무선랜 침입 탐지/차단 강화를 위한 무선기기 정보 자동 수집, 관리 시스템 구현에 관한 연구

박종훈○, 김효곤
고려대학교 컴퓨터정보통신대학원
chamsae@korea.ac.kr, hyogon@korea.ac.kr

A study on the automatic information gathering and management system of the wireless devices for reinforcing wireless intrusion detection and prevention

Jong-Hun Park○, Hyo-Gon Kim
Graduate School of Computer & Information Technology, Korea University

요 약

현대 사회는 노트북, 스마트폰 등 무선 통신기기의 발전,확산 및 유무선 통합 컨텐츠의 활발한 개발로 인해 어느 때보다 무선랜의 사용이 확산되고 있다. 하지만 물리적인 침투를 해야만 공격 및 내부정보 접근이 가능한 유선 네트워크에 비해 전파 도달 범위 내의 어디서나 누구나 접속이 가능한 무선 네트워크는 상대적으로 보안 취약점을 내포하고 있다. 이러한 취약점 개선을 위한 가장 중요한 정보가 무선 네트워크에 접속 대상인 인가, 비인가 사용자 정보를 얼마나 효율적으로 수집 관리하는 가에 있다. 현재는 OA 및 보안 관리자가 수동적으로 수집,관리하는 무선기기 정보를 본 논문에서는 자동화 수집 시스템 및 무선 침입차단시스템(WIPS)와 연계한 시스템 아키텍쳐를 제시하고 구현하였으며, 실제 이동통신사 무선 네트워크에 적용하여 정보 수집율이 향상되고 외부 침입에 대한 능동적 대처 능력이 향상되었음을 확인 하였다.

1. 서 론

802.11 기반 무선통신기술 발전과 노트북, PDA 및 스마트폰등 단말기의 다양화로 인해 무선랜 사용자가 급증하고 있다. 무선통신은 유선과 다르게 언제, 어디서나 전파 도달 범위의 무선설비에 자유롭게 접속이 가능하며 허니팟과 같이 자신이 의도하지 않은 상황에서 거짓된 무선설비에 접속됨으로써 내부 정보유출의 보안 사고에 취약점을 내포하고 있다.

이러한 보안 취약점을 해결하기 위해 802.1x, WPA, 802.11i 등 인증, 암호화 기법이 개발되고 있으나, 이런 인증, 암호화 기법은 무선 트래픽 분석 및 인가 사용자로의 위장 등의 의도적인 외부 침입에는 취약점을 문제점을 내포하고 있다. 인증, 암호화 기반의 무선랜 보안 기술의 한계를 극복하기 위해 현재 무선 설비에 접속하려고 시도하는 사용자를 탐지하여 불법 사용자에 대한 접속이 탐지되면 차단하기 위한 시스템이 개발, 현장에 적용되고 있다.

이와 같은 무선침입차단 시스템을 통한 보안 강화를 위해서는 명확한 인가 사용자 구분이 필요하며, 본 논문에서는 인가 사용자 정보를 자동 수집,관리를 위한 시스템 아키텍쳐를 제시,구현하고 실제 이동통신사 망에 적용함으로써 무선기기 정보 수집률을 향상시키고 외부에서의 침입과 내부 사용자의 외부 무선기기 접근에 대한 차단 기능 효과적으로 제공함을 확인 하였다.

2. 관련분야 연구

본 논문의 제안 시스템은 무선 침입탐지/차단에 중요 정보인 인가 사용자 정보를 자동 수집, 관리하고 무선 침입 탐지/차단 시스템과 연계 무선 보안 강화를 위 한 시스템으로 제안하는 시스템과 같은 형태의 시스템은 연구되지 않은 상태로 본 장에서는 기존 무선랜 보안 기술 연구 현황을 보인다.

무선랜 보안 기술은 IEEE 이나 Wi-Fi Alliance 에서 표준화된 기술이 사용되고 있으며, SSID 숨기기, MAC Filtering, WEP(Wired Equivalent Privacy)보안, 802.1x 보안, TKIP보안, VPN기반 보안으로 구분될 수 있다.

