2013
Electronics and
Telecommunications
Trends

사이버 보안 기술 특집

Ⅰ. 서론
Ⅱ. 아이디 보안 취약성 공격
Ⅲ. 무선 디바이스 식별 기술의 분류
Ⅳ. RF 지문 기술
Ⅴ. 결론

무선랜 환경에서 디바이스 식별 기술 동향

A Technical Trend of Device Identification in WLAN

안개일 (G.I. An) 디바이스보안분석연구실 책임연구원
김신효 (S.H. Kim) 디바이스보안분석연구실 책임연구원

* 본 연구는 미래창조과학부가 지원한 2013년 정보통신 · 방송(ICT) 연구개발사업의 연구결과로 수행되었음(과제명: 차세대 무선랜 고속접속보안 및 실시간 침해방지 보안 핵심기술 개발).

무선랜이 폭발적으로 증가함에 따라, 기술 발전에 힘입은 네트워크 품질은 많이 향상되었지만, 보안 품질은 아직도 요원한 상황이다. 본고에서는 무선랜상에서 아이디 보안 취약성을 이용한 공격들과 이를 탐지하고 방어할 수 있는 디바이스 식별 기술에 대한 동향을 파악한다. 무선랜상에서 아이디 보안 취약성을 이용하는 MAC 속임 공격은 공격자의 존재를 속일 수 있을 뿐만 아니라, 네트워크 및 시스템 권한을 획득할 수 있기 때문에 네트워크 보안에 큰 위협이 되고 있다. 무선 디바이스 식별 기술로서는 인증 방식, 프로토콜 분석 방식, 위치확인 방식, RF 지문 방식 등 많은 기법들이 있다. 본고에서는 이러한 기술들 중에서 현재 가장 활발하게 연구되고 있는 RF 지문 기술을 시스템 구조, 디바이스 식별 방법, 보안 취약성, 그리고 보안 응용 관점에서 자세히 분석한다.

© 2013 한국전자통신연구원

Ⅰ. 서론

최근 스마트폰의 등장과 함께 무선랜 사용이 폭발적으로 증가하고 있다. 이러한 사용자의 요구에 부응하기 위해 802.11n에서 802.11ac로 진화하는 등 더 높은 품질을 제공하기 위하여 무선랜 기술은 계속 발전하고 있다. 그러나 무선랜상에서 발생하는 여러 가지 보안 취약성 문제가 무선랜 발전에 발목을 잡고 있으며, 그 중의 하나가 바로 무선 디바이스의 아이디 취약성 문제이다.

무선랜상에서 무선 디바이스를 가장 확실하게 식별하는 아이디는 MAC(Medium Access Control) 주소이다. MAC 주소는 LAN상에서 네트워크 2계층의 아이디로 사용되고 있다. MAC 주소는 LAN 기반의 네트워크 디바이스를 전역적으로 식별할 수 있기 때문에 802.11 무선 네트워크상에서 인증(허가된 디바이스 식별) 및 인가(허가된 네트워크 및 시스템 권한 수준 식별) 메커니즘으로 흔히 사용되고 있다. 무선랜에서 MAC 속임(spoofing) 공격을 하는 공격자들은 MAC 주소 속임을 통하여 자신의 존재를 속일 수도 있을 뿐만 아니라, 인가된 시스템의 MAC 주소 도용을 통하여 네트워크 및 시스템 권한을 획득할 수 있기 때문에 네트워크 보안에 큰 위협이 되고 있다.

본고에서는 무선랜상에서 무선 MAC 주소를 속임으로써 가능한 공격들을 분석한다. 이러한 공격을 방어하기 위한 무선 디바이스 식별 기술로서는 인증 방식, 프로토콜 분석 방식, 위치확인 방식, RF(Radio Frequency) 지문 방식 등 많은 기법들이 있다. 본고에서는 이러한 기술들 중에서 현재 가장 활발하게 연구되고 있는 RF 지문 기술을 특히 강조하여, 시스템 구조, 디바이스 식별 방법, 보안 취약성, 그리고 보안 응용 관점에서 자세히 분석한다.

Ⅱ. 아이디 보안 취약성 공격

유선 이더넷 네트워크와 마찬가지로 802.11 환경에서도 메시지를 보낸 발신 노드의 주소를 암묵적으로 신뢰하며, 진위여부를 검증하기 위한 어떠한 메커니즘도 제공하지 않는다. 공격자는 자신의 신분을 속이거나 다른 사람의 신분 도용을 통한 해킹을 목적으로 이러한 보안 취약성을 이용한다. 무선랜 MAC 주소를 속임으로써 가능한 공격으로써 de-authentication[1], disassociation[1], power-saving[2], AP 위장[2], 단말 위장 공격[2]이 있다.

