ETRI

2014
Electronics and
Telecommunications
Trends

소프트웨어 기술동향 특집

무선 핑거프린팅 기술 및 보안응용

Wireless Fingerprinting Technology and Its Applications

정병호 (B.H. Chung) ICT 융합보안연구실 실장
김신효 (S.H. Kim) ICT 융합보안연구실 책임연구원
김정녀 (J.N. Kim) 사이버보안시스템연구부 부장

* 본 연구는 미래부가 지원한 2014년 정보통신·방송 기술개발사업의 연구결과로 수행되었음.

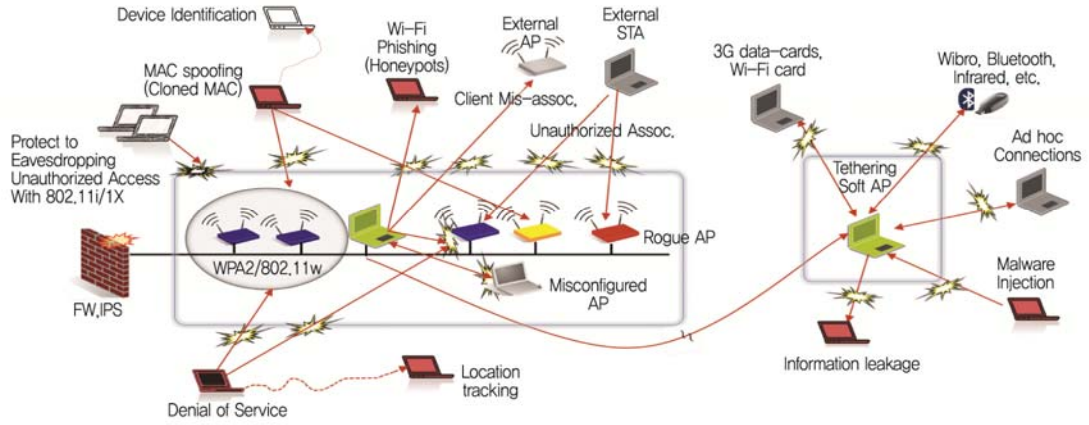
무선환경은 가짜 클론 디바이스가 진짜인 것처럼 위장한 해킹공격에 매우 취약한 것으로 잘 알려져 있다. 그것은 단말기와 기지국(AP: Access Point)이 위변조가 쉬운 디바이스 식별자(예로 MAC(Medium Access Control) 주소, SSID, BSSID (Basic Service Set Identification) 등)를 이용하여 상호 인증하기 때문이다. 무선 핑거프린팅(Wireless Fingerprinting)은 통신과정에서 발생되는 무선신호 특성으로부터 디바이스를 고유하게 식별하는 핑거프린트를 추출하여 송신 디바이스가 가짜 클론 디바이스인지 아닌지 여부를 식별하는 기술이다. 본 기술은 무선물리계층 보안을 위한 인증 및 키 생성, 무선 침입탐지, 공격자의 위치/방향/거리 추적, 무선 포랜식 및 보안관제의 성능을 결정하는 핵심기술로 활용되고 있다. 향후 등장이 예상되는 M2M 무선랜, 무선인지네트워크, 무선센서, 무선차량통신, IoT 무선통신환경에서도 본 기술의 중요성은 더욱 증가하리라 본다. 본고에서는 무선 디바이스의 핑거프린팅 개념을 이해하고, 기술 분류에 따른 세부기법 연구 및 보안응용 동향을 분석함으로써 본 기술의 발전방향을 조망해보고자 한다.

Ⅰ. 서론

1999년 말 무선 인터넷 개념과 함께 처음으로 등장한 무선랜은 전세계적으로 가장 널리 퍼져있는 대표적인 무선 네트워크로 잘 알려져 있다. 초기에 핫스팟 위주의 서비스를 제공하면서 다소 성장이 정체되는 듯 보였으나, 2007년 스마트폰 출현 이후 모바일 서비스 데이터의 폭증 문제를 해소하는 유력한 대안이 되면서부터 시장수요가 폭발적으로 증가하고 있다. 이러한 환경에 발맞춰, 서비스 성능 또한 지난 10여 년간 급속도로 진화해왔다. 속도는 11Mbps(802.11b)에서 수 Gbps(802.11ac)로 100배 이상 고속화되었고, 0.05msec 수준의 고속 핸드오프(802.11r), 차량용 무선통신(802.11v) 및 서브 1GHz 대역에서 km 거리까지 통신 서비스를 제공하는 사물 무선랜(802.11ah) 기술이 개발되고 있다.

반면에, 보안 관점에서 무선랜은 2003년 이후 WEP (Wired Equivalent Privacy)을 보다 강화한 RSN(Robust Secure Network) 보안 아키텍처를 설계하여 새로운 AES(Advanced Encryption Standard) 암호 및 키 관리 체계(802.11i)를 도입하고, 개선된 보안 프로토콜을 이용하여 사용자의 무선 불법접속 제어(802.1x) 및 무선 DoS 공격차단(802.11w) 노력을 진행해 왔음에도 불구하고 여전히 취약한 것으로 알려져 있다. 그것은 무엇보다도 단말기와 무선 네트워크 접속을 지원하는 접속장치(AP: Access Point) 간 상호인증을 하지 않는다는 점과 무선 디바이스 드라이버가 개방되어 있어서 특정 디바이스에 할당된 MAC(Medium Access Control) 주소와 같은 ID 정보를 변복제한 위장 디바이스 제작이 쉽다는 점 때문이다. 이러한 환경에서는 사용자 단말기가 정상적으로 서비스 중인 인가AP에 접속한 것인지 아니면 인가AP를 불법 복제하여 피싱을 유도하는 해커의 클론 AP(Clone Access Point)에 접속한 것인지를 알 수 없게 된다((그림 1) 참조). 결국 이런 취약점들로 인해 무선환경에는 암호학적 인증을 통한 데이터 프라이버시 보호(도청, 위변조 방지 등) 외에도 불법복제된 클론 디바이스들의 위협을 탐색하여 차단하는 디바이스 인증기술이 중요한 이슈가 되었다. 기술적 접근방식으로는 복제 가능한 ID를 통한 인증방식이 아니라 디바이스의 고유한 하드웨어 또는 소프트웨어적 지문 특성을 식별하여 디바이스를 인증하는 핑거프린팅 기술이 많은 관심을 받아왔고, 많은 연구자들에 의해서 활발히 연구되어 왔다[1][2].

본고에서는 Ⅱ장에서 무선 핑거프린팅(Wireless Fingerprinting)의 개념을 소개하고 Ⅲ장에서는 기술 분류에 따른 세부 연구동향을 분석한다. Ⅳ장에서는 무선 핑거프린팅 기술을 응용한 보안제품을 살펴보고 마지막으로 Ⅴ장에서 발전방향으로 결론을 맺고자 한다.



