한국통신학회논문지 '13-08 Vol.38B No.08
http://dx.doi.org/10.7840/kics.2013.38B.8.632

모바일 단말을 이용한 Whitelist 기반 비인가 AP 탐지 및 접속 차단 기법

박 정 수•, 박 민 호*, 정 수 환°

A Whitelist-Based Scheme for Detecting and Preventing Unauthorized AP Access Using Mobile Device

Jungsoo Park•, Minho Park*, Souhwan Jung°

요 약

본 논문에서는 무선랜 환경의 보안위협에 대비해 모바일 단말 및 원격서버 기반의 무선랜 보안 시스템을 제안한다. 최근 무선랜 환경에서의 보안기술은 다양한 방식으로 제안되고 있으며, WIPS, DLP등 많은 제품들이 출시되고 있다. 하지만 이러한 제품들은 가격이 비싸고, 관리가 힘들다는 점에서 소규모 기업에서는 사용하기가 힘든 실정이다. 따라서 본 논문에서는 BYOD 시장의 발달과 스마트폰 하드웨어의 발전에 맞춰 whitelist를 이용한 단말 및 원격서버 기반의 무선랜 보안 시스템을 제안한다. 제안하는 시스템은 관리자에 의해 AP 및 개인 device에 대한 정보가 서버에 저장되고, 개인의 device에 Application설치만으로도 다양한 무선 네트워크 환경에 적용할 수 있는 장점이 있다.

Key Words : WLAN security, Rogue AP, Remote Server, BYOD, Whitelist

ABSTRACT

In this paper, we proposed a system in a wireless LAN environment in case of security threats, the mobile terminal and the remote server-based WLAN security. The security of the wireless LAN environment in the recent technology in a variety of ways have been proposed and many products are being launched such as WIPS and DLP. However, these products are expensive and difficult to manage so very difficult to use in small businesses. Therefore, in this paper, we propose a security system, wireless LAN-based terminal and a remote server using whitelist according to development BYOD market and smartphone hardware. The proposed system that AP and personal device information to be stored on the server by an administrator and Application installed on a personal device alone, it has the advantage that can be Applicationlied to a variety of wireless network environment.

Ⅰ. 서 론

최근 언제, 어디서나 가능한 네트워크 액세스에 대한 수요 증가는 노트북, 태블릿, 스마트폰까지 포함하도록 확장되었다. 또한 원격 근무자나 직원이 사내에서 이동하면서 편리하게 기업의 네트워크를 사용할 수 있도록 기업의 무선랜 도입이 꾸준히 증가하고 있다. 이런 BYOD(Bring Your Own

※ 본 연구는 미래창조과학부 및 정보통신산업진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었습니다. (NIPA-2013-H0301-13-1003)
◆ 주저자 : 숭실대학교 전자공학과 통신망보안 연구실, ddukki86@ssu.ac.kr, 학생회원
° 교신저자 : 숭실대학교 정보통신전자공학부 통신망보안 연구실, souhwanj@ssu.ac.kr, 종신회원
* 숭실대학교 정보통신전자공학부, mhp@ssu.ac.kr
논문번호 : KICS2013-04-191, 접수일자 : 2013년 4월 25일, 최종논문접수일자 : 2013년 8월 14일

Device) 현상은 조직과 사용자에게 네트워크 보안을 해결하는 방법을 바꿔놓고 있으며, 그중에서도 사내에서 관리하는 무선랜 환경의 보안 수준이 낮아 발생하는 사고가 지속적으로 일어나고 있다. 이러한 낮은 수준의 무선랜 보안 기술은 인터넷상에서 보급되는 전문적인 공격 툴을 이용해 무선 전송구간의 데이터를 유출하거나 내부 네트워크에 침투해 기업의 인프라를 마비시키거나 무력화시키는 사고 및 기업에 설치된 유선네트워크의 보안시스템을 우회해 주요 정보를 빼내는 통로로 활용되고도 있다[1]. 이런 사고들을 막기 위하여 WIPS(Wireless Intrusion Prevention System), NAC(Network Access Control)등의 기술이 발달하였으나, 장비가 비싸고 관리가 힘들다는 점에서 소규모 기업에서는 사용을 하기 힘든 실정이다.

본 논문에서는 이러한 문제점을 해결하기 위한 모바일 단말/원격서버 기반의 무선랜 보안 기법을 제안한다. 모바일 단말은 주변의 AP의 beacon frame 정보를 주기적으로 서버로 전송하여 Rogue AP, Mis-Configured AP, External 등의 위협을 확인할 수 있으며, whitelist 기반의 인가된 AP에만 접속하여 Rogue AP의 접속을 원천 차단하다. 또한, MDM(Mobile Device Management) 솔루션을 이용하여 Rogue Client의 생성도 차단한다.

