[UCI]I804:24011-200000234012

2007년 2월
석사학위논문

무선 LAN에서 핸드오프시 PKI 방식을 이용한 실시간 상호 인증기법 설계

조선대학교대학원
정보통신공학과
신 승 욱

무선 LAN에서 핸드오프시 PKI 방식을 이용한 실시간 상호 인증기법 설계

Design of a Realtime Interactive Authentication Method using PKI during Handoff Time in the Wireless Network

2007년 2월 23일

조선대학교대학원
정보통신공학과
신 승 욱

무선 LAN에서 핸드오프시 PKI 방식을 이용한 실시간 상호 인증기법 설계

지도교수 한 승 조

이 논문을 공학석사학위신청 논문으로 제출함.

2006년 10월

조선대학교대학원
정보통신공학과
신 승 욱

신승욱의 석사학위 논문을 인준함

위원장 조선대학교 교수 박 종 안 인

위 원 조선대학교 교수 한 승 조 인

위 원 조선대학교 교수 변 재 영 인

2006년 11월

조선대학교 대학원

목 차

도목차 ····· iii

표목차 ····· iv

ABSTRACT ····· v

제*1*장 서 론 ····· *1*

제*2*장 무선 *LAN* 보안 구조 ····· *3*

제1절 무선 LAN 시스템 보안 개요 ····· 3

1. 무선 LAN 시스템의 동작절차 ····· 3
2. 단말과 AP 사이의 보안 ····· 4
3. AP와 인증 서버 사이의 보안 ····· 7
4. IEEE 802.11b 보안의 취약점 ····· 7

제2절 IEEE 무선랜 보안 프레임워크 ····· 8

1. 802.1x 특징 ····· 8
2. 802.1x의 동작 원리 ····· 9
3. EAP Over LAN의 프레임 형식 ····· 10
4. 802.1x 프로토콜의 동작 ····· 12

제3절 EAP 인증 유형 ····· 14

1. EAP-MD5 ····· 14
2. LEAP(Lightweight EAP) ····· 15
3. EAP-TLS(Transport Layer Security) ····· 16

4. EAP-TTLS, PEAP ····· 18
제4절 인증서 검증 방법 ····· 20
1. CRL 이용 방식 ····· 20
2. OCSP 서버 이용 방식 ····· 22

제3장 무선 LAN 보안 시스템 설계 ····· 24
제1절 기존 인증 유형의 문제점 분석 ····· 24
제2절 기존 인증서 검증 방법의 문제점 분석 ····· 26
제2절 실시간 무선 LAN 보안 시스템 설계 ····· 28
1. 제안 시스템의 기본 조건 ····· 28
2. 제안 시스템의 설계 목적 ····· 28
3 제안 시스템의 구성 ····· 29
4 제안 시스템의 인증 절차 ····· 33

제4장 무선 LAN 보안 시스템 시뮬레이션 및 분석 ····· 35
제1절 제안 시스템의 인증 관련 분석 ····· 35
제2절 안전성과 효율성 분석 ····· 36
제3절 시뮬레이션 구현과 성능 분석 ····· 38

제5장 결론 ····· 47

참고 문헌 ····· 48

도 목 차

그림 1 기본적인 무선 LAN의 동작 절차 ····· 4
그림 2 WEP된 MPDU의 형식 ····· 5
그림 3 WEP 암호 및 복호 절차 ····· 6
그림 4 무선 LAN의 포트 기반 네트워크 접속 위상도 ····· 9
그림 5 802.1x 구성요소의 동작원리 ····· 10
그림 6 802.1x 시스템의 구성과 동작 ····· 12
그림 7 EAP-MD5 인증 방식의 문제점 ····· 15
그림 8 TLS 기반의 상호 인증 방식 ····· 16
그림 9 EAP-TLS 인증절차 ····· 17
그림 10 TLS 터널기반의 EAP 인증절차(EAP-TTLS, PEAP의 경우) ····· 19
그림 11 클라이언트의 사전 등록 절차 ····· 31
그림 12 제안 시스템의 인증절차 ····· 33
그림 13 제안 시스템 시뮬레이션 구성도 ····· 39
그림 14 EAP-TLS 시뮬레이션 구성도 ····· 40
그림 15 EAP-TLS 각 단계별 응답시간 ····· 41
그림 16 제안 시스템 각 단계별 응답시간 ····· 42
그림 17 EAP-TLS 각 단계별 시뮬레이션 결과 ····· 43
그림 18 제안 시스템 각 단계별 시뮬레이션 결과 ····· 43
그림 19 제안 시스템과 EAP-TLS의 인증 응답시간 ····· 44
그림 20 제안 시스템과 EAP-TLS의 시뮬레이션 결과 ····· 45

표 목 차

표 1 IEEE 802.11b에서의 암호 및 인증 방식 ····· 5
표 2 EAPoL 프레임 형식 ····· 10
표 3 EAP-MD5 인증 특성 ····· 25
표 4 EAP-TLS 인증 특성 ····· 25
표 5 EAP-TTLS, PEAP 인증 특성 ····· 26
표 6 CRL 인증서 검증 방법의 특성 ····· 27
표 7 OCSP 인증서 검증 방법의 특성 ····· 28
표 8 제안 시스템과 기존 인증 기능 분석 ····· 35
표 9 전송 내용 안전성 분석 ····· 36
표 10 구간별 핸드쉐이크 횟수 ····· 37

ABSTRACT

Design of a Realtime Interactive Authentication Method using PKI during Handoff Time in the Wireless Network

Shin, Seung-Wook
Advisor: Prof. Han, Seung-Jo, Ph.D.
Department of Information Communications,
Graduate School of Chosun University

There were many exposed problems in previous authentication method on LAN. Especially Open System Authentication Method, Shared Key Method, Mac Based Authentication Method are very hard to use in wireless network that needs security.

So now, many researches have been performed about 802.1x and user authentication method applying PKI. But certificate verification protocol has been used abolished list called CRL since it's first usage of PKI, there were still has a problem about distribution point.

In this paper, I applied CVS to use CA direct not to use CRL and OSCP server in order to improve this problems. Also I suggested the system that can make authentication steps more shorter using authentication server and

interactive authentication system by public certificate(small size/low speed wireless terminal can access to wireless network fast and safely) , analyzed the performance using Opnet Simulator 11.0.

제1장 서 론

무선 LAN은 매력적인 이동성과 유선 LAN에 근접한 속도를 지원하면서 개인 또는 기업의 사용자들에게 빌딩이나 캠퍼스 환경에서 전자상거래, 전자 메일, 데이터 전송과 같은 중요한 정보를 비밀리에 전달하고자 하는 보안성 요구가 더욱 증가하고 있다. 이는 무선매체의 공개성(Openness)에 따른 해킹의 용이성과, 단말의 이동에 따른 보안 체계의 복잡성에 기인한다. 따라서 최근 무선 LAN 기술에 있어서 보안성이 가장 중요한 영역으로 자리잡고 있다[1].

무선 LAN은 전파라는 전송매체를 사용함으로써 매체의 특성상 보안에 대한 취약성을 내포하고 있다. 물리적으로 접근이 어려운 유선과는 달리 무선 구간은 접근이 용이하므로 데이터를 암호화 함으로써 기밀성을 유지하고 인증 된 사용자에게만 네트워크 접속을 허용해야한다[2]. IEEE 802.11b에서는 이러한 사용자 인증 및 기밀성을 위하여 SSID(Service Set Identifier), MAC(Media Access Control) 주소, 그리고 WEP(Wired Equivalent Privacy)키를 이용하고 있다[3]. 하지만 IEEE 802.11b 보안 메커니즘에는 이미 많은 취약점들이 알려져 있다[4]. 이러한 취약점들을 보완하고자 고안된 것이 IEEE 802.1x EAP(Extensible Authentication Protocol)이다[5]. 여기서는 네트워크에 접속을 허용하기위해 여러 가지 인증유형들을 제공하고 있으며, 이러한 인증유형들에는 EAP-MD5, EAP-TLS, EAP-TTLS등이 대표적이지만, 이 또한 상호 인증과 실시간 인증에 있어서 문제점을 가지고 있다.

이와 더불어 최근 인터넷 환경에서 제공되는 응용서비스에 암호화 기술을 이용한 보안시스템이 많이 등장하고 있다. 현재 보안 기능을 일관성 있게 제공해 주는 기술로 PKI(public key infrastructure)를 들 수 있다. PKI를 이용한 서비스들은 서로 통신하는 상대방을 인증하거나 또는 향후 거래 사실의 부인을 방지하기 위하여 인증기관(CA : Certification Authority)에서 발급한 인증서를 이용하는데 사용자는 수신한 인증서를 이용하기 전에는 반드시 인증서의 진위를 검증해야 한다. 인증서

소유자가 인증서를 분실하였거나 인증서의 비밀키를 잊어버렸을 경우 등의 이유로 인증서 유효기간 내에 CA에게 인증서 폐지신청을 할 수도 있기 때문에 반드시 인증서를 발급한 CA에게 인증서 폐지신청을 할 수도 있기 때문에 반드시 인증서를 발급한 CA에게 문의하여 인증서의 진위를 검증해야 한다. 그 동안 주로 이용되고 있는 인증서 검증 방법에는 인증서를 발급한 CA로부터 인증서 폐지목록(CRL : Certificate Revocation List)을 다운로드 하여 자신이 직접 검증하는 방법과 인증서 검증을 대신해주는 온라인 인증서 상태 검증 프로토콜(OCSP : Online Certificate Status Protocol) 서버를 이용하는 방법이 있다[6, 7].

이러한 무선 LAN을 이용하려는 클라이언트는 인증서버가 필요하며 인증서버의 인증서를 검증하기 위하여 네트워크로부터 CRL을 전송받거나 OCSP와 같은 인증서 검증서버에 접속해야 하는데 포트기반 접근제어방식을 이용하는 IEEE 802.1x에서는 클라이언트가 인증서버로부터 인증을 받기 전에는 인증서버 외의 네트워크 자원에 접속할 수 없다. 따라서 클라이언트가 인증서버를 실시간으로 인증할 수 없는 문제가 발생한다.

본 논문에서는 IEEE 802.1x기반의 EAP 인증의 문제점인 상호 인증과 실시간 인증의 문제점을 해결하고, 인증서의 유효성 검증을 빠르고 정확히 할 수 있으며 특정 검증 서버에 부하를 집중시키지 않음으로써 검증시스템의 안정화를 이룰 수 있는 보안 시스템을 설계하고자 한다.

제2장 무선 LAN 보안 구조

제1절 무선 LAN 시스템 보안 개요

1. 무선 LAN 시스템의 동작절차

가. 탐색과정

- AP : 자신에 접속하려는 단말들을 위하여, 자신이 지원할 수 있는 여러 가지의 능력(속도, 암호화등)과 이 AP가 속한 서비스 그룹명인 SSID(Service Set ID)등이 수납된 비컨 메시지를 주기적으로 방송한다.
- 단말 : 각 단말은 먼저 자신의 주변에 어떤 AP가 있는지 탐색하는 과정을 수행한다. 이를 위하여, AP가 전송하는 비컨 메시지를 수동적으로 수신하여 해당 AP의 지원능력이나 SSID를 알게 된다.

나. 인증과정

위의 탐색과정에 의해 적절한 AP를 선택한 단말은 해당 AP에 대하여 자신이 유효한 단말임을 증명하는 인증절차를 수행한다.

다. 결합과정

인증이 성공하면 무선 단말이 AP에 접속하는 과정인 결합(association)과정을 수행한다.

라. 데이터 전송과정

결합과정 이후, 데이터 메시지는 AP를 경유하여 인터넷에 접속하여 서비스를 받을 수 있다.

이러한 이동 무선인터넷 기술 중에서 이동성은 적지만 빠른 전송 속도와 나은 대역폭을 가능케 하는 무선 LAN은 제반 기술의 향상과 장치의 급속한 보급이 이루

어 졌다. 무선 LAN의 대표적인 기술에는 IEEE를 중심으로 하는 802.11과 유럽의 ETSI(European Telecommunications Standards Institute)를 중심으로 하는 HIPERLAN이 있는데, 본 논문에서는 현재 가장 보편화되고 있는 기술인 IEEE 802.11b 기술을 중심으로 무선 LAN 보안 기술을 다룰 것이다[8].

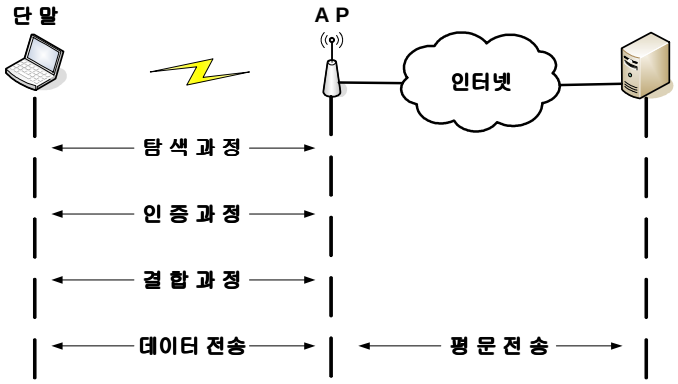


그림 1. 기본적인 무선 LAN의 동작절차

2. 단말과 AP 사이의 보안

현재 널리 보급되어 사용중인 IEEE 802.11b 표준은 무선랜의 인증과 비밀성을 제공하는 두 가지 메커니즘, SSID와 WEP을 정의 하고있다[2]. SSID는 무선랜 서브 시스템에서 장비의 네트워크 이름을 지칭하는 것으로써 초보 수준의 접속 제어를 제공한다. 유선랜과 무선 단말을 연결해 주는 장치인 AP(Access Point)는 자신이 주기적으로 보내는 비콘신호에 SSID를 포함하여 브로드캐스팅한다. 따라서 SSID를 이용해서 네트워크 접속의 허용/불가를 결정하는 것은 매우 위험하다.

WEP은 IEEE 802.11b 무선 LAN 데이터 스트림의 보안성을 제공하기 위하여 정의한 암호화 스킴으로써, 데이터의 암호화와 복호화가 동일키와 알고리즘을 사용하는 대칭형 구조이다. 올바른 WEP키를 소유한 사용자만이 네트워크에 접속하도록 허가하고, 데이터 스트림을 복호화할 수 있도록 하는 접속 제어와 비밀성 보장이 WEP의 사용 목적이다.

IEEE 802.11b 표준에서는 표 1과 같이 개방 인증 방식(Open system)과 공유키 인증방식(Shared Key system)이라는 두 가지의 인증 형태를 정의하였다.

