CAS 시스템 기반의 IPTV 환경에서 사용자 단말 이동성 지원을 위한 인증 프로토콜

정회원 노 효 선*, 준회원 정 서 현*, 정회원 이 정 현**, 종신회원 정 수 환*°

An Authentication Protocol Supporting User Device Mobility in CAS-Based IPTV Environments

Hyosun Roh* *Regular Member,* Seohyun Jung* *Associate Member*,
Jeonghyun Yi** *Regular Member,* Souhwan Jung*° *Lifelong Member*

요 약

IPTV 서비스는 인터넷 망을 통해 가입자가 원하는 양방향 멀티미디어 콘텐츠를 제공하는 통신 방송 융합 서비스이다. 그러나 현재 개발되고 있는 CAS 기반의 IPTV 서비스는 댁내에 존재하는 IPTV 서비스 가용 단말들로 방송 콘텐츠를 재분배하는 과정에서 셋탑박스와 IPTV 서비스 가용 단말간의 보안, 댁외로 이동하는 IPTV 서비스 가입자의 이동성 지원을 위한 보안을 제공하지 못한다. 본 논문에서는 댁내 셋탑박스에서 이동 단말로 안전하게 콘텐츠를 재분배하기 위한 인증 프로토콜과 댁외로 이동한 사용자 단말의 네트워크 접속 인증 및 서비스 접속인증을 위한 인증 프로토콜을 제안 한다. 제안 기법은 대리 서명 기법을 적용하여 기존 CAS 시스템을 통해 전달되는 콘텐츠를 재암호화 과정 없이 전달할 수 있다. 그리고 STB가 인증 서버를 대신하여 발급한 서명을 이용하여 댁외로 이동한 사용자 단말에 대한 네트워크 접속 인증과 IPTV 서비스 접속 인증을 동시에 수행할 수 있다. 또한 기존 보안 기술들과의 비교 분석을 통해 인증 프로토콜 적용에 따른 전체 통신 오버헤드 및 연산시간이 감소함을 보였다.

Key Words : IPTV, CAS, Authentication, Mobility, Set-Top-Box

ABSTRACT

Internet Protocol Television (IPTV) service is the convergence service of the telecommunication and broadcasting that provides various bidirectional multimedia contents by IPTV service subscribe's request through the high-speed internet. However, the proposed technologies current do not guarantee the security such as authentication between Set-Top-Box (STB) and the user mobile devices available IPTV service at home domain, and authentication of mobile user device at out of door. This paper proposes the authentication protocol for distributing content securely from STB to the users' mobile devices at home domain and authentication for network access and IPTV service access when the user's mobile device is moved out of the house. The proposed scheme using the proxy signature enables to distribute and protect securely the contents protected through an underlying Conditional Access System (CAS) without re-encrypting then that the existing scheme should employ. Then this protocol supports the authentication scheme to get service access authentication based on network access authentication using the signature, which the STB issued on behalf of the trust authority of IPTV service provider. Also the proposed authentication protocol reduces the total communication overhead and computation time comparing to the other authentication protocol.

※ 이 논문은 2009년도 정부(교육과학기술부)의 재원으로 한국과학재단의 지원을 받아 수행된 연구임 (No. 2009-0053879)
* 숭실대학교 정보통신전자공학부(peterhyo, iseohyun@cns.ssu.ac.kr, souhwanj@ssu.ac.kr), (° : 교신저자)
** 숭실대학교 컴퓨터학부(jhyi@ssu.ac.kr)
논문번호 : KICS2009-12-627, 접수일자 : 2009년 12월 18일, 최종논문접수일자 : 2010년 1월 29일

Ⅰ. 서 론

최근 초고속 인터넷 망의 빠른 확산은 IPTV (Internet Protocol TV) 서비스의 실현을 가속화 시키고 있다. IPTV는 초고속 인터넷 망을 통해 사용자가 요구하는 서비스 품질을 만족하는 다양한 양방향 멀티미디어 콘텐츠를 고속으로 제공할 수 있는 통신방송 융합 서비스로 고화질의 생방송, VoD (Video on Demand) 서비스, 그리고 다양한 멀티미디어 콘텐츠 등을 제공할 수 있다. 이러한 IPTV 서비스는 기존 PC와 TV가 가진 고유한 특성을 그대로 유지하고 있으며, 아직까지는 유선 인터넷 망을 통해 서비스를 제공하고 있지만 점차 무선 환경을 통해 사용자의 이동성을 지원할 수 있는 IPTV 서비스[1]로 발전하고 있다.

이러한 추세에 따라 ITU-T SG13에서는 FG IPTV (Focus Group IPTV)를 통해 IPTV를 위한 국제 표준화를 진행하고 있다. ITU-T는 FG IPTV를 통해 IPTV 서비스 요구사항 및 IPTV 구조에 대한 표준화[2]를 진행하고 있으며, FG IPTV WG3에서 IPTV를 위한 보안 기술에 대한 표준화[3]를 진행하고 있다. WG3에서 표준화 중인 보안 기술은 크게 서비스 보안 (Service Security) 분야와 콘텐츠 보호 (Content Security) 분야로 구분하여 위험 요소, 보안 요구사항, 보안 구조 및 보안 메커니즘 등을 정리하고 있고 있다[4][5][6].

현재 IPTV 서비스 환경에서 서비스 및 콘텐츠 보호를 위한 대표적인 보안 기술로는 기존 방송 시스템에서 사용되고 있는 서비스 접근 제한 시스템인 CAS (Conditional Access System)[7]와 인터넷에서 디지털 콘텐츠 저작권자 및 제작자의 권리를 보호하기 위해 개발된 DRM (Digital Right Management)[8]이 있다. 그러나 이러한 보안 기술의 경우 IPTV 서비스 환경에 적용하기에는 한계가 존재한다. CAS 시스템은 댁내에 존재하는 다양한 IPTV 서비스 가용 단말로 재분배되는 방송 콘텐츠에 대한 보안을 제공할 수 없으며, CAS 시스템 간의 연동이 제공되지 않기 때문에 콘텐츠 제공업자들이 CAS 기술에 종속되는 문제 등이 있다. 또한 DRM의 경우 아직까지 표준 규격이 정해지지 않고 있으며, DRM 제품 간 상호호환성이 제공되지 않는다는 문제점이 있다. 그리고 소프트웨어 방식의 단일 암호화 적용으로 인한 보안 취약성이 존재한다. 최근 이러한 CAS와 DRM 기술 적용에 따른 문제점을 해결하기 위한 다양한 연구가 진행되고 있다. IPTV 서비스 환경에서 DRM 기술로 CAS 시스템을 대체하여 적용하기 위한 방법, CAS로 기존 DRM을 대체하여 적용하기 위한 방법, 그리고 CAS 기반의 DRM 기술을 적용하는 방법 등[9]이 제안되고 있지만 아직까지는 완전하지 않다. 또한, 최근 IPTV 서비스 가입자의 이동성 지원이 가능한 IPTV 서비스에 대한 필요성은 강하게 대두되고 있지만, 이동하는 IPTV 서비스 사용자를 인증하고, 지속적으로 IPTV 서비스를 안전하게 제공하기 위한 보안 시스템에 대한 적당한 기술을 제안하지 못하고 있다.

