무선 네트워크상에서 실시간 상호인증시스템에 관한 연구

정돈철* · 한승조*

Research of Real Time Mutual Authentication System in Wireless Network

Don-Chul Jung* · Seung-Jo Han*

요 약

Open System 인증방식, Shared Key 인증방식, MAC 주소기반 인증방식 등은 보안이 필요한 무선 LAN에서는 사용이 어려운 실정이다. 따라서 현재는 PKI를 적용한 802.1X 인증방법과, 사용자 인증에 PKI를 적용한 방법이 많이 연구되고 있다. 하지만 인증서 검증 프로토콜은 PKI초기부터 CRL이라고 하는 인증서 폐기목록을 사용하였는데 배포시점에 대한 문제는 여전히 존재한다. 이러한 문제점을 개선하기 위하여 본 논문에서는 CRL과 OCSP 서버를 이용하지 않고 CA를 직접 이용하기 위하여 CVS를 적용시켰다. 또한 저속 저용량의 무선단말이 안전하고 빠르게 무선망에 접속 할 수 있도록 대리 인증 서버를 이용하여 인증 절차를 간소화 시키면서 공인 인증서를 이용한 상호인증이 가능한 시스템을 제안하였다.

ABSTRACT

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. This paper applied CVS to use CA direct not to use CRL and OSCP server in order to improve this problems. Also It suggested the system that can make authentication steps more shorter using authentication server and Mutual authentication system by public certificate(small size/low speed wireless terminal can access to wireless network fast and safely)

키워드

무선랜, IEEE 802.1x, 인증, PKI

Ⅰ. 서 론

무선 LAN은 전파라는 전송매체를 사용함으로써 매체의 특성상 보안에 대한 취약성을 내포하고 있다. 물리적으로 접근이 어려운 유선과는 달리 무선 구간은 접근이 용이하므로 데이터를 암호화함으로써 기밀성을 유지하고 인증 된 사용자에게만 네트워크 접속을 허용해야한다[1]. 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[2]. 하지만 IEEE 802.11b 보안 메커니즘에는 이미 많은 취약점들이 알려져 있다[3]. 이러한 취약점들을 보완하고자 고안된 것이 IEEE 802.1x EAP (Extensible Authentication Protocol)이다[4]. 여기서는 네트

* 조선대학교

접수일자 : 2006. 10. 27

워크에 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 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[5, 6].

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

Ⅱ. 관련연구

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 제공해줄 수 있는, 효율적인 인증 프로토콜을 제안한다. 본 장에서는 기존의 인증방식과 인증서 검증방법들에 대하여 문제점을 분석 후, 제안한 인증 시스템을 제시한다.

2.1. 802.1x 인증 유형

2.1.1 EAP-TLS

Windows XP에서 802.1x 단말에 사용되는 보안 메커니즘인 EAP-TLS는 사용자의 인증서와 서버의 인증서를 서로 교환함으로써 단말과 네트워크 사이에 인증서 기반의 상호 인증을 제공한다. 그리고 안전한 연결성을 보장하기 위해 사용자 기반, 세션 기반의 동적인 WEP키를 생성하여 분배한다. 이 방법은 클라이언트측 인증서와 서버측 인증서를 통해 인증을 수행하며 WLAN 클라이언트와 액세스 포인트 간 후속 통신에 대한 보안을 강화하기 위해 사용자 기본 WEP 키 및 세션 기반 WEP 키를 동적으로 생성한다. 하지만 EAP-TLS의 또한 클라이언트측과 서버측 모두에서 인증서를 관리해야 하며, 이는 규모가 큰 WLAN을 설치하는 경우 번거로운 작업이 될 수 있다. 그리고, 클라이언트는 인증 절차가 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.

2.2.2 EAP-TTLS

EAP-TTLS는 EAP-TLS의 확장형이며, 단말과 인증서버 모두의 인증서가 사용되는 EAP-TLS가 가장 확실한 인증 방법이다. 하지만 모든 단말에 인증서를 설치하는 것은 비용이나 관리면에서 단점이 있다. 그러나 EAP-TLS

와는 다르게 서버측 인증서만을 사용하고, 각 무선랜 단말은 인증서 사용을 배제하였다. 또한 기존의 패스워드 프로토콜을 지원하도록 하였으며 사용자 정보는 TLS 프로토콜을 통해 안전하게 터널링 되도록 하였다. 따라서 무선링크를 포함한 인증서버까지의 전체 네트워크상에서 사용자는 외부 도청자에 대하여 익명성이 보장된다. 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.

