ISSN 1598-0170 (Print)
ISSN 2287-1136 (Online)
http://www.jksii.or.kr

DHCP 스누핑 기반의 비인가 AP 탐지 기법

A Rogue AP Detection Method Based on DHCP Snooping

박 승 철[1*]
Seungchul Park

요 약

와이파이 환경에서 비인가 AP(rogue AP)의 접속은 스니핑(sniffing), 피싱(phishing), 파밍(pharming) 공격 등 다양한 사이버 공격에 노출될 수 있는 매우 위험한 행위이다. 따라서 비인가 AP를 신속하고 정확하게 탐지하여 와이파이 사용자가 해당 AP에 대한 접속을 회피할 수 있도록 적절하게 경고하는 것은 와이파이 보안의 핵심 요구사항이 되고 있다. 본 논문은 인가된 AP에 대한 설치 정보와 스위치의 DHCP 스누핑 정보를 활용하여 비인가 AP를 정확하고 신속하게 탐지하여, 무선 단말에 실시간으로 통보하는 새로운 비인가 AP 탐지 기법을 제시한다. 제안된 비인가 AP 탐지 기법은 별도의 장비가 불필요하고 간단하여 많은 수의 탐지 센서와 탐지 서버로 구성되는 무선 침입 방지 시스템(wireless intrusion prevention system)에 비해 저가격에 구현가능하다. 그리고 타이밍 정보, 위치 정보, 화이트 리스트 기반 등의 기존 비인가 AP 탐지 기법에 비해 탐지의 정확성이 높고, 신속하며, 개방 환경을 포함하여 다양한 환경에 유연하게 적용가능한 장점이 있다.

☞ 주제어 : 와이파이 보안, 비인가 AP, 비인가 AP 탐지, DHCP 스누핑

ABSTRACT

Accessing unauthorized rogue APs in WiFi environments is a very dangerous behavior which may lead WiFi users to be exposed to the various cyber attacks such as sniffing, phishing, and pharming attacks. Therefore, prompt and precise detection of rogue APs and properly alarming to the corresponding users has become one of most essential requirements for the WiFi security. This paper proposes a new rogue AP detection method which is mainly using the installation information of authorized APs and the DHCP snooping information of the corresponding switches. The proposed method detects rogue APs promptly and precisely, and notify in realtime to the corresponding users. Since the proposed method is simple and does not require any special devices, it is very cost-effective comparing to the wireless intrusion prevention systems which are normally based on a number of detection sensors and servers. And it is highly precise and prompt in rogue AP detection and flexible in deployment comparing to the existing rogue AP detection methods based on the timing information, location information, and white list information.

☞ keyword : WiFi security, rogue AP, rogue AP detection, DHCP snooping

1. 서 론

이제 가정, 사무실, 그리고 공공장소 등에서 와이파이는 필수적인 네트워크 서비스가 되었고, 대부분의 모바일 단말들은 와이파이를 통해 인터넷을 접속하고 있다. 모바일 사용자들은 단순한 웹 서비스뿐만 아니라 사용자의 민감한 정보 전송을 필요로 하는 인터넷 쇼핑, 인터넷 뱅킹과 같은 금융 거래 서비스도 와이파이 네트워크를 통해 활발하게 수행하고 있다. 와이파이 네트워크는 기술적으로 사용 기관의 보안 정책에 맞게 충분한 보안 서비스를 제공할 수 있도록 설계되어 있다. 그러나 허가 없이 누구나 설치할 수 있는 와이파이 네트워크의 특성상, 관련 기관의 승인 없이 설치되어 사용되는 비인가 AP(Access Point)(rogue AP)가 기관의 일관성 있는 보안 정책 집행을 방해하는 중요한 보안 위협이 되고 있다 [1,2]. 특히 악의적인 공격자에 의해 SSID(Service Set IDentifier) 스푸핑(spoofing) 등을 통해 정상적인 AP를 가장하여 설치된 비인가 AP는, 사용자가 인지하기 어렵고 따라서 쉽게 접속하게 된다. 비인가 AP를 통해 전송되는 정보는 해당 AP를 장악한 공격자에 의해 스니핑(sniffing)될 수 있고, 피싱(phishing)과 파밍(pharming)과 같은 중간자 공격에 노출될 수 있기 때문에, 사용자의 패스워드, 카드 번호, 계좌 번호, 보안카드 번호 등 민감한 개인 정보의 노출과 그에 따른 금융 사고로까지 연결될 수 있다. 현재 PC뿐만 아니라 대부분의 스마트폰이 테더링

1 School of Computer Science and Engineering, Korea University of Technology and Education, Cheonan, Chungnam-Do, 31253, Republic of Korea
* Corresponding author (scpark@koreatech.ac.kr)
[Received 12 January 2016, Reviewed 27 January 2016, Accepted 25 March 2016]

(tethering) 기술 등을 적용하여 AP 서비스를 제공할 수 있기 때문에 공격자들이 4G/LTE 네트워크에 연결된 비인가 AP를 쉽게 설치하여 사용자를 유혹할 수 있다[3]. 따라서 비인가 AP를 신속하고 정확하게 탐지하여 와이파이 사용자에게 통지함으로써 의도하지 않은 비인가 AP 접속을 차단하는 것은 와이파이 보안의 매우 중요한 요소가 되고 있다.

