편집위원 : 정수환(숭실대)

IEEE 802.11w 무선 보안 표준 기술

송왕은, 정수환
숭실대학교

요 약

IT기술의 발전으로 인하여 스마트 폰, 테블릿 PC, 노트북 등의 고사양을 가진 모바일 단말의 보급률이 증가하고 있으며, 모바일 단말이 사용하는 IEEE 802.11 표준 기술 또한 지속적인 보완작업과 개정작업을 통해 지원하는 주파수 대역 확장 되었으며, 데이터 전송속도도 빨라지고 있다. 하지만 기술이 발전하고 있음에도 불구하고, Management Frame의 무결성 확인 과정의 부재로 인한 보안 취약성이 아직 남아 있으며, 이를 악용하는 악성행위자의 ARP Spoofing 공격, AP DoS(Denial of Service) 공격, Mac Spoofing 을 기반한 Rouge AP 공격 등에 취약하다. 공공기관, 회사에서는 위 같은 취약점으로부터 무선네트워크를 보호하기 위해 WIPS 시스템을 도입하였지만, 이 또한 Management Frame의 취약성을 근본적으로 해결 할 수 없었다. 때문에 IEEE 802.11 워킹그룹은 Management Frame 보안성을 향상시킨 IEEE 802.11w-2009 표준 기술이 제안 하였으며, 이로 인해 Management Frame의 무결성을 확인하지 않아 발생하는 취약성으로 인한 보안 위협을 근본적으로 방지할 수 있게 되었다. 하지만 IEEE 802.11w 표준 환경을 적용함으로써 새로운 유형의 보안 위협이 발생되었다. 따라서 본고에서는 IEEE 802.11w 표준에 대하여 살펴보며, IEEE 802.11w 표준 환경에서의 보안 기술에 대한 동향 알아본다.

Ⅰ. 서 론

최근 IT 기술이 급속도로 발전하면서 스마트 폰 테블릿 PC등과 같은 고사양의 모바일 단말의 공급이 늘어나고 있다. 현재 고사양의 모바일 단말은 기존 데스크 탑 PC의 업무환경을 충분히 지원할 수 있는 스펙을 가지고 있기 때문에 자연스럽게 개인의 모바일 단말을 업무에 사용하는 BYOD(Bring on Your Device) 환경이 생겨났으며, 과거와 달리 모바일 단말에서 처리하는 데이터량이 많아지고, 사용하는 테이터의 형식 또한 단순 텍스트 형태가 아닌 동영상, 그림, 문서 등 다양한 형태의 데이터 처리에 대한 요구가 늘어나고 있으며, 이러한 요구에 따라 IEEE 802.11 표준 기술 또한 꾸준하게 발전하고 있다. 흔히 무선랜 (Wireless Local Area Network), Wi-Fi 라고 명칭되는 IEEE 802.11 표준 기술은 1997년 802의 11번째 워킹 그룹으로 시작되었다. 이 후 지속적인 보완 및 개정을 통해 데이터 전송속도는 〈표 1〉과 같이 2Mbps에서 7Gbps까지 증가 하였으며, 지원 주파수 대역은 〈그림 1〉과 같이 기존 2.4GHz와 5GHz 대역 이외에도 900MHz(802.11ah), TV White Space(802.11af) 등의 주파수대역을 지원하는 표준 기술 규격도 새롭게 개정되었다[1].

표 1. IEEE 802.11 표준 별 지원 주파수 및 속도

	주파수 대역	속도 (최대)
802.11	2.4Hz	2bps
802.11 a/g	2.4/5Hz	54bps
802.11 n	2.4/5Hz	600bps
802.11 ac	5Hz	3.2bps
802.11 ad	60Hz	7Gbps

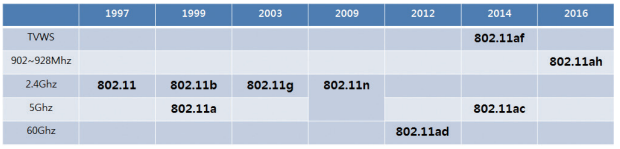


그림 1. 802.11 표준 별 주파수 사용 대역

하지만 지속적인 발전에도 불구하고 여전히 Management Frame의 무결성을 확인하지 않음으로써 발생하는 보안 취약점이 존재한다. 기존의 IEEE 802.11 표준 기술 환경을 지원하는 AP(Access Point)와 모바일 단말은 전송 받은 Management Frame에 대한 추가적인 검증과정 없이 즉각적으로 Management Frame의 요청을 수행한다. 때문에 악성행위자는 Spoofing을 통해 무선 네트워크 상의 AP와 단말의 정보를 변조할 수 있으며, AP DoS, Rouge AP 등과 같은 악성행위를 손쉽게 수행한다. 따라서 공공기관, 기업에서는 악성행위