앞서 설명한 문제들을 해결하기 위해 본 논문에서는 댁내에 존재하는 다양한 IPTV 서비스 가용 단말을 이용하여 사용자가 IPTV 서비스를 안전하게 제공받을 수 있도록 지원하기 위한 댁내 IPTV 서비스 가용 단말 등록 및 인증 프로토콜을 제안한다. 또한, 사용자가 댁내에서 사용하던 IPTV 서비스 가용 단말을 통해 댁외에서도 지속적인 IPTV 서비스를 제공받을 수 있도록 지원하기 위한 이동성 지원을 위한 인증 프로토콜을 제안한다. 제안하는 인증 프로토콜은 대리 서명 기술을 적용하여 IPTV 서비스 제공업자의 인증 서버 대신 댁내에 설치된 STB (Set Top Box)가 댁내에 존재하는 IPTV 서비스 가용 단말을 위한 서명을 생성 및 발급할 수 있도록 하였다. 서명을 발급받은 댁내의 IPTV 서비스 가용 단말은 STB가 발급한 서명을 인증서처럼 사용하여 댁내 및 댁외에서 IPTV 서비스 접근을 위한 사용자 또는 단말 인증을 할 수 있도록 제안되었다.

본 논문의 구성은 다음과 같다. 2장에서는 관련 연구 설명을 통해 IPTV 서비스 환경, IPTV 서비스 환경의 보안 문제점 및 보안 요구사항, 그리고 기존 IPTV 서비스 환경의 보안 기술을 간략하게 요약 설명한다. 3장에서는 본 논문에서 제안하는 인증 프로토콜을 각 단계별로 자세하게 설명한 후, 4장에서 안정성 및 성능을 비교 분석한다. 마지막으로 5장에서 결론을 맺는다.

Ⅱ. 관련연구

이번 장에서는 본 논문에서 제안하는 인증 프로토콜이 적용되는 IPTV 서비스 환경에 대한 간략한 설명과 IPTV 서비스 환경에 존재하는 보안 문제점 및 보안 요구사항을 설명한다. 그리고 IPTV 서비스 환경에서 서비스 보안과 콘텐츠 보안을 위해 적용 가능한 CAS와 DRM 기술을 설명한다.

2.1 IPTV 서비스 환경

IPTV 시스템은 인터넷을 통해 대량의 멀티미디어 콘텐츠를 사용자의 요구수준에 맞게 양방향으로 제공할 수 있다. 그림 1은 이러한 IPTV 서비스 환경의 구조도를 보여준다. 그림 1에서처럼 IPTV 서비스 환경은 크게 콘텐츠 제공업자, 서비스 제공업자, 네트워크 제공업자 그리고, IPTV 서비스 가입자 등으로 구분된다. 콘텐츠 제공업자는 다양한 멀티미디어 콘텐츠에 대한 소유권을 가지고 있으며, IPTV 서비스 사업자 또는 개인 사용자에게 서비스되는 멀티미디어 콘텐츠를 IPTV 서비스 제공업자에게 제공한다. IPTV 서비스 제공업자는 콘텐츠 제공업자가 제공한 멀티미디어 콘텐츠를 서비스 가입자에게 전달하기 위한 서비스 관리 기능, 콘텐츠 전달 기능 그리고 다양한 IPTV 어플리케이션 등을 제공한다. 특히 서비스 제공업자는 가입자 인증/과금 등을 관리하며 전달되는 멀티미디어 콘텐츠를 보호하기 위한 보안을 제공한다. 네트워크 제공업자는 IPTV 서비스 제공업자가 요구하는 네트워크를 구성 및 유지한다. 서비스 제공업자와 네트워크 제공업자는 동일한 사업자일 수 있다. 그리고 마지막으로 IPTV 서비스 가입자는 서비스를 제공받는 사용자로서 IPTV 서비스 가입시 댁내에 설치된 STB를 통해 다양한 멀티미디어 콘텐츠를 인터넷 망을 통해 제공받는다.

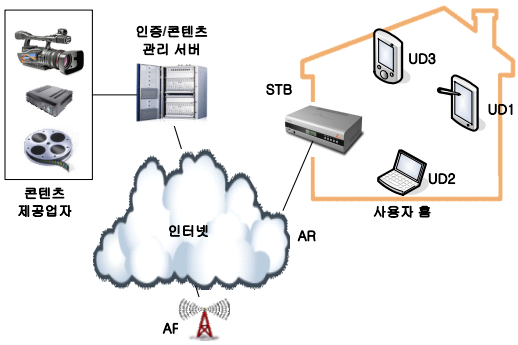

그림 1. IPTV 서비스 환경

2.2 IPTV 서비스 환경의 보안 문제점 및 요구사항

IPTV 서비스는 공개된 인터넷 망에서 IP를 통해 멀티미디어 콘텐츠가 IPTV 서비스 가입자에게 전달되기 때문에 발생하는 보안 문제들과 IPTV에 적용이 고려되고 있는 CAS와 DRM의 제한성에서 발생하는 문제점이 존재한다. 다음은 이러한 보안 문제점에 대해서 정리하였다[2].

IPTV 서비스의 불법 시청: IPTV 서비스의 멀티미디어 콘텐츠는 인터넷을 통해 서비스 가입자에게 전달된다. 때문에 멀티미디어 콘텐츠가 전송되는 중간에서 제 3자에 의한 네트워크 세션 가로채기(TCP-Hijackin) 공격이 가능하다. 또한 IPTV 서비스 네트워크 환경의 취약성 분석을 통해 전송되는 멀티미디어 콘텐츠를 불법적으로 다운로드 하거나 사용자 인증 과정 등을 우회 접근하여 유료 IPTV 서비스 방송 등을 시청할 수 있다.

