Monitor Mode를 이용한 모바일 디바이스 사용자 추적 방안에 대한 연구

김건용* 김형철** 이원용** 유명성** 박강민**
정재완** 오동현** 심기욱** 이경문**

*KITRI BoB - Team G0Host **KITRI BoB - Team G0Host

A Study on User Device Tracking Method Using Monitor Mode

Geon Yong Kim* Hyeong Cheol Kim** Won Yong Lee**
Myoung Seoung You** Kang Min Park** Jae Wan Jeong**
Dong Hyeon Oh** Ki Wook Shim** Kyoung Moon Lee**

*KITRI BoB - Team G0Host **KITRI BoB - Team G0Host

요 약

Wi-Fi가 지원되는 Station들은 이전에 접속하였던 Access Point에 빠르게 접근하거나, Hidden Wifi를 찾기 위해서 주기적으로 자신의 하드웨어 주소 및 신호 세기를 802.11 Probe Request type으로 Broadcast 하여 AP에 전달한다. 이러한 기술로 인해 해당 Station 주위에서 Monitor Mode Packet 수집 장치를 이용하여 Sniffing 할 수 있고, 이를 이용해 모바일 디바이스 사용자가 어느 시점에 특정 공간에 위치해 있었는지를 추정할 수 있다. 본 논문에서는 이러한 부분에 초점을 맞추어 비식별 MAC Address를 이용하여 타깃을 추적할 방안을 제시한다. 또한, 이러한 기능을 응용하여 발생할 수 있는 시나리오들을 제시하고자 한다.

I. 서론

1.1 연구 배경

Wi-Fi는 최근 단거리 통신의 핵심 솔루션이며, 이용 빈도가 증가하는 추세이다. 특히, 최근의 모바일 디바이스는 대부분 Wi-Fi 솔루션을 탑재하여 출시하고 있다. Wi-Fi 통신은 802.11i 보안 표준인 AES 암호화 방식을 이용한 WPA2를 주로 사용하여 암호화된 통신을 하고 있다. 하지만, AP와 Station의 연결을 위해서 필요한 Packet을 주고받는 경우, 이 과정에서 각각의 AP, Station 구분을 위한 고유 구분자들은 암호화가 이루어지지 않고 Plain Text로 전송되기 때문에 이를 수집하여 재식별한다면 각 장치를 소유한 사람을 식별할 수 있다.

이러한 개인정보 수집은 Wi-Fi를 사용하는 모든 모바일 디바이스 사용자에게 이루어질 수 있다. Wi-Fi 모드를 활성화하면 AP 검색을 위해서 Station Device의 인터페이스는 AP를 향해서 Broadcast Probe Request Packet을 전송하고, 해당 과정에서 고유 식별자인 MAC Address가 유출된다. 이를 이용한다면, Signal Strength를 이용하여 사용자를 추적할 수 있고, 모니터 모드 Packet Sniffer가 미리 여러 곳에 설치되어 있다면 특정 MAC Address 소유자의 이동 경로를 추적할 수 있다.

1.2. 기술적 배경

Wi-Fi 는 Access Point(AP)와 이를 이용하는 Station으로 구성된다. AP와 Station은 상호간 Key를 생성하고, 암호화된 802.11 Frame Packet을 전송해 이를 Ethernet 형태로 변환하여 통신한다.

