情報保護學會論文誌
第13券 第3號, 2003. 6

공개키 기반구조에서 빠른 핸드오프를 위한 무선랜 인증 기법 설계*

정 종 민**, 이 주 남**, 이 구 연***

Design of Wireless LAN Authentication Mechanism for Fast Handoff Service based on PKI

Jong Min Jeong**, Ju Nam Lee**, Goo Yeon Lee***

요 약

무선랜은 전파라는 전송 매체를 사용함으로써 보안에 대한 취약성을 내포하고 있다. 보안 기능을 제공해 주는 PKI는 보안적인 측면 뿐만 아니라 글로벌 로밍 서비스를 가능하게 하는 원천이 된다. 그러나 PKI를 사용할 경우에 인증 과정에서 인증서 검증과 CRL 검색 등의 많은 오버헤드가 발생하게 된다. 초기 인증과 달리 핸드오프 시 효율적인 무선 서비스 제공을 위해서 사용자 등록 지연을 최소화 할 수 있는 빠른 인증 기법이 필요하다. 본 논문에서는 PKI를 이용한 인증 과정에서 발생할 수 있는 오버헤드를 최소화하여, 핸드오프 시 사용자 등록 지연을 방지 할 수 있는 새로운 인증 기법을 설계한다.

ABSTRACT

Wireless LAN has the advantage of extension, flexibility and easiness of installation and maintenance. However, due to the characteristics of wireless media, it is vulnerable to security attacks. PKI(Public Key Infrastructure) is estimated to be a good solution offering security function to wireless LAN including global roaming. It offers high security functions as authentication, confidentiality and digital signature while it generates big overheads such as CRL search and certificate verification. The overheads can not be avoided during the initial authentication. However, when we consider the case of handoff, it can be minimized through the fast handoff. In this paper, we design a fast handoff authentication mechanism based on PKI in the wireless LAN and analyze the performance of the scheme.

Keyword : wireless LAN, PKI, authentication, fast handoff

I. 서 론

유선랜을 무선으로 확장시킨 무선랜은 공간을 초월하여 네트워크 자원을 사용 가능하게 만들었으나[1] 전송 매체로 전파를 사용하기 때문에 보안상 취약성을 내포하고 있다. 그러므로 통신하는 데이터를 암호화함으로써 기밀성을 유지하고 인증 된 사용자에게만 네트워크 접속을 허용하는 보안 기능이 연구되어지고 있다[2].

* 본 논문은 2003년도 강원대학교 연구년 교수 프로그램에 의하여 연구되었으며 또한 2003년도 강원대학교 두뇌한국21 사업에 의하여 지원되었습니다.
** 강원대학교 컴퓨터정보통신공학과(minee,leejn}@cnclab.kagnwon.ac.kr)
*** 강원대학교 전기전자정보통신공학부(leegyeon@kangwon.ac.kr)

현재 보안 기능을 일관성 있게 제공해 주는 기술로 PKI(public key infrastructure)를 들 수 있다. 무선 환경에서 PKI는 보안 기능뿐만 아니라, 안전한 글로벌 로밍 서비스를 가능하게 하는 원천이 된다. 하지만 제한된 성능을 지닌 무선환경에서 CRL 검색과 인증서 검증에 관련된 부분의 처리는 큰 오버헤드를 유발하게 된다. CRL을 검색하는데 소비되는 시간은 CRL 크기, 디렉토리 저장 위치, 인증서 체인을 구성하는 인증서 수, 그리고 CRL을 검색하는 시스템의 사양에 따라 처리 속도가 결정된다. 즉 무선 환경에서도 이 부분을 얼마만큼 효율적으로 처리하는지가 중요한 요소가 된다.

무선랜은 특성상 사용자 이동이 빈번하게 발생하며, 핸드오프 시마다 완전 인증(full authentication)을 수행하기 때문에 많은 오버헤드를 야기 시킨다[3]. 따라서 핸드오프 시 효율적인 무선 서비스를 제공하기 위해서는 사용자 등록 지연을 최소화 할 수 있는 빠른 인증 메커니즘이 필요하다[4]. 이를 위해 본 논문에서는 무선랜의 사용자 인증을 위해 PKI기반의 방법을 고려하였으며, 그 경우에 필수적으로 사용되는 인증서에 대한 CRL 검색과 검증 과정을 최소화함으로서, 효율적인 무선 인터넷 서비스를 제공하기 위한 빠른 핸드오프를 지원하는 인증 기법을 제안한다.

서론에 이어 2장에서는 기존의 무선랜 인증 방법과 핸드오프 성능 개선 방안에 대해서 살펴보고 3장에서는 빠른 핸드오프를 지원하는 인증 기법을 제안한다. 4장에서는 제안한 인증 기법의 성능을 분석하고, 5장에서 본 논문의 결론을 맺는다.

II. 관련 연구

2.1 무선랜 인증 방법

본 절에서는 현재 사용되고 있는 무선랜의 인증 방법에 대하여 살펴본다[5].

2.1.1 오픈시스템(Open System) 인증 방법

오픈 시스템 인증은 802.11의 디폴트 인증 프로토콜로써, 무선 단말기가 네트워크에 접속 하고자 할 경우에 SSID(service set ID)가 포함된 probe 요구를 전송하면 SSID가 일치하는 AP(access point)에서 무선 단말기에게 응답을 보내고 접속을 허용하는 방법이다. 이 방법은 무선 단말기가 암호화되지 않은 SSID를 브로드캐스트로 전송하고, SSID와 함께 전달되는 인증용 패스워드도 평문 형태이므로 인증을 위한 사용자 정보가 그대로 네트워크에 노출된다. 또한 패스워드에 대한 입력 시도의 제약이 없으므로 보안 측면에서 아주 취약한 방법이다.

2.1.2 공유키(Shared Key) 인증 방법

AP와 무선 단말기가 공통적으로 가지고 있는 WEP(wired equivalency privacy) 키를 이용하여 데이터를 암호화하고 사용자를 인증하는 방법이다. 무선 단말기가 네트워크 접속을 요청하면, AP는 무선 단말기를 인증하기 위해서 챌린지(challenge)를 전송한다. 무선 단말기는 WEP 키를 이용하여 챌린지를 암호화하여 AP에게 재 전송한다. AP는 암호문을 복호한 후 원문과 비교하여 인증을 허가하게 된다. 그러나 공유키 인증 방법도 암호화에 사용되는 WEP 키의 수가 고정되어 있으며, 사전에 무선단말기와 AP가 공유된 키 테이블을 가지고 있어야 하는 단점이 있으므로 이에 대한 보완이 요구된다.

