무선 네트워크 환경에서의 ECbA(Elliptic Curve based Authentication)시스템 설계

정은희**, 양승해**, 김학춘***, 이병관****

ECbA(Elliptic Curve based Authentication) System on the wireless network environment

Eun-Hee Jeong*, Seung-Hae Yang**, Hak-Chun Kim***, Byung-Kwan Lee****

요 약

무선 네트워크 시장이 증가하면서 가장 큰 이슈로 떠오른 것이 안전한 자료 전송과 사용자 인증에 관한 보안 문제이다. 본 논문에서는 타원곡선 알고리즘을 이용해 무선 네트워크에서 사용자가 인증서버의 신분을 확인할 수 있는 상호 인증 메커니즘과 인증 서버가 사용자의 신분을 확인할 수 있는 사용자 인증 메커니즘으로 구성된 ECbA(Elliptic Curve based Authentication) 시스템을 제안하였다. 제안된 ECbA 시스템에선 인증에 키 길이가 작은 타원곡선 알고리즘을 이용함으로써 메시지 전송량을 줄이고, 연산 시간을 단축시켰을 뿐만 아니라, 기존의 인증 메커니즘인 EAP-TLS의 인증 스텝 단계를 9단계 과정에서 제안한 인증 메커니즘에서 6단계로 줄였기 때문에 통신비용이 적게 들고, 상호 인증 시간에 소요되는 시간이 기존의 인증보다 절감시킬 수 있다. 또한, 키교환 메커니즘을 사용하여 사용자 인증때마다 새로운 키를 분배하므로 안전한 통신 제공하며, 키 길이 160bit인 세션 키를 사용하므로 전수조사 공격에 안전할 뿐만 아니라 인증서버가 사용자 인증 요청을 제어하므로 DoS 공격을 방지할 수도 있다.

ABSTRACT

As wireless network market is increasing rapidly, the biggest issue is to transfer safe data and to authenticate users. This paper proposes ECbA(Elliptic Curve based Authentication) which consists of the mutual authentication mechanism that users can ascertain the identity of an authentication server and the user authentication mechanism that an authentication server can make sure users' identity, by using Elliptic Curve algorithms. The proposed ECbA system diminishes the message quantity and the execution time by using the small elliptic curve algorithm with the small key length in authentication. In addition, as this paper reduces the authentication steps of existing EAP_TLS into 6 authentication steps, the communication cost and mutual authentication time can be saved. As this paper distributes new keys, whenever authenticating users by using key exchange mechanism, it provides safe encryption communication and prevents DoS attack by controlling the users authentication request by authentication server.

키워드 : ECbA, 상호인증, Cross Authentication, 사용자 인증, SSID, WEP, EAP-MD5, EAP-TTL, EAP-TTLS, PEAP

Ⅰ. 서 론

최근에는 사무실 내에서 뿐만 아니라 자동차나 거리, 공항이나 지하철역 등 다양한 환경에서 인터넷 접속 요구가 증가하면서 시간과 장소에 구애받지 않고 인터넷을 이용할 수 있는 무선랜에 대한 일반인들의 관심이 날로 증가하고 있다. 무선랜은 배선이 필요 없어 단말기의 재배치가 쉽고 이동 중에도 통신이 가능할 뿐만 아니라 빠른 시간 안에 네트워크 구축이 용이하다는 장점이 있는 반면, 사용 매체의 공개성에 따른 해킹 및 접근이 용이하기 때문에 전자상거래, 전자메일, 데이터 전송과 같이

* 강원대학교 지역경제학과 조교수(jeongeh@kangwon.ac.kr) ** (주)CDS 연구실장
*** 송호대학 조교수 **** 관동대학교 컴퓨터공학과 교수

데이터 보안 중요도가 높은 응용에서 보안성 요구가 더욱 증가하고 있다[1].

