# 공중 무선랜 시스템에서 로밍을 고려한 사용자 인증방식의 설계 및 구현

종신회원 이 현 우*, 정회원 김 정 환*, 류 원*, 윤 종 호**

# Design and Implementation of User Authentication Schemes for Roaming in Public Wireless LAN Systems

Hyun-woo Lee* ***A Lifelong Member***, Jeong-hwan Kim*, Won Ryu* and Chong-ho Yoon***
***Regular Members***

요 약

본 논문은 무선랜 기술을 활용한 초고속 무선인터넷 서비스에서 사용자 인증방식에 사용되는 프로토콜의 설계와 구현에 관한 것이다. IEEE 802.11b를 기반으로 한 공중 무선랜 서비스는 최근 고속 무선 인터넷 접속 솔루션으로써 각광받고 있다. 공중 무선랜 환경에서는 특히 중앙 집중화된 인증방법과 향상된 보안대책이 필요하며 사용자 단말의 이동 시 로밍에 대한 보장이 요구된다. 본 논문에서는 IEEE 802.1x에 기반의 사용자 인증보안 기능을 설계하고 방법과 실제 임베디드 리눅스를 기반으로 한 무선랜 Access Point(AP)에서 구현하여 동작을 시험하였으며, 로밍 시 필요한HAPP 절차에 대하여 검토하였다. 또한 업체를 통한 상용화를 진행하며, KT 네스팟 인증시스템과 정상적인 연동기능 및 관리기능이 동작함을 확인하였다.

Key Words : wireless LAN, authentication, roaming.

ABSTRACT

Currently, Wireless LAN(WLAN) service is widely deployed to provide high speed wireless Internet access through the mobile stations such as notebook and PDA. To provide enhanced security and user access control in the public WLAN area, WLAN access points should have the capability of IEEE 802.1x-based user authentication and authorization functionality. In this paper, we provide a brief understanding of IEEE 802.1x standards and related protocols likeEAPoL(Extended Authentication Protocol Over LAN), EAP, RADIUS and describe how the IEEE 802.1x is designed and implemented in our embedded linux-based WLAN AP which is named i-WiNG.(Intelligent Wireless Internet Gateway).

## Ⅰ. 서 론

최근 무선랜 기술은 IEEE 802.11b를 따르는 다양한 저가 제품의 출시와 노트북, PDA와 같은 개인 휴대 단말의보급 확대에 따라, 3G 망에서의 패킷 데이터 서비스를 보완 대체할 수 있는 서비스로 새롭게 등장하여 빠르게 성장하고 있다. 초기 무선랜은 가정, 기업과 같은 비교적제한적인 공간에서 제공되던 유선랜 대체역할에서 이제 고정 무선(Fixed-Wireless)의 특징을 갖는 공중 무선 접속망으로써의 그 영역을 확장하고 있다. 이에 발맞춰, KT, 하나로통신을 비롯한 국내외 유무선서비스 사업자들은 공항, 호텔 등과 같은 핫스팟(Hotspot) 지역에 무선랜 AP(Access Point)를 설치하여 가입자들에게 고속 무선 인터넷 서비스를 제공하는 공중 무선랜 서비스(Public WLAN Service)를 실시하고 있다[1].

이러한 공중 환경에서의 무선랜 서비스를 제공하

* 한국전자통신연구원 광대역통합망연구단 통합망핵심기술연구그룹(hwlee@etri.re.kr, hw-jung@etri.re.kr)
** 한국항공대학교 전자 • 정보통신 • 컴퓨터공학부(yoonch@mail.hangkong.ac.kr)
논문번호 : 040167-0430, 접수일자 : 2004년 5월 3일

기 위해서는 인증, 보안, 로밍, 과금 등과 같은 다양한 기술들이 적절히 제공되고 해결되어야 한다.