2.1.3 MAC 주소기반 인증 방법

무선랜 카드의 MAC 주소를 이용하는 방법으로 무선 단말기가 자신의 MAC 주소가 포함되어 있는 인증 요구 메시지를 AP로 전송하게 되면 AP는 자신이 저장하고 있는 MAC 리스트를 검색하여 접속을 허용한다. 그러나 AP에 저장할 수 있는 MAC 주소에 한계가 있으며, 암호화되지 않은 MAC 주소를 전송하므로 쉽게 스니핑(sniffing) 당할 수 있다. 또한 대부분의 무선랜카드의 MAC 주소는 소프트웨어적으로 변경 가능하여 공격자가 MAC 주소를 재 사용할 수 있는 단점이 있다.

2.2 802.1X를 이용한 인증 모델

많은 사람들이 공유하는 SSID나 WEP 키는 노출될 가능성이 크고, MAC 주소를 사용자 별로 필터링하는 것은 무선랜 사용자가 증가함에 따라 거의 불가능해 졌다. 기존의 무선랜 인증 방법의 한계로 인해 802.1X가 새로운 인증 방법으로 도입되었다. 802.1X를 무선랜에 적용함으로써 기존의 무선랜 인증 방법에서 제기되었던 문제들을 해결할 수 있었다[6]. 동적인 키 갱신을 이용하여 무선 구간의 데이터 기밀성을 해결하고, AP와 인증 서버를 분리함으로써 무선 단말기 사용자의 제약 없는 글로벌 로밍 서비스와 서비스를 요청하는 무선 단말기의 수에 무한한 확장

성을 제공할 수 있게 되었다[7].

2.2.1 802.1X의 동작 원리

802.1X 인증 모델은 네트워크 서비스를 제공받으려는 인증 요구자(supplicant)와 인증 절차를 수행하는 인증자(authenticator), 인증 서버(authentication server)로 구성된다. 이때 인증 요구자와 인증자를 PAE(port access entity)라고 한다[8]. 802.1X에서는 포트 기반 접근제어를 사용하는데 이를 위하여 비 제어 포트와 제어 포트의 개념이 사용된다. 비 제어 포트는 인증 요구자가 네트워크의 인증 서버와 같이 인증에 필요한 인증 관련 자원만을 사용할 수 있는 포트로써, 인증이 성공적으로 이루어지면 제어 포트를 이용하여 네트워크 자원을 자유롭게 사용할 수 있게 된다. 802.1X는 전송 프로토콜로 EAP(extensible authentication protocol)를 이용한다. 인증 요구자와 인증자 사이의 통신은 EAPOW(EAP over WLAN)를 사용하고, 인증자와 인증 서버 사이의 통신은 EAPOL(EAP over LAN)을 사용한다[9].

2.2.2 802.1X를 이용한 인증 방법

802.1X를 이용한 인증 방법을 살펴보면 다음과 같으며, [표 1]에 각 구조에 대한 비교를 정리한다.

① EAP-MD5

EAP-MD5는 가장 초기의 EAP 인증 유형으로 유일한 필수(mandatory) 구현 방식이다. 이 방법은 802.1X에서 기본 수준의 EAP를 지원하는 대표적인 EAP 인증 유형이다. 이 유형에서는 인증을 위하여 사용자 이름과 패스워드가 전송되는데, 사용자 이름은 암호되지 않은 상태, 패스워드는 MD5로 해쉬 되어 전송된다.

② EAP-TLS

EAP-TLS는 사용자 인증서와 서버의 인증서를 서로 교환함으로써 무선 단말기와 무선 네트워크 사이에 PKI 기반의 상호 인증을 제공한다. 그리고 안전한 연결을 보장하기 위해 사용자 기반, 세션 기반의 동적인 WEP 키를 생성하여 분배한다. 이 구조에서도 사용자 이름은 암호되지 않은 상태로 전달되나, 패스워드의 사용이 불가능하고 반드시 인증서를 이용하여 인증을 처리하게 된다.

③ EAP-TTLS

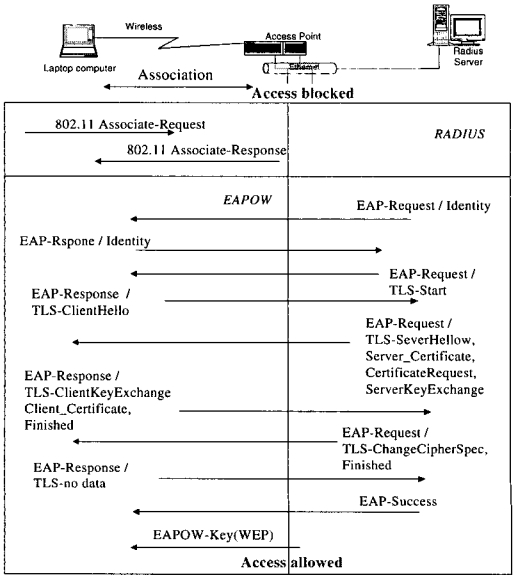
EAP-TTLS는 EAP-TLS의 확장 형태이다. 그러나 EAP-TLS와는 다르게 서버 측의 인증서만을 사용하고, 무선 단말기의 인증서는 사용하지 않는다. 또한 기존의 패스워드 프로토콜을 지원하며, 사용자 정보는 TLS 프로토콜을 통해 안전하게 터널링 된다. 따라서 무선 링크를 포함한 RADIUS까지의 전체 네트워크 상에서 사용자는 외부 도청자에게 익명성이 보장된다.

다음의 [표 1] 에서 EAP-MD5, EAP-TLS 및 EAP-TTLS의 인증형태를 간단히 비교하였다.

〔표 1〕 주요 EAP 인증 형태 비교

비교 항목	EAP-MD5	EAP-TLS	EAP-TTLS
Dynamic WEP	No	Yes	Yes
상호 인증	No	Yes	Yes
인증 방식	MD5-hash	인증서	패스워드
관리 용이성	좋음	나쁨	좋음
사용자 정보전송	암호화 안됨	암호화 안됨	암호화

[그림 1]은 EAP-TLS의 인증 과정을 나타낸 것이다. EAP-TLS는 현재 연구되고 있는 무선랜의 802.1X 인증 방법 중 PKI를 적용한 대표적인 인증 방법으로, TLS 핸드쉐이크를 EAP 프로토콜로 확장한 것이다. EAP-TLS를 이용하면 무선 단말기는 서버의 인증서를 통해 네트워크를 인증하고, 서버는 사용자 인증서를 통해 사용자를 인증할 수 있어 상호 인증이 가능하며 동적인 세션키의 사용이 가능하다.



〔그림 1〕 EAP-TLS 인증 과정

2.3 무선랜 핸드오프 성능 개선 방법

기존에 이루어진 빠른 핸드오프 및 성능 분석에 관하여 살펴본다.

