망 인프라 공유를 위한 무선랜 시스템들간의 상호 인증 연동 방법

이 완 연†

요 약

기존의 무선랜 시스템 관련 연구에서는 단일 시스템 환경에서 통신 중에 발생하는 보안 문제를 해결하거나 이동 중에 발생하는 재인증을 빠르게 지원하는 방법들을 주로 연구하였다. 본 논문에서는 다수의 무선랜 시스템들을 연동하여 통신 인프라를 상호간에 공유하여 사용하고자 할 때, 자신의 무선랜 시스템에 가입된 사용자들이 타 무선랜 시스템 영역에서도 인증을 성공적으로 수행할 수 있도록 지원하는 방법을 제시한다. 제시된 방법에서는 타 무선랜 시스템에 소속된 무선 접속장치 또는 인증 서버가 자신의 무선랜 시스템에 소속된 인증 서버와 연동하여 사용자의 인증 과정을 중재하도록 설계되었다. 제시된 인증 연동 방법은 802.1X와 EAP-MD5 규격을 기반으로 구현된 무선랜 시스템들을 대상으로 구현되었다.

An Authentication Interworking Mechanism between Multiple Wireless LANs for Sharing the Network Infrastructure

Wan Yeon Lee†

ABSTRACT

The previous studies focussed on the security problem and the fast re-authentication mechanism during handoffs in a single wireless LAN system. When the multiple wireless LAN systems share their network infrastructure one another, we propose an authentication mechanism allowing the subscriber to perform the authentication procedure with the authentication server of its own wireless LAN system even in areas of other wireless LAN systems as well as in areas of its own wireless LAN system. In the proposed mechanism, the access point or the authentication server of other wireless LAN systems plays a role of the authentication agent between the subscriber and the authentication server of the subscriber's wireless LAN system. The proposed authentication mechanism is designed on the basis of the 802.1X and EAP-MD5 protocols.

키워드 : 무선랜(Wireless LAN), 인증(Authentication), 연동망(Interworking System), 인프라 공유(Sharing Infrastructure), 802.1X, EAP-MD5

1. 서 론

최근 들어 무선랜(Wireless LAN) 서비스를 다양한 장소에서 상용으로 제공하는 무선랜 사업이 활성화되고 있다[1]. 상용의 무선랜 통신 서비스는 학교, 공항, 캠퍼스, 카페 등과 같이 사업자의 통신 인프라가 구성된 특정 환경에서 무선 통신 기기(무선랜 카드를 장착한 노트북 또는 무선 단말기)를 가지고 있는 서비스 가입자들에게 무선 통신 서비스를 상용으로 제공하는 것이다. 상용의 무선랜 시스템은 다양한 장소에서 무선 통신을 제공한다는 특징 때문에 유선망과는 달리 물리적인 침입이 없이도 쉽게 데이터를 가로채거나 무선 접속장치(AP : Access Point)를 통하여 내부 유선망으로 침투가 가능하다. 과거의 무선랜 시스템에서는 WEP(Wired Equivalent Privacy)라는 방법을 통하여 무선 통신 보안 기능을 제공하였지만, WEP 방법이 해킹에 취약한 것으로 알려짐에 따라 무선랜 시스템에서의 통신 보안 기능에 개선이 필요하게 되었다[2, 3]. 따라서 무선랜 시스템에서 통신 보안 문제를 해결하기 위해 여러 무선랜 장비 제조업체와 표준화 제정 단체들이 많은 개선 규격을 제공하였으며, 대표적인 규격으로는 무선 접속장치에서 암호학적인 인증 알고리즘을 통하여 정상적으로 인증 받은 사용자에 한하여 내부 네트워크로 접속시켜주는 포트기반의 인증 규격인 IEEE 802.1X가 있다[4]. IEEE 802.1X에서는 인증을 위한 기반 구조(Framework)을 제공하며 실제 암호학적인 인증 알고리즘은 EAP(Extensible Authentication Protocol)라는 프로토콜을 통하여 제공된다[5]. EAP의 세부 규격으로는 현재 국내에서 가장 널리 쓰리는 방식인 사용자 ID와 패스워드를 사용하여 인증하는 EAP-MD5가 있으며[5, 6], 이외에

※ 본 논문은 정보통신연구진흥원에서 지원하는 정보통신기초기술연구사업 연구결과임(과제 번호 : B1220-0401-0188).
† 정 회 원 : 한림대학교 정보통신공학부 교수
논문접수 : 2004년 7월 8일, 심사완료 : 2004년 9월 25일

EAP-TLS, EAP-TTLS, PEAP 등과 같은 방식들이 있다[2, 3].

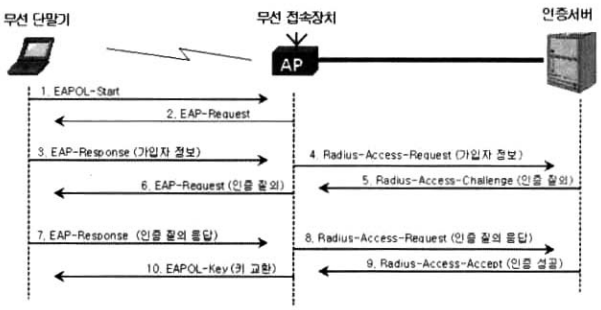
유비쿼터스 컴퓨팅(Ubiquitous Computing) 환경을 구현하기 위해서는 기존에 설치된 동종 또는 이기종 망들간에 상호 연동을 통하여 통합된 환경을 사용자들에게 제공하여야 하고, 이러한 통합된 망 환경을 제공하기 위해서 기존에 설치된 시스템들을 최소의 수정을 통하여 유기적으로 통합하는 새로운 기술이 연구되고 있다[7-9]. 그러나 기존의 무선랜 관련 연구에서는 단일 무선랜 시스템 환경에서 안전한 무선 통신 보안 기능을 제공하기 위한 보안 방법들[2, 3], 그리고 단일 무선랜 시스템 환경에서 사용자가 이동함에 따라 통신을 주고받는 무선 접속장치가 변경됨으로 인해서 발생하는 재인증을 신속하게 지원하는 방법들[10-12]에 관련된 내용만을 주로 다루었다. 즉, 다수의 무선랜 시스템들로 구성된 망 환경에서 무선랜 시스템들간의 상호 연동을 통하여 통합된 망 환경을 제공하는 연구는 전혀 다루어지지 않았다. 만약 다수의 무선랜 사업자가 이미 여러 지역에 무선랜 통신 인프라를 구축하고 있고 사업자별로 구축된 통신 인프라를 서로 공유하여 사용할 수 있다면, 추가로 통신 인프라를 구축하는 비용 없이도 더 많은 지역에서 무선 통신 서비스를 제공할 수 있을 것이다. 따라서 다수의 무선랜 사업자가 개별적으로 무선랜 시스템 통신 인프라를 가지고 있는 경우, 무선랜 시스템들간의 연동을 통하여 망 인프라를 상호 공유할 수 있도록 통합된 망 환경을 제공하는 방법을 연구할 필요가 있다.