IPTV 서비스 콘텐츠의 불법 복제 및 유출: IPTV 서비스 제공업자가 멀티미디어 콘텐츠를 암호화하여 전송하면 서비스 가입자의 댁내에 설치된 STB에서 복호화 되어 IPTV 단말로 전송되거나 다시 재 암호화되어 전송된다. 이때 복호화 된 멀티미디어 콘텐츠를 쉽게 복제하여 유출할 수 있다.

새로운 수신 제한 시스템 적용의 어려움: IPTV 서비스 환경에 적용된 수신 제한 시스템이 오류 또는 해킹으로 정상적인 동작이 어렵게 될 경우 현재의 IPTV 서비스 환경에서는 새로운 수신 제한 시스템으로 변경하는 것이 매우 어렵다. 만약 새로운 수신 제한 시스템을 적용할 경우 기존 수신 제한 시스템이 설치된 STB 등과 같은 장비들도 함께 교체해야 하는 문제가 있다.

수신 제한 시스템 간의 호환성 부재: 현재의 IPTV 서비스 단말은 IPTV 서비스 사업자가 제공하고 있으며, 제공된 단말에 설치되는 수신 제한 시스템은 단말을 제공하는 IPTV 서비스 사업자들 마다 서로 다른 수신 제한 시스템을 적용하고 있다. 때문에 동일한 IPTV 방송이라도 서비스 제공업자가 다를 경우 방송 시청이 불가능한 문제가 있다.

2.3 IPTV 서비스 환경을 위한 보안 기술

앞서 살펴본 것과 같이 IPTV 서비스 환경에는 다양한 보안 문제점이 존재한다. 이러한 보안 문제들을 해결하여 안전하게 IPTV 콘텐츠를 서비스 가입자에게 전달하기 위한 보안 기술들이 연구되고 있다. 그중 서비스 보안을 위한 대표적인 보안 기술인 CAS (Conditional Access System)와 콘텐츠 보안을 위한 DRM (Digital Right Management) 기술을 이용하기 위한 연구가 진행되고 있다.

CAS는 방송 수신 제한 시스템으로 케이블 TV, 위성 DMB (Digital Multimedia Broadcasting) 등에서 사용되고 있다. IPTV 서비스 환경에서는 CAS를 이용하여 서비스 사업자의 헤드엔드와 서비스 가입자의 STB 간에 전달되는 방송 콘텐츠를 암호화하

여 전달하는데 사용된다. 먼저 CAS는 제어 단어 (Control Word: CW)를 생성하여 전달할 방송 콘텐츠를 스크램블하여 전송한다. 이때 사용된 CW는 서비스 가입자의 STB에서 디스크램블하여 사용자가 방송 콘텐츠를 제공받을 수 있도록 하기 위해 사용되고, CAS 시스템에서 ECM (Entitlement Control Message)을 통해 서비스 키 SK (Service Key)로 암호화하여 STB으로 전송한다. SK는 CAS 시스템에서 DK (Distribution Key)로 암호화한 후 EMM (Entitlement Management Message)을 통해 STB로 전송된다. EMM과 ECM을 수신한 STB는 스크램블되어 전송된 방송 콘텐츠를 디스크램블하여 사용자에게 IPTV 서비스를 제공한다.

DRM은 인터넷 환경에서 디지털 콘텐츠 제작자의 승인 없이 콘텐츠가 불법적으로 복제 및 사용되는 것을 막기 위해 개발된 콘텐츠 보안 기술이다. 우선 콘텐츠 제공업자는 자신의 콘텐츠에 대해 패키징 (Packaging) 과정을 수행하여 DRM 서버에 콘텐츠 정보를 등록하고, 콘텐츠를 암호화하여 콘텐츠 패키지를 생성한다. 이렇게 생성된 콘텐츠 패키지는 콘텐츠 서버에 등록되고, 사용자가 콘텐츠를 구입하면 구입자 컴퓨터로 콘텐츠 패키지가 다운로드 된다. 구입자는 콘텐츠 패키지를 다운로드 한 다음 DRM 서버로부터 라이센스를 발급받는다. 발급 받은 라이센스에는 DRM으로 암호화된 콘텐츠를 복호화하는데 필요한 복호화 키와 사용 권한이 포함되어 있다. 이러한 과정은 DRM 콘트롤러에 의해 수행되고, 제 3자가 불법적으로 구매자의 콘텐츠 패키지를 복사하더라도 사용할 수 없도록 콘텐츠 보안을 지원한다.

Ⅲ. 제안 기법

이번 장에서는 앞서 그림 1을 통해 설명한 IPTV 서비스 환경에서 댁내에 존재하는 이동 가능한 IPTV 서비스 가용 단말들로 안전하게 IPTV 서비스 콘텐츠를 재분배하고, 단말의 댁외 이동성 지원을 위해 본 논문에서 제안하는 인증 프로토콜의 세부동작 과정을 단계별로 설명한다.

3.1 시스템 구성

본 논문에서 제안하고 있는 인증 프로토콜은 다음과 같이 댁내와 댁외에서의 인증 단계로 구분된다.

댁내 인증 단계 : 댁내에 존재하는 IPTV 서비스 가용 단말에게 STB에서 수신한 방송 콘텐츠를 안전하게 재분배하기 위한 등록 및 인증 단계.

댁외 인증 단계 : 댁내 STB에 등록 및 인증을 수행한 IPTV 서비스 가용단말이 댁외로 이동시 지속적으로 IPTV 서비스를 제공받을 수 있도록 지원하기 위한 인증 단계.

제안하는 인증 프로토콜은 위와 같이 댁내와 댁외에서 IPTV 서비스 가용단말을 안전하게 인증하기 위해 Schnorr 서명[10]을 이용한 대리 서명 기법[11]을 적용하였다. 대리 서명 방식은 원 서명자가 자신의 서명 권한을 선택한 대리 서명자에게 위임한 다음, 대리 서명자가 원 서명자를 대신하여 원 서명자가 생성하는 것과 같은 서명을 생성 및 발급할 수 있도록 지원하는 서명 기술이다. 이를 위해 제안 기법에서는 다음과 같이 시스템을 구성하였다.