2.3.1 IEEE802.11 MAC 핸드오프 성능 분석

A. Mishra 등은 IEEE802.11의 MAC 핸드오프에 관한 성능 분석을 하였는데, 핸드오프의 논리적인 단계를 probe 지연, 인증 지연, 재 조합 지연으로 구분하여 각 단계가 전체 핸드오프의 지연에 영향을 미치는 정도를 측정하였다. 실험 결과 probe 시간이 핸드오프 지연에 가장 큰 요소로 평가되었으며, 또한 Lucent, Cisco, ZoomAir 등의 여러 제품들을 비교하여 본 결과 핸드오프 지연에 상이한 성능을 보이고 있음을 나타내었다[10].

2.3.2 선행 인증(Pre-Authenticated)을 통한 빠른 핸드오프

S. Pack 등은 무선 단말기가 기본 서비스 영역(basic service set)에 들어오면, 현재 AP 뿐만 아니라, 인접한 다수의 AP들과 인증 절차를 선행하여 핸드오프 시 재 인증에 대한 지연을 최소화하여 빠른 핸드오프를 가능하게 할 수 있음을 보이고 있다. 현재의 AP와 인접한 AP들의 집합을 핸드오프 영역으로(frequent handoff region) 정의하게 되는데, 이는 무선 단말기의 움직임 패턴과 AP의 위치에 의해 결정된다. 또 이러한 요소를 결정하기 위해서는 사용자의 로깅 정보와 핸드오프 이벤트에 대한 로킹 데이터베이스 시스템이 사용되게 된다[11].

2.3.3 Proactive 캐슁을 통한 핸드오프 성능 개선

A.Mishara 등은 Proactive 캐슁 알고리즘을 제안하였는데, 재 조합기간 동안의 IAPP(inter access point protocol) 지연을 제거하기 위해 이웃한 AP들에게 보안 문맥을 초기 조합 단계에서 미리 전달하고자 하였다. 그렇게 함으로써 핸드오프 시 새로운 AP의 캐쉬에 미리 저장되어 있는 문맥을 사용하여 빠른 핸드오프를 가능하게 하였다. 물론 이를 위해 AP들이 잠재적인 이웃 AP들의 관계를 구성할 수 있어야 하며, 이에 대한 리스트를 유지해야 한다. 실험 결과를 통해 이동성이 높을 때 핸드오프 지연이 망 성능의 중요한 역할을 하고 있으며, LRU(least recently used) 캐슁일 경우 이동성이 일정 한도까지 높아 질 수록 캐쉬적중률도 좋아져 빠른 핸드오프가 가능함을 보여주고 있다[12].

위와 같이 기존 핸드오프 성능 개선을 위한 몇 가지 연구와 802.1X에서 제시하고 있는 무선랜의 인증 형태를 정리하였다. 빠른 핸드오프를 위한 방안에 대해 추가적으로 B. Aboba의 연구[13]를 살펴보더라도 핸드오프 기간 동안 발생하는 재 조합의 단계를 초기 조합 단계에서 선행하는 형태를 보여 주고 있다. 물론 이 경우 핸드오프 과정은 단축되어 질 수 있으나, S. Pack의 경우 무선 단말기가 초기 조합 단계에서 인접한 다수의 AP와 인증을 선행해야 하므로 무선 단말기의 부하가 발생하여 초기 조합의 지연이 발생할 소지가 있다. 또한 A.Mishara 등이 제안한 AP 간의 캐슁을 통해 미리 문맥을 교환한 방식은 AP 간의 신뢰 기반 없이 자료를 전달하므로 보안 문제가 발생할 수 있다.

위와 같이 무선랜에 관하여 여러 방법 등을 살펴보았으나 무선랜의 인증 보안을 위해서는 PKI 기반의 802.1X의 인증 기술이 최적임을 알 수 있다. 그러나 PKI에서는 인증서 사용이 필수적인데, 이는 인증서 검증 및 CRL 검색의 오버헤드가 핸드오프 시 성능에 많은 부담으로 작용하게 됨을 의미한다. 본 논문에서는 이를 해결하고 빠른 핸드오프를 제공하기 위하여

- PKI방식의 AP간의 상호 인증을 통한 안전한 통신
- 무선단말기의 초기 조합 단계에서 인접 AP와의 통신 요구하지 않음,
- 핸드오프 시 발생하는 인증서 재검증 및 CRL 검색에 따른 성능 저하를 방지하기 위해 CRL 검색 및 인증서 재검증의 과정을 AP에 위임 등

의 기능이 포함된 빠른 인증을 통한 핸드오프 성능 개선 방안을 제안하였다.

III. 제안 구조

2장에서 살펴보았듯이 오픈시스템 인증 방법, 공유키 인증 방법 및 MAC 주소기반 인증 방법은 이미 많은 문제점들이 노출되었기 때문에 현재는 PKI를 적용한 802.1X 인증 방법이 연구되고 있다[14]. 하지만 EAP-TLS의 경우처럼 사용자 인증에 PKI를 사용하였을 경우에는 인증서 검증과 CRL 검색 등의 많은 오버헤드가 발생한다. 초기 인증 과정에서 인증서 검증 및 CRL 검색은 필수적이나, 연결 설정 전이므로 서비스 제공에는 큰 문제가 되지 않는다. 그러나 핸드오프 시의 인증 과정에서 인증서 검증 및

CRL 검색으로 인한 오버헤드는 사용자가 서비스를 안정적으로 제공받는데 장애가 된다. 그러므로 본 논문에서는 핸드오프 시 오버헤드를 최소화 할 수 있는 새로운 인증 기법을 제안한다.

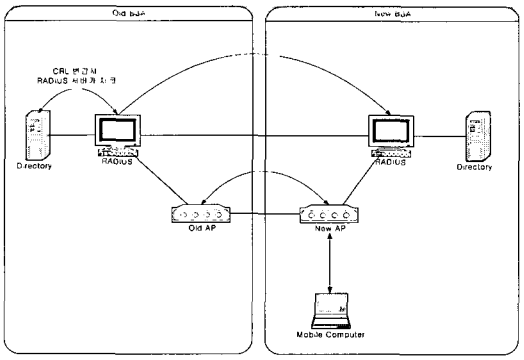
3.1 핸드오프 시 인증 방법

PKI를 사용하는 무선 네트워크 사용자가 증가함에 따라 CRL 크기도 커질 것이며, 이는 곧 인증 시간의 증가를 의미한다. 따라서 무선 단말기의 핸드오프 시 인증 과정에서 CRL을 매번 검색하는 것은 많은 시간이 소비되어 효율적인 무선 서비스를 제공할 수 없게 된다. 따라서 무선 단말기 인증시 CRL 검색 과정을 얼마만큼 빠르게 처리하는지가 효율적인 서비스 제공에 중요한 영향을 미치게 된다.

