ETRI

2013
Electronics and
Telecommunications
Trends

차세대 무선랜 보안 기술 동향

Technologies for Next Generation Wireless LAN Security

김신효 (S.H. Kim) 스마트객체보안연구팀 책임연구원
이석준 (S. Lee) 스마트객체보안연구팀 선임연구원
권혁찬 (H.C. Kwon) 스마트객체보안연구팀 책임연구원
안개일 (G.I. An) 스마트객체보안연구팀 책임연구원
조현숙 (H.S Cho) 사이버융합보안연구단 단장

* 본 연구는 방송통신위원회 방송통신기술개발사업 일환으로 수행하였음(12-912-06-002, 차세대 무선랜 고속접속보안 및 실시간 침해방지 보안 핵심기술 개발).

사용자들은 스마트폰의 무선랜 접속을 통해 편리하게 인터넷 서비스를 사용할 때 무선 구간 도청의 위험성 정도만 인지하는 수준이지만, 편리하다는 그 이면에는 불특정 다수에 의한 도청 위험성뿐만 아니라, 무선랜은 타 무선 네트워크에 비해 비교적 저렴하고 손쉬운 공격 도구를 이용하여 네트워크 무력화가 가능하다는 큰 단점이 있다. 이에 따라 무선랜 보안성 강화를 위해, IEEE 등 관련 표준화 기구에서는 무선랜 보안과 셀룰러 망 연동, 로밍, 무선 메시 네트워크 등 다양한 활용을 염두에 둔 보안 규격을 정의하였으며, 표준 영역에서 다루지 않는 무선랜 보안 위협에 대응하는 장비에 대한 시장의 요구도 분명하다. 본고에서는 2012년 최신 무선랜 표준에서의 보안 기술과 Gbps급 차세대 무선랜 환경에서의 보안의 취약점을 이용한 공격과 이를 탐지하고 방어하는 무선랜 침해방지 기술에 대하여 논한다.

Ⅰ. 서론

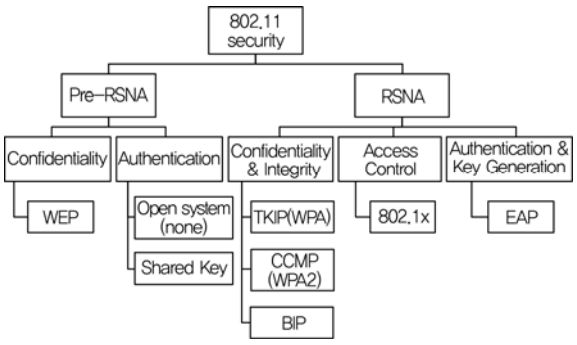
최근 스마트 기기 보급의 폭발적인 증가로 이동통신망에 비해 속도 및 가격 면에서 이점을 가진 무선랜을 통한 인터넷 접속 요구가 많아지고 사설, 공공, 통신망 회사에 의한 무선랜 설치는 해당 주파수에 혼선이 될 정도로 증가하였다. 하지만 무선랜 접속의 편리성 이면에는 무선 전파 수신 범위 내에서 위험에 언제든지 노출될 수 있고 정보 누출의 주요한 통로로 인식되면서 사용자 및 관리자 차원에서 보안 설정 후 사용하거나, 무선랜 보안 장비의 도입을 추진하기 시작하였다. 또한, Gbps급 초고속 무선랜 표준화와 침해방지 등 차세대 무선랜 보안에 대한 시장의 요구가 증대되어 관련 연구 역시 활발히 진행되고 있다. 본고에서는 IEEE 802.11 표준화 기구에서 정의한 무선랜 보안 기술과 차세대 무선랜 침해방지 기술 동향에 관하여 논한다.

Ⅱ. IEEE 802.11 표준의 보안 기술

IEEE 802.11 그룹은 각 태스크 그룹에서 진행한 표준 개정안을 통합하여 2012년도 3월 최신 무선랜 규격을 릴리즈하였다. 이 표준 규격은 전송속도 면에서는 수백 Mbps 속도를 지원하는 802.11n과 관리 프레임 보호 기술, 셀룰러 망 등 타 네트워크와의 연동과 로밍 및 무선랜 메시 네트워크까지 포함하면서 관련 보안 기술도 포함하고 있다[1]. 또한 각 태스크 그룹에서는 Gbps급 전송속도를 지원하는 802.11ac와 고속접속보안을 위한 802.11ai 등에 대한 표준화가 진행 중이다. 최신 802.11 무선랜 표준에서 보안과 관련한 내용을 간추리면 다음과 같다.