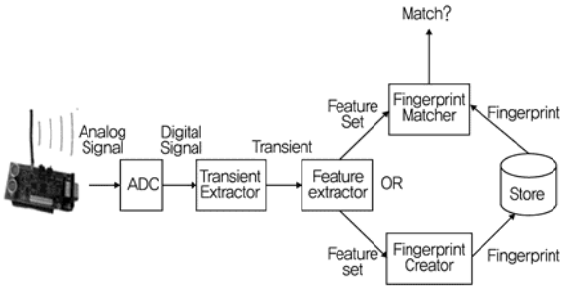
(그림 1) 핑거프린팅 기술을 이용하는 무선보안 응용환경

II. 무선 핑거프린팅 개념

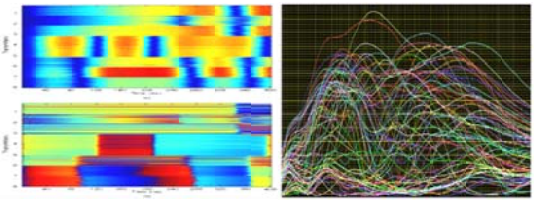
무선은 유선과 달리 네트워크 접속점이 분리되어 있어서 기본적으로 디바이스와 무선 접속장치 간에 브로드캐스트 통신을 한다. 따라서 공격자는 특별한 노력을 하지 않더라도 개별 디바이스들이 통신하는 트래픽(데이터, 관리, 제어를 위한 메시지)을 모니터링한 정보를 활용하여 DOS, 피싱, 중간자공격 등 다양한 공격을 할 수 있다. 물론, 네트워크 관리자 역시 공격자처럼 이러한 트래픽 상황을 모니터링하여 공격 위협의 발생 여부를 탐지하고 대응 가능하다. 그런데 문제는 인가AP의 MAC 주소, SSID, BSSID(Basic Service Set Identification) 등 디바이스 식별정보를 동일하게 복제한 공격자의 클론AP 데이터와 인가AP의 데이터가 섞여서 송수신될 때 무선공격이 발생되고 있는지 여부를 탐지하고, 어느 것이 공격자가 보낸 데이터 프레임인지 구별할 수 있으며, 수신신호의 세기로 볼 때 어느 위치에 있는 디바이스가 공격자인지를 식별할 수 있는 능력은 매우 중요하다. 당연히 이러한 침입탐지 및 대응능력이 무선 네트워크의 보안성능을 결정하기 때문이다.

따라서 핑거프린팅 기술은 특정 무선 디바이스로부터 수신된 정보(예를 들면, 무선모뎀 등 물리적 하드웨어 계층정보, 비콘 헤더 등 MAC 소프트웨어 계층정보 등)분석을 통하여 특정 디바이스를 고유하게 식별하고 유일하게 분류할 수 있는 특징적 지문, 즉 핑거프린트를 추출하는 것이 중요하고 이러한 특징을 추출하는 방식에 따라 다양한 기법들이 존재한다.

핑거프린팅 메커니즘은 (그림 2)와 같이 크게 핑거프린트 생성과 분류단계로 나누어진다. 먼저 생성단계에서는 디바이스가 송신하는 무선신호를 수집하고 신호처리하여 디바이스를 유일하게 구별할 수 있는 특징들을 추출하는 단계이다. 통상, 이 단계는 무선 모니터링 센서에 의해서 수행되는데, 브로드캐스팅되는 수많은 채널상에서 데이터 프레임을 수집하고 패턴을 분석해야



(a) 무선 핑거프린팅 메커니즘



(b) 무선 디바이스 핑거프린팅 예제

(그림 2) 무선 핑거프린팅 메커니즘 및 샘플 예제

하므로 〈표 1〉과 같이 핑거프린트 추출에 필요한 메모리 용량과 계산 양을 최소화하면서, 디바이스를 유일하게 식별하고, 탐지기법을 우회하기 어려운 특징 집합을 개발하는 것이 연구의 핵심이다.

핑거프린팅 분류단계에서는 대체적으로 K-NN, SVM 등과 같이 잘 알려진 기계학습 분류기를 이용한다. 이전 단계에서 추출한 특징값들을 통계적 방식으로 분류하고, 학습과정에서 추출하여 보관하고 있는 디바이스의 핑거프린트와 매치하는지를 판단함으로써 클론 디바이

〈표 1〉 무선 핑거프린팅 요구 성질

특성	정 의
유일성	동일제조사/동일제품(모델)의 무선 NIC 카드를 사용할지라도 서로 구별
반복성	동일 디바이스에 반복적으로 핑거프린팅을 추출하더라도 동일한 결과
최소성	디바이스를 유일하게 식별하는 최소 차원의 핑거프린팅 특징 집합 추출
견고성 (우회방지)	해커가 핑거프린트를 위조하거나 핑거프린팅 센서를 우회하기 어려움.
투명성	사용자 디바이스의 HW나 SW 수정을 요구하지 않음.
복원성	위치 따라 가변적인 무선채널의 노이즈, 다중경로효과, MIMO* 등에도 견고함

*MIMO(Multiple Input Multiple Output)

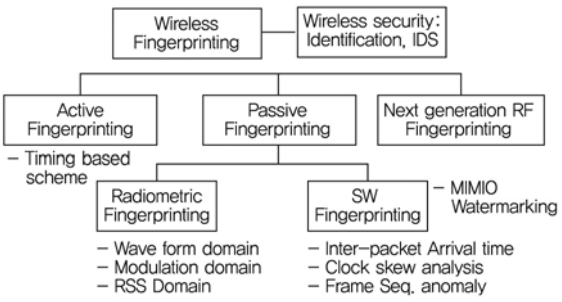
스 여부를 판단하게 된다.

Ⅲ. 무선 핑거프린팅 기술동향

무선 핑거프린팅 기술은 크게 핑거프린팅 데이터를 센싱하는 방식에 따라 액티브와 패시브 방식으로 분류된다. 패시브 방식은 또 핑거프린트 특징을 추출하는 기법에 따라 RF 핑거프린팅과 SW 핑거프린팅으로 세분화될 수 있다((그림 3) 참조).

먼저, 액티브 방식은 핑거프린트를 추출하는 디바이스가 주변에 위치한 AP 디바이스에 적극적으로 탐지요청패킷(Probe request)을 보내서 응답을 보내준 데이터를 기반으로 핑거프린트를 생성하고 디바이스의 위장 AP(Rogue Access point) 여부를 판단하는 방식이다. 이 방식의 한계는 똑똑한 클론AP가 액티브센서의 탐지기법을 이해하고 탐지요청패킷에 응답을 보내지 않음으로써 쉽게 공격자 탐지를 우회할 수 있다는 점이다. 따라서 이 방식은 네트워크 모니터링센서보다는 단말기 환경에서 유용하게 적용할 수 있는 방식이다. 단말기가 무선 네트워크에 접속하기 위해서는 반드시 주변 AP와 연결절차를 거치기 때문이다.