본 논문의 구성은 다음과 같다. Ⅱ장에서는 무선랜 환경에서 발생가능 한 보안위협 유형과 현재 상용화 중인 WIPS의 개요 및 한계점에 대해 알아보고, Ⅲ장에서 제안 시스템을 통한 모바일 단말과 원격서버 기반의 무선랜 보안 기법 방안에 대해 설명하고, Ⅳ장에서는 기존 시스템과의 비교를 하고 Ⅴ장에서 결론을 맺는다.

Ⅱ. 관련 연구

2.1. 무선랜 보안 위협

최근 위협이 되고 있는 무선랜 위협은 내부 사용자가 외부 AP 또는 네트워크에 접속하는 것을 허용할 것인가, 내, 외부 사용자의 개인 AP를 사내에 설치하는 것을 허용할 것인가, 외부 사용자가 내부에 접속하는 것을 허용할 것인가 이렇게 세 가지로 분류 할 수 있다. 이러한 경우에서 발생할 수 있는 무선랜 위협은 다음과 같다[2].

2.1.1. Rogue AP

Rogue AP들은 사용자 편의성을 위해 무선 보안 기능을 설정하지 않고 임의적으로 설치 및 사용된다. Rogue AP의 설치는 건물 내부에 한정되어 있는 것이 아니라서, 외부로부터의 해킹에 무방비로 노출되는 역할을 한다.

2.1.2. 보안정책 위반(Mis-Configured) AP

무선 랜 AP는 기본적인 보안기능 및 구성 방법을 제공하고 있으나 암호화 미적용, WEP과 같은 약한 수준의 보안 설정 또는 보안 정책에 위반되는 보안설정의 경우 전체 네트워크에 문제를 초래할 수 있게 된다.

2.1.3. 비인가 AP 접속(Client Mis-Association)

인가된 클라이언트가 외부의 비인가 AP에 접속하여 내부의 보안통제 범위를 벗어난 케이스를 말한다. 만약 비인가 AP 접속이 허용되는 경우라면 외부로의 자료유출이 가능하여 막대한 금전적 손실을 초래할 가능성이 높다.

2.1.4. Ad Hoc 연결(Ad-Hoc Connection)

무선 단말들 끼리 AP의 개입 없이 구성되는 네트워크로, Peer-to-peer 연결과 같은 것이다. 무선 사용자가 단말기를 통한 연결을 이용하여 악의적인 침입자가 사용자의 취약점을 검색하거나 공격 가능 하며, 바이러스 감염과 같은 해킹이 가능하다.

2.1.5. AP의 MAC 변조(AP MAC Spoofing)

무선 랜 AP로부터 주기적으로 전송되는 Beacon에는 AP의 MAC 주소(AP고유 ID)와 SSID (네트워크 ID정보)가 포함 되어있다. 클라이언트들은 주변의 다양한 AP에서 전송하는 각기 다른 Beacon의 정보를 수집할 수 있는 소프트웨어 기반 Tool들을 사용하여 SSID와 MAC의 변경이 가능하다. 인가된 AP의 MAC주소를 도용한 불법AP는 Packet Dropping, Corruption, Modification을 통해 무선랜 통신 방해 공격이 가능하다.

2.1.6. 불법복제 AP (Honey Pot AP)

악의적인 목적을 가진 침입자가 SSID와 같은 간단한 기업의 무선랜 정보를 통하여 설치한다. 무선 단말은 전계강도가 강한 AP에 우선 접속하기 때문에, 사용자는 접속된 AP가 정상적인 것인지 인지하지 못하게 되고, 사용자는 자신의 ID, Password와 같은 정보를 전송하게 된다.

2.1.7. DoS Attack

DOS는 공격자의 위치에 따라 내부/외부로 구분이 가능하며, 정상적인 서비스를 방해할 목적으로 대량의 데이터를 보내 대상 네트워크에서 서비스를 제공하는 AP들에 접속된 사용자들을 무선 랜으로부터 무력화 하는 공격이다. 종류에는 SYN Flooding, UDP Flooding, ICMP Flooding 등이 있다[3].

2.2. 무선랜 보안 위협 방지 기법

최근 스마트폰 테더링, 와이브로, 무선랜카드 등을 이용하여 내부 사용자가 인터넷을 우회하여 외부 네트워크에 접속하여 발생하는 보안 위협사례가 많이 증가 하고 있다. 이러한 방법들은 보안 시스템을 우회할 수 있기 때문에, 내부 정보 유출 가능성도 가지게 된다. 이러한 문제점을 해결하는 방법은 다음과 같은 것들이 있다.

