무선랜 환경에서 세션키를 이용한 모바일 IPTV 인증 프로토콜

정회원 백 종 규*, 손 규 식**, 조 인 휘*°

A Mobile IPTV Authentication Protocol using Session Key in Wireless LAN

John Baek*, Kyu-Seek Sohn**, Inwhee Joe*° ***Regular Members***

요 약

모바일 IPTV는 IPTV의 양방향 서비스에 이동성을 함께 제공함으로써 사용자 편의를 증대시킬 수 있는 서비스이다. 최근 모바일 IPTV를 위한 인터넷 가입자 접속 망으로 무선 랜이 주목을 받고 있다. 상업적인 모바일 IPTV를 무선 랜을 통해 제공하려면 IPTV 가입자가 무선 랜의 AP(Access Point) 사이를 이동할 때 서비스 재접속을 위한 빈번한 인증이 필요하다. 기존의 유선 랜과 무선 랜을 위한 인증 규격으로 대표적인 것이 IEEE 802.1X인데 이는 끊김이 없는(Seamless) 모바일 IPTV를 제공하기에는 인증 시간이 너무 길다는 단점이 있다. 본 논문은 모바일 IPTV에 적용되는 무선 랜의 보안을 강화하고 인증 시간을 줄이기 위하여 기존의 IEEE 802.1X방식의 취약성을 분석하고 보완하여 모바일 IPTV에 적용시킬 수 있을 정도로 인증 시간이 짧으면서도 강력하게 인증키를 보호하는 인증 모델을 제안하였다. 제안하는 방법에서 사용자 인증과 하드웨어 인증을 나누어 처리하고 이를 통합 인증하며 기밀성 유지를 위한 세션키 방식을 적용함으로써 인증 절차를 간소화하여 인증 시간을 줄이고 인증 과정의 보안을 강화하였다.

Key Words : 이동 IPTV, 무선 랜, 보안, 인증, 802.1X, 세션키

ABSTRACT

Recently the mobile IPTV service has been spread through the wireless LAN(WLAN). In order to provide the commercial mobile IPTV service through the WLAN, re-authentication for the mobile IPTV terminal is required whenever the mobile terminal roams between APs(Access Points). The most popular one of the authentication protocol standards for the wired and/or wireless LAN is IEEE 802.1X. However IEEE 802.1X takes much time to authenticate the terminal and is not adequate for the seamless mobile IPTV service. We introduce the session key and separate the user authentication and the hardware authentication. And we strengthen the device authentication by the initial registration. By these, the proposed authentication protocol reduces the authentication time and can protect the authentication key securely.

Ⅰ. 서 론

IPTV(Internet Protocol Television)는 인터넷 기술과 멀티미디어 기술의 바탕 위에서 이루어진 통신과 방송 융합 기술의 대표적인 한 예로서 현재의 TV 방송 서비스에서 벗어나 앞으로 전자상거래나 SNS

* 한양대학교 컴퓨터공학부 이동네트워크 연구실 (iwjoe@hanyang.ac.kr), (° : 교신저자)
** 한양사이버대학교 정보통신공학과 (kssohn@gmail.com)
논문번호 : KICS2010-12-633, 접수일자 : 2010년 12월 29일, 최종논문접수일자 : 2011년 11월 28일

(Social Network Service)의 구심점으로 그 역할을 확장해 나갈 것으로 기대되고 있다 [1],[2]. IPTV 서비스는 국내의 경우 법제화 및 콘텐츠 보안 및 인증에 관련한 표준화의 미비로 본격적인 서비스가 다소 지연되고 있지만 프랑스, 홍콩, 스페인, 이탈리아, 중국, 미국 등 이미 IPTV서비스가 시작된 나라의 경우 상당한 파급효과를 내면서 새로운 멀티미디어 서비스로서 자리 잡고 있다 [3].