무선 랜은 이동성 면에서 유선망 보다 뛰어나고, 통신 속도 또한 이동통신에 비해 빠르기 때문에 무선 홈 네트워크의 블루투스(Bluetooth), RF 등의 기술보다 넓은 영역을 지원하고 전송속도가 빠른 강점으로 확산 가능성이 높은 사업영역으로 평가되고 있다. 또한 무선 랜은 향후 확대될 이동 네트워크의 모든 요소를 포함하고 있으며 다양한 환경 요소를 제공하고 있다. 하지만, 무선 랜은 전파를 매개체로 브로드 캐스팅되며, 적용되는 공간적 범위가 넓기 때문에 도청, 위장, 스푸핑, 기기의 도난 등의 문제가 있음으로 기존의 유선 네트워크보다 보안성이 취약하다.

본 논문에서는 무선 랜 보안의 취약점을 분석하고 무선랜의 사용자 인증 및 기밀성을 지원할 수 있는 ECbA(Elliptic Curve based Authentication) 시스템을 제안한다. ECbA 시스템은 기존의 인증 방법 단계보다 간소화된 인증 방법을 제공함으로써 인증 단계를 줄인다. 따라서 통신비용을 절감할 수 있다.

II. 관련연구

2.1 무선랜의 보안

대부분의 무선랜 제품에 적용된 802.11b표준이 나왔던 1999년도에는 무선랜의 보안문제에 관해 심각하게 고려하지 않았었다. 따라서 SSID는 보안에 대한 대안이 될 수 없으며 MAC을 이용한 접근제어 또한 한계가 있다. 이에 802.11b에서 사용한 WEP은 초기에 40비트의 암호화를 지원하다가 실시간으로 해독될 수 있다는 사실이 밝혀지자 128비트 암호화로 사용하고 있으나, 이것 또한 안전하지 않다고 해서 802.1x의 보안 표준을 적용하게 되었다[2].

2.1.1 MAC 필터링

MAC Filtering은 무선랜 NIC(Network Interface Card)의 고유한 주소인 MAC Address를 이용하여 미리 MAC이 등록된 사용자만 접근을 허용하는 방식이다. AP는 접속이 허용된 MAC 주소의 목록을 저장하고 있으며, 관리자의 조작에 의해 편집이 가능하고, MAC 주소가 고유함으로써 강력하고 안전한 접근제어 방식이라는 장점이 있지만 MAC 주소는 해커에 의해 만들어 질 수도 있고, PC카드에 노출되어 있으므로 유출이 쉬우므로 안전한 방법은 아니다.

또한, AP가 MAC 주소를 보유하는데 한계가 있으므로 MAC Address 지원의 한계가 이동성을 위한 영역의 확장성의 한계가 된다. 이것은 무선랜 서비스를 하는 사업자에게는 치명적일 수 있으며, 이러한 한계를 해결할 방안으로 MAC Address를 AP간에 공유하는 기능을 요구하기도 한다[3].

2.1.2 SSID(Service Set Identifier)

SSID는 무선랜 서브시스템에서 장비의 네트워크 이름을 지칭하는 것으로 접속 제어에 대한 초보적인 기능만을 제공한다.

802.11b의 인증 기술은 비암호화와 암호화 방법으로 나눌 수 있으며, 비암호화 방식에는 SSID값을 Null로 입력하여 네트워크 접속이 허용되는 Open System 인증과 정확한 SSID 값을 입력해야만 네트워크 접속이 허용되는 Closed System이 있다[4,5].

SSID는 여러 사람이 공유하는 패스워드이기에 보안에 대한 신뢰도가 낮을 수 밖에 없으며, AP 및 무선랜 카드 업체에서도 SSID를 각각의 업체에서 정한 기본값으로 설정하여 판매하는 것이 일반적이다. 물론 사용자는 이 값을 변경하여 사용할 수 있다.

SSID는 지정된 무선 랜 BBS(Basic Service Set)안에서 교환되는 모든 패킷의 헤더에 포함되어 있으며, 유선 랜과 무선 단말을 연결해주는 장치인 AP(Access Point)는 자신이 주기적으로 브로드캐스트 할 수 있으며, 무선랜 카드에서는 AP에 접속 가능한 지역 내에서 AP로부터 브로드캐스트 되는 SSID를 수신한 뒤 이를 이용해 AP에 접속할 수 있다.

2.1.3 WEP(Wired Equivalent Privacy)

802.11b의 인증 기술 분류에서 암호화 방법을 사용하는 WEP는 통신을 하고 있는 모든 사람들이 동일한 비밀키를 공유함으로써 정확한 WEP키를 모르는 사람은 네트워크에 접속하는 것을 방지하는 방식이다.