1. De-Authentication 공격

무선단말이 무선 네트워크 서비스를 사용하기 위해서는 먼저 AP(Access Point)를 선택하고 그 AP로부터 인증을 받기 위한 authentication 과정을 거쳐야 한다. authentication 프로토콜은 인증을 해제하는 de-authentication 메시지를 정의하고 있다. 공격자는 공격목표인 타깃단말의 MAC 주소를 도용한 위조된 de-authentication 메시지를 AP에게 보냄으로써 타깃단말이 무선 네트워크에 접속하는 것을 방해할 수 있다.

2. Disassociation 공격

무선단말과 AP는 authentication 외에 association 과정을 수행한다. Association 과정은 무선단말과 AP가 전송속도 및 보안옵션을 최종 협상하여 데이터 링크를 설정하는 과정이다. Authentication 과정과 마찬가지로, association 과정에서도 association 연결을 해제하는 de-association 메시지가 정의되어 있다. 공격자는 공격목표인 타깃단말의 MAC 주소를 도용한 위조된 de-association 메시지를 AP에게 보냄으로써 타깃단말이 무선 네트워크에 접속하는 것을 방해할 수 있다.

3. Power-Saving 공격

IEEE 802.11에서는 무선단말의 전원을 절약하는 기능을 제공하고 있다. 무선단말은 슬립(sleep) 모드로 들

어갈 동안 자신에게 전송된 데이터를 AP가 버퍼링하게 하고, 주기적으로 깨어나서 AP로부터 TIM(Traffic Indication Map)을 수신함으로써 자신에게 전송된 데이터가 있는지를 확인한다. 만약 TIM에 자신이 수신할 데이터가 있다는 표시가 있으면 그 데이터를 수신하기 위하여 AP에게 poll 메시지를 보낸다. 이 메커니즘에는 두 가지 보안 취약점이 있다. 먼저, 공격자는 AP 내에 버퍼된 데이터를 수신할 무선단말의 MAC 주소를 도용한 위조된 poll 메시지를 AP에게 전달하거나, AP 주소를 도용한 위조된 TIM 메시지를 공격목표 단말에게 보낼 수 있다. 위조된 poll 메시지를 받은 AP는 버퍼된 데이터를 회신 후 삭제하며, 위조된 TIM 메시지를 받은 무선단말은 수신할 데이터가 없어서 다시 슬립 모드로 들어가기 때문에 그 데이터의 소유주인 무선단말에게 DoS(Denial of Service) 공격을 가할 수 있다. 또 다른 공격으로서 무선단말과 AP 간의 시간동기를 조작하여 무선단말의 TIM 수신을 방해할 수 있다.

4. AP 위장 공격

공격 AP는 정상 AP의 아이디(MAC 주소 및 SSID 등)를 도용함으로써 공격 AP를 정상 AP로 인식하도록 무선단말들을 속일 수 있다. 이러한 공격 AP를 로그(rogue) AP라고도 한다. 로그 AP는 정상 AP와 다른 채널을 사용하거나, 또는 더 강한 신호를 송신하여 정상적인 무선단말들이 자신을 접속하게 만든다. 로그 AP는 접속된 단말들이 위조된 웹 포탈에 접속하도록 하여 사용자의 ID와 암호를 탈취하는 공격을 수행할 수도 있으며, 또는 man-in-the-middle 공격을 통하여 무선단말을 도청하거나 메시지를 위조할 수도 있다.

5. 단말 위장 공격

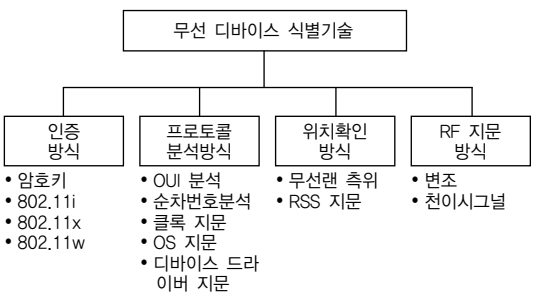
무선랜상에서 무선단말을 인증하는 방법 중 하나가 MAC 주소 기반의 접근제어 인증이다. 공격자는 정상 무선단말의 MAC 주소를 위조하여 인증검사를 통과함으로써 무선랜뿐만 아니라 무선랜에 연결된 네트워크 자원들을 마음대로 접근하여 사용할 수 있게 된다.

Ⅲ. 무선 디바이스 식별 기술의 분류

무선랜상에서의 아이디(특히 MAC) 보안 취약성 문제에 대응하기 위하여 MAC 주소가 위조된 무선 디바이스를 탐지할 수 있는 무선 디바이스 식별 기술이 제안되었다. (그림 1)에 도시된 바와 같이 무선 디바이스 식별 기술은 크게 인증 방식, 프로토콜 분석 방식, 위치 확인 방식, 그리고 RF(Radio Frequency) 지문 방식으로 분류될 수 있다.