패시브 방식은 네트워크상에 모니터링센서를 설치하고, 수신신호 영역 내의 무선 트래픽 내용을 수동적으로 모니터링하다가 센서 주변에 있는 위장AP를 찾아서 동작을 차단하는 방식이다. 이때 센서는 브로드캐스팅되



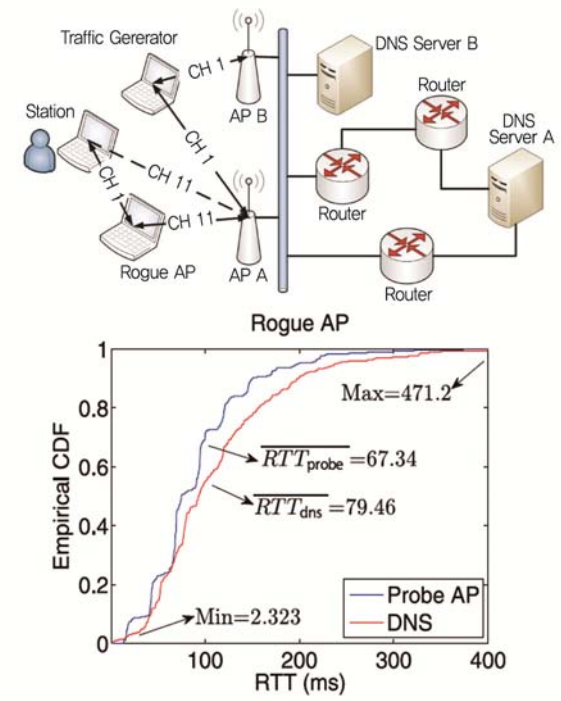
(그림 3) 무선 핑거프린팅 방식 분류

는 수신신호를 분석하여 핑거프린트를 추출하고, 통신 트래픽이 정상AP로부터 수신된 것인지 아니면 위장/복제AP가 보낸 것인지를 분류한다. 이 방식의 단점은 하나의 센서만으로 네트워크 상에 존재하는 모든 AP와 디바이스를 완벽히 탐지하기 어려울뿐만 아니라, 모니터링해야 할 무선채널 수와 센싱 트래픽 용량이 증가할수록 센서의 메모리 및 계산 용량이 증가하여 확장성이 떨어지고 탐지 비용이 비싸진다는 문제가 있다. 아울러 탐지센서가 단말기와 AP 중간에서 트래픽을 모니터링하는 방식이므로 센서의 설치위치에 따라 성능이 달라진다. 공격자가 전파신호 강도를 줄여서 동작하거나 지향성 안테나를 이용한 탐지센서 우회공격에 취약할 수 있다는 한계도 있다. 하지만 현재 시장에 출시된 대부분의 보안응용 제품은 패시브 방식을 적용하고 있다.

1. 액티브 핑거프린팅

윌리엄&메리 대학의 H. Han et al[3]은 2011년 액티브 핑거프린팅 방식을 이용하여 무선 네트워크 관리자의 지원 없이 단말기가 핫스팟에서 위장/복제AP에 접속하고 있는지 여부를 스스로 판단하는 기법을 제안하였다. 기본 동기는 단순하다. 해커로부터 공격을 받고 정보가 유출되는 이유는 위장/클론AP에 접속했기 때문이므로 단말이 접속할 때 이를 피하면 된다는 것이다. 단말이 위장AP를 통하여 무선AP에 접속을 하였다면 통신 홉 수가 증가할 거라는 논리를 가지고, 사용자 단말기로부터 AP와 DNS(Domain Name System) 서버까지의 걸리는 통신 지연시간을 핑거프린트로 이용하였다. 즉 단말기가 접속할 AP에 탐지요청패킷을 보낸 후 응답받은 평균왕복시간차(RTT: Round Trip Time)와 로컬 DNS 룩업 요청 메시지를 보내 응답 받은 평균시간차가 설정된 기준 값을 초과하면 위장AP에 접속된 것으로 판단한 것이다.

유선은 지연시간이 없고 무선의 경우 통신 홉 수가 증



(그림 4) 클론AP 공격환경 및 평균 RTT 기반 복제/위장AP 탐지[3]

가함에 따라 지연시간도 증가할 것으로 가정한 것인데, 무선 단말기 수가 100인 실험 환경에서 트래픽 부하조건에 따라 정상AP 대 위장AP의 평균 RTT 차가 1~11.44msec, 정확도(100~60%)인 성능을 보였다((그림 4) 참조). 이 방식은 결국 수 밀리 초 단위의 지연시간이 트래픽 부하로 인한 지연인지 아니면 위장AP에 의한 통신 홉 수 증가와 위장AP 시스템의 컴퓨팅 성능에 의한 지연인지에 대한 정확한 판단이 중요하고, 더욱이 Gbps급 무선환경에서는 유무선 간의 통신 지연시간 차이가 거의 없어질 것이므로 평균 RTT차와 같은 특징을 핑거프린트로 활용하기는 한계가 있다.

2. 패시브 RF 핑거프린팅

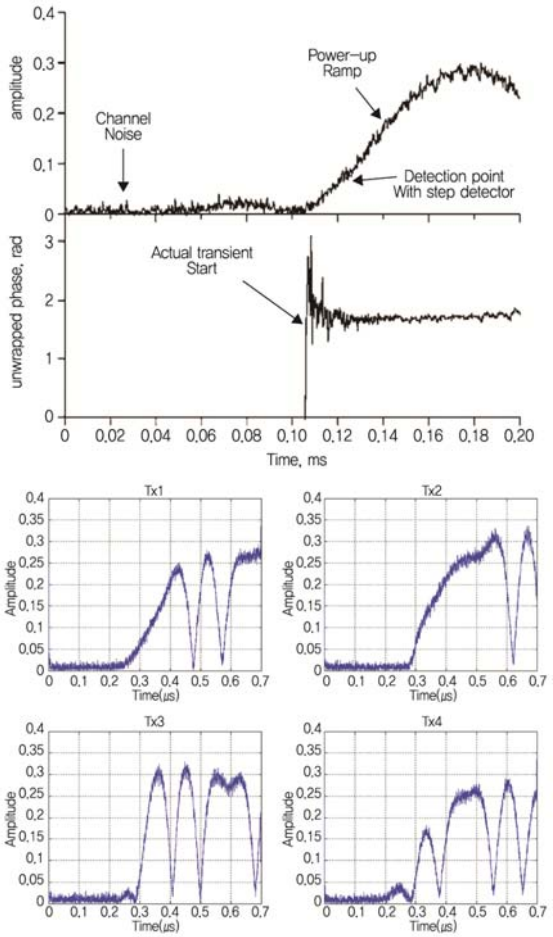
RF(Radio Frequency) 핑거프린팅 방식[4][5]은 디바이스의 물리적 전송 특성을 이용하여 무선 디바이스의 유일성을 식별하는 기술이다. 예를 들어 RF 주파수합성기, RF 전력증폭기, 변복조기 등과 같은 RF 송신기의 아날로그 부품들은 표준규격을 벗어나지 않은 한도 내에서 제작 허용오차가 발생할 수 있다. 이러한 허용오차들은 동일 회사, 동일 모델의 제품일지라도 다르게 존재할 수 있어 이 오차가 갖는 특징을 잘 분석하면 디바이스를 유일하게 식별할 수 있는 핑거프린트 추출이 가능하다는 것이다. 시스템 관점에서, 복제단말 탐지센서는 임의의 디바이스로부터 데이터 프레임을 수신하게 되면 실시간으로 RF 핑거프린트를 추출하고 사전에 DB에 보관된 RF 핑거프린트와 MAC ID를 비교 매칭하여 해당 디바이스가 MAC 주소를 위장한 클론 디바이스인지 아닌지 여부를 판단하게 된다.

