韓國 컴퓨터情報學會 論文誌
第10卷 第5號, 2005. 11.

2005-10-5-2-7

실시간 상호인증 지원을 위한 무선랜 보안시스템에 관한 연구

이 상 렬*

A Study of Wireless LAN Cryptosystem for Supporting Realtime Mutual Authentication

Sang-Ryul Lee*

요 약

인증서의 유효성을 검증하기 위해 CRL(Certificate Revocation List)을 이용할 경우 시간차 문제 때문에 실시간으로 그 유효성을 검증할 수 없으며 OCSP(Online Certificate Status Protocol)를 이용할 경우 규모가 큰 보안시스템에서는 검증서버에 과부하를 주는 문제가 있다. 그리고 IEEE 802.1x 무선랜 표준에서는 클라이언트가 인증서버로부터 승인받기 전에는 유선랜으로의 접근이 허용되지 않기 때문에 인증서버를 실시간으로 인증할 수 없다. 본 논문에서는 이러한 문제점들을 해결하기 위하여 무선랜에서 통신 내용을 보호하고 통신자 간의 신원을 상호 실시간으로 확인할 수 있는 보안시스템을 설계하였다. 설계된 인증서 검증 프로토콜은 검증 결과의 현재성은 물론 시스템의 높은 안전성과 효율성을 보여주었으며 인증서의 유효성 검증 속도도 시스템의 규모와 상관없이 항상 일정하며 사용자가 신뢰하고 있어야 할 기관의 수도 적고 검증서버의 과부하도 막을 수 있었다. 그리고 고속 고용량과 저속 저용량의 클라이언트에 적합한 사용자 인증 및 키 교환 프로토콜은 실시간 상호 인증은 물론 인증 사실의 공인을 가능하게 하였다.

Abstract

The Certificate Revocation List(CRL) or the Online Certificate Status Protocol(OCSP) has been used to validate certificates. However, the CRL cannot validate certificates in realtime because of the Time-Gap problem and the OCSP server overloads in a large scale secure system. In addition, the client cannot access a wired LAN until the client has been authenticated by the authentication server on the IEEE 802.1x framework. Therefore, the client cannot validate the authentication server's certificate using a certificate validation server. Thus, the client cannot authenticate the authentication server in realtime. To solve these problems this paper designed a secure system that can protect the content of communications and authenticate users in realtime on a wireless LAN. The designed certificate validation protocol was proved that the stability and efficiency of the system was very high, the result of the validation had the presence, the speed of the validation was not affected by the system scale, the number of authorities user must trust was reduced to one, and the overload of the validation server was protected. And the designed user authentication and key exchange protocols were proved that the mutual authentication was possible in realtime and the fact of the authentication could be authorized by the CA because of using the authorized certificates.

▸ Keyword : 무선랜(wireless LAN), 상호인증(mutual authentication), 공개키 기반구조(public key infrastructure)

• 제1저자 : 이상렬
• 접수일 : 2005.10.08, 심사완료일 : 2005.11.09
* 상지영서대학 인터넷정보과 교수

Ⅰ. 서 론

무선랜은 전송 매체로 전파를 이용하기 때문에 보안상 유선보다 도청 및 변조가 쉽게 이루어질 수 있다. 따라서 무선랜 사용자는 무선 구간에서 전송 데이터의 기밀성이 유지되길 원하며 무선랜 사업자는 승인된 사용자만이 무선랜을 이용할 수 있길 원한다. IEEE 802.11b에서는 이러한 사용자 인증 및 기밀성을 위하여 SSID(Service Set Identifier), MAC(Media Access Control) 주소 그리고 WEP(Wired Equivalent Privacy)키를 이용[1]하고 있으나 IEEE 802.11b 보안 메커니즘에는 이미 많은 취약점들이 알려져 있다.[2] 이러한 취약점들을 보완하고자 고안된 것이 IEEE 802.1x EAP(Extensible Authentication Protocol)[3]이다. 여기서는 해쉬 함수를 이용한 챌린지(Challenge)/응답(Response), 인증서를 기반으로 하는 TLS(Transport Layer Security)[4], One-Time Password 등과 같은 다양한 사용자 인증 메커니즘이 이용되고 있다.

비대칭키 암호방식[5]을 이용하는 PKI(Public Key Infrastructure) 보안시스템에서 인증서 유효성 검증을 위하여 CRL(Certificate Revocation List)[6]을 이용하는 경우는 인증서 폐지 목록이 일정한 주기로 변경되기 때문에 인증서의 유효성을 정확히 검증할 수 없다는 문제가 있다. 그리고 OCSP(Online Certificate Status Protocol)[7] 서버를 이용하는 경우는 인증서의 유효성을 실시간으로 정확히 검증할 수 있다는 장점은 있으나 보안시스템의 규모가 커질 경우 서버에 부하가 집중되어 실시간 서비스 제공이 힘들어지고 또한 서버에 장애가 발생될 경우에는 보안시스템의 모든 사용자가 서비스를 제공받을 수 없게 된다.

무선랜을 이용하려는 클라이언트는 RADIUS[8] 또는 Diameter[9] 등과 같은 인증서버의 인증서를 검증하기 위하여 네트워크로부터 CRL을 전송받거나 OCSP와 같은 인증서 검증서버에 접속해야 하는데 포트 기반 접근제어 방식[10]을 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 CA(Certification Authority)들이 계층적 다중구조로 구성된 대규모 보안시스템에서 인증서의 유효성 검증을 빠르고 정확히 할 수 있으며 특정 검증서버에 부하를 집중시키지 않음으로써 검증시스템의 안정화를 이룰 수 있는 방법을 연구하고 클라이언트가 인증서버의 인증서를 실시간으로 검증할 수 있는 방법을 연구함으로써 클라이언트와 인증서버 간의 상호 인증을 실시간으로 할 수 있는 보안시스템을 설계하고자 한다.