1. 인증 방식

인증 방식은 공유키나 비밀키 등의 키 설정을 통하여 사용자 및 디바이스가 무선랜에 접근할 권한이 있는지를 확인하는 암호학적인 인증 방식[3]이다. 무선 디바이스 인증은 디바이스 내에 암호키를 내장하고, 이를 이용한 서명과 검증을 통해 수행될 수 있다. 사용자 인증을 위해서 IEEE 국제표준단체에서는 802.1x 인증을 포함하는 802.11i를 표준으로 정의하고 있다. 또한 802.11 MAC의 보안 취약성으로 야기되는 de-authentication 공격 및 disassociation 공격을 방어하기 위한 목적으로 무결성 검증을 제공하는 관리 프레임 보호 기능을 802.11w 표준으로 정의하고 있다.



(그림 1) 무선 디바이스 식별 기술 분류

2. OUI 분석 방식

네트워크 카드를 생산하는 하드웨어 제조사들은 자사의 제품을 식별할 수 있도록 IEEE 국제표준단체로부터 MAC 주소의 프리픽스(prefix)로 사용되는 3바이트 OUI(Organizationally Unique Identifier) 값을 할당받는다. OUI 분석 방식[4]은 수신한 MAC 주소의 OUI 값이 IEEE에 등록되지 않은 값이거나, 또는 수신한 MAC 주소로 식별되는 디바이스의 제조사명과 미리 등록된 제조사명과 서로 다른지를 비교함으로써 MAC 주소 속임 공격을 탐지한다.

3. 순차 번호 분석 방식

802.11 네트워크의 MAC 계층에서는 4비트의 프레그먼트(fragment) 번호와 12비트의 순차번호(sequence number)로 구성된 2바이트의 SEQ(SEQuence) 제어 필드를 정의하고 있다. 순차번호는 패킷당 1씩 증가한다. 프레임 크기가 크면, 전송측에서는 순차번호를 고정하고 프레그먼트 번호만 증가시키면서 패킷을 전송한다. 수신측에서는 순차번호와 프레그먼트 번호를 사용하여 패킷을 재조립한다. 기존 무선공격 툴들은 대체적으로 무선카드의 펌웨어 기능을 제어하는 기능을 제공하지 않기 때문에, 공격자는 전송하는 프레임의 SEQ 필드 값을 바꾸지 못한다. 순차 번호 분석 방식[5],[6]은 수신 프레임의 순차번호 변화 패턴이 비정상적인지를 분석함으로써 MAC 주소 속임 공격을 탐지한다.

4. 클록 지문 분석 방식

기기에 있는 클록 발진기마다 미세한 시간 차이가 있는데 이것을 발진기 왜곡(clock skew)이라고 한다. 클록 지문 분석 방식[7]은 타임스탬프를 사용한 TCP 프로토콜이나 ICMP 프로토콜을 사용하여 그 미세한 클록 차이를 측정하고, 미리 등록된 참조 클록 지문(클록 차이 값)과 서로 일치하는 지를 비교함으로써 무선 디바이스의 MAC 주소가 위조되었는지를 탐지한다.

5. OS 지문 방식

OS(Operating System) 지문 방식[4]은 무선 디바이스의 운영체제를 식별하는 방식이다. 다른 OS상에서 구현된 무선 시스템은 TCP, UDP, ARP 그리고 ICMP 패킷을 생성할 때 서로 다른 특성을 갖는다. OS 지문 방식은 무선 디바이스가 보낸 패킷(예, TCP SYN)을 수집하고 분석하여 결정한 OS가 사전에 등록된 OS와 서로 같은지를 검사함으로써 MAC 주소 속임 공격을 탐지한다. OS 지문 방식은 수동형 방식과 능동형 방식으로 나눌 수 있다. 수동형 방식은 네트워크 패킷 모니터링을 통해 디바이스의 OS를 식별하는 방식이고 능동형 방식은 상대 시스템에게 패킷을 보낸 후 그 응답을 분석하여 OS를 식별하는 방식이다.

6. 디바이스 드라이버 지문 방식

무선단말들은 액티브 스캐닝(active scanning) 모드로 동작하여 무선랜에 접속하는 경우에는 probe request 프레임을 브로드캐스트하면서 각 채널을 검색한다. 무선단말은 한 채널에서 한 프레임을 브로드캐스팅된 후 min-channel-time로서 정의된 시간 동안 기다리며, 다음 채널로 넘어가기 전까지 max-channel-time로서 정의된 시간 동안 기다린다. Probe request 프레임 간의 시간 차이는 디바이스 드라이버마다 미세한 차이가 존재한다. 디바이스 드라이버 지문 방식[7]은 probe request 프레임 간의 시간 차이를 디바이스 드라이버 지문값으로 하여 무선단말을 식별하는 방법이다.

7. 무선랜 기반의 측위 방식

측위 방식[8]은 무선 디바이스의 위치 값을 사용하여 MAC 주소 속임을 탐지하는 방식이다. MAC 주소의 위치에 어떤 변화가 있다는 것은 MAC 주소 속임을 의심

할 수 있다. 측위 방식은 각 AP의 위치를 측정한 후, 원래의 위치 값과 다른지를 검사함으로써 MAC 주소 속임 공격을 탐지한다. 측위 방법은 ToA(Time of Arrival), TDoA(Time Difference of Arrival), AoA(Angle of Arrival), 핑거프린트 방식 등이 있다.