SSID 숨기기는 보안 엑세스를 위해 지정된 SSID를 알고 있는 사용자만 접속 가능하게 하는 방법이며, MAC Filtering은 SSID보다 향상된 방법으로 무선랜에 접속할 수 있는 사용자 MAC 주소를 사전에 등록하여 허가된

MAC만 접근이 허용하는 기법이다. [5]
WEP 보안은 Wi-Fi에서 유선과 동일한 보안을 제공하기 위해 개발된 기술로 단말기와 AP간 WEP 암호화를 통해 데이터를 전송하는 방식으로 64Bit, 128Bit키를 사용한다. [5]
802.1x 보안은 인증서버가 등록된 계정과 비밀번호 기반으로 인증을 수행하여 인증 결과에 따라 무선랜 접속을 제어하는 보안 방식이다. 인증 메시지 교환시에 이더넷, 토큰링 혹인 무선랜에서 기존의 통신 규약인 EAP(Extensible Authentication Protocol)를 사용한다.
TKIP 보안은 WEP 알고리즘의 취약점을 보완하기 위해서 개발되었으며, WPA(WiFi-Protected access) 표준으로 무선 장비에 구현되고 있다[5]
이와 더불어 인증,암호화 기반의 무선랜 보안 기술의 한계점이 나타남에 따라 유선상의 침입 탐지/차단 기술을 무선랜에 적용하여 무선 설비에 접근을 시도하는 사용자를 관리하여 비 인가 접속 시도자 및 인가 사용자의 외부 무선 설비 접속을 탐지,차단하기 위한 무선 침입 탐지/차단 기술이 지속적으로 개발되고 있는 상황이다.

3. 제안 시스템

본 논문에서 제안하는 시스템은 내부 무선랜 자원에 대한 접근을 통제하기 위한 사용자 식별 시스템으로 기존 관리자에 의해 수동적 관리됨으로 발생되는 정보 수집 부재로 인한 보안 위협을 해결하기 위한 시스템이다. 제안 시스템은 사용자 정보를 수집을 위한 모듈, 수집된 정보를 관리,처리하는 서버 모듈과 실제 무선침입 탐지/차단 시스템에 정보를 전달하는 전송 모듈로 구성되어 있다.

3.1 요구 정보 식별

무선랜 침입탐지/차단 시스템에서 무선 장비를 인가한다는 것은 엄밀한 의미에서 무선 장비가 장착된 단말PC 사용자의 무선 사용을 인가한다는 의미와 특정 방식의 무선 통신 기기를 이용한 통신을 인가한다 는 두 가지 의미가 있다.
첫째로 '사용자가 어느 단말PC의 무선 기기를 사용하는가' 를 인가하기 위한 식별 정보는 다음과 같이 구분될 수 있다.

정보항목	설명
User System ID	- 타 단말PC와 구별되는 사용자 단말PC의 명칭
User ID	- User System(사용자 단말PC)을 사용하는 다른 사용자와 구별되는 사용자명 - 기업에서는 사원번호와 같은 체계성 있는 User ID 부여시 관리에 보다 유리
Wireless Device	- User System에 장착되어 활성화된 무선 디바이스 - 일반적으로 MAC Address가 됨

표1. 무선 장치 인가/차단을 위한 관리 정보

상기 3가지 정보는 그 속성상 각각이 별도로 존재하는 것이 아니라, 서로 연계된 상태로 존재하는 묶음 정보이어야 분류가 가능하다. 따라서 3가지 정보는 하나의 단말에서 동시에 검출함으로써 서로의 연관성을 부여하여야 한다.
둘째로 '사용자에게 어느 무선 기기 사용을 인가'하기 위한 정보는 상기 첫 번째와 동일한 정보를 사용하며, 추가로 인가/비인가를 결정하는 추가 정보가 필요하다.

정보항목	설명
User System ID	- 타 단말PC와 구별되는 사용자 단말PC의 명칭
User ID	- User System(사용자 단말PC)을 사용하는 다른 사용자와 구별되는 사용자명 - 기업에서는 사원번호와 같은 체계성 있는 User ID 부여시 관리에 보다 유리
Wireless Device	- User System에 장착되어 활성화된 무선 디바이스 - 일반적으로 MAC Address가 됨
Authorized Flag	'User System ID + User ID + Wireless Device'에 대한 인가/차단 플래그

표2. 무선 기기 인가/차단을 위한 관리 정보

3.2 제안 시스템 구성

본 논문에서 제안하는 시스템의 핵심 기능은 3.1절에서 소개된 데이터를 관리함으로써, 무선보안 관리자가 무선기기 정보보다 이해가 쉬운 단말PC 정보, IP 주소 등을 이용하여 편리하게 인가/ 차단을 실행할 수 있게 하고, WIPS (침입탐지/차단 시스템)가 제공하지 못하는 비 무선랜 통신기기 사용에 대한 인가/차단을 실현할 수 있게 하는데 있다.
이를 위해 제안 시스템은 그림1과 같이 크게 사용자 시스템에 탑재되는 에이젼트와 서버 시스템에 탑재되는 서버 프로그램으로 구성 하였으며, 무선랜 기기 정보의 경유는 서버가 관리하는 인가/차단 정보를 WIPS로 전달될 수 있도록 하였다.