WEP의 인증 요청과 인증 승인 흐름은 그림 1과 같다. 무선사용자가 AP에 인증을 요청하면 AP는 임의수를 생성한 후 challenge를 무선 사용자에게 전송하면 무선 사용자는 공유하고 있던 비밀키로 암호화한 후 그 값(response)을 AP에 전송한다. AP 또

한 무선사용자와 동일한 비밀키를 이용해 response를 복호화 시킨 후 Challenge 값과 비교하여 동일하면 인증을 승인하여 네트워크 접속을 허용하고, 그렇치 않으면 네트워크 접속을 허용하지 않는다.

WEP는 가변 길이 키를 지원하는 스트림 암호인 RC4를 사용하는데 이러한 인증방법은 기초적인 암호 기술로서 상호 인증이 불가능하다. 따라서 무선 사용자는 AP를 인증할 수 없기 때문에 정당한 AP와 통신하는지 알 수 없으므로 신뢰성이 없으며 보안성이 취약하다[6].

물론, 주기적으로 암호키를 변경해주면 어느 정도 신뢰를 향상할 수 있으나 SSID와 같이 개인별 암호키가 아닌 여러 사람이 한 개의 암호키를 공유해야 한다는 문제가 남는다.

2.2 EAP(Extensible Authentication Protocol)

EAP는 SSID와 WEP의 문제점들을 보완하여 나온 인증 메커니즘으로 WEP의 인증부분에 공개키 구조를 도입하여 중앙집중식 인증관리를 하는 것이다. 따라서 EAP는 PKI 구축이 필수적이다.

2.2.1 EAP-MD5

EAP-MD5는 가장 초기의 인증 유형이고 EAP 방법 중에서 유일하게 의무사항으로 정의되어 있는 방법으로 아이디와 패스워드 기반의 네트워크 인증 방식이다.

EAP-MD5는 구현이 단순하고, 인증서버에서 사용자 이름과 패스워드 정보의 데이터만 관리하면 되는 편리성을 제공하지만, 단방향으로 가입자에 대한 인증만 지원하기 때문에 상호인증이 불가능하다. 또한 무선랜 접속구간보안에 필요한 마스터 키 생성 방식을 정의하고 있지 않아 문제가 되고 있다[8].

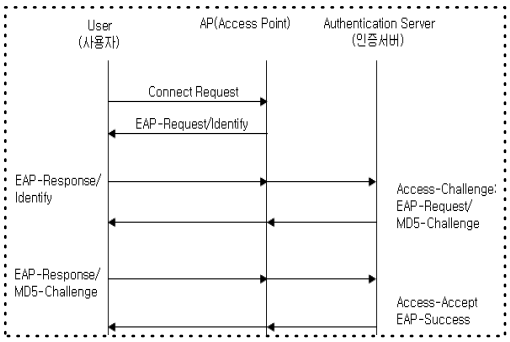

그림 1. EAP-MD5 인증 흐름도

Fig. 1 The Flow of EAP-MD5 Authentication

2.2.2 EAP-TLS

EAP-TLS(Transport Layer Security)는 사용자와 인증서버 사이의 상호 인증과 무선 랜에서의 비밀성을 제공하기 위해 사용하는 암호화에 필요한 키에 대한 키 분배 메커니즘을 제공한다. EAP-TLS는 PKI 기반의 인증서를 사용하여 인증서버와 사용자가 상호 인증을 하는데, 인증서의 안전한 배포와 사용자와 인증서를 모두 관리해야한다는 문제점이 발생한다.

또한, 사용자가 인증서버의 인증서가 신뢰할 수 있는 인증서인지를 판단해야하므로 서버의 인증서가 미리 설치되어 있어야 한다는 문제점도 발생한다.