- 802.11i(MAC(Medium Access Control) security enhancement)
  - 데이터 프라이버시 보장
  - TKIP(Temporal Key Integrity Protocol)
  - CCMP(Counter Cipher Mode with Block Chaining Message Authentication Code Protocol)
- 802.11w(Management Frame Protection, 이하 MFP)
  - BIP(Broadcast Integrity Protocol)
- 802.11r(Fast BSS(Basic Service Set) Transition, 이하 FT)
  - FT security: 초기 모빌리티 도메인 연결(association)과 재연결, 자원 요청 등
  - FT protocol authentication
- 802.11s/u(Mesh network & Interworking with External Networks)
  - SAE(Simultaneous Authentication of Equals)
  - AMPE(Authenticated Mesh Peering Exchange)

(그림 1)에서 보듯이, 802.11 보안은 RSNA(Robust Security Network Association)로 설명될 수 있다. 즉, 무선랜 보안 표준 영역은 RSNA 이전(Pre-RSNA)과 이후(RSNA), 그리고 기밀성과 무결성, 인증 및 키관리 관점에서 논할 수 있을 것이다. TKIP, CCMP 등 MAC 보안 확장을 제시한 802.11i는 2007년 표준에 포함되어있으나, 무선랜 보안의 근간이 되므로 이를 본고에서도 중심으로 다룬다.



(그림 1) 802.11 보안

1. Pre-RSNA

가. 기밀성 제공 방법

1993년경 초기 무선랜에서 정의한 보안 규격 즉, Pre-RSNA는 무선 구간의 기밀성 제공을 위해 WEP (Wired Equivalent Privacy) 암호 알고리즘이 있으며, 이는 이름에서도 알 수 있듯이, 유선과 동등한 수준의 데이터 보호를 위한 목적으로 개발되었다. WEP에서 사용되는 RC4 스트림 암호는 24비트의 짧은 IV(Initial Vector)를 사용하는 등 암호 알고리즘 자체 취약점이 존재하고, 키분배 메커니즘이 정의되어 있지 않아서 AP와 단말 간 미리 정해진 암호키만 사용하여야 한다. 또한 하나의 AP에 접속하는 모든 단말은 동일한 암호키를 사용하므로, 악의적인 사용자는 자신이 알고 있는 암호키를 이용해 AP에 접속한 다른 사용자의 무선 구간 데이터를 엿들을 수 있는 큰 문제점을 안고 있다.

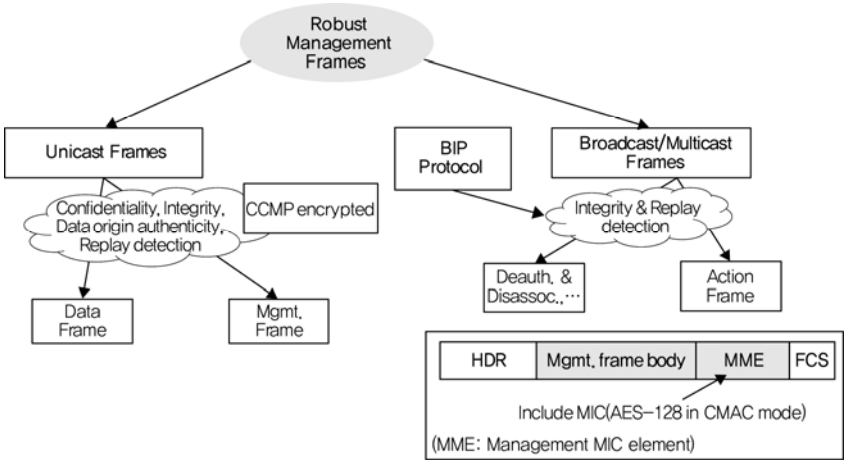
나. 인증 방법

Pre-RSNA의 단순한 인증 방법은 오픈 시스템 인증(Open System Authentication)과 공유키 인증(Shared Key Authentication) 방법이 있다. 오픈 시스템 인증은 인증을 요구하는 모든 단말에 대하여 인증을 허용하는, 실제적으로는 암호학적인 인증이 포함되어 있지 않은 방법이다. 다만 이 과정은 표준에 정의되어 있어 모든 AP와 단말은 초기 연결을 마친 후 반드시 거쳐야 한다. 공유키 인증 방법은 단말과 AP 간 공유하고 있는 암호키를 확인하기 위해서, AP가 인증 요구 메시지에 challenge text를 포함하여 전송하면, 단말은 이 정보를 자신이 알고 있는 WEP 암호키로 암호화하여 AP로 전송하고 이를 확인하는 과정을 통해 인증을 완료한다.

2. RSNA

가. 기밀성 및 무결성 제공 방법

RSN(Robust Security Network)의 기밀성 및 무결성 제공 방법을 개략적으로 표현하면 (그림 2)와 같다. 즉, 단말과 AP 간 유니캐스트되는 데이터 프레임이나 관리 프레임은 일반적으로 CCMP로 프레임 바디를 암호화를 함으로써 기밀성과 무결성 및 재사용 탐지 기능을 제공한다. 반면에, 브로드캐스트 또는 멀티캐스트되는 인증 해제(deauthentication), 연결 해제(disassociation) 등의 관리 프레임 및 자원 할당 등에 활용되는 액션 프레임의 보호를 위해서는 BIP 프로토콜을 사용한다. 이는 암호화가 아니라 CMAC(Cipher-based MAC) 값을 프레임 바디 이후에 추가하여 무결성과 재사용 탐지 기능을 제공한다.