그럼에도 불구하고 현재까지 대부분의 와이파이 네트워크 환경에서 비인가 AP 탐지와 사용자에 대한 경고 서비스는 제공되고 있지 않다. 그 주된 이유는 현재 비인가 AP에 대한 보안 대책으로 제시되고 있는 WIPS(Wireless Intrusion Prevention System)가 복잡하고 고비용 구조이기 때문이다[1,4]. 고비용 WIPS에 대한 대안으로 유선 단말이 연결되어야 할 스위치 포트에 비정상적으로 연결된 비인가 AP, 인가된 AP에 와이파이로 재연결된 비인가 AP, 또는 3G/LTE에 연결된 비인가 AP를 경유할 때 발생하는 트래픽의 타이밍 정보의 차이를 활용하거나, 인가 AP의 위치 정보를 미리 등록하고 등록되지 않은 비인가 AP의 위치 정보를 활용하거나, 또는 기관의 인가 AP에 대한 화이트 리스트(white list)를 활용하는 비인가 AP 탐지 기법들이 제안되었다. 그러나 복잡성, 높은 탐지 오류율, 긴 탐지 시간, 또는 사용자 편의성 결여 등의 이유로 이러한 기법들이 실제 환경에 적용되고 있지 못한 것이 현실이다.

본 논문은 특정 기관의 인가 AP 설치 시에 수집되는 AP의 SSID와 MAC 주소, 스위치 ID와 포트 번호 등의 등록 정보와 인가 AP가 연결된 스위치에서 수집되는 스위치 ID, 포트 번호, 그리고 와이파이 단말에 할당되는 IP 주소 등의 DHCP 스누핑(snooping) 정보를 활용하는 간단하고, 정확하며, 신속한 비인가 AP 탐지 기법을 제시한다. 접속한 AP를 통해 IP 주소를 할당받은 와이파이 단말은 기관 네트워크의 특정 위치에 연결된 탐지 서버에 접속한 AP의 MAC 주소와 할당받은 IP 주소를 전송함으로써 비인가 AP 여부를 확인받을 수 있다. 본 기법은 별도의 탐지 센서와 전용 탐지 서버 설치를 요구하지 않기 때문에 저비용으로 구현이 가능하고, 접속한 AP의 비인가 AP 여부를 실시간으로 확인받을 수 있다. 그리고 비인가 AP 탐지 클라이언트 앱(rogue AP detection application)을 설치한 와이파이 단말은 동일한 기법을 지원하는 어떤 기관에서도 별도의 등록 절차 없이 비인가 AP 탐지 서비스를 제공받을 수 있기 때문에 유연한 적용을 보장한다.

2. 관련 연구

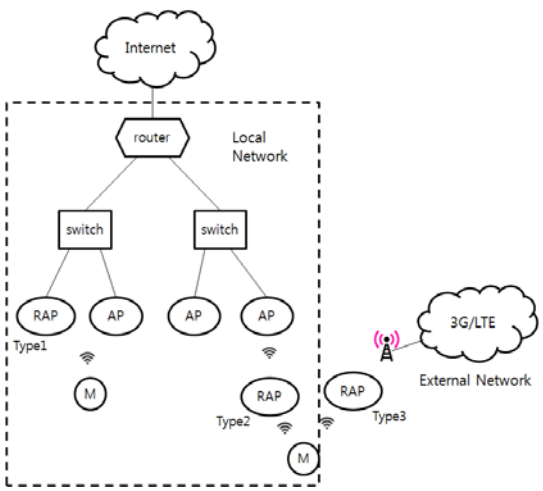
기존의 가장 대표적인 비인가 AP 탐지 기술은 AirTight[5], Air Marshal[6]와 같은 WIPS이다. WIPS는 WiFi 신호를 스캐닝하고, 필요하면 유.무선 구간을 통해 특수한 트래픽(예, marker packet)을 주입하고 관찰하며, 서버의 제어하에 사용자의 비인가 AP 접속을 차단하는 탐지 센서(detection sensor)와, 스캐닝한 정보를 바탕으로 비인가 AP 여부를 판정하고 관리자에게 와이파이 관제 서비스를 제공하는 탐지 서버(detection server)로 구성된다. 일반적으로 탐지 센서는 유선 네트워크에 연결되고 30미터 내외의 탐지 범위를 제공한다. 따라서 넓은 범위의 와이파이 서비스를 제공하는 기관은 많은 수의 고가의 탐지 센서를 설치해야 한다. 2015년 말 현재 1개의 탐지 센서 가격은 1,000 달러를 상회하고, 탐지 서버의 경우 15,000 달러를 상회한다. 따라서 공중망과 같은 광범위한 와이파이 환경이나 충분한 보안 인프라 비용 투입이 어려운 기관에서 WIPS 구축은 현실적으로 어렵고, 특히 작은 기관에서의 WIPS 도입은 비현실적이다. 유선 네트워크에 연결되어야 하는 탐지 센서의 특성상 유선 네트워크로부터 멀리 떨어진 3G/LTE 기반의 비인가 AP의 탐지 어려움도 WIPS의 문제점이 되고 있다.