원 서명자 : 서비스 제공업자의 신뢰할 수 있는 인증 서버 TA (Trust Authority)로 정의.

대리 서명자 : TA를 대신하여 서명을 생성하는 노드로 IPTV 서비스 가입자의 댁내에 설치된 STB로 정의.

사용자 단말 (User Device: UD) : 이동성이 지원되는 IPTV 서비스 가용 단말로 스마트 폰, 노트북, PDA 등을 의미하고, WLAN 또는 WiBro/WiMAX를 사용할 수 있는 단말로 정의.

서비스 보호를 위한 보안 기술 : CAS를 통해 서비스 제공업자의 헤드엔드와 STB 간에 전달되는 방송 콘텐츠가 보호됨을 가정.

초기 인증 : 서비스 가입자의 댁내에 설치된 STB를 서비스 제공업자가 인증하기 위한 과정으로 IPTV 서비스 가입시 제공되는 스마트 카드 또는 서비스 제공업자가 제공하는 보안 기술을 통해 안전한 방법으로 수행됨을 가정.

무선 네트워크 환경 : STB에 등록된 UD가 댁외에서 접속 가능한 무선 네트워크 환경은 WLAN과 WiBro/WiMAX 환경을 가정.

다음은 제안하는 보안 프로토콜에서 TA가 STB에게 자신의 서명 권한을 위임하고, STB가 댁내에 존재하는 IPTV 서비스 가용단말을 위해 안전하게 서명의 생성 및 분배를 위해 적용된 Schnorr 서명의 동작과정을 설명한다.

서명생성 : 서명자는 큰 소수 p, q를 선택한 후

$g \in Z_p^*$를 구한다. 그리고 다시 k를 $1 \le k \le q-1$에서 임의로 선택한 다음 $r = g^k \bmod p$를 계산하고, 서명자의 개인 키 x를 이용하여 공개 키를 $y = g^x \bmod p$와 같이 생성한 다음 공개한다. 이후 서명한 메시지 m과 r을 해쉬한 $e = h(m \| r)$를 계산한 다음 전송할 서명 $s = xe + k \bmod q$을 생성한다. 서명이 생성된 다음 s, e를 검증자에게 전송한다.

서명 검증: 검증자는 s, e를 수신한 다음 서명을 검증한다. 검증자는 사전에 서명자가 공개한 p, q, g, y 등을 이용하여 $r_v = g^s y^{-e} \bmod p$와 $e' = h(m \| r_v)$을 계산한 다음 $e' = e$ 을 비교함으로써 서명을 검증 한다.

3.2 용어 정리

다음 표 1에서 제안하는 인증 프로토콜에서 사용되는 주요 용어를 정리하였다.

표 1. 용어 정리

용어	정의
TA	서비스 제공업자의 인증 및 등록 서버
STB	Set Top Box
UD_i	댁내 IPTV 서비스 가용 단말
x_x	x의 개인 키
y_x	x의 공개 키
X_x	x의 Diffie-Hellman 비밀 값
Y_x	x의 Diffie-Hellman 공개 값
TK_x	x의 임시 세션 키
TSK_{xy}	무선 구간에서 x와 y간에 공유하는 세션 키
CW	CAS에서 방송 콘텐츠를 스크램블 할 때 사용하는 제어 단어
SK	CAS에서 제어 단어를 암호화하여 전달하기 위해 사용하는 서비스 키
s_x	x를 위해 생성된 서명
PS_x	STB가 x를 위해 TA를 대신하여 생성하는 서명
V_x	x가 자신의 개인키를 이용하여 생성한 검증 값
MSK	IPTV 서비스 가입시 서비스 제공업자가 스마트카드로 분배하는 마스터 비밀 키
ID_x	x의 식별자
$h(\cdot)$	128 bit 일방향 해쉬 함수
t_x	타임 스템프

3.3 IPTV 서비스 환경을 위한 인증 프로토콜

이 절에서는 제안하는 인증 프로토콜의 동작을 댁내와 댁외로 구분하여 설명한다. 먼저, IPTV 서비스 가입자는 온/오프라인으로 IPTV 서비스 제공업자에게 가입 신청을 한 후 댁내에 STB가 설치되었음을 가정하고, 가입자는 IPTV 서비스 제공업자가 제공하는 스마트카드를 통해 초기 마스터 비밀 키 MSK를 안전하게 분배 받았음을 가정한다. 그리고 CAS 기반의 IPTV 서비스 환경을 가정하고, TA와 STB, UD에 Schnorr 서명을 위한 초기 설정을 가정한다.

3.3.1 댁내 인증 프로토콜

다음의 그림 2는 댁내에 존재하는 IPTV 서비스 가용단말인 UD를 STB에 등록하고, 등록된 UD가 IPTV 서비스를 제공받고자 할 때 STB가 UD를 인증하는 과정을 보여준다.

1단계: 사용자의 IPTV 서비스 가입단계로 온/오프라인을 통해 이루어진다. IPTV 서비스 제공업자와 가입자 간에 스마트카드 또는 다른 안전한 방법으로 MSK가 공유되고, 서비스 가입자에 대한 IPTV 서비스 프로파일 등이 공유된다.

2단계: 가입자의 댁내에 STB가 설치된 후 최초 서비스 사용을 위해 TA와 초기 인증을 요청한다. 요청 메시지에는 ID_{STB}, STB의 Diffie-Hellman 공개 값[12]인 Y_{STB}와 메시지를 전송한 시간 정보가 MSK로 암호화되어 MAC_{MSK}와 함께 전달된다.

3단계: TA가 STB에 대한 검증 및 인증을 성공하면 TA는 STB에게 가입자의 댁내에 존재하는 UD_i에게 자신을 대신하여 서명을 생성 및 분배할 수 있는 권한을 위임한다. 권한 위임을 위해 다음 식과 같이 서명을 생성한다.

- 임의의 소수 p와 q를 선택
- $g \in Z_p^*$
- 임의의 K를 $1 \le K \le q-1$에서 선택
- $r = g^K \bmod p$로 정의
- $y_{TA} = g^{x_{TA}} \bmod p$로 정의
- $H = h(ID_{STB} \| Y_{STB} \| r \| t_{TA})$
- $s_{STB} = x_{TA} H + K \bmod q$
- $V_{TA} = x_{TA} H$

4단계: TA는 STB에게 s_{STB}, V_{TA}, H, t_{TA}를 MAS로 암호화하여 전달한다.

