이동 장비에서 안전한 IPTV 서비스를 사용하기 위한 사용자 인증 메커니즘

정회원 정 윤 수*, 김 용 태**°, 박 길 철***, 이 상 호****

User Authentication Mechanism for using a Secure IPTV Service in Mobile Device

Yoon-Su Jeong*, Yong-Tae Kim**°, Gil-Cheol Park***, Sang-Ho Lee**** ***Regular Members***

요 약

멀티미디어 콘텐츠를 초고속으로 제공하기 위한 IPTV 기술은 기존 네트워크 기술, 멀티미디어 기술 및 인터넷 기술 등을 결합하여 구축된 망이다. 그러나 현재 운용되고 있는 인터넷, 방송 및 웹 기술들은 이동장비를 통해 콘텐츠 서비스를 제공받는 사용자와 콘텐츠 서버간의 안전성 문제가 보장되어있지 않기 때문에 IPTV에 최적화되어 있지 않다. 이 논문에서는 콘텐츠를 제공받는 사용자가 이동장비를 통해 선택한 서비스를 안전하게 수신받기 위한 이동 장비와 콘텐츠 서버간의 사용자 인증 메커니즘을 제안한다. 제안된 메커니즘은 요금을 납부한 사용자의 서비스를 불법적으로 이용하는 사용자를 예방하기 위해 사용자 자신이 생성한 난수와 인증토큰을 사용하고 있다. 또한 제안 프로토콜은 사용자의 이동장비에 부착된 자바카드와 권한부여 서버사이에 공유키를 사용하여 사용자 정보, 사용자 프로파일과 같은 민감한 데이터를 암호화한 후 MAC을 사용하여 무선 구간에서 자주 발생하는 reply 공격과 man-in-the-middle 공격을 예방하고 있다.

Key Words : IPTV 서비스(IPTV Service), 사용자 인증(User Authentication), 콘텐츠 보안(Content Security), 이동 장비(Mobile Equipment)

ABSTRACT

IPTV technology for providing multimedia content with high-speed is the network which combines existing network, multimedia and internet technology etc. But internet, broadcasting and web technologies which is now being used is not optimized to IPTV because the security problem between user who gets content service through mobile units and content server is not guaranteed. This paper proposes user certification mechanism between mobile device and content server to receive the service which the user for the content chooses by mobile device safely. The proposed mechanism uses the random number which user creates and certification token for preventing illegal user who uses other's service that already paid. Also the proposed protocol encrypts the delicate data like user's information or profile using shared-key between java card attached on user's mobile device and grant server and then prevents reply attack which happens often in wireless section and man-in-the-middle attack by MAC.

※ 본 연구는 지식경제부 지역혁신센터사업인 민군겸용보안공학연구센터 지원으로 수행되었음
* 충북대학교 전자계산학과 네트워크보안 연구실(bukmunro@gmail.com)
** 한남대학교 멀티미디어공학부 강의전담 교수(ky7762@hannam.ac.kr)(° : 교신저자)
*** 한남대학교 멀티미디어공학부 교수(gcpark@hnu.kr), **** 충북대학교 전기전자컴퓨터공학부 교수(shlee@chungbuk.ac.kr)
논문번호 : KICS2008-11-507, 접수일자 : 2008년 11월 17일, 최종논문접수일자 : 2009년 3월 18일

Ⅰ. 서 론

최근 인터넷은 ADSL/VDSL(Asymmetric Digital Subscriber Line/Very high-speed DSL), 케이블 모델 그리고 ETTS(Ethernet To The Subscriber)와 같은 가입자 액세스 네트워크가 수십 Mbps에서 수백 Mbps까지 지원을 확대해나가고 있다. 또한 인터넷은 VoD 뿐만아니라 위성 DMB, 지상파 DMB 등의 방송 서비스를 제공함으로써 IPTV 서비스에 대한 연구가 활발히 진행되고 있다[1]. 그러나 현재까지 IPTV 시스템은 표준 모델이 존재하지 않아 기존 방송 서비스에서 사용하는 CAS(Conditional Access System)을 이용하여 서비스에 접근하는 사용자의 접근 여부를 제어하고 있다.

IPTV 서비스는 방송 서비스와 주문형 서비스를 모두 지원하고 있어 방송 서비스에서 사용하는 CAS와 DRM만으로는 안정성이 충분히 제공되지는 않는다[4,5,6]. IPTV 서비스를 위해 최근 연구에서는 DRM으로 기존의 CAS를 대체하는 방법, CAS 기반의 DRM 구축 방안 등이 제시되고 있지만 그 실효성에 많은 문제점이 있다. 또한 IPTV 서비스를 제공받는 사용자의 이동장비는 CAS의 구조적인 문제로 인하여 VoD와 PVR(Personal Video Recorder) 등의 기능에 직접적으로 대응하기 어려운 문제점을 가지고 있으며 사용자의 이동장비와 콘텐츠 서버간의 무선 구간에서 발생되는 불법 사용자의 서비스 이용에 적당한 대응책을 찾지 못하고 있다.

이 논문에서는 IPTV 서비스를 지원하는 이동 장비와 콘텐츠를 제공하는 콘텐츠 서버간의 안전한 콘텐츠 서비스를 제공받기 위한 사용자 인증 메커니즘을 제안한다. 제안된 메커니즘은 요금을 납부한 사용자의 서비스를 불법적으로 이용하는 사용자를 예방하기 위해 이동장비의 자바카드와 권한부여 서버 사이에 난수와 인증토큰을 사용하고 있다. 특히 사용자의 이동장비 내에는 사용자 정보, 사용자 프로파일과 같은 민감한 데이터를 암호화한 후 메시지 무결성 검증을 위해 MAC을 사용하고 있다. 제안 메커니즘은 사용자의 이동장비에서 MAC을 사용함으로써 무선 구간에서 자주 발생하는 reply 공격과 man-in-the-middle 공격을 예방하고 있다.

이 논문의 구성은 다음과 같다. 2장에서는 IPTV 서비스와 IPTV 보안 기술에 대하여 분석한다. 3장에서는 사용자의 이동장비와 콘텐츠 서버간의 안전한 서비스 수신을 위해 사용자의 수신자격을 판별할 수 있는 사용자 인증 메커니즘을 제시하고, 4장에서는 제안 프로토콜에 대한 효율성 및 보안성에 대하여 분석·평가한다. 마지막으로 5장에서는 이 연구의 결과를 요약하고 향후 연구에 대한 방향을 제시한다.