2.2.1. IEEE 802.1x 인증 기법

암호화 인증 보안과 접근권한 통제를 중앙관리를 통해 강력한 보호 정책을 펼칠 수 있는 방법이다. 이는 인증하고자 하는 클라이언트 단말과, 인증 중계역할을 하며 통신을 접속 또는 차단하는 인증장치인 AP, 사용자 정보를 구별하여 접속 허용 또는 차단하는 인증 서버가 필요하다. 인증 메시지 교환 시에는 EAP(Extensible Authentication Protocol) 프로토콜을 사용하게 된다. EAP 인증 프로토콜의 유형은 다음 표 1과 같다[4].

표 1. EAP 프로토콜의 유형과 기능
Table 1. Type and funtion of EAP Protocol

Function	MD 5	TLS	TT LS	PE AP	FA ST	LE AP
Client has certificate	X	○	X	X	X	X
Server has certificate	X	○	○	○	X	X
WEP key mangement	X	○	○	○	○	○
Rogue AP detection	X	X	X	X	○	○

2.2.2. WIPS

WIPS는 액세스 포인트(AP)에 접근 권한이 없는 사용자들의 접속을 제한해 데이터를 보호할 수 있는 방법으로, 기존의 유선 방화벽과 VPN 보안 시스템에서 제공되던 보안 기능을 무선랜으로 확장한 것이다. 보안 취약점을 야기하는 기업 내외부의 부적절한 AP와 클라이언트의 연결을 차단, 보안 사고를 예방하게 된다. 또한, 특정 조직에서 운영되는 무선랜을 지속적으로 모니터링 하여 인가되지 않은 무선장비들의 접근을 자동으로 탐지 및 방지함으로써, 무선랜의 안정성을 높이고 통합 관리를 할 수 있도록 지원하는 시스템으로 하드웨어, 펌웨어 또는 소프트웨어 형태 등으로 구현된 다양한 형태의 시스템을 포함한다. WIPS는 노출돼 있는 무선 네트워크에서 이용되는 무선 AP의 범위 내 불법AP나 사용자 단말기를 이용한 침입 시도, 애드혹(Ad-Hoc) 연결, AP의 MAC변조 공격 등을 탐지 및 차단하는 기능을 제공한다. 이를 통하여 무선랜 가용성을 높이고, 불법 침입을 탐지, 차단할 수 있다. 하지만 이러한 WIPS는 실제 설치 및 관리에 있어 비용적인 문제가 있다. 실제로 WIPS 서버는 기기 하나당 약 한화 13,000,000원 수준이고, 센서 하나 당 약 한화 900,000원 이며, 유지비용은 연간 설치비용의 12% 정도라서 소규모 회사에서는 도입하기 힘든 실정이다[5].

2.2.3. NAC (Network Access Control)

NAC(네트워크 접근 제어)는 사용자 PC가 내부 네트워크에 접근하기 전에 보안정책을 준수했는지 여부를 검사하여 네트워크 접속을 통제하는 기술이다. 이러한 NAC은 내부 네트워크에 접근하는 모든 단말에 대하여 접근 제어를 수행하고, IP/MAC 관리 네트워크에 연결 된 모든 단말에 대한 IP/MAC 정보 수집 및 관리를 한다. 또한 허가되지 않거나 웜·바이러스 등 악성코드에 감염된 PC 또는 노트북, 모바일 디바이스 등이 회사 네트워크에 접속되는 것을 원천적으로 차단해 보안수준을 높여준다. 하지만 이런 NAC의 단점은 다음과 같다. 비인가 PC 탐지기능이 떨어지고, 고정 ARP를 통한 우회 ,IP 변조 및 ARP 캐시 포이즈닝을 통한 네트워크 마비 등에 문제를 가지고 있다.

2.2.4. MDM

MDM(Mobile Device Management)은 회사 내의 부서별, 개인별로 IT 정책을 정의하여 차별적으로 적용이 가능한 기업형 모바일 단말 관리 서비스이다. 기업 자산으로서의 모바일 단말기를 위해 소프트웨어 배포나 실시간 진단 및 컨트롤, 원격 백업 및 복구, 삭제, 관리 등의 다양한 기능을 제공한다. 데이터 원격 삭제를 통한 분실관리, 화면 잠금, 암호 길이 및 변경 주기 설정, 디버깅 및 루팅 허용 정책을 통한 보안 설