본 논문에서는 현재 공중 무선랜에서 요구되는 IEEE 802.1x를 기반으로한 사용자 인증 및 보안기능과 multi-vendor AP간의 상호연동을 위한 IAPP(Inter Access Point Protocol)에 대해서 살펴보기로 한다[2][3]. 그리고, 임베디드 리눅스를 기반으로 한 무선랜 AP 상에서 IEEE 802.1x 기능이 실제 어떻게 동작 구현되는 지를 보이고, IAPP는 어떻게 지원되어야 하는 지를 설명한다.

본 논문의 순서는 다음과 같다. 2장에서는 무선랜 사용자 인증/보안의표준 기술로 자리잡고 있는 IEEE 802.1x와 그와 관련된 프로토콜들을 고찰하고, 3장에서는 현재 IEEE TGf 그룹에서 표준화 작업이 계속 진행중인 IAPP에 대해서 살펴본다. 4장에서는 본 과제에서 개발한 임베디드 리눅스 기반의 무선랜 AP인 i-WiNG(Intelligent Wireless Internet Gateway)을 소개한 다음, i-WiNG AP상에서의 IEEE 802.1x의 기능 구현 및 동작을 보이고, IAPP를 위한 고려사항들을 제시하며, 마지막으로 결론을 맺는다.

## Ⅱ. 포트기반의 네트워크 접근제어 방법

공중 무선랜 서비스를 가능하게 하는 기술의 중요한 요소중의 하나는 바로 무선환경에서의 적절한 사용자 인증과 보안 기능의제공에 있다. 현재 사용자 인증및 포트 제어를 위한 IEEE 802.1x 규격을 무선랜에서도 사용할 수 있도록 권고하고 있으며, 이는 공중 무선랜 서비스를 위해서 무선랜 AP에 반드시 지원되어야 할 기술로 자리를 잡고 있다.

IEEE 802.1x는 무선랜 AP나 이더넷 스위치와 같은 점대점(point-to-point) 연결 특성을 갖는 시스템의 포트에 연결되는 장치에 대한 인증(authentication)과 권한(authorization)의 제어를 통해 물리적 접속을 허용하는 방법과 이를 위한 각 인증 주체(Port Access Entity)들의 동작을 규정하고 있으며, 또 연결 구간에서 전송되는 데이터의 암복호화에 필요한 키를 동적으로 분배하기 위한 방법을 제시하고 있다. 또한 이를 위해 IEEE 802.1x는 먼저 구조적인 형상을 규정하고 그 구조상에서 인증서기반의 인증, 스마트카드, one-time password와 같은 다양한 인증방법을 수용할 수 있게 하고 있다. 또, 802.3 이더넷망, 802.5 FDDI, 802.11 무선랜 등과 같은 다양한 망을 위해 포트 기반의 망 접근

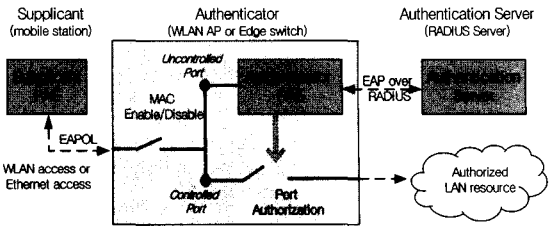


그림 1. IEEE 802.1x 구조적 형상도

제어를 제공한다. 여기서 포트라함은, 물리적인 LAN 세그먼트에 접속되는 시스템의 접합점이 될 수도 있고, 802.11 단말과 AP사이의 연결설정(association)과 같은 논리적인 포트도 될 수 있다.