Ⅱ. 관련 연구

인증서 유효성을 검증하는 방법들의 특징과 장단점을 파악하고 IEEE 802.1x를 이용한 다양한 EAP 인증유형의 특징과 문제점을 분석한다.

2.1 인증서 검증 방법

인증서 상태 검증 방법 중에서 그동안 많이 이용되어온 CRL과 OCSP를 이용한 검증 방법에 대하여 각각 특징 및 장단점을 알아본다.

2.1.1 CRL 이용 방식

CRL은 인증서의 폐지 여부를 확인할 수 있는 가장 일반적인 방법으로서 CA가 인증서 폐지 목록을 보통 하루에 한두 번 정도로 주기적으로 생성하여 디렉토리에 게시한다. 인증서 상태를 확인하고자 하는 자는 이 디렉토리로부터 CRL을 다운로드 하여 검사한다.

CRL, Delta-CRL[11] 그리고 간접 CRL 방식 모두가 인증서 폐지 목록이 일정한 주기로 갱신되기 때문에 인증서의 현재 상태에 대한 시간차(Time-Gap) 문제가 발생하여 완벽한 실시간성을 제공해줄 수가 없다. 또한 CRL과 Delta-CRL 방식은 사용자 자신이 인증서 폐지 목록을 직접 비교하여 수신한 인증서의 인증 여부를 판단하기 때문에 자신의 판단 착오로 인하여 발생한 문제에 대해 향후 법적인 보호를 받을 수 없다는 단점이 있다. 그리고 IETF의 RFC 3280[6]에서는 다중 CA 시스템에서 활용할 수 있는 인증 경로 검증 절차를 제시하고 있으나 이는 인증 경로 상의 모든 인증서를 순차적으로 검증하는 방식이어서 인증 경로가 긴 경우 인증서 검증에 많은 부하가 걸릴 것이다.

2.1.2 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 전자서명된 상태 결과를 클라이언트에게 보내준다. Internet Draft OCSP v2는 구체적인 동작을 정의하고 있지 않으며 클라이언트와 서버 간에 교환되는 메시지 구성과 형태만을 정의하고 있다.[12]

OCSP 서비스 또한 CRL 방식을 완전히 배제하고 있지 못하기 때문에 요청과 응답에 있어서 응답 메시지의 현재성에 문제가 있을 수 있다. 그리고 다중 CA 구조의 대규모 시스템에서 OCSP 서버를 이용할 경우 모든 클라이언트들이 집중적으로 OCSP 서버에 접속할 것임으로 실시간 서비스 제공이 어려워질 수 있는 문제가 있다.

2.2 EAP 인증유형

다음은 IEEE 802.1x에서 많이 이용되는 인증유형들의 특징, 인증 프로토콜 그리고 문제점들에 대하여 살펴본다.

2.2.1 EAP-MD5

EAP-MD5는 가장 초기의 EAP 인증방식으로 IEEE 802.1x 프레임워크에서 기본 수준의 EAP를 지원하는 대표적인 EAP 인증방식이다.

EAP-MD5에서는 인증을 위하여 사용자 이름과 패스워드가 전송되는데 사용자 이름은 암호화되지 않은 상태로 그리고 패스워드는 MD5로 해쉬되어 전송된다. 이 방식은 인증서버는 클라이언트를 인증할 수 있으나 클라이언트가 인증서버를 인증할 수 없다는 단점이 있다. 즉 단방향 인증만 가능하며 공인인증서를 이용하지 않기 때문에 공인된 인증이 아니다.

2.2.2 EAP-TLS

EAP-TLS[13]는 Windows XP에서 IEEE 802.1x 단말에 사용되는 보안 메커니즘으로서 TLS 핸드쉐이크를 EAP 프로토콜로 확장한 인증방식이다.

EAP-TLS는 클라이언트와 인증서버 모두 상대방 인증이 가능하여 양방향 인증이 가능하며 공인된 인증이다. 그러나 클라이언트는 인증 절차가 완료되기 전에는 네트워크를 이용할 수 없기 때문에 네트워크로부터 CRL을 수령하거나 OCSP 서버에게 인증서 유효성 검증을 요청할 수 없다. 따라서 클라이언트는 인증서버를 실시간으로 인증할 수 없다는 문제점이 있다.

2.2.3 PEAP

PEAP(Protected EAP)는 Microsoft와 Cisco에서 지원하는 인증방식으로 서버 인증은 PKI의 인증서를 이용하고 클라이언트 인증은 MD5-챌린지, GTC, OTP와 같은 단방향 인증방식을 이용한다.

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

III. 제안 시스템

제안하고자하는 시스템이 달성해야만 하는 목표 요구조건과 이 목표 요구조건의 만족 여부를 검증할 수 있는 방법을 제시한다. 그리고 목표 요구조건을 만족시킬 수 있는 공개키 기반 무선랜 보안시스템의 기본 구성을 제시하고 이러한 보안시스템 환경 하에서 인증서 유효성 검증을 효율적으로 처리할 수 있는 검증 절차를 제시하며 끝으로 클라이언트의 두 가지 서로 다른 환경 하에서 실시간으로 상호 인증이 가능하며 인증 사실을 공인받을 수 있는 인증 프로토콜을 각각 제시한다.

3.1 제안 시스템의 목표 요구조건 및 검증 방법

제안 시스템이 기본적으로 갖추고 있는 환경 조건을 기술하고 제안 시스템이 달성해야하는 구체적인 목표 요구조건과 이의 만족 여부에 대한 검증 방법에 대하여 기술한다.