8. RSS 지문 방식

RSS(Received Signal Strength)는 무선 시스템이 발신하는 무선 신호로서 무선 공격자가 그 값을 수정할 수 없기 때문에 시스템을 식별할 수 있는 좋은 특성 값이 된다[5],[9]. 대부분의 상용 802.11 칩셋은 프레임당 RSS 신호를 측정한다. RSS 값은 전송파워, 송신자와 수신자 간의 거리, 물리적 무선 환경에 의존한다. 일반적으로 무선 디바이스는 전송 파워를 갑자기 변화시키지 않기 때문에 같은 MAC 주소인데도 RSS 측정값에 갑자기 심한 변화가 있다는 것은 주소 속임을 의심할 수 있다. 따라서 MAC 주소를 도용하는 공격자와 MAC 주소가 도용된 희생자 디바이스 간의 거리가 멀수록 그 둘의 RSS 패턴이 서로 다르기 때문에 쉽게 MAC 주소 속임 공격을 탐지할 수 있다.

9. RF 지문 방식

RF 특성이란 시그널 천이 동안 관찰되는 특성 및 변조되어 전송되는 파형 특성을 말한다. 일반적으로 같은 무선 칩셋과 같은 펌웨어를 가진 무선 디바이스들도 미세하게나마 서로 다른 RF 특성을 갖는다고 한다. RF 지문 방식[10]-[12]은 무선 디바이스상에서 나타나는 물리계층(physical-layer)에서의 독특한 특징을 기반으로 하여 무선 디바이스를 식별하는 방식이다. 자세한 설명은 다음 장에서 기술한다.

〈표 1〉은 본 장에서 소개한 디바이스 식별 기술을 분석한 결과이다.

〈표 1〉 디바이스 식별 기술 분석

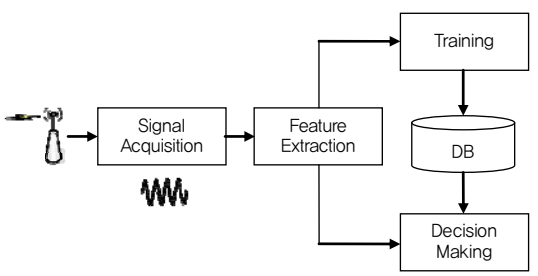
방식 \ 특징	식별 대상	정확도	단점
인증	AP, 단말	최상	자원소모
OUI	AP, 단말	하	재현공격 취약
순차 번호	단말	중	재현공격 취약
클록 지문	AP, 단말	중	재현공격 취약
OS 지문	AP, 단말	중	재현공격 취약
디바이스 드라이버 지문	단말	중	재현공격 취약
측위	AP	상	이동형 불탐
RSS 지문	AP	상	이동형 불탐
RF 지문	AP, 단말	최상	고가

Ⅳ. RF 지문 기술

RF 지문 기술은 물리계층에서의 무선 디바이스 식별 기술이라고도 한다. RF 지문 기술의 목적은 무선 디바이스상에서 나타나는 물리계층에서의 독특한 특징을 기반으로 하여 무선 디바이스를 식별하는 것이다. 물리계층에서의 무선 디바이스 식별 기술은 크게 변조(modulation) 기반 방식과 천이 시그널(transient signal) 기반 방식으로 구분될 수 있다. 본 장에서는 무선 디바이스 식별 시스템의 일반적인 구조를 소개하고 변조 및 천이 시그널 기반 방식에 대해 자세히 기술한다.

1. RF 지문 방식의 구조 및 방법

RF 지문 기반의 무선 디바이스 식별 시스템의 일반적인 구조는 (그림 2)에 도시되어 있다.



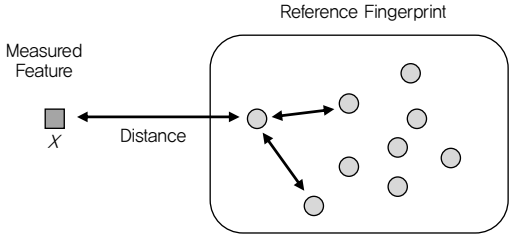
(그림 2) 디바이스 식별 시스템의 일반적인 구조

무선 디바이스 식별 시스템은 다음과 같이 크게 시그널 수집 기능, 물리 특성 추출 기능, 그리고 훈련 및 의사결정 기능으로 분류된다.