무선랜에서의 IEEE 802.1x 프로토콜을 위한 구성요소는 그림 1과 같이 인증요청자(Supplicant), 인증자(Authenticator), 인증서버(Authentication Server)로 이루어진다. 인증요청자는 무선랜 카드를 장착한 노트북에 해당되며, 이는 인증자가 특정 포트를 통해 제공하는 서비스(예, MAC connectivity)를 사용하고자 하는 개체이다. 인증자는 무선랜 AP나 스위치에 해당되며, 여러 물리적, 논리적 포트를 가지고 있으며 이를 통해 서비스를 제공한다. 인증자의 주요역할은 인증서버와의 인증과정을 중재하고, 인증 결과에 따라 포트 제어를 수행하는 데 있다. 인증서버는 인증요청자의 인증요구를 인증자를 통해 전달받으며, 인증 성공여부를 인증자에게 전달하여 포트사용에 대한 허가를 지시하는 역할을 한다.

## Ⅲ. 무선랜에서의 로밍 기술

IEEE TGf에서는 multi-vendor AP들간의 동일 서브넷에서의 로밍을 지원하기 위한 802.11f 규격을 제정중에 있다[3]. IAPP는 동일 서브넷에서 단말(STA)이 AP를 이동할 때, AP내부에서 정의되는 서비스 프리미티브들과 AP간의 프로토콜을 규정하고 있다. 하지만, 아직 규격이 완성되지 않은 상태이며, 특히 AP간에 주고 받는 정보(Context Block)에 대한 정의가 모호하게 되어있다.

그림 2는 IAPP를 통한 서브넷 로밍의 과정을 보여주고 있다. AP간을 이동할 때, Old AP(AP1)의 BSSID는 단말(STA)에 의해 new AP(AP2)에게 전달된다. 만약, new AP가 IAPP(Inter-Access Point Protocol)을 지원하지 않는다면, 단말은 EAP-start 메시지를 받고 재인증을 거쳐야 된다. 만약 IAPP가

지원된다면, new AP는 RADIUS 서버에게 old AP의 주소와 AP간 통신에서 사용될 Security Block을 받아온다. 이에 new AP는 old AP와 보안채널의 통신을 설정하고, old AP가 가지고 있던 단말에 대한 정보를 수신한다. 정보의 내용에는 old AP에서 사용되던 계정 및 과금 레코드나 새로운 WEP 키 생성을 위한 인증정보 등이 될 수 있다. 이후 단말은 AP로부터 재설정 응답(re-association response)을 받으며, 새로운 인증 절차 없이 서비스 자원을 사용할 수 있게 된다.

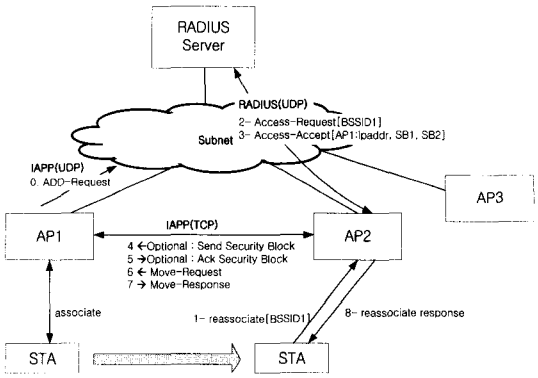


그림 2. IAPP를 통한 무선랜 로밍

## Ⅳ. i-WiNG AP의 IEEE 802.1x 인증기능 설계 및 구현

### 1. 무선랜 AP : i-WiNG

무선랜 서비스의 핵심장치인 무선랜 AP는 802.11 기반의 무선 데이터 송수신과 유선 데이터간의 트래픽을 중계하는 Layer 2 브릿지 기능이 주요한 역할이다. 본 논문에서 개발한 공중 무선랜에 기반한 지능형 무선 인터넷 게이트웨이(i-WiNG, Intelligent Wireless InterNet Gateway)는 무선랜 AP에 유무선 인터넷 연결에 대한 브릿징 기능이외에, IEEE 802.1x 사용자 인증/보안 기능, 시간제/종량제 과금 기능, 지역 정보제공 서비스[4]등 공중 무선랜 서비스에 특화된 기능을 탑재한 무선랜 AP와 이와 관련된 i-WiNG 클라이언트, 인증서버, 응용서버 등의 주변 시스템으로 구성된다. i-WiNG AP는 MPC 860P를 기반으로 한 보드에 확장성, 범용성, 가격 경쟁력을 고려해 임베디드 리눅스상에 다양한 프로토콜 및 응용 프로그램을 구축하고 있다. 그림 3은 i-WiNG AP시스템의 형상을 나타내고 있다.