3.1.1 제안 시스템의 환경 조건

제안 시스템은 포트 기반 접근제어 방식의 IEEE 802.1x 프레임워크 상에서 공개키 기반구조의 암호시스템을 이용하고 인증서 발급 및 관리를 담당하는 인증기관이 다중으로 설치되어 있는 경우로 가정한다.

3.1.2 제안 시스템의 목표 요구조건

제안하고자하는 보안시스템은 다음과 같은 네 가지 기능적인 요구조건을 만족시키는 것을 목표로 하고 있다.

- 요건1 : 클라이언트와 인증서버 사이에 상호 인증이 가능하여야 한다.

- 요건2 : 클라이언트와 인증서버는 상호간을 실시간으로 인증할 수 있어야 한다.
- 요건3 : 인증 사실은 공인받을 수 있어야 한다.
- 요건4 : 인증 단계에서의 통신 내용과 클라이언트와 AP 사이의 무선 구간에서의 통신 내용은 보안이 유지되어야 한다.

그리고 이러한 기능적인 요구조건을 만족시킴과 동시에 다음과 같은 세 가지 성능적인 요구조건도 동시에 만족시키는 것을 목표로 한다.

- 요건5 : 인증서 검증방법에 있어 시스템의 효율성과 안전성이 저하되지 않아야 하며 검증 속도도 느려져지지 않아야 하며 신뢰해야할 기관의 수도 많아지지 않아야 한다.
- 요건6 : 인증 프로토콜의 효율성을 유지하기 위해서는 핸드쉐이크 횟수가 증대되지 않아야 한다.
- 요건7 : 과다한 암호연산으로 인하여 클라이언트의 부하가 증대되지 않아야 한다.

3.1.3 요구조건에 대한 검증 방법

<표 1>에서는 제안한 시스템이 목표 요구조건을 만족하는지를 검증할 수 있는 방법을 제시하고 있다.

표 1. 요구조건에 대한 검증 방법
Table 1. Verification methods about requirements.

요구조건		검증 방법
기능면	요건1	클라이언트가 인증서버를 인증하고 인증서버가 클라이언트를 인증하는지를 검증한다.
	요건2	인증서 유효성 검증을 실시간으로 할 수 있으며 인증서 유효성 검증 결과의 현재성을 보장할 수 있는지를 확인한다.
	요건3	공인된 인증서를 이용하여 사용자 인증을 할 경우 인증 사실을 공인받을 수 있음으로 공인된 인증서 사용 여부를 확인한다.
	요건4	인증 프로토콜에서 전송 단계별로 전송되는 내용이 안전하게 전달되는지를 확인하며 클라이언트와 AP 사이의 WEP키가 안전하게 교환되는지를 검증한다.
성능면	요건5	인증서 유효성 검증을 위하여 조회해야할 횟수와 특정 검증 기관의 파괴가 시스템에 미치는 영향을 조사하고 시스템의 규모가 커짐에 따라 검증 속도의 변화를 파악하고 사용자가 시스템 내에서 신뢰하고 있어야 기관의 수는 얼마나 되는지를 파악한다.
	요건6	인증 프로토콜의 구간별 통신횟수 및 전체 통신횟수를 조사한다.
	요건7	인증 프로토콜이 완료될 때까지 클라이언트가 암호연산을 하기 위해 소요되는 시간을 조사한다.

3.2 제안 시스템의 구성

제안하는 PKI 무선랜 보안시스템의 주요 구성 요소는 인증 요청자인 MS(Mobile Station), 인증자인 AP, 인증서버인 AS, MS의 사용자 대리인인 UA(User Agent) 그리고 인증서 발급 및 관리 기관인 CA로 구성된다. CA에는 인증서의 유효성을 검증하는 서버 CVS(Certificate Validation Server)를 포함하며 UA는 MS의 인증서를 보관하고 AS가 MS를 인증할 때 MS를 대신하여 인증 과정을 수행한다. 또한 UA는 MS를 대신하여 AS를 인증한다. (그림 1)은 제안하는 보안시스템의 구성도를 보여준다.

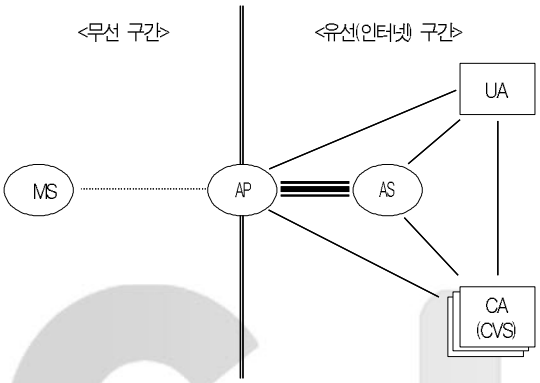

그림 1. 제안 시스템의 구성
Fig. 1. Architecture of the suggested system.

3.3 인증서 검증 절차

본 논문에서는 인증서를 검증하기 위하여 CRL을 이용하지도 않고 OCSP 서버와 같은 별도의 기관을 두지 않고 CA를 직접 이용하도록 한다. CA가 CRL을 생성 관리하거나 OCSP 서버에 응답하는 동작을 하지 않기 때문에 궁극적으로 CA의 부담을 증가시키지 않으면서 CRL이나 OCSP 서버를 이용할 때의 단점을 해소할 수 있다.

