행한다.

3. 제안 모델

본 연구는 리눅스 시스템에서 제공하는 IPTABLES와 커널에서 제공하는 Message Queue[7]를 이용한다. 제안한 모델은 Access Point와 AirSensor 및 W-TMS 모듈로 구성된다. 구체적으로 AirSensor와 Access Point로부터 무선 트래픽과 클라이언트 정보를 수집하여 W-TMS에서는 MAC Spoofing 공격에 대한 탐지 및 차단 기능을 수행하여 안전한 무선 네트워크 환경 구축 및 관리 기법을 제시하고자 한다.

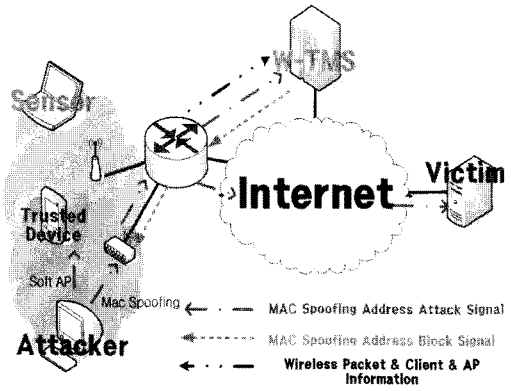
3.1 전체 시스템 구조

본 연구에서 제시한 전체적인 모듈 구조는 다음과 같다.

Access Point	IPTABLES를 이용한 패킷의 QUEUE 저장
	IPQ Library를 이용한 패킷 분석
	Send 패킷 Information
	Receive Protection Signal
	패킷 Drop or Accept
AirSensor	Channel Hopping을 통한 패킷 감지
	패킷 분류 모듈
	패킷의 공격 탐지 모듈
	패킷 정보 전송 모듈
W-TMS	Receive 패킷 Information
	Display 패킷 Information
	Detect MAC Spoofing
	Send Protection Signal

(표 1) 전체 모듈의 분류

Access Point에서는 접속한 무선 클라이언트에 대한 패킷 정보를 W-TMS로 전송을 하며, W-TMS는 패킷 정보를 저장함과 동시에 MAC Address Lookup 테이블을 작성한다. MAC Address Lookup 테이블에는 무선 클라이언트의 MAC 주소와 IP 주소, 연결된 AP의 주소, 접속시간 정보가 저장된다. 이때 클라이언트에 대한 정보는 AP에서 뿐만 아니라 AirSensor에서도 채널 호핑을 통하여 수집하며 이에 대한 정보 역시 W-TMS로 보내진다. W-TMS에서는 실시간으로 업데이트 되는 MAC Address Lookup 테이블 정보를 이용하여 MAC Spoofing 공격에 대한 판단 과정을 수행한 후 판단에 따른 결과를 AP로 전송한다. AP는 W-TMS로부터 전달 받은 판단 결과에 따라 해당 패킷에 대한 차단 모듈을 수행한다. 제안한 시스템의 전체적 구조와 세부 작동 방식은 다음과 같다.



(그림 4) 제안 시스템의 전체적 구조

① AirSensor와 Access Point를 통해 주변 무선 클라이언트의 트래픽 및 패킷 정보 수집
② Access Point와 AirSensor에서 수집된 정보를 W-TMS로 전송 및 MAC Address Lookup 테이블 정보 갱신
③ 공격자의 MAC Spoofing 공격 수행
④ Access Point와 AirSensor에서 공격자에 대한 MAC 주소와 IP 주소 및 접속시간 정보를 W-TMS로 전송
⑤ W-TMS에서는 기존의 MAC Address Lookup 테이블에 저장된 IP 주소 및 MAC 주소와 Access Point와 AirSensor로부터 전송된 정보와의 비교를 통해 MAC Spoofing 공격을 탐지
⑥ W-TMS가 탐지한 MAC Spoofing 공격 트래픽에 대해 Access Point에서 차단 과정 수행

본 연구는 위와 같은 단계를 거쳐 MAC Spoofing 공격을 차단하며 AirSensor와 Access Point, W-TMS의 연동을 통해 무선 네트워크 환경에서 실시간으로 MAC Spoofing 공격을 탐지/차단할 수 있다. Access Point, AirSensor 및 W-TMS에서 수행하는 세부 과정은 다음과 같다.