가. 과도파(Transients) 특성 분석방식

과도파는 데이터 송신 시, RF 송신기에 전원이 공급될 때 발생하는 짧은 구간(약 200ns)의 출력신호((그림 5) 참조)를 의미하고, 데이터를 수신한 디바이스에서 과도파 시간 구간에 있는 신호의 스팩트럼(주파수, 진폭 등)을 잘 분석하면 송신 디바이스의 RF 송신기를 유일하게 식별할 수 있는 특징을 추출할 수 있다는 사실이 밝혀진 후 많은 연구가 진행되어 왔다.

온타리오 대학의 O. Ureten et al[6]은 2007년 RF 송신기에서 출력되는 과도파의 진폭과 주파수 위상 편차를 이용하여 2.4Hz 대역 802.11b 디바이스를 핑거프린팅하는 기법을 제안하였다. Watkins Johnson사의 신호수신기와 텍트로닉스사의 신호분석기를 이용하여 송신 디바이스의 RF를 수신하고 과도파 특징을 추출하였고, 디바이스 식별을 위한 핑거프린트 분류기로 확률신경망(PNN)을 이용하였다.

과도파 분석 방식은 매우 짧은 구간(약 200ns)에 발생하는 신호의 동작 패턴을 검출하는 시점이나 부품의 노후화, 날씨, 노이즈 등 RF 수신조건에 따라 과도파 특징값이 영향을 받게 되어 핑거프린팅 성능이 저하될 수 있



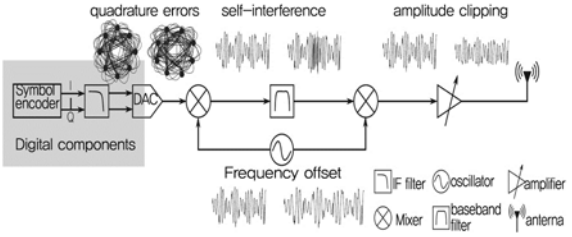
(그림 5) 과도파 구간과 4개의 무선랜 NIC(동일 제조사/모델)에 대한 과도파 동작패턴 예제[6]

다는 점과 과도파 수집 및 분석에 고가의 HW센서가 필요하다는 점들이 극복되어야 할 문제이다.

나. 변복조(Modulation) 특성 분석방식

과도파 분석기법이 무선 디바이스의 RF 전력증폭기 도메인에서 발생하는 특성을 활용한 반면에, 변복조 특성 분석방식은 RF 복조 도메인에서 RF 송신기의 허용오류 특성((그림 6) (b)) 참조)을 이용하여 송신 디바이스의 RF 송신기를 식별하는 기법이다.

윈스콘신대학의 V. Brik at al[7]는 2008년 802.11b RF 모뎀의 I/Q 변복조과정에서 이상적인 파형과 측정



(a) RF 송신기 HW단에서의 제작 허용오류 유형

Error type	unit	Reference	Range	Definition
Frequency	Hz	2142Mhz	±60.3	±25ppm f_c
Phase	°	Ideal symbol	±10	asin(E_{max})
Magnitude	n/a	Ideal symbol	±0.17	$\pm E_{max}$
EVM	n/a	Ideal symbol	[0,0.35]	upto 2 E_{max}
I/Q offset	n/a	Ideal symbol	[0,0.17]	upto E_{max}
Sync	%	Max Corr.	[0,1]	correlation

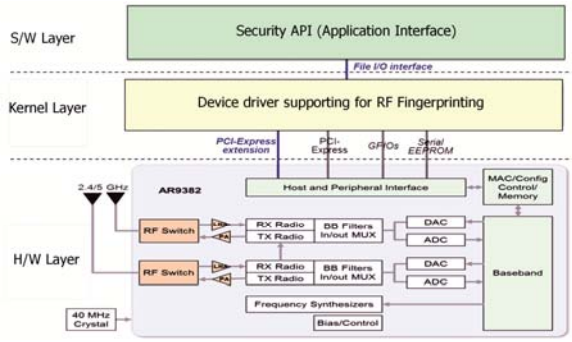
(b) 무선 변복조 오류 측정기준

(그림 6) 무선 변복조 오류 특성 및 측정기준[7]

된 파형 사이의 차이로 인해 발생하는 1) 하나의 심볼에 대한 오류값들 즉, 위상오류(각도편차), 진폭오류, 오류벡터 크기(EVM: Error Vector Magnitude), 심볼클럭오류와 같은 I/Q 복조오류와 2) 수신된 하나의 프레임(또는 한 프레임 내의 전체 심볼) 수준에서 보여지는 평균오류 즉, 송신기와 수신기간 동기화 상관값(Sync Correlation), I/Q편차, 주파수 편차 등을 활용하여 송신 디바이스를 식별하는 핑거프린팅 기법을 제안하였다.

RF 송신기에서 보낸 신호는 수신단에서 복조될 때 이상적인 신호 파형에 비해 왜곡되어 검출될 수 있는데, 이것은 RF 송신기 HW 부품의 제작 허용오류나 채널특성 또는 신호잡음이 그 원인이 될 수 있다((그림 6) (b) 참조). 따라서 변복조 단계에서 RF 핑거프린트를 선택할 때 HW 제작 허용오류가 원인이 되는 특징들 즉, 같은 RF 송신기부터 수신된 여러 프레임에 일관성있게 나타나는 특징들은 우선순위를 가지고 증폭시키고, 무선 채널 상태 또는 노이즈가 원인이 되어 여러 프레임 사이에서 랜덤하게 보여지는 특징들은 그 효과가 축소되도록 처리할 필요가 있다.