- 시그널 수집 기능: 무선랜을 모니터링하면서 무선 디바이스의 무선 시그널을 캡처한다. 무선 시그널을 정확하게 측정하는 것이 매우 중요하다.
- 물리 특성 추출 기능: 무선 디바이스를 구별할 수 있는 특성 정보를 추출하여 선택한다. 오류를 포함하고 있는 데이터는 제거한다.
- 훈련 및 의사결정 기능: 훈련 기능은 새로이 발견된 무선 디바이스를 식별하기 전에, 먼저 합법적인 무선 디바이스에 대한 RF 지문을 측정하여 DB에 저장하는 기능을 말한다. 의사결정 기능은 새로운 무선 디바이스의 신호가 무선랜에서 발견되면 그 디바이스에서 측정된 RF 지문을 DB에 저장되어 있는 RF 참조 지문과 비교함으로써 그 무선 디바이스를 식별하는 기능이다.

훈련 및 의사결정 기능에서 디바이스의 RF 지문을 생성하고 식별하는 분류 알고리즘으로서 K-NNDD(K-Nearest Neighbor Data Description)와 SVDD (Support Vector Data Description Machine) 알고리즘이 많이 사용되고 있다.

K-NNDD 알고리즘[13]은 경계선을 통한 최인접 분류기를 기반으로 하고 있는 단일 클래스 분류 방법으로서 (그림 3)에 도시된 바와 같이 정상적인 참조 지문과 새로이 관측된 지문 간의 거리를 계산하여, 그 값을 미리 정해진 임계값과 비교하여 합법적인 디바이스인지 또는 MAC 주소를 도용한 디바이스인지를 판단한다.



(그림 3) 거리 기반의 단일 클래스 분류 방법

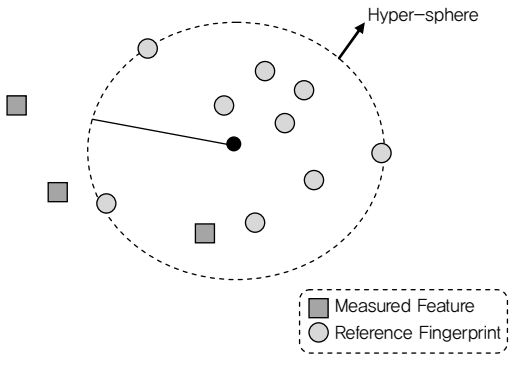
K-NNDD에서는 식 (1)과 식 (2)와 같은 수식에 따라서 무선 디바이스를 식별한다.

$$d_1(x) = \sum_{i=1}^{k_1} \frac{ed(x - NN_i(x))}{k_1} \quad \cdots\cdots\cdots\cdots\cdots\cdots \text{식 (1)}$$

$$d_2(x) = \sum_{i=1}^{k_1} \sum_{j=1}^{k_2} \frac{ed(NN_i(x) - NN_j(NN_i(x)))}{k_1 \cdot k_2} \cdots \text{식 (2)}$$

여기서, ed는 유클리디언 거리(Euclidean distance)를 말하며, $NNi(x)$는 관측된 특성 값 x와 i번째로 가까운 참조 지문값을 말한다. k_1은 관측된 특성값과 비교할 참조 지문값의 개수를 말하며, k_2는 k_1개의 참조 지문값 각각에 대해 비교할 참조 지문값의 개수를 말한다. 식 (1)의 $d_1(x)$는 관측된 특성 값과 인접한 참조 지문값 사이의 평균 거리를 의미하며, 식 (2)의 $d_2(x)$는 $d_1(x)$에서 서 선택된 참조 지문값들과 그들과 인접한 참조 지문값들 사이의 평균 거리를 의미한다. $d_1(x)$의 값이 $d_2(x)$보다 크면 그 특성 값이 참조 지문과 부합되지 않는다고 판단하여 그 특성 값을 갖는 무선 디바이스는 위조된 디바이스로 판정한다.

SVDD 알고리즘[14]은 주어진 데이터에 대해서 그 데이터를 분리할 수 있는 초평면(hyperplane) 중에서 가장 거리가 먼 초평면을 찾는 방법인 SVM(Support Vector Machine)의 한 응용 형태로서 단일 클래스 분류를 제공한다. SVDD의 기본개념은 (그림 4)에 도시되어 있다. SVDD는 수집된 합법적인 무선 디바이스의 참조



(그림 4) SVDD의 기본 개념

지문값들을 모두 포함하면서 반지름이 최소인 초구(hypersphere)를 찾는 방법이다.

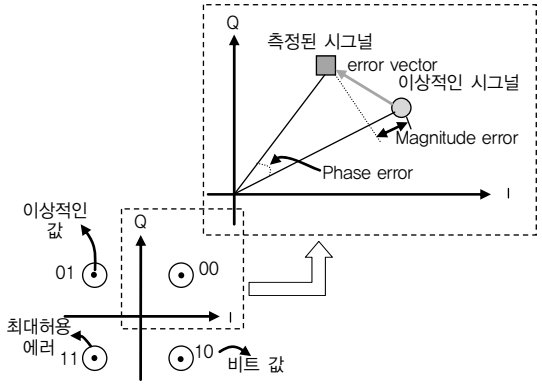
2. 변조 기반의 RF 지문 기술

변조 기반의 RF 지문 기술[11],[12]은 생산되는 모든 무선 트랜시버는 제조상의 오류로 허용할 수 있는 아주 작은 에러가 발생하며, 이러한 에러는 같은 회사에서 출시된 기기들도 서로 다르다는 사실에 입각한다.