우리나라에는 수 년 전부터 이미 DMB(Digital Multimedia Broadcasting) 기능을 가진 휴대폰이나 전용 수신 단말기를 통해 제공되는 이동형 디지털 TV 서비스가 일반화 되었고 Wibro, HSDPA(Highspeed Downward Packet Access) 그리고 IEEE 802.11x 기반의 무선 랜(WLAN: wireless LAN) 접속 기능이 포함된 노트북 PC, 스마트폰 등의 사용자 수가 많으므로 모바일 IPTV 서비스를 위한 제반 여건이 갖추어진 상태이다. 앞으로도 스마트폰이나 태블러 PC 등의 모바일 멀티미디어 기기의 사용자는 지속적으로 증대될 것이므로 모바일 IPTV 서비스의 수요 역시 지속적으로 증가할 것으로 보인다 [4].

모바일 IPTV 서비스가 활성화되기 위해서는 QoS (Quality of Service) 보장, 콘텐츠 보안, 서비스 가입자에 대한 인증, 이동성 등에 대한 기술적 문제가 해결되어야 한다 [5]. 현재 국내 표준화를 위해 구성된 TTA PG 219 산하에 모바일 IPTV 기술을 연구하기 위한 실무 반(WG 2193)은 ITU-T IPTV Focus Group의 6개 WG 에서 연구되고 있는 기술들 중 모바일 IPTV와 관련 있는 기술들 중 기본적인 IPTV 이슈를 포함하여 핸드오프, 이동성 지원기술, Data Scalability, Codec, Service Discovery & Selection, Cross-Layer QoS 등 관련기술들을 중심으로 연구할 계획이다 [4].

본 논문은 모바일 IPTV의 가입자의 서비스 접근 통제를 위한 가입자 인증 성능의 개선을 다루었다. 특히, 기존의 IEEE 802.1X의 취약점을 보완하여 무선 IPTV에 적용시킬 수 있는 보다 강화된 인증 및 보안이 유지될 수 있고 휴대용 IPTV 기기로서 이동성을 지원할 수 있도록 핸드오프 시에도 빠른 재 인증과 동일 수준의 보안이 유지될 수 있는 인증 방법을 제시하였다. 이를 위해 기존 802.1X 의 보안 취약점에 대하여 분석하고 WEP키를 대체하는 세션키의 생성을 위해 이용될 디피-헬먼 키 교환 방식(Diffie-Hellman Key Exchange)과 타원곡선암호화 이론에 대하여 알아보았으며 IPTV를 무선 환경에 적용시키기 위해 강화된 인증, 보안 방법에 대하여 제안하였다. 마지막으로 제안한 인증 방법과 기존의 메커니즘을 모의실험을 통해 비교 분석 및 성능 평가를 하고 요약을 통해 결론을 맺었다.

Ⅱ. 제안된 인증 프로토콜

2.1 개요

기존 802.11b의 인증 메커니즘을 위해 사용된 SSID나 MAC address Filtering, Static WEP key 방식은 도청 공격에 의한 위장이 쉽고 WEP키는 전수 공격에 취약하며 IV 및 키 스트림 재사용 문제가 발생하여 안전한 사용자 인증 및 통신을 보장하지 못한다. 이를 보완하기 위한 802.1X의 방법은 EAP를 기반으로 해시 함수를 이용하거나 Kerberos, 인증서, OTP(One Time Password)등의 다양한 인증 메커니즘을 제공하고 있지만 여전히 중간자 공격이나 스푸핑 공격 그리고 구조적 원인에 의한 서비스 거부 공격에 노출되어 있다 [6].

모바일 IPTV는 기존의 802.1X 방식의 인프라를 통해 서비스될 가능성이 크므로 이러한 취약점을 보완하여 보다 안전한 인증과 데이터 전송이 가능하도록 상호인증을 통한 강력한 기밀성 유지가 필요하다. 특히 모바일 IPTV 단말의 특성 상 제한된 H/W 자원을 고려하여 인증 과정의 오버헤드를 줄이기 위해 복잡하고 많은 계산이 필요한 인증 작업은 유선 네트워크에 연결된 AP와 인증서버에서 수행하게 하고 이동 단말은 최소한의 인증만을 유지하도록 하는 것이 제안된 인증 프로토콜의 핵심이다.

