

WLAN망 AP에서 사용자 인증과 자원관리 프로토콜의 구현 및 테스트

정선화*, 손형선*, 박석천*
*경원대학교 소프트웨어대학
e-mail:scpark@kyungwon.ac.kr

Implementation and Test of User Authentication and Resource Management Protocol in WLAN Network Access Point

Sun-Hwa Jung*, Hyung-Seon Son*, Seok-Cheon Park*
*Division of Software, Kyungwon University

요 약

본 논문에서는 WLAN의 여러 가지 문제점을 해결하기 위해 WLAN망에서 유무선의 중계기 역할을 하고 있는 AP에 사용자 인증과 자원관리 기능을 지원하는 확장형의 AP를 제안하였다. 이를 위해 WLAN망 AP에서 사용자 인증과 자원관리 프로토콜의 메시지 및 동작 절차를 설계하고 구현하였다. 사용자 인증과 자원관리 프로토콜을 포함하고 있는 AP의 테스트를 위해 WLAN망에 구현한 두 대의 Main AP 및 Sub AP를 위치시키고, PC형 라우터를 통해 외부망과 연결하여 테스트망을 구축하였다. 이동단말과 테스트를 수행한 결과 본 논문에서 구현한 사용자 인증 모듈과 자원관리 모듈이 정상적으로 동작함을 확인하였다. 따라서 본 연구는 WLAN AP와 이동단말 간에 경제적이면서 신뢰적인 사용자 인증을 위한 기초 기반 기술로 활용될 수 있을 것으로 생각되며, WLAN 자원들을 효율적으로 관리하는데 일익을 담당할 것으로 사료된다.

1. 서론

WLAN 기술은 현재 급속도로 진화 중인 초고속 무선인터넷 및 유비쿼터스망을 위한 필수적인 무선 액세스 기술로 인식되고 있어 WLAN의 시장 잠재력이 매우 커지게 되었다. 이에 따라 WLAN에 대한 관심 및 연구가 집중되고 있으며, 특히 무선구간 전송속도 향상과 WLAN 보안기술이 이슈가 되고 있다. 현재 제공하고 있는 보안 기술은 메시지 도청 공격에 취약함으로 인해 전면적으로 보완되어야 하는 문제점을 가지고 있다. 또한 기존의 WLAN AP는 트래픽 모니터링 및 자원관리 기능을 가지고 있지 않기 때문에 망의 트래픽 상황 감시 및 장애를 극복하는 역할을 수행하지 못할 뿐만 아니라 기능 확장에 있어서 새로운 장비로 교체해야 하는 비용상의 문제점이 있다. 이와 같은 여러 가지 이유에서 현재 많이 사용하고 있는 IEEE 802.11 계열의 표준

을 기반으로 하면서 보안문제, 트래픽 모니터링, 자원관리 등의 문제들을 해결한 확장 기능의 AP의 연구 수행이 필요하다고 판단된다. 따라서 본 논문에서는 IEEE 802.11 계열의 표준을 그대로 수용하면서 AP의 기본 기능 제공뿐만 아니라 AP내에 RADIUS 서버를 대체한 사용자 인증과 자원관리 등의 확장 기능을 구현하고 테스트하는 것을 목적으로 하였다.

2. 사용자 인증과 자원관리 프로토콜의 설계

본 논문에서는 그림 1과 같이 AP를 기본 기능과 확장 기능으로 구분하여 설계하였다. 기본 기능에는 브릿지 역할을 수행하는 모듈을 확장 기능에는 사용자 인증 처리 모듈과 이동단말 및 Sub AP들의 자원관리를 위한 SNMP 프로토콜 처리 모듈을 설계하였다.