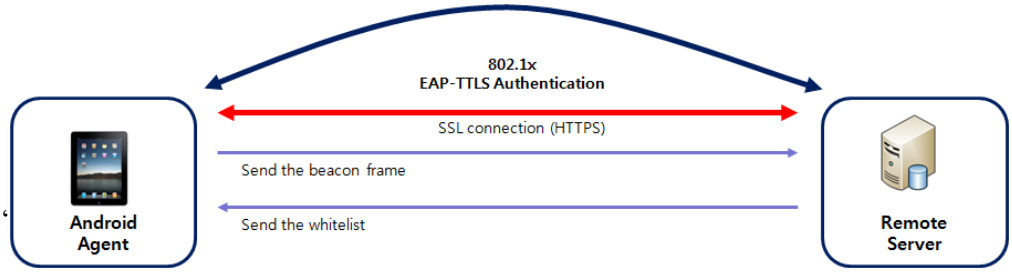

그림 1. 제안 시스템 구성
Fig. 1. Proposed system configuration

정 제어, I/O 제어 및 저장 매체 제어를 통한 모바일 단말 잠금 설정을 할 수 있다. 또한, 어플리케이션 및 프로세스 모니터링을 통하여 관리하고 S/W는 OTA 배포가 가능한 방식이다. MDM의 단점은 다음과 같다. 기업 보안 정책에는 기기 사용 방식에 관한 규칙도 포함되므로 패스워드 설정이나 앱 다운로드 과정 등에 제약이 있을 수 있다. 또한, 기업이 보안상의 이유로 직원 기기에 저장된 모든 데이터(개인적인 사진이나 비디오를 포함한)를 삭제할 수 있게 된다. 또한 기업이 개인기기를 감시할 가능성이 발생하게 된다[6].

2.3. BYOD(Bring Your Own Device)

스마트폰의 발달과 함께 시작된 모빌리티 산업의 발달은 기업의 새로운 통신 플랫폼인 엔터프라이즈 모빌리티를 부각시키며 무선 네트워크 확산을 발전시키고 있다. 이러한 부분에서 스마트 디바이스를 비즈니스에 적극 활용하기 위하여 BYOD 모델의 도입이 확산되는 추세이다. BYOD는 개인 소유의 노트북, 스마트폰, 테블릿을 각자의 업무환경에 맞추어 사용하는 것이다. 개인용과 업무용 구분 없이 사용하는 것이 보편화되는 입장에서 개인 소유의 디바이스를 업무에 이용하는 것은 기업 입장에서도 효율적으로 업무를 진행할 수 있으며, 디바이스 활용에 대한 유연성이 증가하기 때문에 새로운 업무 프로세스로 자리를 잡아가고 있다. 하지만 이러한 BYOD는 허술한 보안이나 관리 정책으로는 오히려 문제를 야기할 수 있다. 따라서 BYOD 도입을 위해서는 보안과 관리에 대한 보다 강력한 조치와 통제 정책이 필요한 시점이다. BYOD 디바이스를 서버에 등록하고 강력한 인증체계와 무선 네트워크의 암호화를 통하여 사용자를 확인하는 과정, 모바일 디바이스의 분실우려를 위한 MDM 기능 구현이 동시에 이루어져야 할 것이다. 또한, 유·무선 인프라에 대한 점검이 지속적으로 이루어져서 안전한 네트워크 구축을 해 두어야 할 것이다[7].

2.4. Whitelist 기반의 보안 시스템

Whitelist를 이용한 보안은 “승인된 것만 보안한다”라는 의미의 시스템으로 안전이 증명된 것만 허용하여 악의성이 입증된 것을 차단하는 블랙리스트방식과는 반대되는 방식이다. 안전이 입증된 것만 허용되기 때문에 보다 강력한 보안성을 유지할 수 있으나 운용의 어려움이 있다. 그러한 이유로 제한적인 활용이 불가피하다. 일반적인 환경에서는 whitelist 기반의 보안을 구성하기에는 많은 한계가 존재하지만, 관리되는 환경에서는 보안성을 향상하고, 효율성을 확대할 수 있다. WIPS 또한, whitelist 기반의 관리를 통하여 관리되고 있다. WIPS에서는 Rogue AP를 탐지하는 방법으로 AP의 passive scanning을 통하여 whitelist 기반으로 판단하게 되는데 , MAC 주소와 AP의 위치, SSID, 채널정보를 이용하여 활용하고 있다. 특히 제안하는 시스템은 관리자에 의해 관리되는 무선랜 환경에서 유용하게 사용될 수 있다. 이러한 whitelist 기반 솔루션이 가져야 하는 특징으로는 엔드포인트의 어플리케이션에 대한 관리방안이 제공되어야 하며, 고정 시스템 및 장비에 쉽게 설치하고 실행이 가능하여야 한다. 네트워크에 연결되어있는 시스템의 경우에는 중앙에서 배포 및 관리가 가능해야 하며, 낮은 하드웨어 사양에서도 동작할 수 있도록 리소스적인 측면을 고려하여야 한다. 본 논문은 이러한 특징들을 이용하여 모바일 단말/원격서버 기반 무선랜 보안 시스템을 제안한다.