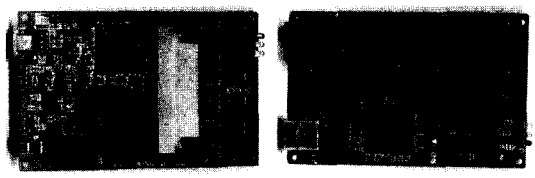

그림 3. i-WiNG AP Board의 형상

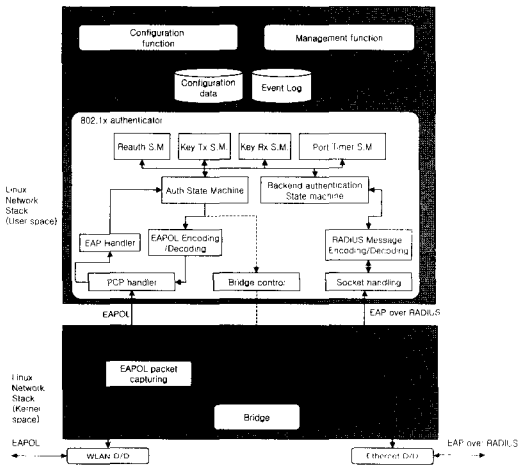


그림 4. i-WiNG의 IEEE 802.1x 기능 블럭도

### 2. i-WiNG AP에서의 IEEE 802.1x 기능설계

i-WiNG AP는 임베디드 리눅스를 기반으로 하였기 때문에, IEEE 802.1x기능 설계 시 그림 4에서처럼, 커널 영역과 사용자 영역에서의 역할이 구분되어졌다. 먼저, 커널 영역에서 수행되어야 될 부분은 EAPOL 메시지를 선택적으로 수신하고 상위 어플리케이션으로 전달할 수 있도록 하는 EAPOL 필터링 기능과, 상위 응용처리부에서 정상적인 802.1x 인증을 완료 후에, 특정 클라이언트에 대해 막혀 있던 포트를 열어주기 위해 커널 내 브릿지의 기능 변경이 되어야 한다.

사용자 영역에서는 802.1x 인증 세션을 제어하는 인증자(authenticator)가 존재하며, 그 내부에 주요한 각 모듈에서는 다음과 같은 일들을 수행하도록 설계되었다.

- EAP 메시지 처리 루틴 : 인증요청자(supplicant)로부터 EAP 메시지의 추출하여 저장하고 이를 다시 RADIUS 메시지로 변환하는 역할, 서버로부터 응답된 RADIUS 메시지의 해석 및 EAP 속성값의 추출과 저장하는 역할, 인증 성공/실패시의 EAP 메시지 생성의 역할을 수행한다[5][6].

- 구성정보와 이력기록 : 클라이언트와 혹은 인증서버간의 통신을 위한 구성정보 및 인증자의 포트 제어 정책, 재인증 설정정보, 관리 행위에 의해 설정되어지는 기타 정보 등으로 이루어지며, 인증 시도, 성공/실패에 대한 로그 및 이력을 기록하는 역할을 한다.

802.1x 인증 처리는 규격에 정의된 상태머신에 의해서 정의된다. 인증자에는 총 7개의 상태머신이 존재하는 데 인증 세션 전체에 있어 중요한 역할을 하는 것은 인증자 PAE 상태머신과 후단 인증처리(bakend authentication) 상태머신이 담당하고 있다.

