비인가 모바일 AP 탐지를 위한 채널 스캔의 구현에 관한 연구

황재룡*

*해군사관학교

An Implementation of Wireless Channel Scanning for Unauthorized Mobile APs Detection

Jaeryong Hwang*

*Korea Naval Academy

E-mail : jhwang@navy.ac.kr

요 약

모바일 WiFi 핫스팟은 비인가 WiFi 서비스 제한구역에서 내부자료 유출 및 수집과 같은 보안상 문제점을 일으킨다. 이에 따라 본 논문에서는 무선랜 드라이버를 수정하여 주기적으로 무선 채널을 탐색하는 탐지기를 구현한다.

ABSTRACT

On the area which is restricted an unauthorized WiFi service, mobile WiFi hotspot causes security problems like leaking and gathering internal data. In this paper, we modify a wireless lan driver and implement a detector that periodically scans the wireless channels.

키워드

모바일, WiFi, 핫스팟, 주기적 스캔

Ⅰ. 서 론

WiFi 서비스의 대중화와 모바일 단말 기술의 비약적인 발전은 비인가 WiFi 서비스를 제한하는 공간에서 임의의 사용자들에 의해 모바일 WiFi 핫스팟 형성을 가능하게 한다. Android 및 iOS 기반의 스마트 기기들은 3G 및 LTE의 이동통신망과 Wi-Fi 인터페이스를 이용하여 쉽게 모바일 WiFi 핫스팟을 구성할 수 있다. 이와 같은 기술을 사용하여 모바일 WiFi 핫스팟이 언제 어떤 장소에서든지 쉽게 구성되어 주변 WiFi 기기들에 인터넷 접속을 제공해 줄 수 있다. 따라서 비인가 WiFi 서비스가 제한되는 공간에서도 노트북이나 스마트폰과 같은 기기를 보유한 사용자들은 자신이 필요한 위치에서 언제든지 쉽고 빠르게 WiFi를 사용하여 인터넷 접속이 가능하다.

비인가 모바일 WiFi 핫스팟은 내부자료 유출과 같은 보안상 문제를 야기할 수 있다. 불법 정보통신 장비를 반입하여 손쉽게 외부 인터넷으로 자료유출이 가능하다. 뿐만 아니라 WiFi의 SSID(service set identifier)를 인가된 WiFi 서비스인 것처럼 위장하게 되면 인터넷 접속 트래픽을 모으고 훔쳐보는 것이 가능해진다[1].

따라서 본 논문에서는 비인가 WiFi 서비스를 제공하는 무선 AP를 탐지하고자 한다. 이를 위하여 리눅스 기반의 무선랜 드라이브를 수정하여 무선 채널을 주기적으로 스캔하도록 구현한다. Madwifi[2] 드라이버는 오픈 소스로서 사용자들의 요구사항을 반영하여 수정이 가능하다. 또한 다양한 무선 채널 스캔 방법을 제공하고 있다. bgscan(background scan)은 빠른 핸드오프를 위하여 현재 연결되어 있는 AP와의 연결을 유지한 채 다른 무선 채널 탐색을 통하여 새로운 AP를 발견하기 위해 사용된다. 본 논문에서는 bgscan의 일부기능을 조정하여 주기적으로 무선 채널 탐색을 통해 비인가 무선 AP의 존재여부를 확인한다. 테스트베드 구축을 통하여 무선 채널상의 전송 데이터 확인을 통하여 주기적으로 무선 채널을 탐색하는 것을 확인할 수 있다.

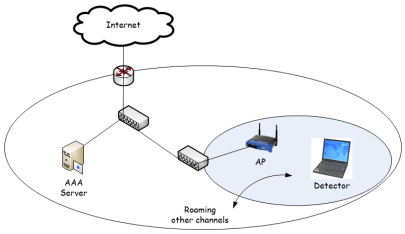

그림 1. 시스템 모델

II. 비인가 모바일 AP 탐지기 구현

본 논문에서는 비인가 WiFi 서비스가 제한되는 시나리오를 고려한다. 비인가 모바일 AP를 탐지하기 위하여 그림 1과 같이 탐지기(Detector)는 인가된 WiFi AP에 연결되어 있으며 무선 채널의 주기적인 스캔을 통하여 획득한 AP의 정보(SSID, MAC address, IP address)를 AAA 서버(authentication authorization accounting)와 데이터를 주고받으며 인가 여부를 확인한다.