Ⅱ. 관련연구

2.1 IPTV 서비스

IPTV(Internet Protocol TV)는 차별화된 초고속 광대역 네트워크를 이용해 디지털영상서비스, 양방향 데이터 서비스 및 다양한 개인 맞춤형 서비스를 TV를 통해 제공하는 방송과 통신간의 대표적 융합 서비스이다[1]. 즉 IPTV는 방송 및 인터넷 서비스는 물론 주문형 비디오(VoD), 전자 프로그램(EPG), T-커머스, 방송 프로그램 연동형 데이터 베이스와 같은 새로운 양방향 콘텐츠를 제공하는 등 통신과 방송 서비스를 모두 이용할 수 있다. 특히, IPTV의 가장 큰 특징은 기존 TV의 일방적이고 수동적인 서비스에서 탈피, 이용자가 실제 TV를 보면서 능동적으로 반응을 보일 수 있다. 기존 TV 방송같은 채널 선택은 물론 비디오 대여점에 가지 않고도 리모컨으로 간단히 최신 영화를 신청해 보는 주문형(On Demand) 서비스가 가능하다.

2.2 IPTV 서비스 모델

현재 FG IPTV에서는 대용량의 IPTV 멀티미디어 서비스(방송형 서비스)의 전송을 효율적으로 제공하기 위한 기능적 요구사항과 기능들에 대해서 표준화를 진행하고 있다. IPTV 서비스 요구사항은 망의 장비에서 멀티캐스트 기능을 가지고 있는지 여부에 따라서 순수 IP 멀티캐스트 모델, 대안 멀티캐스트 모델 그리고 하이브리드 모델로 구분된다. 순수 IP 멀티캐스트 모델은 IP 네트워크를 구성하는 망 장비에서 기본적으로 멀티캐스트 전송을 가능하게 하는 멀티캐스트 트리 구성 및 라우팅 기능

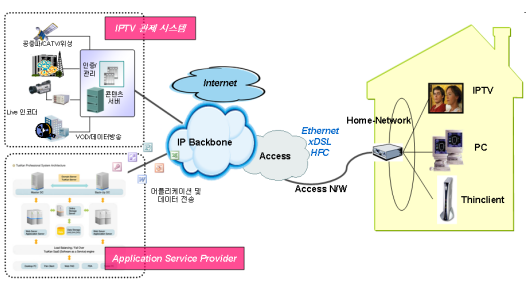

그림 1. IPTV 서비스 구성도

을 제공해주는 환경에서 IPTV 멀티캐스트 서비스를 제공하는 모델이다. 대안 멀티캐스트 모델은 IPTV 네트워크에서 멀티캐스트 전송이 불가능한 환경에서 효율적인 IPTV 서비스를 제공하기 위해서 CDN, P2P와 같은 추가적인 프로토콜을 사용하여 멀티캐스트 전송 서비스를 제공하는 모델이다. 하이브리드 모델은 모든 IPTV 네트워크에서 멀티캐스트 전송이 불가능한 환경에서 일부 구간은 IP 멀티캐스트 프로토콜을 이용하고, 일부의 구간은 대안 멀티캐스트 모델을 사용하여 IPTV 멀티캐스트 전송 서비스를 제공하는 모델이다.

2.3 이전연구

IPTV 서비스 보안을 위해 최근까지 연구된 브로드캐스트 암호화[7,8,9]와 멀티캐스트 키 관리[10,11,12,13]와 같은 기술들은 pay-TV 시스템의 액세스 제어를 위해 응용되고 있다. 이 기술들은 일반적으로 하나의 그룹만을 위한 권한을 고려하고 있다. 이 방법들은 시스템의 많은 통신과 계산 부하가 존재하게 된다. 브로드캐스트 암호 기법을 위해서는 고정 계층에 위치하기위해 모든 사용자에게 키 설정 값을 부여한다. 브로드캐스트 암호 기법[8,9]을 위해서는 불법적인 사용자를 무효화시키는 기능에도 불구하고 통신과 계산 로드가 크게 나타난다. 반면 멀티캐스트 키 관리 기법[10,11,12,13]은 동적 사용자 계층을 포함하고 있어 제공자와 모든 사용자 사이의 계층 관리와 동기화가 가능하다. [14]는 워터마크 기술을 기반으로 Pay-TV에 적용시킨 기법을 제안하고 있다. 이 기법은 저작권 관리 문제를 처리하기 위해 동일 시간동안에 제어 액세스을 위한 마스크 프레임을 사용하였다.

Ⅲ. 이동장비를 위한 사용자 인증 메커니즘

3.1 시스템 구조

IPTV 서비스 환경에서 이동 장비를 사용하는 제안 메커니즘의 서비스 구조는 그림 2와 같다. 그림 2에서 제안 메커니즘의 서비스 구조를 구성하는 구성요소는 사용자 장비(User Equipment, UE), 응용 서버(Application Server, AS), WAP 프록시 게이트웨이(WAP Proxy Gateway, WPG), 콘텐츠 서버 그리고 EPC(Electronic Promgram Guide) 서버 등이 있다. 사용자 장비는 휴대폰, PDA 등을 의미하며 USIM 카드와 같은 장비가 사용자 장비 안에 부착된다. 응용 서버는 인식자 관리 서버, 인증서버 등

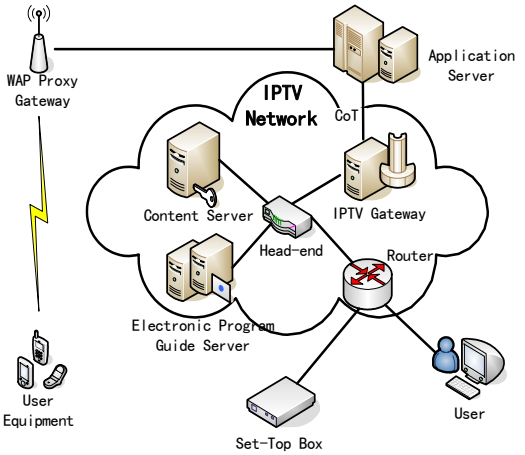

그림 2. 제안 메커니즘의 서비스 구조

으로 구성되며 IPTV 서비스를 요청하는 사용자들에게 쉽게 IPTV 서비스에 참여할 수 있도록 도와주는 기능이 있다. WAP 프록시 게이트웨이는 무선 응용 프로토콜(Wireless Application Protocol, WAP)에 기반하여 트래픽 안전성을 제공하기 위해서 유선 지역에서는 SSL를 제공하고 무선지역에서는 WTLS를 제공한다. 콘텐츠 서버는 사용자가 선택한 IPTV 서비스를 사용자에게 제공하기 위한 콘텐트 관리 및 서비스 등을 제공한다. EPC 서버는 사용자가 요청하는 IPTV 서비스에 대한 프로그램을 관리하는 기능을 한다.