본 논문에서 제안하는 인증방법은 모바일 IPTV에 적용될 수 있도록 보다 강화된 인증과 데이터 통신을 위해 기존의 방식에서 암호화를 위해 사용되었던 WEP 키를 세션키로 대체하고 세션키 생성 이후의 인증데이터 교환은 AES(Advanced Encryption Standard) 대칭키 암호방식으로 이루어진다. 사용자 인증과 하드웨어(H/W) 인증을 분리하며 Device 인증을 강화하기 위해 별도의 초기 등록과정을 추가하였다. 모바일 IPTV 단말기가 어느 한 AP 구역에서 다른 AP 구역으로 이동하여 IPTV 세션을 핸드오프할 때 AP 간의 상호 인증을 통해 IPTV 서비스 가입자에 대한 재인증 과정의 오버헤드를 줄일 수 있는 방법을 제시한다.

2.2 초기 등록 과정

초기 등록 과정은 모바일 IPTV 단말기의 인증에 필요한 정보를 인증서버에 등록하는 과정이다. 그림 2는 이 과정의 메시지 교환도이다. 모바일 IPTV 사용

그림 1. 모바일 IPTV 단말기의 초기 등록 과정

자는 웹 브라우저를 이용하여 IPTV 사용자 등록 페이지에 로그인하고 사용자 정보를 이용하여 인증서버로부터 UAN(User Authentication Number)를 받는다. 사용자가 자신의 모바일 IPTV 단말기의 웹 브라우저를 통해 UAN을 입력하면 IPTV 단말기는 인증서버에 UAN을 제시하고 OTP를 받고 이를 이용하여 자신의 MAC 주소, BIOS 번호 등의 H/W 정보를 암호화하여 인증서버로 전송한다. 이때 단말기와 인증서버 간에는 SSL(Secured Session Layer) 등과 같은 안전한 전송 경로가 사용된다고 가정한다. 인증서버는 단말기의 H/W 정보를 이용해 인증키 KAuth2를 생성하고 hash 한 후 보관한다. KAuth2는 추후 인증 과정에서 단말기가 생성한 H/W 인증키를 검증하는데 사용된다.

2.3 최초 접속 과정

최초 접속 과정은 모바일 IPTV 사용자가 IPTV 서비스를 이용하기 위해 자신의 단말기를 인증 받고 서비스 서버에 접속하려고 시도하는 과정이다. 그림 2는 모바일 단말기가 인증서버로부터 인증을 받는 과정을 나타낸 것이다.

모바일 IPTV 단말기는 AP와 미리 공유된 비밀키 Ks를 이용하여 자신의 공개 정보 Ya와 사용자 정보 IDua를 암호화하여 전송하면 AP는 인증서버의 공개키(Kpb)로 비밀키 Ks와 사용자 정보를 암호화하여 인증서버로 보낸다. 사용자 정보는 보안의 강도에 따라 인증서 대신에 ID, Password 등의 개인정보로 대체될 수 있다. 인증서버는 제공받은 사용자 정보를 이용하여 사용자 인증키인 KAuth1을 생성하고 해시한 후 자신의 서명을 덧붙여 비밀키 KS로 암호화하여 AP로 전송한다. AP는 이에 자신의 공개 정보 Yap를 덧붙여 비밀키 KS로 암호화하여 단말로 전송한다.

단말과 AP는 ECC-DH 키 교환 프로토콜을 이용하여 세션키를 교환한다. 단말과 AP는 개인키로 쓰일 Random Number a와 b를 각각 생성하고 단말의 공개키 Ga mod p와 AP의 공개키 Gb mod p를 각각 계산한다. 이들을 공유 비밀키 Ks로 암호화하여 교환한다. 단말은 AP의 공개키와 자신의 개인키 a로 Kab=(Gb)a mod p를 계산한다. AP는 단말의 공개키와 자신의 개인키 b로 Kba=(Ga)b mod p를 계산한다. Kab=Kba 이므로 단말과 AP는 새로운 공통의 비밀키를 갖게 되는데 이것이 단말과 AP 사이의 세션키 SK이다.