본 논문에서는 특정 무선랜 사업자에 가입한 사용자가 이 사업자의 통신 인프라가 구축되지 않은 지역에서 타 무선랜 사업자의 통신 인프라를 통하여 통신 서비스를 제공 받을 수 있는 방법을 연구한다. 타 사업자의 통신 인프라 환경에서 통신 서비스를 제공 받기 위해서는 타 사업자의 망 영역에서도 무선 통신 사용을 위한 사전 인증 절차가 필요하고, 타 사업자의 통신 인프라를 통하여 성공적으로 인증을 수행할 수 있어야 한다. 본 논문에서는 사업자간에 개별적으로 존재하는 통신 시스템들간의 연동을 지원하기 위하여, 타 사업자망의 무선 접속장치나 인증 서버가 사용자가 가입한 사업자 망의 인증 서버와 연동하여 인증을 수행하는 방법을 제안한다. 제시된 연동 방법은 현재 국내에서 가장 많이 사용되고 있는 802.1X와 EAP-MD5 규격을 기반으로 하는 인증 서버들을 대상으로 하였다.

본 논문의 구성은 다음과 같다. 2장에서는 기존의 단일 무선랜 시스템에서 사용되고 있는 802.1X 규격과 EAP-MD5 규격 기반의 인증 방법에 대해서 설명한다. 3장에서는 다수의 무선랜 시스템들의 망 인프라를 상호 연동하여 공유할 수 있도록 지원하는 세 가지 사용자 인증 연동 방법들을 제시한다. 4장에서는 제안된 세 가지 방법들의 장단점을 분석하여 가장 효율적인 방법을 선택하고, 선택된 방법을 실제의 소프트웨어 프로그램으로 구현한 결과에 대하여 설명한다. 마지막으로 5장에서는 본 논문에서 제안된 내용들을 요약·정리한다.

2. 기존의 무선랜 시스템에서 인증 방법

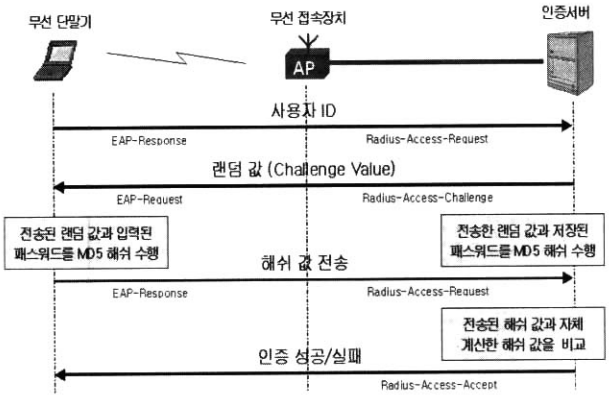
기존의 무선랜 시스템에서는 사용자와 인증 서버간의 인증 절차를 802.1X 규격에 근거하여 구현하고 있다. 무선랜 시스템에서 802.1X 규격의 역할은 무선 단말기와 무선 접속장치, 그리고 인증 서버들간의 인증 절차 및 키 분배 과정을 정의하고 있다[3, 4]. 무선 접속장치는 인증이 성공적으로 이루어진 무선 단말기에 대해서만 통신 포트를 인가하여 무선 통신 서비스를 제공한다. 또한 인증 과정에서 동적으로 생성된 세션 키는 인증 서버로부터 무선 접속장치로 분배되어, 무선 접속 구간에서 데이터 통신 보안 기능을 제공하는데 활용된다[2, 3]. 802.1X의 인증 절차에서 사용자 확인을 위한 세부적인 방법은 EAP 규격을 이용하고 있다[5, 6]. EAP는 다중 인증 메커니즘을 지원하는 일반적인 프로토콜로서 스마트 카드, Keberos, 공용키 암호화, One Time Password를 포함한 수많은 인증 유형을 지원한다[5]. 이 논문에서 대상으로 하는 인증 유형은 패스워드를 MD5 함수를 사용하여 해쉬한 결과 값을 전송하는 CHAP-MD5이다[13].



(그림 1) 802.1X 규격에 기반한 무선랜 접속 과정

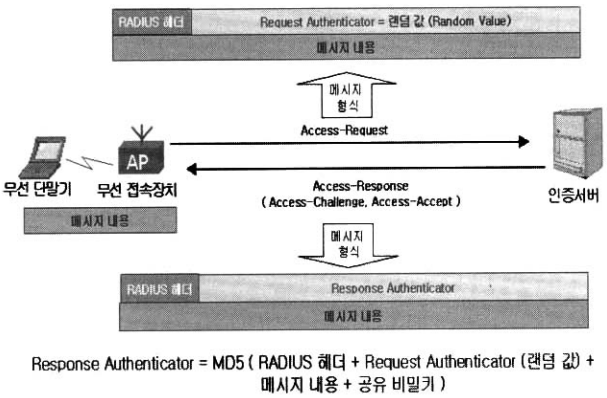
(그림 1)은 무선랜 시스템에서 통신 접속을 위한 802.1X 규격의 메시지 전달 과정을 보여주고 있다[2]. 세부 절차를 살펴보면, 사용자가 통신 접속을 위하여 무선 단말기로부터 EAPOL-Start 메시지를 무선 접속장치에게 보내고, 무선 접속장치는 EAPOL-Start 메시지를 받은 후 가입자 인증에 필요한 가입자 정보를 단말기에게 요청하는 EAP-Request 메시지를 보낸다. 가입자 정보는 무선 단말기로부터 EAP-Response 메시지에 저장되어 무선 접속장치에 전달되며, 무선 접속장치로부터는 Radius-Access-Request 메시지 형태로 전환되어 인증 서버에게 전달된다. 인증 서버는 전달된 가입자 정보를 확인하고, Radius-Access-Challenge 메시지를 통하여 사용자 인증을 위한 추가 인증 질의를 수행한다. 인증 질의 내용을 담고 있는 Radius-Access-Challenge 메시지는 무선 접속장치에 전달되고, 인증 질의 내용은 EAP-Request 메시지에 저장되어 무선 단말기에게 전송한다. 무선 단말기는 인증 질의에 대한 응답을 EAP-Response 메시지를 통하여 무선 접속장치에게 전달하며, 무선 접속장치는 Radius-Access-Request 메시지를 통하여 인증 서버에게 전송한다. 인증 서버는 전달된 인

증 질의에 대한 응답을 분석하며, 인증이 성공하면 Radius-Access-Accept 메시지를 통하여 인증이 성공했음을 알린다. 최종적으로 인증 성공 메시지를 수신한 무선 접속장치가 무선 단말기에게 무선 통신 사용을 허가하고, 무선 단말기와 암호화된 통신을 시작하게 된다.