사용자는 PC(Personal Computer)와 STB(Set-Top Box)와 같은 사용자 장치를 통해 IPTV 서비스를 요청하며 UE(User Equipment)는 이동성을 가지는 사용자 장비를 의미한다. 응용 서버는 IPTV 게이트웨이를 통해 IPTV 네트워크에 있는 EPC 서버와 콘텐츠 서버의 조건을 만족하는 프로그램의 정보와 내용을 요청한다. 응용서버가 IPTV 네트워크 외부에 위치하고 있는 통신 프로토콜을 알지 못하더라도 [1]처럼 오픈 APIs를 사용함으로써 게이트웨이를 통해 통신이 가능하다. 사용자 장비는 WAP 게이트웨이를 통해 인증 요청을 수행하며 인증 서버는 사용자를 검증하여 합법적인 사용자인지를 판별한다. IDENTITY 애플릿은 사용자 장비내에 포함되어 있으면서 UE의 사용자 인식자를 생성하여 AS게 전달하는 역할을 수행한다.

3.2 용어정의

제안 프로토콜에서 사용하는 주요 용어를 정의하면 표 1과 같다.

표 1. 제안 프로토콜의 용어 정의

용 어	정 의
UE	사용자 장치
AS	응용 서버
GW	게이트웨이
CP	콘텐트 제공자
ID_U	사용자 U의 인식자
HI	하드위에 인식자
ID_{UE}	사용자 장비의 정보
AC	인증결과 코드
UP	사용자 프로파일
E_X(M)	키 X을 사용함으로써 데이터 M의 대칭 암호
D_X(M)	키 X을 사용함으로써 데이터 M의 대칭 복호
S(s_X, M)	키 s_X를 이용하여 데이터 M의 서명
MAC_X(M)	키 X을 사용함으로써 데이터 M의 MAC
$Cert_A$	엔터티 A의 X.509 인증서
AT_X	X의 인증 토큰
X_{PK}	엔터티 X의 인증서의 공개키
X_{SK}	엔터티 X의 인증서의 개인키
t_X	엔터티 X에 의해 생성된 타임스탬프
TID	UE와 AS 간 사용된 세션 ID
$M_1 \parallel M_2$	M_1과 M_2의 연접 함수

3.3 IPTV 인증 프로토콜

제안된 IPTV 인증 프로토콜은 그림 3처럼 사용자 등록, 사용자 인증, 사용자 권한부여, 사용자 제어 등의 4가지 동작과정으로 구성된다. 사용자 등록은 IPTV 서비스를 제공받기를 원하는 사용자의 기본 정보를 등록하는 과정이고 사용자 인증은 등록된 사용자가 서비스를 제공받기 위해 서버로부터 인증을 부여받는 과정이다. 사용자 권한 부여 과정은 응용서버가 IPTV 서비스의 사용료를 지불한 사용자를 판별하는 과정이다. 마지막으로 사용자 제어는 사용자가 선택한 서비스 항목을 제공받기 위한 과정을 나타낸다.

3.3.1 IPTV 사용자 등록

IPTV 사용자 등록 과정은 이동 사용자가 IPTV 서비스에 가입되어야 동작되며 만일 이동 사용자가 가입이 이루어지지 않았다면 이동 사용자는 가입절차에 따라 가입을 수행한다. 가입이 완료되면 AS에는 가입이 완료된 이동 사용자와 AS간 공유될 마스터 키 K_S와 세션 인식자 TID가 쌍을 이루어 저장된다. 가입된 이동 사용자에 대한 정보 TID는 등록과 동시에 IPTV STB에 저장된다. 이동 사용자가 IPTV 서비스를 요청할 경우 IPTV STB에 저장되어 있는 정보 TID는 이동 사용자가 휴대하고 있는 휴대폰, PDA와 같은 장비내에 동일하게 저장한다.

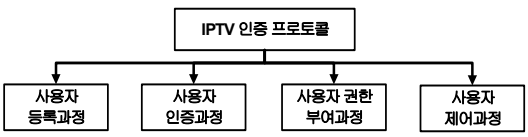

그림 3. IPTV 인증 프로토콜 동작과정

3.3.2 IPTV 사용자 인증 과정

IPTV 사용자 인증 과정은 이동 사용자가 IPTV 서비스를 요청할 경우 이동 사용자가 콘텐츠 서비스를 제공받을 수 있는지를 판별하는 과정이다. 콘텐트 제공자가 IPTV 사용자 인증 처리를 수행하기 전에 이동 사용자는 자신의 장비와 USIM 사이에 공유할 마스터 키 K_{USIM}를 AKA 메커니즘을 통해 부여받는다. 이동 사용자와 USIM은 공유할 마스터 키 K_{USIM}를 설정한 후 상호인증 처리절차를 수행하며 구체적인 처리절차 과정은 그림 4와 같다.

- 단계 1 : UE → USIM
  UE는 USIM 애플릿을 구동하기 위한 요청 메시지를 보낸다.
- 단계 2 : USIM ← UE
  USIM은 UE에게 전달받은 요청 메시지를 확인한 후 USIM의 인식자 ID_{USIM}와 USIM과 UE 사이에 공유할 공유키 키 K_{USIM}를 UE에게 전달한 후 UE는 전달받은 정보를 UE 장비에

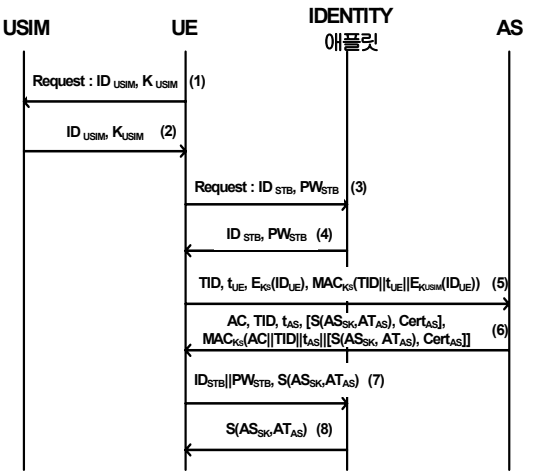

그림 4. IPTV 사용자 인증 처리과정

저장한다.