전체적으로 변복조 특성방식에 기반한 핑거프린팅 기술은 변복조 특성들이 기본적으로 무선 표준규격에 정

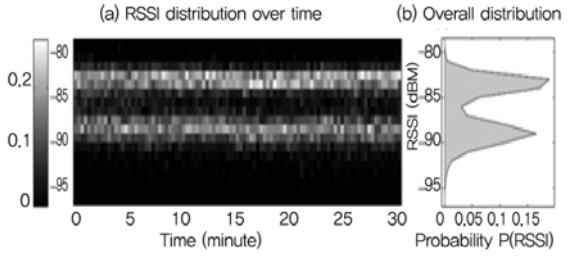


(그림 7) 변복조 특성 기반 RF 핑거프린트 플랫폼 구조

의되어 있다는 점에서 보다 정형화된 핑거프린트 생성이 가능하다는 장점이 있다. 그러나 실용화 관점에서 보면, 이러한 특성들은 I/Q 복조과정에서 산출되는 중간 계산값에 해당되므로 무선 칩 셋에서 직접 핑거프린트 특성을 추출하는 기술개발이 해결과제이다((그림 7) 참조).

다. 수신신호세기(RSS) 특성 분석방식

수신신호세기(RSS: Received Signal Strength)는 공격자가 임의적으로 위조하기 어려우면서 송신기의 전파 발신거리와 전파환경에 밀접한 연관성을 갖는 물리적 특성으로 무선 위치인식에 활용되어 왔다. 다트머스대학의 Y. Sheng et al[8]은 2010년 송신기 RSS 측정값을 이용하여 복제 디바이스를 탐지하는 핑거프린팅 기법을 그리고 스텐포드대학의 D. Faria et al[9]는 2006년 시그널프린트(주변의 여러 핑거프린트센서로부터 수집된 RSS값 집합)을 추적함으로써 디바이스를 식별하는 기법을 제안하였다.



(그림 8) 동일위치-시간변화에 따른 RSS 분포[9]

RSS 기반 핑거프린팅 방식의 가장 큰 장점은 무선 모뎀상에서 RSS 특징값 추출을 위한 추가적인 노력이나 비용이 필요없다는 점이다. 반면에 이 방식은 몇가지 기술적 한계도 가지고 있다. 디바이스를 식별하는 성능이 공격자와 피해자 간 거리(RSS값 오차범위)에 민감하므로 피해자(인가AP) 가까운 곳에서 공격자(클론AP)가 복제공격을 시도할 경우 탐지 정확도가 떨어진다는 점이다. 더욱이 RSS 신호자체가 동일한 위치에서도 시간에 따른 변화값이 커서((그림 8) 참조) 핑거프린트의 유일성 또는 반복성 측면에서 성능오차가 크다는 한계가 있다. 그리고 이러한 환경에서 정확도 향상을 위해서는 탐지센서를 촘촘히 설치해야 하므로, 이에 따른 비용 부담 증가 또한 단점이 된다고 본다.

3. 패시브 SW 핑거프린팅

패시스 SW 핑거프린팅은 디바이스로부터 수신한 무선 MAC 계층 통신 프로토콜 메시지들 간의 상관관계 분석(예, 도착 시간, 클락스큐, 도착 순서 등)을 통하여 클론AP 판별이 가능한 특징을 추출하는 기법이다. 이러한 방식들은 HW 도움 없이 SW 알고리즘 만으로 실현이 가능하여 기존의 다양한 무선통신환경에 적용하기가 쉽고, 성능 업그레이드도 용이하다는 장점이 있다. 반면에, 클론AP 탐지 및 식별 관점에서 보면, 트래픽 분석으로부터 클론AP의 출현여부를 탐하지는 것은 가능하나, 동시에 송신하고 있는 여러 AP들 중에서 어느 위치의 AP가 클론AP인지를 구별하기는 쉽지 않고, 탐지시간이 많이 걸리며, 핑거프린팅 우회공격에 취약하다는 문제가 주요 연구이슈가 된다.

가. 인접패킷 간 도착시간차(IAT) 분석방식

택사스A&M대학의 Y. Song, et al[10]은 2010년 동일한 디바이스로부터 송신된 두 개의 인접 패킷 간 도착시간(IAT: Inter-packet Arrival Time) 차이 분석을 통

하여 클론AP 존재 여부를 판단하는 기법을 제안하였다. 즉, 정상AP의 1-홉 통신과 위장/클론AP의 2-홉 통신은 무선랜 802.11b/g CSMA(Carrier Sense Multiple Access)/CD 통신 프로토콜(DIFS, SIFS, ACK, Backoff time 등) 측면에서 더 많은 지연시간을 갖는다고 인지하고, 이를 구별하는 기법이다. 이론적인 IAT 계산시간과 실제 측정시간 간의 비율을 기준 값으로 하여 클론AP로의 접속여부를 판단하였다. 이 방식은 소프트웨어적으로 탐지하기 때문에 구현비용이 싸다는 장점이 있는 반면에 수신 데이터 수가 적은 상황에서는 탐지성능이 낮고(또는 탐지속도가 느리고), 수신 메시지의 수신신호세기(RSS) 변화 따라 메시지 재전송이 많이 발생하는 경우 탐지성능이 영향을 받을 수 있다는 문제도 있다.

따라서 시간 기반 분석방식의 탐지성능 향상을 위해서는 트래픽 부하 변화, 수신신호세기 변화, 재전송 등 시간변화에 영향을 주는 변수들이 클론AP 추정 및 판단에 어떠한 영향을 미치는지를 해석하고, 이러한 동적 변수들에 적응하는 알고리즘 및 판단 모델값을 결정해야 한다. 아울러 클론AP를 통한 무선 피싱 또는 중간자 공격의 대부분은 ID/비밀번호와 같은 프라이버시 정보획득을 목표로 하므로 가급적 무선인증 이전 단계 수준의 빠른 탐지속도를 제공할 필요가 있다.

나. 클럭스큐(Clock Skew) 분석방식

유타대학의 S. Jana, et al[11]는 2010년 클럭스큐를 이용하여 클론AP를 탐지하는 방식을 제안하였다. 무선 비콘 및 Probe 응답패킷에 포함되어있는 시간동기화(TSF: Time Synchronization Function) 값을 이용하여 AP의 클럭스큐를 추정하고, 패킷 수신센서에서 클론AP의 출현여부를 탐지하는 휴리스틱 방식이다. 기본적인 아이디어로 AP에 내장된 CPU 클럭생성기(크리스털 오실레이터)의 경우 절삭공정을 통한 제작과정에서 기계적 정확도가 갖는 한계(마이크로 수준)때문에 유사한 유형의 크리스털 제품일지라도 주파수 허용오차가 조금씩 다르다는 특성을 가지고 있다. AP는 이러한 특성을 갖는 CPU 클럭을 이용하여 비콘 메시지의 TSF 시간값을 생성하므로 이를 잘 분석해 보면 송신AP를 유일하게 식별할 수 있는 특징을 찾을 수 있다는 점에 주목했다. 즉, AP로부터 주기적으로 비콘 메시지를 수신할 때마다 야기된 TSF 시간값 편차의 추이를 분석해 보면 특정 비콘을 송신한 AP의 클락스큐 추정이 가능하고, 이 특징을 핑거프린트로 활용하여 클론AP 식별할 수 있다는 것이다.