자의AP DoS, Rouge AP 같은 공격을 방어하기 위해 WIPS 시스템을 이용하여사내 무선 네트워크의 보안을 관리하고 있다. 하지만 WIPS 솔루션은 WIPS Senser를 이용하여 무선네트워크의 악성행위를 감시하기 때문에 서비스가 범위가 제한적이며, WIPS 시스템 자체가 Management Frame의 무결성을 확인 하지 않는 취약점을 이용하여 악성행위자의 단말과 보호대상의 연결을 차단하는 보안 솔루션이다. 따라서 Management Frame의 취약점에 대한 근본적인 해결책이 될 수 없기 때문에 IEEE 802.11 워킹 그룹에서는 Management Frame의 취약점을 강하화기 위해 무결성을 확인하는 과정을 추가함으로써, Management Frame의 보안성을 향상시킨 IEEE 802.11w-2009 표준을 제안하였다[8].

IEEE 802.11w를 무선 네트워크에 적용할 경우 Management Frame의 취약성을 이용한 AP DoS, Rouge AP과 같은 악성행위를 사전에 차단 할 수 있지만, WIPS 시스템이Rouge AP를 탐지하기 전 모바일 단말과 연결 되었을 경우 현재의 WIPS 시스템은 모바일 단말과 Rouge AP간의 연결을 차단 할 수 없는 새로운 보안 이슈가 발생하였다[7].

본고에서는 2장에서는 IEEE 802.11w 표준에 대하여 살펴보고, IEEE 802.11w의 보안 기술 동향에 대하여 알아보며, 마지막으로 3장에서 결론을 내린다.

Ⅱ. 본 론

1. IEEE 802.11w 표준

IEEE 802.11w 표준의 명칭은 MFP(Management Frame Protection)이며, Management Frame의 보안 취약성을 보안하기 위해, 기존 IEEE 802.11 표준에 Management Frame의 무결성 확인 과정을 추가한 표준이다. 현재 IEEE 802.11 표준 환경 하에서 Management Frame을 전송 받은 AP 와 모바일 단말은 전송 받은 메시지의 무결성 검증 작업 없이 즉각적으로 Management Frame의 동작을 수행한다. 따라서 추가적인 보안 솔루션 없이는 Management Frame의 취약성을 이용한 악성행위를 차단 할 수 없으며, 보안 솔루션을 사용하더라도 악성행위를 근본적으로 방지 할 수 없다. 따라서 IEEE 802.11w 표준에서는 단말과 AP간의 Data, Management Frame을 유니케스트로 전송 할 경우, CCMP(Counter with CBC-MAC Protoco) 프로토콜을 사용하여 Frame을 암호화하여 전송한다. CCMP는 무선랜 AES를 기반으로 하며, 128비트 블록 단위로 암. 복호화를 수행한다. AES는 ECB(Electronic Code Book),