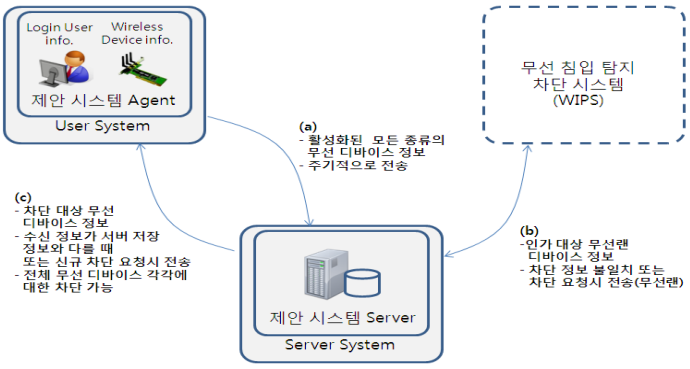

그림1. 제안 시스템 구성

3.2 에이젼트

제안 시스템에서는 먼저 '어느 사용자가 어느 단말PC의 무선기기를 사용하는가'를 관리 하기 위해 주기적으로 단말PC, 로그인 사용자 및 무선기기 정보를 함께 검출하여, 서버로 전송하는 사용자 단말에 탑재되는 에이젼트 프로그램을 구현한다.

3.2.1 에이젼트 전송 데이터

에이젼트로 부터 서버로 전달해야 할 정보는 표1 과 같이 정의 될 수 있으나, 실제 구현에서는 본 제안 시스템 사용자인 무선 보안 관리자가 요구할 수 있는

관리 기능을 보다 편리하게 구현하기 위해 몇 가지 추가적인 정보를 함께 서버로 전송해야 한다. (그림 2 참조)

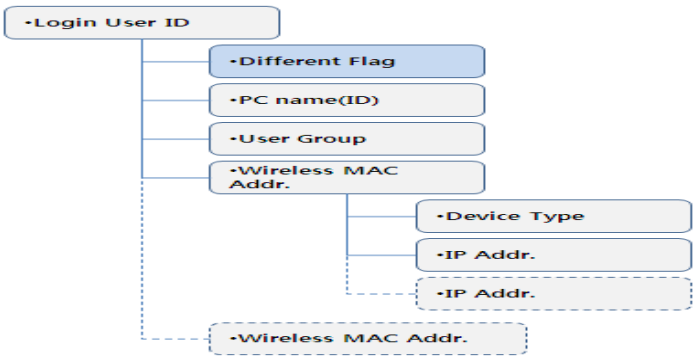

그림 2. 에이젼트 전송 데이터 항목 상세

무선기기 관리 정보는 결국 어떤 사용자의 사용을 차단하는 것이므로 개념적으로 그림2와 같이 사용자에 종속적인 데이터로 구성된다. 무선기기 관리 정보를 데이터 항목은 다음과 같다.

항목	설명
Login User ID	사용자ID. 사원번호와 같은 의미 있는 사용자 사용이 관리에 유리함.
Different Flag	Agent는 무선 디바이스 관리 정보를 주기적으로 전송하는데, 이때 직전에 보낸 데이터와 다를 경우에 이 플래그에 표시함.
PC Name(ID)	컴퓨터 이름이며, 체계적인 이름을 사용하는 것이 관리에 유리
User Group	사용자가 속한 작업 그룹이며, 체계적인 이름을 사용하는 것이 관리에 유리
Wireless MAC Addr.	각 무선 디바이스의 MAC Address를 가리킴
Device Type	802.11, Wibro, HSDPA, bluetooth 등으로 구분
IP Address	설정된 주소

표3. 무선기기 관리 정보

참고로 무선기기 관리 정보에는 1대의 단말PC에 여러 개의 무선기기가 존재 할 수 있고, 각각의 무선기기는 여러 개의 IP Address가 나타날 수 있다.

3.2.2 에이젼트 아키텍처 및 모듈 구성

제안 시스템은 무선랜 침입 탐지/차단 시스템(WIPS)과 연동하여 그 기능을 강화할 목적으로 구현되므로 WIPS로 불법 사용을 차단 할 수 있는 802.11 무선랜 부분을 제외하고 HSDPA, Wibro, Bluetooth와 같은 다른 무선 통신기기에 대해서도 에이젼트 프로그램이 어플리케이션 수준의 API를 이용하여 무선 통신기기 사용을 차단 할 수 있도록 구성 하였다.

에이젼트는 '사용자가 현재 사용중인 단말PC의 어느 기기를 차단할 것인가'에 대한 정보를 서버로부터 수신하여 차단을 실행한다. 이때 사용되는 차단 정보는 무선 보안 관리자가 서버에서 무선기기 정보를 확인하고 인가/차단을 결정함으로써 만들어지는 정보이다. 이를 위하여 에이젼트는 먼저 단말PC에서 검출한 무선기기 관리 정보를 서버에 전송한다.