서로 다른 CA로부터 발급받은 인증서를 검증하기 위해서는 먼저 상대방의 CA를 자신의 CA가 인증해준 후에 상대방의 CA로부터 인증서의 유효성 검증을 요청한다. 모든 사용자가 복잡한 CA 계층구조를 알고 있다면 인증서 발급 CA의 인증 여부를 즉시 알 수 있지만 항상 새로운 CA 계층구조를 모든 사용자가 알고 있기란 사실상 불가능하다. 본 논문에서 제안하는 시스템에서는 사용자들의 편의를 위하여 자신의 인증서를 발급한 CA만을 신뢰하고 있다고 가정한다. 따라서 자신이 신뢰하는 CA에서 발급한 다른 인증

서들은 CA의 인증 여부를 질의할 필요가 없으나 그 밖의 CA들에 대해서는 자신이 신뢰하는 CA에게 CA의 인증 여부를 질의해야 한다. 자신이 신뢰하는 CA가 인증서 발급 CA의 인증 여부를 결정하기 위해서는 인증서 내부에 인증경로를 포함하고 있어야 인증 여부를 결정하기 쉽다. 따라서 CA가 인증서를 발급할 때 반드시 인증서 내부에 인증경로를 포함시킨다. 만일 인증서 발급처만 있고 인증경로가 포함되어 있지 않을 경우에는 CA 계층구조 상에서 두 사용자 간의 경로 사이에 CA가 n개 있다면 인증서 검증을 위한 총 검증 요청 수는 n + Σ(각 CA들의 하위 CA 개수) 가 되어 인증서 검증을 위해서 시스템에 매우 큰 부담을 줄 것이다.

따라서 모든 CA는 최상위 루트 CA로부터의 인증경로를 보관하고 있어야 하며 경로 변경 시에는 즉시 하위 CA들에게 이를 통보하여야 한다. 이럴 경우 자신이 신뢰하는 CA에게 한 번만 질의하면 인증서 발급 CA의 인증 여부를 알 수 있고 또한 상대방이 신뢰하는 CA에게 한 번만 질의하면 인증서의 유효성을 알 수 있다. (그림 2)는 인증서 내부에 인증경로를 포함하고 있을 경우 인증서를 검증하는 절차를 보여준다.

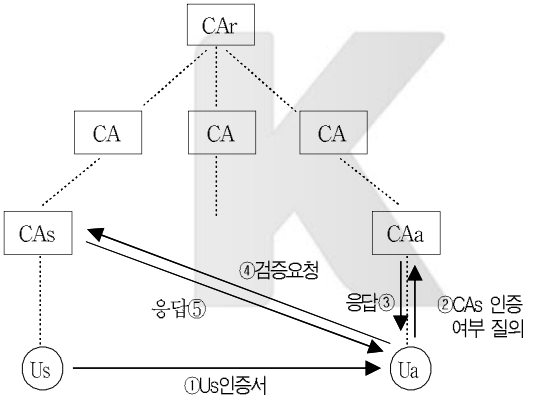

그림 2. 인증경로 포함시 검증 절차
Fig. 2. Validation procedure with certification path.

③ 응답 메시지 : {Rsp}SK_{CAa}, $Cert_{CAa}$
⑤ 응답 메시지 : {Rsp}SK_{CAs}, $Cert_{CAs}$

3.4 상호 인증 및 WEP키 교환 프로토콜

본 절에서는 CPU의 처리속도가 고속이고 자료 저장 공간이 고용량인 클라이언트와 저속이고 저용량의 클라이언트 환경 하에서 각각 실시간으로 상호 인증이 가능하며 인증 사실을 공인받을 수 있고 동시에 WEP를 안전하게 생성 분배할 수 있는 프로토콜을 제시한다. 프로토콜에서 사용되는 기호의 정의는 다음과 같다.

- C_X : CA가 사용자 X에게 발급한 공인 인증서
- S_X : 사용자 X의 비밀키로 서명한 서명문
- ID_X : 사용자 X의 ID
- K_{XY} : 사용자 X와 Y 사이의 대칭키
- $\{M\}K_{XY}$: 대칭키 K_{XY}로 메시지 M을 암호화한 암호문
- PK_X : 사용자 X의 공개키
- $\{M\}PK_X$: 사용자 X의 공개키 PK_X로 메시지 M을 암호화한 암호문
- SK_X : 사용자 X의 비밀키
- $\{M\}SK_X$: 사용자 X의 비밀키 SK_X로 메시지 M을 서명한 서명문이기도 하며 M이 사용자 X의 공개키 PK_X로 암호화한 암호문일 때 이를 복호화하는 문이기도 함

3.4.1 고속 고용량 클라이언트용(A형) 프로토콜

MS가 자신의 인증서를 보유하고 있으며 공개키 계산을 할 수 있는 경우로서 MS와 AS가 공인된 상호 인증을 수행하며 MS와 AP 간에 이용될 WEP키를 교환하는 프로토콜은 (그림 3)과 같다. 여기서 UA는 MS를 대신하여 AS를 실시간으로 공인된 인증을 해주는 역할을 한다.

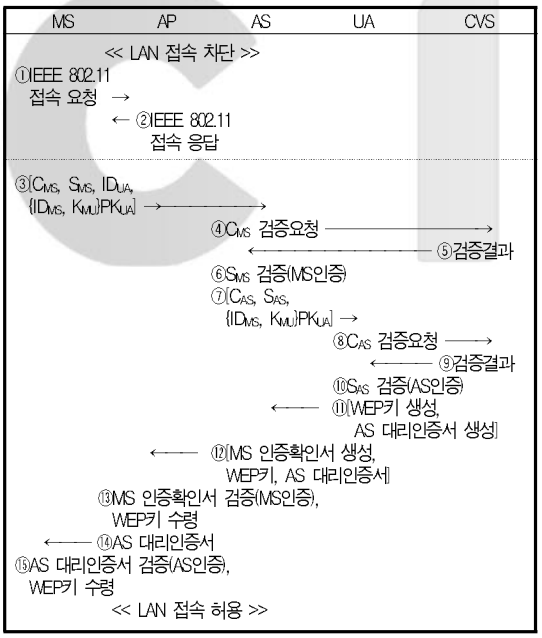

그림 3. A형 상호 인증 및 WEP키 교환 프로토콜
Fig. 3. Mutual authentication and WEP key exchange protocol in A-type system.