3.2 AP에서의 무선 패킷 정보 전송

3.2.1 무선 패킷에 대한 QUEUE 저장 모듈

Access Point에서는 무선 네트워크 인터페이스 카드로부터 들어오는 패킷을 QUEUE에 저장하는 역할을 수행한다. Access Point에서는 무선 네트워크 카드와 유선 네트워크 카드가 Bridge 형태로 구성이 되며 무선 네트워크 카드를 통하여 들어온 패킷은 Bridge를 통하여 유선 네트워크 카드로 나간다. 이때 Bridge를 통하는 무선 패킷을 QUEUE에 저장하여 패킷의 분석을 수행하는 모듈이 수행할 수 있게 한다.

3.2.2 무선 패킷 정보 추출 모듈

리눅스 커널의 QUEUE에 저장된 패킷은 IPQ 라이브러리의 도움으로 분석을 수행할 수 있다. 패킷의 분석에서는 기본적으로 IP Header[8]와 TCP Header[9]를 볼 수 있으며 이러한 패킷의 정보를 추출하여 해당 패킷의 수신지 주소와 송신지 주소, 패킷의 프로토콜 타입 등 다양한 정보를 추출한다. 추출된 MAC 주소는 MAC Spoofing을

판단하는데 있어서 중요한 정보가 된다.

3.2.3 무선 패킷 정보 전송 모듈

무선 패킷의 정보를 추출하여 패킷의 정보를 W-TMS에게 전송하는 역할을 수행한다. 실시간으로 모든 패킷의 정보를 전송할 경우 Access Point의 성능이 저하가 되기 때문에 확률 p에 따라 전송한다. 이때의 확률 p는 클라이언트의 정보를 기반으로 판단하게 된다. 클라이언트의 MAC 주소와 시간 정보를 저장한 다음 패킷이 동일한 MAC 주소를 가지고 있을 경우 전에 저장된 패킷의 정보와 x초의 간격이 있을 경우 패킷 정보를 W-TMS로 전송 하도록 하였다.

```
D_c : Data From Wireless Network Client c
C_t : Client's Using Time
S_t : System Time

Send Information( ) {
  If C_t = NULL then
     C_t = S_t
  else
     If p_t && (S_t - C_t > x sec) then
        Send_Packet_Information( D_c)
}
```

3.2.4 차단 정보 수신 및 차단 모듈

앞서 패킷의 정보를 전송하는 모듈에서는 W-TMS로 전송 후 패킷을 보내는 클라이언트의 MAC Spoofing 판단 여부를 기다린다. 이러한 판단은 뒤에서 설명할 W-TMS에서 내리며 본 모듈에서는 W-TMS로부터 MAC Spoofing 판단에 대한 결과를 기다리는 역할을 수행한다.

W-TMS로부터 MAC Spoofing으로 판단된 신호를 받을 경우 AP 내의 MAC Address Blocking List에 등록이 되며 이는 QUEUE에 저장된 패킷의 전송 및 차단에 대한 판단 기준이 된다.

AP에서는 MAC Address Blocking List 정보를 확인 후 현재 QUEUE에 저장된 패킷이 MAC Address Blocking List에 등록이 되어 있을 경우 패킷을 DROP 시키며 MAC Address Blocking List에 등록이 안 되어있을 경우 패킷을 ACCEPT 시켜 패킷이 원활히 전송될 수 있도록 도와준다.