- 단계 3 : UE → IDENTITY 애플릿
  UE는 STB 하드웨어 인식자 ID_{STB}나 패스워드 PW_{STB}와 같은 IPTV 가입자 정보를 요청하기 위한 요청 메시지(request message)를 IDENTITY 애플릿에게 보낸다.
- 단계 4 : IDENTITY 애플릿 → UE
  IDENTITY 애플릿은 STB 하드웨어 인식자 ID_{STB}, 패스워드 PW_{STB}와 같은 사용자 정보 응답을 UE에게 전달한다.
- 단계 5 : UE → AS
  UE는 AS에게 인증 요청 메시지를 전달한다. AS에게 전달하는 요청 메시지에는 TID와 타임스탬프 t_{UE} 등이 포함된다. 사용자 정보는 K_S으로 암호화되어 있으며 메시지의 무결성을 위해 MAC을 사용한다.

$$\{\text{TID}, t_{UE}, E_{K_S}(ID_{UE}), MAC_{K_S}(\text{TID}\|t_{UE}\|E_{K_{USIM}}(ID_{UE}))\} \quad (1)$$

- 단계 6 : AS → UE
  AS는 수신된 TID를 사용하여 데이터베이스에서 TID와 일치하는 마스터 키 K_S를 검색하여 $D_{K_S}(ID_{UE})$를 복호화한 후 사용자 정보 ID_{UE}를 이용하여 권한이 있는 사용자 인지를 판단한다. AS는 사용자의 권한부여 여부에 따라 인증토큰 AT_{AS}와 인증 결과 코드 AC를 인증서와 함께 생성한다. 이 때, AS는 AS의 개인키로 인증토큰 AT_{AS}을 S(AS_{SK}, AT_{AS})처럼 서명하고 인증서 $Cert_{AS}$를 생성한 후 타임스탬프 t_{AS} 정보와 함께 UE에게 전달한다. 만약 사용자가 권한부여를 받지 못하였다면 서명 S(AS_{SK}, AT_{AS})와 인증서 $Cert_{AS}$는 메시지에서 제외한다.

$$\{AC, \text{TID}, t_{AS}, [\text{S}(AS_{SK}, AT_{AS}), Cert_{AS}], MAC_{K_S}(AC\|\text{TID}\|t_{AS}\|[\text{S}(AS_{SK}, AT_{AS}), Cert_{AS}])\} \quad (2)$$

- 단계 7 : UE → IDENTITY 애플릿
  UE는 데이터의 무결성을 체크하기 위해 AS로부터 전달받은 메시지를 검증한다. 만일 검증이 성공적으로 이루어지면 UE는 자바 카드의 IDENTITY 애플릿에 서명 S(AS_{SK}, AT_{AS})를 저장한다.
- 단계 8 : IDENTITY 애플릿 → UE
  IDENTITY 애플릿은 UE에게 단계 7에서 생성된 결과 값 S(AS_{SK}, AT_{AS})을 전달한다.

3.3.3 IPTV 사용자 권한 부여 과정

IPTV 사용자 권한 부여 과정은 IPTV 서비스에 대한 서비스 사용료를 지불한 정상적인 사용자를 판별하는 과정이다. IPTV 사용자 권한 부여에 대한 구체적인 동작과정은 그림 5와 같다.

- 단계 1 : UE → AS
  UE는 AS에게 IPTV 서비스에 대한 요청 메시지를 전달한다.
- 단계 2 : AS → UE
  AS는 정당한 IPTV 가입자인지를 판별하기 위해 UE에게 인증 토큰을 요청한다.
- 단계 3 : UE → IDENTITY 애플릿
  UE는 IDENTITY 애플릿에게 인증 요청 메시지를 전달한다.
- 단계 4 : IDENTITY 애플릿 → UE
  IDENTITY 애플릿은 UE에게 인증 토큰 S(AS_{SK}, AT_{AS})을 전달한다. 만일 IDENTITY 애플릿이 인증코드를 보유하고 있지 않으면 IDENTITY 애플릿은 UE에게 에러 코드를 응답 메시지로 보낸다.
- 단계 5 : UE → USIM
  UE가 수신된 인증 토큰이 정확한지를 검증한 후에 만일 UE가 에러 코드와 함께 응답 메시지를 수신했거나 인증 토큰이 맞지 않다면 UE는 세션을 종료하고 IPTV 서비스의 인증 처리 절차를 재시작한다. 만일 UE가 보유한 인증토큰이 정확하다면 USIM에게 메시지를 생성하기 위한 TID와 K_{USIM}를 요청한다. 이 때 요청 메시지는 AS에 대한 공개 이름 ID_{AS}이 포함되어 있어야 한다.
- 단계 6 : USIM → UE
  USIM은 K_{USIM}와 TID를 UE에게 전달하며 UE에게 전달된 정보는 AS의 ID_{AS}와 관련이 있다.
- 단계 7 : UE → AS
  IPTV 가입자인 UE는 AS에게 IPTV 서비스를 위해 서비스 요청 메시지에 인증 토큰 S(AS_{SK}, AT_{AS})을 포함시켜 전달한다. 전달 과정중에 UE는 사용자가 올바른 가입자인지를 판별하기 위해 요청 메시지에 마스터 키 K_S로 암호화된 MAC을 추가한다.

$$\{\text{TID}, t_{UE}, \text{S}(AS_{SK}, AT_{AS}), MAC_{K_S}(\text{TID}\|t_{UE}\|\text{S}(AS_{SK}, AT_{AS}))\} \quad (3)$$