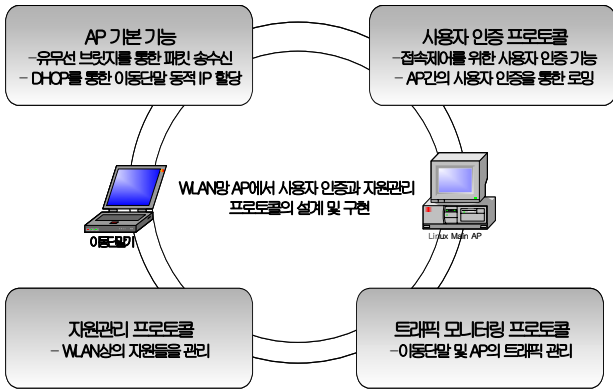


그림 1 설계 시스템의 개요도

WLAN은 허가되지 않은 사용자를 통한 불법적인 정보 유출 방지와 끊임없는 서비스를 제공받을 수 있는 이동성, WLAN상의 자원들의 효율적인 관리 등을 고려해야 한다. 따라서 본 논문에서는 IEEE 802.11b 보안의 취약점을 해결하기 위해서 AP 내에 RADIUS 프로토콜을 포함하여 설계하였으며, 이를 통해 안전한 사용자 인증 및 장비 추가 구입에 따른 비용 문제를 해결하였다. 또한 이동단말의 이동시에 한번의 인증과정을 통해서 다른 서비스 영역에서도 끊임없는 서비스를 제공받을 수 있도록 설계하였으며, SNMP 프로토콜을 사용하여 WLAN상의 자원들을 효율적으로 관리하는 시스템을 설계하였다.

본 논문에서 설계한 WLAN망 AP에서 사용자 인증과 자원관리 프로토콜은 그림 2와 같이 브릿지, 사용자 인증, 트래픽, 자원관리를 위한 모듈을 탑재하여 AP의 기본 서비스 제공뿐만 아니라 보안, 자원관리 등의 확장된 서비스까지 제공하도록 구성하였다.

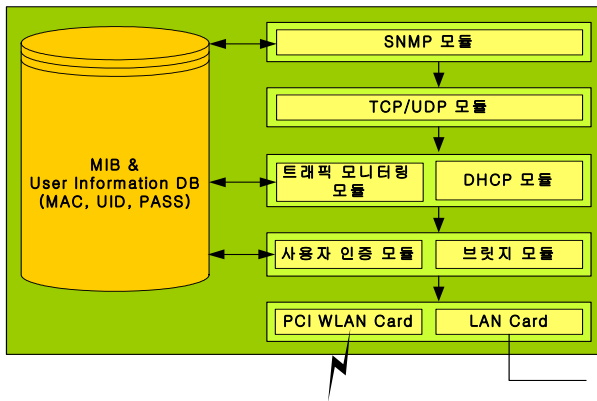


그림 2 AP의 기능 구성도

3. 사용자 인증과 자원관리 프로토콜의 구현

본 장에서는 2장에서 설계한 AP 기본 기능인 무선 연결 초기화 및 브릿징 모듈과 확장기능인 사용자 인증, 트래픽 모니터링 및 자원관리 등의 모듈을 구현하였다.

3.1 AP의 구현

이동단말이 WLAN망에서 외부망(WWW)으로부터 서비스를 제공받기 위한 AP의 모듈 구조는 그림 3과 같다. 구현한 단말기는 HostAP 디바이스 컨트롤러를 통해 무선 연결을 초기화하고, 패킷 브릿징 모듈을 사용하여 WLAN망과 유선망간의 패킷을 전송한다. AP내의 사용자 인증 시스템을 통해 사용자 인증을 수행하여 허락된 사용자에게 외부망의 서비스를 제공한다.

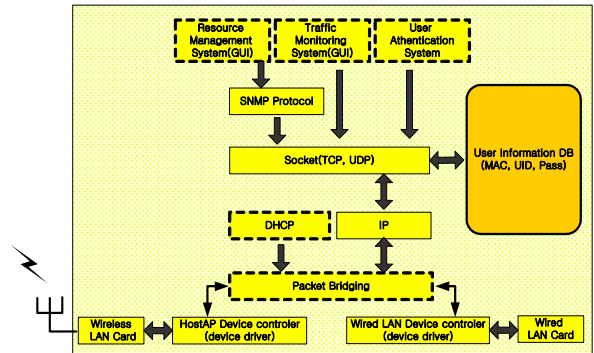


그림 3 AP내의 사용자 인증과 자원관리 프로토콜 구성 모듈 구조

주요 세부 모듈의 기능은 다음과 같다.