표 1. IEEE 802.11b에서의 암호 및 인증 방식

	암 호 방 식	인 증 방 식
IEEE 802.11b	WEP - 40 WEP - 104	Open System Shared Key (RC4 암호방식 사용)

개방 인증 방식은 어떤 단말이라도 AP를 경유하여 인터넷을 사용할 수 있는 단말에 대한 실질적인 인증을 하지 않는다. 즉, 전체 인증과정이 평문으로 이루어지는 방식으로, 단말은 WEP키를 가지고 있지 않아도 AP로의 연결이 가능하다. 공유키 인증방식에서는 AP가 시도 패킷을 단말에게 보내면 단말은 이를 WEP키로 암호화하여 AP로 응답한다. 만일 단말이 키를 가지고 있지 않거나, 키가 맞지 않으면 인증은 실패하여 연결이 허용되지 않는다. 하지만 위 표 1에서 보듯이 인증 방식과 암호 방식은 별개로 설정될 수 있다. 개방 인증 방식을 사용하더라도 데이터 암호화는 IEEE 802.11b에서 지원하는 암호 방식을 사용가능하다.

데이터 기밀성은 WEP을 이용해 제공되는데 WEP 암호 방식은 무선 구간에서 전송되는 MAC프레임들을 40bit 길이의 WEP 공유 비밀 키와 임의로 선택되는 24bit의 IV(Initialization Vetor)로 조합된 총 64bit의 키를 이용한 RC4 스트림 암호 방식이다.

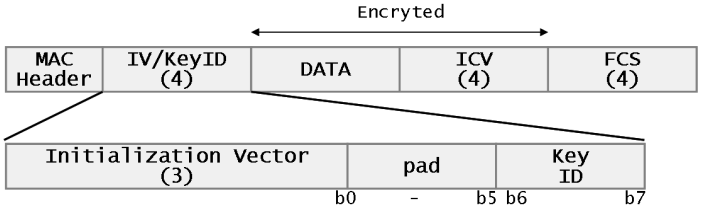
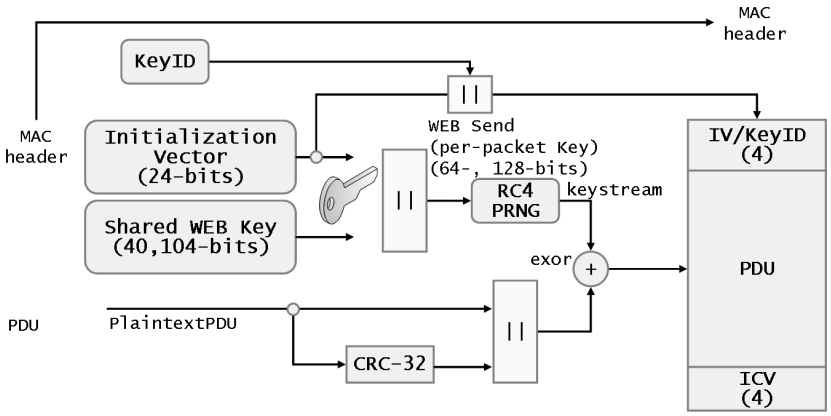


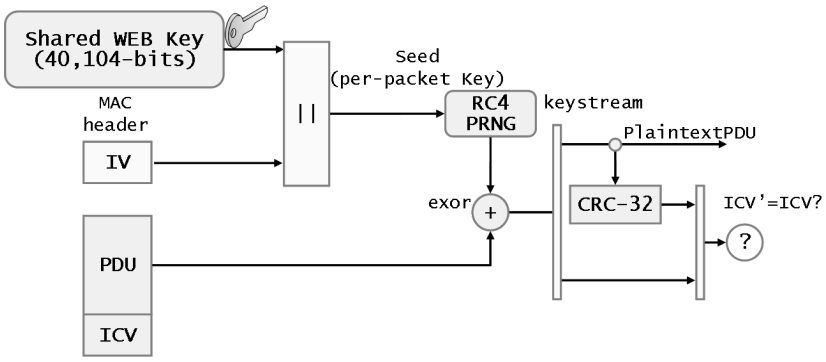
그림 2. WEP된 MPDU의 형식

AP는 단말을 인증하기 위해 random challenge를 보내면, 단말은 40bit의 암호키와

24bit의 IV를 결합하여 이를 RC4 PRNG 암호화 알고리즘에 입력시켜 의사 난수 키 스트림을 생성하고, 이를 이용해 평문을 암호화하여 전송한다. AP는 이를 복호화 하여 단말을 인증한다[2].



(a) 암호 과정



(b) 복호 과정

그림 3. WEP 암호 및 복호 절차

3. AP와 인증 서버 사이의 보안

RADIUS(Remote Authentication Dial-In User Service)는 NAS(Network Access server)와 인증 서버사이에 인증, 서비스 허가, 과금에 관한 정보 전달을 위한 프로토콜로써, 유선 환경에서 로밍 PPP(Point to Point Protocol) 사용자를 인증하기 위한 AAA(Authentication, Authorization, Accounting) 프레임워크로 제안되었다[9]. 이는 곳곳에 분산된 NAS를 통하여 서비스에 접속하려는 사용자들을 하나의 데이터 베이스에 통합적이고 효율적으로 관리할 수 있는 이점이 있다. 마찬가지로 무선 LAN에서도 서비스를 원하는 사용자 수가 증가하고 각 사업자들의 AP가 여기 저기 존재함에 따라 사용자 정보의 통합적인 관리와 사업자들간에 능동적인 정보 교환이 필요하다. RADIUS 서버는 사용자의 연결 요구에 대해 사용자 인증을 해주고, AP는 인증받은 사용자에게 허가된 서비스를 제공한다.

4. IEEE 802.11b 보안의 취약점

IEEE 802.11b 표준에서 사용자 인증은 MAC(Media Access Control) 주소를 이용하여 암호화되지 않은 상태로 수행된다. 각 AP는 인가된 단말의 MAC주소 리스트를 가지고 있고 접속을 요청하는 단말의 MAC 주소를 자신의 리스트와 검사하여 유효한 사용자인지를 판별한다. 하지만 이와 같은 MAC 주소 인증 방식에서 누군가 네트워크를 도청하고 있다면 브로드캐스트되는 MAC주소를 금방 알아챌 수 있다. 기존의 무선 LAN은 보안 문제뿐만 아니라 확장성에도 문제가 있다. 사용자 장치의 MAC주소는 무선 LAN의 각 AP에 저장되어 있어야 하는데 이는 관리상의 불편함이 있을 뿐만 아니라, 만일 관리상의 실수가 생긴다면 심각한 보안 사고를 초래할 수 있다[10].

WEP은 원래 유선랜과 같은 수준의 보안성을 제공하고자 만들어졌으나 근래 여러 보고서에 의하면 WEP 프로토콜은 크랙이 쉽고 무선 데이터 정보 전송시 위험성이 심각하다고 알려져 있다[4]. WEP 알고리즘은 암호키가 상수이고 IV가 너무 작다. 24bit 길이의 IV는 재사용이 가능해서 동일한 의사 난수 키 스트림(Key Sequence)을 생성시키기 쉽다. 따라서 IV의 크기가 작은 점을 이용하여 <IV, 키 스트림>을 저장

한 실시간 공격 가능성이 많은 것도 WEP의 단점이 된다[4, 10].

제2절 IEEE 무선랜 보안 프레임워크

IEEE 802 무선 LAN 기반구조 관리에서 서비스 허가를 얻은 사용자와 올바른 장치에게만 서비스를 제공하는 서비스 제약이 필요하게 되엇다. 802.1x란 임의의 사용자가 네트워크에 접근할 때 접근 포트에서부터 인증을 실시하고자 하는 포트 기반 네트워크 접속제어(Port based Network Access Control) 구조이다[11]. 이는 점대점 연결 특성을 가진 랜 포트에 연결된 인증된 장치에게만 서비스를 제공하기 위해 IEEE 802 무선 LAN 기반구조의 물리층 접속 특성을 이용한다. 여기서 포트란 랜 기반 구조에 부착되는 단일 접속점으로써 서비스를 제공하거나 받을 수 있는 수단으로써 MAC 브릿지의 포트, 네트워크 인터페이스카드 등이 있다.

1. 802.1x의 특징

기존 무선 LAN 시스템에서는 단말들이 Open System 또는 공유키를 사용한 인증절차에 의해 AP에 연결되고, 필요에 따라서 WEP 방식의 데이터 암호화에 의해 프레임들을 보호한다.

하지만, 이러한 인증절차 및 암호화 방법은 하나의 AP에 접속하는 모든 단말들이 WEP 공유 키를 공유하기 때문에 보안에 취약한 문제가 있다. WEP 키는 해당 단말 시스템에 대한 키 일뿐 이 단말을 사용하는 사용자에 대한 인증 및 데이터 암호용이 아니다. 또한, 단말마다의 계정관리, 과금처리 등의 부가 기능이 지원되지 못한다.

IEEE 802.1x는 유선 PPP망에서 사용되고 있던 인증용 프로토콜인 EAP를 유무선 LAN에 활용한 표준이며, 이것은 EAP 메시지를 PPP 프레임 대신에 수납할 수 있는 EAPoL(EAP over LAN) 프레임 형식과 절차를 정의하고, 사용자별로 브리지 또는 무선 엑세스 포인트의 물리적인 포트의 사용권을 외부의 인증서버로부터 획득해야만 해당 사용자의 망 접근을 허용하는 절차에 대한 규정으로써, 포트 접근제어 프로토콜이라 한다. 이렇듯 포트별로 인증절차를 수행하도록 한 경우에는 단말이 아닌, 사용

자별로 개별적인 과금정책이나, 사용제한, 대역할당, 필요시 WEP 키 변경 등을 제공할 수 있는 장점이 있다.

포트 기반 접속 제어의 동작을 기술하는 측면에서 시스템의 포트는 접속 제어 작용에서 두 가지 역할로 구분할 수 있다. 시스템의 서비스를 제공받으려는 Supplicant와 해당 포트로의 접속을 허용하기 전에 인증 절차를 수행하려는 Authenticator이다. Supplicant의 인증을 수행하기 위하여 Authentication Server를 이용하는데 현재 많이 사용되고 있는 Authentication Server는 RADIUS가 있다.

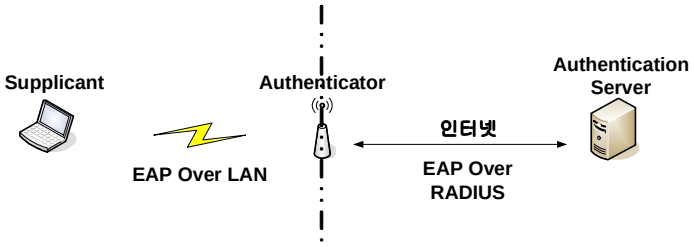


그림 4. 무선 LAN의 포트 기반 네트워크 접속 위상도

2. 802.1x의 동작 원리

포트 기반 네트워크 접속 제어를 이용하면 랜 접근에 대한 두 개의 구별된 지점을 만들어 내는 효과가 있다. Controlled Port는 포트가 인증 상태에 있을때에만 PDU(Protocol Data Unit)들의 교환을 허용하고, Uncontrolled Port는 인증 상태에 상관없이 PDU들의 교환을 허용한다. Controlled Port에서는 Authorized와 Unauthorized의 두 가지 상태를 이용하여 PDU들의 흐름을 제어한다.

그림 4는 Authenticator, Supplicant, Authentication Server사이의 관계와 그들 사이의 정보교환을 보여준다. Authenticator System은 Uncontrolled Port를 이용하여 Supplicant System과 Authentication Server System 사이에 인증을 수행하고, 인증에 성공했을 경우에 Controlled Port를 인가하여 서비스를 제공한다. 이와 같이 포트 기반 네트워크 접속 제어는 Controlled Port를 조직함으로써 인증된 사용자만이 서비스에 접속할 수 있도록 하는 인증 메커니즘이다.

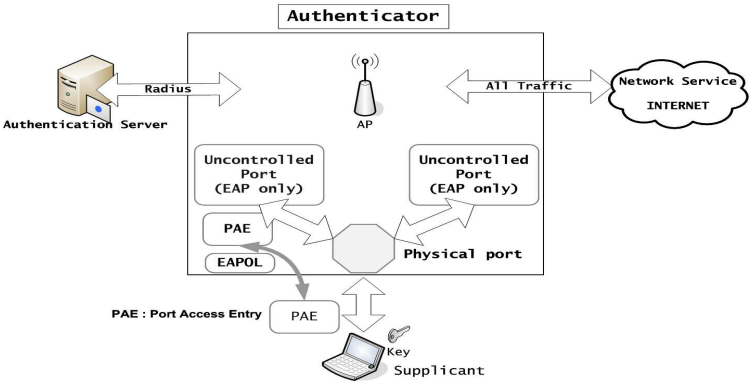


그림 5. 802.1x 구성요소의 동작원리

3. EAP Over LAN의 프레임 형식

802.1x에서 규정한 EAPoL 프레임은 단말과 AP간에 EAP패킷을 이더넷이나 무선 LAN상에서 수납하는 것으로써 프레임 구조는 표 2와 같다.

표 2. EAPoL 프레임 형식

	MAC/토큰링/FDDI MAC	
	LLC	3
	SNAP (PID = 0X888e)	5
EAPoL	Protocol Version = 1	1
	Packet Type = (0,1,2,3,4)	1
	Body Length	1
EAP	Body = EAP message	n

- Protocol Version : 1
- Packet Type : EAPoL 패킷 형식을 지시한다.
  - 0X00 : EAP-Packet
  - 0X01 : EAPoL-Start
  - 0X02 : EAPoL-Logoff

- 0X03 : EAPoL-Key
- 0X04 : ASF Aalert

- Packet Body Length = Body의 길이를 표시한다.
- Packet Body : EAP 메시지가 수납된다.

802.1x는 Supplicant, Authenticator, Authentication Server 사이의 인증 정보 교환 수단으로써 EAP를 차용하여 기존 인증 프로토콜의 장점을 취한다[12]. EAP는 다중 인증 메커니즘을 지원하는 일반적인 프로토콜로써 스마트 카드, Kerberos, 공용키 암호화, OTP(OneTime Password)를 포함한 수많은 인증 구조를 지원한다.

802.1x에서는 Supplicant와 Authenticator사이의 프레임 전송을 위하여 표 2와 같이 EAPoL이라는 프레임 기술을 정의하고 있다. 현재까지는 802.3 이더넷 MAC와 토큰링/FDDI MAC을 위한 EAPoL 프레임이 정의 되어 있다.

4. 802.1x 프로토콜의 동작

802.1x의 사용자 수준의 인증기능을 제공하는 인증절차는 그림 6과 같이 이용자와 서비스 제공자 그리고 인증서버 사이의 포트 기반 네트워크 접속 메커니즘의 과정을 보여준다.