고비용 WIPS에 대안으로 제시된 다수의 비인가 AP 탐지 기법들은 비인가 AP의 무선 구간을 경유할 때 발생하는 타이밍 정보의 차이를 활용한다. [4]는 유선망에 연결된 비인가 AP의 와이파이 무선 구간을 경유하는 트래픽의 지연시간(RTT-Round Trip Time) 특성과, 정상적인 유선 단말이 해당 포트에 연결되었을 경우의 지연시간 특성과의 차이를 관찰하여 비인가 AP가 연결되었음을 파악한다. [7]은 인가 AP에 와이파이를 통해 재연결된 비인가 AP의 와이파이 무선 구간을 경유하는 트래픽의 지연시간 특성을 파악하여 비인가 AP를 판정하는 방법을 제시하고 있다. 또한 [8]은 3G/LTE망에 연결된 스마트폰 기반의 비인가 AP를 경유할 때 3G/LTE망에서 추가적으로 발생하는 지연시간 특성을 관찰함으로써 비인가 AP 여부를 판정하고 있다. 트래픽의 지연시간 특성은 네트워크의 혼잡 상황에 따라 차이가 크기 때문에 지연시간 특성에 의존한 비인가 AP 탐지는 오류율이 높을 수밖에 없고, 유의미한 지연시간 특성을 파악하기 위해서는 반복적인 지연시간 측정이 요구되어 비인가 AP 판정에 긴 시간이 소요될 수밖에 없는 문제가 있다.

[9]는 인가 AP의 위치 정보를 유지하고 탐지된 AP의 위치를 인가 AP의 위치 정보와 비교하여 비인가 AP 여부를 탐지하는 방법을 제시하고 있다. 위치 정보 기반의 비인가 AP 탐지는 별도의 위치 정보 측정 장치를 필요로 하고, 위치 정보 측정 오차로 인한 비인가 AP 탐지 오류가 발생할 수 있으며, 무선으로 연결된 인가 AP를 사용하는 경우 위치 정보 갱신이 어려운 문제가 있다. 그리고 [10]은 기관의 인가 AP에 관한 정보를 화이트 리스트(white list)로 정리한 후 등록된 내부 사용자의 와이파이 단말에게 전송하고, 화이트 리스트에 포함되지 않은 AP를 비인가 AP로 판정하여 사용자가 접속할 수 없게 차단한다. 이 기법은 사전에 사용자의 ID와 패스워드 등록을 필요로 하여 회사와 같은 폐쇄된 조직에서는 적용 가능하지만, 많은 사용자들이 자유로이 방문하는 개방된 기관에서는 사용하기가 현실적으로 매우 어렵다.

3. 비인가 AP 유형

(그림 1)은 특정 기관의 와이파이 사용자에게 보안 위협 요소가 되고 있는 비인가 AP의 유형을 보이고 있다.



(그림 1) 비인가 AP 유형
(Figure 1) Rogue AP Types

3.1 직접 연결 비인가 AP(유형 1 RAP)

그림 1에서 보는 것처럼 유형 1 비인가 AP(type 1 RAP)는 기관의 LAN에 유선으로 연결된, 직접 연결 비인가 AP(directly connected RAP)이다. 직접 연결 비인가 AP는 기관의 LAN 스위치에 접근이 가능한 내부 사용자에 의해 주로 설치되고, 관리자의 승인 없이 자신의 업무적 필요에 따라 기관의 보안 정책과 무관하게 설치될 수도 있고, 악의적인 목적으로 내부 사용자의 접근을 유도하기 위해 설치될 수도 있다. 악의적인 내부 사용자에 의해 설치되는 후자의 유형 1 비인가 AP는 SSID와 MAC 주소가 인가 AP와 동일하게 스푸핑(spoofing)됨으로써 사용자가 의심 없이 접근하게 되고, 따라서 보안상 심각한 위협에 처할 수 있으므로 반드시 탐지하여 사용자의 접근을 차단할 필요가 있다.

3.2 간접 연결 비인가 AP(유형 2 RAP)

유형 2 비인가 AP(type 2 RAP)는 기관의 LAN에 연결된 정상 AP에 와이파이로 연결된, 간접 연결 비인가 AP(indirectly connected RAP)이다. 간접 연결 비인가 AP는 2개의 와이파이 NIC(Network Interface Card)를 가진 노트북 등을 통해 쉽게 구현될 수 있고, 내부 사용자뿐만 아니라 와이파이 접근 권한을 확보한 악의적인 외부 공격자에 의해서 설치될 수도 있다. 악의적인 내부 또는 외부 공격자에 의해 SSID와 MAC 주소가 스푸핑된 비인가 AP는 사용자에 의해 식별되기가 어려울 뿐만 아니라, 스위치 포트에 연결되지 않기 때문에 관리자에 의해 탐지되기도 쉽지 않아 더욱 위협적인 비인가 AP가 될 수 있다.