3.3. AirSensor에서의 무선 패킷 정보 전송

3.3.1 Channel Hopping을 통한 패킷 탐지

IEEE 802.11에서는 AP마다 서로 다른 채널을 사용하게 함으로써 혼잡 신호나 다른 무선기기와의 주파수 혼선을 줄이고 있다[10]. 무선 네트워크에서 다양한 채널을 주기적으로 바꾸어주며 각각의 채널에서 통신되는 패킷을 탐지하는 기법을 Channel Hopping[11]이라 부른다. 따라서 본 연구에서 제시한 AirSensor에서는 여러 개의 채널을 탐지하고 데이터를 추출할 수 있는 Multi-Channel Scanning(Channel Hopping)을 통한 패킷 탐지 시스템을 이용하였으며 패킷 분류 및 공격 탐지 기능도 수행한다.

```
Channel Hopping Function
Listen() : Wireless Network Listen Mode
WNI : Wireless Network Interface Structure
Ch : Channel Number
DetectionAttack() : Compare DATA With Rule files

ChannelHoping(WNI){
   While(1)
      For i=0 to 13
         WNI->Ch=i;
         Data=Listen(WNI);
         AttackDetection(Data);
}
```

3.3.2 무선 패킷 분류 모듈

무선 네트워크에서는 패킷의 타입이 지정되어

있다. 패킷의 종류에는 관리 프레임 및 데이터 프레임 등 다양한 형태의 프레임이 정의되어 있다[12]. 본 연구에서는 데이터 프레임일 경우 프레임 내에 저장된 패킷 정보를 무선 공격 탐지 모듈로 전송 한다. 또한 관리 프레임일 경우 Auth Flooding 또는 DeAuth Flooding 공격 등을 판단한다.

3.3.3 무선 데이터 프레임 공격 탐지 모듈

AirSensor는 무선 네트워크 프레임내 데이터 패킷에 대한 분석을 수행한다. 이렇게 추출한 데이터 패킷 정보에 대해서 AirSensor는 W-TMS에서 탐지하는 MAC Spoofing 공격 탐지 외에 따로 시그니처 기반의 Snort-wireless[13]의 룰을 이용하여 공격 탐지 기능을 추가적으로 수행한다.

```
D_c : Data From Wireless Network Client c
R : Rule Attack Data
Response() : Send Response Packet

AttackDetection(D_c){
   Open(R);
   If( Compare(D_c , R) )
      Alert Attack Signal(D_c)
      Send_RST_Signal(D_c);
}
```

3.3.4 무선 프레임 정보 전송 모듈

Channel Hopping 기반 프레임 분석 과정에서 패킷의 송신지 IP 주소와 수신지 IP 주소 및 MAC 주소까지 추출이 가능하다. 따라서 AirSensor에서 W-TMS로 송신지 IP 주소, 수신지 IP 주소, AP의 IP 주소, AP의 BSSID, 클라이언트의 MAC 주소 정보를 전송한다. 이 정보들은 W-TMS에서 MAC Address Lookup 테이블에 저장되며 MAC Spoofing의 판단 정보로 이용된다.

3.4 W-TMS의 MAC Spoofing 공격 탐지 및 차단

3.4.1 무선 패킷 정보 수신 모듈

W-TMS는 무선 네트워크 정보를 수집하는 역할을 수행한다. 기본적으로 AirSensor와 Access Point로부터 무선 네트워크의 패킷 정보와 클라이언트, Access Point 정보를 수집 및 저장한다. W-TMS에서 저장하는 MAC Address Lookup 테이블은 다음과 같다.

Time	IP_a	IP_c	M_c
2008.01.01 23:55:50	192.168.0.2	192.168.0.104	00:FF:BB :11:22:33
2008.01.01 12:30:45	192.168.1.2	192.168.1.101	00:FF:CC :11:22:33
Client 접속 시간	AP의 IP 주소	Client의 IP 주소	Client의 MAC

표 2 MAC Address Lookup 테이블

저장되는 정보로는 클라이언트의 패킷이 지나간 시간(Time)과 접속한 Access Point의 IP 주소(IP_a), 클라이언트의 IP 주소(IP_c), 클라이언트의 MAC 주소(M_c)를 저장한다. 패킷의 정보가 저장되는 형태는 Routing Lookup 테이블과 유사하며 무선 트래픽에 대한 MAC Spoofing 공격 탐지의 자료로 이용한다.