⑪ 전송되는 WEP키 : {WEP키}PK_{AS}
전송되는 AS 대리인증서 : {대리인증내용}K_{MU}

3.4.2 저속 저용량 클라이언트용(B형) 프로토콜

MS가 자신의 인증서를 보유하고 있지도 않으며 공개키 계산을 할 수도 없는 경우로서 유선을 통하여 MS의 사용자가 UA에게 초기화 사항을 등록해두는 등록 단계와 무선을 통하여 실제적으로 MS와 AS가 공인된 상호 인증을 수행하는 인증 단계로 나눈다. 등록 단계는 AS가 UA를 통하여 MS를 인증할 수 있도록 해주기 위함이며 인증 단계에 앞서 매번 수행하는 것이 아니고 이용 초기에 한 번만 수행하면 된다.

1) 등록 단계

MS의 사용자 U_{MS}가 서명된 위임서와 대칭키를 UA에게 등록하는 단계로서 그 프로토콜은 (그림 4)와 같다. U_{MS}는 유선 인터넷을 통하여 UA에 접속을 하며 UA는 MS가 전송한 위임서를 변조할 수 없어야 하고 K_{MU}를 안전하게 보관 관리하여야 한다.

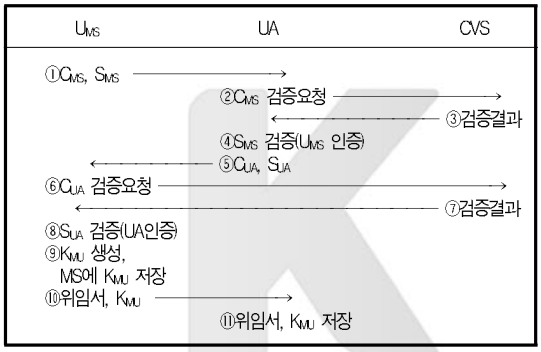

그림 4. B형 등록 프로토콜
Fig. 4. Registration protocol in B-type system.

⑩ 전송되는 위임서 : {위임내용}SK_{MS}
전송되는 K_{MU} : {K_{MU}}PK_{UA}

2) 인증 단계

MS와 AS가 공인된 상호 인증을 수행하며 MS와 AP 간에 이용될 WEP키를 교환하는 프로토콜은 (그림 5)와 같다. 여기서 UA는 MS를 대신하여 AS를 실시간으로 공인된 인증을 해주며 AS가 MS를 인증할 수 있도록 해준다.

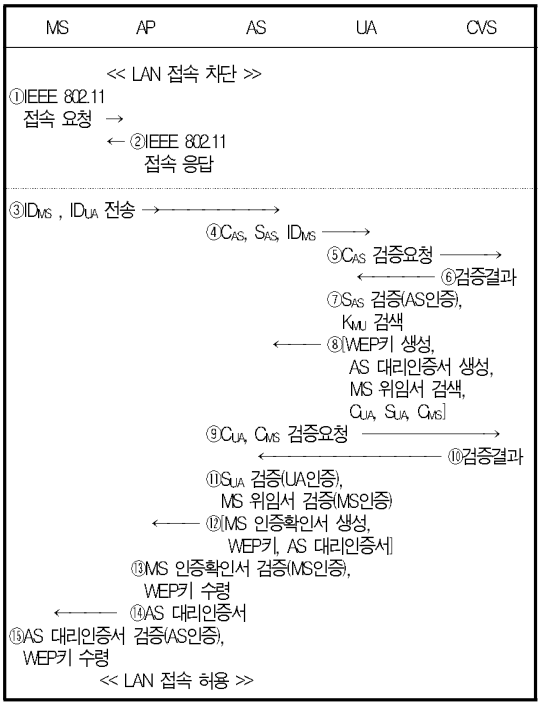

그림 5. B형 상호 인증 및 WEP키 교환 프로토콜
Fig. 5. Mutual authentication and WEP key exchange protocol in B-type system.

⑧ 전송되는 WEP키 : {WEP키}PK_{AS}
전송되는 AS 대리인증서 : {대리인증내용}K_{MU}
전송되는 MS 위임서 : {{위임내용}SK_{MS}}SK_{UA}

Ⅳ. 제안 시스템의 특성 분석

제안한 보안시스템이 목표 요구조건을 충족시키는지를 제시된 검증 방법을 이용하여 다른 프로토콜들과 비교해가며 분석해본다.

4.1 기능적인 목표 요구조건의 만족 여부 분석

기능적인 면의 목표 중에서 인증과 관련된 <요건1>, <요건2>, <요건3>은 EAP-MD5, EAP-TLS 그리고 PEAP 인증 프로토콜들과 비교해가며 만족 여부를 분석하며 보안과 관련된 <요건4>는 인증 프로토콜의 안전성과 무선구간의 안전성을 조사함으로써 만족 여부를 분석한다.

4.1.1 상호 인증 요건

EAP-MD5에서는 AS는 MS의 사설 패스워드를 이용하여 MS를 인증하지만 MS가 AS를 인증하는 프로토콜이 없어 상호 인증이 불가능하다. EAP-TLS에서는 AS와 MS가 공인인증서와 본인 서명문을 이용하여 상대방을 인증함으로 상호 인증이 가능하다. PEAP에서는 AS가 MS를 인증할 때는 사설 패스워드를 이용하고 MS가 AS를 인증할 때는 공인인증서와 본인 서명문을 이용함으로 상호 인증이 가능하다. 제안 시스템에서는 A형과 B형 모두 공인인증서와 본인 서명문 또는 위임서를 이용함으로 상호 인증이 가능하다.