3.3 외부 연결 비인가 AP(유형 3 RAP)

유형 3 비인가 AP(type 3 RAP)는 외부의 네트워크에 연결된, 외부 연결 비인가 AP(externally connected RAP)이다. 외부 네트워크는 기관내부의 대부분의 장소에서 접근이 가능한 3G 또는 LTE 이동 통신망이 일반적으로 사용되고, 이 경우 비인가 AP는 테더링 기능 등을 통해 스마트폰에 구현되는 것이 일반적이다. 공격자는 기관 내부의 네트워크를 접근할 필요가 없이 자신의 스마트폰을 사용하여 어디에서든지 비인가 AP를 쉽게 설치할 수 있다. 따라서 유형 3 비인가 AP는 유형 1과 유형 2의 비인가 AP에 비해 더욱 위협적이라 할 수 있다. 유형 1과 유형 2의 비인가 AP와 마찬가지로 유형 3 비인가 AP도 SSID와 MAC 주소 스푸핑을 통해 정상 AP를 가장하여 사용자의 접속을 유도하는 것이 보편적이다.

4. DHCP 스누핑 기반 비인가 AP 탐지 알고리즘

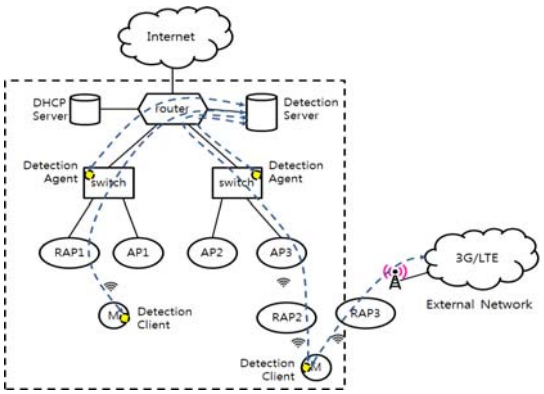
4.1 개념

본 논문에서 제시하는 비인가 AP 탐지 알고리즘은 인가된 AP 설치 시에 수집되는 정보와, 와이파이 단말(M)이 와이파이를 접속하고 DHCP 서버를 통해 IP 주소를 할당받을 때 AP가 연결된 스위치에서 수집되는 DHCP 스누핑 정보를 사용하여, 와이파이 단말이 인가된 AP를 통해 IP 주소를 할당받았는지 여부를 확인함으로써, 현재 접속된 AP가 인가 AP 또는 비인가 AP인지를 판정한다. 만약 와이파이 단말이 인가된 AP를 통해 IP 주소를 할당받았다면 다음 두 가지 사항이 충족되어야 한다. 첫째, 와이파이 단말이 접속한 AP의 MAC 주소는 반드시 AP 설치 정보에 포함되어 있어야 한다. 둘째, 와이파이 단말에 할당된 IP 주소는 와이파이 단말이 접속한 AP가 연결된 스위치 ID와 포트 ID에 대응되는 DHCP 스누핑 정보에 반드시 포함되어 있어야 한다. 만약 둘 중 하나라도 충족되지 않는 경우 와이파이 단말이 접속한 AP는 비인가 AP로 판정된다.

와이파이 단말이 IP 주소를 할당받았음에도 불구하고 IP 주소에 대응되는 DHCP 스누핑 정보가 없다면, 이는 해당 IP 주소가 단말이 소속한 기관의 LAN이 아닌 다른 네트워크(예, 3G/LTE)에 의해 할당되었음을 의미하므로, 와이파이 단말은 외부 연결 비인가 AP(유형 3 RAP)에 접속하고 있음을 의미하는 것이다. 와이파이 단말이 할당받은 IP 주소에 대응되는 DHCP 스누핑 정보가 존재하다라도, AP 설치 정보에서 IP 주소가 할당된 스위치의 포트에 와이파이 단말이 접속한 AP가 설치되어 있지 않은 것으로 나타난다면, 해당 와이파이 단말은 소속 기관의 LAN에 연결되어 있지만 정상적으로 인가를 받고 설치되지 않은 직접 연결 비인가 AP(유형 1 RAP)에 접속하고 있음을 의미한다. 와이파이 단말이 할당받은 IP 주소에 대응되는 스누핑 정보가 존재하고, IP 주소가 할당된 스위치의 포트에 와이파이 단말이 접속한 AP가 설치되어 있더라도, 해당 포트에 설치된 AP의 MAC 주소와 와이파이 단말이 접속한 AP의 MAC 주소가 동일하지 않다면, 와이파이 단말은 해당 포트에 연결된 인가 AP에 와이파이로 연결된 간접 연결 비인가 AP(유형 2 RAP)에 접속하고 있음을 의미한다. 비인가 AP가 자신이 접속된 AP의 MAC 주소와 같은 주소로 스푸핑할 수 없기 때문에 인가 AP에 와아파이로 접속된 비인가 AP가 MAC 주소를 스푸핑하더라도 이 관계가 성립한다.

4.2 시스템 구성

제안된 비인가 AP 탐지 알고리즘을 수행하기 위한 시스템의 구성은 그림 2와 같다. 그림 2에서 DHCP 서버의 위치는 논리적인 것으로 물리적으로 라우터에 구현되거나 별도의 서버로 구현될 수 있다.