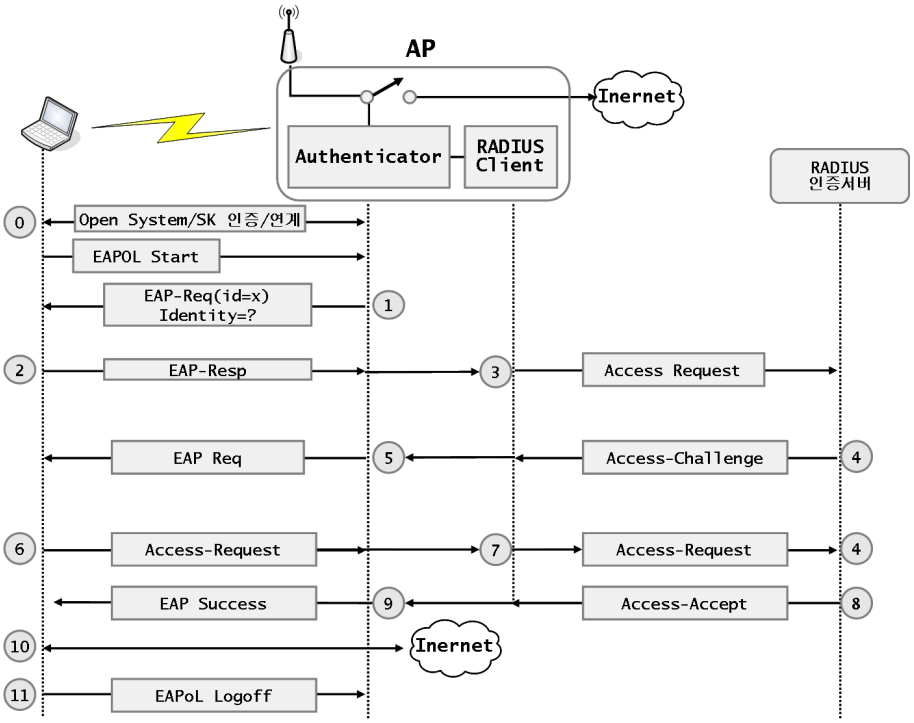


그림 6. 802.1x 시스템의 구성과 동작

- 단계 0 단말과 AP
  - 단말은 Open System 또는 Shared Key 방식으로 시스템 수준의 인증절차를 수행하여 AP와 연결한다.
- 단계 ① AP
  - 단말로부터 EAPoL Start 메시지를 수신하거나, 단말이 접속된 사실을 감

지하면 사용자 이름을 전송하라는 EAP-Request[Identity] 메시지를 EAP Packet에 수납하여 단말에게 요청한다. Identity 항목에는 AP의 정보인 SSID, AP의 이름등이 수납된다.

- 단계 ② 단말
  - 자신의 사용자 이름이 수납된 EAP-Response[Identity] 메시지로 응답한다.
- 단계 ③ AP
  - 단말로부터 수신한 EAP-Response[Identity] 메시지를 RADIUS 메시지인 RADIUS Access-Request로 생성하여 인증서버에 중계한다.
- 단계 ④ RADIUS 서버
  - RADIUS Access-Challenge 메시지에 CV(Challenge Value)가 수납된 EAP Request 메시지를 구성하여 AP에 송신한다.
- 단계 ⑤ AP
  - RADIUS 메시지의 EAP 속성을 꺼낸후, EAPoL 패킷에 다시 수납하여 단말에 중계한다.
- 단계 ⑥ 단말
  - EAP-Response(Challenge Response) 메시지로 AP에 응답한다.
- 단계 ⑦ AP
  - 단말로부터 전달받은 EAP-Response(Challenge Response) 메시지를 RADIUS 메시지인 RADIUS Access-Request로 생성하여 RADIUS 인증서버에게 중계한다.
- 단계 ⑧ RADIUS 서버
  - 정당한 사용자인 경우, EAP Success 메시지를 구성한 후, 이것을 RADIUS Access Accept 메시지의 EAP 속성에 수납하여 AP에 송신한다.
- 단계 ⑨ AP
  - EAP Success 메시지를 단말에 중계하면서, 사용자를 인증하고, 해당 단말이 인터넷에 접근할 수 있도록 한다.
- 단계 ⑩ 단말
  - EAP Success 메시지를 수신하면, 이후부터 AP를 경유하여 외부 인터넷에 접근할 수 있게 된다.

- 단계 ⑪ 단말
  - Log off시에는 EAPoL Logoff 메시지를 AP에 송신한다. 하지만, 이 메시지는 아무런 보안 특성이 없어, 해커가 임의로 전송하면 문제가 발생하기 때문에 실제로는 사용되지 않는다. 그리고, AP도 이 메시지를 무시한다.

제3절 EAP 인증 유형

기존 무선 LAN 단말은 AP와의 아무런 사용자 인증절차가 없는 개방 시스템 인증 방법이나 단말과 AP간에 수동으로 설정된 공유 키가 일치하는지를 WEP 암호문의 교환으로 확인하는 수준의 간단한 인증을 사용한다. 하지만, 이 WEP에 의한 암호방식은 사용중인 키가 노출되는 문제 때문에 안전한 인증을 하지 못하는 문제가 있다.

이에 802.11 WGi에서 새롭게 정의한 ESN(Enhanced Security Network) 프레임워크에서는 안전한 키 분배와 상호 인증 지원을 요구하고 있다. EAP 인증 유형은 이를 위한 방안으로써 여러 무선랜 사업자들은 독자적으로 EAP 인증 유형을 개발하고 있다. 주로 많이 사용되고 있는 EAP 인증 유형은 다음과 같다[9].

1. EAP-MD5

가장 초기의 EAP 인증 유형이고, 유일한 필수(mandatory) 구현 방식이다. 이 프로토콜은 802.1x 프레임워크에서 기본 수준의 EAP를 지원하는 대표적인 EAP 인증 유형이다. 하지만 패스워드 기반의 인증 방식은 사용자와 인증서버간 상호인증이 없어, 사용자는 서버를 무조건 믿기 때문에 불법 AP에 의심없이 접속할 수 있는 문제가 있다. 그림 7에서와 같이 해커가 불법으로 설치한 AP에 EAP-MD5로 인증절차를 수행하는 단말은 이 AP와 수행하는 인증절차로부터 해당 AP가 불법으로 설치되어 있는 것인지 알 수가 없다.

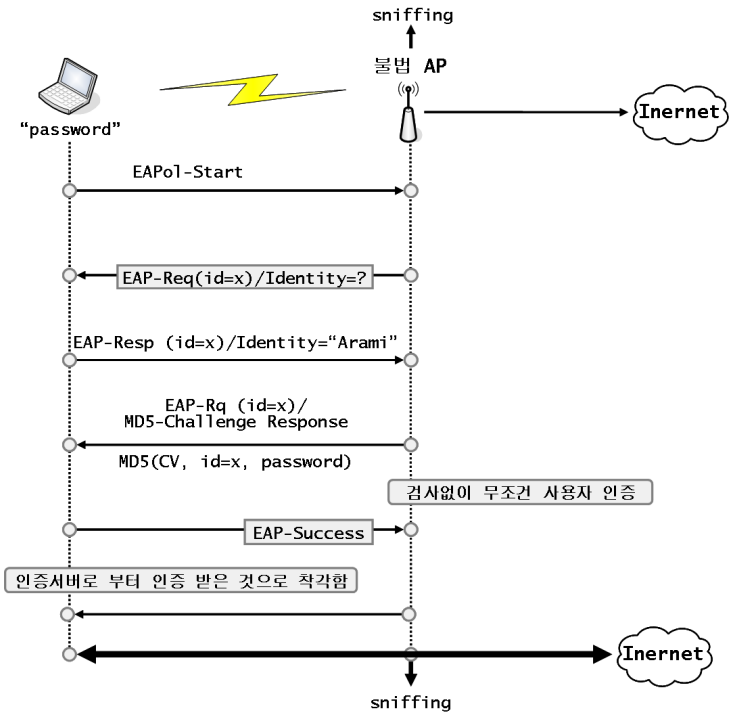


그림 7. EAP-MD5 인증 방식의 문제점

이러한 문제점은 단말 입장에서 유효한 서버인지 확인하지 않고, 서버 입장에서 단말만 인증하였기 때문이다. 이는 상호인증이 수행되지 않았기 때문에 발생한 것이다. 또한, EAP-MD5에서는 인증을 위하여 사용자 이름과 패스워드가 전송되는데 사용자 이름은 암호화되지 않은 상태로 그리고 패스워는 MD5로 해쉬되어 전송되기 때문에 공인 인증서를 이용하지 않으므로 공인된 인증이라 할 수 없다.

2. LEAP(Lightweight EAP)

EAP-Cisco Wireless라고도 불리는 이 프로토콜은 시스코 무선랜 AP에 주로 사용되며, 국제표준은 아니다. 이 LEAP는 인증시에 간단하게 사용자 단말의 패스워드 해시값을 사용한다. 그리고, LEAP는 사용자 인증과 서버인증을 모두 수행하는 상호인

증절차가 사용되며, 상호인증 후에는 무선구간 보호용 키도 인증서버로부터 AP에게 전달된다. 이후 데이터 전송은 동적으로 생성되는 WEP키를 이용해서 암호화된다.

하지만, 이 또한 서버 입장에서는 사용자를 인증할 수 있지만, 사용자 입장에서는 인증서버가 유효한 서버인지 확인하지 못하고 무조건 믿을 수 밖에 없는 일방향 인증 방법으로서 해커가 불법으로 설치한 불법 엑세스포인트에 아무런 의심없이 접속하는 문제가 발생한다. 위와 같이 인증서 기반의 인증절차가 아닌 Challenge 방식에 의해 상호인증을 수행하지만, 불법 AP에 의심없이 접속할 수 있는 문제는 여전히 존재할 수 밖에 없다.

3. EAP-TLS(Transport Layer Security)

TLS는 각각의 인증서를 이용하여 상호 인증하고, 그 결과에 의해 쌍방간에 공유하는 비밀 키를 생성하여 이후 전송되는 데이터들을 보호하는 프로토콜이다. 이러한 TLS 기능 중의 클라이언트와 서버간 상호인증 기능을 무선 단말인증용으로 활용하여 도청이나 간섭, 메시지 위조와 같은 비 권한 제어를 방지할 수 있다[13]. 또한 단말 입장에서도 AP를 경유하여 인증서버가 유효한 서버인지를 확인하는 상호인증 기능이 지원가능하게 되었고, 안전한 연결성을 보장하기 위해 사용자 기반, 세션 기반의 동적인 WEP키를 생성하여 분배한다. EAP-TLS는 TLS단말과 인증서버간에 설정되는 TLS기반에서 동작하며, 인증서 사용 여부에 따라 분류하면 그림 8과 같다.

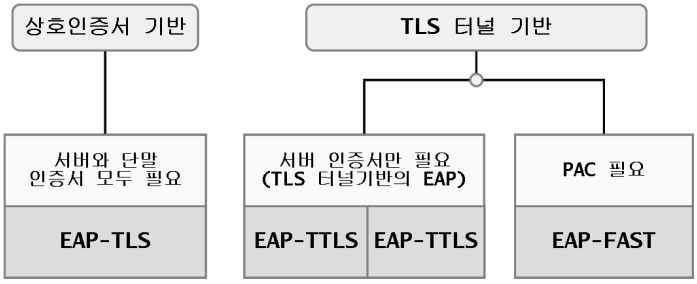


그림 8. TLS 기반의 상호 인증 방식

- 상호 인증서 기반의 상호인증방식

- EAP-TLS : 단말과 인증서버 모두 인증서 필요

- 인증서버 인증서만 사용한 TLS 터널 기반의 상호인증 방식
  - EAP-Tunneld TLS(EAP-TTLS)
  - Protected EAP(PEAP)

- PAC(Pretected Access Credential)를 사용한 TLS터널 기반의 상호인증방식
  - EAP-FAST : 인증서 대신에 일종의 패스워드인 PAC를 사용하여 TLS 터널을 설정한 후, 별도의 EAP 인증 방식으로 사용자를 인증함.

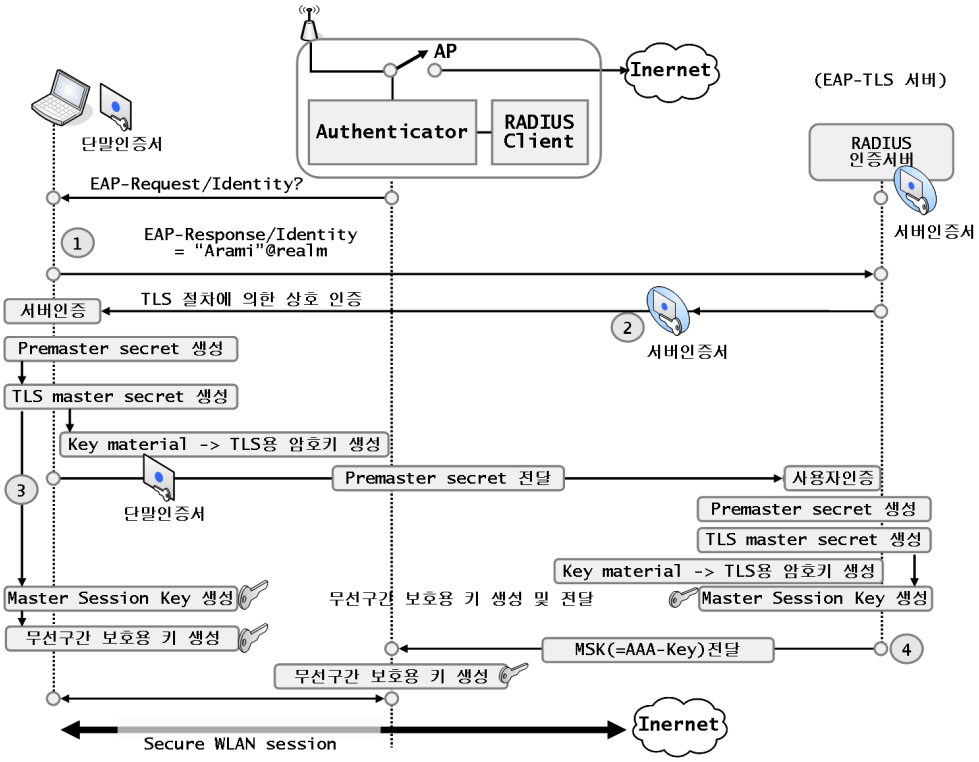


그림 9. TLS 기반의 상호 인증 방식

- 단계 ① 단말은 자신의 ID를 서버로 보내어 TLS 연결절차를 개시한다.