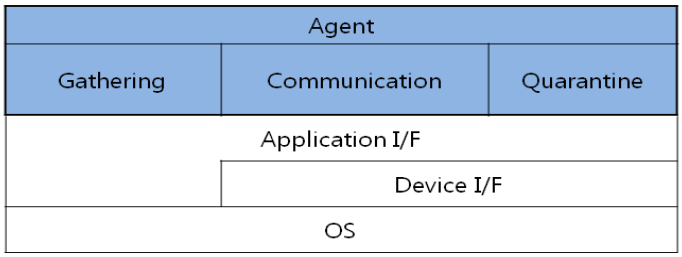

그림 3. 에이젼트 아키텍쳐

그림3은 이러한 기능을 구현하기 위한 에이젼트 아키텍쳐를 표현하고 있다. 그림에서와 같이 에이젼트는 기기 관리 정보 수립 및 차단을 위해 직접 기기를 제어하는 대신 어플리케이션 API를 통해 인터페이스 함으로써 프로그램이 보다 안정적으로 동작할 수 있도록 하였다.

에이젼트는 그림3에서 같이 "Gathering, Quarantine, Communication," 3가지 모듈로 구성되며 그 역할은 표4와 같다.

구성 모듈	설명
Gathering	- 표1에 표시된 정보를 검출 - 각 디바이스 Control에 필요한 Application API를 이용하여 구현
Communication	- Gathering 모듈에서 수집한 정보(표1)를 주기적으로 서버로 전송 - 서버로부터 차단 대상 디바이스 정보를 수신
Quarantine	- 수신한 차단 정보를 사용하여 디바이스 사용 차단 실행 - 각 디바이스 Control에 필요한 Application API를 이용하여 구현

표4. 에이젼트 모듈 기능 설명

3.3 서버

본 제안 시스템의 1차적인 기능 목표는 무선 보안 관리자가 보다 편리하고 정확하게 '어느 사용자에게 어느 무선기기 사용을 인가/차단해야 하는가' 판단하고 인가/차단을 실행할 수 있는 정보를 손쉽게 제공하는데 있다.

3.3.1 서버 관리 데이터

서버가 각 에이젼트로부터 수집한 무선기기 관리 정보는 무선 보안 관리자가 요구하는 다양한 조건의 조회, 분류, 설정 작업이 가능하도록 관계형 데이터베이스를 이용하여 구현했다

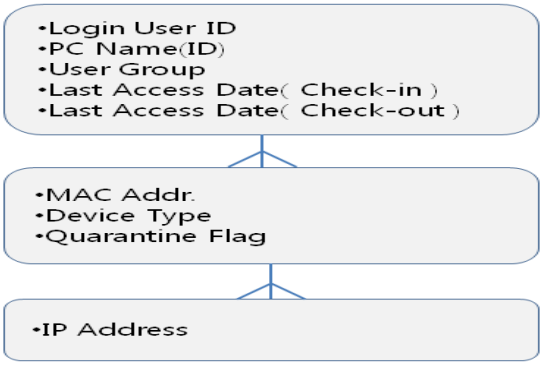

그림4. 무선기기 관리를 위한 DB 데이터

그림4는 제안 시스템 서버가 무선기기 관리를 위해 유지하는 데이터의 관계를 표현한다. 무선기기 관리 정보의 유지와 관리를 관계형 데이터베이스를 이용하여 구현함으로써 서버가 관리하는 무선 기기 정보가 관리자에게 편리하게 제공될 수 있도록 구현하였고, 인가/차단 작업도 관계형 데이터베이스의 기능을 활용하여 집합적인 처리가 가능하도록 했다.
참고로 그림4에 표시된 Last Access Date(Check-in/out) 필드는 에이젼트로부터 전송되는 무선기기 정보 자체를 추적하여 사용자가 무선기기를 사용하고 중지한 시점을 제공하기 위해 필요하며, Quarantine Flag는 무선기기의 사용을 인가/차단 하기 위하여 서버가 유지하는 데이터이다.

3.3.2 서버 아키텍처 및 모듈 구성

서버는 다수의 에이젼트로부터 수신한 무선기기 정보를 서버가 관리중인 정보와 비교, 시스템 반영하는 등의 작업을 자동화된 처리와 관리자의 모니터링에 필요한 각종 현황 정보 제공 등의 조회성 작업을 동시 에 처리할 수 있어야 한다.
제안 시스템의 서버는 그림5와 같이 설계함으로써 대규모 사용자 환경에서 다양한 작업이 동시 처리될 수 있도록 설계하였다.