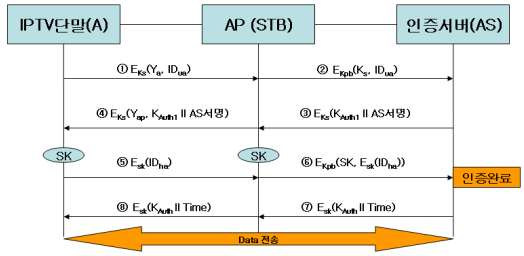

그림 2. 모바일 IPTV 서비스에 최초 접속하기 위한 인증 과정

이제 단말은 모바일 IPTV 서비스 접속을 위한 인증을 받기 위해 세션키 SK로 자신의 IDua를 암호화하여 AP로 보낸다. 세션키를 이용한 암호화 통신은 128bit AES 방식을 이용한다. AP는 세션키 SK와 세션키로 암호화된 단말 ID 값 Esk(IDua)을 인증서버의 공개 키 Kpb로 암호화하여 인증서버에 전송하면 인증서버는 초기 등록 과정을 통해 등록된 단말의 H/W 정보로 KAuth3를 생성하고 초기 등록에서 생성된 KAuth2와 비교하여 검증한다. 검증이 완료되면 KAuth1과 KAuth3를 이용하여 최종 인증키 KAuth를 생성하고 Time Stamp와 함께 단말로 전송하여 인증을 완료한다. AP와 인증서버 간에 VPN 등의 안전한 통신 환경이 구축되어있다고 가정하면 AP와 인증서버 구간에서는 암호화를 생략할 수 있다.

2.4 AP간 이동 및 재접속 과정

모바일 IPTV 단말기가 인접한 AP 사이를 이동할 때에는 AP 상호 간의 인증이 이미 완료되어 이들끼리 신뢰 관계가 있고 안전한 데이터 전송 채널이 형성되어 있다고 가정한다. 대개의 경우 공용 AP들은 통신 사업자나 ISP(Internet Service Provider)의 관리 아래에 있고 사설 AP들 역시 통신 사업자나 ISP에 일정 대역을 대여하는 형태로 운영되어야 하므로 이들의 관리를 받게 되어 AP 간의 신뢰성 보장이나 안전한 데이터 전송 채널 구성이 가능하다는 가정은 유효하다.

단말기(MS: Mobile Station)가 AP(A)에서 인접 AP(B)로 이동하기 위해 이동요청(Re-associate request)을 AP(B)에 보내면 AP(B)는 AP(A)에 Handoff-Req로 핸드오프 정보를 요구한다. AP(A)는 Handoff-Resp 메시지에 자신의 ID, 세션키(SK), 단말기의 인증정보(Ya, IDua)를 보낸다. AP(B)는 자신의 무선 자

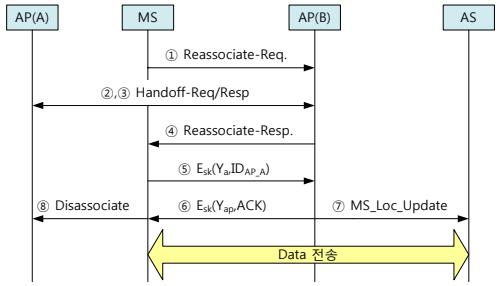

그림 3. AP간 이동 및 모바일 IPTV 서비스 핸드오프 과정

원의 상태와 AP(A)로부터 인수한 핸드오프 정보를 검토하여 단말기에 접속 가능 여부를 Reassociate-Resp 메시지로 응답한다.