- 단계 ② 단말과 인증서버간에 일반적인 TLS 연결절차에서 수행되는 각자의 인증서를 사용한 상호인증 과정을 수행한다. 이 과정에서 단말이 임의로 생성한 Premaster secret값으로부터 쌍방은 TMS(TLS Master Secret)를 공유한다.

- 단계 ③ 단말과 서버는 TMS로부터 단말과 엑세스 포인트간에 사용할 무선구간 암호용 키인 Master Session Key(MSK)를 생성한다.

- 단계 ④ EAP-TLS 인증서버는 MSK를 엑세스 포인트에 전달한다.

- 단계 ⑤ 마지막으로, 단말과 AP는 동일한 MSK로부터 무선구간에서 사용될 암호 키를 생성한 후, EAPoL-Key/프레임을 이용한 4-웨이 핸드쉐이킹이라고 부르는 키 보유 확인 및 방송용 그룹키 분배절차를 수행한다.

EAP-TLS는 위와 같은 인증절차를 거쳐 클라이언트와 인증서버 모두 상대방 인증이 가능하여 양방향 인증이 가능하며 공인된 인증이다. 그러나 클라이언트는 인증절차가 완료되기 전에는 네트워크를 이용할 수 없기 때문에 네트워크로부터 CRL(Certificate Revocation List)을 수령하거나 OCSP(Online Certificate Status Protocol) 서버에게 인증서 유효성 검증을 요청할 수 없다. 따라서 클라이언트는 인증서버를 실시간으로 인증할 수 없는 문제점이 있다.

4. EAP-TTLS, PEAP

단말과 인증서버 모두의 인증서가 사용되는 EAP-TLS가 가장 확실한 인증 방법이지만, 모든 단말에 인증서를 설치하는 것은 비용이나 관리면에서 단점이 있다. 따라서 그림 10과 같이, 서버측 인증서만을 사용한 TLS 보안 터널을 설정한 후, 이 TLS 연결로상에서 다양한 종류의 사용자 인증 방법을 추가 사용하는 TLS 터널 방식의 EAP 인증 방법인 EAP-TTLS나 PEAP가 무선 LAN 시장에서는 더 많이 사용되고 있다.

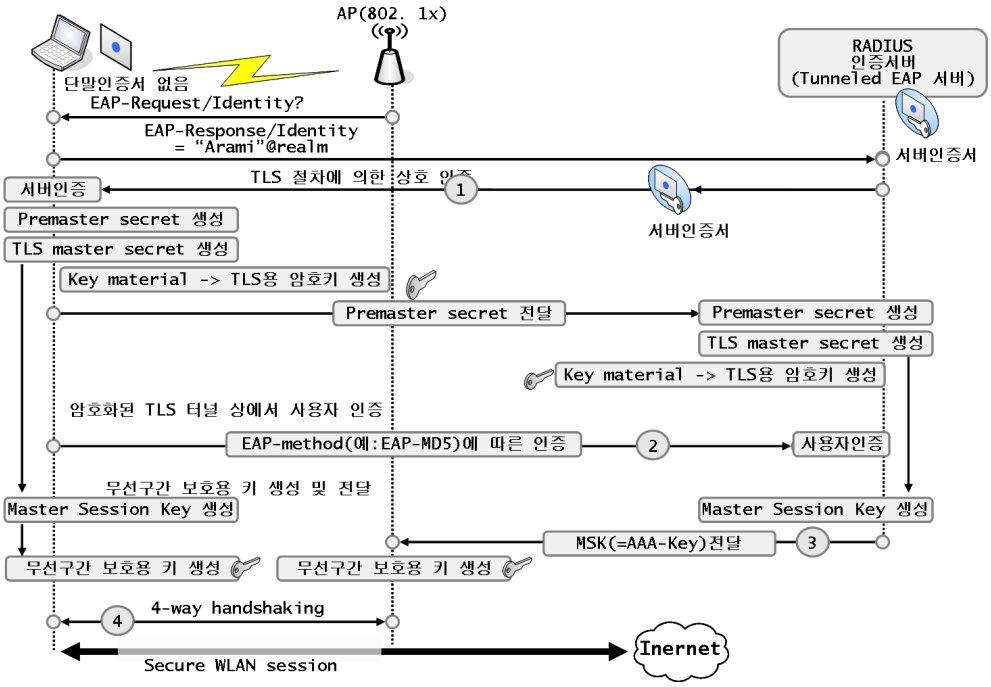


그림 10. TLS 터널기반의 EAP 인증절차(EAP-TTLS, PEAP의 경우)

- 단계 ① 단말과 인증서간에 서버 인증서만 사용한 TLS 절차에 의해 서버에 대한 인증과정을 먼저 수행한다. 이 과정에서 단말이 임의로 생성한 Permaset secret 값으로부터 쌍방은 TLS master secret(TMS)를 공유하게 되고, 이로부터 key material을 생성하면서 TLS 터털 보호용 암호키를 생성한다.

- 단계 ② 인증서버는 단말과의 TLS터널상에서 다양한 종류의 EAP 인증방식을 사용하여 사용자 인증을 수행한다.

- 단계 ③ 사용자를 인증한 인증서버는 단말과 액세스 포인트간에 사용할 무선구간 암호용 키 생성용 키인 MSK를 액세스 포인트에게 전달한다.

- 단계 ④ 마지막으로, 단말과 AP는 동일한 MSK로부터 무선구간에서 사용될 암

호키를 단말과 AP가 가지고 있는 ciphersuite로부터 생성하고, EAPoL-Key 프레임을 이용한 4-way handshaking라 부르는 키 보유 확인 및 방송용 그룹 키 분배절차를 수행한다.

EAP-TTLS, PEAP는 클라이언트와 인증서버 모두 상대방 인증이 가능하여 양방향 인증이 가능하다. 그러나 클라이언트에게 인증서를 발행하지 않아도 되는 장점이 있는 반면 클라이언트 인증은 공인된 인증이 아니다. 그리고 EAP-TLS와 동일한 이유로 클라이언트는 인증서버를 실시간으로 인증할 수 없다는 문제점을 가지고 있다.

제4절 인증서 검증 방법

PKI 보안시스템에서는 인증서를 이용하여 상대방의 신원을 확인한다. 인증서에 대한 기본 형식은 ITU-T에서 제안한 X.509 인증서 표준을 따른다[14]. 초기 X.509 버전 1에 이어 버전 2에서는 인증서 폐지목록을 포함 시켰으며, 버전 3에서는 인증서를 정의하는 다양한 환경에 맞는 조건과 서명 알고리즘들의 선택이 가능하도록 확장 영역을 추가하였다.

인증서 상태 검증 방법에서는 인증서 폐지목록(CRL:Certificate Revocation List), 인증서 폐지시스템(CRS:Certificate Revocation system), 인증서 폐지 트리(CRT:Certificate Revocation Tree), OCSP(Online Certificate Status Protocol) 그리고 Scvp(Simplified Certificate Validation Protocol) 등이 있는데 이중에서 CRL 방식과 OCSP 방식이 가장 많이 이용되어 왔다. 다음은 이 두가지 방법에 대하여 각각 특징 및 장단점을 알아본다.

1. CRL 이용 방식

전자 인증서를 사용하는 인터넷 공간에서 사용자 인증서의 유효기간은 인증서에 표기된 날짜로 검증을 하지만, 사용자가 키를 분실했을 경우 요즘처럼 인터넷 뱅킹 및 여러 가지 인증 응용프로그램을 사용하는 상황에서 상당히 치명적인 피해를 초래

할 수 있다. 이와 같은 이유로 인하여 CRL은 인증서의 폐지 여부를 확인할 수 있는 가장 일반적인 방법으로서 CA가 인증서 폐지 목록을 보통 하루에 한두 번 정도로 주기적으로 생성하여 디렉토리에 게시한다. 이러한 인증서 상태를 확인하기 위해서는 이 디렉토리로부터 CRL을 다운로드 하여 검사를 해야만 한다.

가. CRL의 내용

- 폐기된 인증서의 리스트와 각 폐기된 인증서의 폐기 사유
- CRL을 발행한 자의 이름(Issuer)
- CRL이 발행된 날짜, 시간
- 다음 CRL이 발행될 시간

나. CRL의 사용

- 인증서의 주인에게 메시지를 암호화해서 보내려고 할 때
- 인증서의 주인으로부터 온 메시지의 서명을 확인할 때

다. CRL의 이용 단계

(1) 필요한 인증서를 가져와서 유효기간을 검사
(2) 인증서의 일련번호를 확인
(3) CRL을 CA의 디렉토리에서 다운을 받는다.
(4) CRL에 있는 전자서명을 확인
(5) 인증서의 일련번호를 확인하여 CRL로부터 인증서의 폐기여부를 조사한다.
(6) 인증서가 폐기되었다면 사용자에게 해당 메시지를 보낸다.
(7) 유효한 인증서라면 인증을 완료한다.

라. CRL의 장점

- CRL은 사용자에게 여러 가지 방법으로 분배될 수 있다.
- Transaction의 부인방지를 할 수 있도록 CRL은 저장 될 수 있다.
- 많은 PKI 응용 프로그램들이 디렉토리로부터 CRL을 가져올 수 있다.

마. CRL의 문제점

인증서를 검증하기위해서는 항상 현재의 CRL을 가지고 있어야 하며, 로컬 시스템일 경우에는 저장하고 있는 파일을 자주 갱신해야 한다. CRL을 다운 받는 시스템은 자주 다운 받아서 항상 최신의 정보를 가지고 있어야 한다. 그리고, 폐기된 인증서가 자꾸 쌓이면 CRL의 크기가 너무 커져서 이 CRL을 다운 받기 위해서 시스템이 느려질 수 있다. 또한, CA에 설정된 주기에 따라서 정기적으로 발행되므로 너무 빈번히 발행해도 시스템에 무리가 있을수 있으며, 발행주기가 너무 크면 이미 폐기된 인증서를 유효한 것으로 사용할 수 있는 문제점 때문에 실시간성을 제공해 줄 수가 없다.

그리고, 수신한 인증서의 인증여부를 사용자 자신이 인증서 폐지목록을 직접 비교하여 수신한 인증서의 인증여부를 판단하기 때문에 자신의 판단 착오로 인하여 인증 발생한 문제에 대해서는 향후 법적인 보호를 받을 수 없다.

IEEE의 RFC 3280에서는 다중 CA 시스템에서 활용할 수 있는 인증 경로 검증 절차를 제시하고 있으나 이는 인증 경로상의 모든 인증서를 순차적으로 검증하는 방식이여서 인증 경로가 긴 경우 인증서 검증에 많은 부하가 걸릴 것이다[15].

2. OCSP 서버 이용 방식

OCSP는 1996년 6월에 IETF RFC2560으로 표준화되어 발표되었다. OCSP는 온라인 방식의 인증서 상태 확인 프로토콜로서 클라이언트가 인증서의 일련번호를 OCSP 서버로 보내면 OCSP 서버는 인증서 상태를 확인한 후 전자 서명된 상태 결과를 클라이언트에게 보내준다. Internet Draft OCSP v2는 구체적인 동작을 정의하고 있지 않으며 클라이언트와 서버 간에 교환되는 메시지 구성과 형태만을 정의하고 있다[16].

가. OCSP의 장점

- CRL을 배포하지 않아도 되므로 CRL 배포에 대한 문제점 개선
- OCSP 요구/응답 구조가 클라이언트 서버모델의 정보 조회 구조이므로 더 많은 서비스 제공이 가능하다.(응답메시지가 CRL 보다 작다)
- OCSP 메시지를 HTTP(Web), SMTP(Mail), LDAP(directory) 같은 Application Layer 프로토콜로 전달할 수 있다.
- 인증서의 상태정보를 요구하는 클라이언트는 인증서의 특정한 정보를 알고 정보를 요청하므로, 모든 리스트를 보여주는 CRL보다 익명성이 보장된다.
- 인증서의 상태를 요구한 사용자는 OCSP서버가 직접 친필 서명한 인증서 상태 정보를 받아 두면 부인 봉쇄를 방지 할 수 있으며, CRL을 저장해 두는 것보다 간단하다.

나. OCSP의 단점

- 대부분의 OCSP서버가 인증서의 상태정보를 주기적으로 발행되는 CRL의 내용에 기초하기 때문에 CRL의 주기적 발행에서 오는 문제점들은 해결되지 않는다.
- OCSP서버는 인증서 상태요구가 많아진다면 서비스 불능(Denial of Service)상태가 될 수 있다.
- 에러 메시지는 서명하지 않기 때문에 공격자가 허위 에러 메시지를 사용자에게 보낼 수 도 있다.

제3장 무선 LAN 보안 시스템 설계

2장에서는 기존의 IEEE 802.1x를 이용한 다양한 인증 유형의 특징과 문제점을 파악하고, 인증서 유효성을 검증하는 방법들에 대한 특징과 장단점을 살펴보았다. 초기의 무선 LAN 오픈 시스템 인증 방법이나 공유 키 인증 방법은 이미 많은 문제점들이 노출되었기 때문에 현재는 PKI를 적용한 802.1x 인증방법이 연구되어지고 있지만, 높은 보안성을 제공하는 EAP-TLS의 경우에는 인증서 검증과 CRL 검색 등의 많은 오버헤드가 발생하고, 초기 인증시 상호 인증을 위한 인증서 교환 프로토콜의 효율성이 떨어지며, CRL 방식에서 CA에 의한 인증서 폐지 목록을 주기적으로 갱신하기 때문에 인증서의 현재 상태에 대한 시간차(Time-Gap) 문제가 발생하여 완벽한 실시간성을 제공해줄 수가 없다. 이와 같은 기존의 보안 시스템에 대한 문제점을 분석하여 본 논문에서는 상호인증이 가능하고 실시간성을 제공해주며, 효율적인 인증 프로토콜을 설계하였다.

제1절 기존 인증 유형의 문제점 분석

1. EAP-MD5

- 인증을 위하여 사용자 이름과 패스워드를 전송되는데 사용자 이름은 암호화 되지 않고, 패스워드만 MD5로 해쉬되어 전송된다.
- 인증서버는 클라이언트를 인증할 수 있으나 클라이언트가 인증서버를 인증할 수 없다.
- 단방향 인증만 가능하며, 공인인증서를 사용하지 않기 때문에 공인된 인증이라 할 수 없다.