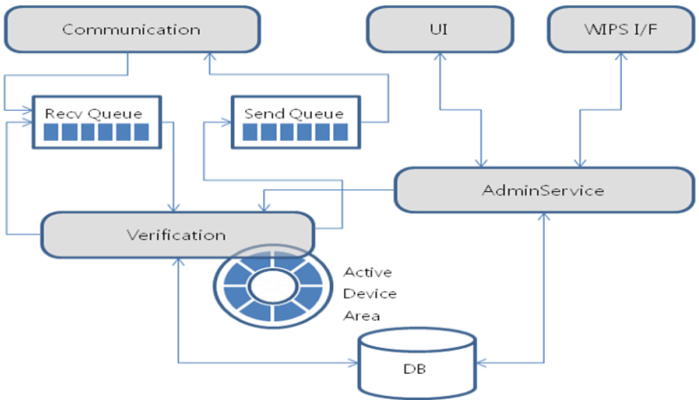

그림 5. 서버 아키텍쳐

서버 아키텍쳐의 모듈별 기능은 아래와 같다

모듈명	설명
Communication	Agent와 통신. 활성화된 무선 디바이스 정보와 차단 수신과 송신 처리
Recv Queue	무선 디바이스 정보 대량 수신을 위한 장치
Send Queue	무선 디바이스 차단 정보 대량 송신을 위한 장치
Active Device Area (ADA)	전체 무선 디바이스 정보 및 차단 정보 중에서 현재 활성화 된 것만을 메모리에서 관리위한 자료 구조. 이중에서 무선랜 부분에 대한 정보는 WIPS와 연동
Verification	다음과 같은 3가지 기능을 수행 1. 무선 디바이스 정보 수신시 차단 또는 활성화 되어야 할 디바이스가 설정과 일치 하는지 검사(없으면 ADA에 추가하고 DB에 저장) 2. 주기적으로 ADA를 검사하여 Last Access Date가 기준 시간을 초과 하였는지 조사하여 ADA에서 삭제(DB에 반영) 3. AdminService 모듈을 요청을 받아 ADA 현황 데이터를 DB에 반영
AdminService	본 제안 시스템의 화면에 출력할 각종 현황 정보의 조회 및 설정 요구를 처리하며 WIPS 인터페이스를 통해 인가/차단 무선랜 디바이스 정보를 전달
UI	본 제안 시스템의 화면
WIPS I/F	WIPS 인터페이스이며 WIPS에서 제공하는 전용 API

표 5. 서버 모듈별 기능

3.3.3 활성 기기 정보 유지 구현 Logic

제안 시스템의 핵심 기능은 대량의 사용자 단말PC가 끊임없이 네트워크에 접속과 종료를 반복하는 환경에서, 단말PC에 설치된 에이젼트로부터 전송되는 무선기기 정보를 이용하여 실제로 사용중인 단말PC에서 활성화되는 무선기기 정보와 서버가 실시간으로 관리하는 정보가 동일하도록 지속적으로 유지하고, 서버에 저장된 인가/차단 정보에 따라 사용자 단말PC에 설치된 에이젼트에 기기 인가/차단 정보를 에이 젼트와 WIPS로 전달하는데 있다.
이와 같은 서비스 구현을 위해 그림4에서 제시된 데이터 필드와 동일한 멤버 데이터로 하는 ADA(Active Data Area)라고 하는 자료 구조를 사용하여 현재 Active 상태의 무선기기 정보를 메모리로 관리하고 이를 DB와 동기화 시키는 방법을 사용 하였다.
그림6 및 표6은 Verification 모듈이 활성 기기 정보를 유지 관리하는 흐름도 및 설명을 표시하였다.