- 인증자 PAE 상태 머신 : 사용자 인증 상태를{INITIALIZE, DISCONNECTED, CONNECTING, AUTHENTICATING, AUTHENTICATED, ABORTING, HELD}로 구분하여 사용자 인증 과정을 전체를 관할하는 802.1x 규격에 정의된 상태 머신이다. 후단 인증처리 상태 머신과 인증상태 관련 전역 변수값의 설정을 통해 이벤트를 전달하며, 인증 성공 또는 실패시 제어 명령을 통해 해당 클라이언트에 대해 브리지 기능을 직접 제어한다.
- 후단 인증처리(bakend authentication) 상태 머신 : 후단 인증처리 상태 머신은 RADIUS 인증서버와의 통신을 관리하여, 그 상태를 규격에 정의된 {INITIALIZE, REQUEST, RESPONSE, SUCCESS, FAIL, TIMEOUT, IDLE}로 구분하여 관리한다. Authenticator 상태머신으로부터 인증시작의 signal(authStart)을 받아 후단 인증 처리를 시작하며, RADIUS 메시지의 송수신을 처리하고, 최종적으로 인증서버로부터 허용(Access Accept) 혹은 거절(Access Reject)의 메시지를 받고 이를 인증 요청자에게 EAP-Success/Failure 메시지로 변환 전송후에 이를 인증자 상태머신에 알리고 끝나게 된다.

이들 이외에, 포트 타이머 상태 머신은 802.1x 인증과 관련된 각종 타이머 값들을 초기화하고 구동하는 역할을 하며, 재인증 타이머 상태 머신은 재인증 정책이 수립되었을 때, 주기적인 재인증을 보장하는 책임을 진다. Key Receive/Transmit 상태머신은 암호화키의 송수신을 책임지며, 제어방향 상태머신은 인증자의 접속 관리 정책을 반영하는 역할을 한다.

## 3. 인증자(Authenticator)의 구현

인증자는 무선랜 AP기능을 수행하는 i-WiNG 시스템상에 동작이 되며, 리눅스 커널 2.4.2 상에서 동작한다. 802.1x를 이더넷상에서 구현한 공개코드(open1x project)를 참조하여 이를 수정 및 추가 변경하였다. open1x 프로젝트[7]는 규격에 나타난 보안 문제[9]를 찾아내는 데 초점이 있으나 본 구현은 실제 무선랜에서 802.1x를 충실히 수행하도록 구현하였다. 이를 위해 실제 서비스를 위한 사용자 권한 부여를 위한 브릿지 제어 부분과 다중 사용자동시 접속 처리 및 타이머 기능 등이 추가 변경되었다.

## 4. 브릿지의 제어기능

IEEE 802.1x 인증을 성공적으로 마친 인증 요청자에 대해서는 포트사용에 대한 허가를 하여야 한다. 이를 위하여 커널내에 존재하는 브릿지의 동작을 수정 변경하고, 이를 사용자 레벨에서 명령을 내릴 수 있도록 bridge 제어관련 ioctl 명령어을 추가하였다.

```
struct net_bridge_fdb_entry {
        struct net_bridge_fdb_entry *next_hash;
        ……
        mac_addr  addr;
        struct net_bridge_port  *dst;
        unsigned long ageing_timer;
        unsigned  is_local:1;
        unsigned  is_static:1;
        unsigned  is_auth:1;
};
```

그림 5. 브릿지 포워딩 데이터베이스 엔트리의 구성

```
……
if (dest[0] & 1) {
        br_flood(br, skb, 1);
        if (!passedup)  br_pass_frame_up(br, skb);
        else  kfree_skb(skb);
        return;
}

/* check is_auth */
dst = br_fdb_get(br, dest);
if(!br->authforce_enabled){
    src_fdb=br_fdb_get(br, src);
    if(!src_fdb->is_auth)
        goto freeandout;
}

if (dst != NULL && dst->is_local) {
    if (!passedup)  br_pass_frame_up(br, skb);
        else  kfree_skb(skb);
    br_fdb_put(dst);
    return;
}
……
```