4.1.2 실시간 인증 요건

EAP-MD5에서는 AS가 MS를 인증하는 기능만 있으며 AS가 MS를 인증을 할 때는 MS의 공인인증서를 이용하지 않고 사설 패스워드를 이용하기 때문에 인증서의 유효성을 검사하기 위하여 네트워크를 접속할 필요가 없다. 따라서 사용자 인증은 실시간으로 가능하다. EAP-TLS에서는 AS와 MS가 공인인증서와 본인 서명문을 이용하여 상대방을 인증함으로 MS는 AS의 인증을 받을 때까지는 유선랜을 접속할 수 없음으로 AS의 공인인증서를 CVS를 통하여 실시간으로 검증할 수 없다. 따라서 MS는 AS를 실시간으로 인증할 수 없다는 문제점이 있다. PEAP에서는 AS가 MS를 인증할 때는 사설 패스워드를 이용함으로 인증 사실을 공인받을 수 없다. 그리고 MS가 AS를 인증할 때는 공인인증서와 본인 서명문을 이용함으로 EAP-TLS에서와 동일한 이유로 MS는 AS를 실시간으로 인증할 수 없다는 문제점이 있다. 제안 시스템에서는 A형과 B형 모두 공인인증서와 본인 서명문 또는 위임서를 이용함으로 MS의 UA가 CVS를 통하여 MS를 대신하여 AS를 인증해줌으로 MS가 AS를 실시간으로 인증할 수 있다.

비록 실시간 인증이 가능하다 하더라도 인증서 검증 방식에 따라 인증서 검증 결과의 현재성이 없을 수도 있기 때문에 실시간 인증 결과에 문제를 발생시킬 수 있다. CRL 방식은 인증서가 폐지되는 시점과 CRL에 기록되는 시점과의 시간차 문제를 갖고 있기 때문에 이 방식은 기본적으로 검증 결과의 정확성을 보장받을 수 없다. OCSP의 경우 OCSP 서버의 구현 방식에 따라 차이가 있다. CA로부터 직접 확인을 받지 않고 CRL을 이용할 경우 검증 결과의 현재성은 CRL 방식과 동일하다. 그러나 제안한 시스템에서는 인증서를 폐지할 경우 즉시 그 정보가 CA의 폐지 목록에 기록됨으로 CA는 항상 인증서의 최신 상태 정보를 갖게 된다. 따라서 인증서 검증 결과의 현재성을 완벽히 보장해줄 수 있기 때문에 실시간 인증 결과의 신뢰성을 높일 수 있다.

4.1.3 인증 사실의 공인 요건

EAP-MD5에서는 사설 패스워드를 이용하여 AS가 MS를 인증함으로 인증 사실을 공인받을 수 없다. EAP-TLS에서는 AS와 MS가 공인인증서와 본인 서명문을 이용하여 상대방을 인증함으로 상호 공인된 인증이 가능하다. PEAP에서는 MS가 AS를 인증할 때는 공인인증서와 본인 서명문을 이용함으로 인증 사실을 공인받을 수 있으나 AS가 MS를 인증할 때는 사설 패스워드를 이용함으로 인증 사실을 공인받을 수 없다. 제안 시스템에서는 A형과 B형 모두 공인인증서와 본인 서명문 또는 위임서를 이용함으로 인증 사실을 공인받을 수 있다.

<표 2>는 기능적인 면의 목표 중에서 인증과 관련된 <요건1>, <요건2>, <요건3>의 만족 여부를 보여준다.

표 2. 인증 기능 특성
Table 2. Authentication characteristics.

프로토콜 / 항목	EAP-MD5	EAP-TLS	PEAP	제안 시스템	
				A형	B형
상호인증	MS가 AS 인증 불가	가능	가능	가능	가능
실시간인증	가능	MS가 AS 인증시 불가	MS가 AS 인증시 불가	가능	가능
공인여부	비공인	공인	MS 인증 비공인	공인	공인

4.1.4 보안 요건

인증 단계에서 통신 내용의 안전성과 MS와 AP 사이의 무선 구간에서 통신 내용의 안전성을 분석한다.

1) 인증 프로토콜의 안전성

통신 내용의 보안은 세션 개설 중에는 물론 상호 인증 단계부터 이루어져야 한다. 제안한 상호 인증 프로토콜에서 노드들 간에 전송되는 내용들이 얼마나 안전한가를 분석해본다. <표 3>은 A형 시스템, <표 4>는 B형 시스템의 상호 인증 프로토콜에서 각 단계별로 전송되는 내용과 그 내용의 보안 필요성 그리고 보안이 필요한 부분의 처리 결과를 보여준다. 결과에서 보듯이 인증 프로토콜에서 전송되는 내용 중 보안이 필요한 부분은 적절한 암호 방식을 이용하여 암호화하여 전송되고 있음을 알 수 있다. 따라서 제안한 인증 프로토콜의 안전성은 보장받을 수 있다.

표 3. A형 시스템의 전송 내용 안전도 분석표
Table 3. Stability table of transmitted contents in A-type system.