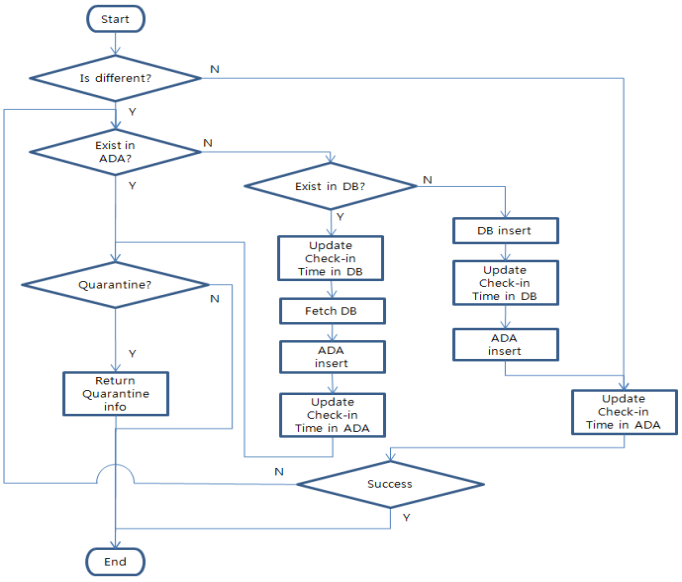

그림6. 활성 기기 정보 유지를 위한 처리 흐름도

판단	동작 설명
Is different?	- Agent가 전송하는 무선 디바이스 정보에서 Different Flag를 검사 - Agent가 직전에 보낸 정보와 동일한가?(Default는 '다르다'임)
Exist in ADA?	- 수신한 무선 디바이스 정보가 ADA에 있는지 검사 - 없다면 DB에 있는데 ADA 로딩전(즉, Check-out상태)이거나 처음 탐지된 무선 디바이스 정보일 수 있음
Quarantine?	- ADA에서 차단 설정된 디바이스 인가를 검사? - 차단이 설정되어 있으면 Agent로 차단 대상 디바이스 정보를 리턴
Exist in DB?	- 수신한 무선 디바이스 정보가 DB에 있는지 검사 - 차단 정보 획득을 위해 ADA에 바로 insert 하지 하고 DB 데이터 Fetch함
Success?	- ADA 정보와 단말PC의 활성화된 무선 디바이스 정보를 일치시키기 위하여 Agent로부터 무선 디바이스 정보를 수신할 때 마다 Last Update Time(Check-in)을 Update함. - 이때 정보 전송에 UDP 사용시 직전 정보가 유실가능성 있으므로, 성공 여부를 검사하여 실패시에도 현재 수신한 정보로 인가/차단 검사를 하도록 하였음

표6. 기능 설명

활성 무선기기 정보 유지를 위해 Verification 모듈 은 그림6과는 별도로 ADA에서 Last Access Time (Check-In)이 일정 시간을 초과한 무선기기 정보가 있는지를 검사하여, DB의 저장된 해당 기기 정보에 대하여 Last Access Time(Check-out)을 ADA에 있는 Last Access Time(Check-In)으로 갱신 한 후, ADA에서 해당 항목을 삭제하며, 해당 Logic은 아래와 같다.

```
Loop
    Wait NextInterval //주기적으로 반복
    GetTimeout_Limit // 무선 디바이스가 비활성 상태라고 판단할 기준 시간
    Loop // ADA에 적재된 전체 무선 디바이스를 검사
            Get one wireless device info. Set from ADA //ADA에서 무선 디바이스 정보 1건 FETCH

            If Check-in_Time < Timeout_Limit // 기준 시간 보다 오래되었으면
            Then
                    Begin
                            Update Last_Access_Time(Check-out) with Check-in_Time
                            //DB에 기록을 남김
                            Delete the wireless device info. Set from ADA
                            //ADA 자료구조의 크기를 일정하게 유지
                    End
            End If
    End Loop
End Loop
```

그림 7. Time Out ADA 정보 삭제 로직

3.3.4 WIPS 무선랜 인가/차단 정보 연동

본 논문의 제안 시스템은 WIPS와 무선랜 기기에 대한 인가/차단 정보를 연동하도록 구현하여, WIPS를 사용하는 무선 보안 관리자의 보다 편리한 인가/차단 업무를 수행 할 수 있도록 하였다. 그림.8,9는 이러한 동기화 과정을 구현한 Pseudo-code이다.

```
Synchronize ADA to DB          // Admin Service 모듈이 Verification 모듈에 요청
                               // ADA와 DB의 Last Access Time(Check-in)을 동기화
Select
UserPcName, MAC_ADDR, isActive, IP_ADDR, Vendor, Authorized_Flag
Into Update_Required_Clit_List
From DB
Where Device_Type='802.11'
And Last_Access_Time(Check-in) = Current  // 최근 동기화== 현재 활성화된 디바이스

If Update_Required_Clit_List is NOT NULL
    Update WIPS DB with Update_Required_Clit_List
EndIf
```

그림8. WIPS와 인가/차단 정보 동기화(일간,일괄처리)

```
Loop
    Wait Next Interval //주기적으로 반복

    Select
    UserPcName, MAC_ADDR, isActive, IP_ADDR, Vendor, Authorized_Flag
    Into Update_Required_Clit_List
    From DB
    Where Device_Type='802.11'
    And Last_Access_Time(Check-in) > Interval // 최근 활성화된 디바이스 목록 작성

    If Update_Required_Clit_List Is NOT NULL
            Update WIPS DB with Update_Required_Clit_List // WIPS DB 갱신
    EndIf
End Loop
```

그림9. WIPS와 인가/차단 정보 동기화(실시간)

4. 실험결과 및 분석

본 장은 논문에서 제안한 시스템을 국내 이동통신사 무선랜 환경에 시험 적용 후 무선랜 사용자 정보 자동 수집 및 WIPS 연동하여 인가 정보를 반영한 시험 결과이다. 이를 통해 무선 보안이 가장 중요한 인가, 비인가 사용자 분류 정확도가 높아져 내부 정보 유출 방지 효과가 있었다.