비인가 무선 AP 탐지를 위하여 리눅스 기반의 WiFi 탐지기를 구현한다. 오픈 소스 기반의 무선랜 드라이버인 Madwifi는 수정이 가능하여 필요한 기능의 구현이 가능하다. 또한 다양한 무선 채널 스캔 방법을 제공한다. 따라서 본 논문에서는 주기적인 인가된 무선 AP와 연결되어 있는 상황에서 다른 무선 채널로의 주기적인 스캔을 실시하기 위하여 background scanning기법을 활용한다. 일반적인 무선 채널 스캔과 달리 bgscan모드에서는 일정 시간동안 AP로부터 데이터가 수신되지 않으면 WiFi 노드(client)는 드라이브에 캐시되어 있는 이웃채널에서 active 스캔을 실시한다. 그림 2는 bgscan의 일부를 수정하여 주기적으로 무선채널을 탐색하며 비인가 AP를 탐지하기 위하여 구현한 탐지기의 동작을 설명하고 있다. 탐지기를 나타내는 <client>는 연결되어 있는 AP와 데이터를 주고받다가 일정한 주기로 스캔 트리거에 의해 이웃 채널을 탐색한다. 이때 AP로부터 데이터 전송이 일어나지 않도록 하기 위하여 AP에게 power save on 메시지를 보내고, 자신으로부터 AP로 전송하기 위한 데이터는 큐에 보관한다. 지정된 채널에서 active/passive 스캔을 실시 후에 원래의 채널로 돌아와 AP에게 power save off 메시지를 보내고 자신의 큐에 담겨있던 메시지를 AP로 전송한다. 이때 원래의 채널로 돌아오게 되면 탐색한 채널에서 수집한 정보를 AAA서버로 보내어 인가여부를 판별한다. 이와는 달리 WiFi 노드와 연결되어 있는 인가된 AP는 데이터 전송중 WiFi 노드(client)노드로부터 power save on 메시지를 받게 되면 별도의 큐에 데이터를 저장한다. 그러다 power save off 메시지를 받게 되면 저장되어 있는 데이터를 WiFi 노드에게 전송한다.

구현한 탐지기의 성능을 확인하기 위하여 인가된 AP로부터 WiFi노드로 데이터를 전송하는 상황에서 WiFi 노드의 동작을 확인하였다. 이를 위하여 Wireshark[3]을 이용하여 WiFi 노드와 AP의 데이터 전송내용을 살펴보았다. 그림 3에서 보는 바와 같이 WiFi 노드는 AP에게 power save on 메시지를 보낸 후 이웃 채널로 스위치 함에 따라 AP로부터 전송되는 프레임을 수신하지 못하여 AP가 계속해서 프레임을 재전송하는 것을 확인할 수 있다. 그러다 다시 원래 채널로 돌아와 power save off 메세지를 보낸 후에 정상적으로 다시 데이터 전송이 이루어짐을 확인할 수 있다.

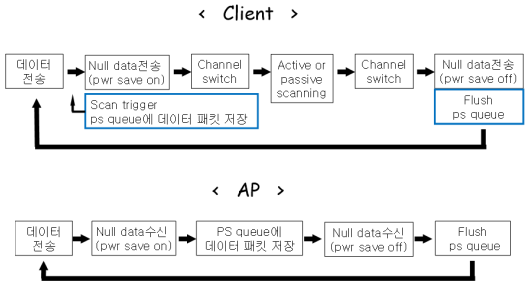

그림 2. 무선채널 탐색 동작

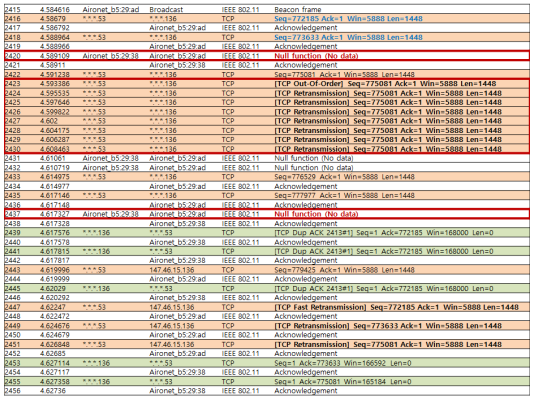

그림 3. 무선 채널 탐색 결과

III. 결 론

본 논문에서는 비인가 WiFi 서비스가 제한되는 공간에서 모바일 WiFi 핫스팟은 내부자료 수집 및 유출을 용이하게 함에 따라 리눅스 기반의 무선랜을 수정하여 주기적으로 무선 채널을 탐색하여 비인가 무선 AP 탐지를 구현하였다.

참고문헌

[1] B. Potter, "Wireless Hotspots: Petri Dish of Wireless Security", ACM Communications, vol. 6, 2006.

[2] Multiband Atheros Driver for WiFi, http://www.madwifi.org/.

[3] Wireshark http://www.wireshark.org