EAP-TLS를 이용한 인증 메커니즘은 그림 2와 같이 9단계의 과정을 통해 네트워크와 사용자의 상호 인증을 한다[8]

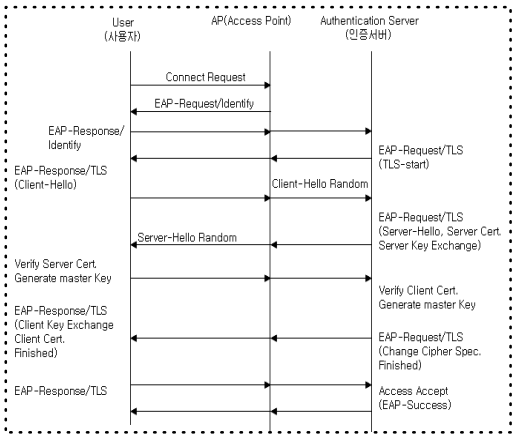

그림 2. EAP-TLS 인증 흐름도

Fig. 2 The Flow of EAP-TLS Authentication

2.2.3 EAP-TTLS

EAP-TTLS(Tunneled Transport Layer Security)는 EAP-TTL의 확장형태로서 사용자에 대한 인증은 비밀번호로 하고 서버인증은 인증서를 이용하여 상호 인증을 하는 방법으로 EAP-TLS의 단점인 인증서를 이용해 사용자를 인증하는데 발생하는 문제점을 해결하였다.

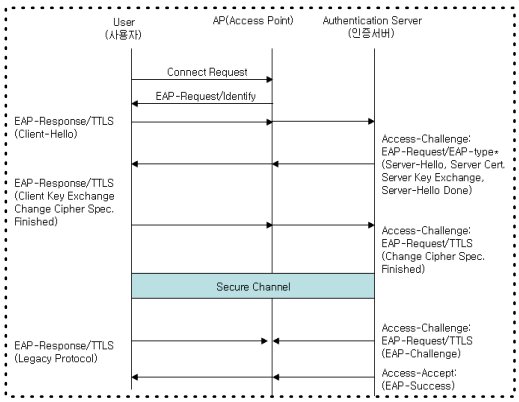

그림 3. EAP-TTLS 인증 흐름도

Fig. 3 The Flow of EAP-TTLS Authentication

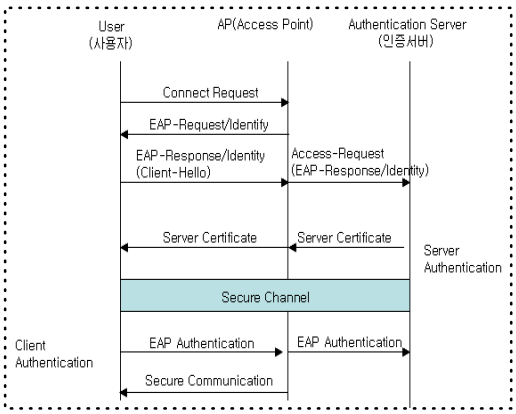

그림 4. PEAP 인증 흐름도

Fig. 4 The Flow of PEAP Authentication

하지만, EAP-TTLS는 인증서가 없는 환경에는 적합하지 않고, 사용자가 서버로부터 받은 서버 인증서가 신뢰할 수 있는지에 대한 검증이 얼마나 정확하게 이루어질 수 있느냐에 대한 문제가 발생할 뿐만 아니라 서버의 인증서를 검증하기 위해선 서버의 인증서를 발행한 루트 인증서를 사용자가 가지고 있어야 하는 문제점이 발생한다.

EAP-TTLS를 이용한 인증 메커니즘은 그림 3과 같이 사용자에 대한 인증은 비밀번호로 하고 서버 인증은 인증서를 이용하여 상호 인증을 한다[8].

2.2.4 PEAP

EAP-MD5는 단방향으로 클라이언트측에 대한 인증만 제공하기 때문에 불법 AP 신호가 더 세다면 클라이언트측은 아무 검증도 거치지 못하고 사용자 ID를 유출할 수 있는데, 이를 보완하기 위해 MS사에서 양방향 인증이 가능한 PEAP(Protected EAP)라는 프로토콜을 추가하였다.

PEAP에서 서버는 PKI 기반 인증 메커니즘을 사용하고 클라이언트는 EAP 인증 유형을 모두 사용할 수 있으므로 EAP-MD5와 같은 알고리즘으로 클라이언트측 인증에 사용할 수 있다[9].