단말기가 AP(B)에 접속할 수 있는 경우, 단말은 AP(A)와 공유한 세션키(SK)로 자신의 공개 정보와 이전 AP의 ID(IDAP_A)를 암호화하여 AP(B)에게 전달한다. AP(B)는 이미 AP(A)로부터 인수한 세션키(SK)로 이를 복호화 할 수 있다. 세션키(SK)는 원래 AP(A)와 단말만 알 수 있었고 AP(B)는 AP(A)와의 상호 신뢰 관계 아래에서 안전 채널을 통해 세션키를 인수하므로 AP(B)는 단말을 신뢰할 수 있고 단말도 AP(B)가 신뢰할 수 있는 AP임을 확인할 수 있다. 핸드오프를 마무리하는 단계로 단말기는 AP(A)에 Disassociate 메시지로 접속 종료를 통보하고 AP(B)는 인증서버에 단말의 위치가 자신에게 소속되었음(단말기의 위치가 변경되었음을) Loc_Update 메시지로 인증서버(AS)에 통보한다. 이와 같이 모바일 단말기가 AP들 사이를 이동할 때 세션키 생성이나 재인증 작업이 필요 없어서 AP 간의 모바일 IPTV 서비스의 핸드오프 시간을 단축할 수 있게 된다.

Ⅲ. 성능 평가

3.1 제안 인증방법과 기존 메커니즘의 비교

본 장에서는 논문에서 제안하는 인증 방법의 성능 개선을 검증하기 위해 기존의 인증 방법의 성능과 비교하였다. 성능 비교 지표는 인증을 위한 계산 시간이다. 비교 대상이 된 기존 인증 방법은 무선 인증을 위해 널리 사용되고 있는 802.1X의 대표적인 2가지 방식인 EAP-MD5와 EAP-TLS방식인데 이들과 제안된 인증 방법의 메커니즘은 표 1과 같다 [7]-[9].

표 2는 최초 접속 단계에서 만말기와 AP 및 인증서버 간에 인증이 완료되기까지 클라이언트(즉, 이동단말)가 수행하는 비대칭키 암호연산과 대칭키 암호

표 1. 제안된 인증 방법과 기존 메커니즘의 비교

구 분	802.1X (MD5)	802.1X (TLS)	제안방법
키 생성	X	Yes	Yes
암호통신	동적 WEP Key	동적 WEP Key	ECC-DH 세션키
인증방식	단방향	양방향	양방향
인증서	X	O	선택가능
인증메커니즘	취약	안전	안전
H/W, User 동시인증	X	X	O
상호인증	X	O	O

표 2. 최초 접속 단계에서 인증방식별 시스템의 암호화 구성과 연산 시간

구 분	EAP-MD5	EAP-TLS	제안모델
비대칭키 암호연산	0회	2회	1회
대칭키 암호연산	1회	1회	4회

표 3. AP 간 이동 단계에서 인증방식별 시스템의 암호화 구성과 연산 시간

구 분	EAP-MD5	EAP-TLS	제안모델
비대칭키 암호연산	0회	2회	0회
대칭키 암호연산	1회	1회	4회

연산을 하는 횟수를 보여 준다. 표 3은 AP 간 이동 단계에서 단말기와 AP 및 인증서버 간에 인증이 완료되기까지 이동 단말장치가 수행하는 비대칭키 암호연산과 대칭키 암호 연산을 하는 횟수를 보여 준다. 일반적으로 비대칭키 암호연산 시간은 대칭키 암호연산 시간의 수백 배에서 수천 배 정도 [10],[11]로 알려져 있으므로 본 논문에서 제안된 인증 방식이 EAP-TLS에 비하여 최초 접속 시에는 2 배 정도 속도가 빠르고 핸드오프의 경우에는 대폭적으로 속도가 개선됨을 예상할 수 있다. 이와 같은 속도의 개선을 다음 절에서 시뮬레이션을 통해 확인하였다.