5단계: STB가 서명을 수신하면 다음의 식과 같

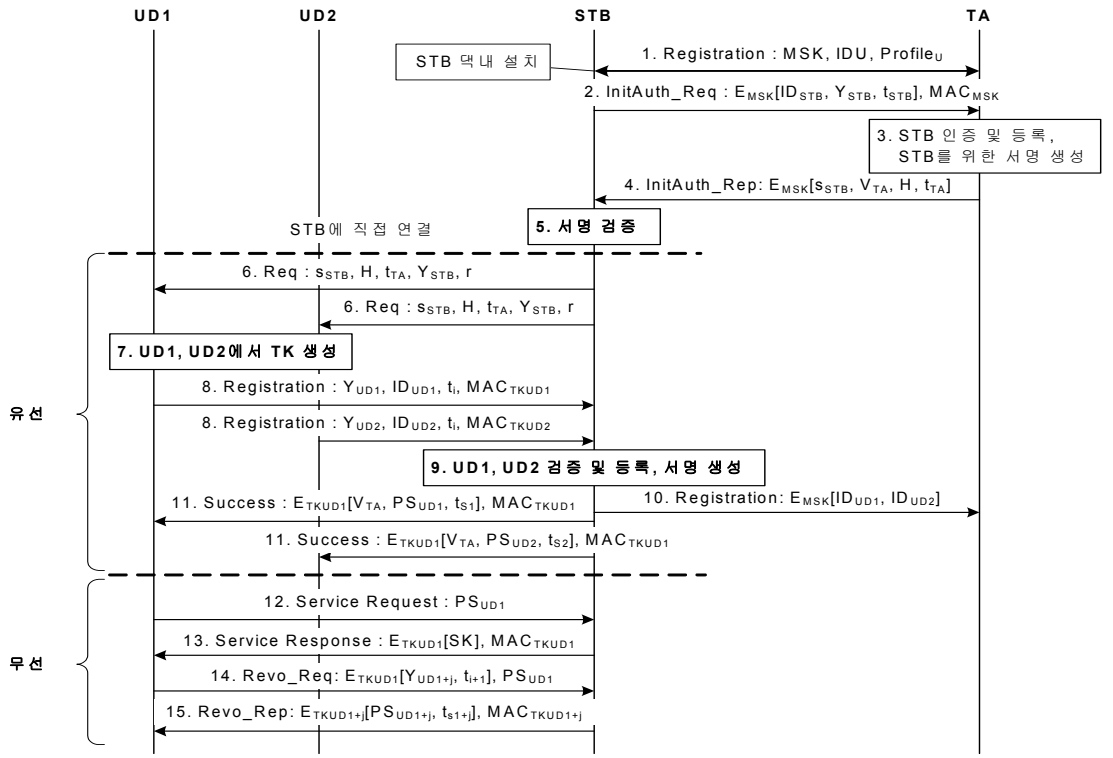

그림 2. 댁내 인증 프로토콜

이 서명을 검증하고, 대리 서명을 생성할 때 사용할 개인 키 px_{STB}와 공개 키 py_{STB}를 생성한다.

- $r' = g^{s_{STB}} y_{TA}^{-H} \bmod p$
- $H' = h(ID_{STB} \| Y_{STB} \| r' \| t_{TA})$
- $H' = H$
- $px_{STB} = s_{STB} + X_{STB} Y_{STB}$
- $py_{STB} = g^{px_{STB}} \bmod p$

6단계: 댁내에서 IPTV 서비스 가입자는 IPTV 서비스 제공업자가 허용한 UD 사용 허가 숫자만큼의 UD를 STB에 안전한 방법으로 등록한다. 이때 UD는 STB에 USB 등의 유선 케이블을 통해 연결되고, 이러한 연결은 최초 STB에 UD를 등록할 때 한번만 수행된다. 유선으로 UD가 STB에 연결이 되면 STB는 TA로부터 수신한 서명 s_{STB}과 자신의 Diffie-Hellman 공개 값 Y_{STB}를 UD_i에게 전달한다. 그림 2에서는 UD1과 UD2가 등록하는 과정을 보여준다.

7단계: UD_i는 수신한 s_{STB} 서명을 검증하여 STB를 인증하고, Y_{STB}를 이용하여 STB와 공유하게 되는 세션키 TK_{UDi}를 Diffie-Hellman 키 생성 방법으로 생성한다. 서명 검증은 5 단계와 같다.

8단계: UD_i는 STB에게 등록 요청 메시지를 전달한다. 등록 요청 메시지에는 UD_i의 식별정보 ID_{UDi}, 메시지 생성 시간 t_i, Diffie- Hellman 공개 값 Y_{UDi}과 MAC_{TKUDi} 값이 전달된다.

9단계: STB는 등록 요청 메시지를 수신하면 포함된 정보를 통해 UD_i를 검증하고 등록한다. 등록이 성공하면 STB는 TA를 대신하여 등록한 UD_i에게 발급할 서명을 다음 식과 같이 생성한다. $SP_{MSK-UD1}$은 보안 값으로 UD_i가 댁외로 이동할 경우 TA에서 UD_i를 검증할 때 사용한다.

- $H_{UDi} = h(ID_{UDi} \| Y_{UDi} \| Y_{STB} \| t_{Si})$
- $SP_{MSK-UD1} = h(MSK \| ID_{STB} \| ID_{UD1})$
- $PS_{UDi} = px_{STB}(H_{UDi}, SP_{MSK-UD1})$

10단계: STB는 자신에게 등록한 UD_i의 식별 정보를 TA에게 전달하여 TA에 UD_i를 등록한다.

11단계: STB는 등록 성공 메시지에 생성한 서명 PS_{UDi}, TA가 전달한 검증 값 V_{TA}와 MAC_{TKUDi} 값을 포함하여 UD_i에게 전달한다. 이때 UD_i에게 전달되는 V_{TA} 검증 값은 UD_i가 댁외로 이동하여 네트워크 접속 지점과의 상호 인증 시 STB가 발행한 서명을 검증하는데 사용된다.

12단계: STB에 초기 등록 과정을 성공적으로 끝낸 UD_i는 댁내에서 사용자가 원할 때 언제든지 등록된 UD_i를 통해 IPTV 서비스를 제공받을 수 있다. 사용자가 IPTV 서비스를 요청하면 UD_i는 STB가 발행한 서명 PS_{UDi}를 STB에게 전달한다.