(그림 2) RSN 기밀성 및 무결성 제공 방법

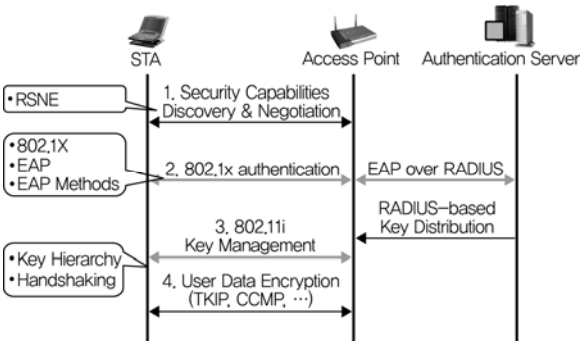
TKIP는 기존 WEP를 지원하는 하드웨어 장비를 대상으로 backward compatibility를 제공하면서도 어느 정도의 보안성을 제공하기 위한 방법으로써, 최근 활발히 출시되고 있는 802.11n 환경에서는 더 이상 기본(필수)으로 제공하지 않는다.

CCMP는 기밀성을 위하여 AES(Advanced Encryption Standard)의 counter 모드와 인증 및 무결성을 위한 CBC-MAC(Cipher Block Chaining-Message Authentication Code)를 결합하여, WEP 및 TKIP에 비해 보안성을 높인 무선 구간 암호 방식이다. 이를 지원하기 위해서는 기존 MPDU(MAC Protocol Data Unit)는 확장되어, 헤더에 암호키 식별자인 Key ID와 PN(Packet Number)을 추가하여 패킷의 재사용을 방지한다.

802.11 표준과는 별도로 무선랜 장비 간 호환성 보장을 위한 Wi-Fi Alliance는, 보안과 관련하여 WPA(Wi-Fi Protected Access) 및 WPA2, 그리고 MFP에 대한 Wi-Fi Certified 프로그램을 운용 중이다[2].

나. IEEE 802.1X 기반의 인증 및 접근제어 방법

RSN 인증 및 접근제어, 그리고 키관리는 단말, AP, 인증서버(대부분 RADIUS(Remote Authentication Dial In User Service) 인증서버)의 세 엔티티에 의해 이루어진다. 먼저 단말과 AP 간 네트워크 발견(network discovery)과 보안 협상(security negotiation) 중에 RSNE(Robust Security Network Information Element)를 교환함으로써 양자 간 보안연결(Security Association, 이하 SA)을 위한 기초정보를 얻는다((그림 3)의 1 과정). 이후 802.1X 표준(2004년도 표준)을 기반으로 하는 인증 과정에 EAP(Extensible Authentication Protocol)로 RADIUS 인증서버와 통신을 거치고((그림 3)의 2 과정), 단말과 AP 간 핸드셰이킹에 의해 키일치로 실제적인 SA를 완료하고((그림 3)의 3 과정), 이후 사용자 데이터에 대한 무선 구간의 암복호가 이루어진다((그림 3)의 4 과정).



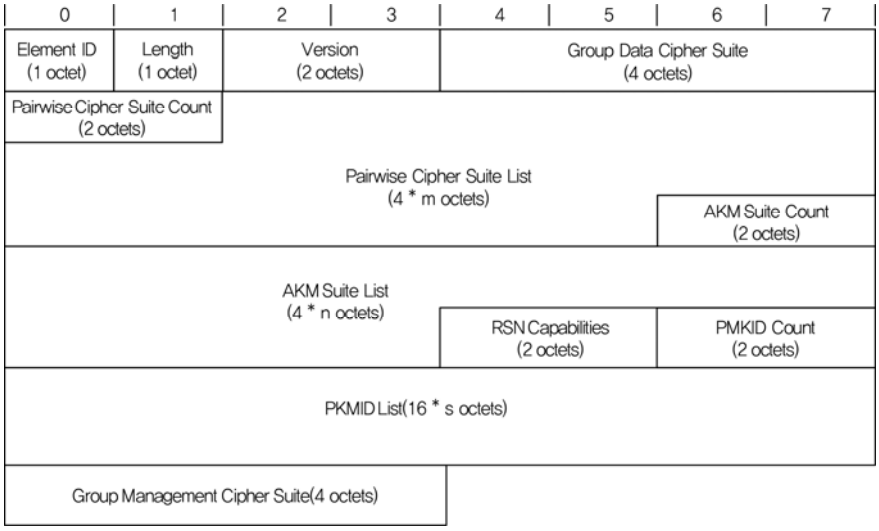
(그림 3) RSN 인증 및 키관리 과정

프로브(probe) 요청 또는 비콘(beacon) 프레임 등에 삽입되는 RSNE는 보안 협상을 위한 정보를 제공하는데, 여기에는 다수의 pairwise cipher suite 및 authentication key management suite, 그리고 하나의 group data cipher suite를 포함한다. 이외에 관리 프레임 보호 기능을 지원하는지 유무 등을 표현하는 RSN capabilities, AP에 연결된 각 단말의 암호키 관리를 위한 다수의 PMKID(Pairwise Master Key Identifier), 브로드캐스팅 관리 프레임 무결성 제공을 위한 group management cipher suite 등으로 구성된다. 이의 구조를 도시하면 (그림 4)와 같다.