(그림 2) EAP-MD5 규격을 이용한 사용자 인증 절차 흐름도

사용자 인증에 사용되는 EAP-MD5 규격에서는 가입자 정보로 '사용자 ID' 값을 사용하고, 인증 질의 방법으로는 사용자의 패스워드 정보를 분석하여 정당한 가입자인지 여부를 확인한다. (그림 2)는 802.1X 규격의 무선랜 접속 과정에서 사용자 인증에 사용되는 EAP-MD5 규격의 동작 과정을 보여주고 있다. 세부 동작 과정을 살펴보면, (그림 1)의 802.1X 규격에서 3번의 EAP-Response 메시지와 4번의 Radius-Access-Response 메시지를 통하여 가입자 정보인 사용자 ID 값이 인증 서버에게 전달된다. 인증 서버는 전달된 사용자 ID의 존재 여부를 확인하고, 사용자 ID가 존재하면 인증 질의를 위하여 16바이트 랜덤 값(CV : Challenge Value)을 생성하여 5번의 Radius-Access-Challenge 메시지와 6번의 EAP-Request 메시지를 통하여 무선 단말기에게 전송한다. 무선 단말기는 전송된 랜덤 값과 사용자로부터 입력된 패스워드 값을 사용하여 MD5 해쉬 알고리즘의 수행 결과 값을 계산하고, 계산된 해쉬값을 7번의 EAP-Response 메시지와 8번의 Radius-Access-Request 메시지를 통하여 인증 서버에게 전송한다. 인증 서버는 자신의 데이터베이스에 저장된 패스워드 값과 전송하였던 랜덤 값(CV)을 사용하여 똑같이 MD5 해쉬 값을 계산하고, 무선 단말기로부터 전송된 해쉬 결과 값과 비교한다. 두 개의 해쉬 계산 값이 동일하다면 사용자가 입력한 패스워드 정보와 인증 서버가 저장하고 있는 패스워드 정보가 동일한 것을 의미하고, 인증 서버는 무선 접속장치에게 9번의 Radius-Access-Accept 메시지를 통하여 인증이 성공했음을 알리고 무선 통신 사용을 허가하도록 한다. EAP-MD5 규격에서는 무선 단말기가 사용자의 패스워드 정보를 인증 서버에게 직접 전송하지 않고, 대신 패스워드 정보를 사용한 해쉬값을 인증 서버에게 전송함으로서 사용자의 패스워드 정보가 유출되는 것을 방지하면서 안전하게 확인할 수 있다.



Response Authenticator = MD5 (RADIUS 헤더 + Request Authenticator (랜덤 값) + 메시지 내용 + 공유 비밀키)

(그림 3) RADIUS 메시지 형식

인증 과정에서 무선 접속장치와 인증 서버간에 주고받는 메시지는 RADIUS 메시지 형식을 따라 정의된다[6]. (그림 3)은 RADIUS 메시지 형식을 보여주고 있다. RADIUS 메시지 형식에서는 무선 접속장치와 인증 서버간의 안전한 통신을 위하여, 무선 접속장치와 인증 서버만이 알고 있고 외부에는 알려지지 않은 사전에 정의된 '공유 비밀키' 값을 사용한다. 무선 접속장치로부터 인증 서버에게 전달되는 메시지인 Radius-Access-Request의 Request Authenticator 영역에는 무선 접속장치가 생성한 16 비트 랜덤 값이 저장된다. 그리고 인증 서버로부터 무선 접속장치로 전달되는 메시지인 Radius-Access-Challenge 메시지나 Radius-Access-Accept 메시지의 Response Authenti-cator 영역에는 다음과 같이 계산한 해쉬 결과 값이 저장된다.

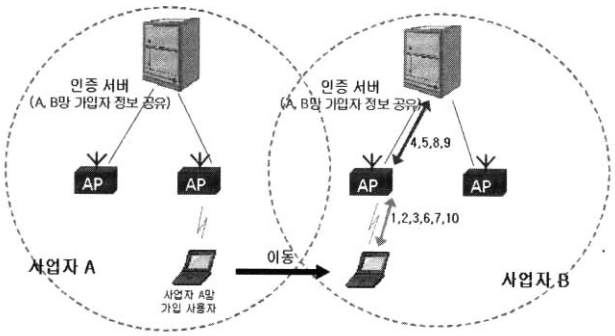
Response Authenticator = MD5(RADIUS헤더 + 전송된 랜덤값(Request Authenticator) + 메시지 내용 + 공유 비밀키)

무선 접속장치는 인증 서버에게 메시지를 보낼 때마다, 랜덤 값을 생성하여 Request Authenticator에 저장하여 보낸다. 그리고 인증 서버로부터 응답으로 전달된 메시지의 Response Authenticator 값과, 자신이 전송한 Request Authenticator 값과 공유 비밀키를 사용하여 해쉬한 결과 값을 비교하여 동일한 경우에만 정당한 수신 메시지로 인정한다. Request Authenticator 값은 무선 접속장치에서 메시지(Radius-Access-Request)를 보낼 때마다 달라지고, 그 결과 인증 서버로부터 전달되는 응답 메시지(Radius-Access-Challenge 또는 Radius-Access-Accept)에 저장되어 전달되는 Response Authenticator의 값도 매번 Request Authenticator 값에 따라 다르게 생성된다. 이처럼 공유 비밀키를 아는 노드만이 메시지를 송신하거나 수신하도록 허가하는 방법을 통하여, 제 3의 노드가 응답 메시지를 변경하거나 다른 메시지를 전송하는 것을 방지한다. 공유 비밀키는 망 관리자가 직접 관리하고, 무선 접속장치와 인증 서버에만 입력된다.