그림 6. 브릿지 패킷 포워딩 조건검사 과정

브릿지에 접속되어 있는 인터페이스들(wlan0, eth0)은 브릿지 포워딩 데이터베이스에 동적으로 관리되어지는 개체로서 표현이 되는데, 그림 5와 같이 IEEE 802.1x를 위해 인증 상태(is_auth) 필드를 추가하였다. 그리고 그림 6에서처럼 패킷 포워딩 조건을 검사하는 부분에서 이 필드에 대한 검사를 추가함으로써 데이터 필터링 기능이 동작하도록 구현하였다.

## 5. 기능 및 성능시험

구현된 i-WiNG의 사용자 인증 및 보안기능의 동작시험을 위해 무선랜 카드가 장착되고 802.1x 기능이 내장된 윈도우XP OS의 노트북을 단말로 이용하여 무선랜망에 접속시험을 수행하였다. 단말에서 실행중인 ping패킷이 정상적인 인증이 이루어진 후부터 응답 패킷이 수신되는 것을 확인하였고, 인증전에는 AP 브리지의 필터링 기능에 의해 접근이 차단됨을 확인하였다.

또한 업체를 통합 상용화를 진행하며 구현된 AP를 KT 네스팟 서비스 제공을 위한 PMS(Protection Management System)에 연동하여 IEEE802.1x 기반의 인증기능이 정상적으로 동작함을 확인하였고, 그 밖의 다양한 관리기능도 시험하였다.

개발된 i-WiNG의 성능 시험을 위해서 NetIQ사의 Chariot 을 사용하여 시뮬레이션 수행하고, KT 공중 무선랜 서비스 네스팟에서 실제 운용중인 IEEE802.1x 인증기능이 제공되는 IEEE802.11b 기반의 시스코의 340시리즈 AP와 결과치를 비교하였다. NetIQ사의 Chariot 은 새로운 기술을 이용하여 새로운 응용 서비스를 구축하기 전에 이러한 적용이 현재의 네트워크 성능에 미치는 영향을 파악할 수 있는 어플리케이션 레벨의 종단간 네트워크 성능 측정 및 분석 툴이다.

그림 7은 서비스 사용자 단말 갯수에 따라서 제공가능한 최대전송률 및 평균전송률의 성능측정을 위한 시험망 구성도이다. 성능측정을 위한 AP로 i-WiNG을 중심으로 무선랜 카드가 장착된 사용자 단말과 응용서버로 구성되며 성능측정 결과값을 표시하는 Chariot 콘솔이 사용된다.

시뮬레이션을 위해서는 우선 Chariot콘솔에서 성능측정 종단1인 단말에 스크립트를 설정하면 성능측정 종단2인 응용서버에 스크립트를 전달하고 성능측정을 위한 시험이 진행된다. 이후 시뮬레이션이 완료되면 성능측정 결과값이 Chariot 콘솔에 전달되