표 1. EAP 종류별 특징

Table. 1 The characteristics of EAP

EAP-MD5	장점	▪ 구현이 쉽다 ▪ 경량화된 Protocol이다 ▪ MS Windows XP/CE.net에서 지원
	단점	▪ 보안성이 떨어진다 ▪ Dynamic WEP Key 지원이 불가능
EAP-TLS	장점	▪ 보안성이 높으며 사용하기 쉽다 ▪ Dynamic WEP Key 지원이 가장 용이하다
	단점	▪ 관리 및 초기설치가 어렵고 계산량이 많다 ▪ 인증서 관리 시스템/공개키 기반 구조가 필요하다
EAP-TTLS	장점	▪ 높은 보안성과 편리한 관리 ▪ Dynamic WEP Key 지원이 가장 용이하다 ▪ EAP-TLS 단점을 대부분 극복
	단점	▪ 구현이 어렵고 계산양이 많다 ▪ 정식표준이 아니어서 지원되는 플랫폼이 제한적이다.
PEAP	장점	▪ 높은 보안성과 편리한 관리 ▪ Dynamic WEP Key 지원이 가장 용이하다 ▪ EAP-TLS 단점을 대부분 극복하고 TTLS와 유사하다
	단점	▪ MS Windows XP/2000 SP4에서 지원 ▪ 구현이 어렵고 계산양이 많다 ▪ 정식표준이 아니어서 지원되는 플랫폼이 제한적이다.

III. ECbA 시스템 설계

본 논문에서 제안하는 ECbA 시스템은 타원곡선(ECC : Elliptic Curve Cryptography) 알고리즘을 사용한다. ECC는 RSA의 키 길이가 1024bit일 때 160bit로 RSA에 비해 키 길이가 매우 작으며, 메모리 공간을 적게 차지하기 때문에 유선뿐만 아니라 무선 네트워크에 적합한 알고리즘이다. 따라서, 본 논문에서 제안하는 인증 시스템은 타원곡선 알고리즘을 이용해 인증값을 생성하여 서로의 신분을 상호 인증하거나, 서버가 사용자의 신분을 확인하는 인증 시스템을 제안한다.

3.1 상호 인증(Cross Authentication) 메커니즘

본 논문에서 제안하는 상호 인증 메커니즘은 공개키 기반 구조를 이용해 별도의 인증서 없이 공유 비밀키를 이용해 서로의 신분을 인증할 수 있도록 하였다. 그림 5는 제안하는 상호 인증 메커니즘의 상호 인증 과정을 설명하는 흐름도로서, 단계별로 살펴보면 다음과 같다.

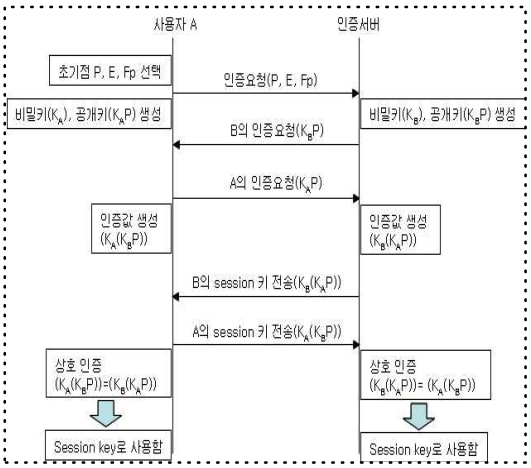

그림 5. 상호 인증 시스템 흐름도

Fig.5 The Flow of Cross Authentication System

[1 단계] 사용자 A는 인증서버에게 인증을 요청하면서 타원곡선 알고리즘에 필요한 초기점 P, 타원곡선 E 그리고 Fp를 전송하면서 상호 인증을 요청한다. 또한 초기점 P와 타원곡선 E 그리고 Fp를 이용해 사용자 A 자신의 비밀키 K_A를 정하고, 초기점 P를 비밀키 K_A만큼 Addition 연산을 하여 공개키 K_AP를 계산한다.

[2 단계] 인증서버는 비밀키 K_B를 정하고 사용자 A로부터 전달받은 초기점 P를 비밀키 K_B 만큼 Addition 연산을 하여 공개키 K_BP를 계산한 후, 공개키 K_BP를 사용자 A에 전송하여 인증서버의 인증을 요청한다.