표 3. EAP-MD5 인증 특성

프로토콜 / 항 목	EAP - MD5
상 호 인 증	클라이언트가가 AS 인증 불가
실 시 간 인 증	가 능
공 인 여 부	비 공 인

2. EAP-TLS

- 클라이언트와 인증서버 모두 상대방 인증이 가능하다.
- 클라이언트와 인증서버 모두 공인 인증서를 사용하므로 공인된 인증이다.
- 클라이언트는 인증 절차가 완료되기 전에는 네트워크를 이용할 수 없기 때문에 CRL을 수령하거나 OCSP 서버에게 인증서 유효성 검증을 요청할 수 없으므로 클라이언트는 인증서버를 실시간으로 인증할 수 없다.

표 4. EAP-TLS 인증 특성

프로토콜 / 항 목	EAP - TLS
상 호 인 증	가 능
실 시 간 인 증	클라이언트가 AS 인증시 불가
공 인 여 부	공 인

3. EAP-TTLS, LEAP

- 클라이언트와 인증서버 모두 상대방 인증이 가능한 양방향 인증이다.
- 클라이언트는 인증서를 사용하지 않는 장점이 있지만, 클라이언트 인증은 공인된 인증이 아니다.
- EAP-TLS와 동일한 이유로 클라이언트는 인증서버를 실시간으로 인증이 불가능하다.

표 5. EAP-TTLS, PEAP 인증 특성

프로토콜 / 항 목	EAP - TTLS, PEAP
상 호 인 증	가 능
실 시 간 인 증	클라이언트가 AS 인증시 불가
공 인 여 부	클라이언트 인증 비공인

제2절 기존 인증서 검증 방법의 문제점 분석

1. CRL 이용 방식

- 인증서를 검증하려면 항상 현재의 CRL을 가지고 있어야 하지만, 인증서 폐지목록은 일정한 주기로 갱신되기 때문에 현재 상태에 대한 시간차(Time-Gap) 문제가 발생하여 실시간성을 제공할 수 없다.
- 인증서 폐지 목록을 자신이 직접 비교하여 수신한 인증서의 인증 여부를 판단하기 때문에 이로인한 문제가 발생시 법적인 보호를 받을 수 없다.
- 폐기된 인증서가 자꾸 쌓이면 CRL의 크기가 너무 커져서 이 CRL을 다운 받기 위해서 시스템이 느려질 수 있다.
- 다중 CA 시스템 구조에서 활용할 경우 인증 경로상의 모든 인증서를 순차적으로 검증하는 방식이어서 인증 경로가 길어질 경우 인증서 검증에 많은 부하가 걸린다.

표 6. CRL 인증서 검증 방법의 특성

방 법 / 항 목	CRL
시스템 효율성	조회횟수=n + Σ
검증 속도	시스템 규모에 반비례
신뢰해야할 기관수	CA 개수

- CRL은 CA 계층구조 상에서 두 사용자간의 경로 사이에 CA가 n개 있다면 인증서 검증을 위한 총 검증 요청수는 n + Σ(각 CA들의 하위 CA 개수) 가 되어 인증서 검증을 위해서 시스템에 매우 큰 부담을 줄 것이다.

2. OCSP 이용 방식

- 주기적으로 발행되는 CRL의 내용에 기초하기 때문에 요청과 응답에 있어서 응답 메시지의 현재성에 문제점은 해결 될 수 없다.
- 인증서 상태요구 서비스가 많아지게 되면 서비스 불능(Denial of Service)상태가 될 수 있으며, 이는 DoS 공격에 취약하다.
- OCSP 서버가 다운되면 CRL서비스로 전환해서 인증서 상태 정보조회가 가능해져야하는데 이는 시스템의 복잡도를 더 높이고, CRL의 단점들을 완전히 제거하지 못한 것이 된다.
- 다중 CA 구조의 대규모 시스템에서 OCSP 서버를 이용할 경우 클라이언트들의 서비스가 집중될 경우 실시간 서비스 제공이 어려워질 수 있다.

표 7. OCSP 인증서 검증 방법의 특성

방 법 / 항 목	OCSP
시스템 효율성	조회횟수=n + Σ
검증 속도	시스템 규모에 반비례
신뢰해야할 기관수	1 개

제3절 실시간 무선 LAN 보안 시스템 설계

이제까지 기존 무선 LAN 보안 시스템에서 적용되었던 인증 유형과 인증서 검증방법의 문제점들을 분석하여 아래와 같이 보안적인 측면과 시스템 효율성에 관하여 개선할 점을 본 논문의 제안 목표로 정하였으며, 이러한 목적에 맞는 무선 LAN 보안 시스템을 설계하고자 한다.

1. 제안 시스템의 기본 조건

기존의 시스템에서의 문제점을 개선하기 위하여 본 논문에서 제안한 무선 LAN 보안 시스템은 포트 기반의 접근제어 방식의 IEEE 802.1x 프레임워크상에서 공개키 기반구조의 암호시스템을 이용하고, 인증서 발급 및 관리를 담당하는 인증기관(CA)이 다중으로 설치되어 있는 환경을 제안 시스템의 기본 조건으로 가정후에 본 논문에서 구현하고자하는 무선 LAN 보안 시스템을 설계하고자 한다.

2. 제안 시스템의 설계 목적

가. 인증관련

- 클라이언트와 인증서버는 상호 인증이 가능해야한다.
- 클라이언트와 인증서버는 상호 실시간 인증이 가능해야한다.
- 공인 인증서를 사용하여 인증 사실을 공인 받을 수 있어야 한다.

나. 시스템 효율성

- 인증서 검증방법은 효율적이며, 안전한 방법이어야 한다.
- 검증 속도도 기존 시스템보다 느려서는 안된다.
- 인증 프로토콜의 효율성을 위하여 핸드쉐이크 과정이 복잡해서는 안된다.
- 무선 단말인 클라이언트의 과다한 암호연산으로 인한 부하가 증대되지 않아야 한다.

3. 제안 시스템의 구성

가. 인증 요청자 : MN

- C_{mn} : CA가 발급한 공인 인증서
- S_{mn} : 사용자 MN의 비밀키로 서명한 서명문
- ID_{mn} : 사용자 MN의 ID
- K_{MP} : MN과 PA(Proxy Authentication) Server 사이의 대칭키
- PK_{mn} : 사용자 MN의 공개키
- SK_{mn} : 사용자 MN의 비밀키

나. 무선 네트워크 중계자 : AP

Authenticator System 기능을 수행하며, MN이 네트워크 접속을 시도했을 경우 Uncontrolled Port를 이용하여 Supplicant System과 Authentication Server System

사이에 인증을 수행하고, 인증이 성공하였을 경우에 Controlled Port를 인가하여 서비스를 제공해주며, WEP 키를 이용한 MN과 AP사이에 데이터 기밀성을 가능하게 해준다.

다. 인증 서버 : AS

공개 키 기반 구조(PKI)에서 전자 서명 및 공개 키 인증서의 유효성과 데이터의 소유나 존재를 확인하기 위한 서버로써, 무선 LAN 시스템에서 클라이언트를 인증하는 서비스를 제공한다.

라. 대리 인증 서버 : PA

기존 인증 방식의 인증 절차에서 상호 인증을 수행하기 위해서는 수 차례의 핸드쉐이크 과정을 거쳐야만 상호 인증이 가능하였다. 이러한 과정에서 단말은 인증서의 검증을 위하여 매번 암·복호화를 함으로써 이동성을 고려한 무선단말은 많은 부하를 받을 것이며, 수 차례의 핸드쉐이크 과정을 거치면서 제한된 무선 네트워크망에서 자원을 소비하게 된다. 이러한 문제점을 개선하기 위하여 제안 시스템에서는 대리 인증 서버를 사용을 제안 하였다. 이는 EAP-TLS 와 같이 보안상 강력한 인증 방법을 제공하고는 있지만, 저속 저용량의 무선단말에 있어서 부하가 많이 걸리는 인증 방식은 사용이 불가능 하다. 따라서 본 논문에서는 강력한 보안을 제공하는 EAP-TLS와 같이 클라이언트와 인증 서버 모두 인증서를 사용한 상호 인증과, 저속 저용량의 무선단말 또한 이를 사용할 수 이용할 수 있도록 하기 위하여 대리 인증 서버를 사용하였다.

이는 인증 서버에서 먼저 클라이언트를 인증 후 인증 서버 자신을 인증 하기 위해서는 대리 인증 서버를 이용하여 자신의 인증을 마친 후, 대리 인증서버는 이를 클라이언트에게 통보 함으로써 클라이언트는 인증 서버의 검증 내용만 확인 후 네트워크에 접속이 가능하다. 이는 무선 단말 시스템에 부하를 줄일 수 있으며, 간단한 인증 절차만을 거친 후 무선 네트워크에 접속을 할 수 있게 되어 인증 시간을 단축 시킬것이다. 하지만 이를 위하여 클라이언트와 대리 인증 서버사이에서는 무선 네트워크를

사용하기 이전에 유선망을 통한 사전 등록 단계를 거쳐서 대리 인증 서버에 클라이언트의 대리 인증을 위한 위임서와 대리 인증 서버와 클라이언트간에 사용될 대칭키를 생성하여 보관 하여야 한다.

사전 등록 단계는 유선망을 사용하여 클라이언트와 대리 인증 서버사이에 공인 인증서를 이용한 상호 인증을 거친 후 무선 네트워크에 접속시 대리 인증 서버의 서비스를 받을 수 있다.

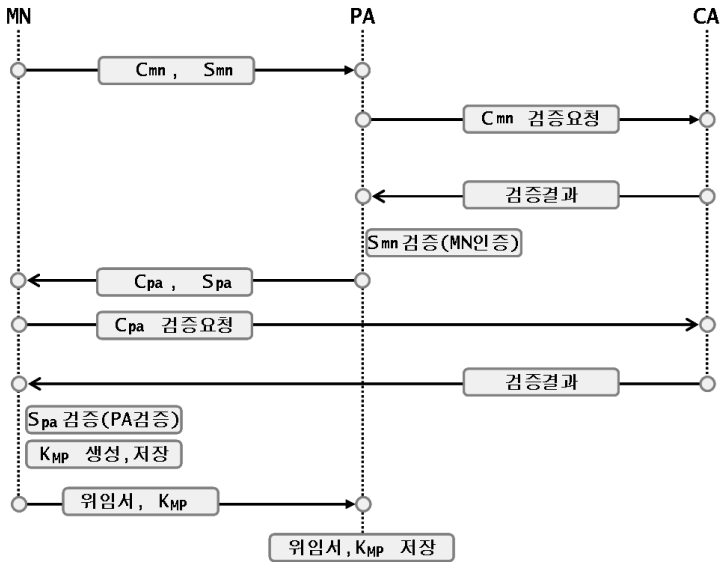


그림 11. 클라이언트의 사전 등록 절차

마. 인증서 검증 프로토콜 : CVP

인증서 검증 프로토콜은 PKI 초기부터 CRL이라고 하는 인증서 폐기목록을 사용하였는데 배포시점에 대한 문제와 책임소재 때문에 지속적으로 논의의 대상이 되어 왔다. 그러다가 OCSP가 제안되면서부터 본격적인 연구의 대상이 되었으며 SCVP(Simple Certificate Validation Protocol), DPD/DPV(Delegated Path Discovery/Delegated Path Validation), OCSPv2등이 제안되면서 다양한 검증 방법들이 연구 되었으며, CVP는 2002년 7월 Bull의 Denis Pinkas가 최초로 제안하였다.

본 논문에서는 CRL을 이용하지 않고 OCSP 서버와 같은 별도의 기관을 두지 않고 CA를 직접 이용하도록 하여 CRL을 생성 관리하거나 OCSP 서버에 응답하는 동작을 하지 않기 때문에 CA의 부담을 증가 시키지 않으면서 CRL이나 OCSP 서버를 이용할 때의 단점을 해소할 수 있게 하기 위하여 CVP를 사용하였다. 이러한 CVP 인증서 대리 검증 서비스에 대한 새로운 프로토콜에 대한 주요내용을 아래와 같다.

- 특정 인증서에 대한 대리 검증 서비스를 요청 받아 해당 인증서의 유효성 여부를 결과 메시지로 전송하기 위한 프로토콜이다.
- 기존의 OCSP 서비스 및 DPD / DPV와 목적은 같지만 제안 접근 방식에서 차이가 있다.
- 기존에 제안된 대리 검증 서비스 프로토콜에 비해 보다 사용자 측면에서의 제안 내용이 부각되었다.
- PKI 도메인에서의 EE(End Entity)의 위치를 보다 현명한 사용자로 가정하며 인증서 검증에 대한 정책 선택 및 CVP 서버가 사용하게 될 신뢰 데이터, 검증 대상 인증서, 인증서 폐기 목록, 해당 인증서에 대한 OCSP 결과 메시지 등을 사용자로 하여금 직접 결정하여 CVP 서버에 서비스를 요청할 수 있다.
- 자신이 검증하고 싶은 인증서에 대한 특정 시간의 인증서 폐기 목록이나 OCSP 결과 메시지 등을 포함한 서비스 요구 메시지를 전송할 수 있으며, CVP 서버는 해당 메시지를 전폭 수용하여 검증 서비스를 처리하도록 되어 있다.

CVP는 기존 방식들에 대한 장단점을 충분히 분석해서 나온 매우 효율적인 대리 검증 서비스를 위한 프로토콜로써 제안 시스템에 구성요소로써 사용하였다.

4. 제안 시스템의 인증 절차

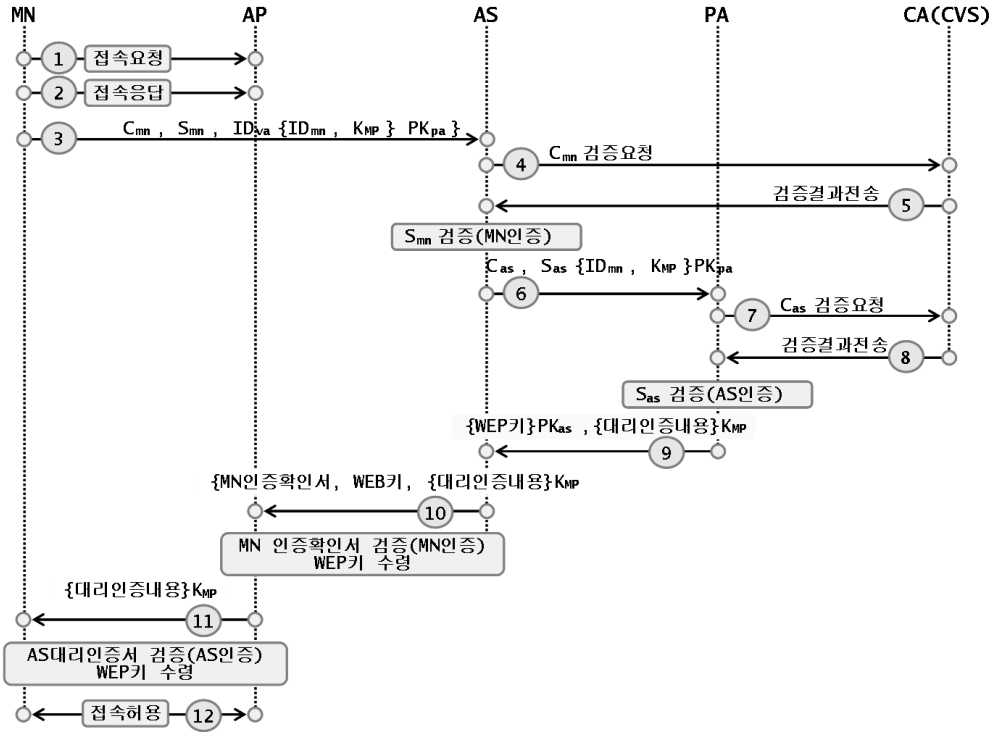


그림 12. 제안 시스템의 인증절차

- 단계 ① MN → AP : IEEE 802.11 접속요청

  무선 단말기는 최적의 AP를 선택하여 접속을 요청한다.