3.2 성능 평가 시뮬레이션 시스템

제안하는 인증 방법과 기존의 인증 방법들의 성능을 비교하기 위해 시뮬레이션을 실시하였다. 이를 위하여 Client, AP, 인증서버의 통신환경은 소켓 통신을 이용하였고 JDK 1.4.2 환경에서 ECLIPSE 3.1에 클

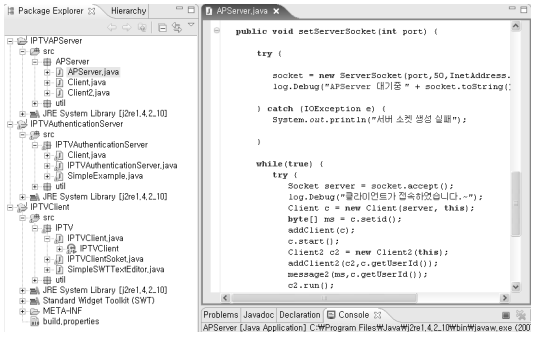

그림 4. 모의시험 프로그램의 구조

라이언트를 위한 인터페이스로 SWT, JFace를 이용하여 개발되었다. 시뮬레이션 컴퓨터의 CPU는 Intel Core Duo(2.0GHz)이고 OS는 Windows XP(SP2)이고 Socket 라이브러리를 이용하였다.

AP와 인증서버는 각각 하나의 프로세스 스레드로 동작하도록 했고 메시지 송수신 이벤트 출력 화면을 통해 인증과정을 확인할 수 있도록 하였다. 사용자 인증과정에서의 암호화와 세션키 생성 이후의 암호화는 모두 128 bit AES 방식을 이용하였다. 다음 그림 4는 구현된 모의시험 시스템 프로그램의 구조이다.

3.3 클라이언트 인증 시뮬레이션 결과

그림 5는 시뮬레이션 시스템 상에서 이동 단말기가 WLAN 및 모바일 IPTV 서비스에 최초 접속할 때 제안된 방식의 인증 시간을 각 단계별로 측정한 로그 화면의 예이다. 그림 6은 802.1x 방식과 제안된 방식의 인증 시뮬레이션 시간을 비교한 것이다. 각 방식의 인증시간은 최초 접속에서 인증이 완료 될 때까지의 시간이고 각 방법의 인증시간을 3회씩 측정하여 평균한 값이다. 이들의 값은 EAP-MD5 방법, EAP-TLS 방법, 제안된 방법에 대하여 각각 400 msec, 2500 msec, 그리고 1200 msec이다. 그림 7의 그래프로 보는 바와 같이 제안된 인증방법은 해시 함수를 이용한 단방향 인증 방법인 EAP-MD5보다는 더 걸리지만 제안된 방식은 세션키의 생성 및 인증서의 검증, 실제 DB의 Query, 최적화 등 여러 보안 성능을 강화하고 양방향 인증을 함에도 불구하고 EAP-TLS 방식보다는 인증 속도가 향상되어서 더 적은 시간으로 보다 강화된 인증을 할 수 있음을 알 수 있다.

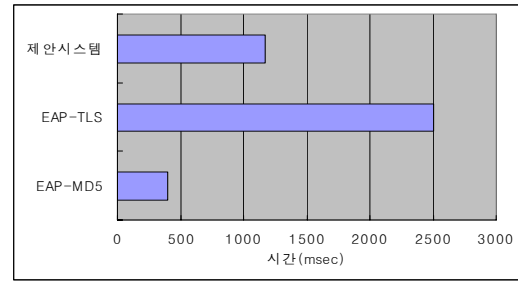

그림 6. 제안된 방식과 기존 방식의 성능 비교 (최초 접속)