3.4.2 MAC Spoofing 공격 탐지 모듈

Access Point와 유무선 공유기들은 Router 역할을 수행하거나 브릿지 역할을 수행할 경우 기존의 클라이언트에 대한 IP 주소를 할당 정보를 가지고 있다. 따라서 MAC Spoofing 공격을 시도할 경우 공격자는 IP 주소 충돌을 막기 위해 할당되지 않은 IP 주소를 사용한다. 따라서 일반 사용자와 공격자의 IP 주소가 중복될 수는 없기 때문에 MAC 주소와 IP 주소 두가지를 가지고 비교를 할 경우 공격자 판단을 내릴 수 있게 된다.

일반 사용자가 IP 주소를 바꿀 경우 기존의 MAC 주소는 그대로 유지하면서 다른 사용자에 의해 설정되지 않았던 IP 주소로 바꾸는 것으로

이 경우에는 새로운 클라이언트 정보로 등록이 된다. 하지만 MAC Spoofing 공격을 할 경우 새로운 MAC 주소 또는 IP 주소가 신규로 등록되는 것이 아니라, 기존의 IP 주소와 MAC 주소에 대한 두 개의 정보가 모두 W-TMS에 이미 등록이 되어 있는 상태에서 기존에 사용자의 IP에 대한 MAC 정보로 바뀐 상태로 W-TMS에 수신되기 때문에 일반 사용자의 적법한 IP 변형과 공격을 정확히 판단할 수 있다.

결국 W-TMS에서는 MAC Address Lookup 테이블내에 기록된 정보를 대상으로 특정 시간 내에 같은 MAC 주소에 대하여 IP 주소가 변경될 경우 MAC Spoofing 공격으로 판단할 수 있다. 따라서 제안한 MAC Spoofing 공격 탐지 모듈은 다음과 같다.

```
MA : MAC Address Lookup Table
M_c : MAC Address of Client c
C_ip : Client IP Address
C_ip' : New Client IP Address
SpoofDetection(M_c) {
  If MA == NULL then
    MA += M_c
  else
    Find M_c From MA
    If MA's C_ip == C_ip' then
      Update MA's Time
    else
      Alert MAC Spoofing Attack(M_c)
      Send_Client_Block_Signal to AP
}
```

앞서 설명한 것과 같이 공격자에 의해 MAC 주소에 할당된 IP 주소가 임의적으로 바뀌는 것을 탐지하여 MAC Spoofing 공격으로 판단하고 해당 클라이언트가 접속하고 있는 Access Point로 MAC Spoofing에 대한 결과를 전송한다. 전송된 결과에 따라 Access Point는 MAC Address Blocking List에 저장하고 해당 트래픽에 대한 차단을 수행하게 된다.

4. 구현 결과 및 성능 평가

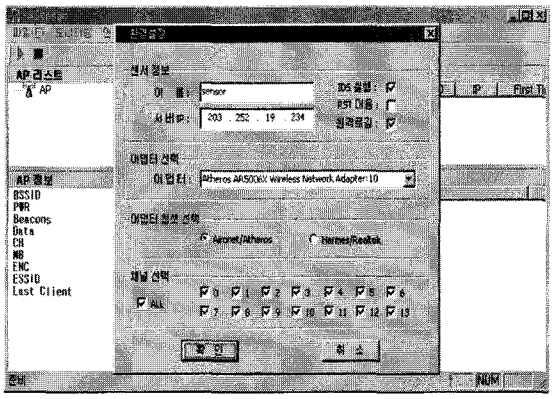
본 연구에서 제안하는 모델의 실제 구현은 Access Point 역할을 수행하는 유무선 공유기에 임베디드 리눅스[14]를 설치, 크로스 컴파일을 통하여 모듈을 연동 시켰다. 그리고 AirSensor의 경우 Channel Hopping과 Wireless 패킷 Sniffing이 가능한 Atheros 칩을 이용하여 실험하였다. W-TMS는 닷넷 프레임워크 환경에서 개발이 되었으며 C#을 이용하였다.