- 단계 ② AP → MN : IEEE 802.11 접속응답

  무선 네트워크에 접속하기위한 인증 과정의 시작을 알린다.

- 단계 ③ MN → AS : [C_{mn}, S_{mn}, ID_{pa}, {ID_{mn}, K_{MP}}PK_{pa}]

  CA가 MN에게 발급한 인증서(C_{mn}), MN의 개인키로 서명한 서명문(S_{mn}), PA의 ID(ID_{pa})와 함께 MN의 ID(ID_{mn}), MN와 PA사이의 대칭키(K_{MP})를 PA의 공개키(PK_{pa})로 암호화하여 AP를 통하여 AS에 전송한다. 이와같이 MN에서 사전에 PA에 유선망을 통하여 PKI방식을 이용한 상호인증을 마쳤으며, 이에대한 MN과 PA사이에 사용가능한 대칭키를 PA의 공개키로 MN의 ID와 함께 암호화하여 기존의 EAP-TLS 방식에 추가하여 전송함으로써, 클라이언트에서는 한번의 데이터 전송만

으로 인증서버와 상호인증이 가능하다.

- 단계 ④ AS → CVP : C_{mn}

  CA가 MN에게 발급한 인증서의 유효성 검증을 위하여 CVP에 전송

- 단계 ⑤ CVP → AS : 검증결과 전송

- 단계 ⑥ AS → PA : [C_{as}, S_{as}, {ID_{mn}, K_{MP}}PK_{pa}]

  AS는 ⑤에서 전송받은 S_{mn}에 대하여 검증을 완료함으로써 MN를 인증한다. 이후 AS자신을 인증하기 위하여 PA에게 CA가 AS에게 발급한 인증서, AS의 개인키로 서명한 서명문과 함께 MN의 ID, MN와 PA사이의 대칭키를 PA의 공개키로 암호화하여 전송한다. 기존의 EAP-TLS 방식에서는 클라이언트와 직접 인증과정을 거치는 단계에서 클라이언트에 인증서 확인을 위한 연산과, 유선망에 비하여 한정되고 보안에 취약한 무선망을 사용함으로써 인증시간의 지연과 무선망에 트래픽을 더욱 증가 시켰다. 따라서, 단계 ⑥에서와 같이 인증과정만을 클라이언트를 대신하여 처리해 줄 수있는 서버의 이용은 무선망을 이용하지 않고, 계산능력이 빠른 서버를 이용함으로써 인증에 걸시는 시간을 단축시킬 수 있다.

- 단계 ⑦ PA → CVP : C_{as}

  CA가 AS에게 발급한 인증서의 유효성 검증을 위하여 CVP에 전송

- 단계 ⑧ CVP → PA : 검증결과 전송

- 단계 ⑨ PA → AS : [{WEP키}PK_{as}, {대리인증내용}K_{MP}]

  PA는 ⑧에서 전송받은 S_{as}에 대하여 검증을 완료함으로써 AS를 인증한다. 이후 WEP키는 AS의 공개키로 암호화한 정보와 AS 대리인증서를 MN과 PA의 대칭키로 암호화하여 AS에 전송한다.

- 단계 ⑩ AS → AP : [MN 인증확인서, WEP키, {대리인증내용}K_{MP}]

  ⑥에서 MS의 인증완료에 따른 MN의 인증확인서, WEP키, AS 대리인증서를 AP에 전송

- 단계 ⑪ AP → MN : [{대리인증내용}K_{MP}, WEP키]

  수신한 MN 인증확인서를 검증한후 WEP키와 AS 대리인증서를 MN에 전송

- 단계 ⑫ MN : AS 대리인증서 검증하여 AS를 인증후 WEP키를 이용하여 무선 네트워크에 접속한다. 이와 같이 단 한번의 핸드쉐이크과정을 거쳐 인증서버와 상호인증을 마치고 AP를 통하여 외부 네트워크에 접속이 가능하게 되었다.

제4장 무선 LAN 보안 시스템 시뮬레이션 및 분석

제안한 보안 시스템이 기존의 보안 시스템과 비교하여 인증과 관련된 부분의 개선된 점과, 안전성 그리고 시스템의 효율면에서 비교 분석을 할 것이다. 또한 시스템의 성능을 분석하기 위하여 OPNET 11.5를 이용하여 시뮬레이션 결과를 분석 해 본다.

제1절 제안 시스템의 인증 관련 분석

1. 상호 인증

제안 시스템에서는 클라이언트와 인증 서버 모두 공인 인증서와 본인 서명문을 이용함으로 상호 인증은 가능하다.

2. 실시간 인증

제안 시스템에서는 인증서를 폐지할 경우 즉시 그 정보가 CA의 폐지 목록에 기록됨으로 CA는 항상 인증서의 최신 상태 정보를 갖게 된다. 따라서 인증서 검증 결과의 현재성을 보장해줄 수 있기 때문에 실시간 인증이 가능하다.

3. 인증 사실의 공인 여부

제안 시스템에서는 클라이언트와 인증 서버 모두 공인 인증서와 서명문을 이용함으로써 인증 사실을 공인 받을 수 있다.

표 8. 제안 시스템과 기존 인증 기능 분석

프로토콜 / 항 목	EAP-MD5	EAP-TLS	EAP-TTLS, PEAP	제안 시스템
상 호 인 증	MN이 AS 인증 불가	가 능	가 능	가 능
실 시 간 인 증	가 능	MN이 AS 인증시 불가	MN이 AS 인증시 불가	가 능

공 인 여 부	비 공 인	공 인	MN 인증 비공인	가 능

제2절 안전성과 효율성 분석

1. 인증 프로토콜의 안전성

통신 내용의 보안은 노드들 간에 전송되는 내용들이 얼마나 안전한가를 분석을 시도해 표 9와 같이 전송되는 내용 중 보안이 필요한 부분에 적절한 암호 방식을 이용하여 암호화하여 전송되고 있는지를 알아보았다.

표 9. 전송 내용 안전성 분석

전 송 내 용	암 호 방 식	분 석
인증서	평문	이미 공개된 내용
서명문	비밀키	조회 가능하나 변조 불가
ID	평문	공개 무방
대칭키(K_{MP})	공개키(PK_{pa})	PA만 해독가능
검증요청	평문	검증요청내용 공개 무방
검증결과	공개키	검증 요청자만이 해독 가능
WEP키	공개키(PK_{as})	AS만이 해독 가능
AS 대리인증서	대칭키(K_{MP})	PA만 생성, MN만 해독 가능
MS 인증확인서	세션키	AS가 생성, AP만이 해독 가능

2. 인증 프로토콜의 효율성

인증 프로토콜의 효율성은 통신량보다는 통신 횟수에 비례한다. 이는 무선 구간에서 상호 인증을 위해 전송되는 통신 내용은 각 프로토콜마다 차이는 있으나 대체로 간단한 질의와 응답으로 구성되기 때문이다. 따라서 통신 횟수를 중심으로 각 프로토콜을 분석해 보았다.

표 10. 구간별 핸드쉐이크 횟수

프로토콜 / 구 간	*EAP-MD5*	*EAP-TLS*	*EAP-TTLS, PEAP*	제안 시스템
MN ↔ AP	3	9	6	2
AP ↔ AS	3	9	6	2
AS ↔ PA	0	0	0	2
AS ↔ CVP	0	0	0	2 or 4
PA ↔ CVP	0	0	0	2 or 4
합 계	6	18	12	10 or 12

제안 시스템의 총 핸드쉐이크 횟수는 최대 12회로써 기존의 EAP-TTLS, PEAP와 같거나 EAP-TLS 보다는 적다. 하지만 실시간 공인된 상호 인증 기능을 가능하게 하면서도 총 통신횟수가 EAP-TLS보다 작고, 공인된 상호 인증을 지원하지 못하는 EAP-TTLS, PEAP와 같거나 작다는것은 제안된 시스템의 효율성이 높음을 볼 수 있다.

제3절 시뮬레이션 구현과 성능 분석

2절까지 제안 시스템에 관한 인증, 안정성, 효율성 측면에서 기존 시스템의 문제점들을 분석하고 개선한 방법들에 대하여 설명하였다. 이렇게 새롭게 제안한 무선 LAN 보안 시스템을 Opnet 11.5 시뮬레이터를 이용하여 성능을 분석하였다.

1. 시뮬레이션 모델에 적용되는 파라미터

- 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 지수분포를 따른다
- V_{cer} : 인증서 필드를 검증하는데 소요되는 시간으로 각 호스트나 서버의 성능에 관계없이 동일하다고 가정한다.
- K_{enc} : 메시지 보호를 위한 암호화 작업의 처리율로서 각 호스트나 서버의 성능에 관계없이 동일하다고 가정한다.
- K_{dec} : 암호화된 메시지에 대한 복호화 작업으 처리율로서 각 호스트나 서버의 성능에 관계없이 동일하다고 가정한다.
- P_{siz} : 인증을 위해서 전송되는 메시지 크기를 나타내며 동일한 값을 갖는다.
- C_{siz} : 인증서 크기로써 인증서의 종류에 상관없이 동일한 값을 갖는다고 가정한다.