본 논문에서는 각 AP간의 상호 인증을 통해서 CRL 검색 과정의 오버헤드를 줄일 수 있는 새로운 인증 기법을 설계하였다. 제안한 인증 기법을 위해서 AP는 자신의 주변에 위치한 AP들과 미리 완전 인증을 통해서 상호 인증 과정을 수행해야 한다. 이 과정을 통해서 각 AP는 인접한 AP에 대한 정보와 공개키를 획득하고 이를 저장하게 된다. AP의 경우는 가입과 탈퇴가 빈번한 무선 단말기와는 달리 구성의 변화가 자주 있지 않기 때문에 AP가 구동될 때에 주변의 AP들을 인식하는 과정에서 상호인증을 맺는 것이 단말기의 핸드오프 시에 인증을 하는 구조보다 훨씬 효율적이 된다. 즉 인증서의 CRL 검증도 AP의 구동시에 수행하게 되며 이후의 새로 CRL에 등록되는 AP의 인증서의 경우는 RADIUS 서버에서 해당 AP의 주변 AP에게 통보하게 된다.

무선 단말기의 초기 인증 과정에서는 AP가 무선 단말기의 인증서와 CRL을 검색해야 하지만 핸드오프 인증에서는 각 AP간의 상호 인증을 통해서 CRL 검색 과정을 생략 하게된다. 이때 생략된 CRL 검색 과정을 보완하기 위해서 RADIUS 서버는 OCSP를 통해서 무선 단말기 인증서의 CRL 정보를 주기적으로 확인하고 CRL 변경사항이 생기면 해당 무선 단말기에게 서비스를 제공하고 있는 AP에게 사용자 인증 무효를 통보한다. 따라서 무선 단말기의 핸드오프 시 인증 과정에서 CRL 검색에 소요되는 시간만큼 무선 단말기에게 빠른 핸드오프를 제공할 수 있게 된다. 이때 사용자 인증은 AP와 무선 단말기간에 인증서를 통해 획득한 공개키를 사용하기 때문에 완전 인증에 대응하는 안전한 인증 과정을 수행하게 된다.

[그림 2]는 무선 단말기의 핸드오프 시 인증과정을 나타낸다.



〔그림 2〕 핸드오프 시 인증 방법

무선 단말기는 서비스를 제공하고 있는 AP의 SNR (signal to noise ratio)값이 기준치 이하로 떨어지면 새로운 AP를 찾기 위하여 스캐닝을 시작하며 가장 큰 SNR을 갖는 AP를 선택한다. 이동할 AP를 결정한 후에는 무선 단말기와 이동할 AP간에 인증 과정이 수행된다. 이때 이동할 AP는 무선 단말기에 대한 인증 과정을 이전 AP를 통해서 수행하게 된다. 이전 AP와 이동할 AP는 이미 상호 인증을 수행한 신뢰할 수 있는 개체들이기 때문에 이전 AP가 수행한 무선 단말기에 대한 인증 결과를 이동할 AP도 신뢰할 수 있게 된다. 이때 무선 단말기는 이동할 AP와 인증 과정이 끝나기 전까지는 이전 AP와 세션을 계속 유지한다.

3.2 인증 절차

[그림 3]은 핸드오프 시 인증을 위한 기본 동작 과정을 나타낸 것이며, 교환되는 메시지를 살펴보면 다음과 같다.

① MS → newAP : Request_Reassociate

무선 단말기는 스캐닝을 통해서 이동할 AP를 선택한 후 Reassociate를 요청한다.

② newAP → MS : Response_Reassociate

핸드오프를 요청 받은 새로운 AP는 무선 단말기에게 인증 과정의 시작을 알린다.

③ newAP → MS : Request_oldAP_ID

무선 단말기의 핸드오프를 요청 받은 새로운 AP는 무선 단말기에게 기존 서비스를 제공하던 이전 AP 정보를 요청한다.

④ MS → newAP : Response_oldAP_ID

무선 단말기는 이전 AP 정보를 새로운 AP에게 전송한다.

⑤ newAP → oldAP : {newAP_ID, MS_ID, n1, {n1}K_{newAP-}}K_{oldAP+}

새로운 AP는 상호 인증을 통해 획득한 이전 AP의 공개키로 자신의 ID와 무선 단말기 ID, nonce를 암호화하여 이전 AP에게 전송한다. 새로운 AP는 nonce에 개인키로 암호화한 내용을 포함시킴으로서 송신자를 확인하게 한다.

⑥ oldAP -> newAP : {oldAP_ID, MS_ID, K_{MS+}, old WEPKey, n1+1}K_{newAP+}

이전 AP는 자신의 개인키로 암호문을 복호화 한 후, 자신에게 전송된 무선 단말기 ID를 통해 자신에게 인증받은 무선 단말기인지를 확인하고, 자신의 ID와 무선 단말기 ID, MS의 공개키, 사용중인 WEP Key 그리고 새로운 AP로부터 수신한 nonce 정보를 새로운 AP의 공개키로 암호화하여 전송한다.

⑦ newAP -> MS : (ACK, Failure) or (ACK, Success, {old WEPKey +1, K_{newAP+}, n2}K_{MS+})

새로운 AP는 자신의 개인키로 암호문을 복호화 한 후, 무선 단말기의 ID와 nonce 값을 확인한 후 무선 단말기에 대한 인증 과정을 성공적으로 마치게 되면, old WEPKey의 정보 및 새로운 AP의 공개키를 nonce와 함께 MS의 공개키로 암호화하여 전송한다.

⑧ MS -> newAP : {old WEPKey +2, n2+1}K_{newAP+}

MS는 기존의 AP사이에서 사용했던 WEPKey와 newAP로부터 받은 old WEPKey를 비교한다. MS는 old WEPkey의 정보를 통하여 새로운 AP가 기존의 AP로부터 인증을 받은 AP임을 확신하게 된다. 즉 MS는 기존의 AP를 통하여 새로운 AP를 인증 할 수 있게된다. 비교후 MS는 old WEPKey 및 nonce 정보를 새로운 AP의 공개키로 암호화하여 전송한다.

⑨ newAP -> MS : {new WEPKey, n2+2}K_{MS+}

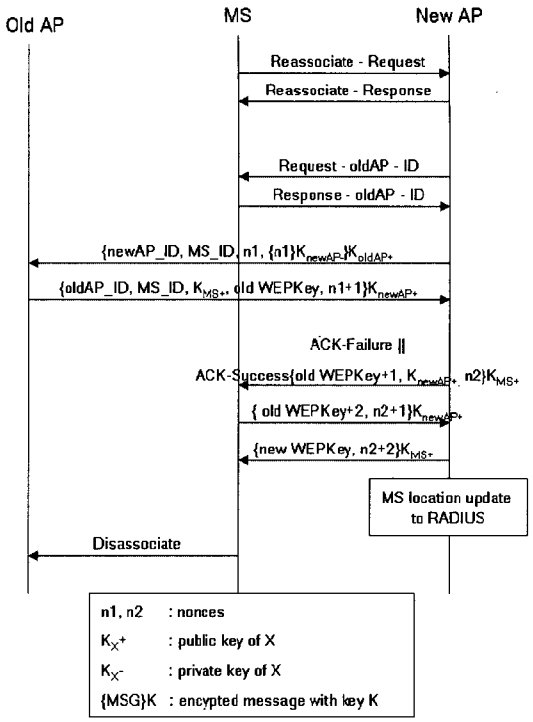
새로운 AP는 데이터 암호화에 사용할 새로운 세션키를 nonce 정보와 함께 무선 단말기의 공개키로 암호화하여 전송한다. Nonce 정보를 사용하는 것은 재전송 공격을 방지하기 위해서이다.