다만, 비콘 메시지를 기반으로 핑거프린트를 추출하는 방식이므로 클론AP가 아닌 클론 단말기를 탐지하는 데는 한계가 있다. 아울러 클러스큐 임계값에 대한 정밀도가 수백 마이크초 수준으로 너무 작아서 클럭스큐 추정오류에 외부 요인(예를 들어, 인가AP와 클론AP의 비콘 메시지가 혼재되어 수신되는 경우 발생 가능한 유입오류 또는 외부에 설치된 AP의 온도 변화에 따른 클럭스큐의 변화 등)이 민감하게 영향을 미칠 수 있다는 문제도 있다.

다. 프레임 시퀀스 Anomaly 분석기법

뉴욕주립대학의 F. Guo at al[1]은 2006년 무선 MAC 프로토콜 메시지 해더의 시퀀스 번호 패턴 분석을 통하여 클론AP를 식별하는 기법을 제안하였다. 원래 디바이스에서 송신할 데이터의 크기가 MAC 프레임의 크기보다 클 때 쪼개서 송신한 데이터를 수신측에서 순서대로 재조립하는 목적으로 사용되는 시퀀스 번호를 핑거프린트 특성으로 활용하였다. 그리고 통신하는 데이터 메시지 중간에서 시퀀스 순서가 틀어졌다면 그것은 MAC을 복제한 공격자(클론 디바이스)가 끼어 들었기 때문일 것이라는 논리를 가지고 접근하였다. 아울러, 무선 네트워크 중간에 침입탐지센서를 두고 주변에 위치한 디바이스들이 송신하는 무선 메시지를 모니터링하여 클론 디

바이스를 탐지하는 구조를 제안하였다.

하지만 이러한 시퀀스 분석방식 아래서는 클론 디바이스의 공격이 아닐지라도 여러 이유로 송신 메시지의 시퀀스 순서가 틀어지는 갭이 발생할 수 있다. 예를 들어, 하나의 센서가 주변의 모든 디바이스들의 송신 메시지를 수신하지 못하고 잃어버리거나, 디바이스가 센서에서 멀어질 수록 수신강도가 약해져 중복된 재전송 패킷이 많아지게 된다. 결국 이러한 무선전송 특성 및 센서 수신 특성이 미치는 영향을 고려하여 핑거프린팅 기법을 설계할 필요가 있다.

4. 차세대 무선 RF 핑거프린팅

지금까지 앞서 논의한 대부분의 핑거프린팅 기법은 단일입출력안테나(SISO: Single Input Single Output)를 가진 CSMA/CD 통신환경에서 송신기의 특성을 인증하고 클론AP를 찾아내는 기술로 802.11a/b/g 기반 저속 무선환경 아래서 연구되었다. 그러나 최근 Gbps급 고속 무선통신에서는 고집적 변조(256 QAM(Quadrature-Amplitude Modulated), OFDM), RF 광대역폭(〈160MHz), 블록 ACK MAC, 채널본딩, 다중입출력안테나(8-MIMO (Multiple Input Multiple Output), MU-MIMO, 빔포밍을 이용한 공간 다이버시티 같은 채널 특성과 새로운 통신기술의 적용이 확대되어 감에 따라 그에 대응되는 새로운 핑거프린팅 기술연구가 요구된다.

아직까지 이 분야는 연구 초기 단계에 있다. 대체적으로 물리적 계층에서 MIMO 채널의 공간 다이버시티 특성을 이용한 보안 향상, 클론 디바이스의 공격탐지 등에 대한 기법연구가 주류를 이룬다. 주요한 접근방식은 MIMO 기반 핑거프린트 특징 분석방식[12]과 MIMO 채널 워터마킹 방식[13]으로 분류할 수 있다.

가. MIMO 기반 핑거프린트 특징 분석방식

단일 안테나(SISO) 환경에서 연구된 기존의 핑거프린팅 기법을 N개의 송수신기를 갖는 MIMO로 확대 적용하는 문제로 여러 개의 MIMO 수신채널로부터 추출된 송신채널의 특성을 조합하여 송신 디바이스의 RF 핑거프린트를 결정하는 방식이다.

〈표 2〉 MIMO(3) 송신기 핑거프린트 특징 예[12]

Rank	Number of Transmitters(N_{Tx})		
	1	2	3
1	Freq Offset	Freq $Offset_1$	Freq $Offset_1$
2	SYNC Corr	SYNC $Corr_1$	SYNC $Corr_1$
3	I/Q Offset	I/Q $Offset_1$	I/Q $Offset_1$
4	EVM	I/Q $Offset_2$	I/Q $Offset_2$
5	Symbol Clock Error	EVM_1	I/Q $Offset_3$
6	I/Q Gain Imbalance	SYNC $Corr_2$	EVM_1
7	I/Q Rotation	EVM_2	EVM_3

2011년 메릴랜드대학의 Y. Shi at al[12]는 MIMO 송신기를 갖는 디바이스의 핑거프린팅 기법을 제안하였다. 이 기법은 2008년에 윈스콘신대학 V. Brik at al[7]가 발표한 결과 즉, 1개의 송수신기(SISO)에 대한 변복조 핑거프린팅 특성을 기반으로 802.11n MIMO 통신을 지원하는 디바이스의 RF 핑거프린팅 특징 선택 및 정확도를 향상시키는 기법을 제안하였다. 실험을 통하여 주파수 편차, 프레임 동기화 상관값, I/Q 편차가 MIMO 핑거프린트팅의 중요한 특징이 되고(〈표 2〉 참조), 특정 시점 또는 통신환경 조건에 따라 변동하는 RF 핑거프린트 특성들은 학습모델을 통하여 안정화시킬 수 있으며, 송신기의 수가 많은 MIMO가 SIMO보다 디바이스의 식별 정확도를 더 향상시킬 수 있음을 보였다.

나. MIMO 채널 워터마킹 방식

비디오 워터마킹과 유사하게 MIMO 송신기가 데이터 신호 위에 핑거프린팅 신호를 중첩시켜 송신하면, 무선 메시지를 수신한 디바이스의 MIMO 수신기가 데이터 복조과정에서 데이터와 핑거프린트를 추출한다. 추출된 핑거프린트를 기반으로 무선채널을 인증하는 방식이다[13][14]. 물리계층의 통신채널을 인증하는 것이므로, 상위 MAC 계층의에서 ID를 불법적으로 복제하여 클론

디바이스를 만들고 위장공격을 한다고 할지라도 채널인증이 되지 않을 것이기 때문에 쉽게 탐지하여 공격을 무력화할 수 있다는 것이 기본 아이디어이다.