13단계: STB는 수신한 서명을 검증한 다음 CAS 시스템으로 보호되어 전달되는 방송 콘텐츠를 디스크램블하기 위해 필요한 SK를 TK_{UDi}로 암호화하여 계산한 MAC_{TKUDi} 값과 함께 UD_i로 전달한다. SK를 수신한 UD_i는 SK를 이용하여 스크램블되어 전달되는 방송콘텐츠를 디스크램블하여 사용자가 IPTV를 시청하도록 지원한다.

14단계: 14단계와 15단계는 STB에서 발행한 서명을 갱신하는 과정으로써 일정한 주기 또는 사용자나 STB이 원할 때 수행된다. 사용자가 서명의 재발급을 요청할 경우 UD_i는 STB에게 새롭게 선택한 Diffie-Hellman 공개 값 Y_{UDi+j}과 선택한 시간 정보를 TK_{UDi}로 암호화하여 이전에 발급받은 서명과 함께 STB로 전달한다.

15단계: STB이 UD_i에 대한 검증 및 인증을 성공하면, UD_i가 암호화하여 전송한 값을 이용하여 9단계에서와 같이 새로운 서명을 생성한 다. 그리고 UD_i에게 Y_{UDi+j}를 이용하여 새롭게 생성한 TK_{UDi+j}로 암호화하여 $MAC_{TKUDi+j}$ 값과 함께 전달함으로써 서명의 재발급 과정을 마무리한다.

3.1.2 이동성 지원을 위한 IPTV 서비스 가용 단말 인증 과정

위의 그림 3은 IPTV 서비스 가입자가 댁내에서 STB에 등록 후 사용하던 IPTV 서비스 가용 단말을 가지고 댁외로 이동하여 지속적인 IPTV 서비스를 사용할 경우 IPTV 서비스 제공을 위한 인증 과정을 보여주고 있다. 그림에서처럼 제안하는 보안 프로토콜은 댁외로 이동한 서비스 가입자가 가용한 주변 네트워크 접속 지점에게 인증 요청 메시지를 보내는 것으로 인증과정이 시작된다. 다음은 각 과정별 세부 동작을 설명한다.

1단계: 댁내에 있던 사용자가 UD_i를 가지고 외부

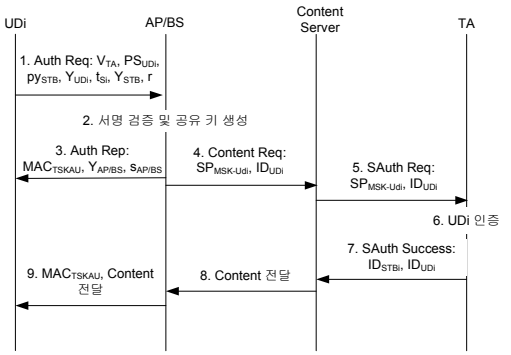

그림 3. 댁외 인증 프로토콜

로 이동하여 UD_i에서 가용한 무선 접속 망을 통해 IPTV 서비스를 제공받고자 할 경우 UD_i는 검색된 무선 접속 지점인 AP 또는 BS로 STB가 발행한 서명 PS_{UDi}와 py_{STB}, Y_{UDi}, t_{si}, V_{TA}, Y_{STB}, r 등의 정보를 인증 요청 메시지에 포함하여 전달한다.

2단계: 인증 요청 메시지를 수신한 AP/BS (Access Point / Base Station)는 TA의 공개 키 y_{TA}로 검증 값 V_{TA}를 확인 한 다음 py_{STB}를 검증함으로써 TA가 서명 권한을 위임한 STB_i가 정상적으로 생성 및 발행한 서명임을 다음의 식처럼 검증하고, 서명 검증을 통해 UD_i를 인증한다. UD_i에 대한 검증 및 인증이 성공하면 UD_i의 Y_{UDi} 값을 이용하여 임시 공유 세션키를 생성한다.

$$- \; y_{TA}^{H} = g^{V_{TA}} = g^{x_{TA}H'} = y_{TA}^{H'}$$

$$- \; py_{STB} = g^{s_{STB} + X_{STB}Y_{STB}} = g^{x_{TA}H + K} Y_{STB}^{Y_{STB}}$$
$$= y_{TA}^{H} r \; Y_{STB}^{Y_{STB}}$$

3단계: AP/BS는 UD_i에게 TA가 발급한 서명 $s_{AP/BS}$와 자신의 Diffie-Hellman 공개 값 $Y_{AP/BS}$, 그리고 TSK_{AU}를 이용하여 계산한 MAC_{TSKAU}을 응답 메시에 포함하여 UD_i에게 전달함으로써 UD_i와 AP/BS 간의 상호 인증을 수행 한다.

4단계: UD_i에 대한 검증 및 인증이 성공하면 AP/BS는 콘텐츠 서버에게 UD_i에게 전달할 IPTV 서비스 콘텐츠를 요청한다. 이때 UD_i의 서명에 포함되어 있던 $SP_{MSK-UDi}$와 ID_{UDi}를 콘텐츠 서버로 전달한다.

5단계: 콘텐츠 서버는 콘텐츠 요청 메시지에 포함된 정보를 TA에게 전달하여 콘텐츠를 요청한 UD_i에 대한 서비스 인증을 요청한다.

6단계: TA는 STB_i와 공유하는 MSK를 이용하여 SP_{MSK-UD_i}를 검증함으로써 UD_i가 STB_i를 통해 등록된 사용자임을 확인한다.

7단계: TA에서 UD_i에 대한 서비스 인증이 성공하면 TA는 서비스 인증 성공 메시지에 ID_{STBi}와 ID_{UDi} 정보를 포함하여 콘텐츠 서버로 전달한다.

8단계: 콘텐츠 서버는 AP/BS로 CAS 시스템으로 암호화된 방송 콘텐츠를 전달한다.

9단계: AP/BS는 콘텐츠 서버가 전달한 방송 콘텐츠와 UD_i와 공유하게 되는 TSK_{AU}로 생성한 MAC_{TSKAU} 값을 포함하여 UD_i에게 전달한다.