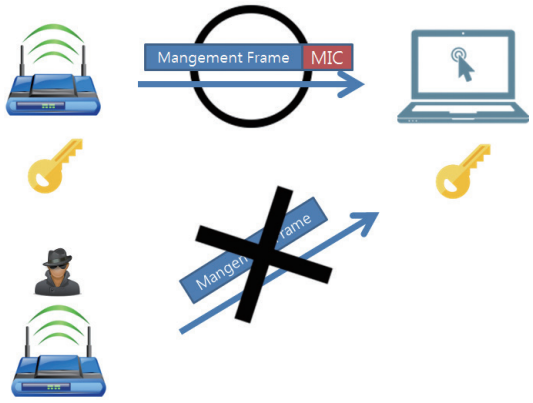


그림 2. MIC를 이용한 무결성 검증

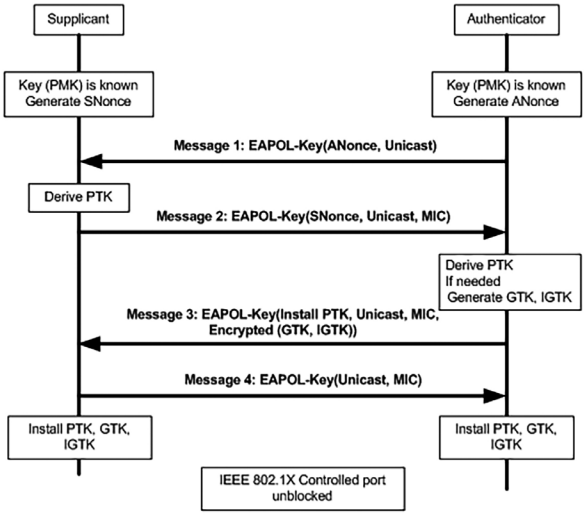


그림 3. 키 핸드 세이크 과정

CBC(Cipher Block Chaining), CFB(Cipher Feedback), OFB(OutputFeedback), CTR(Counter)등 과 같이 5가지의 동작모드로 구성되며, CCMP는 메시지의 인증 및 무결성 검증을 위한 CBC 모드와 메시지의 기밀성을 위한 CTR 모드로 구성된다[2]. 반대로 브로드케스트 또는 멀티케스트를 사용하여 Management Frame을 전송할 경우, BIP(Broadcast Integrity Protocol) 프로토콜을 사용한다. BIP 프로토콜은 CCMP 프로토콜과 달리 Frame 자체를 암호화 하지 않고, 〈그림 2〉와 같이 CMAC(Cipher-based MAC)를 기반으로 하여 생성한 MIC(Message Integrity Code)을 Management Frame 바디에 추가함으로써, AP와 모바일 단말 간에 주고받는 Management Frame의 메시지 무결성이 증명되며, Management Frame의 재사용 유무를 확인 할 수 있다.

〈그림 3〉은 모바일 단말과 AP 간의 키 핸드 세이크 과정을 보여준다. PMK는 키 핸드 세이크 과정이 일어나기 전 AP와 모바

일 단말에 공유된 상태로 가정했다. 핸드 세이크 과정 이 후 생성된 암호 키들은 모바일 단말과 AP에 각각 저장된다. 각 키들의 이름 및 설명은 아래와 같다[3].

- PMK (Pairwise Master Key)
  모바일 단말과 AP간의 키 핸드 쉐이크 과정 전에 공유된 동일한 크기의 키
- PTK (Pairwise Transient Key)
  PMK와 모바일 단말과 AP에서 생성된 랜덤 변수를 이용하여 제작된다. 하나의 모바일 단말과AP간에 트래픽을 보호하는데 사용되는 키
- GTK(Group Transient Key)
  그룹 주소로 전송된 모바일 단말과 AP 간 PMK 와 이를 이용해 유도된 트래픽을 보호하는 키
- IGTK (Integrity GTK)
  그룹 주소로 전송되는 Management Frame의 무결성을 검증하는데 사용되는 키

모바일 단말과 AP의 키 생성 및 공유를 위해서는 EAPOL (EAP over LAN) 메시지를 교환하는 4-Way 핸드쉐이크 과정이 필요하다. 1단계, AP는 랜덤 변수 ANonce를 생성하여 모바일 단말에 전송한다. 2 단계, AP로 전송받은 ANonce와 자신이 생성한 랜덤변수 SNonce를 사전에 AP와 공유된 PMK를 사용하여 PTK를 생성한다. 이 후 MIC를 생성하여 SNonce와 함께 AP에 전송한다. 3 단계, AP는 모바일 단말과 마찬가지로 전송받은 SNonce, ANonce, PMK를 사용하여 PTK를 생성하며, MIC를 확인하여 자신과 모바일 단말이 생성한 PTK와 동일한지 확인하다. 이 후 PTK가 일치할 경우 GTK와 IGTK를 PTK로 암호화하여 모바일 단말에 전송한다. 4 단계, 모바일 단말은 MIC를 AP에 전송하며 과정을 4-Way 핸드 세이크 과정을 맞친다. 이후 AP가 새로운 GTK와 IGTK를 다수의 모바일 단말에 배포하기 위해서는 추가적으로 그룹 키 핸드 세이크 과정이 필요하다[5][8].