다. 키관리 방법

RSNA에서의 주요 암호키는 다음과 같으며, 이 키들은 단말과 AP 간 키 핸드셰이크 과정을 마친 이후에 양쪽에 설치된다.

- PMK(Pairwise Master Key): 단말과 AP 간의 마스터키
- PTK(Pairwise Transient Key): PMK로부터 유도되어 생성되며, 하나의 단말과 AP 간 트래픽 보호에 사용되는 TK(Temporal Key)와 KCK(Key Confirmation Key) 및 KEK(Key Encryption Key)로 구성
- GMK(Group Master Key) 및 GTK(Group Transient Key): 그룹 주소로 전송되는 단말들과 AP 간 마스터키와 이를 이용해 유도되는 트



(그림 4) RSNE 구조

래픽 보호용 키

- IGTK(Integrity GTK): 그룹 주소로 전송되는 관리 프레임에 대한 무결성 제공

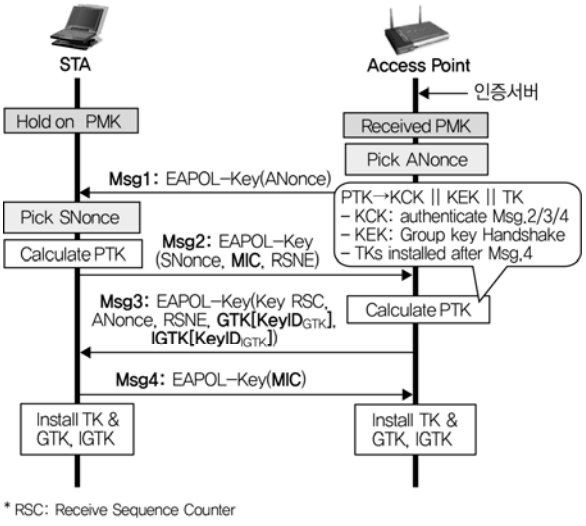
단말과 AP 간 키 공유를 위해서는 EAPOL(EAP over LAN) 메시지를 주고 받는 4-way 핸드셰이크를 필요로 한다. 이 과정은 AP가 ANonce를 임의로 생성하여 첫 번째 메시지를 단말로 전달하고, 단말은 SNonce를 생성하여 ANonce와 함께 PTK를 계산해내는 한편, 자신이 생성한 SNonce를 AP에게 두 번째 메시지로 전송한다. SNonce를 수신한 AP는 PTK를 계산하여, 수신한 MIC(Message Integrity Code)를 통해 이 키 값이 일치하는지 확인하고, 이 키로 GTK 및 IGTK를 캡슐화해서 단말에게 세 번째 메시지를 보낸다. 네 번째 메시지로 단말은 MIC 값을 AP에 보냄으로써, 단말과 AP는 TK, GTK, IGTK를 설치한다. 이 과정을 (그림 5)에 도시하였다. AP가 새로운 GTK 및 IGTK를 다수의 단말에게 배포하기 위해서는 그룹키 핸드셰이크가 필요하며, 이 외에 IBSS(Independent Basic Service Set), FT, 메시 네트워크, peer 통신(단말 간 통신)을 위한 핸드셰이크도 필요 시 수행하여야 한다. 이에 대한 보안 연결은 다음절에서 언급한다.

라. RSN의 보안연결(Security Association)

무선랜 RSN에서 SA가 완료되었음은 보안을 위해 사용되는 정책과 암호키의 집합이 각 종단의 엔티티 내에 일관성 있게 저장되었음을 의미한다.

표준에서 정의하고 있는 RSN의 SA는 다음과 같다.

- PMKSA: 802.1X 키교환 완료, SAE 인증 완료 또는 PMK 캐시 상태
- PTKSA: 4-way 핸드셰이크 또는 FT 4-way



(그림 5) 4-way 핸드셰이크 과정

핸드셰이크 완료
- GTKSA: 그룹키 핸드셰이크, 4-way 핸드셰이크, 또는 FT 4-way 핸드셰이크 완료
- IGTKSA: 그룹키, 4-way 핸드셰이크, FT 4-way 핸드셰이크, FT 재연결 완료
- PMK-R0(PMK, first level) 및 PMK-R1(PMK, second level) SA: FT 초기 모빌리티 도메인 연결 완료
- Mesh PMKSA: 메시 인증 프로토콜 완료
- Mesh TKSA: AMPE 완료
- Mesh GTKSA: AMPE 또는 메시 그룹키 핸드셰이크 완료
- SMK(Station-To-Station Link Master Key)SA: SMK 핸드셰이크 완료
- STK(Station-To-Station Link Transient Key) SA: 4-way SMK 핸드셰이크 완료

Ⅲ. 차세대 무선랜 침해방지 기술

1. 무선랜 공격 및 대응 메커니즘

가. 도청 및 무선 스캐닝

무선랜 도청 및 무선 스캐닝 공격은 크게 2가지 목적을 가진다. 첫째로, 암호화를 하지 않는 무선 구간의 다양한 정보(개인정보, 위치정보, VoIP 도청 등)를 불법적으로 유출하는 것이며, 둘째로는 무선랜 접속과 관련한 정보(SSID(Service Set Identifier), 주변 AP 및 단말의 MAC 주소, 무선 네트워크 종류, 보안 설정 등)를 획득/분석하여 다른 공격을 위한 기반 자료로 이용하려는 것이다.