⑩ newAP -> RADIUS : MS_Location_Update

새로운 AP는 RADIUS 서버에게 무선 단말기의 갱신된 위치 정보를 통보하여 CRL 정보 변경시 메시지 전송 장소를 새로운 AP로 변경한다.

⑪ MS -> oldAP : Disassociate

무선 단말기는 이전의 AP와 세션을 종료한다.



〔그림 3〕 핸드오프시 인증절차

위의 절차에서 재전송 방지 및 메시지 유효성을 증명하기 위해 사용된 nonce는 본 논문의 경우 동기화된 클럭을 요구하는 시간 값이 아닌 일종의 one-time 키의 개념으로 사용된다. 즉 ⑤에서 newAP가 oldAP에게 전송한 n1의 응답으로 ⑥에서 n1의 확인과 새로운 nonce를 보내야 하는데, oldAP 입장에서 n1의 확인과 새로운 nonce를 대신하여 이를 개념적으로 결합한 n1+x을 보낸다. 이는 ⑦,⑧,⑨ 에서의 n2에게도 같이 적용된다. 또한 oldWEPKey가 아닌 oldWEPKey + x를 사용한 이유는 oldWEPKey의 수신뿐만 아니라 정상적인 키의 접근이 가능함을 나타내어 신뢰 정도를 증가시키기 위해서이다.

위의 과정 중 ⑤의 메시지는 새로운 AP가 이전 AP의 공개키를 이용하여 암호화 함으로써 이전 AP가 자신과 상호 인증을 수행한 AP인지 여부를 확인하게 된다. 그리고 ⑥의 메시지는 이전 AP가 새로운 AP의 공개키를 이용함으로써 새로운 AP가 자신과 상호 인증을 수행한 인증 된 AP인지를 확인하게 된다. ⑤,⑥의 메시지 교환을 통해서 기존에 맺은 두 AP간의 상호 인증 관계를 다시 한번 확인하게 된다. 그리고 ⑨의 메시지는 새로운 AP가 무선 단말기의 공개키로 세션키를 암호화하여 전송함으로써 핸드오

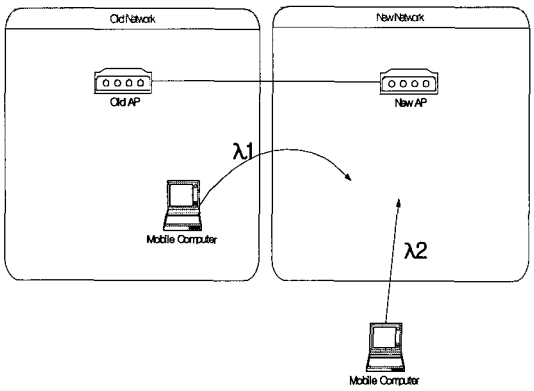
프를 수행하는 무선 단말기에게 안전하게 WEP 키를 전달할 수 있다.

Ⅳ. 성능 분석

본 절에서 제안된 인증 기법에 대한 성능 분석을 수행한다. 무선 서비스를 받기 위해 초기 인증을 요청하는 무선 단말기의 발생은 포아송 분포를 가지는 확률 변수로 모델화 할 수 있으며, 이때 인증이 완료될 때까지의 서비스 시간은 CRL 검색시간과 인증서 검증시간, 패킷 전송시간의 합으로 나타낼 수 있다. CRL 검색시간은 CRL 크기와 저장 위치에 따라 액세스 시간이 달라질 수 있고, 인증서 종류에 상관없이 인증서 검증시간과 패킷 전송시간이 동일하다고 가정한다. 그리고 핸드오프를 요청하는 무선 단말기의 발생도 역시 포아송 분포를 가진다고 가정한다. 핸드오프 시 인증 과정은 공개키를 이용하므로 인증처리에 일정한 시간이 소비된다고 가정한다[15].

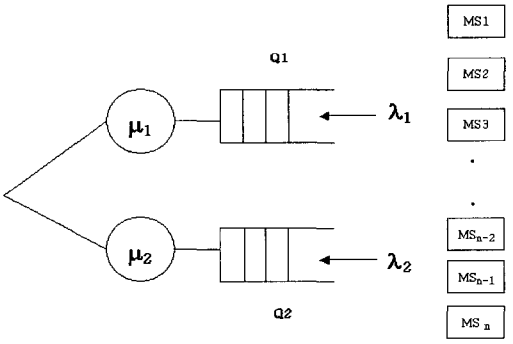
4.1 큐잉 모델

[그림 4]는 분석을 위한 환경을 나타낸 것이다. 그림에서 볼 수 있듯이 초기 인증을 요청하는 단말기가 λ_2의 도착률로 발생되고, 핸드오프를 요청하는 단말기는 λ_1의 도착률로 발생된다. 특정 AP에게 초기 인증을 요청하는 무선 단말기와 핸드오프를 요구하는 무선 단말기의 요청이 모두 존재하는 경우, AP는 우선 순위 큐잉에 의해서 핸드오프 시 인증 서비스를 우선적으로 수행하게 된다.



〔그림 4〕 분석을 위한 시나리오

[그림 4]에서 각 AP의 큐잉모델은 [그림 5]와 같이 Q1, Q2 두개의 큐로 구성된다. Q1은 Q2보다 높은 우선 순위를 가지는 큐로써 핸드오프 시 인증 서비스를 처리한다. 이때 처리시간은 deterministic 분포로 나타낼 수 있는 메시지의 암호화, 복호화 시간과 패킷 전송시간의 합으로 나타낼 수 있다. 이때 Q1에서의 도착율은 λ_1으로 나타낸다. Q2는 초기 로그인 과정의 인증 서비스를 처리하는 큐로써 처리시간은 exponential 분포로 표현할 수 있는 CRL 검색시간과 deterministic 분포로 표현할 수 있는 패킷 전송시간과 인증서 검증시간의 합으로 나타낸다. Q2에서의 도착율은 $\lambda 2$로 나타내며 Q2의 처리 순위는 Q1보다 낮은 우선 순위를 갖는다. Q1, Q2는 FIFO방식을 적용하며, Q2에서 초기 인증 서비스가 처리중인 경우에 핸드오프 요청이 발생하면 현재 처리 중인 초기 인증 서비스가 끝난 후에 핸드오프를 위한 인증 서비스를 수행하는 비 선점 방식이 적용된다.