[3 단계] 사용자 A는 인증서버에게 자신의 공개키 K_AP를 전송하여 인증을 요청한다.

[4 단계] 인증서버는 전달받은 사용자 A의 공개키 K_AP를 인증서버의 개인키로 Additon 연산을 하여 인증값 $K_B(K_AP)$를 계산한다. 그리고 계산된 인증값 $K_B(K_AP)$을 사용자 A에게 전송한다.

[5 단계] 사용자 A는 전달받은 사용자 B의 공개키 K_BP를 사용자 A의 개인키로 Additon 연산을 하여 인증값 $K_A(K_BP)$를 계산한다. 그리고 계산된 인증값 $K_A(K_BP)$을 인증서버에게 전송한다.

[6 단계] 인증서버는 자신이 계산한 인증값 $K_B(K_AP)$과 사용자 A로부터 전달받은 인증값 $K_A(K_BP)$를 비교하여 인증서버는 사용자 A의 신분을 확인한다.

[7 단계] 사용자 A는 자신이 계산한 인증값 $K_A(K_BP)$과 인증서버로부터 전달받은 인증값 $K_B(K_AP)$를 비교하여 사용자 A는 인증서버의 신분을 확인한다.

즉, 사용자 A, 인증서버는 5단계를 거쳐 서로의 신분을 확인한다.

3.2 사용자 인증(User Authentication) 메커니즘

본 논문에서 제안하는 사용자 인증 메커니즘은 사용자 ID 및 디바이스 정보를 이용한 인증으로 난수발생 대신에 타원곡선을 이용한 공개키로 사용자 ID를 Exclusive-OR연산을 한 후 해쉬한 값으로 사용자의 신분 및 인증 서버를 상호 인증한다.

그림 6은 제안하는 사용자 인증 메커니즘의 인증과정을 설명한 것으로 각 단계별 설명은 다음과 같다.

[1 단계] User가 AP에 접속하면 AP는 인증서버에 인증을 요청하게 된다. 또한 AP는 User에게 사용자 ID 또는 Device ID를 요청한다. User는 사용자 ID 또는 Device ID를 AP에 전송하면, AP는 전

송받은 사용자 ID 또는 Device ID를 인증서버에 전송한다.

[2 단계] 인증서버는 타원곡선 $GF(p)$, 초기점 P, 비밀번호 K_A, 인증서버의 공개키 K_AP를 계산하여 인증서버 공개키 K_AP를 AP에 전송하면, AP는 인증서버로부터 전송받은 인증서버의 공개키 K_AP를 User에게 전송한다.

[3 단계] User는 자신의 사용자 ID 또는 Device ID와 인증서버의 공개키를 Exclusive-OR 연산을 한 후 그 값은 해쉬함수로 연산하여 해쉬값을 계산한다.

$$U\_Hash = Hash(사용자ID \oplus K_AP)$$

[4 단계] User는 계산된 해쉬값 U_Hash를 AP에 전송하고, AP는 User의 해쉬값 U_Hash를 인증서버에 전달한다.

[5 단계] 인증서버는 [2 단계]에서 전송받은 사용자 ID와 자신의 공개키로 Exclusive-OR 연산을 하여 사용자의 Hash값과 비교할 A_Hash값을 계산한다.

$$A\_Hash = Hash(사용자ID \oplus K_AP)$$

인증서버는 U_Hash와 A_Hash를 비교하여 사용자의 신분을 인증한 후 그 결과를 AP에 전송한다.

[6 단계] AP는 User의 접속을 허용한다.

즉, 제안된 사용자 인증 메커니즘에서는 6단계의 인증과정을 수행하여 사용자의 신분을 확인 한 후 사용자의 접속을 허용한다.