(그림 2) 비인가 AP 탐지 시스템 구성
(Figure 2) System Configuration of Rogue AP Detection

본 알고리즘이 수행되기 위해서는 와이파이 단말이 비인가 AP 탐지 클라이언트(DC-Detection Client)를 가지고, AP가 접속된 스위치는 비인가 AP 탐지 에이전트(DA-Detection Agent), 그리고 기관의 LAN에는 비인가 AP 탐지 서버(DS-Detection Server)가 필요하다. DC는 와이파이 접속 시에 접속된 AP의 정보(SSID, MAC 주소, 보안 정책 등)와 할당받은 IP 주소를 DS에게 전송하고, 접속한 AP가 인가된 AP인지 아니면 비인가 AP인지를 DS로부터 통보받는다. DA는 해당 스위치의 DHCP 스누핑 정보 갱신 내용을 DS에게 즉시 전송한다. DA에 의해 수집되고 DS에 의해 관리되는 DHCP 스누핑 정보는 표 1과 같이 와이파이 단말에게 할당되는 IP 주소(Client IP Addr), 와이파이 단말의 MAC 주소(Client MAC Addr), DHCP 서버의 IP 주소(Server IP Addr), 스위치 ID(Switch ID), 그리고 포트 ID(Port ID)이다.

(표 1) DHCP 스누핑 정보
(Table 1) DHCP snooping information

Client IP Addr	Client MAC Addr	Server IP Addr	Switch ID	Port ID
192.168.10.5	00e0.1865.d3a6	192.168.10.254	10.01a3.23d4.54df	1.0.10
...	...	...	...	...

DS는 DC 및 DA와 통신하며 DC가 접속한 AP가 비인가 AP인지를 판정하여 DC에게 통보하는 역할을 수행한다. DS는 인가된 AP 설치 시에 표 2와 같이 SSID와 AP MAC 주소, AP의 보안 정책, AP가 연결된 스위치 ID와 포트 ID 등의 설치 정보를 유지한다.

(표 2) AP 설치 정보
(Table 2) AP installation information

SSID	AP MAC Addr	Security Policy	Switch ID	Port ID
tech_ac	05e4.4fa5.23ac	...	10.01a3.23d4.54df	1.0.10
tech_ac	05e4.4fbg.12da	...	10.45ed.fa3c.256d	2.0.19
...	...	...	...	...

DS는 DC가 전송하는 AP MAC 주소에 대응되는 AP 설치 정보의 스위치 ID와 포트 ID를 추출한다. 그리고 DS는 DHCP 스누핑 정보로부터 해당 스위치 ID와 포트 ID에 할당된 IP 주소를 추출한다. 마지막으로 DS는 스누핑 정보로부터 추출된 IP 주소와 DC가 할당받은 IP 주소를 비교함으로써 와이파이 단말이 접속한 AP의 비인가 AP 여부를 판단한다. 대부분의 소속 AP가 SSID의 네트워크 이름을 공유하는 엔터프라이즈 LAN 환경에서 DS의 도메인 이름은 DS가 관리하는 AP의 SSID의 네트워크 이름과 연계되어 설정됨으로써 와이파이 단말이 별도의 설정 없이 쉽게 접속할 수 있게 한다. 예를 들어 SSID의 네트워크 이름이 tech_ac이고 기관의 도메인 이름이 abc.com인 경우 DS는 tech_ac.abc.com 도메인 이름을 가짐으로써, AP를 접속한 와아파이 단말이 자동으로 DS를 접속할 수 있게 한다. AP들의 SSID가 다수의 네트워크 이름을 가지는 경우에도 대응되는 DS의 도메인 이름을 다수 설정하여 사용할 수 있다.

4.3 알고리즘

본 논문이 제안하는 비인가 AP 탐지 알고리즘은 AP를 접속하는 와이파이 단말(M)의 DC가 접속한 AP의 SSID와 MAC 주소를 DS에게 전달함으로써 개시된다. 알고리즘은 1단계로 SSID 또는 MAC 주소를 스푸핑하지 않은 비인가 AP(NS-RAP, Non-Spoofed RAP)인지를 탐지하고, 두 번째 단계로 스푸핑된 유형 3 비인가 AP(S3-RAP, Spoofed-type3 RAP)를 탐지하고, 세 번째 단계로 스푸핑된 유형 1 비인가 AP(S1-RAP, Spoofed-type3 RAP)를 탐지하고, 네 번째 단계로 스푸핑된 유형 2 비인가 AP(S3-RAP, Spoofed-type2 RAP)를 탐지한다. 4 단계의 비인가 탐지 알고리즘을 무사히 통과하면 해당 AP는 인가 AP로 판정되어 DC에게 통보되고, 해당 사용자에게 알려진다. 비인가 AP 탐지 알고리즘은 다음과 같다.

0단계: 와이파이 단말의 RAP 탐지 시작

DC는 DHCP 서버로부터 할당받은 IP 주소와 접속한 AP의 SSID와 MAC 주소를 DS에게 전송한다. 기관의 보안 정책에 따라 접속한 AP의 보안 정책(암호화 기법, 인증 기법 등)을 DS에게 전송하게 할 수도 있다.

1단계: NS-RAP 탐지(Non-Spoofed Rogue AP Detection)

DS는 DC가 전송한 SSID와 AP MAC 주소를 AP 설치 정보와 비교한다. AP 설치 정보에 일치하는 SSID 또는 AP MAC 주소가 존재하지 않으면, 해당 AP를 스푸핑되지 않은 비인가 AP(NS-RAP)로 판정한다.