〔그림 5〕 큐잉 모델

이와 같은 큐잉 모델에서 각 큐에서의 평균대기시간은 식(1)과 같이 표현할 수 있다[16].

$$E(W_k)=\frac{\sum_{i=1}^{2}\lambda_i E(P_i^2)}{2(1-\sum_{i=1}^{k-1}\rho_i)(1-\sum_{i=1}^{k}\rho_i)}\ (k=1,2) \qquad (1)$$

위의 식에서 W_1, W_2는 각각 Q1, Q2에서의 평균대기시간이고, P_1, P_2는 Q1, Q2에서 하나의 인증에 대하여 소요되는 처리시간을 나타내는 랜덤변수이다. ρ_1, ρ_2는 각각 초기 인증 및 핸드오프 시 인증으로 인한 서버의 utilization을 나타내는 변수로서 $\rho_1=\lambda_1 E(P_1)$, $\rho_2=\lambda_2 E(P_2)$의 값을 갖는다. 여기서 E(·)는 기대치를 나타낸다.

4.2 동작 과정 및 파라미터 적용

큐잉 모델에 적용되는 파라미터들은 다음과 같다.

- W_{ban} : 무선 네트워크의 대역폭으로서, 모든 무선 네트워크에서는 동일하다고 가정한다.
- L_{ban} : 유선 네트워크의 대역폭으로서, 모든 유선 네트워크에서는 동일하다고 가정한다.
- C_{ser} : 디렉토리 서버를 방문하여 CRL을 검색하는데 소요되는 처리시간으로 지수 분포를 따른다고 가정한다.
- V_{cer} : 인증서 필드를 검증하는데 소요되는 시간으로 각 호스트나 서버의 성능에 상관없이 동일하다고 가정한다.
- K_{enc} : 메시지 보호를 위한 암호화 작업의 처리율로 각 호스트나 서버의 성능에 상관없이 동일하다고 가정한다.
- K_{dec} : 암호화된 메시지에 대한 복호화 작업의 처리율로 각 호스트나 서버의 성능에 상관없이 동일하다고 가정한다.
- P_{siz} : 인증을 위해서 전송되는 메시지 크기를 나타내며 동일한 값을 갖는다.
- C_{siz} : 인증서 크기로써 인증서의 종류에 상관없이 동일한 값을 갖는다고 가정한다.

위의 파라미터를 이용하여 무선 네트워크를 통한 패킷 전송시간 (T_W)와 인증서 전송시간(T_C)는 다음과 같이 나타낼 수 있다.

$$T_w = \frac{P_{siz}}{W_{ban}}, \quad T_c = \frac{C_{siz}}{W_{ban}}$$

유선 네트워크를 통한 패킷 전송시간(T_L)은 다음과 같이 나타낼 수 있다.

$$T_L = \frac{P_{siz}}{L_{ban}}$$

메시지의 암호화 시간과(T_E) 복호화 시간은(T_D)은 다음과 같이 나타낼 수 있다.

$$T_E = \frac{P_{siz}}{K_{enc}}, \quad T_D = \frac{P_{siz}}{K_{dec}}$$

위에서 설명한 큐잉 파라미터들을 직접 규잉 모델에 적용하여 동작 과정을 설명하면 다음과 같다.

4.2.1 초기 인증 절차

무선 단말기가 무선 서비스를 받기 위하여 무선 네트워크(W_{ban})를 이용하여 AP에 인증서(C_{siz})를 전송하면 AP는 무선 단말기 인증을 위해서 유선 네트워크(L_{ban})를 통해 RADIUS 서버에게 인증서(C_{siz})를 전송한다. RADIUS 서버는 무선 단말기의 홈 디렉토리에서 CRL을 확인한 후(C_{ser}), 인증서를 검증한다(V_{cer}). RADIUS 서버가 AP에게 검증 완료를 통보하면(L_{ban}), AP는 무선 네트워크(W_{ban})를 이용하여 인증 확인 메시지(P_{siz})를 무선 단말기에게 전송하고 무선 네트워크 접속을 허용한다.

4.2.2 핸드오프 시 인증 절차 - 제안 구조

무선 단말기가 핸드오프를 위해 무선 네트워크(W_{ban})를 이용하여 인증 요청 메시지(P_{siz})를 AP에게 전송한다. 핸드오프를 요청 받은 AP가 무선 네트워크(W_{ban})를 이용하여 무선 단말기에게 서비스를 제공하던 이전 AP의 정보(P_{siz})를 요구하면 무선 단말기는 이전 AP의 정보(P_{siz})를 새로운 AP에게 알려준다. 새로운 AP가 이전 AP에게 유선 네트워크(L_{ban})를 이용하여 자신의 정보(P_{siz})를 공개키로 암호화(K_{enc})하여 전송하면, 이전 AP는 전송받은 암호화된 메시지(P_{siz})를 복호화(K_{dec})한 후 메시지 내용을 확인한다. 그리고 무선 단말기의 공개키를 담은 메시지(P_{siz})를 다시 암호화(K_{enc})하여 새로운 AP에게 전송한다. 무선 단말기가 이동할 새로운 AP는 암호화된 메시지(P_{siz})를 자신의 개인키로 복호화(K_{dec})하여 메시지를 확인한 후, 무선 네트워크(W_{ban})를 이용하여 인증 확인 메시지(P_{siz})를 무선 단말기에게 전송하고 무선 네트워크 접속을 허용한다. 본 제안절차에서는 초기 인증 절차보다 인증에 걸리는 오버헤드가 줄어들게 되는데, 이는 핸드오프 시 무선 단말기의 인증을 선행 된 유선 AP 간의 상호 인증으로 대신하기 때문이다. 즉 무선 단말기를 인증하기 위한 CRL 검색 과정의 오버헤드가 생략될 수 있으며, 유선 구간의 상호 인증이 무선 단말기의 CRL 검색 등 무선 구간의 상호 인증에 비해 빠른 속도로 수행되므로 무선 네트워크 성능에 향상을 제공하게 된다.

4.2.3 핸드오프 시 인증 절차 - 일반 구조

본 논문에서는 제안된 구조의 인증 절차의 성능 향상 정도를 비교하기 위해서 제안된 구조를 이용하지 않는 일반적인 방법으로서의 핸드오프 방법에 대하여서도 고려한다. 이 경우 핸드오프 시 인증 절차는 초기 인증 절차와 같은 과정을 갖게된다.