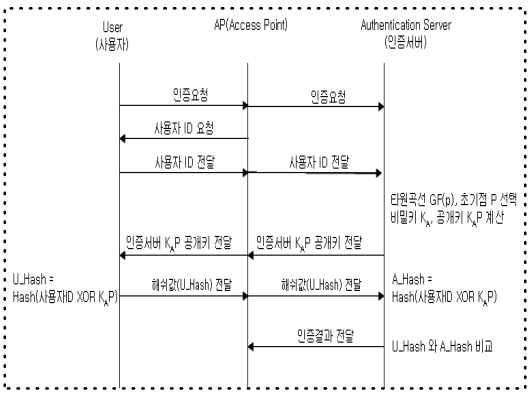

그림 6. 사용자 인증 시스템 흐름도

Fig.6 The Flow of User Authentication System

Ⅳ. 구현 및 평가

ECbA 시스템을 테스트하기 위해 무선랜 네트워크를 사용하는 사용자인 클라이언트와, 클라이언트의 네트워크 접속을 중개하는 AP, 그리고 클라이언트와 AP에 대한 인증을 수행하는 인증서버로 구성된다.

ECbA 시스템은 IEEE802.1x의 취약점인 스푸핑 공격을 방지하기 위해 클라이언트, AP, 인증서버 각각 상호인증을 수행하기 때문에 위장이 불가능하여 매우 안전하다. 또한, 인증서버가 사용자의 인증 요청을 제어할 수 있기 때문에 DoS 공격을 방지할 수 있다.

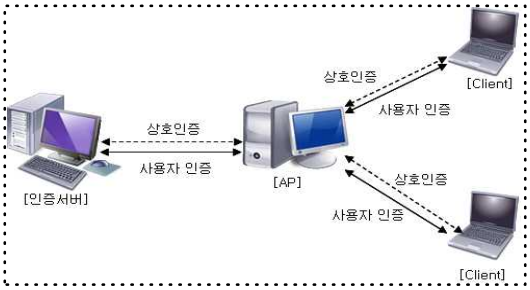

그림 7. ECbA 시스템 구성도

Fig. 7 Structure of ECbA System

IEEE802.11b는 사용자 인증과정에 키 메커니즘이 없으므로 한 개의 키로 장기간 사용하므로 암호통신 보안성이 떨어진다. 하지만, IEEE802.1x의 EAP- MD5를 제외한 나머지 EAP 종류는 사용자 인증과정에서 키 교환 메커니즘을 사용할 수 있으므로 비교적 안전하다고 볼 수 있다. 본 논문에서 제안한 ECbA 시스템도 키 교환 메커니즘을 사용하고, session key의 길이가 160bit 이므로 전수조사 공격에도 안전할 뿐만 아니라 사용자 인증때마다 새로운 키가 분배되기 때문에 안전한 암호통신을 제공한다.

표 2는 기존의 인증시스템과 본 논문에서 제안한 ECbA 시스템을 비교한 것이다.

표 2. 기존 인증시스템과 ECbA 시스템 비교[10]
Table. 2 The comparison of ECbA system and existing Authentication System

항목	IEEE 802.11b	IEEE 802.1x	ECbA 시스템
	MAC, SSID, WEP	EAP-MD5, EAP-TLS	
AP위장	매우 취약	취약	안전
인증서버 위장	해당사항 없음	안전	안전
DoS 공격	취약	취약	안전
인증시스템 의안정성	매우 취약	안전	안전
키교환의 안정성	매우 취약	취약/안전	안전

Ⅴ. 결론

무선 네트워크 시장이 증가하면서 가장 큰 이슈로 떠오른 것이 안전한 자료 전송과 사용자 인증에 관한 보안 문제이다.

IEEE 802.11b에서 제공하는 MAC Filtering, SSID, WEP는 사용자 인증 및 데이터 암호화에 취약하다. MAC의 경우 사용자 인증이라기보다 장치 인증이므로 무선랜 카드를 분실했을 때, 악용될 소지가 있고, SSID의 경우 AP가 SSID를 주기적으로 브로드캐스팅하기 때문에 해커나 악의적인 사용자가 패킷을 도청하여 해당 AP로부터 전송되는 데이터를 도청할 수 있다. WEP의 경우도 키 스트림 및 IV 재사용 공격이 등에 취약하다.

IEEE 802.1x에서 EAP 유형들은 IEEE 802.11b의 사용자 인증 취약점을 보안했지만, 인증 프로토콜의 구조적인 문제로 인해 세션 하이재킹 및 중간 공격 등에 취약하다.