위에서와 같은 과정을 통해 댁외로 이동한 IPTV 서비스 가입자는 댁내 STB_i가 TA를 대신하여 발행한 서명으로 네트워크 접속 인증 및 IPTV 서비스 인증을 받은 후 필요한 IPTV 서비스를 지속적으로 제공 받을 수 있다.

Ⅳ. 안전성 분석 및 성능 비교

이 장에서는 본 논문에서 제안하는 인증 프로토콜에 대한 안전성 분석 및 성능을 비교 하였다.

4.1 안전성 평가

제안하는 인증 프로토콜의 안전성은 TA가 STB에게 생성하여 분배하는 서명, STB가 TA 대신 생성하여 UD에게 분배하는 서명의 강도에 있다. 제안 기법이 적용된 환경에서 공격자는 자신이 TA 또는 정상적인 STB, UD로 가장하여 정상적인 서명을 발급받아 불법적으로 IPTV 서비스를 제공받기 위한 공격을 시도할 수 있다. 그리고 TA가 STB에게 생성하여 발급하는 서명, STB가 UD를 위해 생성 및 발급하는 서명을 수정 또는 위조 공격을 통해 IPTV 서비스를 불법적으로 사용하기 위한 시도를 할 수 있다. 또한 UD가 댁외 이동한 경우 정상적인 UD로 가장하여 IPTV 서비스를 제공받으려는 공격을 시도할 수 있다. 다음은 이러한 공격에 대해 각 구간별로 제안 기법의 안전성을 설명한다.

TA와 STB 간의 안전성

제안하는 인증 프로토콜은 TA와 STB 둘 간에 주고받는 메시지를 MSK로 암호화하여 전달한다. 때문에 MSK를 알지 못하는 공격자는 중간자 공격을 통해 메시지를 위조하거나 도청하는 것이 불가능하다. 또한 공격자는 TA가 STB를 위해 생성하는 서명을 위조 또는 수정하는 것이 매우 어렵다. 우선 TA가 생성하는 서명은 TA만 알고 있는 개인 키 x_{TA}를 이용하여 생성된다. 또한 서명에는 TA가 임의로 선택한 K와 이를 이용하여 생성한 r 값이 해쉬되어 서명에 포함된다. 때문에 TA의 개인 키 정보를 알지 못하는 공격자는 중간에서 TA가 생성하는 서명을 위조하거나 수정할 수 없다. 또한 공격자가 정상적인 STB로 가장하여 TA의 서명 권한을 위임 받기 위한 공격에 대해서도 안전하다. 공격자가 정상적인 STB로 가장하기 위해서는 둘 간에 공유하는 MSK를 알아야 하지만, 이 MSK는 스마트 카드 등과 같은 안전한 방법으로 분배되기 때문에 공격자가 알아내는 것이 매우 어렵다. 또한 둘 간에 전달되는 IPTV 서비스 콘텐츠는 CAS 시스템으로 보호되어 전달되기 때문에 중간에서 IPTV 서비스를 불법적으로 사용하는 것은 불가능하다.

STB와 UD 간의 안전성

공격자가 가입자의 댁내 무선 환경을 통해 재분배되는 IPTV 서비스를 불법적으로 사용하기 위해서는 STB에 정상적인 UD로 가장하여 등록하거나, 정상적인 UD의 서명을 위조 또는 변경 하여 STB가 UD에게 전달하는 SK 또는 CW의 값을 알아야 한다. 그러나 공격자가 이것은 알아내기는 매우 어렵다. 제안 인증 프로토콜에서 사용자가 원하는 UD를 STB에 등록하는 과정은 USB와 같은 유선을 통해 이루어진다. 이 과정은 최초 등록 시 일회만 요구되고, 등록하는 사용자가 직접 STB가 연결된 UD를 통해 이루어지기 때문에 공격자가 정상적인 UD로 가장하여 STB에 등록하기는 불가능하다. 또한 공격자는 STB가 UD에게 TK_{UDi}로 암호화하여 전달하는 CAS 시스템의 SK를 알아내는 것이 불가능하다. SK를 알아내기 위해서 공격자는 우선 STB와 UD 간에 공유하는 TK_{UDi}를 생성할 수 있어야 한다. 공격자가 원하는 TK_{UDi}를 생성하기 위해서는 STB와 UD 간에 중간자 공격을 성공하거나, STB가 UD에게 생성하여 분배한 서명을 위조 또는 변경해야 한다. 그러나 공격자는 STB의 px_{STB}를 생성할 수 없기 때문에 서명을 위조 또는 변경 할 수 없다. 따라서 공격자는 TK_{UDi}를 위조 또는 변경하기 위한 중간자 공격을 할 수 없고, SK를 알아 낼 수 없기 때문에 댁내에서 재분배되는 IPTV 서비스를 불법적으로 사용하는 것은 불가능하다.

UD와 네트워크 접속 지점 간의 안전성

제안하는 인증 프로토콜은 댁외로 이동하는 사용자에게 네트워크 접속 인증과 서비스 접속 인증을 안전하게 제공하기 위해 STB가 TA를 대신하여 UD에게 발행한 서명을 사용한다. 따라서 공격자가 댁외에서 불법적으로 IPTV 서비스를 사용하려면 UD의 서명을 위조 하거나, 서비스 인증을 위해 콘텐츠 서버가 TA에게 전달하는 보안 값 $SP_{MSK-UDi}$를 위조 또는 변경하여 네트워크 인증 및 서비스 인증에 성공해야 한다. 그러나 공격자는 앞서 설명한 것처럼 UD의 서명을 위조하거나 변경하는 것이 불가능하다. 그리고 서비스 인증을 위해 사용되는 보안 값 $SP_{MSK-UDi}$ 또한 STB와 TA 간에 공유하는 MSK를 통해 생성되기 때문에 공격자가 임의로 위조하거나 변경할 수 없다. 만약 공격자가 무선 네트워크 환경의 보안 취약성을 이용하여 네트워크 접속에 성공하였다 하더라도 $SP_{MSK-UDi}$를 생성할 수 없기 때문에 정상적인 IPTV 서비스에 불법적으로 접근할 수 없다.

위에서 설명한 것처럼 제안하는 인증 프로토콜은 IPTV 서비스 환경에서 불법적인 IPTV 서비스 사용을 위한 공격자의 여러 가지 공격을 예방할 수 있다.

