WLAN 서비스에서 사용자 인증과 로밍방식의 설계

Design and Implementation of User Authentication and Roaming Schemes in public WLAN environments

김 동 옥*, 강 동 진**
Kim Dong-Ok, Kang dong jin

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 like EAPOL(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). For the network security and user authenti -cation purposes, a supplicant who wants to access Internet should be authorized to access the AP port using the EAPOL.

Keywords : WLAN, I-WLAN, EAP, Macro Handoff

I. 서 론

공중 환경에서의 무선랜 서비스를 제공하기 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 그룹에서Draft 작업이 계속 진행중인 IAPP에 대해서 살펴본다. 4장에서는 i-WiNG AP상에서의 IEEE 802.1x의 기능 구현 및 동작을 보이고, IAPP를 위한 고려사항들을 제시하며, 마지막으로 결론을 맺는다.

II. 포트기반 네트워크 접근제어방법

IEEE 802.1x는 무선랜 AP나 이더넷 스위치와 같은 point-to-point 연결 특성을 갖는 시스템의 port에 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 architectural framework을 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 무선랜등과 같은 hybrid network를 위해 포트 기반의 망 접근제어를 제공한다. 여기서 포트라함은, 물리적인 LAN segment에 접속되는 시스템의 접합점이 될 수도 있고, 802.11 station과 access point사이에서 설정되는 association 과 같은 논리적인 포트도 될 수 있다.

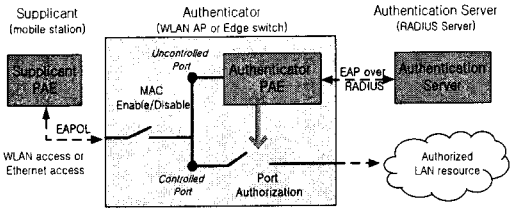

그림 1. IEEE 802.1x Architectural Framework

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(MAC connectivity)를 사용하고자 하는 개체이다.

접수일자 : 2009년 8월 9일
최종완료 : 2009년 8월 9일
*한국정보통신기능대학
교신저자, E-mail : dokim@icpc.ac.kr

표 2 비용 계산 시 사용되는 파라미터

파라미터	값	설명
D_{CN-MA}	6	CN-MAP 사이의 거리 (홉 수)
D_{HA-MA}	4	HA-MAP 사이의 거리 (홉 수)
C_P^{HA}	24	HA에서 글로벌 위치 등록 갱신 메시지를 처리하는 데 드는 비용
C_P^{CN}	6	로컬 위치 등록 갱신 메시지를 처리하는데 드는 비용
C_P^{MAP}	12	MAP에서 로컬 위치 등록 갱신 메시지를 처리하는데 드는 비용
κ	2	무선망에서 패킷의 단위 전송 비용
τ	1	유선망에서 패킷의 단위전송 비용

III. 시뮬레이션 및 결과 분석

시뮬레이션은 C언어와 SMPL을 이용한 가상의 망에서 이루어지며 각 시뮬레이션의 공통된 가정 사항은 표 1과 같다. 전체 네트워크는 총 400개의 서브넷으로 이루어져 있으며 각 서브넷의 모양은 정사각형으로 근사화한다. 각 서브넷에는 하나의 무선 접속 라우터가 존재하며 서브넷의 중심에 위치한다. 각 무선 접속 라우터의 무선 전파 통달 거리는 100m로 동일하며 하나의 서브넷은 여러 MAP으로부터 관리 받을 수 있다. 하나의 MAP은 최소 1개, 최대 400개의 서브넷을 관리 할 수 있다. 이동 단말은 하나의 CN과 통신하며, 현재의 서브넷으로부터 이웃 서브넷들 중 하나로 자유롭게 이동한다.

표 1. 시뮬레이션을 위한 가정

파라미터	값	설명
N_{SUBNET}	400	총 서브넷 개수
N_{M_SUBNET}	1 < = N_{M_SUBNET} <=400	하나의 MAP 도메인에 속하는 서브넷 개수
AR_{RANGE}	100 m	무선 접속 라우터의 전파 통달 거리
N_{MN} , N_{CN}	1	MN과 CN의 개수

비용 계산 시 사용되는 고정 파라미터는 표 2와 같다. D_{CN-MAP}, D_{HA-MAP}는 CN, HA와 MAP 간 거리를 나타내며 각각 6, 4로 가정한다. 유선망에서 패킷의 단위 전송 비용 (패킷 하나를 유선망의 한 홉 구간 전송하는데 드는 비용) τ는 1로, 무선망에서 패킷의 단위 전송 비용 κ는 2로 설정한다. 글로벌 위치 등록 갱신 메시지가 HA에서 처리되는 비용 C_P^{HA}는 24, CN에서 처리되는 비용 C_P^{CN}는 6, 로컬 위치 등록 갱신 메시지가 MAP에서 처리되는 비용 C_P^{MAP}는 12로 가정한다.

단말의 이동속도와 패킷전송률이 전체 통신비용에 미치는 영향을 분석한다.