그림 7은 시뮬레이션 시스템을 이용하여 이동 단말기가 WLAN의 AP 간을 이동하여 모바일 IPTV 서비스 핸드오프를 할 때 제안된 방식이 소비하는 시간을 단계별로 측정한 로그 화면의 예이다. 그림 8은 기존 802.1X 방식과 제안된 방식의 핸드오프 인증 시간을 비교한 것이다. 각 방법의 서비스 핸드오프 시간을 3회씩 측정하여 평균한 값을 취하였다. 이들의 값은 EAP-MD5 방법, EAP-TLS 방법, 제안된 방법에 대하여 각각 377 msec, 2433 msec, 그리고 428 msec이었다. 기존 방식인 EAP-MD5와 EAP-TLS 방식의 AP 간 재인증 시간은 모두 최초 접속의 경우와 비슷하나 제안된 방식은 재접속과 인증을 위하여 비대칭 암호

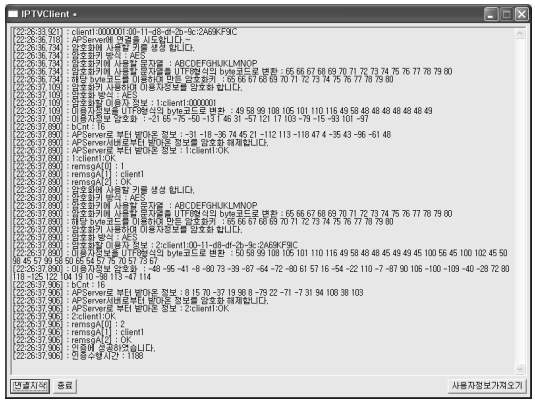

그림 5. 최초 접속 인증 절차 로그 화면

그림 7. 단말기 핸드오프 인증 절차 로그 화면

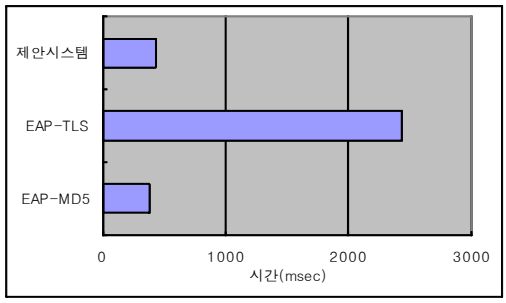

그림 8. 제안된 방식과 기존 방식의 성능 비교 (AP 간 이동)

화 연산을 사용하는 키 분배 과정이 없이 최초 접속 시에 할당된 세션키만을 이용하여 인증을 하므로 시간이 대폭 감소되었음을 알 수 있다.

이때 제안 방식이 표 3에 정리한 바와 같이 4 회의 대칭키 연산을 함에도 불구하고 2회의 대칭키 연산만을 하는 EAP-MD5 방식에 비하여 4 배가 아니라 약간 증가한 비슷한 시간이 걸리는 이유는 각 방식에 대한 시뮬레이션 초기에 단말기와 AP 간에 메시지 교환을 위한 소켓(Socket)을 연결하는데 걸린 시간이 공통적으로 포함되어 있기 때문이다.

Ⅳ. 결론 및 향후 과제

본 논문에서는 모바일 IPTV도입에 필요한 조건 중 무선 랜 구간에서 강화된 인증과 보안에 초점을 맞추었고 기존802.1x의 취약성을 분석하고 보완하여 모바일 IPTV단말에 적용시킬 수 있는 인증방법을 제안하였다. 제안된 인증방법이 기존의 802.1X 방식에 비하여 다음과 같은 5가지의 개선을 보임을 시뮬레이션 실험으로 확인하였다.

1. 기존 WEP 키를 ECC-DH 방법으로 교환되는 세션키로 교체함으로써 무선구간에서의 기밀성이 강화되었다.
2. 공개키 방식과 해시 함수를 이용하여 단말기, AP 및 AS 간의 상호인증과 무결성을 보장하였다.
3. 단말의 사용자 정보와 H/W정보를 분리하여 전송하고 이들을 통합적으로 인증함으로써 모바일 IPTV의 과금을 위한 보다 강화된 인증을 실현하였다.
4. AP 간 이동 및 재접속 시 인증과정을 반복하지 않고 세션키와 인증키 전송만으로 인증을 완료하도록 하였다.
5. 모바일 IPTV의 H/W제약을 극복하기 위해 비대칭키 인증과 같이 계산량이 많고 복잡한 과정은 H/W 자원이 비교적 풍부한 AP와 인증서버 쪽으로 분산시켜 인증에 필요한 오버헤드를 최소화 시켰다.