- SNMP protocol : 자원관리 시스템을 통해 관리국과 에이전트간의 통신을 위한 SNMP 메시지를 처리한다.
- Socket(TCP, UDP) : SNMP, 사용자 인증 시스템 등을 통해 TCP/UDP 소켓을 생성하며, 생성된 소켓을 통하여 TCP 스트림 또는 UDP 데이터그램을 생성한다.
- IP(IPv4) : IPv4 서비스를 제공한다.
- DHCP : AP에 결합된 이동단말들에게 동적으로 IP를 생성하여 부여한다.
- Packet bridging : 데이터링크 계층에 패킷 중계 장치에서 수행되며 WLAN망과 유선망간의 패킷을 전송한다.
- HostAP device controller : 이동단말과 AP간의 무선 연결 초기화를 수행한다.

3.2 AP의 기본 기능 및 확장 기능부 구현

AP 기본 기능부는 무선연결 초기화 과정에 따라 AP와 이동단말 간에 메시지 송수신 절차를 통해 허가된 사용자에게 동적 IP를 할당하여 AP와 결합하도록 구현하였다. AP 기본 모듈에는 무선연결 초기화, DHCP, 브릿지의 기능을 구현하였고, 구현한 모듈은 리눅스 커널소스에 포함시켜 커널 컴파일을 통하여 추가하였다.

AP 확장 기능부는 사용자 정보를 입력받아 허가된 사용자에게 AP의 접근 및 외부망의 서비스를 제공하는 사용자 인증을 구현하였으며, 이동단말이 서브넷 AP로 이동시에 간단한 사용자 인증 확인을 통한 로밍을 수행하도록 구현하였다.

또한 AP를 통과하는 패킷들을 추출하고 분석하여, 분석된 정보를 DB에 저장하는 트래픽 모니터링 프로토콜을 구현하기 위하여 SNMP 프로토콜이 WLAN상의 서브넷 AP 또는 이동단말의 패킷 트래픽, CPU, RAM 등의 사용률 정보를 실시간으로 모니터링하여 자원들을 관리하도록 하였다. 이렇게 SNMP 프로토콜을 이용하여 수집된 트래픽 정보들을 실시간으로 그래프로 보여주기 위하여 MRTG(Multi Router Traffic Grapher)를 적용하였다. 구현된 사용자 인증, 트래픽 모니터링, 자원관리 등의 프로토콜들은 AP 리부팅(rebooting)시 자동으로 활성화될 수 있도록 설정하였다.

4. 사용자 인증과 자원관리 프로토콜의 테스트

본 논문에서 구현한 프로토콜의 시험은 이동단말과 AP간의 무선 연결 초기화 과정을 통한 AP와의 결합에서 사용자 인증을 수행 기능과 AP를 통과하는 특정한 패킷을 캡처하여 트래픽양 분석 및 WLAN상의 효율적인 자원관리가 이루어지는가에 대한 것이다.

4.1 테스트망의 구성

본 논문에서 구현한 WLAN망 AP에서 사용자 인증과 자원관리 프로토콜의 동작성을 테스트하기 위해서는 유무선이 연결된 기반구축형 테스트망을 구성하여야 한다. 이를 위하여 본 논문에서는 Linux PC 라우터를 구성하여 외부망과 연결하고, 허브를 통해 Main AP와 Sub AP가 위치한 테스트망을 구성하였다.

그림 4는 WLAN망 AP에서 사용자 인증과 자원관리 프로토콜의 동작을 테스트하기 위한 테스트망의 구성도를 나타낸 것이다.