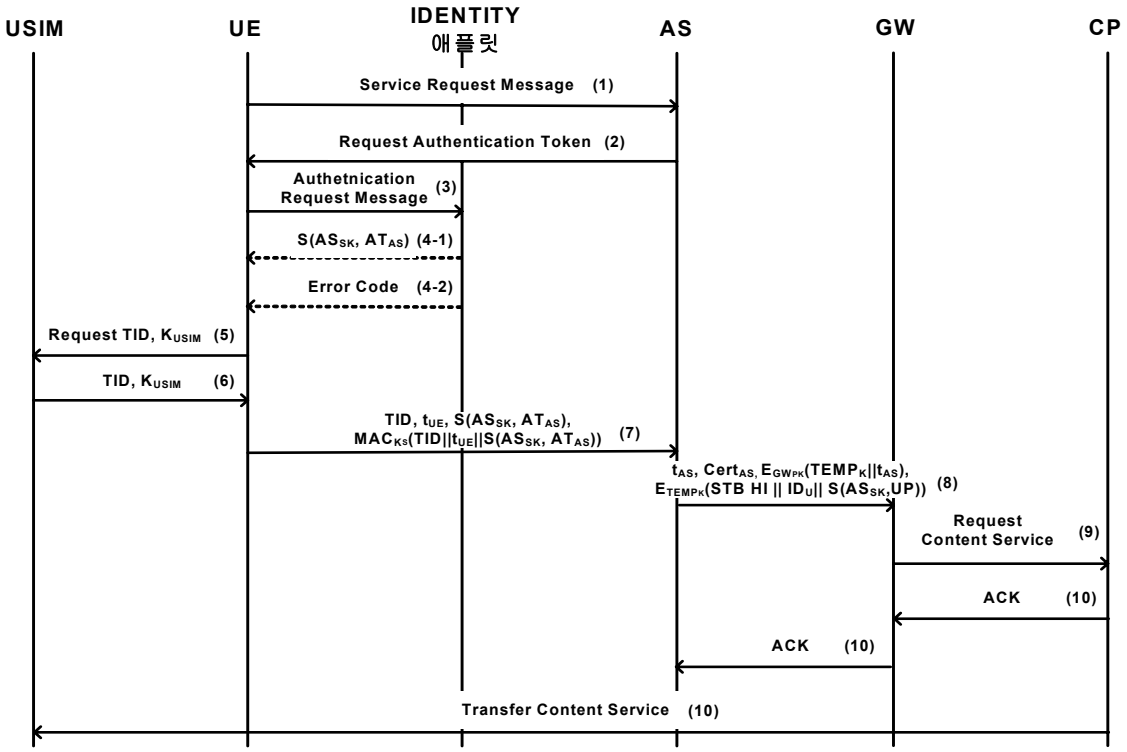

그림 5. IPTV 사용자 권한 부여 과정

- 단계 8 : AS → GW
  AS는 수신된 TID을 사용하여 데이터 베이스에 저장된 TID와 비교한 후 마스터 키 K_S를 검색한다. 만일 TID와 일치하는 마스터 키 K_S를 찾는다면 AS는 마스터 키 K_S로 새로 계산된 MAC_{K_S}와 함께 UE로부터 전달된 MAC_{K_S}를 비교 검증한다. 만일 무결성 체크가 실패한다면 AS는 UE에게 실패 인지 메시지를 보내고 세션을 종료한다. AS가 UE로부터 전달받은 인증 토큰 검증이 성공적으로 수행된다면 AS는 가입자의 정보를 참조할 수 있는 사용자 프로파일 UP을 생성한다. 사용자 프로파일 UP와 함께 AS는 STB HI와 사용자 인식자 ID_U를 암호화하기 위해 임시 비밀키 $TEMP_K$를 생성한다. 임시 비밀키 $TEMP_K$는 게이트웨이의 공개키 GW_{PK}로 암호화하여 생성된 정보들과 함께 게이트웨이에게 전달된다.

$$\{t_{AS},\ E_{GW_{PK}}(TEMP_K||t_{AS})\},\ E_{TEMP_K}(\text{STB } HI||ID_U||\text{S}(AS_{SK}, UP)), Cert_{AS}\} \quad (4)$$

- 단계 9 : GW → CP
  게이트웨이 GW는 AS_{PK}를 사용하여 AS의 서명 S(UP, AS_{SK})을 체크한다. 만일 검증이 성공한다면 게이트웨이 GW는 컨텐트 제공자(오픈 서비스 프레임워크)에게 수신된 메시지를 포워드한다. 컨텐트 제공자(오픈 서비스 프레임워크)는 수신된 메시지를 내부 네트워크에서 인식할 수 있는 적당한 메시지로 변환하고 CP에게 변환된 메시지를 전달한다.
- 단계 10 : CP → STB
  각 CP는 사용자 프로파일의 명확성(validity)을 체크한다. 만일 명확하다면 각 CP는 수신된 메시지에 포함된 사용자 파일과 함께 CP의 사용자 데이터를 비교한다. 그리고 특정 사용자의 STB에게 데이터를 전달하는 동시에 각 CP는 사용자에게 콘텐츠 서비스를 제공하는 동안 게이트웨이 GW와 AS에게 응답 메시지 ACK를 보낸다.

3.3.4 IPTV 이동 사용자 제어 과정

이동 사용자들은 게임, 교육, 쇼핑과 같은 양방향 실시간 서비스를 위해 STB에 연결한 TV와 함께 IPTV 콘텐츠를 이용한다. IPTV 이동 사용자 제어