2.2. 인증서 검증 방법

2.2.1 CRL 이용 방식

전자 인증서를 사용하는 인터넷 공간에서 사용자 인증서의 유효기간를 확인하여 그 인증서의 유효성을 알고자 할 때 이용하는 것이 CRL(Certificat Revocation Lists)이다. 사용자의 인증서 유효기간은 인증서가 가지고 있는 유효기간을 검사하여 알 수 있지만 만약 사용자가 개인키를 해킹당해서 다른 사람이 사용한다면 상당히 치명적인 피해가 발생할 것이다. 이럴 겨우 사용자는 자신의 개인키와 인증서에 대한 폐기 신청을 CA에게 해야 한다. 그리고 그 폐기된 인증서와 거래를 하는 모든 곳에 그 인증서의 유효성을 검사하는데 사용한다. 또 CRL은 폐기된 인증서의 리스트와 각 폐기된 인증서의 폐기 사유, CRL을 발행한 장의 이름, 발행된 날짜와 시간, 그리고 다음 CRL이 발행될 시간 등을 담고 있다. 이 인증서에 관한 내용은 차후에 검증결과를 증명할 수 있도록 저장할 필요가 있다. 이러한 CRL에게도 한계점은 있다. 인증서를 검증하려면 항상 현재의 CRL을 가지고 있어야 하는데 그러기 위해서는 자주 갱신을 해야한다. 갱신을 자주하다 보면 폐기된 인증서가 많아져 CRL의 크기가 커져 시스템이 느려질 수 있다. 또한, CA에 설정된 주기에 따라서 정기적으로 발행되므로 너무 빈번히 발행해도 시스템에 무리가 있을 수 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[7].

2.2.2 OCSP 서버 이용방식

OCSP(Online Certificate Status Protocol)는 CRL의 배포 문제의 한계를 극복할 수 있는 방법으로 CRL을 뒷받침하거나 CRL을 대신할 수 있다. OCSP는 인증서의 상태정보를 원하는 클라이언트 응용 프로그램의 요구 메시지 구조와 인증서의 상태 정보를 알고 있는 서버 프로그램의 응답 메시지 구조에 대한 정의만을 하고있다. 이러한 OCSP는 서버가 인증서의 상태정보를 주기적으로 발행되는 CRL의 내용에 기초하기 때문에 CRL의 주기적 발행에서 오는 문제점들은 해결되지 않으며, OCSP서버는 인증서 상태요구가 많아진다면 서비스 불능(Denial of Service)상태가 될 수 있는 문제점이 존재한다.

Ⅲ. 제안 시스템의 설계

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 구 현하고자하는 무선 LAN 보안 시스템을 설계하고자 한다.

3.1. 제안 시스템의 구성요소

(1). 인증 요청자 : MN(Mobile Node)
- Cmn : CA가 발급한 공인 인증서
- Smn : 사용자 MN의 비밀키로 서명한 서명문
- IDmn : 사용자 MN의 ID
- KMP : MN과 PA(Proxy Authentication) Server 사이의 대칭키
- PKmn : 사용자 MN의 공개키
- SKmn : 사용자 MN의 비밀키

(2). 무선 네트워크 중계자 : AP(Access Point)

(3). 인증 서버 : AS(Authentication Server)

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.

(4). 대리 인증 서버 : PA(Proxy Authentication) Serve

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 무선단말에 많은 부하를 초래하며, 수 차례의 핸드쉐이크 과정을 거치면서 제한된 무선 네트워크망에서 자원을 소비하게 된다. 이러한 문제점을 개선하기 위하여 제안 시스템에서는 대리 인증서버를 사용을 제안 하였다.

(5) 인증서 검증 프로토콜 : CVP(Certificate Validation Protocol)

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.

3.2. 제안 시스템의 인증 절차

아래 그림 1은 EAP-TLS의 인증절차이고, 그림 2는 제안한 시스템의 인증절를 도식화하였다. 그림처럼 제안된 시스템의 무선단말 의 통신횟수가 기존 EAP-TLS의 통신횟수와 비교하였을 때 6회의 통신횟수가 단축됨을 알 수 있다. 이는 무선 단말에서의 통신시간의 단축과 인증서를 암・복호화시 걸리는 시간을 대리 인증서버가 대신하여 줌으로써 가능하게 되었다. 이는 제한된 무선 Lan에서의 인증을 위한 통신 트래픽을 보다 빠른 유선망에서 대리 인증서버가 대신함으로써 무선 단말에 부하와 트래픽을 현저히 줄여줌과 동시에 인증시간의 단축을 가져오게 할 수 있다.

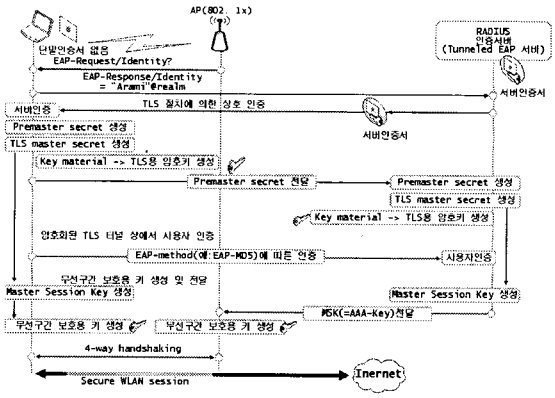

그림 1. EAP-TLS 인증절차
Fig. 1. EAP-TLS Authentication Procedure

(1) MN → AP : IEEE 802.11 접속요청

무선 단말기는 최적의 AP를 선택하여 접속을 요청한다.