무선랜 카드와 모니터링 모드를 지원하는 디바이스 드라이버, 그리고 무선랜 프레임 분석 도구를 이용할 경우 기본적인 도청 환경이 구성 가능하며, 무선랜 프레임(즉, L2 계층) 및 L3 계층의 데이터 분석이 가능한 공개 및 상용 도구도 다수 있다. 무선 스캐닝 도구는 브로드캐스트되는 무선랜 신호를 수집하여 SSID는 물론, ARP(Address Resolution Protocol) 또는 DHCP(Dynamic Host Configuration Protocol) 트래픽까지도 조사함으로써 각 무선랜 기기의 MAC 및 IP 주소까지 파악이 가능하다.

이들은 대부분 무선 신호가 도달하는 전파 가청 범위 내에서만 활용이 가능하지만 저렴한 가격으로 구입할 수 있는 원통형 감자칩 용기, 일명 'Cantena'로 가청 범위를 수 km로 확장할 경우, 강력한 공격 도구로 돌변한다. 이와 같은 도청 및 스캐닝은 무선랜의 기본 성격을 이용한 공격으로써 이를 근본적으로 막을 수는 없으나, Ⅱ장에서 설명한 무선랜 사용자 데이터 암호화 등 보안 표준을 준수하면 어느 정도 방어가 가능하다.

나. 서비스 거부 공격

무선랜 서비스 거부 공격은 기존 인터넷 망에서의 서비스 거부 공격과는 다소 다르게, 단말과 AP의 정상적인 통신이 이루어질 수 없도록 RF 신호(즉, 물리 계층) 혹은 무선랜 프레임을 다량 발생하는 형태의 공격이다.

물리 계층상의 서비스 거부 공격은 공격 대상이 되는 AP의 서비스 주파수 대역에 강한 전파를 보내서, 주파수 혼선으로 원활한 서비스가 이루어지지 않도록 하는 공격이다. 일반적으로, 이러한 공격은 AP의 throughput이 매우 저하된 상태가 지속될 경우 또는 RF 신호 분석기 등을 이용하여 공격 유무를 개략적으로 파악할 수 있으나, 정확하게 탐지하기는 다소 어렵다. RF 신호 분석기와 지향성 안테나 등을 이용하여 공격이 이루어지는 위치를 알아내고 물리적으로 그 장치를 제거하는 방법으로 대응이 가능할 것이다.

L2 프레임 위조를 이용한 서비스 거부 공격은, de-authentication, disassociation 프레임 등을 가짜로 보냄으로써 기존의 접속을 끊어버리는 공격, association flooding과 같이 접속을 매우 많이 맺도록 하여 AP의 접속 테이블이 오버플로우가 나도록 하는 등, 다른 정상

단말이 AP에 접속할 수 없도록 하는 공격도 있다. 이러한 공격들은 L2 프레임, 특히 제어 프레임과 관리 프레임을 지속적으로 모니터링하여 단위 시간 동안 비정상적인 패턴의 프레임들이 분석된다거나, duration field의 값이 비정상적으로 클 경우 공격으로 판단할 수 있을 것이다.

EAPOL-Start Flooding, EAPOL-Logoff 위조, 인증 프로세스 내에 임의의 EAP-Success 혹은 EAP-Failure 패킷 삽입, 4-way 핸드셰이크 과정에서의 키 공유가 이루어지지 않도록 하는 공격도 가능하다. 이외에 BIP의 취약점, 즉, AP와 모든 단말이 공통된 그룹키를 사용하는 점을 이용하여 인증을 받은 공격자가 deauthentication 프레임을 생성하여 다른 단말의 연결을 종료시키는 서비스 거부 공격도 가능하다[3]. 이와 같이 인증이 완료되기 이전 또는 인증된 단말에 의해 발생한 서비스 거부 공격은 시도도 어렵지만 이에 대한 대응도 어려운 편이다.

다. WEP 및 WPA 키 크래킹 공격

WEP 프로토콜은 Ⅱ장에서 지적한 바와 같이 다수의 취약점으로 인해 공개 도구로 대체로 3분 이내에 크래킹이 가능한 것으로 알려져 있다. WPA는 일반적으로 키 크래킹이 어렵다고 알려져 있으나, 알려진 단어에 기반한 공격(dictionary attack)은 AirCrack 등의 도구에 의해서도 일부 가능하며, Beck-Tews 공격이라고 알려진 방식에 의해 제한된 환경에서 짧은 데이터 패킷만을 복호화할 수 있는 부분적인 공격도 존재한다.