참 고 문 헌

〔1〕 ITU-T Focus Group on IPTV, http://www.itu.int/ITU-T/IPTV, 2006.

〔2〕 “Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i,” NIST, 2007.

〔3〕 N. Borisov, I. Goldberg, D. Wagner, “Intercepting Mobile Communications; The Insecurity of 802.11, International Conference on Mobile Computing and Networking,” pp.180-188, 2001.

〔4〕 박수홍, 황철주, “IPTV이동성 지원 기술과 Mobile IPTV 표준화 동향,” TTA 저널, 제107권, 2007.

〔5〕 Soohong Park, Seong-Ho Jeong, “Mobile IPTV: Approaches, Challenges, Standards, and QoS Support,” IEEE Internet Computing, Vol.13, No.3, pp.23-31, May/June 2009.

〔6〕 홍성균, “강화된 사용자 인증 및 기밀성을 지원하는 무선 랜 보안시스템,” 2005. 8.

〔7〕 이주남, 이구연,“빠른 핸드오프를 지원하는 PKI 기반의 무선 랜 인증기법설계,” *정보통신논문지*, 제7권, 2003.

〔8〕 김병기, 홍상선, 전영길,“유비쿼터스 무선환경을 위한 개인 상호인증 시스템,” *한국 인터넷 정보학회* 제5권 1호, 2004. 2.

〔9〕 왕기철, 정병호, 조기환,“이동 애드혹 네트워크에서 세션키 설정 방안,” *정보과학회논문지: 정보통신* 제 31권 제 4호, 2004. 8.

〔10〕 최영철, 박상준, 원동호,“클라이언트-서버환경에 적합한 효율적인 인증서 상태 및 경로검증 시스템,” *정보보호학회*, 13권 1호, 2003. 2.

〔11〕 Lisa Wu, Chris Weaver, and Todd Austin, “CryptoManiac: A Fast Flexible Architecture for Secure Communication,” Proceedings in 28th Annual International Symposium on Computer Architecture, Vol., No., pp.110-119, June, 2001.

백 종 규 (Jong-Gyu Baek) 정회원

1996년 2월 인하대학교 섬유공학과 학사
2008년 2월 한양대학교 컴퓨터공학과 석사
2007년 11월 Alcatel-Lucent Korea (Bell Labs Seoul) 차장
2009년 12월~현재 Hewlett Packard Korea 부장
<관심분야> Network Security, Wireless Network, Information Security, Mobile Internet

손 규 식 (Kyu-Seek Sohn) 정회원

1982년 2월 한양대학교 전자공학과 학사
1984년 2월 한양대학교 전자통신공학과 석사
2003년 8월 한국과학기술원 전자전산학과 박사
2002년 4월 LG전선(주) 광통신 연구소 전임연구원
2004년 3월~현재 한양사이버대학교 정보통신공학과 조교수
<관심분야> Network Reliability, Mobile Internet, Ad-hoc Networks, Information Security

조 인 휘 (Inwhee Joe) 정회원

1983년 2월 한양대학교 전자공학과 학사
1994년 12월 미국 University of Arizona, Electrical and Computer Engineering, M.S.
1998년 9월 미국 Georgia Tech, Electrical and Computer Engineering, Ph.D.
1992년 12월 (주) 데이콤 종합연구소 선임연구원
2000년 6월 미국 Oak Ridge 국립연구소 연구원
2002년 8월 미국 Bellcore Lab (Telcordia) 연구원
2002년 9월~현재 한양대학교 컴퓨터공학부 교수
<관심분야> Mobile Internet, Cellular System and PCS, Sensor Networks, Network Security