4.1 구현 결과

4.1.1 AirSensor

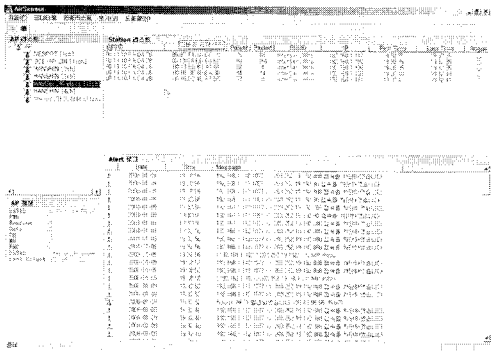
AirSensor는 WinAPI와 MFC를 이용하여 GUI를 개발하였으며 무선 네트워크 환경에 맞추어 Access Point와 무선 클라이언트 정보를 모니터링 할 수 있게 구현하였다.

AirSensor의 동작은 아래의 [그림 4]와 같은 환경설정을 통하여 Sniffing을 하고자 하는 네트워크 인터페이스 카드와 채널을 선택할 수 있으며 W-TMS의 주소를 입력하여 W-TMS와의 통신 여부를 선택할 수 있다.



(그림 5) AirSensor에서의 환경설정

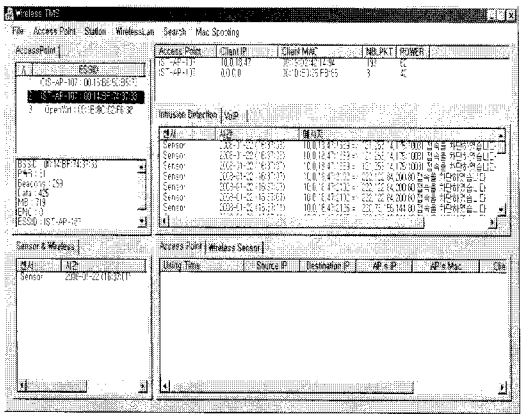
W-TMS와 접속이 이루어지면 AirSensor는 아래 [그림 5]와 같이 무선 데이터를 스니핑 하기 시작하며 Rouge Access Point와 클라이언트에 대한 정보를 수집한다. 그리고 데이터 패킷일 경우 MAC 주소와 시간 정보를 이용하여 일정 주기로 W-TMS로 패킷 정보를 전송한다.



(그림 6) AirSensor를 통한 무선 클라이언트와 AP 트래픽 모니터링

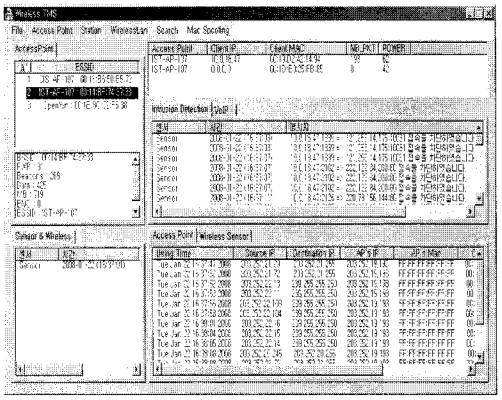
4.1.2 W-TMS

W-TMS는 아래 [그림 6]과 같이 AirSensor와 Access Point로부터 패킷에 대한 정보를 받으며 AirSensor가 보낸 Access Point와 클라이언트에 대한 정보를 보여준다.