4.1 시험 구성

무선랜 에이전트 설치된 PC, 수집서버, WIPS(AirTight사 제품)으로 구성 하였으며, 에이전트 배포는 운영중인 PMS(설치유도시스템)에서 자동 배포하도록 구성하였다

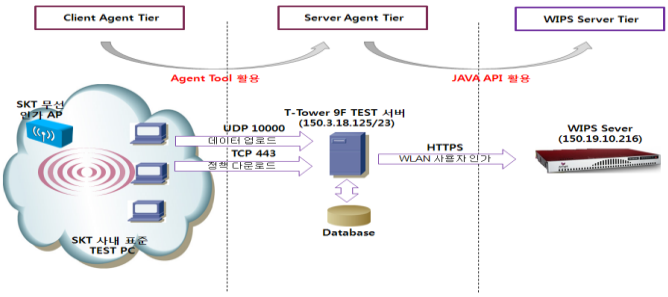

그림10. 시험 구성도

- 테스트 PC 정보
  - MAC (00:13:CE:C3:39:32)
  - IP Address (150.3.18.142), SSID(T-Wlan)
- 수집서버 IP Address : 150.3.18.125
- WIPS IP Address : 150.19.10.216

4.2 시험 결과

에이전트는 60초 간격으로 무선기기정보(MAC, IP, SSID등)을 서버로 전송하며, 서버는 수집된 정보를 DB로 관리한다. 서버는 수집된 정보를 무선 보안 관리자가 관리 효율성을 제공하기 위해 다양한 유저 인터페이스를 제공한다

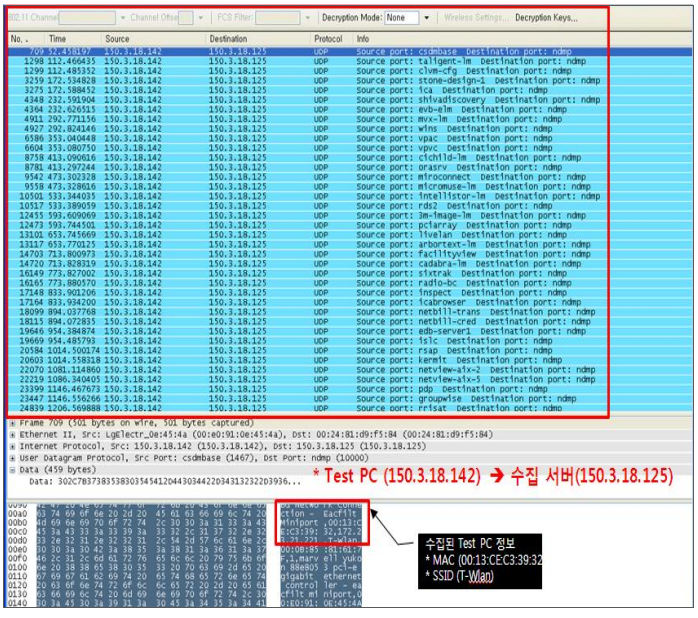

그림.11 에이전트의 주기적 기기 정보 전송

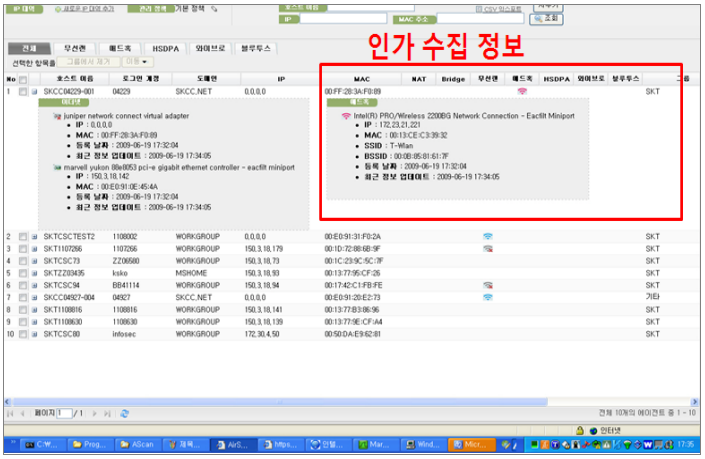

그림.12 서버 무선기기 정보 수집 결과

서버는 수집된 무선기기정보를 WIPS 시스템으로 실시간 전송하며, WIPS 시스템은 전달받은 무선기기 정보를 인가 사용자로 분류하여 외부에서의 침입 및 내부 인가 사용자의 외부 무선 통신기기 접근을 차단하는 기준 정보로 활용한다.