2단계: S3-RAP 탐지(Spoofed-type3 Rogue AP Detection)

DS는 DHCP 스누핑 정보로부터 DC의 IP 주소에 대응되는 스위치 ID와 포트 ID를 탐색한다. 만약 대응되는 스위치 ID와 포트 ID가 존재하지 않으면 해당 IP 주소는 기관의 LAN이 아닌 외부 네트워크에서 할당된 IP 주소이므로 외부 연결 비인가 AP(S3-RAP)로 판정한다.

3단계: S1-RAP 탐지(Spoofed-type1 Rogue AP Detection)

DS는 AP 설치 정보보부터 2단계에서 탐색한 스위치 ID와 포트 ID에 대응되는 AP MAC 주소를 탐색한다. 만약 대응되는 AP MAC 주소가 존재하지 않으면, 와이파이 단말이 접속한 AP는 기관의 LAN에 연결된 AP는 맞지만 정상적으로 설치된 인가된 AP가 아니므로 직접 연결 비인가 AP(S1-RAP)로 판정한다.

4단계: S2-RAP 탐지Spoofed-type2 Rogue AP Detection)

3단계에서 탐색한 AP MAC 주소는 와이파이 단말에 IP 주소를 할당한 AP의 MAC 주소이다. DS는 이 AP MAC 주소가 DC가 전송한 AP MAC 주소와 같은지를 비교한다. 만약 같지 않으면 와이파이 단말이 접속한 AP는 인가된 AP에 와이파이로 접속된 비인가 AP, 즉 간접 연결된 비인가 AP(S2-RAP)로 판정된다.

5단계: 판정 결과 통보

1-4단계 모두를 통과하면 DS는 DC가 접속한 AP를 인가 AP로 판정한다. DS는 판정 결과를 DC에게 통보하고 DC는 사용자에게 적절하게 알린다.

5. 검증 및 평가

5.1 검증

특정 와이파이 단말(Mi)이 SSID 또는 MAC 주소가 인가 AP로 스푸핑되지 않은 단순한 비인가 AP(NS-RAP)를 접속하는 경우, 와이파이 단말이 접속한 AP의 SSID와 MAC 주소는 AP 설치 정보에 존재할 수가 없다. 따라서 식 1 또는 식 2와 같은 관계 확인을 통해 비인가 AP임을 쉽게 검증할 수 있다. 식에서 {x(y)[z]}의 의미는 z에 의해 색인되는 x 정보의 y 필드 전체를 의미하고, A.B는 A의 B 정보를 의미한다. accessed, snooped, 그리고 installed는 각각 접근대상의 정보, 스누핑 정보, 그리고 설치 정보를 나타낸다. 결과적으로 본 논문에서 제안한 비인가 AP 탐지 알고리즘을 통해 어떤 유형의 비인가 AP라 할지라도 만약 해당 AP가 스푸핑하지 않은 다순 AP라면 모두 탐지될 수 있음을 알 수 있다.

$$M_i.accessed(AP.SSID) \notin \{installed(AP.SSID)\} \quad (1)$$

$$M_i.accessed(AP.MAC-addr) \notin \{installed(AP.MAC-addr)\} \quad (2)$$

특정 와이파이 단말(Mi)이 기관 내부의 인가 AP의 SSID와 MAC 주소로 스푸핑되어 있으나 기관의 LAN이 아닌 외부의 네트워크에 연결되어 있는 비인가 AP를 접속하는 경우를 가정해 보자. 그림 2의 RAP3과 같이 3G/LTE 네트워크에 연결된 스마트폰으로 구현되고 스푸핑된 비인가 AP(S3-RAP)가 여기에 해당된다. 이 경우 와이파이 단말(Mi)에 할당된 IP 주소(Mi.accessed(IP-addr))는 외부 네트워크에서 할당되었으므로 기관의 LAN의 스위치에서 수집한 DHCP 스누핑 정보에 포함될 수가 없다. 따라서 식 3과 같이 와이파이 단말(Mi)에 할당된 IP 주소를 색인으로 DHCP 스누핑 정보의 스위치 ID와 포트 ID를 검색한 결과(snooped(switchID.portID)[Mi.accessed(IP-addr)])는 null이 될 수밖에 없다. 결과적으로 본 논문에서 제안한 비인가 AP 탐지 알고리즘을 통해 유형 3의 비인가 AP는 스푸핑한 경우라 할지라도 모두 탐지될 수 있음을 알 수 있다.

$$\begin{Bmatrix} snooped(switchID.portID)[\\ M_i.accessed(IP-addr)] \end{Bmatrix} = \omega(\text{null}) \quad (3)$$