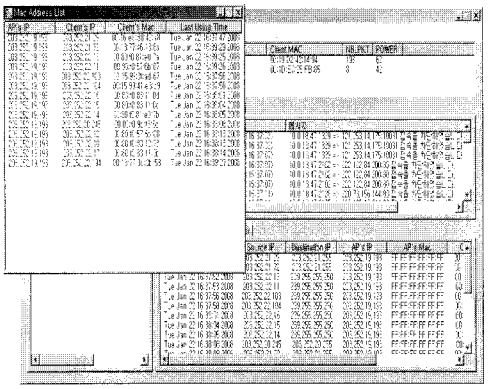
(그림 7) W-TMS를 통한 무선 클라이언트와 AP 트래픽 모니터링

또한 W-TMS는 [그림 7]과 같이 AirSensor와 클라이언트로부터 받은 패킷 정보를 사용시간과 송신지 IP 주소, 수신지 IP 주소, AP의 IP 주소, AP의 BSSID, 클라이언트 MAC 주소, 프로토콜 타입 등을 보여준다.



(그림 8) W-TMS를 통한 무선 패킷 정보 수집

W-TMS는 AirSensor와 AP로부터 수신된 패킷 정보를 보여주면서 MAC 주소에 대한 정보를 중심으로 [그림 8]과 같이 MAC Address Lookup 테이블을 지속적으로 갱신하며 MAC Spoofing으로 판단이 될 경우 Access Point로 MAC Spoofing 공격 탐지 및 차단 신호를 보낸다.



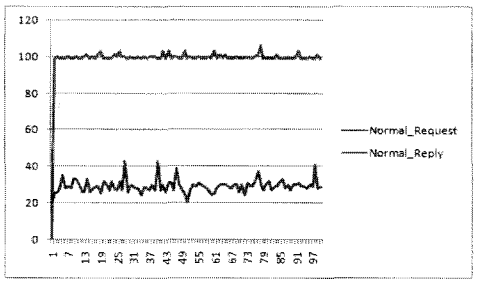
(그림 9) MAC Spoofing 공격 탐지를 위한 W-TMS에서의 무선 MAC 주소 수집

W-TMS로부터 MAC Spoofing 탐지 신호를 받은 Access Point는 해당 MAC 주소에 대하여 차단 기능을 수행한다.

4.2. 성능 평가

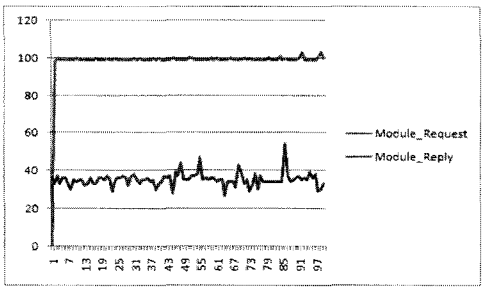
본 연구를 통해 개발된 시스템에 대한 성능 평가를 위해 우선 무선 클라이언트에서 Victim으로 전송한 ICMP 패킷의 전송률을 측정하였다. ICMP 패킷의 경우 전송되는 패킷의 횟수와 응답 패킷의 횟수를 정할 수 있기 때문에 Access Point에서의 Victim에 대한 전송률 통계가 가능하다.

또한 MAC Spoofing 공격에 대해 탐지하고 차단하는 시간을 비교 평가하였다. 패킷의 정보 추출은 일반적으로 많이 이용하고 있는 Ethereal(WireShark)를 이용하였다.



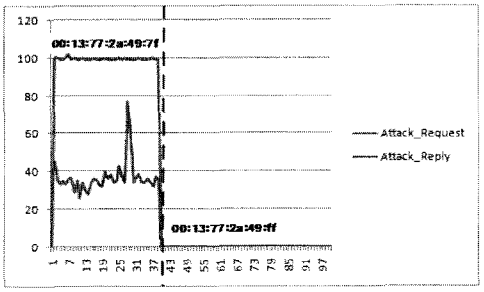
(그림 10) 일반적인 AP를 통한 ICMP 패킷의 흐름

[그림 9]에서 보여주는 차트는 일반적으로 PING을 100번 시도 할 경우 AP를 통해 전달된 패킷 송수신 결과이다. PING은 ICMP[15] 신호를 순차적으로 보내고(Request) 받는(Reply) 과정을 거치기 때문에 ICMP 패킷에 대한 시간 차이가 거의 직선을 이루며 흐르는 것을 볼 수 있다.