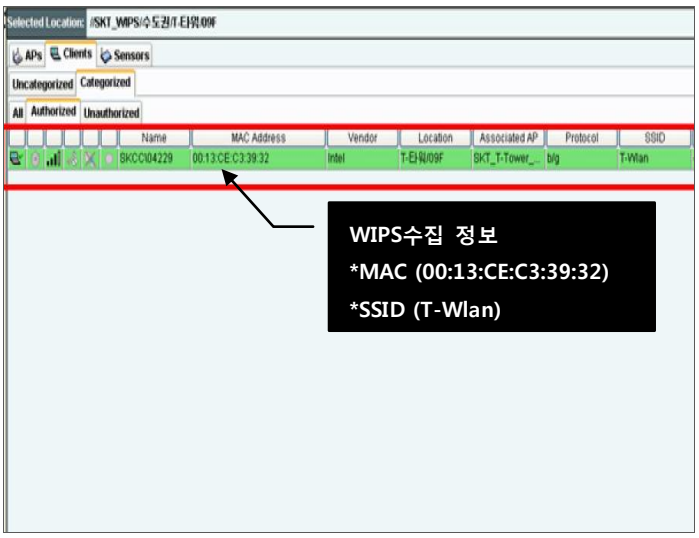

그림.13 WIPS 무선 기기 등록 정보

시험 테스트 외 실제 이동통신사 무선 네트워크에 적용한 결과 관리대상 무선기기 총 12,000대중 본 제안 시스템 적용 전 약 30%대의 수집률을 보였으나, 약 3개월간 운영결과 수집률이 80%대로 증가함을 확인하였다

시험결과와 같이 무선기기정보 수집이 실시간, 자동화됨에 따라 주요 무선랜 침입 탐지/차단 관리영역 중 인가 무선기기 정보 부족으로 발생되는 무선랜 보안 취약점의 개선 효과를 보았으며, 인가 사용자의 비인가 무선기기 접속 및 비 인가 사용자의 인가 무선기기 접속에 대한 탐지/차단률이 본 제안 시스템 적용 이전보다 약 40% 이상 향상됨을 모의해킹을 통해 확인 할 수 있었다.

No	공격유형	적용 전	적용 후
1	Rogue AP	100%	100%
2	Mis-Configured AP	100%	100%
3	Honeypot AP	100%	100%
4	Client Mis-Association	50%	90%
5	Unauthorized Association	50%	90%
6	Ad-hoc Connection	80%	100%
7	AP MAC Spoofing	100%	100%
8	DoS Attack	100%	100%
9	WEB Key Cracking	100%	100%

5. 결 론

본 논문에서는 기존 사용중인 무선 침입차단시스템(WIPS)을 이용한 외부 침입 및 내부 정보의 외부 유출의 중요 관리 정보인 인가 사용자 정보에 대한 자동화 수집 시스템 아키텍쳐에 대해 연구하였으며, 구현된 시스템을 실제 환경에 적용하여 기능 검증을 완료하였다. 실제 무선 보안환경 적용 전 인가 무선 기기 정보 수집율이 30%를 보였으나, 적용 후 80%까지 증가함을 확인할 수 있었으며, 모의해킹 시도 시 사용자 정보 부족으로 발생되는 인가 클라이언트의 외부 접속 및 비 인가 클라이언트의 내부 접속 시도에 대한 탐지 차단 확률이 높아짐을 확인 하였다.

본 제안 시스템을 적용 함으로써 관공서나 기업체는 무선랜 사용자에 대한 관리 취약점을 해소 할 수 있을 것으로 판단되며, 이로써 내부 정보 자산의 유출을 막음으로써 지적재산권 보호에 기여할 것으로 판단된다. 향후 연구과제로는 무선랜, 3G 등 무선통신 기반의 스마트폰 사용이 확산되면서 정보보안이 요구되는 대상이 증가하면서 스마트폰에 대한 보안 관리의 필요성이 대두됨으로 본 논문에서 제안한 시스템을 다양한 운영체제에 적용할 수 있는 연구가 필요하다.

참고문헌

1. 신동훈, “무선랜 침해사고 예방대책 연구”, 한국정보과학회 학술발표 논문집, 2004.

2. 송창렬, “무선랜 보안 구조”, 정보과학회지, 2002.

3. 신동훈, “무선랜 AP를 이용한 침입자 탐지 방법 연구”, 한국정보과학회 학술발표 논문집, 2004.

4. 이형우 “무선 네트워크 침입탐지/차단 시스템(Wireless IPS) 기술”, 한국통신학회지, 2005.

5. 정현철, “무선랜 보안 실태 조사 및 분석을 통한 보안 강화방안 연구”, 한국정보처리학회 학술발표 논문집, 2006.