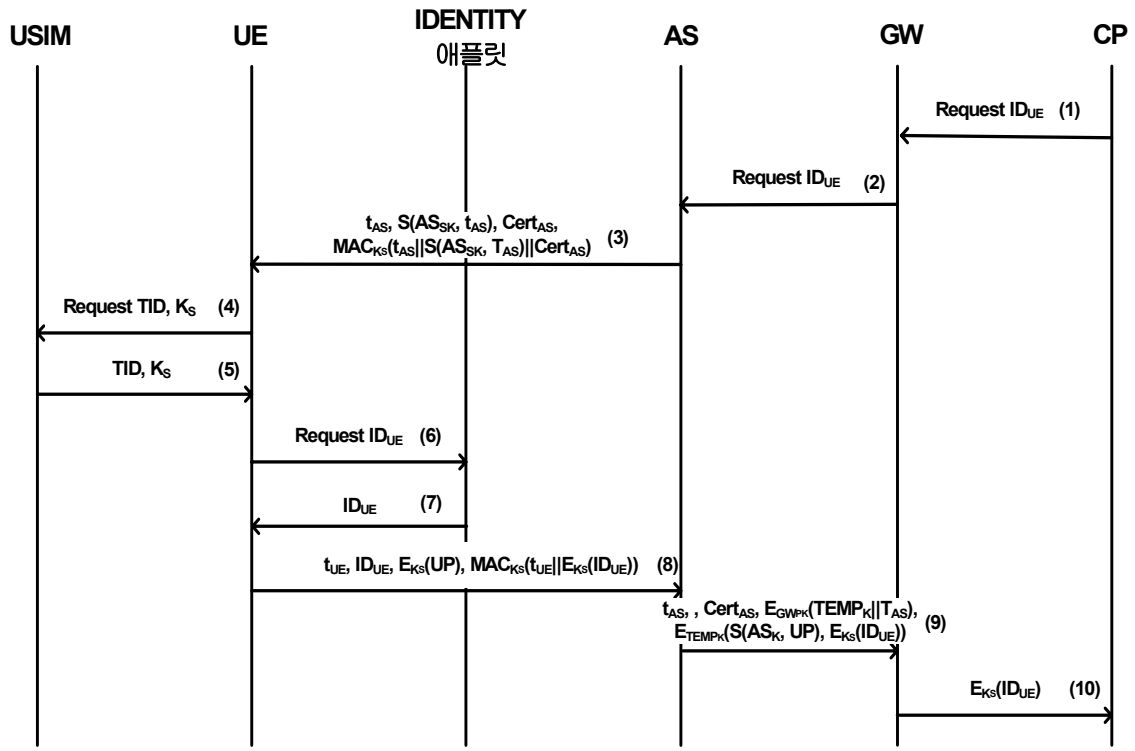

그림 6. IPTV 이동 사용자 제어 과정

과정에서는 이동 사용자가 사용하는 민감한 데이터를 STB를 사용하는 것처럼 이동 사용자의 민감한 데이터를 보장받을 수 있도록 이동 사용자를 제어하고 있다. IPTV 이동 사용자 제어 과정에 대한 구체적인 동작 과정은 그림 6과 같다.

- 단계 1 : CP → GW
  CP가 콘텐츠를 제공하려고 할 때 CP는 GW에게 이동 사용자 정보 ID_{UE}를 요청한다.
- 단계 2 : GW → AS
  GW는 AS에게 이동 사용자 정보 ID_{UE}를 재요청하고 요청된 데이터에 대한 전달 유·무를 결정한다.
- 단계 3 : AS → UE
  AS는 이동 사용자 요청 정보를 UE에게 전달하며 전달되는 AS의 메시지는 안전하여야 한다.

$$\{t_{AS},\ \mathrm{S}(AS_{SK},\ t_S),\ \mathcal{C}ert_{AS},\ MAC_{K_S}(t_{AS}\|\mathrm{S}(AS_{SK},\ t_S)\|\mathcal{C}ert_{AS})\} \quad (5)$$

- 단계 4 : UE → USIM
  UE는 AS의 서명을 체크한 후 서명이 정확하다면 UE는 USIM에게 K_S와 TID를 요청한다.
- 단계 5 : USIM → UE
  USIM은 UE에게 이전 명령의 K_S와 TID를 전달한다. 전달된 정보는 AS의 ID_{AS}와 관련이 있다. UE는 AS의 연관성을 위해 UE에서 계산된 MAC'_{K_S}와 AS로부터 전달받은 MAC_{K_S}을 비교 검증한다. 검증된 결과가 만약 정확하지 않으면 세션은 종료하고 연결은 보류한다.
- 단계 6 : UE → IDENTITY 애플릿
  만일 요청된 메시지가 IDENTITY 애플릿이나 ID에 의해 제공된 것이라면 UE는 이동 사용자에게 사용할 수 있는 메시지를 보여주지만 그렇지 않을 경우 UE는 사용자가 직접 자신의 정보를 UE 장비 화면에 보여주도록 한다. 이동 사용자는 정보 준비 과정을 수행하기 위해 수락 또는 거절하며 사용자 수락이 요청되면 UE는 IDENTITY 애플릿에게 데이터 요청을 전달한다. 만일 데이터가 존재하지 않으면 메시지는 제거되고 사용자는 직접적으로 정보를 입력한다.
- 단계 7 : IDENTITY 애플릿 → UE

IDENTITY 애플릿은 UE에게 요청된 사용자의 데이터를 전달한다.

- 단계 8 : UE → AS
  UE는 AS에게 단계 3에서 생성된 메시지를 전달한다.

$$\{ID_{UE},\ t_{UE},\ [E_{K_S}(\mathrm{UP})],\ MAC_{K_S}(t_{UE}\|[E_{K_S}(ID_{UE})])\} \quad (6)$$

- 단계 9 : AS → GW
  ID_{AS}는 UE로부터 요청된 사용자 프로파일과 사용자에 의해 제공된 데이터에 기반하여 GW에게 응답 메시지를 전송한다.

$$\{t_{AS},\ ,\ Cert_{AS},\ E_{GW_{PK}}(TEMP_K\|t_{AS}),\ E_{TEMP_K}(\mathrm{S(UP},\ AS_K)\|E_{K_S}(ID_{UE}))\} \quad (7)$$

- 단계 10 : GW → CP
  GW는 수신된 메시지 중 $E_{K_S}(ID_{UE})$를 컨텐트 제공자(오픈 서비스 프레임워크)에게 포워드한다. 컨텐트 제공자는 수신된 메시지를 내부 네트워크의 적당한 메시지로 변환하고 사용자 정보를 요청한 특정 CP에게 요청된 메시지를 보낸다. CP는 전달받은 메시지를 복호화한후 사용자 정보를 확인한다.

Ⅳ. 성능평가

4.1 실험 네트워크 구축

제안 메커니즘에서 사용자가 네트워크 1에서 네트워크 2로 핸드오버할 경우 게이트웨이 역할을 하는 기지국과 인증 서버간의 정보교환으로 네트워크를 이동하는 실험 네트워크 구성을 그림 7과 같이 가상으로 구축하여 실험하였다.