2. 시뮬레이션 모델 설계

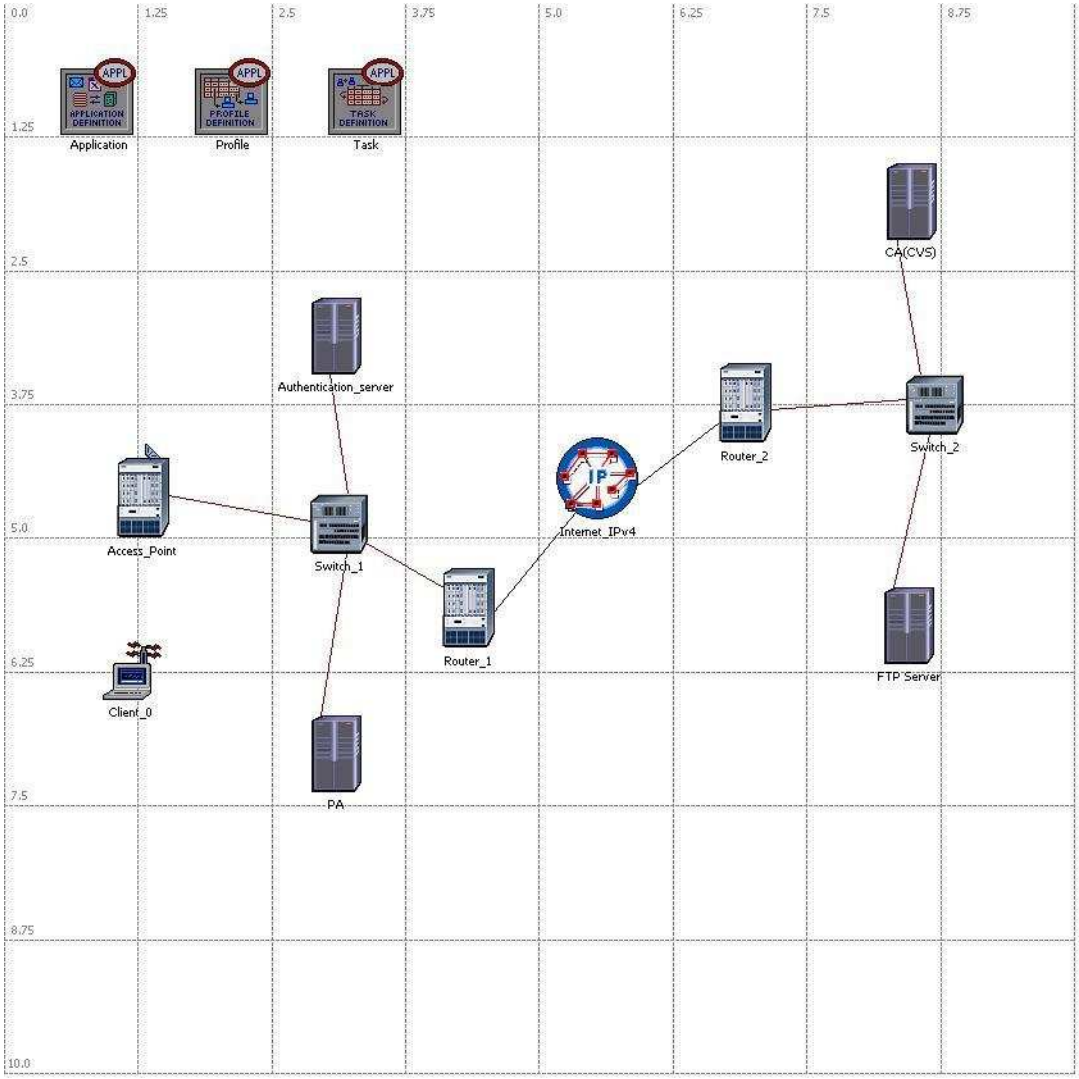


그림 13. 제안 시스템 시뮬레이션 구성도

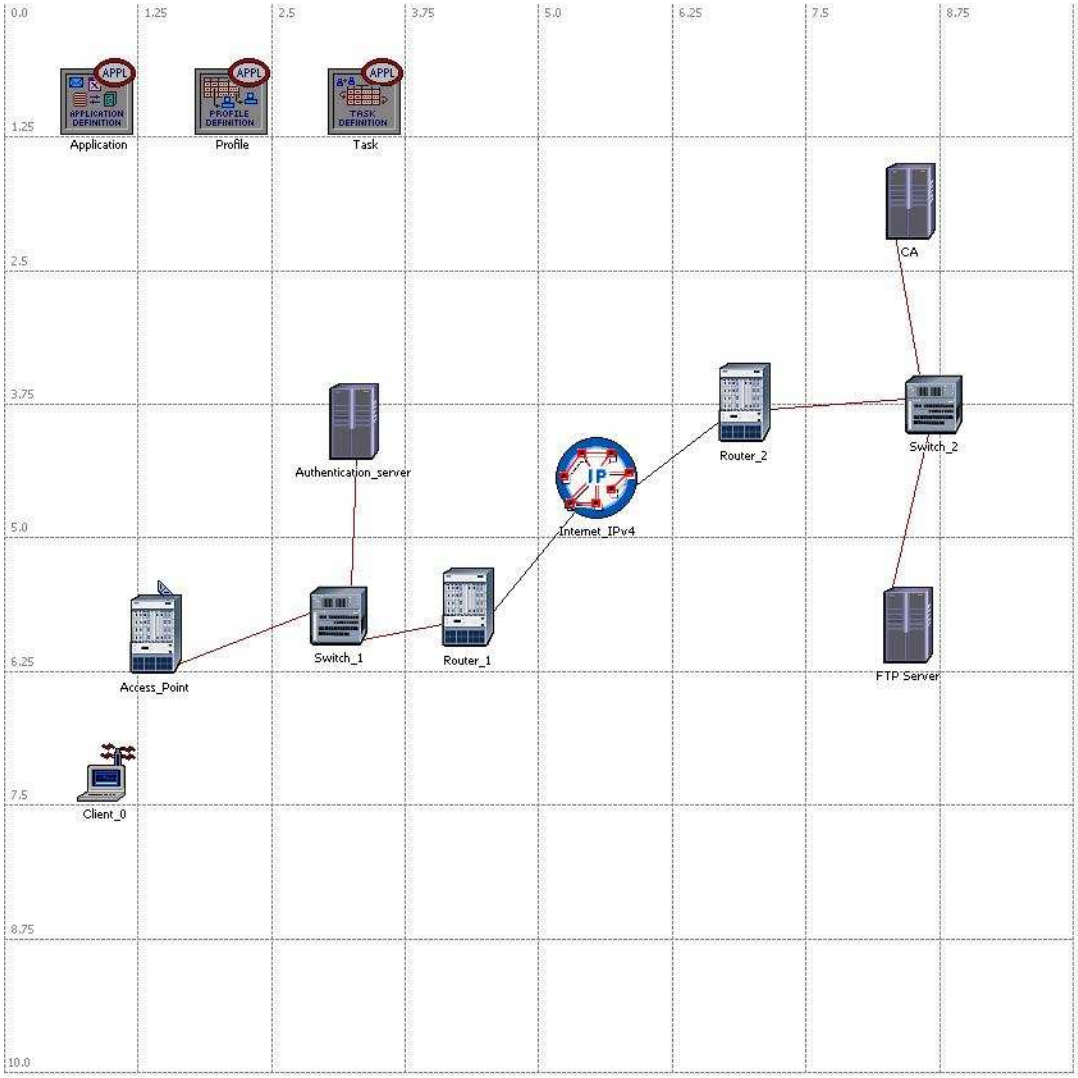


그림 14. EAP-TLS 시뮬레이션 구성도

위 그림 13, 14와 같이 무선 네트워크를 Opnet 11.0 시뮬레이터를 이용하여 설계하였으며, 이를 이용하여 기존의 EAP-TLS 인증방식과 제안한 시스템과의 비교분석을 하였다. 무선 LAN 환경은 위의 시뮬레이션 파라미터를 기반으로 시뮬레이션을 구성하였으며, 구성 모델은 Opnet 11.0에서 지원하는 무선 Network 표준 모델과 Ethernet 영역의 표준 모델을 사용하였으며, Application 영역에서는 시뮬레이

션 파라미터 값을 적용하여 기존의 EAP-TLS 모델과 제안 시스템 모델을 시뮬레이션하여 아래 그림과 같은 결과를 얻었다.

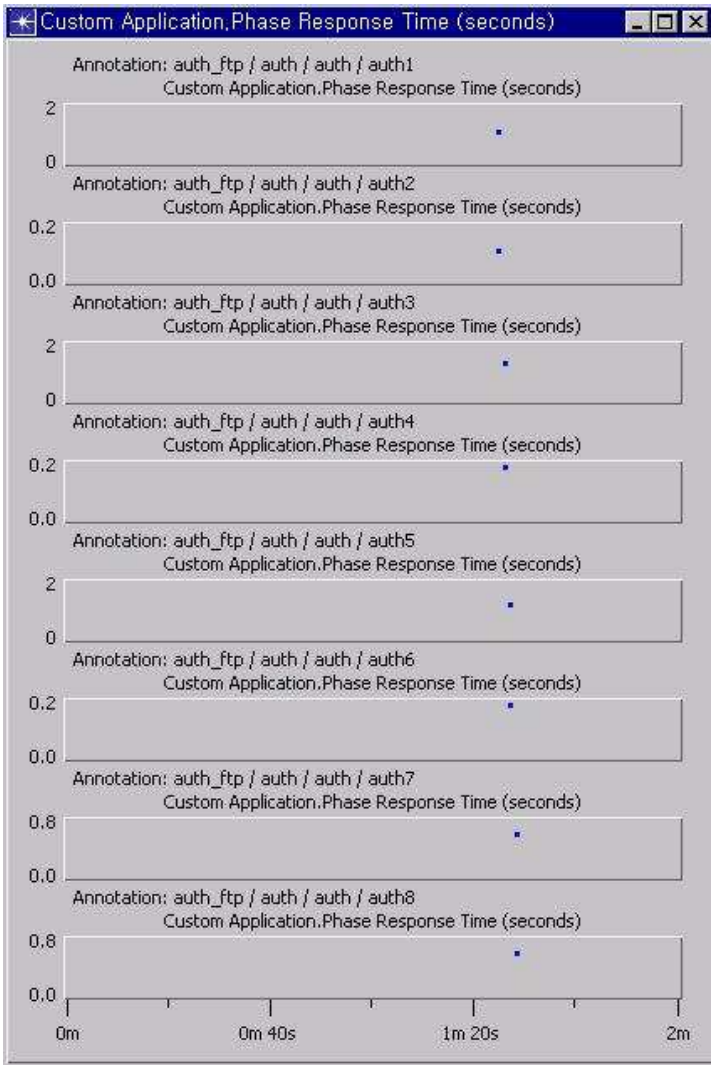


그림 15. EAP-TLS 각 단계별 응답시간

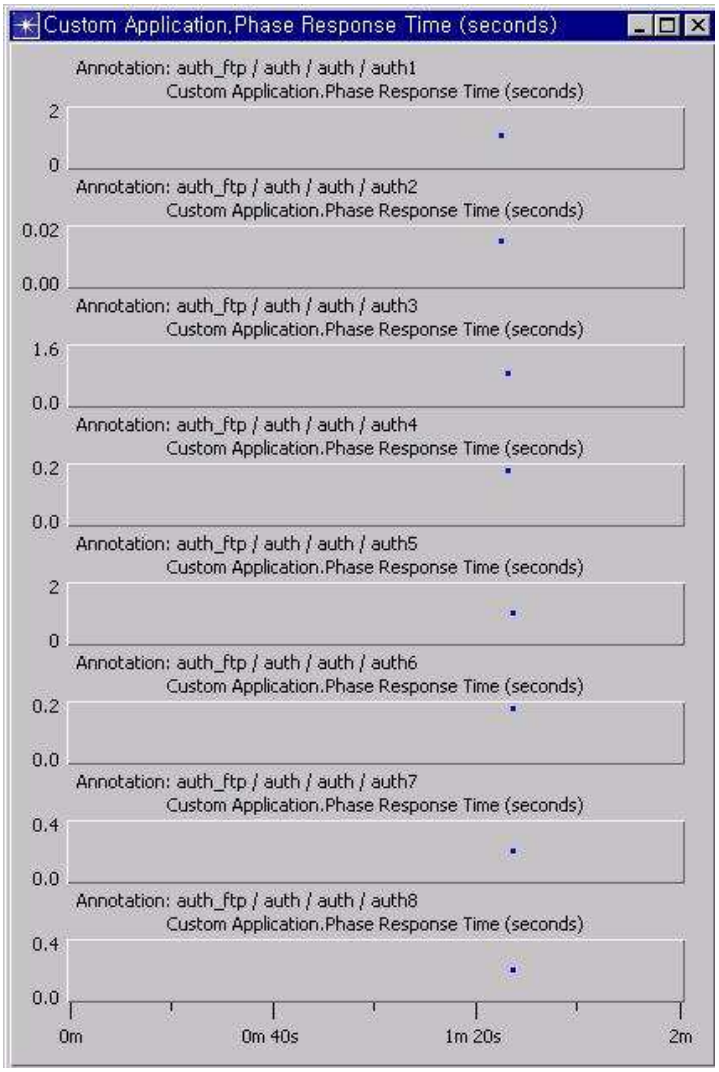


그림 16. 제안 시스템 각 단계별 응답시간

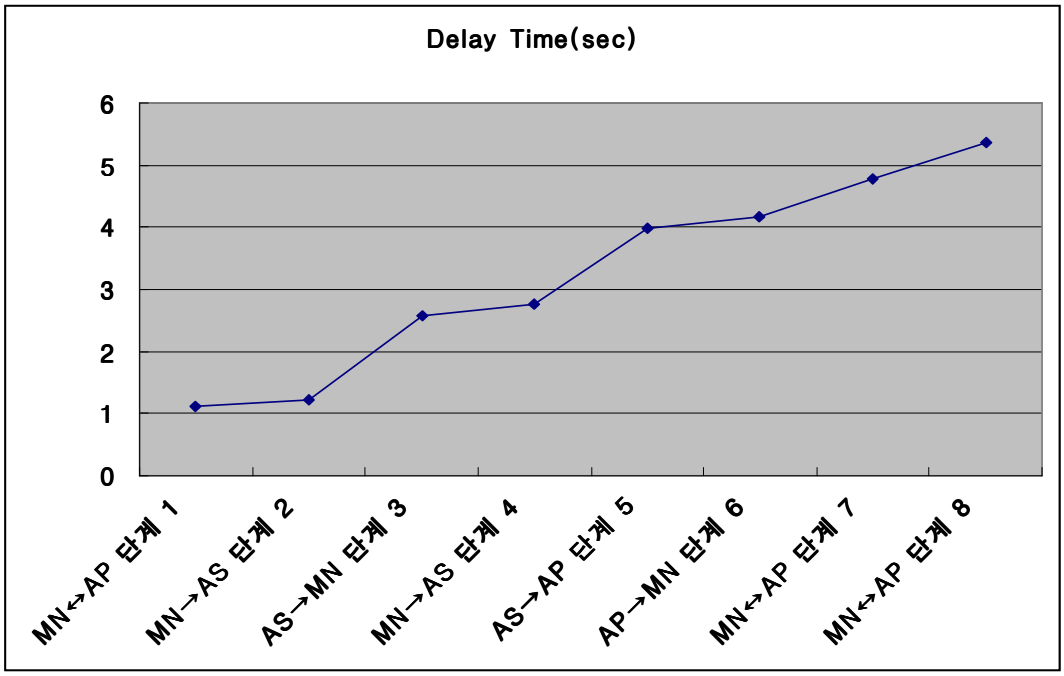


그림 17. EAP-TLS 각 단계별 시뮬레이션 결과

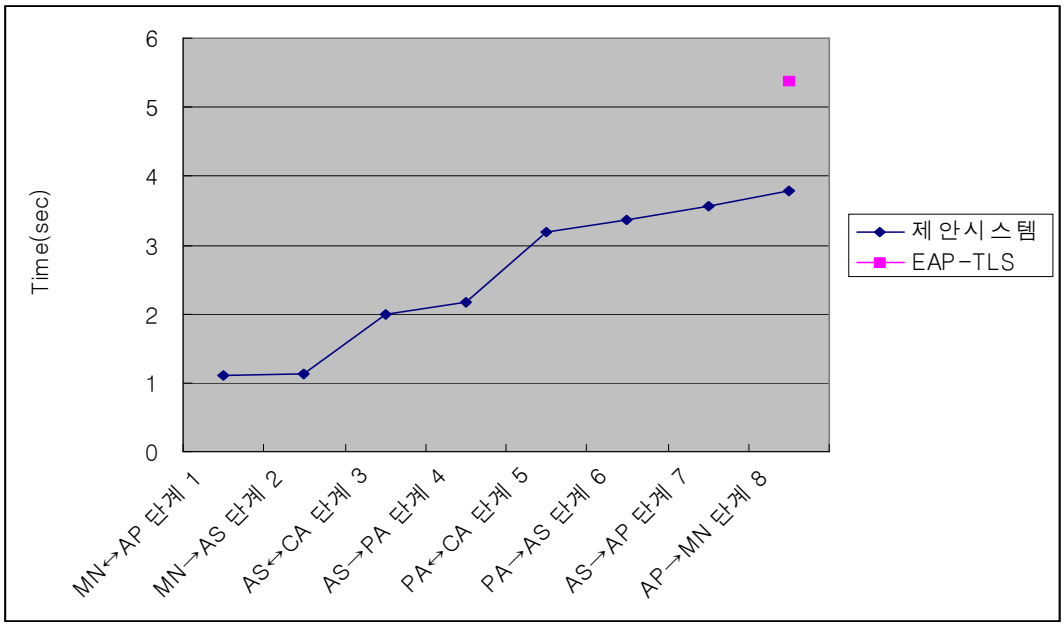


그림 18. 제안 시스템 각 단계별 시뮬레이션 결과

위 그림 15, 16은 EAP-TLS의 인증에 걸리는 시간을 각 단계별로 나누어서 시뮬레이션한 결과를 나타내고 있다. 제안 시스템과 비교하기 위하여 4Way 핸드쉐이크 단계는 간략화하여 마지막 MN↔AP, MN↔AP의 구간에서 나타내었다. 위 시뮬레이션 결과에서 보듯이 MN→AS구간과 AS→AP 단계에서 1sec 이상의 시간이 지연됨을 볼 수 있다. 이는 MN과 AS에서 상호인증에 필요한 데이터를 주고받는데 필요한 시간을 나타내고 있다. 이는 MN과 AS사이에 무선망이 존재하며, 정보의 처리량의 제한된 모바일기기가 인증서를 처리하는 과정에서 응답시간이 현저히 증가함을 알 수 있다. 따라서 본 논문에서는 클라이언트측에서 사용되는 모바일 기기의 처리량과 인증시 속도가 느린 무선망을 사용함으로써 발생되는 지연시간을 줄여보고자 대리인증서버를 사용한 상호인증 시스템을 제안하여 위 그림 17, 18과 같이 시뮬레이션 결과를 얻었다.