3. 제안된 방식

3.1 문제 정의

기존의 시스템 환경에서는 사용자가 다수의 인증 서버에 접속하여 인증을 수행하는 무선랜 시스템들간의 상호 인증을 연동하는 방법은 제공되지 않는다. 따라서 본 장에서는 특정 무선랜 사업자에 가입된 사용자가 이 사업자의 서비스가 제공되지 않는 타 사업자 영역으로 이동하였을 경우, 타 사업자 망을 통해서 통신 서비스를 제공하는 방법을 제시한다. 타사 망을 통해서 통신 서비스를 제공받기 위해서는 타사 망 영역에서 정당한 사용자라는 인증 절차 필요하고, 이를 지원하기 위해서는 타사 망 영역에서 사용자가 가입한 망의 인증 서버와 연동하여 인증을 수행하는 절차가 필요하다. 따라서 본 논문에서는 타사 망의 시스템 환경에서 자신의 가입한 망의 인증 서버와 연동하는 방법을 제시한다.

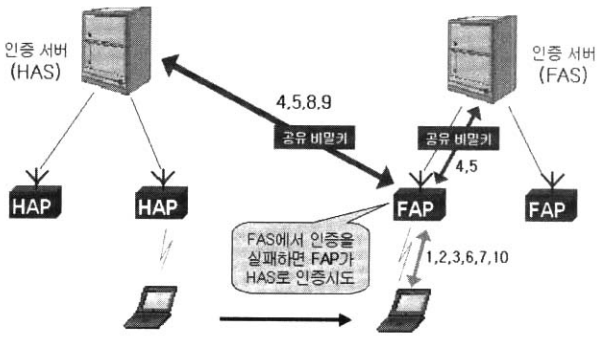


(그림 4) 인증 서버가 여러망의 가입자 정보를 모두 관리하는 방법

(그림 4)는 A망 사업자에 가입한 사용자가 A망을 통해서 통신이 제공되지 않고 B망을 통해서만 통신이 가능한 지역으로 이동한 경우로, B망 영역에서 인증을 수행하는 예를 보여주고 있다. B망 영역에서 A망에서와 같이 동일하게 인증을 성공적으로 수행할 수 있는 가장 쉬운 방법은, (그림 4)에서 보여주듯이 B망의 인증 서버가 A망의 가입자 정보를 모두 저장하는 방법이다. (그림 4)는 A망에 가입한 사용자가 B망의 무선 접속장치를 경유하여 B망의 인증 서버를 통하여 인증을 수행하는 과정을 보여주는 그림으로, 양방향 화살표 옆에 표시된 번호들은 802.1X 기반 인증 과정에 필요한 메시지들을 나타내고 이 번호들은 (그림 1)에서 보여주고 있는 메시지 절차 번호들을 의미한다. 이 방법은 서로 다른 사업자 망의 사용자 정보를 완전히 공유하는 것으로, 가입자 정보를 사용자의 동의 없이 타인에게 공개하는 문제점을 가진다. 또한 사용자의 가입 또는 탈퇴, 정보 변경 등의 수정이 이루어질 때 중복(duplication) 문제로 인해서 사업자의 인증 서버들 간에 사용자 정보를 동기화하기가 어렵다는 문제점을 가진다. 즉, 자사의 가입자 정보를 타 사업자에게 공개하지 않으면서 타 사업자 망을 통해서 인증을 성공적으로 수행하기 위해서는, B망을 통해서 A망의 인증 서버와 연동하는 과정이 필요하게 된다. 이러한 연동 과정은 기존에 구현된 시스템의 수정을 최소화하도록 설계되어야 한다. 따라서 본 논문에서는 기존에 구현된 시스템을 최소로 수정하면서, 사용자 정보를 사업자별로 관리할 수 있는 인증 연동 방법을 연구한다. 제시된 방법에서는 무선랜 사업자들 간에 망 인프라의 공유 사용에 대한 협의가 사전에 이루어졌다고 가정하고, 인증 서버는 사업자별로 개별적으로 운영한다고 가정한다.

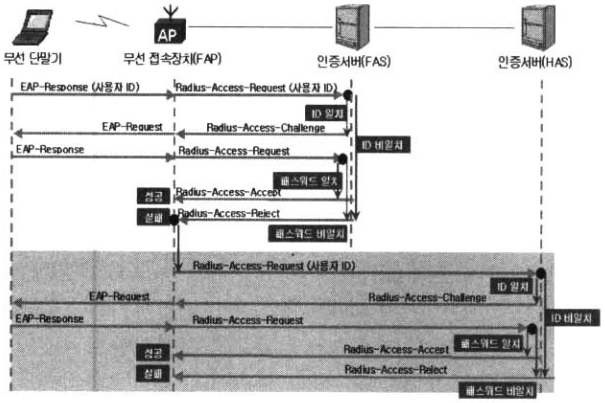
3.2 인증 연동 방법

제안된 방법을 설명하기 위해서 다음과 같은 용어를 정의하여 사용한다. HAS(Home Authentication Server)는 사용자가 가입한 망의 인증 서버를 나타내고, HAP(Home Access Point)는 사용자가 가입한 망에 존재하는 무선 접속장치를 나타내며, FAS(Foreign Authentication Server)는 타 사업자 망의 인증 서버를 나타내고, FAP(Foreign Access Point)는 타 사업자 망의 무선 접속장치를 각각 나타낸다.



(그림 5) 무선 접속장치에서 다른 망의 인증 서버와 연동하는 방법

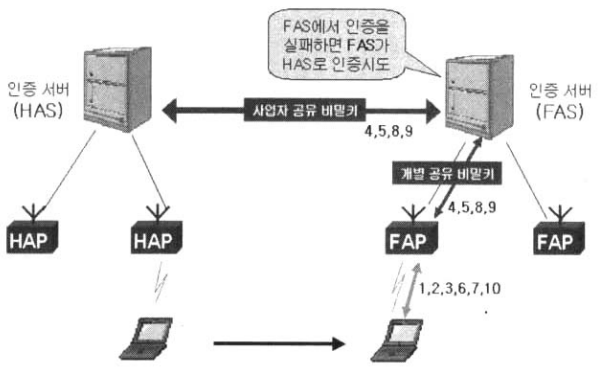
A망에 가입된 사용자가 B망 영역에서 인증을 수행하기 위하여 첫 번째로 제시된 방법은, (그림 5)와 같이 B망의 무선 접속장치(FAP)에서 A망의 인증 서버(HAS)에게 직접 인증을 수행하는 방법이다. 이 방법에서는 B망의 무선 접속장치가 1차로 자사의 인증 서버와 인증을 시도하고 이것이 실패할 경우, 2차로 망 교환 사용을 약속한 타사의 인증 서버와 인증을 시도하는 방법이다. 이 방법에서 B망의 무선 접속장치와 A망의 인증 서버 간에 인증을 성공적으로 수행하기 위해서는 상호간에 동일한 공유 비밀키를 사용하여 응답 메시지의 해쉬값을 생성하여야 한다. 사업자별로 자사의 인증 서버와 무선 접속장치간의 통신 보안을 위해서 사용하고 있는 공유 비밀키를 비밀리에 관리하게 되는데, 이 방법을 사용하기 위해서는 자사에서 사용하고 있는 공유 비밀키 값을 타 사업자의 무선 접속장치에게 알려주어야 하는 문제점을 생긴다. 이는 타 사업자에게 공개된 공유 비밀키를 관리하기 어렵다는 문제점과 망 교환 사용 협약 성립 또는 해제에 따른 연동 대상인 인증 서버 주소의 추가 등록 또는 해제에 관련된 수정 작업을 기존에 설치된 다수의 무선 접속장치들에게 모두 해주어야 하는 문제점을 가진다.