키 핸드 세이크 과정이 이루어진 후 Disassociation, Deauthentication과 같은 Management Frame를 브로드케스트 또는 멀티케스트로 메세지를 전송 할 경우, 키 핸드 세이크 과정에서 생성된 IGTK키를 기반으로 생성된 MIC를 Frame 바디에 추가하여 전송함으로써, Management Frame의 무결성이 증명된 후 요청된 동작을 수행한다. 따라서 IEEE 802.11 표준 환경에서 Management Frame의 조작을 통해 이루어졌던, AP DoS 공격과 정당한 AP와 연결된 모바일 단말을 강제로 차단하여 Rouge AP의 연결을 유도하는 공격이 추가적인 솔루션 없이도 방지 할 수 있게 되었다.

2. IEEE 802.11w의 보안

IEEE 802.11w 표준을 무선랜 환경에 적용한다면, 기존 IEEE 802.11 표준 환경에서 발생 되었던 보안 취약성을 향상 시킬 수 있을 것이며, 그 내용은 다음과 같다.

가. DoS(Denial of Service) 공격

DoS공격은 특정 대상의 정상적인 서비스를 방해하기 위한 공격 방식이며, 가장 일반적인 DoS 공격은 타겟 서버의 처리량을 초과하는 데이터를 전송하는 방식이 사용된다. 하지만 무선랜 환경에서 AP에 가하는 DoS 공격은 일반적인 DoS 공격 외에도 〈그림 4〉와 같이 Disassociation, Deauthentication Managem ent Frame 이용한 DoS 공격 방법을 사용한다. 악성행위자는 MAC Spoofing을 통해 모바일 단말의 MAC Address, IP Address, SSID 등을 위조한 Deauthentication Management Frame을 AP에 전송한다. 하지만IEEE 802.11 표준 환경은 Management Frame의 무결성 검증 과정이 없기 때문에 모바일 단말과의 Deauthentication 과정을 수행한다. 때문에 공공기관, 기업들은 자사의 AP와 모바일 단말을 보호하고자, WIPS 시스템을 구축 및 유지해 왔지만 근본적인 해결방법이 될 수 없었다[4][6].

따라서, 기존 Management Frame의 취약점을 향상시키기 위해서 IEEE 802.11w 표준이 제안되었다. 〈그림 3〉과 같이 AP와 모바일 단말 간의 키 핸드 세이크 과정을 통해 생성된 암호화 키로 Management Frame의 무결성을 체크함으로써, MAC Spoofing을 통한 DoS 공격을 근본적으로 차단할 수 있게 되었다. 하지만 IEEE 802.11w 표준은 MAC Spoofing 을 기반한 Management Frame을 변조한 DoS공격 이외 다른 유형의 DoS 공격에 대한 취약점이 남아있다. AP 와 단말이 통신하고 있는 주파수를 재밍시키는 DoS 공격과 무결성 검증 과정이 없

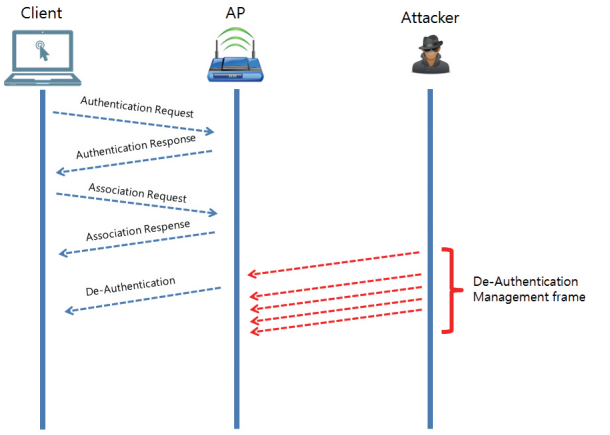


그림 4. AP DoS 공격

는 Layer 2을 이용한 DoS 공격이다. 때문에 IEEE 802.11w 표준 환경을 무선랜에 지원해도 보안 솔루션 구축 및 지속적인 관리 없이는 DoS 공격을 차단 할 수 없다.