라. 불법 AP 및 단말에 의한 공격

불법 AP가 내부망의 침입 통로가 되는 경우가 다수이고, 2001년도 한 조사에 따르면 20%의 AP가 불법으로 내부망에 연결되어 사용되고 있지만 네트워크 관리자가 이들을 알아내기가 어렵기 때문에, 대부분의 무선랜 침해 탐지 및 방지 관련 연구는 주로 내부망에 연결되어 있는 불법 AP에 초점을 맞추고 있다.

일반적으로, 무선랜 네트워크 관리자의 보안 정책에 위배되어 설치, 동작하는 모든 종류의 AP 및 단말은 불법 AP 및 단말로 가정할 수 있다. 이는 주로 화이트리스트 및 블랙리스트에 기반하여 탐지한다. 이 리스트에는 허가된(혹은 금지된) 기기에 대한 MAC 주소와 허용된 무선 채널과 SSID, 인증 방식, 암호 방식 외에도 수신 데이터의 timestamp라든지 기기 제조 회사에 따른 RF/모뎀 특성을 구분한 RF 핑거프린팅 정보 등을 포함할 수 있다.

산업계에서는 주로 무선 침입 탐지 및 방지 센서(이하 WIPS(Wireless Intrusion Prevention System) 센서)를 이용해서 센서 주위의 불법 AP 및 단말을 탐지하는 것이 일반적이지만, 센서의 가격이 비싸고 확장성에 한계가 있을 뿐만 아니라 전파 수신 영역 내에서만 활용할 수 있는 등의 제약이 있다. 학계의 연구는 주로 유무선망에서 패킷의 통계적인 특성을 이용해서 불법 AP를 탐지하는 연구가 보편적이지만, 통계적인 정확성을 높이기 위한 연구가 더 필요하다는 단점이 존재한다.

무선 탐지를 이용한 접근 방식으로는 Branch 외의 연구[4], Bahl 외의 연구[5] 등이 있으며, 불법 AP에 대한 물리적인 위치를 판단하는 방법(주로 삼각 측량에 의존)을 포함하고 있다[4],[5]. 유선 탐지를 이용한 접근 방식으로는 Beyah 외의 연구[6], Wei 외의 연구[7], Mano 외의 연구[8] 등이 있는데, 주로 트래픽의 IAT(Inter-Arrival Time), TCP ACK 패킷의 도착 시간, RTT(Round-Trip Time)의 평균 및 분산 등 통계적인 방법을 이용하고 있으며, 이 중에서 Mano 외의 연구는 패킷을 직접 잘라내서 전송하면서 시간을 측정하므로 효율성이 떨어진다는 단점을 가진다[6]-[8]. 이들은 모두 무선랜을 통한 전송 속도가 유선망에 이르지 못할 것이라는 가정하의 연구이나, 무선랜의 속도는 Gbps급에 도달하는 802.11ac 드래프트 규격을 만족하는 칩셋이 일부 출시될 만큼 유무선의 격차가 좁혀진 상태에서도 적용이 가능할지는

〈표 1〉 불법 AP 탐지 솔루션 요구 특성

특 성	설 명
설치가능성 (Deployable)	표준에 대한 수정이 없어야 한다.
확장성(Scalable)	어떠한 크기의 네트워크에 대해서도 제공할 수 있어야 한다.
자기 충족성 (Self-contained)	불법으로 식별하기 위한 특별한 정책이 필요하지 않도록 하여야 한다.
수동적	노드에게 probe 또는 요청은 하지 않아야 한다.
신호 범위에 독립적	거리와 관계없이 불법 AP를 탐지해야 한다.
신호 주파수에 독립적	다른 주파수 대역에서도 불법 AP를 탐지해야 한다.
MAC에 독립적	다른 MAC 프로토콜상에서도 동작하여야 한다.
트래픽 유형에 독립적	TCK ACKs와 같은 상위 레이어의 프로토콜에 의존하지 않아야 한다.
네트워크에 독립적	네트워크 또는 정체 수준에 따라 변경될 수 있는 통계에 의존하지 않아야 한다.
학습 데이터에 독립적	무선 및 유선 네트워크 트래픽의 샘플값에 의존하지 않아야 한다.
선명성(Irrefutable)	수정 가능한 주소로 연결하지 않고, 위조할 수 없는 유일한 특성에 연결하여야 한다.

의문이다.

불법 AP를 탐지하기 위하여, 유선 기반 탐지 기법과 무선 탐지 기법이 함께 사용되어야 정확도가 높아지며, 특히 차후에는 이들 탐지 기법을 알아챈 진화된 형태의 공격, 정상적인 AP 뒤에 숨는 불법 AP 등 다양한 형태의 공격에도 대응할 수 있어야 한다고 주장하였다. 〈표 1〉은 향후의 불법 AP 탐지 솔루션에서 필요로 하는 요구 특성을 요약하였다[9].