메릴랜드대학의 P. L. Yu at al[13]은 2011년에 물리계층의 데이터 신호에 명시적으로 핑거프린트를 삽입하여 MIMO 단말기를 인증하는 기법을 제안하였다. 송신기가 공유키-해시함수(Keyed-Hash)를 이용하여 데이터 메시지에 대한 핑거프린트를 생성하고 심볼 동기화 방식으로 데이터신호에 프리코딩하여 MIMO 송신하면, 수신기는 복조된 데이터와 공유키를 이용하여 핑거프린트를 추정하고 수신 메시지로부터 추출한 핑거프린트와 비교하여 MIMO 인증하는 방식이다. 이탈리아 파도바대학 P. Barraca at al[15]은 2012년에 MIMO/OFDM으로 송신된 다중경로 채널의 페이딩 상관성 분석을 통하여 채널신호의 출처를 인증하고, MAC 클론 디바이스를 이용한 메시지 위변조 공격을 탐지하는 기법을 제안하였다. 두 개의 다른 지점으로부터 송신된 채널을 구별하기 위한 채널 추정치로 다중 페이딩에 대한 다이버시티를 이용하였다. 단말기와 AP 간 이용자 인증이 수행되는 과정에서 먼저 송신채널에 대한 참조 추정치를 생성한다. 인증이 완료된 후에는 이 참조 추정치와 메시지 송수신 때 마다 새롭게 생성되는 채널 추정치를 비교하는 방식으로 송신채널을 인증한다. 즉 송신기를 식별하고, 인증하기 보다는 단말기의 위치를 인증하는 방식이다. 따라서 공격자가 송신 디바이스에 인접한 곳에서 공격할 경우 탐지를 우회할 수 있는 단점이 있다.

채널 워터마킹 방식은 비인가된 디바이스의 무선접속 시도를 물리계층에서 조기에 제어함으로써 상위 계층에서 망 접속 시 발생하는 불필요한 시그널링 트래픽을 줄이는 효과도 있지만, 구현관점에서 HW 변경이 요구되어 핑거프린트 투명성 요구를 제공하지 못하는 단점도 있다. 특히 채널 페이딩이 심한 환경에서도 견고한 성능

〈표 3〉 무선 핑거프린팅 기반 클론 디바이스 탐지기법 비교 기호: ●(상) ◐(중) ○(하)

센싱 및 특징 분석방식		핑거프린팅 모델		핵심 기능	핑거프린팅 성능 비교			
센싱	분석				유일성	투명성	우회방지	탐지성능
액티브 핑거프린팅	SW	평균 RTT+localDNS 룩업 시간차 분석[3]		무선접속 응답시간 분석으로 클론AP 접속여부 판단	○	●	○	◐
							유선망에 직접 접속한 RAP 탐지불가, 탐지성능(N=100→60%, 1~10s)	
	HW	MIMO 채널인증 워터마킹[13]		핑거프린트 삽입 및 수신 채널 추정 기반 채널인증	●	○	◐	◐
패시브 핑거프린팅	HW	SISO 기반	과도파 특성 분석[6]	과도파 측정/분석 센서로 송신기 HW 식별	●	○	●	◐
			변복조 특성 분석[7]	모뎀 신호처리 중간결과 활용 송신기 HW 식별	●	○	●	●
			수신신호세기 분석[8]	수신신호세기(RSS) 기반 위치인식+단말기 인증	○	●	○	○
							공격자가 피해자 근처에서 공격 시 탐지곤란	
		MIMO 기반 변복조 특성 분석[12]		다수의 안테나 송신기 특성 분석 기반 단말기 식별	●	○	●	●
	SW	인접 패킷 간 도착시간차분석[10]		MAC 패킷 지연시간 분석으로 클론AP 출현탐지	◐	●	○	○
		클럭스큐 분석[11]		CPU의 클럭스큐 특성을 활용한 송신AP 식별	●	●	●	○
							RAP 출현은 인식, 디바이스 식별은 불가	
		수신 프레임 시퀀스 Anomaly 분석[1]		메시지 시퀀스 분석으로 클론AP의 송신 메시지식별	◐	●	○	○

을 제공하면서 핑거프린트 우회를 방지하는 기법연구가 주요 이슈이다.

Ⅳ. 무선 핑거프린팅 보안응용

지금까지 무선 디바이스의 송신모뎀에 내재된 고유한 HW 특성이나 디바이스의 송수신 신호 특성을 SW적으로 분석함으로써, 특정 클론 디바이스 공격을 차단하는 기술동향을 살펴 보았다(〈표 3〉 참조).

무선 핑거프린팅 기술은 크게 무선침입 방지, 공격자의 무선 위치추적 및 무선 포랜식 시스템의 핵심기술로 응용될 수 있다. 침입탐지가 네트워크에서 무슨 사건(보안 침해)이 일어났는지를 인식하는 기능이라 한다면, 핑거프린팅은 여러 개의 가짜 클론들이 존재하는 환경에서도 누가(진짜 공격자) 어디에 위치해있는지를 알려주는 기능을 제공한다. 최근에는 무선 네트워크 상의 침입탐지정보와 단말기 위치정보를 결합하여 스마트 단말기에 대한 MDM(Mobile Device Management) 보안관리를 정교화시키거나, 기업 무선환경에서 개인용 스마트 기기를 이용한 BYOD(Bring Your Own Device) 보안 솔루션에도 활용된다.

핑거프린팅을 이용한 무선침입 방지센서는 AP독립형, 무선컨트롤러 탑재형, 그리고 AP 탑재형 3가지로 형태로 구별될 수 있다. 패시브 핑거프린팅 기술을 적용한 AP 독립형센서는 주변에 설치되어 있는 여러 AP의 채널로부터 송수신되는 트래픽을 시분할 방식으로 번갈아 감청하고 분석하여 침입을 탐지한다. 최근까지 AP 독립형센서가 무선 보안 시장을 주도해왔는데, 이러한 센서 유형은 감시채널 수가 증가할수록 채널 스케줄링 및 모니터링에 대한 부하가 증가되어 성능이 떨어지는 문제가 있다. 따라서 최근에 등장한 Gbps급 무선환경에서는 탐지채널 수에 확장성있는 새로운 핑거프린팅 기법 및 침입방지 아키텍처가 요구된다.