전송 단계	전송내용	보안 필요성	결 과	
			암호방식	비고
③,⑦	인증서	X	평문	이미 공개된 내용
	서명문	X	비밀키(SK_{MS}, SK_{AS})	조회 가능하나 변조 불가능
	ID	X	평문	ID 공개 무방
	대칭키(K_{MU})	O	공개키(PK_{UA})	UA만이 해독 가능
④,⑧	인증서	X	평문	이미 공개된 내용
	검증요청서	X	평문	검증요청내용 공개 무방
⑤,⑨	검증결과	O	공개키(PK_{AS}, PK_{UA})	검증요청자만이 해독 가능
⑪	WEP키	O	공개키(PK_{AS})	AS만이 해독 가능
	AS 대리인증서	O	대칭키(K_{MU})	UA만이 생성 & MS만이 해독 가능
⑫	MS 인증확인서	O	세션키	AS가 생성 & AP만이 해독 가능
	WEP키	O	세션키	AP만이 해독 가능
	AS 대리인증서	O	대칭키(K_{MU})	바이패스(Bypass)
⑭	AS 대리인증서	O	대칭키(K_{MU})	바이패스

표 4. B형 시스템의 전송 내용 안전도 분석표
Table 4. Stability table of transmitted contents in B-type system.

전송 단계	전송내용	보안 필요성	결 과	
			암호방식	비고
③	ID	X	평문	ID 공개 무방
④	인증서	X	평문	이미 공개된 내용
	서명문	X	비밀키(SK_{AS})	조회 가능하나 변조 불가능
	ID	X	평문	바이패스
⑤,⑨	인증서	X	평문	이미 공개된 내용
	검증요청서	X	평문	검증요청내용 공개 무방
⑥,⑩	검증결과	O	공개키(PK_{UA}, PK_{AS})	검증요청자만이 해독 가능
⑧	WEP키	O	공개키(PK_{AS})	AS만이 해독 가능
	AS대리인증서	O	대칭키(K_{MU})	UA만이 생성 & MS만이 해독 가능
	MS위임서	X	비밀키(SK_{MS}, SK_{UA})	조회 가능하나 변조 불가능
	인증서	X	평문	이미 공개된 내용
	서명문	X	비밀키(SK_{UA})	조회 가능하나 변조 불가능
⑫	MS인증확인서	O	세션키	AS가 생성 & AP만이 해독 가능
	WEP키	O	세션키	AP만이 해독 가능
	AS대리인증서	O	대칭키(K_{MU})	바이패스
⑭	AS대리인증서	O	대칭키(K_{MU})	바이패스

2) 무선 구간의 안전성

무선 구간의 보안은 MS와 AP 간에 이용되는 WEP키를 얼마나 안전하게 생성하고 분배하였는가 그리고 사용하는 암호화 알고리즘이 얼마나 안전한가에 기인한다. 제안 시스템의 A형과 B형 프로토콜에서 UA가 WEP키를 AS에게 안전하게 전송하며 AS가 WEP키를 AP에게 안전하게 전송하며 AP가 WEP키를 MS에게 안전하게 전송함으로 AP와 MS 사이에 WEP키의 안전한 교환이 가능하다 할 수 있다.

4.2 성능적인 목표 요구조건의 만족 여부 분석

성능적인 면의 목표인 <요건5>, <요건6>, <요건7>을 만족시키고 있는지를 EAP-MD5, EAP-TLS 그리고 PEAP 인증 프로토콜들과 비교해가며 분석한다.

4.2.1 인증서 검증 방법에 대한 요건

인증서 검증을 위한 절차가 얼마나 간단한지, 검증시스템의 부분적인 장애가 검증시스템 전체에 미치는 영향은 어떤지, 보안시스템의 규모가 커질 때 검증 속도는 어떻게 되는지, 사용자가 신뢰해야할 기관의 수는 얼마나 되는지에 대하여 CRL과 OCSP와 비교해가며 분석해본다. <표 5>는 인증서 검증 방법의 특성을 CRL과 OCSP와 비교하여 보여준다. 제안한 검증 방법이 성능적인 면의 목표 <요건5>를 만족시키고 있음 보여준다.

표 5. 인증서 검증 방법별 특성
Table 5. Characteristics of certificate validation methods.

방 법 / 항 목	CRL	OCSP	제안한 검증방법
시스템 효율성	조회횟수=n+ ∑(각CA들의 하위CA개수)	조회횟수=n+ ∑(각CA들의 하위CA개수)	조회횟수=1회
시스템 안전성	부분파괴= 부분파괴	부분파괴= 전체파괴	부분파괴= 부분파괴
검증속도	시스템규모에 반비례	시스템규모에 반비례	시스템규모와 무관하게 항상 일정
신뢰해야할 기관수	CA 개수	1 개	1 개

4.2.2 인증 프로토콜의 효율성에 대한 요건

무선 구간에서 상호 인증을 위하여 전송되는 통신 내용은 각 프로토콜마다 약간씩 차이는 있으나 대체로 간단한 질의와 응답으로 구성되기 때문에 인증 프로토콜의 효율성은 통신량보다 통신횟수에 비례한다. 따라서 여기서는 통신횟수를 중심으로 각 프로토콜들을 비교해본다.

표 6. 구간별 통신횟수
Table 6. Number of handshakes on each section.

프로토콜 / 구간	EAP-MD5	EAP-TLS	PEAP	제안 시스템	
				A형	B형
MS ↔ AP	3	9	≥ 6	2	2
AP ↔ AS	3	9	≥ 6	2	2
AS ↔ UA	0	0	0	2	2
AS ↔ CVS	0	≥ 0	≥ 0	2 or 4	2 or 4
UA ↔ CVS	0	0	0	2 or 4	2 or 4
합 계	6	≥ 18	≥ 12	10 or 12	10 or 12

<표 6>은 MS와 AS 간의 상호 인증을 거쳐 MS가 유선랜에 접속할 수 있을 때까지의 MS, AP, AS, UA 그리고 CVS 간의 통신횟수를 보여준다. MS ↔ AP, AP ↔ AS 구간 모두 제안 시스템의 통신횟수는 2회로 EAP-MD5, EAP-TLS, PEAP보다 적다. CVS를 이용하여 인증서 유효성을 검증할 경우를 포함하여 시스템 총 통신횟수는 EAP-TLS 경우 최소 18회, PEAP의 경우 최소 12회이지만 제안 시스템은 최대 12회이다.