나. Honeypot AP

Honeypot AP는 악성행위자가 MAC Spoofing을 통해 정당한 AP의 MAC Address, SSID를 이용하여 만든 악의적인 AP이다. 〈그림 5〉와 같이 악성행위자는 AP와 동일한 SSID를 사용하는 Honeypot AP를 설치하고 신호 강도를 높인다. 이 후 AP에 Deauthentication Management Frame을 전송하여 모바일 단말과 AP의 연결을 차단한다. 모바일 단말이 다시 무선 네트워크에 연결하기 위해 AP와 연결을 시도할 경우, 같은 SSID를 가지더라도 신호 강도가 더 강한 Honeypot AP에 연결을 시도 한다. Honeypot AP은 연결된 모바일 단말을 파싱 사이트로 유도하여 개인 정보를 탈취하거나, 결제를 유도할 수도 있으며, 외부로 전송하는 데이터를 중간에서 가로 챌수도 있다. 때문에 IEEE 802.11 표준 환경에서는 Honeypot AP를 이용한 악성행위를 방지하기 위해 WIPS 시스템을 구축 및 관리했다. 하지만 IEEE 802.11w 표준 환경에서는 악성행위자가 MAC Spoofing을 통해 Honeypot AP을 설치해도, 기존의 AP와 모바일 단말의 연결을 차단할 수 없기 때문에 악성행위를 사전에 방지 할 수 있다. 그러나 DoS 공격과 마찬가지로 IEEE 802.11w 표준을 적용하는 것만으로는 Honeypot AP의 생성을 방지 할 수는 없으며, 일반적으로 Honeypot AP의 신호 강도가 더 강하므로 WIPS 같은 보안 솔루션의 적용이 필요하다.

3. IEEE 802.11w 무선 보안 기술

IEEE 802.11w 표준은 Management Frame 의 무결성을 확인하지 않는 취약성을 강화시킨 무선랜 표준이며, Management Frame의 무결성을 확인함으로써, MAC Spoofing을 통한 AP DoS 공격, Honeypot AP 공격을 방지 할 수 있다. 하지만 IEEE 802.11w표준을 충실하게 수행하더라도 무선 네트워크 환경에서 발생 할 수 있는 모든 악성 행위에 대응 할 수 없다. 따라서, 안전한 무선랜 환경을 구축하기 위해서 보안 솔루션의 구축과 관리는 필수적이다. 공공기관, 회사 등은 자사의 무선랜을 관리하기 위해 WIPS 시스템을 도입하였다[3].

일반적으로 WIPS시스템은 〈그림 6〉과 같이 WIPS 관리 서버와 WIPS Sensor 구성된다. WIPS Sensor는 탐지가능 범위를 실시간으로 검사하며, 악성행위를 감지 할 경우 악성행위를 차단한 이후 WIPS 관리 서버에 결과를 전송한다. WIPS 시스템이 차단하는 대표적인 악성행위는 아래와 같다[7].

가. Rouge AP

관리자로부터 인증 받지 못한 AP이다. 악성행위자의 유,무선 네트워크에 연결되어 있으며, 모바일 단말이 사용하는 데이터를 분석하여 정보를 탈취하거나, 파싱사이트로 유도하는 등 여러가지 악성행위에 이용할 수 있는 공격 방법이다. WUPS 센서를 통해 등록도지 않은 SSID, MAC 감지 될 경우 차단한다.

나. Mis-configured AP

사용자의 미숙한 설정으로 인한 보안 취약점으로써, 잘못된 설정으로 인한 DoS 공격 유발, 악성행위자의 타겟이 될 수 있다. 관리 서버의 사전 설정 정보와 불일치 할 경우 차단한다.

다. Client Mis-association

내부 사용자가 외부 AP에 연결되어 사용 할 경우 내부 데이터가 외부로 유출될 수 있으며, 악의적인 데이터가 내부로 유입될 수 있다. 등록되지 않은 외부 AP MAC주소가 확인 될 경우 연결 해제 요청을 한다.