(2) AP → MN : IEEE 802.11 접속응답

무선 네트워크에 접속하기위한 인증 과정의 시작을 알린다.

(3) MN → AS : [Cmn, Smn, IDpa, {IDmn, KMP}PKpa]

CA가 MN에게 발급한 인증서, MS의 개인키로 서명한 서명문, PA의 ID와 함께 MN의 ID, MN와 PA사이의 대칭키를 PA의 공개키로 암호화하여 AP를 통하여 AS에 전송

(4) AS → CVP : Cmn

CA가 MN에게 발급한 인증서의 유효성 검증을 위하여 CVP에 전송

(5) CVP → AS : 검증결과 전송

(6) AS → PA : [Cas, Sas, {IDmn, KMP}PKpa]

AS는 (5)에서 전송받은 Sms에 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.

(7) PA → CVP : Cas

CA가 AS에게 발급한 인증서의 유효성 검증을 위하여 CVP에 전송

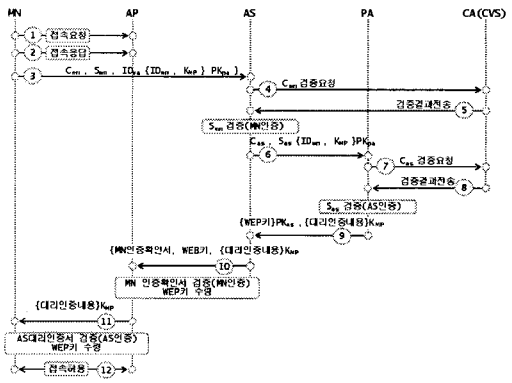

그림 2. 제안 시스템의 인증 절차
Fig. 2. Proposal Authentication Procedure

(8) CVP → PA : 검증결과 전송

(9) PA → AS : [{WEP키}PKas, {대리인증내용}KMP]
PA는 (8)에서 전송받은 Sas에 대하여 검증을 완료함으로써 AS를 인증한다. 이후 WEP키는 AS의 공개키로 암호화한 정보와 AS 대리인증서를 MN과 PA의 대칭키로 암호화하여 AS에 전송한다.

(10) AS → AP : [MN 인증확인서, WEP키, {대리인증내용}KMP]

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

(11) AP → MN : [{대리인증내용}KMP, WEP키]

수신한 MN 인증확인서를 검증한후 WEP키와 AS 대리인증서를 MN에 전송

(12) MN : AS 대리인증서 검증하여 AS를 인증후 WEP키를 이용하여 무선 네트워크에 접속한다.

Ⅳ. 제안 시스템의 분석

위 3장에서 제안한 시스템은 클라이언트와 인증 서버 모두 공인 인증서와 본인 서명문을 이용함으로 상호인증이 가능하며, 인증사실을 공인 받을 수 있다. 그리고, 인증서를 폐지할 경우 즉시 그 정보가 CA의 폐지목록에 기록됨으로 CA는 항상 최신의 정보를 갖게된다. 따라서 인증서 검증 결과의 현재성을 보장해줄 수 있기 때문에 실시간 인증이 가능하다. 이러한 인증시스템의 안전성은 PKI 방식을 이용하고, 클라이언트와 대리인증서버사이에 유선망을 통한 사전등록단계를 거쳐 만들어진 대칭키를 사용함으로써 기존 EAP-TLS방식과 동일한 보안강도를 가졌다고 할 수 있다. 또한 클라이언트가 속한 무선망에서의 통신횟수를 줄이고 유선망의 대리 인증 서버가 인증절차를 수행함으로써 통신횟수와 인증시간을 단축시켜 향후 증가하는 무선 인터넷 이용자들을 고려한다면 제안한 무선 LAN 보안시스템은 클라이언트의 보안과 인증시간 단축에 큰 역확을 할 것이다.

Ⅴ. 결 론

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. 인증방식 또한 상호인증과 관련하여 현재까지 EAP-TLS를 제외하고는 인증 요청자와 인증서버 사이에 공인 인증서를 사용하는 인증 프로토콜은 없는 실정이다. 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 문제점을 개선하였다. 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.

참고문헌

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

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

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

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

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

[6] 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.

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

저자소개

정 돈 철(Don-Chul Jung)

조선대학교 일반대학원
정보통신공학과 박사과정
※관심분야 : 무선 LAN, 네트워크 보안 ·

한 승 조(Seung-Jo Han)

1995년 2월 ~ 1996년 1월 Univ. of Texas 객원교수
1997년 현재 조선대학교 정보통신공학과 교수
※관심분야 : 통신보안시스템설계, 네트워크 보안, ASIC 설계, DRM