Ⅲ. 제안시스템

본 논문에서는 제안하는 모바일 단말/원격서버 기반 무선랜 보안 솔루션은 관리되는 무선 네트워크 환

경에서 BYOD 디바이스에 Application을 설치하고 관리자에 의해 서버에 AP 정보 및 디바이스 정보를 입력하여 관리되는 기능이다.

3.1. 제안시스템 구성

그림 1은 제안시스템의 전체 구성을 보여준다. 모바일 단말, AP, 원격서버를 기반으로 구성되며 서버에서는 최초 APP 실행 시 whitelist를 단말로 전송한다. Whitelist와 단말 정보는 관리자에 의하여 서버에 저장하게 된다. 이때, whitelist는 서버와 SSL 채널을 형성해서 서버로부터 받아오게 된다. 단말은 최초 접속 시 ID/Password를 통하여 서버에 인증하게 되고, 서버는 whitelist를 서버의 인증서를 통하여 서명한 후 전송하여, 서버를 확인시킨다. 단말에서는 whitelist에 등록 된 AP만 접속할 수 있도록 유도한다. Application을 실행할 경우, 최초 화면에 whitelist에 있는 AP만 보여주어 사용자의 AP접속을 유도하는 것이다. 또한, whitelist에 등록 된 AP 이외에 다른 AP는 agent에서 wifi connection을 자동으로 종료하여 선택이 불가하게 하며, 사용자가 안드로이드 기본 설정으로 들어가서 AP를 선택한다고 하더라도 접속 할 수 없도록 한다. 이것은 단말에서 agent가 실행되는 동안, whitelist의 AP 외에는 접속이 불가능 하도록 connection을 끊어 버리기 때문이다. 단말의 블루투스 및 테더링은 MDM 솔루션을 이용하여 application 동작 시에는 사용이 불가능하도록 하여 회사 내부에서 사용자의 Rogue Client 생성을 방지한다. 동작중인 Application에서는 주기적으로 passive beacon frame을 받아 HTTPS 채널을 이용하여 서버로 전송하게 되고, 서버에서는 받아온 beacon frame 정보와 whitelist에 등록된 AP의 MAC, SSID, 인증방식을 비교하게 된다. 악의적인 AP가 MAC, SSID를 위장할 것을 대비하여 인증방식 또한 비교하게 된다. 제안하는 시스템은 EAP-TTLS 인증방식을 사용하고, 만약 공격자가 EAP-TTLS 인증방식을 사용하더라도, ID/Password를 등록하지 않으면, AP에 인증이 되지 않는 시스템이기 때문에 공격자에 의한 MAC 및 SSID spoofing 공격에 대응할 수 있다. 이러한 beacon frame 비교 방법으로 Rogue, Mis-configured, External AP의 동작 유무를 판단할 수 있다. 사용하는 인증 방식은 EAP-TTLS 방식으로, 이는 실제로 대규모 네트워크에 사용되고 있으며, 구현 및 관리가 용이하여 사용하기 편리하다. 서버측의 인증서를 기반으로 인증하는 방식으로 모바일 단말에서는 ID, Password를 통하여 클라이언트를 인증하게 된다. 제안 시스템의 모바일 단말 Agent, AP, 원격서버 각 구성요소와 해당 기능은 표 2과 같다.

표 2. 제안시스템 구성요소의 기능
Table 2. Structural elements's function for proposal system

structural elements	function
Mobile Agent	- Access AP (Registered on the whitelist) - Not registred AP is blocking Locking tethering and bluetooth using MDM Receiving the beacon frame of AP Periodically Sending the beacon frame to server
Access Point	- IEEE 802.1x authentication
Remote Server	- Authentication using EAP-TTLS - Sending the whitelist to device - Web page for managing AP and Device

3.2. 제안시스템 시나리오

그림 2는 application과 서버 동작 시나리오를 보여준다. 회사 출근 기능과 결합한 이 시스템은 회사 출근 시 application을 수동으로 키고 RADIUS 서버와 단말 간 EAP-TTLS 인증 메커니즘을 이용하여 인증을 할 경우, 회사에 출근 기록이 남게 된다. 출근 기록을 기반으로 회사에서 application 동작을 하지 않을 수 없도록 한다. 또한, 회사 외부에서 application을 동작하여 출근 확인을 하는 문제를 해결 할 수 있다. 이때, 최초 인증 시간을 기점으로 디바이스 리소스에 문제가 없는 수준에서 회사 정책상 정해놓은 주기를 이용하여 주변 AP의 passive beacon frame을 받아와 서버로 전송하여 주게 된다. 각기 다른 시간에 각기 다른 디바이스에서 서버에게 beacon frame을 전송하게 하여, 지속적으로 주변의 AP 정보를 탐색하기 때문에 beacon 정보를 받아온 서버는 whitelist와 확인하여 회사 내 불법 AP 설치 유무를 판단 할 수 있도록 한다. 또한, application을 종료할 시 application에서 서버로 종료 메시지를 보내주어서 회사 정책상 정해진 일과 시간 내에 종료하였을 경우 관리자에게 경고 메일을 보내주게 된다.