4.2 성능평가

그림 8은 네트워크를 이동하는 사용자 수에 따른 인증 서버(AS)의 전체 계산 지연을 보여주고 있다. 그림 8의 결과처럼 제안 프로토콜과 IPTV 표준 프로토콜은 네트워크간 이동하려고 하는 이동 사용자의 수가 증가 할수록 인증 서버의 계산 로드량이 비례적으로 증가하고 있다. 제안 프로토콜에서 네트워크간 사용자가 1 홉으로 네트워크를 이동할 경우 제안 프로토콜의 인증서버는 IPTV 표준보다 평균 4.6%의 낮은 계산 로드량을 보이지만 4홉이상으로 네트워크사이를 이동사용자가 이동할 경우 제안 프

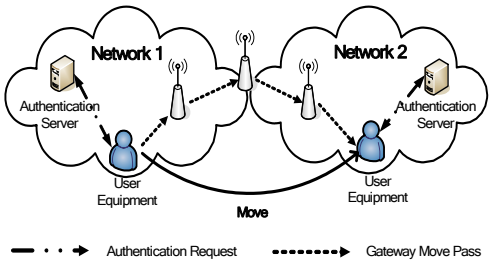

그림 7. 실험 네트워크 구성

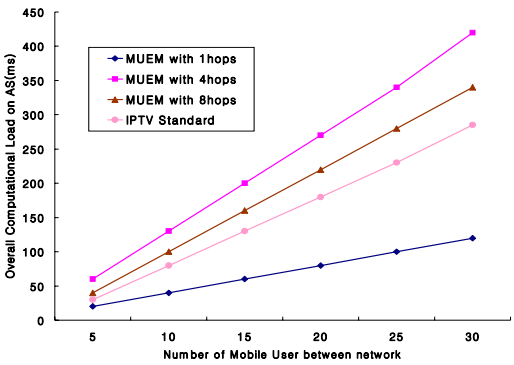

그림 8. 네트워크간 이동 사용자 수에 따른 응용 서버의 전체 계산 로드량

로토콜은 IPTV 표준보다 3.1%의 높은 계산 로드량이 나타났다. 이 같은 결과는 대부분 IPTV 서비스 구조에서 네트워크를 이동하는 이동 사용자가 2홉 이내에서 네트워크를 이동하기 때문이다.

그림 9은 이동 사용자의 속도에 따른 인증 서버에 저장된 인증 정보의 계산량을 보여주고 있다. 그림 9의 결과처럼 이동 사용자의 속도가 9km/m 이상 증가하면 인증 정보의 전체 계산량은 $\log_2 n$크기로 급격하게 증가하게 되며 이동 사용자의 속도

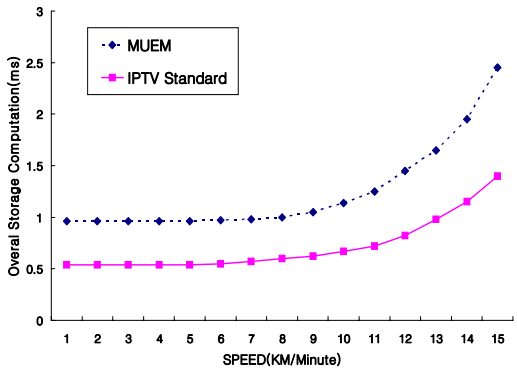

그림 9. 인증 서버의 전체 계산량

가 5km/m 이하로 떨어질 경우 인증 정보의 전체 계산량은 오차범위 0.1ms 이내에서 1ms로 일정하게 유지되었다. 이 같은 결과는 이동 사용자의 속도가 높을수록 네트워크의 통신 범위를 빠르게 벗어나면서 인증서버의 사용량이 증가되었기 때문이다. 제안 프로토콜은 기존 IPTV 표준 프로토콜보다 전체 인증 서버의 인증 정보 저장 계산량 측면에서 효율성이 평균 5~7.8% 높은 결과를 얻었다.

4.3 보안평가

제안 프로토콜에서 사용되는 스마트카드는 보안 공격을 예방하기 위해 UE와 AS사이에 임의의 공유키 K_S를 사용한다. 제안 프로토콜에서 생성된 임의의 공유키 K_S는 물리적으로나 논리적으로 안전하며 K_S를 생성하기 위해 UE가 USIM에게 요청한다. 제안 프로토콜은 UE와 AS사이에 임의의 공유키 K_S를 각 사용자가 서비스를 요청할 때마다 새로 생성된다.

공격자가 위조 서버의 설정을 통해 합법적인 사용자의 민감한 데이터를 수정하려고 하는 공격 방법이 서버 스푸핑 공격이다. 제안 프로토콜은 서버 스푸핑 공격을 예방하기 위해 MAC_{K_S}와 t_{AS}을 사용하고 있다. 제안 프로토콜에서 사용하는 MAC_{K_S}이 정확하지 못하면 자바카드나 AS는 인증과 권한 처리 과정을 포기하고 MAC_{K_S}이 합법적이면 공유키 K_S를 자바카드와 AS에서 생성하도록 한다. 제안 프로토콜에서 사용되는 K_S의 생명주기와 타임스탬프 t_{AS}의 사용으로 인하여 매 세션은 서로 다른 MAC_{K_S}을 생성하여 공격자가 자바카드로부터 K_S를 알지 못하도록 한다.

제안 프로토콜에서 메시지를 생성할 때 사용되는 시간 스탬프 t_{UE}, t_{AS}는 one-way 해쉬 함수에 적용시켜 암호화한다. 해쉬함수에 적용된 시간 스탬프 t_{UE}, t_{AS}는 UE와 AS만이 알고 있으며 제 3자는 알 수 없는 값들이다. 제안 프로토콜에서 매 통마다 생성되는 시간 스탬프는 공격자가 $(t_A^{'}-t_A^{''}) \geq \triangle t_A$만큼의 시간 간격안에 처리할 수 없도록 하여 reply 공격을 예방한다.

제안 프로토콜은 자바카드와 AS사이에 공유키를 이용하여 MAC을 검증하여 man-in-the -middle 공격을 예방하고 있다. 제안 프로토콜에서 자바카드와 AS사이에 전달되는 사용자 정보, 사용자 프로파일과 같은 민감한 데이터를 암호화하여 제 3자의 공격자들이 메시지를 수정할 수 없도록 하였다.