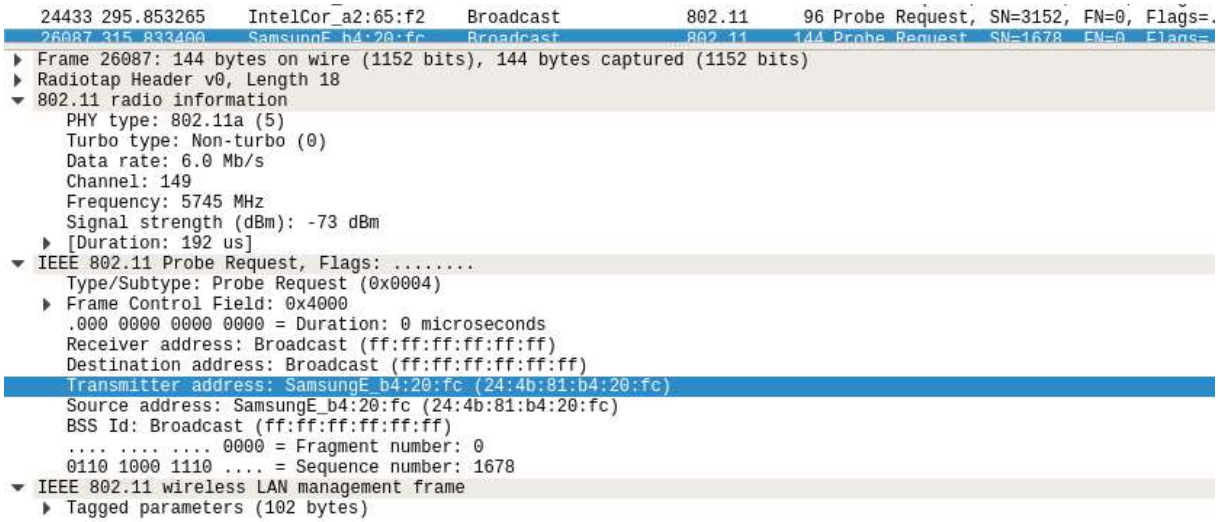

Fig 1. Probe Request Packet Sniffing with Wireshark

802.11 Frame은 그 이용 방식에 따라 관리 프레임, 제어 프레임, 데이터 프레임으로 나뉜다. 여기서 이용하는 것은 관리 프레임의 Subtype인 802.11 프로브 요청 프레임이다. 이는 찾기를 원하는 가까운 AP를 능동적으로 탐색하기 위해(802.11 Scanning), 주어진 주파수 채널 각각에 송출하도록 하는 프레임이다. 해당 프레임은 Frame Control, Duration, Destination Address, Source Address, BSSID, Sequence Control로 이루어진 프레임 헤더를 가진다[2]. 여기서 DA, SA는 각각 Station이 찾기를 원하는 AP의 하드웨어 주소, SA는 해당 Station의 하드웨어 주소를 의미한다. 따라서 SA를 파싱한다면 우리는 Probe Request를 보내는 AP 사용자의 MAC Address를 가져올 수 있다.

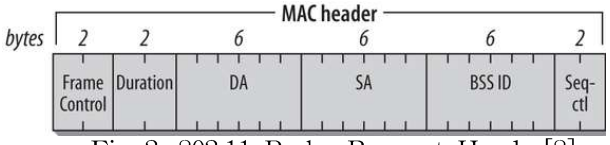

Fig 2. 802.11 Probe Request Header[8]

Monitor Mode 802.11 패킷을 잡기 위해서는 모니터 모드를 이용해야 한다. 우리가 기본적으로 이용하는 모드는 Managed Mode로, 많은 Access Point로 구성된 네트워크에 연결하여 AP와 직접 통신할 수 있도록 하는 모드이다[3]. 반면, Monitor Mode는 주위의 모든 패킷을 수신하여 보는 것으로, 이는 AP와 Station의 연결과는 상관없이 패킷을 수집할 수 있다[4].

이러한 프로그램은 대표적으로. Aircrack-ng의 Airodump-ng가 있다. 해당 프로그램은 Monitor Mode Adapter 주위에서 흘러 다니는 Monitor Mode Packet을 읽어 BSSID, ESSID, 암호화 방식 등을 보여주는 프로그램이다[7].

II. 연구 기술 활용 방안

위의 MAC 주소를 Parsing하는 것을 이용하여 Wireless Tracking을 할 수 있다. 여기서는 두 가지 추적 방안을 제시한다. 첫 번째 방식은 많은 장소에 Monitor Mode Adapter를 설치하고 수집된 MAC Address를 분석하여 인구 분석 통계를 내거나 특정 MAC Address를 가진 대상의 이동 경로를 추적할 수 있는 방법으로, 이를 Wireless Footprint라고 명명한다. 다른 방법은 하나의 Monitor Mode Adapter를 이용하여 단일 대상 혹은 단일 집단을 추적하는 방법으로, 이를 Wireless Tracking이라고 명명한다.

2.1 특정 지역의 유동 인구 추정

광범위한 지역에 Monitor Mode Adapter를 설치하여 여기서 가져온 MAC 주소를 이용해 특정 인물의 이동 경로를 추정하거나, 특정 지역의 유동 인구를 분석할 수 있다.