(그림 5)는 QPSK(Quadrature Phase Shift Keying)의 네 심볼과 변조 에러를 보여주고 있다. 송신측에서는 두 비트의 데이터 값을 두 개의 부 반송파, 즉 I(in-phase)와 Q(quadrature)를 사용하여 π/2의 위상으로 분리하여 인코딩한다. 수신측에서 측정된 그 시그널 값은 이상적인 시그널에 매핑되어야 하지만, 하드웨어 손상, 채널 특성, 수신측 모듈 노이즈로 인해 변조 에러가 발생한다.

변조 기반의 RF 지문 기술은 이러한 변조 에러를 특성값으로 하여 각각의 무선 디비아스를 식별한다. 무선 디바이스의 식별을 위해 특성 정보로서 사용할 수 있는 변조 에러는 〈표 2〉에 나열되어 있다.

변조 기반 기술은 위스콘신 대학을 중심으로 연구가 진행되고 있다. 위스콘신 대학에서 수행된 실험결과를 보면 15m 내에서 이동하는 무선단말들에 대한 식별 정확도가 99%로 매우 높았다.



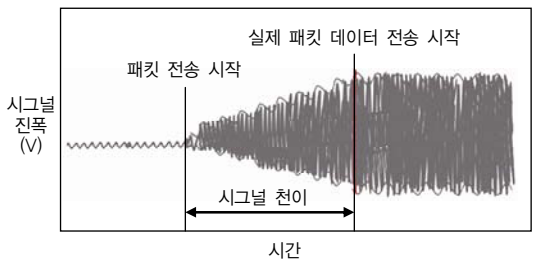
(그림 5) QPSK에서 변조 에러

〈표 2〉 변조 에러에서 RF 특성 정보

RF 특성 정보	설명
Symbol phase error	수신신호의 이상적인 위상각과 관측된 위상각 사이의 차이값
Symbol magnitude error	이상적인 신호의 크기와 관측된 신호의 크기간의 차이값
Symbol error vector magnitude	이상적인 벡터 값과 관측된 벡터 값 간의 벡터 차이값
Frame frequency error	이상적인 캐리어 주파수와 관측된 주파수 간의 차이값
Frame SYNC correlation	데이터 신호를 전달하기 전에 송신측과 수신측은 synchronization preamble(SYNC라고도 함)을 사용하여 동기를 맞춤. 이상적인 SYNC 값과 관측된 SYNC 값의 차이값
Frame I/Q origin offset	(0,0)의 이상적인 I/Q 값과 한 프레임의 모든 측정된 I/Q 값의 차이
Average phase error	한 프레임에 대한 모든 심볼 위상 에러의 평균 값
Average magnitude error	한 프레임에 대한 모든 심볼 크기 에러의 평균 값
Average error vector magnitude (EVM)	한 프레임에서 발생하는 이상적인 에러 벡터 값과 관측된 에러 벡터 값간의 모든 벡터 차이값

3. 천이 시그널 기반의 RF 지문 기술

천이 시그널 기반의 RF 지문 기술[10]은 무선이 켜질 때 정상상태로 가기 바로 전에 발생하는 천이단계 동안 관찰되는 유일한 특성을 이용한다. (그림 6)은 새로운 패킷을 전송할 때 발생하는 무선신호를 도시한 것이다. 패킷 전송을 위해 신호가 송출되는 시점과 실제 패킷 데이터에 해당하는 신호가 송출되는 시점(약 150ns) 사이



(그림 6) 무선 시그널의 천이 모양

에 시그널 천이가 발생한다. 이러한 특성이 유일하게 구별되는 이유는 디바이스의 아날로그 컴포넌트, 즉 트랜시버의 안테나, 증폭기(amplifier), 대역 필터기(band-pass filter), 위상 변위기(frequency mixer)가 모델마다 유일하게 구분되는 미세한 차이가 존재하고 이것이 무선신호를 송출할 때 영향을 미치기 때문이다.

천이 시그널 기술은 취리히 연방공과대학교(ETH)에서 많은 연구를 진행하고 있다. 취리히 대학교에서는 고정된 거리에 있는 무선단말들에 대해서 실험을 하였는데, 에러(equal error rate)가 0.24로 무선 디바이스 식별 정확도가 매우 높았다.

4. RF 지문 기술의 보안 취약성 분석

RF 지문 기술도 재현 공격에 위협을 받을 수 있다. 재현 공격에는 다음의 두 가지 공격 방식이 있다[15].