(그림 11) MAC Spoofing 탐지 모듈 구동 시 ICMP 패킷의 흐름

[그림 10]은 MAC Spoofing공격 탐지를 위한 모듈을 구동 시켰을 경우의 패킷의 흐름이다. 본 연구의 모듈의 실험은 총 100번의 ICMP 신호에 대한 통계를 추출한 것으로 거의 직선에 가깝지만 시간의 간격차이가 큰 경우가 일반적인 경우보다 많은 것을 볼 수 있다. 패킷의 손실은 없지만 패킷의 딜레이가 특정 확률로 생기는 것을 확인할 수가 있다. 경우의 수가 늘어날수록 손실이 일어나거나 패킷의 전송 딜레이가 커질 수 있으나 이는 네트워크의 영향에 의해서도 일어 날수 있는 것이기 때문에 본 연구의 영향으로는 적합하지 않은 결과이다.

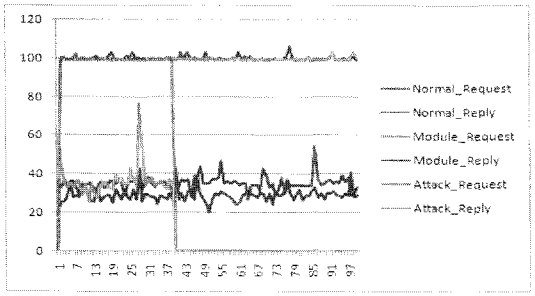


(그림 12) MAC Spoofing 공격 시도 시 공격자로부터 받은 Victim의 패킷 흐름

본 연구에서 개발한 W-TMS 모듈이 구동되고 있을 경우 공격자에 의해 MAC Spoofing 공격을 시도하면 Victim에서 [그림 11]와 같은 형태의 무선 트래픽 흐름을 보인다. 기존의 MAC 주소 00:13:77:2a:49:7f로 전송이 되던 중 38번째 전송에서부터 MAC Spoofing 툴을 통하여 00:13:77:2a:49:ff로 MAC 주소를 수정하여 전송하였으며 이 때 본 연구에서 제안한 모듈은 MAC 주소의 변경을 탐지하고 해당 MAC 주소에 대한 패킷을 차단하였다. 실제로 Victim에서는 38번째 신호 이후에 아무런 ICMP 신호를 받지 않았다. 본 연구에서 제안한 Access Point에서의 MAC Spoofing 공격 차단 모듈이 정상적으로 작동을 하

는 것을 알 수 있었다.

일반적인 경우의 패킷 흐름과 모듈이 구동 되었을 경우와 MAC Spoofing 공격을 시도하였을 경우 발생하는 무선 트래픽은 다음과 같다.



(그림 13) 전체적 패킷 흐름에 대한 차트

앞의 실험 결과를 분석해 볼 때 본 연구에서 제안한 Wireless MAC Address Spoofing 공격의 탐지 및 차단 모듈은 패킷의 전송에 있어서 손실률 없이 전송이 된다는 것을 알 수 있었으며 공격 탐지/차단 과정에서 약간의 무선 트래픽 전송 지연이 발생하였다. 이러한 결과는 네트워크 환경에 따라 약간의 차이가 있을 수 있지만 실제 사용자에게 영향을 미치는 정도는 아니다. 따라서 본 연구의 MAC Spoofing 공격 탐지 및 대응에 대한 제안 모델은 네트워크를 사용자에게 영향을 미치지 않으면서 MAC Spoofing 공격을 탐지 및 차단한다. 본 연구의 제안 모델은 악의적인 공격자가 무선 MAC Spoofing 공격을 실시할 경우 이를 실시간으로 대응하는 향상된 Anti-Spoofing 모델이다.