각 지점에 설치되는 Adapter에서는 802.11 패킷을 Sniffing 하여 Probe Request Frame을 필터링하고, Probe Request Frame에서 Source

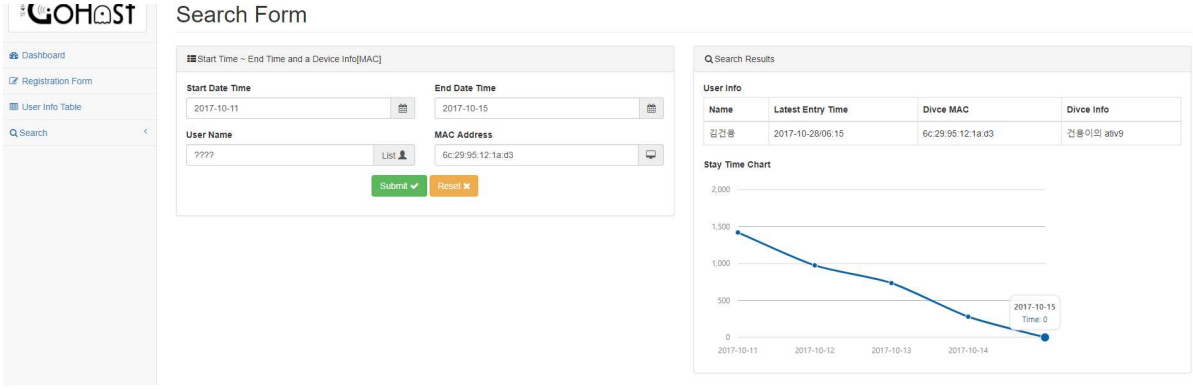

Fig 3. Wireless Footprint with Web GUI (Developed by Team G0Host)

Address를 Parsing하여 중앙 서버로 전송하도록 한다. 802.11 Frame Packet에서 가장 먼저 등장하는 Frame은 Radiotap Header이다. Radiotap Header에서 적절한 Signal Strength를 지정하여 해당 신호 세기보다 세기가 약하다면 valid packet이 아니라고 판단하고 이를 무시하도록 신호 세기에 대한 필터링을 걸어 준다. 또한, TimeStamp를 Parsing 하여 이를 날짜와 시간으로 변환하여 준다. 그 다음으로 오는 Frame은 IEEE 802.11 Frame으로, 여기서는 Probe Request Frame의 Source Address를 Parsing 하여 TimeStamp 정보와 함께 중앙 서버로 전송한다.

중앙 서버에서는 수집되는 Data를 Database에 저장한다. 어느 시점에 어떠한 MAC Address가 해당 위치에 있었는지 알리기 위해 Fig 3과 같이 CLI 혹은 GUI를 이용하여 이를 표현해 줄 수 있어야 한다.

위에서 제시한 기술을 통계적으로 활용할 수 있다. 대규모 집회나 콘서트 등 많은 사람이 드나드는 곳에서 유동 인구수를 추정해야 하는 경우 AP를 제공하여 사용할 수 있도록 하고 Unique MAC Address를 식별하여 얼마나 많은 인원이 그곳에 있었는지를 추정할 수 있다. 이를 상업적으로 활용할 수도 있다. Monitor Mode Adapter를 AP 근처에 설치하여 얼마나 많은 고객이 매장을 방문했고, 인기가 많은 지점과 인기가 떨어지는 지점을 점검할 수 있다. 이를 통해서 점포 위치를 변경하거나 점포를 교체하여 이익을 창출하도록 할 수 있다[9].

2.2 단일 대상에 대한 추적

단일 대상을 추적하고 싶은 경우, Wireless Footprint를 이용하지 않고, 직접 추적할 수 있는 방법이 있다. 기본적으로 Monitor Mode Packet Sniffier는 실시간으로 Packet을 Monitoring할 수 있다. 또한, RadioTap의 Signal Strength를 이용하여 해당 MAC Address 소유자와 자신이 대략 어느 정도 거리에 떨어져 있는지를 파악할 수 있다. 방법은 간단하다. 인파가 많은 곳에서는 끊임없이 수신되는 Source Address가 바뀐다. 그러나 추적하는 대상이 송신하는 Probe Request Packet은 그대로일 것이다. 이를 통해서 후보 그룹 군을 만들어 놓고, 신호 세기를 측정하여 어떤 MAC Address가 우리가 추적하고자 하는 인물의 것인지 찾아낸다. 이렇게 한다면 상대에게 들키지 않는 거리에서 계속해서 추적을 진행할 수 있다[6].