4.3 성능 분석

본 성능분석은 여러 환경에 적용할 수 있으며 그 결과를 핸드오프 기능이 있는 무선랜 설계시에 활용이 가능하다. 제안 방법의 성능 향상 정도를 알아보기 위하여 [표 2]와 같은 파라미터의 상황을 가정하였다. 특정 AP에 핸드오프를 요구하는 무선 단말기의 도착률은 λ_1이고, 초기 인증을 요구하는 무선 단말기의 도착률이 λ_2일때에 utilization 변화에 따른 핸드오프시 인증 대기시간을 알아보았다. 핸드오프 시에 무선 대역폭은 802.11의 2Mbps, 유선 대역폭은 10Mbps로 가정하였으며, 인증서 크기가 일반적으로 1~3KB인데, 본 경우에서는 1KB로 가정하였다. 공개키 암호/복호 처리 속도를 1.6Mbyte/s로 가정하였으며, 인증서 검증 시간을 32ms로 하였으며[17], 인증서 체인에 깊이는 고려하지 않았다. 마지막으로 CRL을 검색하는 시간을 각각 600ms와 900ms로 구분하여 분석하였다.

〔표 2〕 큐잉 파라미터

항 목	값
Vertification of certificate (Vcer)	32 ms
Check of CRL (Cser)	600ms,900ms
Encryption of public key (Kenc)	1.6MByte/s
Decryption of public key (Kdec)	1.6MByte/s
Request, Reponse packet size (Psiz)	1KB
Size of certificate (Csiz)	1KB
Wireless network_bandwidth (Wban)	2Mbps
Lan network_bandwidth (Lban)	10Mbps

식(1)을 이용하여 큐잉 모델에서 핸드오프 시 인증을 위한 인증 대기시간 $E(W_1)$을 구하면 다음과 같다.

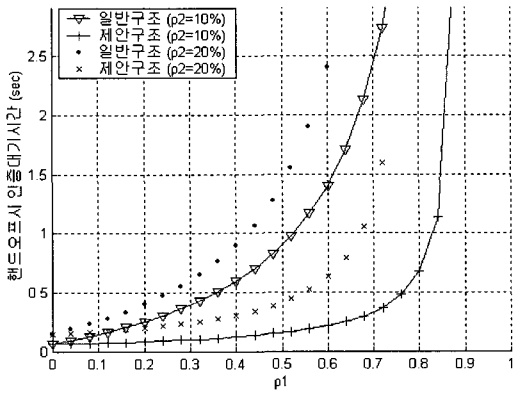
$$E(W_1)=\frac{\lambda_1 E(P_1^2)+\lambda_2 E(P_2^2)}{2(1-\rho_1)} \quad (2)$$

또한 초기 인증시 대기시간 $E(W_2)$을 구하면 다음과 같다.

$$E(W_2)=\frac{\lambda_1 E(P_1^2)+\lambda_2 E(P_2^2)}{2(1-\rho_1-\rho_2)(1-\rho_1)} \quad (3)$$

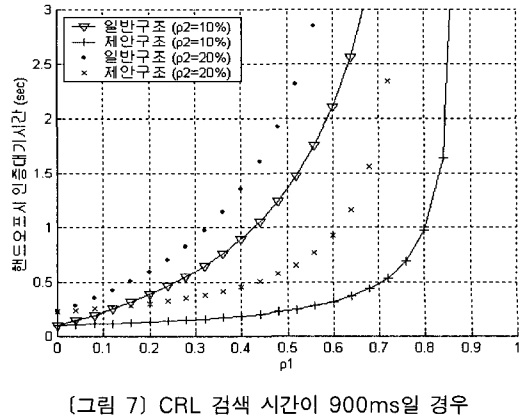
이때 핸드오프 시 인증을 처리하는 Q1의 이용률이 ρ_1, 초기 인증을 처리하는 Q2의 이용률이 ρ_2이므로, 전체 큐의 이용률 ρ는 $\rho=\rho_1+\rho_2<1$의 관계를 갖는다.

[그림 6]은 CRL 검색에 600ms가 소요되는 경우이다. AP의 초기 인증 과정을 처리하는 ρ_2의 비율이 각각 10%, 20%를 차지할 경우에 핸드오프 시 인증 서비스를 수행하는 ρ_1의 비율을 변화시켜 가면서 핸드오프 시 인증 대기시간을 구하였다.



〔그림 6〕 CRL 검색 시간이 600ms일 경우

[그림 7]은 CRL 검색에 900ms가 소요되는 경우이다. AP의 초기 인증 과정을 처리하는 ρ_2의 비율이 각각 10%, 20%를 차지할 경우에 핸드오프 시 인증 서비스를 수행하는 ρ_1의 비율을 변화시켜 가면서 핸드오프 시 인증 대기시간을 구하였다. [그림 6,7]에서 볼 수 있듯이 초기 인증 과정 처리 시간이 일정할 경우 제안 구조의 핸드오프 인증 서비스 대기 시간이 일반 구조의 경우에 비해 작음을 알 수 있다. 또한 CRL 검색 시간이 클수록 성능 향상 정도가 더욱 확연해 짐을 알 수가 있다. 즉 가입자가 많은 경우, CRL 사이즈가 커지게 되므로 본 논문에서의 제안구조가 더욱 유용하게 된다.



〔그림 7〕 CRL 검색 시간이 900ms일 경우

ρ_2=10%일 경우, CRL 검색시간에 따른 일반구조와 제안구조에서의 핸드오프 시 인증 대기시간은 [표 3]와 같다.

〔표 3〕 핸드오프 시 인증 대기시간 측정

ρ_1	20%	40%	60%	80%
일반구조(초)	0.2575	0.6008	1.4020	5.4076
제안구조(초)	0.0886	0.1280	0.2199	0.6792

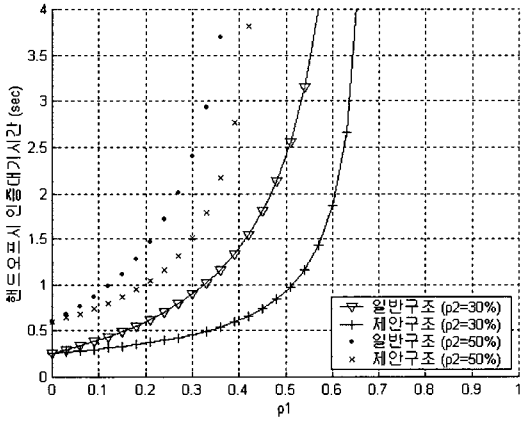
(a) CRL search time = 600ms

ρ_1	20%	40%	60%	80%
일반구조(초)	0.3860	0.9006	2.1013	8.1052
제안구조(초)	0.1315	0.1880	0.3198	0.9789