본 논문에서는 제안한 ECbA 시스템은 타원곡선 알고리즘을 이용해 무선 네트워크에서 사용자가 인증서버의 신분을 확인할 수 있는 상호 인증 메커니즘과 인증 서버가 사용자의 신분을 확인할 수 있는 사용자 인증 메커니즘으로 구성되어 있으므로, 사용자, AP, 인증 서버간에 각각 상호 인증을 한다. 따라서, IEEE802.1x의 취약점인 스푸핑 공격을 방지할 수 있다.

또한, ECbA 시스템은 인증에 키 길이가 작은 타원곡선 알고리즘을 이용함으로써 메시지 전송량을 줄이고, 연산 시간을 단축시켰을 뿐만 아니라, 기존의 인증 메커니즘인 EAP-TLS의 인증 스텝 단계를 9단계 과정에서 제안한 인증 메커니즘에서 6단계로 줄였기 때문에 통신비용이 적게 들고, 상호 인증 시간에 소요되는 시간이 기존의 인증보다 절감시킬 수 있다.

또한, 키교환 메커니즘을 사용하여 사용자 인증 때마다 새로운 키를 분배하므로 안전한 암호통신 제공하며, 키 길이 160bit인 Session key를 사용하므로 전수조사 공격에 안전할 뿐만 아니라 인증서버가 사용자 인증 요청을 제어하므로 DoS 공격을 방지할 수도 있다.

참 고 문 헌

[1] William A. Arbaugh, 802.11 Security Vulnerabilities, University of Maryland, 2003. http://www.cs.umd.edu/~waa/wireless.htm/1

[2] 김신효 외 4, “무선 LAN정보보호 기술 표준화 동향”, 정보보호학회지, p56, August 2002.

[3] IEEE 802.11b, Wireless Lan Medium Access Control(MAC) and Physical Layer(PHY) specification : Higy-Speed Physical Layer Extension in the 2.4GHz Band, 1999.

[4] 송창렬, 정병호, 조기환, “무선랜 보안구조”, 정보과학회지, 제 20권 제4호, 2002, pp5-13.

[5] 조윤순, “무선랜의 이슈 - 보안과 로밍”, 컴퓨터월드, 2003, 11월호

[6] Sean Convey, Darrin Miller, "SAFE: Wireless LAN Security in Depth-version2", 2002

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

[8] Dan Nesset, Albert Young, Simon Blake-Willson, "Serial Authentication Using EAP-TLS and EAP-MD5", IEEE 802.11-01/400r22, July 2001.

[9] W. Simpson, PPP Challenge Handshake Authentication Protocol(CHAP), IETF Network Working Group, 1996

[10]홍성표, “강화된 사용자 인증 및 기밀성을 지원하는 무선랜 보안 시스템”, 조선대학교 대학원 박사학위논문, 2005.8

저자약력

정은희(Eun-Hee Jeong)

1991년 강릉대학교 통계학과 이학사
1998년 관동대학교 전자계산공학과 공학석사
2003년 관동대학교 전자계산공학과 공학박사
2003년-현재 강원대학교 지역경제학과 조교수

<관심분야> 네트워크 보안, 전자상거래, 웹 프로그래밍

양승해(Seung-Hae Yang)

2000년 관동대학교 컴퓨터공학과 학사
2002년 관동대학교 전자계산공학과 공학석사
2005년 관동대학교 전자계산공학과 공학박사
2007년-현재 동우대학 보건행정과 겸임교수
2007년-현재 (주)CDS 연구실장

<관심분야> 네트워크 보안, 전자상거래

김학춘(Hak-Chun Kim)

1992년 호원대학교 전자계산학과 학사
1996년 조선대학교 전산기공학과 석사
2000년 관동대학교 전자계산공학과 공학박사
2006년 연세대학교 대학원 보건행정학과 석사
2001년-현재 송호대학 조교수

<관심분야> 병원 네트워크

이병관(Byung-Kwan Lee)

1975년 부산대학교 기계설계학과 학사
1986년 중앙대학교 전자계산공학과 석사
1990년 중앙대학교 전자계산공학과 박사
1988년-현재 관동대학교 컴퓨터공학과 교수

<관심분야> 네트워크 보안, 전자상거래, 컴퓨터 네트워크