V. 결 론

이 논문에서는 IPTV 서비스를 지원하는 이동 장비와 콘텐츠를 제공하는 콘텐츠 서버간의 안전한 콘텐츠 서비스를 제공받기 위한 사용자 인증 메커니즘을 제안하였다. 제안된 메커니즘은 요금을 납부한 사용자의 서비스를 불법적으로 이용하는 사용자를 예방하기 위해 이동장비의 자바카드와 권한부여 서버 사이에 난수와 인증토큰을 사용하였으며 사용자의 이동장비 내에는 사용자 정보, 사용자 프로파일과 같은 민감한 데이터를 암호화한 후 메시지 무결성 검증을 위해 MAC을 사용하였다. 성능 평가 결과, 네트워크간 사용자가 1 홉으로 네트워크를 이동할 경우 제안 프로토콜의 인증서버는 IPTV 표준보다 평균 4.6%의 낮은 계산 로드량을 보이지만 4 홉이상으로 네트워크사이를 이동사용자가 이동할 경우 제안 프로토콜은 IPTV 표준보다 3.1%의 높은 계산 로드량이 나타났으며 인증 서버의 전체 인증 정보 저장 계산량은 제안 프로토콜이 기존 IPTV 표준보다 평균 5~7.8% 높은 결과를 얻을 수 있었다. 향후 연구에서는 이동 사용자의 권한 접근 및 레벨을 부여하여 사용자 프라이버시를 보장하는 메커니즘을 연구 수행할 계획이다.

참 고 문 헌

〔1〕 J. Lyu et al., “Design of Open APIs for Personaled IPTV Service”, Proceedings of 9th Internaltional Conference on Advanced Communication Technology, Vol. 1, Feb. 2007, pp. 305-310.

〔2〕 A. M. Eskicioglu, “Protecting Intellectual Property in Digital Multimedia Networks,” IEEE Computer, Vol. 36, pp. 39-45, 2003.

〔3〕 B. Rosenblatt, B. Trippe, and S. Mooney, “Digital Rights Management-Business and Technology”, M&T Books, 2002.

〔4〕 J. W. Lee, “Key distribution and management for conditional access system on DBS”, in Proc. Int. Conf. Cryptology and Information Security, 1996, pp. 82-86

〔5〕 F. K. Tu, C. S. Laih, and S. H. Toung, “On key distribution management for conditional access system on pay-TV system,” IEEE Trans. Consumer Electron., vol, 45, no. 1, pp. 151-158,

Feb, 1999.
〔6〕 Y. L. Huang and S. Shi도, "Efficient key distribution scheme for secure media delivery in pay-TV systems", IEEE Trans. Multimedia, vol. 6, no. 5, pp. 760-769, Oct. 2004.
〔7〕 A. Fiat and M. Naor, "Broadcast encryption", in Advances in Cryptology - CRYPTO'93, 1994, vol. 773, pp. 480-491.
〔8〕 D. Naor, M. Naor and J. B. Lotspiech, "Revocation and tracing schemes for stateless receivers", in Advances in Cryptology - CRYPTO'01, 2001, vol. 2139, LNCS, pp. 41-62.
〔9〕 D. Halevy and A. Shamir, "The LSD broadcast encryption scheme", in Proc. CRYPTO 2002, 2002, vol 2442, LNCS, pp. 47-60.
〔10〕 R. Canetti, J. Garey, G. Itkis, D. Micciancio, M. Naor, and B. Pinkas, "Multicast security: A taxonomy and some efficient constructions", in Proc. IEEE Infocomm'99, Mar. 1999, vol. 2, pp. 708-716.
〔11〕 D. Wallner, E. Harder, and R. Agee, "Key Management for Multicast: Issues and Architectures IETF", 1999, RFC 2627.
〔12〕 A. T. Sherman and D. A. McGrew, "Key establishment in large dynamic groups using one-way functions trees", IEEE Trans. Softw. Eng., vol. 29, no. 5, pp. 444-458, May 2003.
〔13〕 H. Harney and E. Harder, "Logical Key Hierarchy Protocol", IETF 1999[Online]. Availaber: Internet Draft, draft-harney-sparta -lkhp-\sec-00.txt
〔14〕 S. Emmanuel and M. S. Kankanhalli, "A Digital rights management scheme for broadcast video", multimedia Syst. J., vol. 8, no. 6, pp. 444-458, 2003.

정 윤 수 (Yoon-Su Jeong) 정회원

1998년 2월 청주대학교 전자계산학과 학사
2000년 2월 충북대학교 대학원 전자계산학과 석사
2008년 2월 충북대학교 대학원 전자계산학과 박사
2008년 3월~현재 충북대 및 한남대 시간강사
<관심분야> 유·무선 보안, 암호이론, 정보보호, Network Security, 이동통신보안

김 용 태 (Yong-Tae Kim) 정회원

1984년 2월 한남대학교 계산통계학과 학사.
1988년 2월 숭실대학교 전자계산학과 석사.
1995년 2월 충북대학교 전산학과 박사수료.
2002년 12월~2006년 2월 (주) 가림정보기술 이사
2006년 3월~현재 한남대학교 멀티미디어 학부 강의전담교수
<관심분야> 멀티미디어, 모바일 웹서비스, Real-time Multimedia Communication

박 길 철 (Gil-Cheol Park) 정회원

1983년 2월 한남대학교 전자계산학과 학사.
1986년 2월 숭실대학교 전자계산학과 석사.
1998년 2월 성균관대학교 전자계산학과 박사.
2006년 3월~2007년 2월 UTAS, Australia 교환교수
1998년 8일~현재 한남대학교 멀티미디어 학부 교수
2005년 2월~현재 한국정보기술학회 이사 멀티미디어 분과 위원장
<관심분야> multimedia and mobile communication, network security

이 상 호 (Sang-Ho Lee) 정회원

1976년 2월 숭실대학교 전자계산학과 학사.
1981년 2월 숭실대학교 전자계산학과 석사.
1989년 2월 숭실대학교 전자계산학과 박사.
1981년 3월~현재 충북대학교 전기전자 컴퓨터 공학부 교수
<관심분야> 네트워크보안, Protocol Engineering Network Management,