5. 결론

본 연구가 진행 되는 기간 동안에도 W-CDMA부터 시작하여 Wibro에 이르기까지 다양한 무선 네트워크 기술이 제시되고 많은 관심을 보이고 있다. 앞으로 무선 네트워크 기술은 필수불가결한 기술이 될 것이다. 따라서 무선 네트워크를 좀더 안전하게 이용하기 위해 본 연구에서는 AirSensor, AP를 기반으로 무선 트래픽에 대한 정보 수집 과정을 수행하고 이를 W-TMS로 전송하여 MAC Spoofing과 같은 무선 네트워크 공격에 능동적으로 대응할 수 있는 기술을 개발하였다. 본 연구를 통해 사설망 또는 내부 네트워크 이용자를 보호하고 나아가 무선 네트워크의 취약점을 이용한 공격자를 판단하여 MAC Spoofing 공격을 실시간으로 탐지/차단할 수 있는 기법을 제시할 수 있었다.

본 연구에서 제시한 기법은 기존 무선 네트워크 환경을 그대로 이용하면서 손쉽게 적용이 가능한 것으로 추후 802.11n이나 802.11i와 같은 발전된 무선 네트워크 기술이 실용화 되어도 적용 가능하다는 장점이 있다.

참 고 문 헌

[1] Steven M. Willens, "NETWORK ACCESS CONTROL SYSTEM AND PROCESS", U.S. Patent 5889958, March 30, 1999. (http://www.patentstorm.us/patents/5889958.html)

[2] 서대희, 이임영, "유비쿼터스 환경을 위한 다중 사용자 기반의 안전하고 효율적인 무선 네트워크 관리 기법 제안", 정보처리학회논문지 C 제13-C권 제1호, 2006.

[3] 류재철, "능동형 무선랜 취약점 진단도구", ITRC FORUM, 2007.

[4] Joshua Wright, GCIH, "Detecting Wireless LAN MAC Address Spoofing", Cisco Certified Network Associate 기술문서, 2003.

[5] Steven J. Scott, "Threat Management Systems, The State of Intrusion Detection", SNORT Technical Report, 2002. (http://ftp.at.linuxfromscratch.org/infosys/security/snort/docs/threatmanagement.pdf)

[6] "IEEE STANDARD FOR LOCAL AND METROPOLITAN AREA NETWORKS", IEEE

Std 802, 2001.
[7] David A Rusling, "Message Queues", The Linux Kernel, 2001.
[8] DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION, "INTERNET PROTOCOL", RFC 791, 1981.
[9] DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION, "TRANSMISSION CONTROL PROTOCOL", RFC 793, 1981.
[10] 윤종호, "무선 LAN 보안프로토콜", 교학사, 2005.
[11] Vishnu Navda, Aniruddha Bohra, Samrat Ganguly, "Using Channel Hopping to Increase 802.11 Resilience to Jamming Attacks", IEEE Infocom Minisymposium, 2007.
[12] "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", ANSI/IEEE Std 802.11, 2003.
[13] http://www.snort-wireless.org/
[14] http://www.openwrt.org/
[15] DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION, "Internet Control Message Protocol", RFC 792, 1981.

◐ 저 자 소 개 ◑

조 제 경(Je-Gyeong Jo)
2006년 한신대학교 정보시스템공학과 (공학사)
2006년 ~ 현재 한신대학교 컴퓨터정보대학원 (석사과정)

관심분야 : 시스템보안, 네트워크보안, 보안공학, etc.
E-mail : aiking@hs.ac.kr

이 형 우 (Hyung-Woo Lee)
1994년 고려대학교 전산과학과 졸업(학사)
1996년 고려대학교 대학원 전산과학과 졸업(석사)
1999년 고려대학교 대학원 전산과학과 졸업(박사)
1999년~2003년 2월 천안대학교 정보통신학부 조교수
2003년~현재 한신대학교 컴퓨터공학부 부교수
관심분야 : 정보보호, 유무선 네트워크 보안, 웹 보안기술
E-mail : hwlee@hs.ac.kr