2.1의 방식과 혼합하여 이용하는 경우, 만약 Monitor Mode Adapter가 여러 군데 설치되었다는 가정을 한다면 이를 수사 목적으로 이용할 수 있다. CCTV 등으로 수배 대상자가 어떠한 곳에 있었는지 확인할 수 있으면, 해당 시간에 해당 위치에서 발생한 Probe Request Packet에서 Source Address를 추출한다. 그 후, 예상 도주 경로에서 발생한 Packet들을 확인하고 여기서 중복되는 Source Address를 식별하여 범인의 것으로 추정한다. 범인의 것으로 추정되는 MAC을 식별한다면 2.1의 방식과 2.2의 방식을 혼합하여 대상을 추적할 수 있다.

III. 결론

802.11 Packet을 이용하여 모바일 디바이스의 통신상에 담긴 비식별 개인정보들을 가져올 수 있다. 하지만, 해당 정보만으로는 비식별 정보를 재 식별하기는 어렵다. 본 논문에서는 비식별 개인정보를 가져오는 과정과, 가져온 비식별 개인정보를 재 식별하는 방법. 그리고 재 식별한 개인정보를 활용할 수 있는 시나리오들을 제시하였다. 이를 이용한다면 수사 과정에서 범인 추적이 보다 수월해질 수 있을 것이다. 또한, 여러 통계적 추산을 위한 데이터 축적에도 많은 도움을 줄 수 있을 것이다.

본 논문에 기술한 내용을 이용하면 누구나 쉽게 모바일 디바이스 사용자를 추적할 수 있다. WPA2 방식으로 암호화가 되어 안전한 통신이라고 생각하였던 802.11 Frame이었지만, 디바이스 식별 정보를 쉽게 Parsing 할 수 있었다. 해당 추적을 방지하기 위해서는 공공 장소에서 제공하는 Public Wi-Fi 이용을 자제하고, LTE 및 3G 데이터를 이용하여 통신하는 것을 추천하는 바이다. 혹은, 각 모바일 디바이스의 벤더 사에서 802.11 Probe Request의 발생량을 최소화하도록 패치하는 것 역시 방법이다.

향후 연구에서는 802.11 Probe Request Frame 뿐만이 아닌, 802.11 Frame 전반에 대한 연구를 진행한다. 암호화된 802.11 Frame을 해독하기 위한 키 재생성 및 이를 통한 패킷 Analysis 방법을 제시하고자 한다.

최근 Wi-Fi 이용률이 증가하는 만큼, 무선 네트워크상의 공격이 발생한다면 개인정보 유출 등의 문제가 발생할 수 있다. 이를 예방하기 위해서는 WIPS와 같은 무선 보안 장비들이 필요하지만, 비싼 가격과 In path 운영 방식으로 인한 네트워크 성능 저하 등이 문제가 되어왔다. 해당 문제를 해결하기 위해서 Monitor Mode를 이용해 Out of path에서 동작하도록 하는 패킷 분석기와 이를 응용한 보안 솔루션에 대한 연구를 진행하고자 한다. 이는 향후 무선 네트워크 보안 솔루션 시장의 스펙트럼을 넓힐 수 있고, 기존의 WIPS 가격이 부담되는 곳에서 해당 솔루션을 활용할 수 있기 때문에 공공 Wi-Fi에 대한 보안성이 향상될 수 있을 것이다.

[참고문헌]

[1] MINISTRY OF THE INTERIOR AND SAFETY. “Personal information non - discrimination measures and industrial applications..” https://www.privacy.go.kr/edu/inf/9.do (2017.10.28.)

[2] Korean ICT Glossary. “802.11 Probe Request Frame”.http://www.ktword.co.kr/abbr_view.php?m_temp1=2344. (2017.10.,28.)

[3] Linux Iwconfig Manual https://linux.die.net/man/8/iwconfig

[4] Wireshark Packet Capture, Auditing Tool “Monitor Mode”, https://wiki.wireshark.org/FrontPage (2017.10.28.)

[5] FRENCH, Clark; WHITE, Peter W. Method and apparatus for indexing database columns with bit vectors. U.S. Patent No 5,649,181, 1997.

[6] ABE, Ryuta, et al. Network-Based Pedestrian Tracking System with Densely Placed Wireless Access Points. In: Information Search, Integration, and Personlization. Springer, Cham, 2017. p. 82-96.

[7] Aircrack-ng wireless network analyzer. “airodump”, https://www.aircrack-ng.org/ (2017.10.28.)

[8] sarwiki.“802.11 Network Structures” https://sarwiki.informatik.hu-berlin.de/ (2017.10.28.)

[9] Zoyi Corp. “WALK INSIGHTS” http://walkinsights.com/ (2017.10.28.)