특정 와이파이 단말(Mi)이 기관 내부의 인가 AP의 SSID와 MAC 주소로 스푸핑되어 있고, 기관의 LAN의 스위치에 직접 연결되어 있는 비인가 AP를 접속하는 경우를 가정해 보자. 그림 2의 RAP1(S1-RAP)이 여기에 해당된다. 이 경우 와이파이 단말(Mi)이 기관의 LAN을 통해 IP 주소를 할당받으므로 식 4와 같이 DHCP 스누핑 정보에 해당 IP 주소를 할당한 스위치 ID와 포트 ID가 존재한다. 그러나 해당 스위치 ID와 포트 ID에 인가 AP가 설치되어 있지 않으므로 식 5와 같이 해당 스위치 ID와 포트 ID를 색인으로 AP 설치 정보를 검색하면 그 결과(installed(AP.MAC-addr)[snooped(switchID.portID)[Mi.accessed(IP-addr)]])는 null이 될 수밖에 없다. 결과적으로 본 논문에서 제안한 비인가 AP 탐지 알고리즘을 통해 유형 1의 비인가 AP는 스푸핑된 경우라 할지라도 모두 탐지될 수 있음을 알 수 있다.

$$\begin{Bmatrix} snooped(switchID.portID)[\\ M_i.accessed(IP-addr)] \end{Bmatrix} \neq \omega(\text{null}) \quad (4)$$

&

$$\begin{Bmatrix} installed(AP.MAC-addr)[\\ snooped(switchID.portID)[\\ M_i.accessed(IP-addr)]] \end{Bmatrix} = \omega(\text{null}) \quad (5)$$

특정 와이파이 단말(Mi)이 기관 내부의 인가 AP의 SSID와 MAC 주소로 스푸핑되어 있고, 기관의 LAN의 스위치에 직접 연결되어 있는 인가 AP에 와이파이로 연결된 비인가 AP를 접속하는 경우를 가정해 보자. 그림 2의 RAP2(S2-RAP)가 여기에 해당된다. 이 경우 식 4와 같이 DHCP 스누핑 정보에 해당 IP 주소를 할당한 스위치 ID와 포트 ID가 존재하고, 해당 스위치 ID와 포트 ID에 인가 AP가 설치되어 있으므로 식 6와 같이 해당 스위치 ID와 포트 ID를 색인으로 AP 설치 정보를 검색하면 그 결과도 존재한다. 그러나 와이파이 단말이 접속한 비인가 AP의 MAC 주소가 기관의 인가 AP의 MAC 주소로 스푸핑되더라도, 같은 MAC 주소를 가진 장치 간에 통신이 불가능하므로 자신이 접속된 인가 AP의 MAC 주소로 스푸핑될 수는 없다. 따라서 식 7과 같이 와아파이 단말(Mi)에 IP 주소를 할당한 스위치 ID와 포트 ID에 설치된 AP의 MAC 주소는 와이파이 단말(Mi)이 접속한 AP의 MAC 주소와 같을 수가 없다. 결과적으로 본 논문에서 제안한 비인가 AP 탐지 알고리즘을 통해 유형 2의 비인가 AP는 스푸핑한 경우라 할지라도 모두 탐지될 수 있음을 알 수 있다.

$$\begin{Bmatrix} installed(AP.MAC-addr)[\\ snooped(switchID.portID)[\\ M_i.accessed(IP-addr)]] \end{Bmatrix} \neq \omega(\text{null}) \quad (6)$$

&

$$installed(AP.MAC-addr)[\\ snooped(switchID.portID)[\\ M_i.accessed(IP-addr)]] \\ \neq M_i.accessed(AP.MAC-addr) \quad (7)$$

5.2 평가

본 논문이 제안하는 DHCP 스누핑 기반의 비인가 AP 탐지 솔루션은 별도의 탐지 센서를 요구하지 않고 간단한 탐지 프로토콜을 S/W로 구현할 수 있으므로, 기존의 WIPS와 비교하여 저비용으로 구축이 가능한 장점이 있다. 2015년 말 현재 1대의 탐지 서버와 1대의 탐지 센서로 구성되는 WIPS를 구축하더라도 약 16,000달러 이상의 비용이 소요되고, 만약 100개 이상의 탐지 센서를 필요로 하는 규모가 큰 기관의 경우 약 100,000달러 이상의 비용을 필요로 할 것이다. 반면 제안된 솔루션의 경우 탐지 서버를 S/W로 구현할 일반적인 서버만 요구하므로 훨씬 저비용으로 구현이 가능하다.

와이파이 트래픽의 지연시간 특성 등 타이밍 정보와 GPS 위치 정보 등을 이용하는 기존의 비인가 AP 탐지 기법들은, 네트워크의 상황과 와이파이 단말의 상황에 따라 측정 결과가 달라질 수 있으므로 비인가 AP 탐지에 오류가 발생할 수 있다. 반면 제안된 탐지 알고리즘은 와이파이 단말이 할당받은 IP 주소와 접속한 AP의 정보를 AP 설치 정보와 DHCP 스누핑 정보와 비교하여 비인가 AP를 판정하므로 탐지오류 발생의 여지가 없다. 그리고 기존의 타이밍 정보와 위치 정보를 사용하는 솔루션들은 의미있는 정보를 얻기 위해 다수의 측정을 필요로 하고, 이는 탐지 시간 지연을 가져오는 요소가 된다. 반면 제안된 솔루션은 비인가 AP 탐지를 위해 와이파이 단말이 탐지 서버와 한 번의 메시지 교환만 필요로 하므로 매우 신속하게 비인가 AP를 탐지할 수 있게 한다.