라. Ad hoc Connection

모바일 단말을 이용하여 인증 되지 않은 AP를 생성하는 공

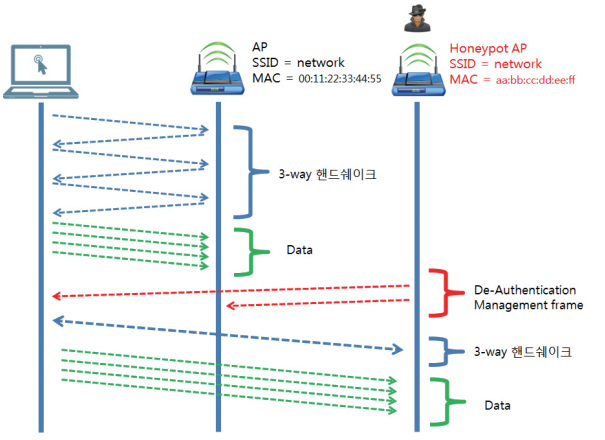


그림 5. Honeypot AP 공격

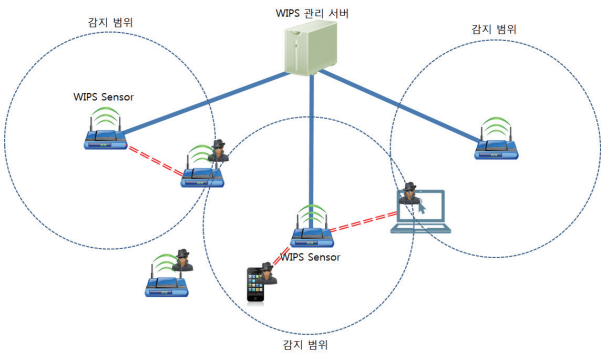


그림 6. WIPS 시스템

격 방법이다. 무선 랜카드를 이용하여 쉽게 구현이 가능하다. Beacon과 Probe Response 데이터 내용 중 Capability Information을 분석하여 IBSS 값이 1인 경우 Adhoc공격으로 판단하여 차단한다.

마. Honeypot AP

Spoofing을 통해 사내 인가된 AP와 동일한 SSID를 이용하여 만든 악의적인 AP이다. 사전에 등록된 SSID가 중복될 경우 SSID와 BSSID의 비교를 통해 Honeypot AP 판단하여 차단한다.

바. AP MAC Spoofing

Honeypot AP와 달리 SSID와 BSSID(MAC address)를 모두 도용하는 공격 방식이다. 사전에 등록된 SSID, BSSID를 비교하여 중복되는 정보를 사용되는 AP를 차단한다.

사. DoS Attack

AP의 정상적인 동작을 방해하기 위해 조작된 Management Frame을 전송하는 공격방식이다. Honeypot AP와 AP MAC Spoofing 공격과 동반 되기도 한다. Management Frame 이 초당 5개 이상 감지 시 DoS 공격으로 판단하여 공격을 차단한다.

하지만 무선 네트워크를 보호하기 위해 개발된 무선랜 표준 기술인 IEEE 802.11w 표준에서 WIPS 시스템을 사용할 수 없는 새로운 보안 이슈가 발생하였다. Rouge AP 탐지 및 차단은 WIPS시스템의 주요한 기능이다. 따라서 사내 네트워크에 Rouge AP가 탐지 될 경우, 즉시 회사의 모바일 단말과 연결을 차단한다. 하지만 감지된 Rouge AP가 IEEE 802.11w 표준을 지원 할 경우 WIPS 시스템은 Rouge AP와 사내 모바일 단말의 연결을 차단할 수 없다[7]. 〈그림 4〉와 같이 WIPS 시스템이 Rouge AP를 감지 할 경우, 변조된 Management Frame을 Rouge AP에 전송하여 모든 연결을 차단한다. 때문에 Rouge AP가 IEEE 802.11w 표준 기술을 사용한다면, 〈그림 2〉와 같이 Management Frame에 MIC 없는 경우 차단 요청이 무시된다. 위의 문제를 해결하기 위해 MIC 탈취, 주파수 대역 재밍, 물리적 차단 등이 제안 되었지만, 모바일 단말과 Rouge AP 간에 생성된 MIC를 변조하기 위해서는 〈그림 3〉의 PTK, GTK, IGTK을 필요하고, 분석에 많은 시간이 소모 됨으로 피해를 막을 수 없다. 또한 주파수 재밍을 할 경우 하나의 Rouge AP를 차단하기 위해 사내의 무선 네트워크에 피해를 입힐 수 있다. 마지막으로 물리적인 차단은 악성행위자가 건물 외부에서 Rouge AP의 신호 강도를 강하게 할 경우 실시간으로 대응하기 어려우며, 추가적인 인력 배치로 인한 금액이 소요된다.