3.3. 제안시스템 테스트 결과

제안하는 테스트의 구성은 연구실 내부로, 주변에 여러 AP들이 존재한다. 이중 관리되는 AP는 한 개로 SSID는 CNSL이며, MAC 주소는 20:4E:7F:52:8C:90이고, IP는 220.70.2.60, 인증방식은 EAP-TTLS를 사용하게 된다. 이러한 정보를 서버에 저장을 해 두게 된다.

서버에는 그림 3과 같이, AP정보를 저장해 두고, 단말에서 접속을 하였을 경우 인가 된 AP에만 접속하는 화면을 보여준다. 그림 4는 application 실행 후 인가 된 AP list를 받아온 화면이고, 그림 5는 인가되지 않은 AP에 접속을 하려할 때 제한되는 화면이다. 마지막으로 그림 6은 인가 된 AP에 접속한 화면이다. 이와 같이 다른 AP의 접속을 원천 차단하고 인가 된 AP에만 접속할 수 있도록 하였다.

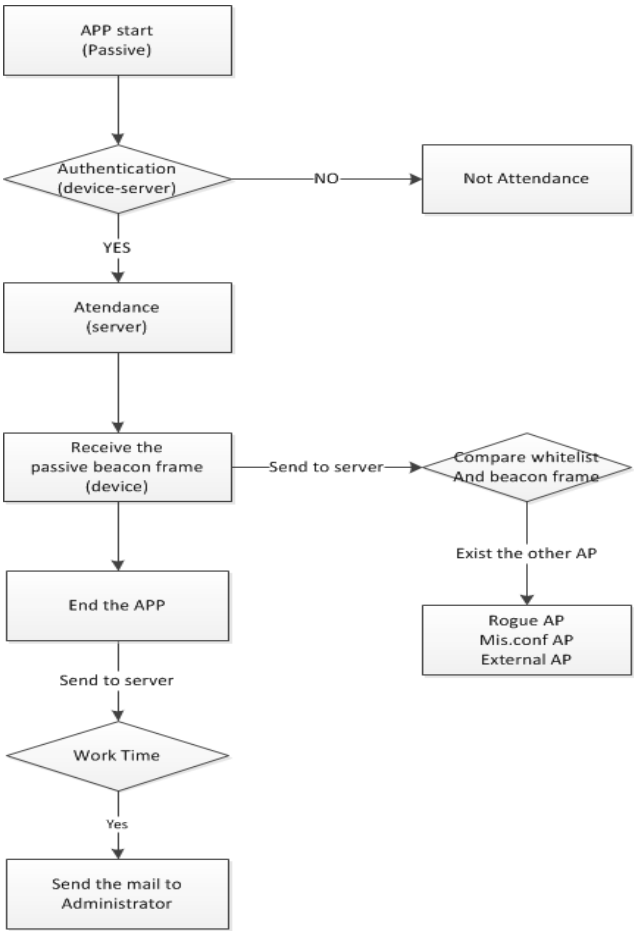

그림 2. 제안 시스템 플로우 차트
Fig. 2. Flow chart for proposal system

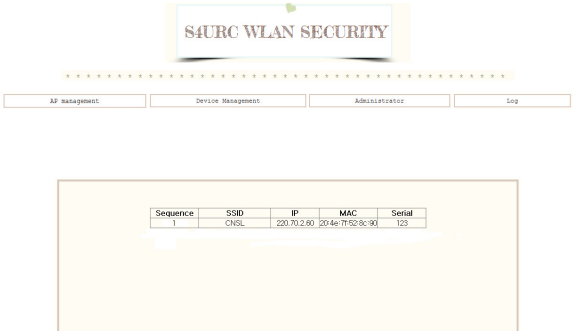

그림 3. 서버에 저장 된 AP 정보
Fig. 3. AP information is stored on the server

그림 4. 주변 AP scan 결과
Fig. 4. AP information is stored on the server

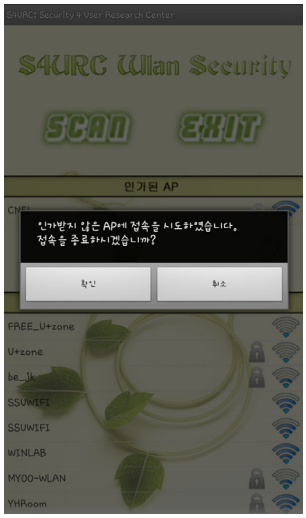

그림 5. 인가되지 않은 AP 접속
Fig. 5. Access the unauthorized AP

그림 6. 인가된 AP 접속
Fig. 6. Access the authorized AP

Ⅳ. 기존 시스템과의 비교

본 제안 시스템은 현재 사용하고 있는 무선랜 보안 솔루션의 기능 중 일부분과 whitelist 기반의 보안방식 및 MDM 솔루션을 결합하여, 모바일 단말 및 원격서버 기반으로 적용하였다. 이는, 기존의 무선랜 보안 솔루션을 구축하는데 소요되는 높은 비용적인 문제와 소규모 기업에서 활용이 어렵다는 문제를 극복할 수 있다. 따라서 비인가 AP 접속 차단, Rogue Client 생성 방지, 비인가 AP 탐지의 기능을 가지게 된다.
이 시스템과 기존 시스템은 가격적인 측면과, 효율성을 중심으로 비교하게 된다. 제안 기법과의 비교는 크게 3가지 탐지 방법을 대상으로 비교하였다. 첫 번째는 AP 기반 탐지 방법이고, 두 번째는 IPRE 방식, 세 번째는 WIPS이다.