- 특성 재현 공격: 공격 대상 디바이스를 구별 짓는 특성 정보와 비슷할 때까지 공격 디바이스의 무선 특성을 바꾸면서 공격하는 방식
- 시그널 재현 공격: 공격 대상 디바이스가 전송하는 시그널을 캡처하여 파형 생성기를 사용하여 그대로 재전송하는 방식

무선특성 데이터인 주파수 오프셋, I/Q 오프셋 , 위상 오프셋 등은 그 값을 조작하는 것이 가능하기 때문에, 이러한 특성을 이용하는 변조 기반의 RF 지문 기술은 상대적으로 특성 재현 공격에 취약하다. 그러나 천이 시그널 기반의 RF 지문 기술은 안테나 방향과 거리 등에 따라 천이 시그널 값이 바뀌므로 특성 재현 공격에 안전하다고 할 수 있다. 시그널 재현 공격은 특성 재현 공격보다 더 단순하면서도 강력한 공격이다. 천이 시그널 기반의 RF 지문 기술이 변조 방식보다 시그널 재현 공격에 더 취약할 수 있다. 공격자는 캡처된 천이 시그널에 공격자의 페이로드를 추가하여 메시지를 위조하는 공격을 시도할 수 있기 때문이다.

비록 RF 지문 기술은 재현공격에 취약하지만, 다른 기술에 비해서는 월등히 안전한 편이다. 공격자가 재현 공격을 하기 위해서는 하드웨어적으로 신호를 조작해야 하기 때문에 무선랜 하드웨어 장비가 요구되며, 또한 신호 분석을 위해 많은 노력과 시간이 요구되기 때문이다.

5. RF 지문 기술의 응용

일반적으로 RF 지문 방식은 디바이스 식별 정확도가 높으며 다른 기술에 비해 재현공격에 안전하므로 다음과 같은 보안 응용에 사용될 수 있다[16].

가. 무선랜에서의 침입탐지

권한 없는 디바이스 및 사용자가 네트워크 자원을 사용할 수 없도록 접근제어의 보조적인 수단을 제공할 수 있다. 접근제어의 기본적인 방법은 암호 기반의 사용자/디바이스 인증이다. 이러한 인증 방식은 인증키가 외부로 유출되는 경우에 큰 문제가 되는데, RF 지문 방식은 인증키가 유출되었는지를 빠르게 탐지할 수 있는 수단을 제공할 수 있다. 예를 들어 공격자가 유출된 인증키를 가지고 무선랜에 접근했을 때, 만약 공격자의 디바이스가 그 인증키 소유자가 주로 사용하는 무선 디바이스가 아니라면 인증키가 유출되었다고 의심할 수 있을 것이다. RF 지문 방식은 이 외에도 로그 AP 및 로그 단말을 탐지하는 데 사용될 수 있다.

나. RFID 복제 탐지

RFID(Radio Frequency Identification) 기술은 도서관, 운송 지불, 동물 식별 등과 같은 많은 분야에서 물품 목록 및 식별 응용으로서 많이 사용되고 있다. RF 지문 기술은 RFID 기반의 신분증 복제를 탐지하는 데 사용될 수 있다. RFID 트랜스폰더를 보호하기 위해 많은 방법들이 제안되었음에도 불구하고, RFID 기반의 신분증

을 복제하는 것은 여전히 가능하다. RF 지문 기술은 무선 디바이스 식별에서 사용했던 방법처럼 RFID 신분증에 대한 시그널지문을 미리 서버에 등록한 후, 향후에 어떤 RFID 신분증이 사용될 때 그 신분증에 대해 측정된 지문과 DB에 저장된 그 신분증의 식별자에 해당하는 참조 지문과 비교하여 복제여부를 탐지할 수 있다. 또 다른 방법으로는 RFID 신분증의 시그널 지문을 RFID 트랜스폰더에 저장하여, 어떤 신분증에 대해 측정된 지문과 그 신분증에 저장된 참조 지문이 서로 같은지를 비교함으로써 복제여부를 탐지할 수 있다.

다. Ad-Hoc 네트워크 보안

센서 네트워크와 같이 멀티홉 네트워크인 무선 ad-hoc 네트워크를 보호하기 위해서 RF 지문이 사용될 수 있다. 무선 ad-hoc 네트워크는 웜홀(wormhole) 공격, 시빌(sybil) 공격, 노드 중복(replication) 공격에 취약하다. 웜홀 공격이란 무선 ad-hoc 네트워크에서 서로 위치가 떨어진 두 공격 노드가 지향성 안테나 또는 유선을 통해 직접 연결하여 터널을 생성하는 것을 말한다. 공격자는 생성된 터널을 이용하여 패킷을 도청하거나 위변조할 수 있다. 시빌 공격이란 공격자가 같은 무선노드에 여러 개의 다른 식별자를 할당하는 것을 말하고, 노드 중복공격이란 여러 개의 무선 노드에 같은 식별자를 사용하는 것을 말한다. 이러한 공격들은 RF 지문 기술을 사용함으로써 메시지를 전송한 노드가 등록된 합법적인 노드인지를 확인할 수 있다.

V. 결론

본고에서는 무선랜상에서 아이디 보안 취약성을 이용한 공격들과 이를 탐지하고 방어할 수 있는 디바이스 식별 기술에 대해 살펴보았다.