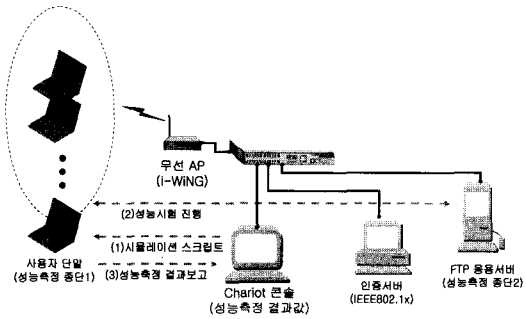


그림 7. 성능측정을 위한 시험환경 구성도

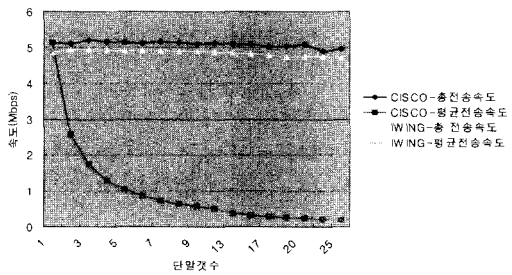


그림 8. IEEE802.1x 기능이 없는 경우의 성능비교

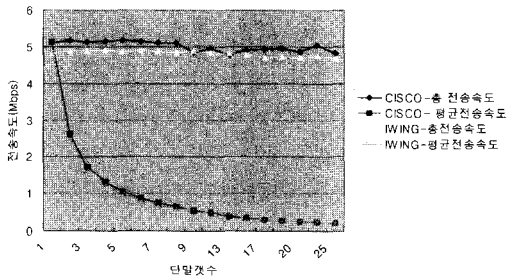


그림 9. IEEE802.1x 기능이 있는 경우의 성능비교

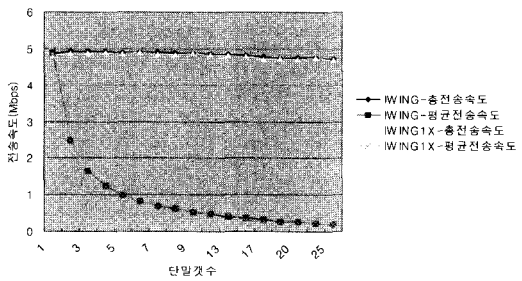


그림 10. 사용자 단말갯수에 따른 최대 전송률 및 평균 전송률(FTP 응용서비스)

어 표시되는데, AP에 서비스 가입자가 1대일 경우, 5대, 10대, 20대일 경우에 대해서 단말별 전송속도와 AP의 최대전송속도 및 가입자별 평균전송속도를 측정하였다. 다음 그림들은 i-WiNG에 접속된 사용자 단말 갯수에 따라 제공가능한 최대 전송률을 시뮬레이션하여 성능측정한 결과를 시스코의 340시리즈 AP와 비교한 결과이다.

이상의 결과를 보면 시스코의 340시리즈 AP와 비교하여 개발된 i-WiNG의 최대전송률과 평균전송률이 떨어지지 않음을 확인할 수 있다.

### 6. IAPP를 위한 추가 고려사항

앞서 3절에서 언급했듯이, 현재 IAPP는 표준화작업 중에 있으며 변화가 예상된다. 현재 시스코와 같은 업체들은 자사 제품들간에 로밍이 지원되는 제품을 일부 발표하고 있는데, 이는 진정한 다수업체의 이기종 AP장치간의 호환성이 보장되는 IAPP라고 할 수 없다. 하지만, 가까운 미래에 수용되어야 할 로밍기능을 위해서 AP에서는 로밍 프레임웍을 위한 다음과 같은 요구사항들이 기본적으로 충족되어야 한다.

- IAPP를 위해서는 서브넷에 브로드캐스트되는 ADD request 패킷을 수신할 수 있어야 하며, 이를 받아 AP가 맺고 있는 연결설정(association) 관리 테이블을 검사하고, 만약 연결이 존재한다면, 해당 단말과의 연결설정을 해제하는 기능.
- 현재 규격에서 권고되는 있는 RADIUS 프로토콜 속성들에 대한 AP와 RADIUS 서버에서의 지원
- RADIUS 서버에서의 서브넷내의 모든 AP IP 주소와 BSSID 매핑 테이블 기능 지원
- AP간에 송수신되는, TCP 프로토콜상의 Send-Security-Block, ACK-Security-Block, Move-Request, Move-Response 오퍼레이션을 위한 IAPP 응용 및 무선랜 디바이스 드라이버와 연계된 context block 해석 처리 기능

## V. 결 론

공중 무선랜에서의 IEEE 802.1x에 기반한 사용자 인증과 보안은 필수적으로 지원되어야 할 기술로 자리잡고 있다. 하지만, 802.1x 역시 무선랜에 적용될 시 다양한 보안 취약점을 가지고 있다[8]. 이런 문제점들을 위한 해결 노력으로, 802.11 TGi[9] 그룹에서는 향상된 WEP(Wired Equivalent Privacy) 기술 방식과 802.1x를 포함, 개선한 표준을 제정하고 있는 중이다. 또한 무선랜 대중화에 따라, 로밍 문제도 현재 큰 이슈가 되고 있으며, 비단 IAPP뿐만 아니라 3G 시스템과의 연동을 위한 노력도 함께 진행되고 있다.