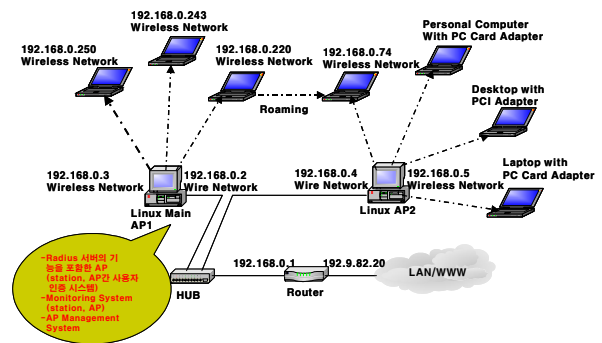


그림 4 테스트망 구성도

테스트망에 위치한 PC 라우터는 학교망과 연결되어 있으며, 현재 학교에서 제공하는 IPv4 어드레스를 사용하였다. 또한 각각 구현한 AP들은 192.168.0.0대의 사설 IP 어드레스를 사용하였고, 이동단말들은 AP와의 접속을 통해 동적 IP를 할당받게 하였다. 테스트망 환경이 실험실내에 위치하여 AP간의 거리가 가까워 채널 간섭이 심한 관계로 AP의 BSSID를 사전에 알아 이동단말이 AP를 직접 선택하도록 하여 테스트하였다.

4.2 테스트

사용자 인증 수행 첫 단계는 MAC 필터링으로서 허가된 이동단말에게 IP할당과 AP의 접근을 허락하고 이동단말의 사용자 정보를 통해 외부망의 접근을 허락하게 된다. 인증이 허락된 사용자는 외부망의 서비스를 제공받을 수 있다.

AP내에 WLAN상의 자원들 정보는 실시간으로 그래픽 파일로 저장된다. 패킷들이 AP를 통과하지 않은 상태와 AP를 통과하는 이동단말의 패킷들이 캡처된 정보를 통해 트래픽 분석이 가능하다.

구현한 시스템의 테스트에는 크게 일반 기능, 인증 기능, 망 관리 기능, 업그레이드 및 확장 기능 등으로 분류하고 세부 항목으로 나누었으며, 이 테스트 항목에 맞게 기능들을 지원하는지를 테스트하였다.

본 논문에서 설계하고 구현한 WLAN망 AP에서 사용자 인증과 자원관리 프로토콜이 2장에서 설계한 AP의 기본 기능인 무선연결을 초기화하고 브릿지 기능이 동작 절차에 따라 이동단말과 AP간에 결합이 이루어지면서 유무선망을 연결하여 원활하게 패킷을 송수신하는 것을 확인하였다. 확장 기능에서는 MAC 필터링에 의해 허가된 사용자에게 AP와의 결합을 허가한 후 제 2단계인 입력받은 사용자 정보를 데이터베이스에 저장된 정보와 비교하여 허락된 사

용자에게 외부망의 서비스를 제공하는 것을 확인하였다. 또한, 자원관리 기능에서는 IP를 가지는 패킷을 모니터링하여 트래픽 양을 분석하고, WLAN상의 이동단말이나 Sub AP들의 메모리, CPU 등의 자원 정보를 실시간으로 분석하여 분석된 정보를 그래픽으로 디스플레이 되는 것을 확인하였다. 또한 본 논문에서는 기존 AP 제품과 구현 시스템의 기능 지원 여부만을 비교 분석하였으며, 특히 구현 시스템의 동작 검증을 위주로 시스템의 테스트 및 검토를 수행하였다.

기존 제품과 구현 시스템은 일반 기능을 모두 지원한다. 그러나 구현 시스템에 추가한 인증, 업그레йд 및 확장 등의 기능에서는 구현 시스템을 제외하고 기존 제품들은 대다수 이 기능들을 지원하지 않았다. 망 관리 기능에서는 기존 제품과 구현 시스템 모두 SNMP을 지원하고 있지만, SNMP 활성화 여부에서는 구현 시스템을 제외하고는 활성화되어 있지 않았다. 인증 기능부분에서 구현 시스템은 미인증된 사용자의 접속프로그램 다운을 위한 특정 웹 페이지 접속에 대한 기능을 제공하지 못하였다. 따라서, 향후 구현한 시스템의 업그레йд 또는 기능 확장시 web-redirection을 추가하게 되면 이러한 문제를 해결할 수 있을 것으로 사료된다.