AP 기반 탐지 방법은 임베디드 형태의 침입탐지/차단 시스템을 AP에 탑재하여 AP에서 무선 트래픽에 대한 정보를 패킷 캡쳐를 한 후 서버로 전송하여 탐지하는 방법으로, AP에 대한 수정이 불가피 하고, SYN Flooding과 같은 공격에는 유용하며 통합적 보안관리, Rogue AP 탐지 Evil Twin AP 탐지는 가능하나 Mis-configured AP, ARP spoofing 탐지는 어렵다[8].

IPRE(Intelligent Plan Recognition Engine)의 경우는 Agent를 이용하여 위협을 탐지하는 방법으로, 추가적인 Agent를 사용하여야 하고, 각각의 agent에서 위협을 탐지하기 때문에, 확장성 및 가격적인 측면, 관리적 측면에서 제한적이며 또한 이 기법은 IEEE 802.11 무선 패킷 캡쳐가 요구되는 공격은 효율적으로 탐지가 가능하나, mis-configured AP를 탐지하는데 제한적이다[9].

WIPS의 기능은 내부 사용자의 외부 AP의 접속, WEP 키 크랙, DoS 공격, 외부 사용자의 내부 네트워크 접속, MAC주소를 도용한 AP, 정책위반 AP, 비인가 불법 AP등을 정확히 탐지/방지 할 수 있으나 가격적인 측면에서 소규모 기업에 적용하기 힘들다[5]. 제안한 시스템은 WIPS의 모든 역할을 수행할 수는 없으나, 경량화 된 WIPS의 형태로 제한된 네트워크의 접속 및 Rogue Client 생성 방지, 불법 AP 탐지, 내부 사용자의 외부 AP의 접속, 외부 사용자의 내부 네트워크 접속 방지가 가능하다. 또한, WIPS와 같이 무선 인프라를 통합 관제하여 디바이스 및 AP를 관리할 수 있다. 이러한 기능들을 가진 제품들은 구축비용이 드는 반면, 제안한 시스템은 기본적인 서버 사용비용만 제공함으로써, 금액적 측면을 최소화 하였다.

세 가지 방식의 시스템과 비교하자면 기존의 WIPS는 통합 보안관리, Rogue AP 탐지, Evil Twin AP 탐지, Mis-configured AP 탐지가 가능하나, IPRE 및 AP 기반의 탐지는 Mis-configured AP 탐지가 불가능하다. 하지만 제안하는 시스템은 Mis-configured AP 및 비인가 AP의 탐지가 가능하게 된다. 또한 이러한 시스템들은 AP의 수정 혹은 Agent, 서버 및 센서의 설치와 같이 관리가 필요하며 설치비용이 발생하게 된다. 하지만 제안하는 시스템에서는 서버 및 개인 디바이스에 application을 설치하는 방식의 시스템이므로 서버 구축에만 금액이 발생하게 된다.

이 제안 기법은 무선 네트워크 환경에서 기존의 무선랜 보안 솔루션의 고비용에 따른 확장성 문제를 해결하고, whitelist 기반으로 하여 승인된 AP 및 디바이스만 사용할 수 있도록 하는 모바일 단말 및 원격서버 기반의 무선랜 보안 기법이다. 실제 환경에서 간단한 Application 설치 및 관리자에 의한 AP, 디바이스 정보 등록으로 쉽게 적용이 가능하고 관리가 편한 기법이다.