1. 단말의 이동속도와 통신비용

단말의 이동속도가 통신비용에 미치는 영향을 분석한다. 우리의 실험에서는 이동 단말이 0 m/s와 100 m/s 사이의 이동 속도로 각각 100,000초 동안 가상의 네트워크를 직선으로 움직이며, 네트워크의 가장자리에 도달한 때는 자유롭게 방향을 바꾸어 직선으로 진행하는 이동 모형을 설정하였다. 이동 단말의 패킷전송률은 1,000 packet/s로 가정하였다. 가상의 네트워크는 400개의 서브넷으로 구성되며 서브넷들을 관리하는 MAP 도메인의 크기가 각각 2, 5, 10, 20인 경우로 나누어 실험하되 MAP 도메인들은 서로 중첩되지 않는다고 가정한다.

단말의 이동속도가 1m/s인 경우에는 MAP 도메인 크기에 따른 위치 등록 갱신 비용의 변화가 크지 않다. 이로 인해 패킷 전달 비용이 총 비용의 변화에 큰 영향을 미치게 되며, 패킷 전달 비용이 최소화 되는 지점에서 총 비용도 가장 작은 값을 갖게 된다. 이 그래프에서 패킷 전달 비용 및 총 비용은 MAP 도메인 크기가 약 2일 때 가장 작은 값을 나타낸다. 단말의 이동속도가 30m/s인 경우에는 MAP 도메인 크기가 증가함에 따라 위치 등록 갱신 비용이 적어지며 패킷 전달 비용은 증가한다. 즉 두 비용은 서로 절충관계에 있으며 두 비용의 합인 총 비용은 MAP 도메인 크기가 클수록 감소하다가 MAP 도메인 크기가 약 5일 때 다시 증가하기 시작 한다. 그림 2는 총 비용이 최소화 되는 MAP 도메인의 크기는 단말의 이동 속도가 증가할수록 더 큰 값을 나타낸다. 결과적으로 단말의 이동속도가 빠를수록 더 큰 MAP 도메인을 선택하여 통신하는 것이 더 효율적임을 확인할 수 있다.

IV. i-WiNG AP의 IEEE 802.1x 기능설계 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

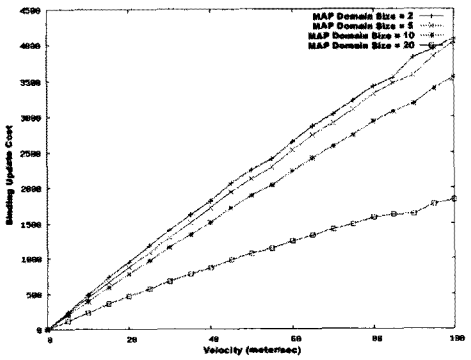

그림 4. 단말의 이동 속도에 따른 위치 업데이트 비용

프로토콜 및 응용 프로그램을 구축하고 있다. 그림 3은 i-WiNG AP시스템의 형상을 나타내고 있다.

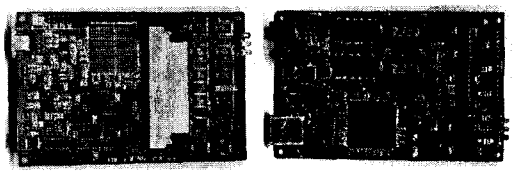

그림 3. i-WiNG AP Board의 형상

2. i-WiNG AP에서의 IEEE 802.1x 기능설계

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

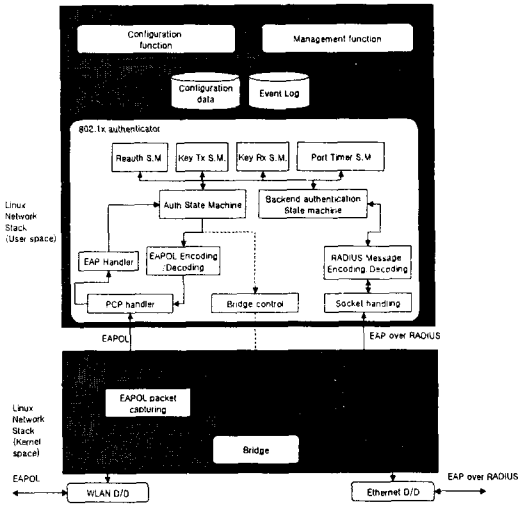

그림 4. i-WiNG의 IEEE 802.1x 기능블럭도

사용자 영역에서는 802.1x 인증 세션을 제어하는 authenticator가 존재하며, 그 내부에 주요한 각 모듈에서는 다음과 같은 일들을 수행하도록 설계되었다.

```
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

V. 결 론

본 논문에서는 무선랜 AP에서 IEEE 802.1x 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 공중무선LAN 서비스를 위한 가입자 관리 방안," 한국통신학회지, 제29권 5호 2006

[2] C.-Der Wann; Y.-Ming Chen, "Mobile location tracking with velocity estimation," *Proceedings of the IEEE 5th International Conference on Intelligent Transportation Systems*, pp. 556-571, 2007.

[3] J. Xie, Ian F. "Akyildiz, A Novel Distributed Dynamic Location Management Scheme for Minimizing Signaling Costs in Mobile IP," *IEEE Transaction on mobile computing*, vol. 1, no. 3, July Sep., 2006.

[4] M. H. MacDougall, *Simulating Computer Systems Techniques and Tools*, The MIT Press, 2007.