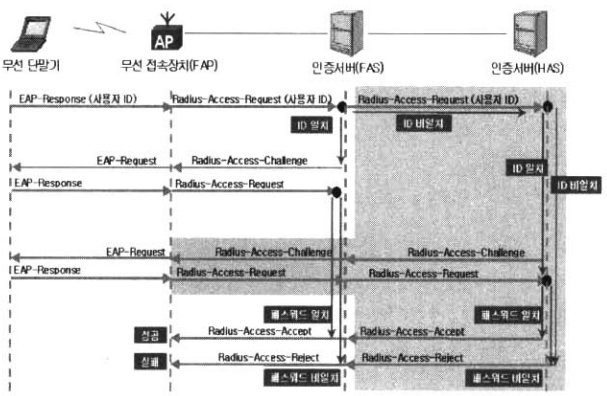
(그림 6) 무선 접속장치에서 인증 연동 작업을 수행하는 방법의 메시지 흐름도

(그림 6)은 (그림 5)에서 제시하였던 방법인 무선 접속장치에서 다른 무선랜 시스템의 인증 서버와 연동하여 인증 작업을 수행하는 방법의 세부 절차를 보여주는 메시지 흐름도이다. 사용자가 타사 망 영역으로 이동하면 인증을 위해 그 망의 무선 접속장치 FAP에 사용자 ID를 전송하고(802.1X 기반의 1, 2, 3번 메시지 절차 수행), FAP는 그 정보를 받아 그 망의 인증 서버인 FAS에게 전송한다(802.1X 기반의 4번 메시지 절차 수행). 사용자 ID를 받은 FAS는 자신의 사용자 정보 데이터베이스에서 전달된 ID와 일치하는 ID를 찾는다. 일치하는 ID를 찾은 경우에는 FAS가 무선 단말기와 EAP-MD5 절차를 통하여 사용자의 패스워드 정보 일치 여부를 확인하고(802.1X 기반의 5, 6, 7, 8번 메시지 절차 수행), 일치하는 ID를 찾지 못한 경우에는 FAS가 FAP에게 인증이 실패하였음을 알린다(802.1X 기반의 9번 메시지 절차 수행). FAP가 인증 실패 메시지를 수신하게 되면, FAP는 사용자에게 실패 메시지를 보내는 대신 기존에 전송된 사용자 ID를 사전에 등록되어 있는 HAS에게 재전송한다(802.1X 기반의 4번 메시지 절차를 다시 수행). HAS는 전달된 사용자 ID를 자신의 사용자 정보 데이터베이스에서 찾아 일치되면, FAP를 경유하여 사용자의 무선 단말기와 EAP-MD5 절차를 통하여 사용자 패스워드 정보 일치 여부를 확인하고(802.1X 기반의 5, 6, 7, 8번 메시지 절차를 다시 수행), 일치하면 FAP에게 인증이 성공하였음을 알린다(802.1X 기반의 9번 메시지 절차 수행). 그리고 HAS마저도 일치되는 ID를 찾지 못하거나 사용자 패스워드 정보가 일치하지 않을 경우에는 FAP에게 인증이 실패하였음을 알리고, FAP는 최종적으로 인증이 실패하였음을 사용자에게 알린다. (그림 6)에서 색칠된 부분은 기존의 무선 접속장치가 수행하는 기능에 비교하여 제시된 방법의 무선 접속장치에서 새롭게 수행하는 기능 부분들이다.

(그림 5)에서 제시한 방법의 문제점을 개선하기 위해서 제시된 두 번째 방법은, (그림 7)과 같이 다른 망 지역의 무선 접속장치(FAP)가 그 망의 인증 서버(FAS)를 경유하여 자사 망의 인증 서버(HAS)와 인증 과정을 수행하는 방법이다. 이 방법에서는 사용자가 B망의 무선 접속장치를 경유하여 B망의 인증 서버와 인증을 먼저 시도하고 B망의 인증 서버가 인증 실패를 결정하면, 망 교환 사용을 약속한 A망의 인증 서버에게 B망의 인증 서버가 추가로 인증을 시도하는 방법이다. 이 방법에서는 B망의 무선 접속장치와 B망의 인증 서버 간에 통신할 때 사용하는 공유 비밀키와 B망의 인증 서버와 A망의 인증 서버 간에 사용하는 공유 비밀키를 개별적으로 생성하고 관리하도록 한다. 이 방법에서 사용되는 자사 망의 무선 접속장치와 인증 서버 간에 사용되는 공유 비밀 키를 '개별 공유 비밀키', 인증 서버들 간에 사용되는 공유 비밀키는 앞으로 '사업자 공유 비밀키'로 명하기로 한다. 사업자 공유 비밀키는 타 사업자에 망 교환 사용에 대한 협약을 진행할 때 생성하여 두 사업자에서만 관리되도록 유지한다. 이 방법은 자사 망의 인증 서버에게 인증이 실패할 때마다 타사의 인증 서버에게 추가로 인증 질의를 수행하는 기능을 추가하여야 한다. 그리고 사업자 공유 비밀키를 사용하여 타사의 인증 서버로부터 전달된 메시지를 개별 공유 비밀키를 기반으로 변환하여 자사 망의 무선 접속장치에게 재전송하고, 개별 공유 비밀키를 사용하여 자사 망의 무선 접속장치로부터 전달된 메시지를 사업자 공유 비밀키를 기반으로 변환하여 타사의 인증 서버에게 재전송하는 기능이 추가로 필요하다.