무선 컨트롤러 탑재형 방식은 무선AP를 통하여 송수신되는 모든 트래픽을 중앙에 위치한 무선 컨트롤러에 전달되고, 컨트롤러가 핑거프린트를 추출하여 침입을 탐지한다. 이 방식 역시 AP 독립형센서와 유사하게 G급 무선 트래픽에 대한 중앙 모니터링은 사실상 어려워 설치될 무선AP 수의 증가, 트래픽 처리속도, 그리고 메모리 용량에 확장성을 갖는 새로운 아키텍처가 요구된다.

마지막으로, AP 통합형센서는 AP와 침입탐지센서가 하나로 통합된 구조이다. 어느 한 시점에 모드전환을 통하여 센서 또는 AP로 동작하거나 또는 하나의 플랫폼 위에서 AP와 센서가 각각 독립적으로 동작하는 방식이 있다. 센서는 현재 AP가 서비스하는 무선 비콘 채널에 대한 침입을 탐지하고 대응한다. 이 방식은 감시해야 할 무선 단말기 수, 채널 용량, 또는 무선 대역폭 증가에 비교적 확장가능하나, 센서가 AP 플랫폼에 종속되어있는 것이 단점이 있다. 예를 들면, 서로 다른 회사 제품의 AP 센서가 설치된 네트워크 환경에서 무선 통합 관제를 위해서는 이종 AP 센서들 간의 상호운용성이 절대적으로 요구되기 때문이다.

Ⅴ. 결론 및 발전방향

본고에서는 무선 디바이스 인증 및 침입방지 핵심기술로 알려진 무선 핑거프린팅 개념과 다양한 특징 추출 기법을 조사 분석하고 보안응용 제품을 살펴 보았다. 무선 핑거프린팅은 송신 디바이스의 물리적 HW 특성과 MAC 프로토콜의 SW 계층 특성을 이용하여 디바이스를 식별하므로 무선네트워크 채널 및 통신 특성에 영향을 받게 된다. 기존에 제안된 대부분의 기법들과 보안응용 제품들은 단일입출력안테나(SISO)를 갖는 802.1a/b/g 무선 네트워크 특성을 타깃으로 연구되어 왔다. 그러나, 최근의 무선 네트워크는 다중입출력안테나(MIMO)를 이용하여 수 Gbpa급 통신속도를 제공하는 무선으로 진화하고 있다. MIMO/공간 다이버시티, 고집적 변조,

채널본딩, 대용량채널 등 기존 무선과는 다른 통신특성을 포함하고 있다. 따라서 대용량 무선채널 및 광대역 트래픽 환경에서 공격탐지 정확도와 속도를 개선하는 차세대 핑거프린팅 기법과 응용시스템 기술연구는 매우 중요하다고 본다.

용어해설

무선 핑거프린팅(Wireless Fingerprinting) 무선 송신기에 내재된 고유한 HW 특성과 MAC 프로토콜의 SW적 신호 특성을 분석하여 송신 디바이스를 유일하게 식별하는 기술

클론AP(Clone Access Point) 인가된 무선 디바이스(단말기, AP)의 ID 식별자(MAC주소, SSID, BSSID, 비콘 시간정보 등)를 복제하여 무선피싱을 유도하거나, 네트워크에 불법 접속하는 디바이스

위장AP(Rogue Access point) 관리자의 허가 없이 내부망에 설치되어 자신도 모르게 해커가 위장AP에 접속하여 내부정보를 해킹하는 통로를 제공하는 무선 기지국

약어 정리

AES	Advanced Encryption Standard
AP	Access Point
BSSID	Basic Service Set Identification
BYOD	Bring Your Own Device
CSMA	Carrier Sense Multiple Access
DNS	Domain Name System
EVM	Error Vector Magnitude
IAT	Inter-packet Arrival Time
MAC	Medium Access Control
MDM	Mobile Device Management
MIMO	Multiple Input Multiple Output
QAM	Quadrature-Amplitude Modulated
RF	Radio Frequency
RSN	Robust Secure Network
RSS	Received Signal Strength
RTT	Round Trip Time
SISO	Single Input Single Output
WEP	Wired Equivalent Privacy

참고문헌

[1] F. Guo and T. Chiueh, "Sequence number -based MAC address spoof detection," *Proc. 8th international conf. Recent Adv. Intrusion Detection*, 2005, pp. 309-329.

[2] J. Franklin at al., "Passive Data Link Layer 802.11 Wireless Device Driver Fingerprinting," *Proc. 15th Conf. USENIX Security Symp.(USENIX-SS '06)*, 2006, pp. 12-12.

[3] H. Han et al, "A timing-based scheme for rogue AP detection," *IEEE Trans. Parallel Distributed syst.*, vol. 22, no.11, Nov. 2011, pp. 1912-1925.

[4] R. Beyah et al, "Rogue-Access-Point Detection," *IEEE Security & Privacy*, Oct. 2011.

[5] K. Gao, C. Corbett, and R. Beyah, "A Passive Approach to Wireless Device Fingerprinting," *IEEE DSN*, 2010, pp. 383-392.

[6] O. Ureten and N. Serinken, " Wireless security through RF fingerprinting," *Can. J. Elect. Comput. Eng.*, vol. 32, no.1, 2007, pp. 27-33.

[7] V. Brik et al.," Wireless device identification with radiometric signatures," *Proc. 14th ACM international conf. Mobile comput. Netw.*, 2008, pp. 116-127.

[8] Y. Sheng et al., " Detecting 802.11 MAC layer spoofing using RSS," *Proc. IEEE Infocom'10, IEEE Press*, Apr. 2008, pp1768 - 1776.

[9] D. B. Faria, "Detecting identity-based attacks in wireless networks using signalprints," *Proc. ACM Workshop Wireless Security*, Sept. 2006, pp. 43 - 52.

[10] Y. Song et al., "Who Is Peeping at Your Passwords at Starbucks?- To Catch an Evil Twin Access Point," *Proc. IEEE DSN'10*, 2010, pp. 323-332.

[11] S. Jana and S. K. Kasera, "On Fast and Accurate Detection of Unauthorized Wireless Access Points Using Clock Skews," *IEEE Trans. Mobile Comput.*, vol. 9, no. 3, Mar. 2010, pp. 449-462.

[12] Y. Shi and M. A. Jensen, "Improved Radiometric Identification of Wireless Devices Using MIMO Transmission," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 4, Sept. 2011, pp1346-1354.

[13] P. L. Yu and B. M. Sadler, "MIMO Authentication via Deliberate Fingerprinting at the Physical Layer," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, Sept. 2011, pp. 606-615.

[14] L. Xiao at al, " MIMO-assisted channel-based authentication in wireless networks," *42nd Annual*

Conf. Inf. Sci. Syst., 2008. CISS 2008, Mar. 2008, pp. 642-646.

[15] P. Baracca, N. Laurenti, and S. Tomasin, "Physical Layer Authentication over MIMO Fading Wiretap Channels," *IEEE Trans. Wireless Comm.*, vol. 11, no. 7, July 2012, pp. 2564-2573.