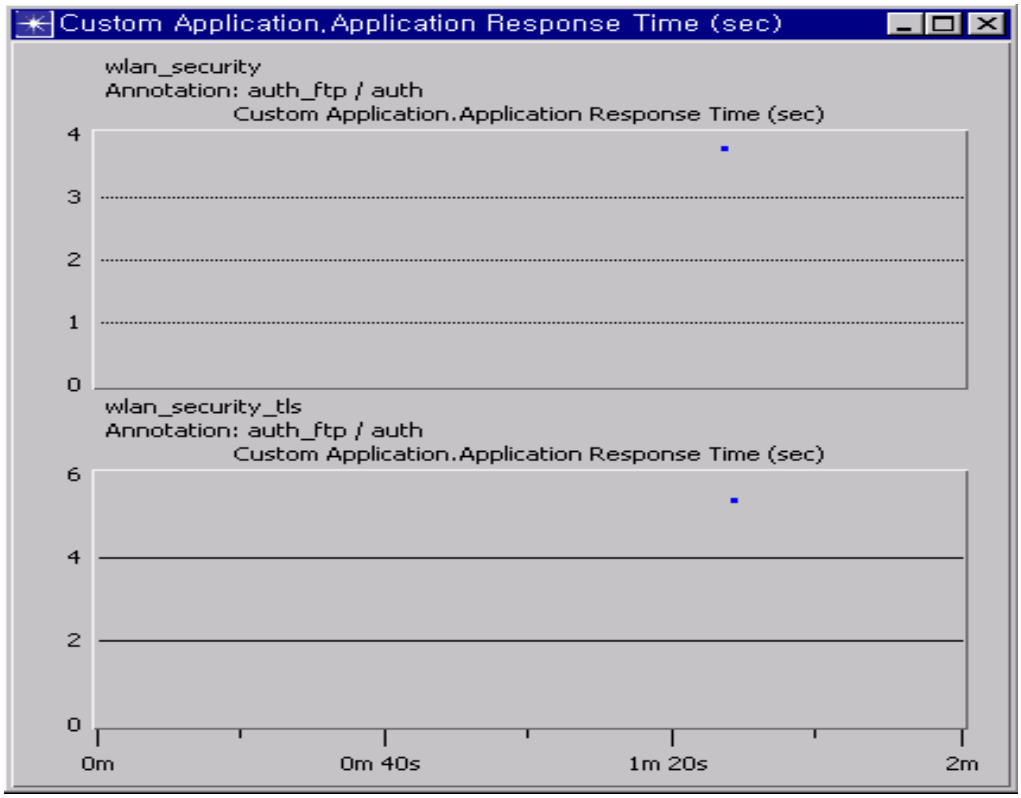


그림 19. 제안 시스템과 EAP-TLS의 인증 응답시간

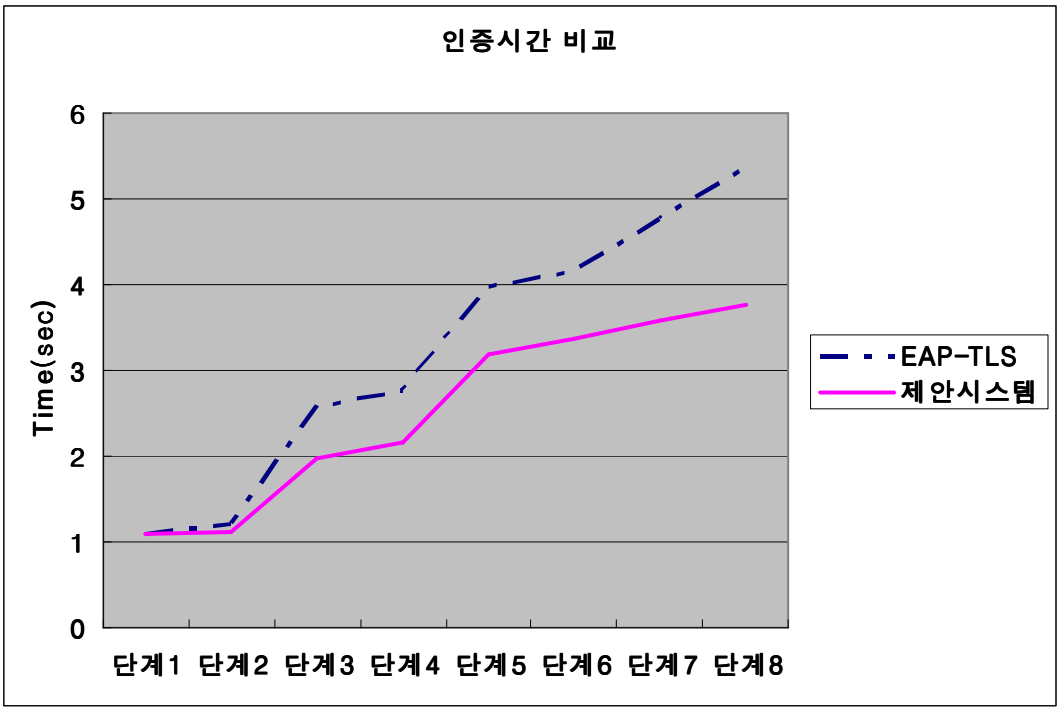


그림 20. 제안 시스템과 EAP-TLS의 시뮬레이션 결과

위 그림 17, 18에서는 본 논문에서 제안한 시스템에 대한 각 단계별 시뮬레이션 결과를 나타내고 있다. 기존의 EAP-TLS방식에 비하여 1.6sec 정도 단축된 인증시간을 위 시뮬레이션 결과에서 확인할 수 있다. 이는 제안한 인증 시스템에서 추가된 대리인증서버가 무선 클라이언트를 대신하여 인증서버를 인증함으로써 인증시간은 단축 되었다. 이와 더불어 새롭게 추가된 대리인증서버 때문에 발생되는 유선망에서의 트래픽과 로컬망에서의 추가된 대리인증서버로 인한 망 구축비용의 증가는 무선망을 구축하려는 사업자측면에서는 부담이 될 수 있다.

하지만, 향후 무선망을 사용하는 사용자들이 급속도로 증가한다면 보안에 대한 요구사항이 늘어날 것이고, 또한 다양한 무선 단말들이 사용될 기존의 인증 시스템으로는 많은 가입자를 수용할 경우 무선망에서의 트래픽은 제안시스템에서보다 현저히 증가된다. 그리고, 단말 또한 소형 무선단말의 경우 인증을 위한 지연시간은

더욱더 증가 될 것이다.

따라서, 위 시뮬레이션 결과에서와 같이 본 논문에서 제안한 시스템을 이용한다면 한정된 무선망에서 단말의 인증에 관련된 트래픽을 줄여줌으로써 같은 무선 네트워크를 이용하는 다른 단말이 인터넷을 사용함에 있어서 여유를 줄 수 있다. 이렇게 무선망에서 줄어든 트래픽을 유선망에서 대역폭을 좀 더 확보한다면 오히려 보다 적은 비용으로 무선 가입자를 확보 할 수 있을 것이며, 대리인증서버의 사용으로 인하여 인증서 처리에 대한 부담이 줄어들어 다양한 무선 단말이 무선망을 사용가능하다면 대리인증서버의 추가는 많은 가입자를 확보할 수 있는 방법이 될 수 있다.

또한 무선망에서 접속을 시도하는 클라이언트는 최종적으로 한번의 핸드쉐이크 과정을 거쳐 인증서버와 상호인증을 완료함과 동시에 기존의 CRL방식의 인증서 검증방식이 아닌 CVS를 사용함으로써 실시간 인증을 동시에 수행 가능한 시스템을 본 논문에서 제안하였다. 이는 향후 인증과 관련하여 실시간 인증의 중요서은 더욱더 커질 것이므로 이에 대한 대비 또한 함께 이루어 질 수 있다.

제5장 결 론

무선랜에서 인증서의 유효성을 검증하기 위해 CRL을 이용할 경우 시간차 문제 때문에 실시간으로 그 유효성을 검증할 수 없으며 OCSP를 이용할 경우 규모가 큰 보인시스템에서는 인증서버로부터 승인받기 전에는 유선랜으로 접근이 허용되지 않기 때문에 인증서버를 실시간으로 인증할 수 없다. 그리고, 기존의 인증 방식의 문제점을 해결하기 위하여 IEEE 802.1x를 이용한 PKI 인증방식이 많이 사용되고 있다. 하지만 이러한 인증방식 또한 상호인증과 관련하여 현재까지 EAP-TLS를 제외하고는 인증 요청자와 인증서버 사이에 공인 인증서를 사용하는 인증 프로토콜은 없는 실정이다.

이러한 이유 때문에 본 논문에서는 인증 경로 검사와 인증서 검증을 CA와 직접 접속하여 처리하는 CVS를 이용하였다. 이에따라 인증서 폐지 정보를 실시간으로 파악할 수 있어 인증서 유효성 검증 결과 값의 현재성을 얻을 수 있었고 각 CVS에 인증서 유효성 검증 업무를 분산시킴으로써 다중 CA 환경에서 특정 검증기관에 부하가 집중되는 것을 막을 수 있다. EAP-TLS의 경우 상호 인증도 가능하고 공인 인증서를 사용함으로써 공인된 인증방식이라 할 수 있지만, 인증상태에 대한 현재성에 있어서는 아직 명확히 해결되지 못하는 문제점이 있다.

따라서 본 논문에서 제안하는 방식인 대리 인증 서버를 이용함으로써 인증, 안전성, 효율성 측면에서 기존 시스템의 문제점이 개선 되었음을 분석하였고, Opnet 11.0를 이용한 시뮬레이션 결과에서 볼 수 있듯이 성능 또한 기존의 EAP-TLS의 인증 대기 시간보다 1.6sec 이상 시간을 단축 시켰음을 볼 수 있다. 향후 무선 LAN이 전국에 보급되어 많은 사람들이 무선 인터넷을 안전하게 사용될 것은 분명한 사실이다. 하지만 보안이 허술한 현재의 무선 인터넷의 문제점을 극복하고 많은 사람이 안전하게 무선망에 접속할 때 보다 빠르고 안전한 인증방식의 필요성은 대단히 중요하다고 볼 수 있다. 이에 본 논문에서는 향후 무선 LAN 사용자가 많아지고, 보안에 대한 인식이 보편화 되었을 때, 효과적으로 적용이 가능한 인증 프로토콜 설계에 있어서 많은 참고 사항이 될 것이다.

참고 문헌

[1] S. K. Miller, "facing the challenge of wireless security," Computer.org, pp.16-18, 2001.

[2] S. Rommer, " Security Issue in Public Access WLAN Architectures," Ericsson Telecom Report, March, 2002

[3] "IEEE 802.11b Wireless LAN Medium Access Control (MAC) Physical Layer (PHY) Specification", IEEE Standard 802.11b, 1999.

[4] W. A. Arbaugh, "Your 802.11 Wireless Network has No Clothes", University of Maryland, Mar. 2001

[5] L. Blunk, J. Vollbrecht, "PPP Extensible Authentication Protocol (EAP)", IETF RFC 2284, Mar. 1998.

[6] R. Housley, W. Ford, W. Pork, D. Solo, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", IETF RFC 3280, Apr. 2002

[7] M. Myers, R. Ankney, A. Malpani, S. Galperin, C. Adams, "X.509 Public Key Infrastructure : Online Certificate Status Protocol - OCSP", IETF RFC 2560, Jun. 1999.

[8] R. Rivest, "The MD5 Message-Digest Algorithm," IETF RFC 1321, April. 1992.

[9] C. Rigney, "Remote Authentication Dial In User Service(RADIUS)," IETF RFC 2865, June. 2000.

[10] Secure Authentication, Access Control, and Data Privacy on Wireless LAN, http://www.funk.com/RADIUS/wlan/wlan_solns.sap, Funk software

[11] IEEE Draft P802.1x/D11, "standard for Port based Network Access Control," IEEE, Mar. 2001.

[12] L. Blunk, "PPP Extensible Authentication Protocol," IETF RFC 2284, Mar. 1998.

[13] T. Dierks, "The TLS Protocol Version 1.0," IETF RFC 2246, Jan. 1999.

[14] C. Adams, S. Farrell, "Internet X.509 Public Key Infrastructure Certificate Management Protocols", IETF Draft, Feb. 2001.

[15] R. Housley, W. Ford, W. Pork, D. Solo., " Internet X.509 Public Key Infrastructure Certificate and CRL Profile", IETF RFC 3280, Apr. 2002

[16] D. Pinkas, "Delegated Path Validation and Delegated Path Discovery Protocols", IETF Draft, draft-ietf-pkix-dpvdpd-00.txt, Jul. 2001

저작물 이용 허락서

학 과	정보통신	학 번	20047624	과 정	석사
성 명	한글: 신 승 욱 한문 : 辛 承 旭 영문 : Seung-wook Shin				
주 소	광주광역시 북구 두암동 329번지 반석힐라 209호				
연락처	E-MAIL : swookgi@naver.com				
논문제목	한글 : 무선 LAN에서 핸드오프시 PKI방식을 이용한 실시간 상호 인증 기법 설계				
	영문 : Design of Realtime Interactive Authentication Method Using PKI during Handoff Time in the Wireless Network				

본인이 저작한 위의 저작물에 대하여 다음과 같은 조건아래 조선대학교가 저작물을 이용할 수 있도록 허락하고 동의합니다.

- 다 음 -

1. 저작물의 DB구축 및 인터넷을 포함한 정보통신망에의 공개를 위한 저작물의 복제, 기억장치에의 저장, 전송 등을 허락함
2. 위의 목적을 위하여 필요한 범위 내에서의 편집·형식상의 변경을 허락함. 다만, 저작물의 내용변경은 금지함.
3. 배포·전송된 저작물의 영리적 목적을 위한 복제, 저장, 전송 등은 금지함.
4. 저작물에 대한 이용기간은 5년으로 하고, 기간종료 3개월 이내에 별도의 의사 표시가 없을 경우에는 저작물의 이용기간을 계속 연장함.
5. 해당 저작물의 저작권을 타인에게 양도하거나 또는 출판을 허락을 하였을 경우에는 1개월 이내에 대학에 이를 통보함.
6. 조선대학교는 저작물의 이용허락 이후 해당 저작물로 인하여 발생하는 타인에 의한 권리 침해에 대하여 일체의 법적 책임을 지지 않음
7. 소속대학의 협정기관에 저작물의 제공 및 인터넷 등 정보통신망을 이용한 저작물의 전송·출력을 허락함.

동의여부 : 동의( ) 반대( )

2007년 2월 23일

저작자: 신 승 욱 (서명 또는 인)

조선대학교 총장 귀하