5. 결론

본 논문에서는 WLAN의 여러 가지 문제점을 해결하기 위해 WLAN망에서 유무선의 중계기 역할을 하고 있는 AP에 사용자 인증과 자원관리 기능을 지원하는 확장형의 AP를 제안하였다. 이를 위하여 WLAN의 망구조 등의 기본 개념, WLAN 인증 및 보안 방법, WLAN 자원 관리 등에 관한 표준화 동향 및 관련 문서를 연구·분석하고, 그 내용을 토대로 WLAN AP의 기본 기능 및 사용자 인증과 자원관리 프로토콜의 메시지 및 동작 절차를 설계하였다. 설계를 기반으로 무선연결 초기화 과정 및 브릿징 모듈 등의 기본 기능과 AP내 사용자 정보 데이터베이스를 이용한 사용자 인증 모듈, AP를 통과하는 트래픽 양을 분석하기 위한 트래픽 모니터링 모듈, WLAN상의 자원들을 관리하는 자원 관리 모듈 등의 확장 기능을 구현하였다. 구현된 확장형 AP의 개발환경은 펜티엄IV PC에 RedHat Linux 9.0 운영체제를 이용하였고, 구현을 위한 언어는 C, PHP 등을 사용하였으며, 시스템의 구조는 기능 업그레йд 및 추가 등의 확장성을 고려하여 가능한 기능별로

모듈화 하였다.

AP의 기본 기능뿐만 아니라 사용자 인증과 자원관리 프로토콜을 포함하고 있는 확장형 AP의 테스트를 위해 WLAN망에 구현한 두 대의 Main AP 및 Sub AP를 위치시키고, PC형 라우터를 통해 외부망과 연결하여 테스트망을 구축하였다. 구축된 테스트망에 이동단말을 위치시켜 무선연결 초기화 과정 및 접속 제어를 위한 사용자 인증을 수행하는지, 또한 허가된 사용자에게 외부망의 서비스 제공 여부와 AP를 통과하는 패킷의 트래픽양 분석, WLAN상의 자원 관리 등을 수행하는지를 테스트하였다. 이동단말과 테스트를 수행한 결과 본 논문에서 구현한 패킷 브릿징 모듈 등의 기본 기능과 사용자 인증 모듈과 자원관리 모듈의 확장 기능이 정상적으로 동작함을 확인하였다. 본 연구는 WLAN AP와 이동단말간에 경제적이면서 신뢰적인 사용자 인증을 위한 기초 기반 기술로 활용될 수 있을 것으로 생각되며, WLAN 자원들을 효율적으로 관리하는데 일익을 담당할 것으로 사료된다.

참고문헌

- [1] 임남주, “무선 LAN 기술의 개요 및 시장 동향”, 전자부품연구원 전자정보센터, 2003. 6.
- [2] 송창렬, “무선랜 보안구조”, 정보과학회 2002. 4.
- [3] 정병호 외, “공중 무선랜 망에서 인증 및 키관리 기술 동향”, 전자통신동향분석 제17권 제4호, 2002. 8.
- [4] 박영만 외, “공중 무선랜에서의 이중요소 인증된 키교환 프로토콜”, 정보보호학회논문지, 2003. 8.
- [5] 서정훈 외, “SNMP를 이용한 NMS 통합 시물레이션 시스템 개발”, 한국정보처리학회, 2001.
- [6] S. K. Miller, “Facing the challenge of wireless security,” Computer.org, pp.16-18, 2001.
- [7] ANSI/IEEE Std 802.11, “Wireless LAN Medium Access Control(MAC) and Physical Layer(PHY) Specifications,” 1999.
- [8] C. Rigney, “Remote Authentication Dial In User Service(RADIUS),” IETF RFC 2865, June 2000.
- [9] C. Finscth, “An Access Control Protocol, Sometimes Called TACACS,” IETF RFC 1492, July 1993.
- [10] W. A. Arbaugh, “Your 802.11 Wireless Network has No Clothes,” University of Maryland, <http://www.cs.umd.edu/>, Mar. 2001.