Ⅴ. 결 론

본 논문에서는 무선랜 환경의 보안위협을 방어하기 위하여 단말과 원격서버 기반의 whitelist 기반 보안 솔루션을 제안하였으며, 제안 기법은 서버에서 단말에 설치된 Application에게 AP의 whitelist를 전송하여주고, Application에서는 whitelist AP만 보여주며, 다른 AP는 차단한다. Application은 일정 주기로 AP의 passive beacon frame을 받아와서 주변의 rogue AP, Mis-configured AP, External AP를 탐지하게 된다.

단말은 AP에 접속할 시 서버와 인증절차를 거쳐서 외부자의 내부 네트워크 접속을 차단하다. 또한, 블루투스 및 테더링을 원천 차단하여 기업 내 모바일 단말을 이용한 Rogue client의 생성을 방지할 수 있다. 즉, 내부 사용자가 외부 AP 또는 네트워크에 접속하는 것을 차단하고, 내, 외부 사용자의 개인 AP를 사내에 설치하는 것을 차단 및 탐지하며, 외부 사용자가 내부에 접속하는 것 또한 차단하여 무선랜 보안에서 중요한 세가지 이슈를 만족하게 된다.

본 제안 시스템을 적용함으로써 WIPS나 무선랜 보안 솔루션을 구축하기 힘든 소규모의 기업체에서 무선랜 사용자에 대한 관리 취약점을 해소 할 수 있을 것으로 판단된다. 또한, MDM기능에서의 일부분을 사용함으로 인하여 회사 내의 악의적인 사용자를 미연에 방지함에 따라 최근 이슈가 되고 있는 내부자의 악의적 소행에 의한 문제를 해결 할 수 있다.

References

[1] H. Han, B. Sheng, C. C. Tan, Q. Li, and S. Lu, “A timing-based scheme for rogue AP detection,” *IEEE Trans. Parallel Distrib. Syst.*, vol. 22, no. 11, pp. 1912-1925, Nov. 2011.

[2] J. Burke, B. Hartselle, B. Kneuven, and B. Morgan, *Wireless security attacks and defense*, Retrieved May 2006, from http://http://www.windowsecurity.com/whitepapers/Wireless_Security/Wireless-Security-Attacks-Defenses.html.

[3] 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.

[4] H. Hwang, G. Jung, K. Sohn, and S. Park “A study on MITM(Man in the Middle) vulnerability in wireless network using 802.1X and EAP,” in *Proc. Int. Conf. Inform. Sci. Security (ICISS ‘08)*, pp. 164-170, Hyderabad, India, Jan. 2008.

[5] AirTight Network, “Airtight network wireless security,” AirTight White Paper, 2012.

[6] L. Liu, R. Moulic, and D. Shea, “Cloud service portal for mobile device management,” in *Proc. IEEE 7th Int. Conf. e-Business Eng. (ICEBE)*, pp. 474-478, Shanghai, China, Nov. 2010.

[7] A. Scarfò, “New security perspectives around BYOD,” in *Proc. 7th Int. Conf. Broadband, Wireless Computing, Commun., Applicat. (BWCCA)*, pp. 446-451, Victoria, Canada, Nov. 2012.

[8] G. Chen, H. Yao, and Z. Wang, “An intelligent WLAN intrusion prevention system based on signature detection and plan recognition,” In *Proc. 2nd Int. Conf. Future Networks (ICFN ‘10)*, pp. 168-172, Sanya, China, Jan. 2010.

[9] H.-W. Lee and C.-W. Choi, “Development of malicious traffic detection and prevention system by embedded module on wireless LAN access point,” *J. Korea Contents Assoc. (KOCON)*, vol. 6, no. 12, pp. 29-39, Dec. 2006.

박 정 수 (Jungsoo Park)

2013년 2월 숭실대학교 정보통신전자공학부 졸업

2013년 3월~현재 숭실대학교 전자공학과 석사과정

<관심분야> 무선 네트워크 보안, 암호학

박 민 호 (Minho Park)

2000년 2월 고려대학교 전자공학과 졸업

2002년 2월 고려대학교 전자공학과 석사

2010년 2월 서울대학교 전기컴퓨터공학부 박사

2010년 3월~2011년 4월 삼성전자 네트워크 사업부 책임연구원

2011년 5월~2013년 2월 Carnegie Mellon University, CyLab 박사후 연구원

2013년 3월~현재 숭실대학교 정보통신전자공학부 조교수

<관심분야> SNS 보안, 클라우드 보안, 유무선 네트워크 보안

정 수 환 (Souhwan Jung)

1985년 2월 서울대학교 전자공학과 졸업
1987년 2월 서울대학교 전자공학과 석사
1988년~1991년 한국통신 전임연구원
1996년 6월 University of Washington 박사
1997년 Stellar One Corp. Senior Engineer
1997년~현재 숭실대학교 정보통신전자공학부 교수
<관심분야> 이동 및 무선 네트워크 보안, VoIP 보안, SNS 보안, 클라우드 보안