(그림 7) 인증 서버에서 다른 망의 인증 서버와 연동하는 방법



(그림 8) 인증 서버에서 인증 연동 작업을 수행하는 방법의 메시지 흐름도

(그림 8)은 개선된 두 번째 방법을 통하여 인증 서버들간의 인증 연동 작업을 수행하는 방법의 세부 절차를 보여주는 메시지 흐름도이다. 사용자가 타사 망 영역으로 이동하면 인증을 위해 FAP에 사용자 ID를 전송하고(802.1X 기반의 1, 2, 3번 메시지 절차 수행), FAP는 그 정보를 받아 FAS에게 전송한다(802.1X 기반의 4번 메시지 절차 수행). 사용자 ID를 받은 FAS는 자신의 사용자 정보 데이터베이스에서 전달된 ID와 일치하는 ID를 찾는다. 일치하는 ID를 찾은 경우 FAS는 무선 단말기와 EAP-MD5 절차를 통하여 사용자의 패스워드 정보 일치 여부를 확인한다(802.1X 기반의 5, 6, 7, 8번 메시지 절차 수행). 일치하는 ID를 찾지 못한 경우, FAS는 사용자에게 실패 메시지를 보내는 대신 기존에 전송된 사용자 ID를 사전에 등록되어 있는 HAS에게 재전송한다(802.1X 기반의 4번 메시지 절차를 다시 수행). HAS는 전달된 사용자 ID를 자신의 사용자 정보 데이터베이스에서 찾아 일치되면 FAS와 FAP를 경유하여 사용자와 EAP-MD5 절차를 통하여 사용자 패스워드 정보 일치 여부를 확인한다(802.1X 기반의 5, 6, 7, 8번 메시지 절차를 두 번씩 수행). HAS에서 패스워드 정보가 일치하면 FAS에게 인증이 성공하였음을 알리고(802.1X 기반의 9번 메시지 절차 수행), FAS는 FAP에게 다시 인증이 성공하였음을 알린다(802.1X 기반의 9번 메시지 절차를 다시 수행). 그리고 HAS마저도 일치되는 ID를 찾지 못하거나 사용자 패스워드 정보가 일치하지 않을 경우에는 FAS를 경유하여 FAP에게 인증이 실패하였음을 알리고, FAP는 최종적으로 인증이 실패하였음을 사용자에게 알린다. (그림 8)에서 색칠된 부분은 기존의 인증 서버가 수행하는 기능에 비교하여 제시된 방법의 인증 서버에서 새롭게 수행하는 기능 부분들이다.

4. 분석 및 구현

4.1 제안된 방법 분석

3.1장에서 제시한 인증 서버가 여러 무선랜 시스템들의 가입자 정보를 모두 관리하는 방법을 '사용자 정보 공유 방법'이라 명하고, 3.2장에서 첫 번째로 제시한 FAP에서 FAS에게 인증이 실패할 경우 FAP에서 HAS로 추가로 인증을 시도하는 방법을 '무선 접속장치 연동 방법'이라고 명한다. 그리고 3.2장에서 두 번째로 제시한 FAS가 인증이 실패할 경우 HAS에게 추가로 인증을 시도하는 방법을 '인증 서버간의 연동 방법'이라고 명하기로 한다. 세 가지 방법을 평가하기 위해서 인증 과정에 소요되는 시간, 구현에 필요한 비용, 사용자 정보 공개 여부, 공유 비밀키 공개 여부, 연동 대상 노드의 빈번한 변경에 따른 망 관리 비용을 평가 척도로 사용하여 세 가지 방법을 비교 평가한다. (그림 1)에서와 같이 10단계의 절차를 통해서 이루어지는 인증에 필요한 시간을 계산하기 위해서 다음과 같은 정의를 사용한다. 먼저 같은 망 영역 내에서 (그림 1)의 k번째 단계에 소요되는 통신 시간을 t_k라고 정의하고, 무선 접속장치와 다른 망 영역의 인증 서버와 통신으로 인한 k번째 단계에 소요되는 시간을 t_k'라고 정의하며, 인증 서버와 다른 망 영역의 인증 서버와 통신에 소요되는 시간을 t_x라고 정의한다. 그러면 세 가지 방법들의 인증에 소요되는 시간은 <표 1>과 같다. 사용자 정보 공유 방법의 인증 소요 시간을 T_0라고 하면 $T_0 = t_1 + t_2 + t_3 + t_4 + t_5 + t_6 + t_7 + t_8 + t_9 + t_{10}$이고, 무선 접속장치 연동 방법의 인증 소요 시간을 T_1라고 하면 $T_1 = t_1 + t_2 + t_3 + t_4 + t_5 + t_4' + t_5' + t_6 + t_7 + t_8' + t_9' + t_{10}$이며, 인증 서버간의 연동 방법의 인증 소요 시간을 T_2라고 하면 $T_2 = t_1 + t_2 + t_3 + (t_4 + t_x) + (t_5 + t_x) + t_6 + t_7 + (t_8 + t_x) + (t_9 + t_x) + t_{10}$이다. 일반적으로 같은 망 영역 내에서의 통신 시간이 다른 망 영역간의 통신 시간보다 작으므로 $t_k < t_k'$라고 가정하고, 무선 접속장치와 다른 망 영역의 인증 서버와의 통신 시간과 인증 서버와 다른 망 영역의 인증 서버와의 통신 시간은 거의 동일하므로 $t_k' \simeq t_x$라고 가정한다. 그러면 $T_1 - T_0 = t_4' + t_5' + (t_8' - t_8) + (t_9' - t_9) > 0$이고, $T_2 - T_1 = t_8 + t_9 > 0$이며, $T_2 - T_0 = 4t_x$이다. 이것은 사용자 정보 공유 방법에 비하여 무선 접속장치 연동 방법의 인증 시간이 $t_4' + t_5' + (t_8' - t_8) + (t_9' - t_9)$만큼 추가 시간이 필요하고, 인증 서버간의 연동 방법은 $4t_x'$만큼 추가 시간이 소요된다는 것을 의미한다. 무선 접속장치 연동 방법에 비하여 인증 서버간의 연동 방법의 인증 시간은 $t_8 + t_9$ 만큼의 추가 시간이 소요된다. 즉, 사용자 정보 공유 방법에 비하여 무선 접속장치 연동 방법이나 인증 서버간의 연동 방법의 인증에 필요한 추가 시간은 비교적 크고, 무선 접속장치 연동 방법이나 인증 서버간의 연동 방법에 소요되는 인증 시간의 차이는 비교적 작다고 볼 수 있다.