제안된 비인가 AP 탐지 알고리즘은 와이파이 단말에 대한 사전 등록 등의 절차 없이 접속하고자 하는 와이파이 네트워크를 운영하는 특정 기관의 탐지 서버를 접속하기만 하면 된다. 그리고 탐지 서버의 도메인 이름을 SSID와 연계시킴으로써 자동으로 탐지 서버를 접근할 수 있다. 따라서 제안된 기법은 어떤 기관의 와이파이 네트워크에서든 와이파이 사용자가 쉽게 사용할 수 있게 한다. 즉, 사용자 편의성을 높이는 장점이 있다.

6. 결론 및 향후 연구

악의적인 공격자가 설치한 비인가 AP 접속이 와이파이 사용자를 스니핑, 피싱, 또는 파밍 공격과 같은 심각한 사이버 공격에 노출시킬 수 있음에도 불구하고, 비용 상의 문제와 기술적인 문제 등으로 인해 대부분의 와이파이 네트워크 환경에서 비인가 AP 탐지와 사용자에 대한 경고 서비스는 아직 제대로 제공되고 있지 않다. 오히려 스마트폰 기반의 비인가 AP 기술의 보급 등으로 인해 비인가 AP에 의한 와이파이 보안 위협은 더욱 증가하고 있는 현실이다. 본 논문은 현재 대부분의 LAN 스위치에서 제공하고 있는 DHCP 스푸핑 기능을 응용하여 간단한 프로토콜을 통해 쉽게 구현할 수 있는 비인가 AP 탐지와 와이파이 사용자에 대한 경고 서비스를 제공하는 알고리즘을 제시하였다. 제안된 알고리즘은 저비용 구현 가능성, 탐지의 정확성과 신속성, 그리고 사용자 편의성 측면에서 기존의 비인가 AP 탐지 기법들과 차별화된다.

본 논문이 제안한 비인가 AP 탐지 알고리즘이 스위치 기반의 모든 LAN 환경에서 보다 용이하게 구현되기 위해서는, 제안된 알고리즘을 기반으로 DHCP 스누핑 기반의 비인가 AP 탐지 프로토콜이 표준화될 필요가 있다. 향후 DHCP 스누핑 기반의 비인가 AP 탐지 프로토콜 개발과 프로토콜의 성능 비교 분석 등에 연구를 집중할 계획이다.

참 고 문 헌 (Reference)

[1] R. Beyah and A. Venkataraman, "Rogue-Access-Point Detection Challenges, Solutions, and Future Directions," *IEEE Security and Privacy*, Sept./Oct 2011, pp. 56-61. http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5963632

[2] Motorola, "Solutions for Detecting and Eliminating Rogue Wireless Networks," *White Paper*, Oct. 2011. http://www.opticalphusion.com/downloads/products/networks/airdefense/CS.pdf

[3] M. Kim, J. Mun, S. Jung, and Y. Kim, "A Mobile Device-based Mobile AP Detection Scheme using NAT Behavior," *Proceedings of 2013 International Conference on IT Convergence and Security*, 16-18

Dec. 2013, pp. 1-4.
http://ieeexplore.ieee.org/xpl/articleDetails.jsp?reload=true&arnumber=6717778

[4] L. Watkins, R. Beyah, and C. Corbett, "A Passive Approach to Rogue Access point Detection," *Proceedings of IEEE Globecom 2007*, 26-30 Nov. 2007, pp. 355-360.
http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=4410983

[5] http://www.airtightnetworks.com/

[6] http://meraki.cisco.com/technologies/air-marshal-wips/

[7] H. Han, B. Sheng, C. C. Tan, Q. Li, and S. Lu, "A Timing-based Scheme for Rogue AP Detection," *IEEE Transactions on Parallel and Distributed Systems,* Vol. 22, No. 11, Nov. 2011, pp. 1012-1925
http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6007016

[8] J. Lee, S. Lee, and J. Moon, "Detecting Rogue AP using k-SVM method," *Journal of The Korea Institue of Information Security and Cryptology*, Vol. 24, No. 1, Feb 2014, pp. 87-95
http://ocean.kisti.re.kr/downfile/volume/kiisc/JBBHCB/2014/v24n1/JBBHCB_2014_v24n1_87.pdf

[9] K. Kao, T. Yeo, W. Yong, and H. Chen, "A Location-aware Rogue Ap Detection System Based on Wireless Packet Sniffing of Sensor APs," *Proceedings of The 2011 ACM Symposium on Applied Computing*, Mar. 2011, pp. 32-36
http://dl.acm.org/citation.cfm?id=1982195

[10] J. Park, M. Park, and S. Jung, "A Whitelist-based Scheme for Detecting and Preventing Unauthorized AP Access Using Mobile Device," *Journal of KICS*, Vol. 38B, No.8, Aug. 2013, pp. 632-640
http://www.readcube.com/articles/10.7840%2Fkics.2013.38B.8.632

◐ 저 자 소 개 ◑

박 승 철 (Seungchul Park)
1985년 서울대학교 계산통계학과 졸업(학사)
1987년 KAIST 전산학과 졸업(석사)
2006년 서울대학교 대학원 컴퓨터공학과 졸업(박사)
2004～현재 한국기술교육대학교 컴퓨터공학부 교수
관심분야 : 컴퓨터 네트워크. 네트워크 보안, 멀티미디어 네트워크.
E-mail : scpark@koreatech.ac.kr