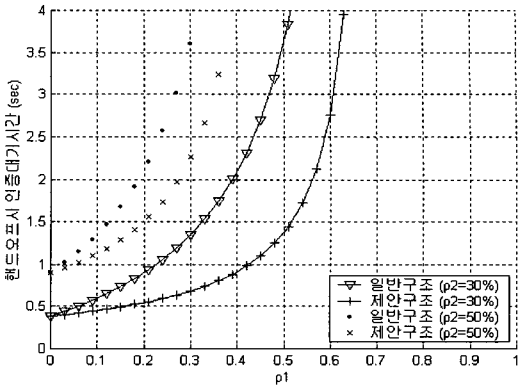
(b) CRL search time = 900ms

핸드오프 시 인증 대기시간을 살펴보면 기존방법의 경우에는 CRL 검색시간이 증가함에 따라 인증 대기시간도 크게 증가함을 알 수 있다. 그러나 제안된 핸드오프 방식을 사용하였을 경우에는 CRL을 직접 검색하지 않기 때문에 CRL 검색시간 변화에 별다른 영향을 받지 않음을 알 수 있다. 또한 핸드오프 요청이 증가할수록 기존 방법과 제안한 방법의 인증 대기 시간 차이가 점차 커짐을 알 수 있다.

[그림 8]과 [그림 9]는 초기 인증 서비스를 수행하는 ρ_2가 각각 30%, 50%를 차지하고 있을 경우에 CRL 검색시간에 따른 핸드오프 시 인증 대기시간을 나타낸다.



〔그림 8〕 CRL 검색 시간이 600ms일 경우



〔그림 9〕 CRL 검색 시간이 900ms일 경우

V. 결 론

무선랜은 특성상 사용자 이동이 빈번하게 발생하며, 핸드오프 시마다 완전 인증(full authentication)을 수행하기 때문에 많은 오버헤드를 야기 시킨다. 따라서 핸드오프 시 효율적인 무선 서비스를 제공하기 위해서는 사용자 등록 지연을 최소화 할 수 있는 빠른 인증 메커니즘이 필요하다. 이를 위해 본 논문에서는 무선랜의 사용자 인증을 위해 PKI기반의 방법을 고려하였으며, 그 경우에 필수적으로 사용되는 인증서에 대한 CRL 검색과 검증 과정을 최소화함으로서, 효율적인 무선 인터넷 서비스를 제공하기 위한 빠른 핸드오프를 지원하는 인증 기법을 제안하였다. 또한 제안된 기법에 대한 성능분석을 수행하였다. 성능 분석 결과 본 논문에서 제안한 인증 기법은 CRL 크기에 상관없이 동일한 인증 처리 시간을 가지므로 무선 인터넷 사용자 증가에 따른 CRL 크기의 증가에 영향을 받지 않게 되어 보다 안정적인 무선 서비스 제공이 가능함을 알 수 있었다. 제안한 인증 기법에 대한 성능분석결과는 제안된 방법이 필드에 적용될 경우 최적의 시스템 구성을 위한 자료로서 유용하게 이용될 것으로 기대된다.

참 고 문 헌

[1] IEEE Standards for Wireless LAN Media Access Control(MAC) and Physical Layer(PHY) Specification, IEEE 802.11, 1999 Edition, 1999.

[2] S. Rommer, "Security issues in Public access WLAN architectures", IEEE802.11-02/250, March, 2002.

[3] T. Moore, B. Aboba, "Authenticated Fast Handoff",

IEEE802.11-01/TBD, November, 2001.
[4] G. Chesson, J. Walker, "Authenticated Key Exchange", IEEE802.11-00/573a, November, 2001.
[5] W. A. Arbaugh, "Your 802.11 Wireless Network has No Clothes", University of Maryland, http://www.cs.umd.edu/~waa/wireless.pdf, March, 2001.
[6] J. Caron, "Public Wireless LAN roaming issues", IInternet-Draft, draft-caron-public-wlan-roaming-issues-00.txt, November, 2001.
[7] C. Rigney, "Remote Authentication Dial In User Service(RADIUS)", IETF RFC 2865, June, 2000.
[8] "Standard for Port Based Network Access Control", IEEE Draft P802.1X/D11, March, 2001.
[9] L. Blunk "PPP Extensible Authentication Protocol(EAP)", IETF RFC 2284, March, 1998.
[10] A. Mishra, M. Shin, W. Arbaugh, "An Empirical Analysis of the IEEE 802.11 MAC Layer Handoff Procee",
[11] S.Pack, Y. Choi, "Pre-Authenticated Fast Handoff in a Public Wireless LAN Based on IEEE802.x Model", IFIP TC6 Personal wirless Communication 2002, October 2002
[12] A. Mishra, M. Shin, W. Arbaugh, "Proactive Caching Strategies for IAPP Latency Improvement during 802.11 Handoff", IEEE 802.11-TBD, http://www.ieee802.org/11/Documents/DocumentHolder/3-084.zip, November, 2002.
[13] B. Aboba, "IEEE 802.1X Pre-Authentication", IEEE 802.11-02/389, http://www.drizzle. com/~aboba/IEEE/11-02-TBDr0-I-Pre-Authentication.doc, June, 2002.
[14] J. Walker, "Overview of 802.11 Security", IEEE, IEEE802.15-01/154, March, 2001.
[15] L. Kleinrock, *Queueing System volume 1, Wiley-Interscience*, pp.89~108, 1975.
[16] T. Hideaki, *Queueing analysis : a foundation of performance evaluation*, North-Holland, pp.160~165, 1991.
[17] 구자범, 김관연, 이재일, 박세현, "차세대 이동통신을 위한 PKI 기반의 이동 보안 구조 연구", 정보과학회지 제20권 제 4호, pp.21~32, April 2002.

〈著者紹介〉

정 종 민 (Jong-Min Jeong) 정회원
1998년 2월 : 강원대학교 정보통신공학과 졸업
2000년 2월 : 강원대학교 정보통신공학과 석사
2000년 3월~현재 : 강원대학교 정보통신공학과 박사과정
<관심 분야 > 이동통신보안, 무선랜 보안

이 주 남 (Ju-Nam Lee) 학생회원
2001년 2월 : 강원대학교 정보통신공학과 졸업
2003년 2월 : 강원대학교 정보통신공학과 석사
2003년 3월~현재 : 서울 통신 기술
<관심분야> 이동통신보안, 무선랜 보안

이 구 연 (Goo-Yeon Lee) 정회원
1986년 2월 : 서울대학교 전자공학과(학사)
1988년 2월 : KAIST 전기및전자공학과(석사)
1993년 2월 : KAIST 전기및전자공학과(박사)
1993년~1996년 : 디지콤정보통신연구소
1996년~1997년 : 삼성전자
1997년~현재 : 강원대학교 전기전자정보통신공학부 부교수
<관심분야> 이동통신, 초고속 통신, 데이터 통신, 보안