무선 디바이스 식별 기술로서 인증 방식, 프로토콜 분석 방식, 위치확 인 방식, 그리고 RF 지문 방식을 소개하였다. RF 지문 기술은 다른 기술해 비해 디바이스 식별 정확도가 높으며 재현공격에도 안전하므로 가장 활발하게 연구되고 있다. RF 지문 기술은 무선랜 침입탐지 응용뿐만 아니라 RFID 복제 탐지 및 ad-hoc 네트워트 보안에서도 활용되는 등 파급효과가 매우 큰 기술이다. 현재 RF 지문 기술은 실험수준의 오프라인 형태로 운용되고 있기 때문에, 무선 디바이스의 실시간 식별을 제공할 수 있는 상용화 연구가 필요한 시점이다.

용어해설

변조(modulation) 기반의 RF 지문 기술 디지털 신호를 아날로그로 변조할 때 하드웨어 손상으로 발생하는 미세한 변조 에러를 디바이스 식별용 지문으로 사용하는 기술

천이 시그널(transient signal) 기반의 RF 지문 기술 패킷 전송 시 신호가 송출되는 시점과 실제 패킷 데이터에 해당하는 신호가 송출되는 시점 간에 나타나는 고유한 천이 시그널을 디바이스 식별용 지문으로 사용하는 기술

약어 정리

AoA	Angle of Arrival
AP	Access Point
DoS	Denial of Service
EVM	Error Vector Magnitude
IEEE	Institute of Electrical and Electronics Engineers
K-NNDD	K-Nearest Neighbor Data Description
MAC	Medium Access Control
OUI	Organizationally Unique Identifier
QPSK	Quadrature Phase Shift Keying
QPSK	Quadrature Phase Shift Keying
RF	Radio Frequency
RFID	Radio Frequency Identification
RSS	Received Signal Strength
SEQ	SEQuence
SSID	Service Set Identifier
SVDD	Support Vector Data Description Machine
SVM	Support Vector Machine
TDoA	Time Difference of Arrival
TIM	Traffic Indication Map

ToA Time of Arrival
WLAN Wireless Local Area Network

참고문헌

[1] R. Cheema, D. Bansal, and S. Sofat, "Deauthentication/Disassociation Attack: Implementation and Security in Wireless Mesh Networks," Int. J. Comput. Appl., vol. 23, no. 7, June 2011.

[2] G. Lackner, U. Payer, and P. Teufl, "Combating Wireless LAN MAC-layer Address Spoofing with Fingerprinting Methods," Int. J. Netw. Security, vol. 9, no.2, Sept. 2009, pp.164-172.

[3] 김신효 외, "차세대 무선랜 보안 기술 동향," 전자통신동향분석, vol. 28, no. 1, 2013. 2, pp. 100-109.

[4] K. Tao, J. Li, and S. Sampalli, "Detection of Spoofed MAC Addresses in 802.11 Wireless Networks," ICETE, 2007, Commun. Comput. Inf. Sci., vol. 23, 2007, pp. 201-213.

[5] D. Madory, "New Methods of Spoof Detection in 802.11b Wireless Networking," Master's Thesis, Darmouth College, June 2006.

[6] F. Guo and T. Chiueh, "Sequence Number-Based MAC Address Spoof Detection," LNCS, vol. 3858, 2006, pp. 309-329.

[7] R. Rubino, "Wireless Device Identification from a Phase Noise Prospective," Master's Thesis, University of Padova, Ma. 2010.

[8] 조영수 외, "실내외 연속측위 기술 동향," 전자통신동향분석, vol. 22, no. 3, 2007. 6.

[9] Y. Sheng, "Detecting 802.11 MAC Layer Spoofing Using Received Signal Strength," INFOCOM, Apr. 2008, pp. 1768-1776.

[10] B. Danev and S. Capkun, "Transient-Based Identification of Wireless Sensor Nodes," Int. Conf. Inf. Proc. Sensor Netw. (IPSN), Apr. 2009, pp. 25-36.

[11] V. Brik et al., "Wireless Device Identification with Radiometric Signatures," ACM MobiCom, Sept. 2008, pp. 116-127.

[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, Dec. 2011, pp. 1346-1354.

[13] 손정환, 김성범, "비모수 추정방법을 활용한 kNNDD의 이상치 탐지 기법", 대한산업공학회지, vol. 38, no. 3, 2012. 9, pp. 191-197.

[14] D. M.J. TAX, R. P.W. DUIN, "Support Vector Data Description, " Journal Machine Learning, vol. 54 issue 1, Jan. 2004, pp. 45-66.

[15] B. Danev et al., "Attacks on Physical-layer Identification," 10th ACM Conf. Wireless Netw. security (WiSec), Mar. 2010, pp. 89-98.

[16] B. Danev, D. Zanetti, and S. Capkun, "On Physical-Layer Identification of Wireless Devices," ACM Comput. Surveys, vol. 45, no. 1, Nov. 2012.