본 논문에서는 무선랜 서비스를 위해 AP에서 사용중인 IEEE 802.1x 기반의 인증 기능의 설계와 구현을 다루었으며, IAPP를 위한 고려사항도 고찰해 보았다. 앞으로, IEEE 802.11i와 같은 향상된 인증 보안 기능을 연구 개발함과 동시에, 로밍에 대한 지속적인 연구도 필요하다.

## 참 고 문 헌


[1] 박우종, 서동범, "유선통신사업자의 공중무선 LAN 서비스를 위한 가입자 관리 방안," 한국통신학회지, 제19권 5호 2002

[2] IEEE Standard, Standard for port based network access control. *IEEE Draft P802.1x/D11*, March 2001

[3] IEEE, Recommend Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol, *Draft 3*, January 2002

[4] 김세한 외, "공중 무선랜 서비스를 위한 지역정보서비스의 설계 및 구현," *COMSW 2002*

[5] L. Blunk and J. Vollbrecht. PPP Extensible Authentication Protocol(EAP). *RFC 2284*, March 1998

[6] C. Rigney and et. al. Remote Authentication In User Service (RADIUS). *RFC 2138*, April 1997

[7] Open1x implementation, http://www.open1x.org

[8] Arunesh Mishra and William A. Arbaugh, "An Initial Security Analysis of the IEEE 802.1X Standard," Feb 2002

[9] IEEE Standard, Specification for Enhanced Security, *IEEE 802.11i/Draft 2.0*, March 2002

이 현 우(Hyun-woo Lee) 종신회원

1993년 2월 : 한국항공대학교 전자공학과 공학사
1995년 2월 : 한국항공대학교 대학원 통신정보공학과 공학석사
2003년 2월 : 한국항공대학교 대학원 통신정보공학과 박사 과정수료
1995년 2월~현재 : 한국전자통신연구원 통합망핵심 기술연구그룹 선임연구원
<관심분야> 트래픽 혼잡제어, 통신망 연동, 무선랜

김 정 환(Jeong-hwan Kim) 정회원

1997년 2월 : 경북대학교 전자공학과 공학사
1999년 2월 : 경북대학교 대학원 전자공학과 공학석사
1999년 2월~현재 : 한국전자통신연구원 통합망핵심기술연구그룹 선임연구원
<관심분야> 개방형 서비스, 무선랜, 통신망 연동

류 원(Won Ryu) 정회원

1983년 8월 : 부산대학교 계산통계학과 이학사
1988년 2월 : 서울대학교 대학원 계산통계학과 이학석사
2002년 8월 : 성균관대학교 대학원 정보공학과 공학박사
1989년 2월~현재 : 한국전자통신연구원 통합망핵심 기술연구그룹 통합망연동기술팀 팀장
<관심분야> 유무선망 연동, 무선인터넷, BcN

윤 종 호(Chong-ho Yoon) 정회원

1984년 2월 : 한양대학교 전자공학과 학사
1986년 2월 : 한국과학기술원 전기 및 전자공학과 석사
1990년 8월 : 한국과학기술원 전기 및 전자공학과 박사
1995년 8월~1996년 8월 : University of Arizona 방문교수
1991년 8월~현재 : 한국항공대학교 전자·정보통신·컴퓨터공학부 교수
<관심분야> 컴퓨터 통신망, 성능분석