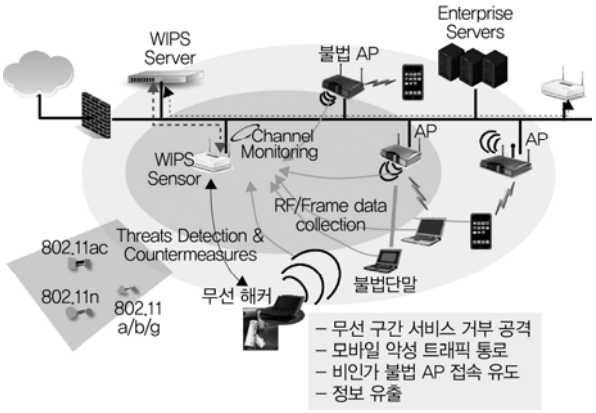
지금까지의 불법 AP와 단말에 대한 대응 및 방어 방식은 서비스 거부 공격을 역으로 이용하는 경우가 대부분이다. 즉, 내부망에 연결된 불법 AP 또는 공격 단말로 의심되는 경우에는 deauthentication 프레임의 소스/도착지 주소를 위조하여 양쪽에 보냄으로써 이 연결을 끊거나, 불법적으로 연결된 AP의 IP 주소 및 MAC 주소가 확인되었다면 ARP 패킷을 위조하여 불법 AP의 IP 주소로 수신되는 패킷이 다른 MAC 주소로 전달되도록 만들어서 정상적인 통신이 이루어지지 않도록 한다.

2. 차세대 무선랜 침해방지 기술

앞 절에서 설명한 바와 같이 802.11 무선랜 보안 표준을 충실히 따르더라도 무선 네트워크에 가해질 수 있는 보안 위협을 모두 대응하기는 현실적으로 어렵다. 기업 또는 공공기관의 내부망 보호를 위해 무선랜 보안 위협을 탐지하고 방어하는 한편, 이들을 통합적으로 관리하기 위한 WIPS 등의 보안 장비를 두는 것이 일반적이다.

WIPS는 (그림 6)에서 보는 바와 같이 불법 AP 및 단말을 탐지하기 위해, 전파 도달 가능 영역별로 무선 구간의 신호를 수집, 분석, 대응하는 WIPS 센서를 배치하고, 이들은 WIPS 서버와의 통신을 통해 제어/관리를 받게 된다. 에어타이트와 에어디펜스, 국내의 코닉글로리 등이 이와 같은 무선랜 WIPS 제품을 판매하고 있다.

하지만 이러한 WIPS 장비는 차세대 무선랜 환경에서 적용하기 위해서는 다음과 같은 점을 고려하여야 한다. 첫째로, MIMO(Multiple Input Multiple Output), 채널 본딩(channel bonding)에 따른 데이터 집합(aggregation), 빔 포밍(beam forming) 등 새로운 VHT(Very High Throughput) 무선랜 전송 기술에 적용 가능하여야 한다. 다시 말하면, MIMO 기술이 적용된 경우에는 여러 안테나를 동시에 감시하고, 본딩된 채널 내의 서브캐리어를 감시하고, 탐지 및 침해 대응도 가능하여야 한



(그림 6) WIPS 개념도

다. 또한 Gbps급 환경에서의 대용량 무선 데이터 수집과 분석, 위협에 따른 대응을 수행할 수 있어야 한다.

둘째로는, 위장 또는 복제된 AP 및 단말을 정확히 식별하여 위치추적 기반으로 보안 위협을 분석할 수 있는 기술 개발이 필요하다. 특히 MAC를 복제하여 설치된 불법 AP는 위험도에 비해 복제 유무를 정확히 판단하는 것도 어렵고, RF 핑거프린팅을 활용하는 방안이 참고문헌 [10]에서 일부 제시되었지만 이를 상용 제품에 활용하기까지는 기술적인 진전이 필요할 것으로 판단된다 [10]. 또한 급증하는 스마트 모바일 기기에 의한 보안 위협에 대응하기 위해서 타 보안 인프라(예를 들면, MDM(Mobile Device Management) 서버, 인증서버, 테더링 감시 프로그램)와 연동하여 감시 및 보안 성능을 높이고 분석도 용이하도록 할 필요가 있다.

마지막으로, 서비스 제공자 입장에서는 스마트 모바일 기기의 폭증으로 인해 가속화되고 있는 무선자원의 비효율적인 사용을 해소하고, 사용자 입장에서는 접속 단절을 피하면서 수백 밀리초 내의 짧은 보안 접속 시간을 보장하면서 일부 침해방지 기능을 제공하는 차세대 무선랜 보안 AP에 대한 기술 개발이 필요할 것이다.

Ⅳ. 결론

지금까지 차세대 무선랜 환경에서의 기밀성 및 무결성 제공과 인증, 접근제어 및 키관리 기술 등 802.11 표준에서의 보안 기술과 침해방지 기술에 대하여 살펴보았다. 특히 무선랜 보안 표준을 충실히 따르는 것 외에도 무선 보안 위협을 차단하고 관리할 수 있는 WIPS 및 유무선 위협 관리 솔루션이 기업망 등에서는 필수적임을 확인하였다.