<표 1> 인증 소요 시간

사용자 정보 공유 방법 인증 소요 시간 (T_0)	$t_1 + t_2 + t_3 + t_4 + t_5 + t_6 + t_7 + t_8 + t_9 + t_{10}$
무선 접속장치 연동 방법 인증 소요 시간 (T_1)	$t_1 + t_2 + t_3 + t_4 + t_5 + t_4' + t_5' + t_6 + t_7 + t_8' + t_9' + t_{10}$
인증 서버간의 연동 방법 인증 소요 시간 (T_2)	$t_1 + t_2 + t_3 + (t_4 + t_x) + (t_5 + t_x) + t_6 + t_7 + (t_8 + t_x) + (t_9 + t_x) + t_{10}$

인증 과정에 소요되는 시간 이외에, 세 가지 방법을 비교하여 평가하면 <표 2>와 같이 정리할 수 있다. 먼저 인증 서버간의 연동 방법과 사용자 정보 공유 방법을 비교하면, 가입자 정보 공개 여부와 연동 노드의 변경에 따른 수정 비용을 제외하고는 동일하다. 사용자 정보 공유 방법은 서로 다른 사업자 망의 가입자 정보를 완전히 공유하는 것으로, 가입자 정보를 사용자의 동의 없이 타인에게 공개하는 문제점을 가진다. 또한 연동 대상인 무선랜 시스템을 변경하고자 하면, 인증 서버의 데이타베이스에 저장된 기존의 연동 대상이었던 무선랜 시스템 가입자 정보를 모두 삭제하고 새로운 연동 대상이 되는 무선랜 시스템의 가입자 정보를 모두 입력해야 하는 것과 같은 수정 작업의 양이 많다. 반면 인증 서버간의 연동 방법에서는 연동 대상 무선랜 사업자의 변경이 생겨도 연동 대상인 인증 서버의 주소만을 변경하면 되므로 연동 노드의 변경에 따른 수정 작업의 양이 미미하다. 따라서 인증 소요 시간이 다소 증가

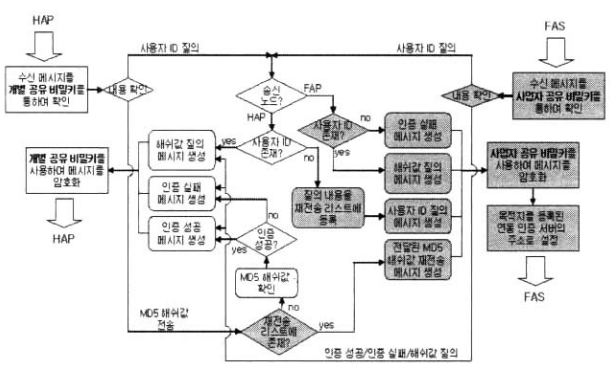
〈표 2〉 세 가지 방법의 비교 평가

	수정이 필요한 망 노드 개수	노드내의 수정 부분	가입자 정보	공유 비밀키	연동 노드의 변경에 따른 수정 비용
사용자 정보 공유 방법	인증 서버 한개	S/W	공 개	비공개	높 음
무선 접속장치 연동 방법	무선 접속장치들 모두	H/W	비공개	공 개	높 음
인증 서버간의 연동 방법	인증 서버 한개	S/W	비공개	비공개	낮 음

하는 인증 서버간의 연동 방법이 가입자 정보를 공개하는 사용자 정보 공유 방법보다 우위에 있다고 평가할 수 있다. 그리고 인증 서버간의 연동 방법에 비교하여 무선 접속장치 연동 방법은, 무선 접속장치 방법의 구현을 위해서는 다수의 무선 접속장치 모두를 수정하여야 하고, 하나의 무선 접속장치를 수정하기 위해서는 H/W 부품을 교체하여야 하며, 공유 비밀키를 타사에게 공개하여야만 하고, 연동 대상이 되는 무선랜 시스템의 인증 서버 주소가 자주 변경될 경우에 많은 수정 비용이 요구되는 단점을 가진다. 따라서 인증 소요 시간이 다소 길더라도 망 관리 비용과 자사 망 통신 보안에 사용되는 공유 비밀키를 공개하지 않아도 된다는 점에서 인증 서버간의 연동 방법이 무선 접속장치 연동 방법보다 우위에 있다고 평가할 수 있다. 인증에 소요되는 시간은 무선 접속장치 연동 방법이 인증 서버간의 연동 방법보다 $t_4 + t_5$ 시간만큼 빠른 것으로 분석되나, 같은 망 영역 내에서의 통신시간인 t_4 또는 t_5의 시간은 매우 짧은 시간으로서 사용자가 느끼는 체감 시간은 차이가 없을 것으로 보인다.

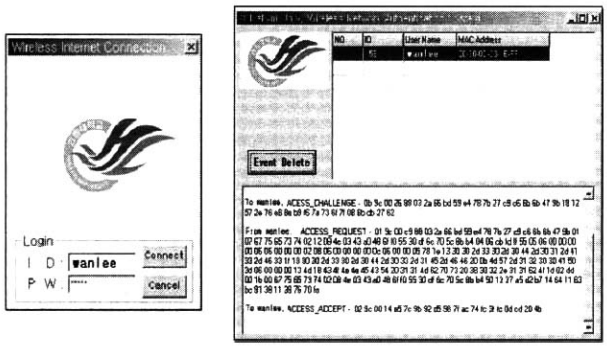
4.2 시스템 구현

무선랜 시스템들간의 연동을 지원하기 위한 방법들 중에서 인증 서버간의 연동 방법이 보안성과 구현 비용, 망 관리 관점에서 가장 효율적인이고 실용적인 방법으로 4.1장에서 평가하였다. 이러한 평가 결과를 바탕으로 인증 서버간의 연동 방법만을 실제 시스템으로 구현하였다. 구현된 시스템의 망 구성도는 (그림 4)와 동일하며, 무선 접속장치는 기존의 상용 제품인 MMC Technology 사의 MW-1200AP 장비를 아무런 수정 없이 사용하였고, 인정 서버는 펜티엄-IV PC상에서 인증 기능을 수행할 수 있도록 802.1X 규격과 EAP-MD5 규격, 그리고 RADIUS 규격을 근간으로 소프트웨어 프로그램으로 구현하였다.



(그림 9) 구현된 인증 서버의 동작 절차도

(그림 9)는 구현된 인증 서버에서 수행하는 기능들의 동작 흐름도이다. (그림 9)에서 색칠이 없는 부분이 기존 무선랜 시스템의 인증 서버에 필요한 기능을 수행하기 위한 부분이고, 색칠이 있는 부분이 타사 망의 인증 서버와 연동하는 기능을 수행하기 위해서 추가로 필요한 동작 부분이다. 개발된 서버용 프로그램은 자사망의 인증 서버인 HAS와 타사망의 인증 서버인 FAS에서 모두 동일하게 동작하도록 구현되었다. 무선랜 사업자들끼리 망 인프라 공유를 사전에 협의하게 되면, 타사 망의 인증 서버 IP 주소를 FAS 주소로 프로그램에 등록시키고 두 사업자들만 관리하는 사업자 공유 비밀키를 정의하여 프로그램에 등록한다. 즉, 연동 대상이 되는 사업자 망의 인증 서버 주소가 자주 바뀌어도 FAS 주소와 사업자 공유 비밀키 값만 변경하면 동작할 수 있도록 구현되었다.