따라서 제안 시스템은 실시간으로 공인된 상호 인증 기능을 가능하게 하면서도 총 통신횟수도 EAP-TLS나 PEAP보다 적어 다른 시스템에 비하여 시스템 효율성이 높다. 결과적으로 제안한 시스템은 성능적인 면의 목표 <요건 6>을 만족시키고 있음을 알 수 있다.

4.2.3 클라이언트의 부하에 대한 요건

무선랜을 이용하는 클라이언트 MS에는 노트북과 같은 고속 고용량의 기기도 있으나 휴대폰과 같은 저속 저용량의 기기도 있다. 따라서 기기의 특성에 따라 적용되는 시스템도 다를 수 있다. MS와 AS 간에 상호 인증이 되기까지 각 인증 프로토콜에서 MS가 비대칭키 암호연산을 하는 횟수, 대칭키 암호연산을 하는 횟수 그리고 총 암호연산 시간은 <표 7>과 같다. 여기서 대칭키 방식을 이용하여 일정 크기의 메시지를 암호화 하는데 소요되는 시간을 1 UT(Unit Time)로 표기하였다. 일반적으로 비대칭키 암호연산 시간은 대칭키 암호연산 시간의 10,000배 정도이다.

표 7. 클라이언트의 암호연산 시간
Table 7. Encryption time of the clients.

항목 / 프로토콜	EAP-MD5	EAP-TLS	PEAP	제안 시스템	
				A형	B형
비대칭키 암호연산 횟수(회)	0	2	2	2	0
대칭키 암호연산 횟수(회)	1	1	2	1	1
암호연산 총시간(UT)	1	20,001	20,002	20,001	1

<표 7>에서 보듯이 제안 시스템 A형의 경우는 MS의 암호연산을 위한 부하가 EAP-MD5보다는 높으나 EAP-TLS와 PEAP과는 유사하다. 따라서 제안 시스템 A형은 다른 시스템들의 단점들을 모두 해결하고서도 특별히 MS의 부하를 증가시키지 않는다. 제안 시스템 B형의 경우는 MS의 암호연산을 위한 부하가 공인인증서를 사용하지 않는 EAP-MD5와 유사한 수준이며 EAP-TLS나 PEAP보다는 월등히 낮다. 따라서 제안 시스템 B형은 휴대폰과 같이 프로세스의 처리 속도가 낮고 자료의 저장 용량이 적은 기기에 효과적으로 이용될 수 있는 인증 프로토콜이다. 결과적으로 제안한 시스템은 성능적인 면의 목표 <요건7>를 만족시키고 있음을 알 수 있다.

V. 결 론

인증서의 유효성 검증을 위하여 CRL 디렉토리나 OCSP 검증서버를 이용하지 않고 인증 경로 검사와 인증서 검증을 CA와 직접 접속하여 처리하는 CVS를 이용하였다. 그 결과 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 있었으며 특정 검증기관에 장애가 발생하더라도 시스템 전체의 안전성에는 영향을 미치지 않게 하였다. 또한 인증 경로를 각 CA의 저장소 및 인증서에 포함시킴으로써 다중 CA 환경에서 인증서 유효성 검증을 신속하게 처리할 수 있게 하였다.

그리고 MS와 AS 간에 실시간 상호 인증과 WEP키 교환이 가능한 두 가지 프로토콜을 제안하였다. 제안한 프로토콜에서는 유선랜 상에 위치한 UA가 MS를 대신하여 AS의 인증서를 검증하게 함으로써 MS와 AS 간의 실시간 상호 인증이 가능하게 하였다. 또한 사용자 인증을 위하여 MS와 AS 모두 X.509 규격의 공인 인증서를 이용하게 함으로써 인증 사실을 공인받을 수 있게 하였다. 특히 저속 저용량의 MS용 프로토콜에서는 MS를 대신하여 UA가 MS의 인증서와 서명문을 AS에게 전송하게 함으로써 MS가 인증서를 소지하지 않고 그리고 비대칭키 암호연산을 하지 않고서도 상호 인증이 가능하게 하였다. 따라서 이와 같은 저속 저용량의 MS용 프로토콜을 이용할 경우에는 MS의 상호 인증을 위한 부하를 대폭 경감시켜줄 수 있다. 이는 앞으로 유비쿼터스 컴퓨팅(Ubiquitous Computing) 사회에서 다양한 소형 단말 장치들에 유용하게 활용될 수 있을 것이다.

참고문헌

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

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

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

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

[5] 정경숙, 정태충, "타원 곡선 상의 Diffie-Hellman 기반 하이브리드 암호 시스템", 한국컴퓨터정보학회논문집, 제8권 제4호, Dec. 2003.

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

[9] P. Calhoun, J. Loughney, E.Guttman, G. Zorn, J. Arkko "Diameter Base Protocol", IETF RFC 3588, Sep. 2003.

[10] "Port-based Network Access Control", IEEE Standard 802.1x, Jun. 2001.

[11] David A. Cooper, "A More Efficient Use of Delta-CRLs", IEEE Symposium on Security and Privacy, May 2000, pp. 190-202.

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

[13] B. Aboba, D. Simon, "PPP EAP TLS Authentication Protocol", IETF RFC 2716, Oct. 1999.

저 자 소 개

이 상 렬

1981 한양대학교 전자공학과 학사
1983 한양대학원 전자공학과 석사
2005 한양대학원 전자공학과 박사
1997~현재 상지영서대학 인터넷정보과 교수
<관심분야> 컴퓨터통신, 시스템 및 네트워크 보안