BYOD(Bring Your Own Device) 등장으로 이를 통한 불법적인 내부망 접속, 스마트 모바일 기기에 의한 불법적인 접속과 멀웨어(malware) 이식의 가능성, 위장 AP 또는 모바일 핫스팟을 통한 데이터 유출 가능성 등 그동안 비교적 견고하게 보호되고 있다고 여겨지던 내부망에 대한 무선 보안 위협은 더욱 확대 추세에 있다. 더군다나 무선랜 접속이 고속, 대용량 서비스 지원이 가능해지면서 이들 환경까지 염두에 둔 차세대 무선랜 위협 탐지 및 대응 기술 개발은 더 이상 미룰 수 없는 시급한 과제이다.

용어해설

RSNA(Robust Security Network Association) 2007년 제정된 802.11i 무선랜 보안 표준에서 제시한 개념으로서, 무선랜 보안의 근간. RSNA는 두 단말 간(AP도 가능) 인증 또는 4-way 핸드셰이크 등의 보안 연결 과정을 마쳐서 두 단말 간 보안키를 공유하고 있음을 의미

WIPS(Wireless Intrusion Prevention System) 유선 IPS와 유사하게 외부 공격으로부터 내부 시스템을 보호하기 위해 무선랜 환경에서의 보안 위협을 탐지하고 대응하는 시스템. 다만, 선을 내부망에 직접 연결하는 과정 없이도 공격이 가능한 무선랜의 특수성으로 인해 일반적으로 무선 신호 가청 범위 내에 이를 수집/분석/탐지/차단하는 센서를 필요로 함.

약어 정리

AES	Advanced Encryption Standard
AMPE	Authenticated Mesh Peering Exchange
AP	Access Point
ARP	Address Resolution Protocol
BIP	Broadcast Integrity Protocol
BSS	Basic Service Set
BYOD	Bring Your Own Device
CBC-MAC	Cipher Block Chaining-Message Authentication Code
CCMP	Counter Cipher Mode with Block Chaining Message Authentication Code Protocol
CMAC	Cipher-based Medium Access Control
DHCP	Dynamic Host Configuration Protocol
EAP	Extensible Authentication Protocol
EAPOL	EAP over LAN
GMK	Group Master Key
GTK	Group Transient Key
IAT	Inter-Arrival Time
IBSS	Independent Basic Service Set
IGTK	Integrity GTK

IV	Initial Vector
KCK	Key Confirmation Key
KEK	Key Encryption Key
MAC	Medium Access Control
MDM	Mobile Device Management
MFP	Management Frame Protection
MIC	Message Integrity Code
MIMO	Multiple Input Multiple Output
MPDU	MAC Protocol Data Unit
PMK	Pairwise Master Key
PMKID	Pairwise Master Key ID
PMK-R0	PMK, first level
PMK-R1	PMK, second level
PN	Packet Number
PTK	Pairwise Transient Key
RADIUS	Remote Authentication Dial In User Service
RSN	Robust Security Network
RSNA	Robust Security Network Association
RSNE	Robust Security Network Information Element
RTT	Round-Trip Time
SA	Security Association
SAE	Simultaneous Authentication of Equals
SMK	STSL Master Key
SSID	Service Set Identifier
STK	STSL Transient Key
STSL	Station-to-Station Link
TK	Temporal Key
TKIP	Temporal Key Integrity Protocol
VHT	Very High Throughput
WEP	Wired Equivalent Privacy
WIPS	Wireless Intrusion Prevention System
WPA	Wi-Fi Protected Access

참고문헌

[1] IEEE 802.11, "Standard for Information Technology-Telecommunications and Information Exchange between Systems Local and Metropolitan area Networks-Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," 2012.

[2] Wi-Fi Alliance, "The State of Wi-Fi Security Wi-Fi CERTIFIED WPA2 Delivers Advanced Security to Homes, Enterprises and Mobile Devices," White Paper, Jan. 2012.

[3] AriTight, WPA2 Hole196 Vulnerability - FAQs. http://www.airtightnetworks.com/WPA2-Hole196

[4] J. Branch et al., "Autonomic 802.11 Wireless LAN Security Auditing," *IEEE Security Privacy*, vol. 2, no. 3, 2004, pp. 56-65.

[5] P. Bahl et al., "Enhancing the Security of Corporate Wi-Fi Networks Using DAIR," *MobiSys*, 2006, pp. 1-14.

[6] R. Beyah et al., "Rogue Access Point Detection Using Temporal Traffic Characteristics," GLOBECOM, vol. 4, 2004, pp. 2271-2275.

[7] W. Wei et al., "Passive Online Rogue Access Point Detection Using Sequential Hypothesis Testing with TCP ACK-Pairs," *Proc. 7th ACM SIGCOMM Conf. Internet Meas.*, 2007, pp. 365-378.

[8] C.D. Mano et al., "RIPPS: Rogue Identifying Packet Payload Slicer Detecting Unauthorized Wireless Hosts through Network Traffic Conditioning," *ACM Trans. Inf. Syst. Security*, vol. 11, no. 2, 2007.

[9] R. Beyah and A. Venkataraman, "Rogue-Access-Point Detection: Challenges, Solutions, and Future Directions," *IEEE Security Privacy*, vol. 9, no. 5, 2011, pp. 56-61.

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