따라서, WIPS 시스템을 IEEE 802.11w 표준에 적용하기 위해서는 위에서 발생된 문제에 관해 추가적인 연구가 필요하다.

Ⅲ. 결 론

본고에서 IEEE 802.11w 표준에 대하여 분석하고 IEEE 802.11w 표준 환경에서의 보안 기술 동향에 대해 살펴보았다. 1997년에 시작된 IEEE 802.11 워킹 그룹은 Management Frame의 무결성을 확인하지 않아 발생하는 보안 취약성을 개선하기 위해서, MIC을 Management Frame의 바디에 추가함으로써, Management Frame의 무결성을 확인 하는 과정을 추가하였다. 그 결과 악의적인 Management Frame을 사전 차단하여 AP DoS, Evil Twin/Honeypot AP의 접속 유도 공격을 방지할 수 있었다. 하지만 재머를 이용한 주파수 대역을 재밍 시키는 AP DoS 공격과 Layer 2를 이용한 DoS 공격은 IEEE 802.11w 표준 기술을 적용하는 것만으로는 대응 할 수 없으며, 기존 무선랜 환경의 대표적인 보안 솔루션인 WIPS가 IEEE 802.11w 표준 기술을 사용하는 Rouge AP를 탐지 할 경우 기존의 동작 방식으로는 이미 연결이 수립된 Rouge AP와 모바일 단말을 연결을 차단 할 수 없는 보안 이슈가 새롭게 발견 되었다.

따라서, 보다 안전하고 효율적인 무선랜 환경을 구축하기 위해서는 IEEE 802.11w 표준을 충실하게 적용하고, WIPS와 같은 보안 솔루션의 구축이 요구된다. 또한 위에서 새롭게 발생할 된 Rogue AP와 모바일 단말의 차단 관련 보안 이슈에 대하여 추가적인 연구가 진행되어야 할 것이다

참 고 문 헌

[1] Jonghyun Baek, SoonTai Park, “국내 무선랜(WiFi) 보안 운영 현황 및 정책 방향”, Korea Institute Of Information Security And Cryptology, REVIEW OF KIISC 21(1), 2011.2, 44-50 (7 pages)

[2] R. Housley, D. Whiting and N. Ferguson, “Counter with CBC-MAC (CCM) : AES Mode of Operation,Proposed to NIST,June 2002.

[3] S.H. Kim, S. Lee, H.C. Kwon, G.I. An, and H.S Cho, “Technologies for Next Generation Wireless LAN Security,” 2013 Electronics and Telecommunications Trends pp. 100-109

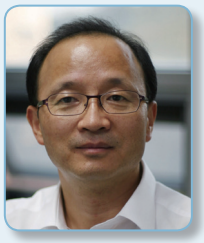
[4] D. Inoue, R. Nomura, and M. Kuroda, “Transient MAC address scheme for untraceability and DOS attack resiliency on wireless network,” in Proc. Wireless Telecommun. Symp., pp. 15-23, Pomona,

U.S.A., Apr. 2005
[5] IEEE, "IEEE 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 Amendment 6: Medium Access Control (MAC) Security Enhancements", IEEE Std 802.11i, July 2004.
[6] AirTight Network, "Airtight network wireless security," AirTight White Paper, 2012.
[7] HP,"802.11w's Impacts on WIPS" HP White Paper, 2014.
[8] 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, Amendment 4: Protected Management Frames" 2009.

약 력

송 왕 은

2014년 숭실대학교 정보통신전자공학부 졸업
2014년~현재 숭실대학교 정보통신공학과 석사과정
관심분야: 클라우드 보안, 모바일 보안, 네트워크 보안



정 수 환

1985년 서울대학교 공학사
1987년 서울대학교 공학석사
1988년~1991년 한국통신 전임연구원
1996년 University of Washington 공학박사
1997년 Stellar one Corp. Senior Engineer
1997년~현재 숭실대학교 전자정보공학부 교수
관심분야: 클라우드 보안, 모바일 보안, 이동 및 무선 네트워크 보안, SNS 보안