(a) 무선 단말기용 접속 프로그램 (b) 서버용 인증 연동 프로그램

(그림 10) 무선 단말기용 접속 프로그램과 인증 서버용 인증 연동 프로그램

(그림 10)은 개발된 시스템에서 사용자가 무선 노트북상에서 통신사용 승인을 받기 위해 사용자 ID와 패스워드를 사용하여 인증을 요청하는 클라이언트용 프로그램과, 인증 서버에서 전달된 사용자의 ID와 해쉬 값을 분석하여 인증을 수행하는 서버용 프로그램의 동작 화면을 보여주고 있다. 클라이언트용 프로그램은 무선 노트북상에서 사용자가 입력한 ID와 패스워드 정보를 안전하게 무선 접속장치를 통하여 인증 서버에게 전달하도록 개발된 프로그램으로, 기존에 개발된 무선 단말기용 접속 프로그램과 기능상의 차이는 없다. 서버용 프로그램은 전달된 사용자의 ID와 패스워드 정보가 정확한지 여부를 EAP-MD5 표준 규격에 근거하여 사용 승인을 결정하고, 주기적으로 무선 통신 서비스 사용량 정보를 수집하는 역할을 수행한다. 기존의 서버용 인증 프로그램에서는 무선 통신 사용을 위한 인증 요구 시에 자체 가입자 정보 데이터베이스에서 통신

요구 사용자 정보를 확인하지만, 개발된 서버용 인증 프로그램에서는 무선 통신 사용을 위한 인증 요구 시에 1차로 자체 가입자 정보 데이터베이스에서 사용자 정보를 확인하고 실패하면 사전에 등록된 다른 인증 서버에게 2차로 인증 질의 절차를 다시 시도하는 기능이 추가되었다.

5. 결 론

본 논문에서는 다수의 무선랜 사업자들이 이미 여러 지역에 무선랜 통신 인프라를 개별적으로 구축하고 있는 환경에서, 사업자별로 구축된 통신 인프라를 공유할 수 있도록 지원하는 방법을 연구하였다. 기존에 구축된 사업자별 통신 인프라의 공유 기능을 제공하기 위해서 무선랜 시스템들간에 상호 인증 연동을 수행하는 세 가지 방법들을 제시하였다. 제시된 방법들은 타사 망의 인증 서버가 다른 사업자들의 가입자 정보 공유를 통하여 인증을 수행하는 방법, 타사 망의 무선 접속장치가 자사 망의 인증 서버와 연동하는 방법, 타사 망의 인증 서버가 자사 망의 인증 서버와 연동하는 방법이다. 비교 분석을 통하여 제시된 방법들 중에서 인증 서버들간의 연동 방법이 인증 소요 시간은 다소 증가하나 가입자 정보의 관리, 통신 보안 정보 관리, 구현 비용, 망 관리 비용 면에서 가장 실용적인 방법으로 평가하였다. 그리고 가장 실용적으로 평가된 인증 서버간의 연동 방법을 실제 무선랜 시스템 환경에서 구현하여 성능의 효율성을 검증하였다.

참 고 문 헌

[1] 김용균, 임영이, 이재환, "공중 무선 랜 서비스 동향", 전자통신동향분석, 제17권 제5호, pp.119-128, Aug., 2002.

[2] 박애순, 윤미영, 김영진, "802.11b 기반 무선 랜 인증 및 보안 기술", 한국통신학회지, 제19권 제8호, pp.114-127, Aug., 2002.

[3] 송지은, 왕기철, 김태연, 조기환, "무선 LAN 환경에서 요구되는 보안 기술", 정보처리학회지, pp.77-86, Mar., 2003.

[4] IEEE 802.1X, "IEEE Standard for Local and Metropolitan Area Networks - Port-based Network Access Control," 2001.

[5] RFC 2284, "PPP Extensible Authentication Protocol (EAP)," March, 1998.

[6] RFC 3579, "RADIUS(Remote Authentication Dial in User Service) Support For Extensible Authentication Protocol (EAP)," September, 2003.

[7] 이완연, 박찬영, "무선 LAN망과 이동통신망을 연동하는 통합 시스템에서의 과금 방안", 정보과학회논문지(정보통신), 제31권 제1호, pp.53-61, Feb., 2004.

[8] 이혜진, 이완연, 박찬영, "다중 무선 LAN 사업자 환경에서 인증 서버들간의 효율적인 연동 방법", 정보과학회 컴퓨터시스템연구회 추계학술발표회, pp.114-119, Nov., 2003.

[9] 이완연, "무선접속망에서 IP 전송 방식과 ATM 전송 방식 상호연동을 위한 IP 버전처리", 정보처리학회논문지C, 제9-C권 제5호, pp.627-636, Oct., 2002.

[10] Y. Matsunaga, A. Merino, T. Suzuki, R. Katz, "Secure Authentication System for Public WLAN Roaming," Proceedings of ACM International Workshop on Wireless Mobile Application and Service on WLAN Hotspots, pp. 113-121, 2003.

[11] J. Zhang, J. Li, S. Weinstein, N. Tu, "Virtual Operator Based AAA in Wireless LAN Hot Spots with Ad-hoc Networking Support," ACM SIGMOBILE Mobile Computing and Communications Review, Vol.6, No.3, pp.10-21, July, 2002.

[12] 송일규, 홍충선, 이대영, "무선 LAN 환경에서 단말 이동시 AP간 메시지 보안 개선 방안", 정보과학회 춘계학술대회, Vol.30, No.1, Apr., 2003.

[13] RFC 1994, "PPP Challenge Handshake Authentication Protocol(CHAP)," August, 1996.

이 완 연

e-mail : wanlee@hallym.ac.kr

1994년 포항공과대학교 컴퓨터공학과(학사)

1996년 포항공과대학교 컴퓨터공학과(석사)

2000년 포항공과대학교 컴퓨터공학과(박사)

2000년~2003년 LG전자 정보통신 선임 연구원

2003년~현재 한림대학교 정보통신공학부 조교수

관심분야 : 차세대 이동통신망, 시스템 소프트웨어, 실시간/분산 시스템