4.2 성능 비교 분석

다음은 본 논문에서 제안하는 보안 프로토콜과 기존에 제안된 IPTV 환경에서의 사용자 인증 기술[13]에 대한 성능을 비교한다. 성능 비교를 위해 본 논문에서 제안하는 인증 프로토콜과 기존 인증 프로토콜은 이미 사용자의 이동 단말이 등록되었음을 가정하였고, 등록된 이동 단말이 댁외로 이동하여 IPTV 서비스를 요청할 때 필요한 동작과정에서의 성능을 비교하였다. 앞의 표 2를 통해 제안 인증 프로토콜과 기존 인증 프로토콜을 비교 정리하였다. 표에서 T_H는 해쉬 함수 계산 시간, T_{Cert}는 인증서 검증 시간을 의미한다. 제안 기법의 p는 임의의 큰 소수를 의미하고, 기존 기법의 n은 RSA의 n이다. 표에서 보여주고 있는 것처럼 제안 기법은 댁외로 이동한 사용자에 대한 네트워크 접속 인증 및 서비스 인증 과정에서 전체적인 통신 오버헤드 및 연산량이 기존 기법에 비해 적다.

기존 기법의 경우 댁외로 이동한 이동 단말은 IPTV 서비스 사용을 위해 네트워크 접속 인증과

표 2. 제안 기법 성능 비교

		제안 기법	• WTLS-RSA[14] 기반 인증
보안 요구사항		IPTV 헤드엔드와 STB 간 CAS 적용	무선 구간 보안 WTLS 적용
사용되는 보안 알고리즘		Schnorr 서명, Diffie-Hellman, 해쉬함수	AKA, RSA, 해쉬함수
인증 수행 시 메시지 교환 수	망 접속 인증	2번	WTLS Full Handshake: 9번, WTLS Abbreviated Handshake: 6번
	서비스 접속 인증	5번	6번
망 접속 인증 시 각 노드 연산량	이동 노드	$T_H + O(2(\log p)^3)$	$3T_H + O(4(\log n)^3 + 4(\log n)^2 + (\log n)) + T_{Cert}$
	AP/BS, WAP Proxy	$T_H + O(3(\log p)^3 + 2(\log p)^2)$	$4T_H + T_{Cert} + O(5(\log n)^3 + 7(\log n)^2)$
서비스 접속 인증 시 각 노드 연산량	이동 노드	T_H	T_H
	AP/BS, WAP Proxy	0	$2T_H + O((\log n)^3)$
	인증 서버	T_H	$T_{Cert} + 3T_D$
인증 수행을 위해 필요한 전체 메시지 교환 수		7번	15번 (WTLS: Full Handshake) 12번 (WTLS: Abbreviated Handshake)
인증 수행에 필요한 전체 연산량		$3T_H + O(5(\log p)^3 + 2(\log p)^2)$	$10T_H + 3T_{Cert} + O(10(\log n)^3 + 11(\log n)^2 + (\log n))$

IPTV 서비스 인증 등 두 번의 인증 절차를 각각 수행해야 한다. 그러나 제안 기법의 경우 네트워크 접속 인증을 성공한 다음 IPTV 서비스 사용을 위한 서비스 인증을 이동 단말에서 새롭게 시작하는 것이 아니라 네트워크 접속 인증과 동시에 통합적으로 수행되기 때문에 전체 인증을 위한 메시지 교환 횟수를 줄일 수 있다. 또한 제안 기법은 IPTV 서비스 인증을 위해 인증 서버에서 한 번의 해쉬 함수 계산만을 필요로 하기 때문에 전체 인증을 위한 연산량 또한 작다. 이는 STB가 인증 서버를 대신하여 이동 단말에게 발급한 서명에 포함된 보안 값 $SP_{MSK-UDi}$을 사용하기 때문이다. 보안 값은 STB가 이동 단말의 서명을 생성할 때 인증 서버와 공유하는 MSK와 이동 단말의 식별 정보를 이용하여 STB가 생성하여 이동 단말을 위한 서명에 포함한다. 네트워크 접속 지점은 이동 단말의 서명을 검증할 때 서명에 포함된 보안 값 $SP_{MSK-UDi}$을 사전에 인증 서버와 안전한 방법으로 형성한 보안 채널을 통해 인증 서버로 전달하고, 인증 서버는 STB와 공유하고 있는 MSK와 네트워크 접속 지점에서 보안 값과 함께 전달한 ID_{UDi}를 해쉬한 값을 비교함으로써 이동 단말에 대한 서비스 인증을 수행한다. 따라서 기존 기법에 비해 서비스 인증시 연산량을 효과적으로 줄일 수 있다. 또한 제안 기법의 경우 대부분의 연산은 인증 서버 및 네트워크 서비스를 제공하는 장비에서 수행되고, IPTV 서비스를 제공받기 전에 수행되기 때문에 인증 과정 추가에 따른 이동 노드에서의 연산부담을 줄일 수 있다.

위에서 설명한 것처럼 본 논문에서 제한하는 인증 프로토콜은 댁내 및 댁외에서 이동 가능한 IPTV 서비스 가용 단말에 대한 효과적인 인증을 제공할 수 있다. 또한, 댁외로 이동한 IPTV 서비스 가용 단말에 대한 네트워크 접속 인증 및 IPTV 서비스 인증 시 인증 과정에서 발생하는 통신 오버헤드 및 각 노드에서 연산량을 효과적으로 줄여 이동하는 사용자에게도 지속적인 IPTV 서비스를 제공한다.

V. 결 론

본 논문은 IPTV 서비스 환경에서 댁내에 존재하는 이동 IPTV 서비스 가용 단말들이 댁내 및 댁외에서 IPTV 콘텐츠를 안전하게 제공받을 수 있도록 지원하기 위한 댁내 및 댁외 인증 프로토콜을 제안하였다. 제안된 인증 프로토콜은 댁내 또는 댁외에서 이동 가능한 IPTV 서비스 가용 단말을 이용한 불법적인 IPTV 서비스 사용을 막기 위해 댁내에 설치되는 셋톱박스가 인증 서버를 대신하여 댁내에서 셋톱박스에 등록하는 IPTV 서비스 가용 단말들에게 Schnorr 서명 기법을 이용한 서명을 발급하고, 이 서명을 통해 인증된 IPTV 서비스 가용 단말들만 정상적으로 IPTV 서비스를 제공 받을 수 있게 하였다. 또한 댁내에서 셋톱박스가 인증 서버를 대신하여 발행한 서명은 가입자가 셋톱박스에 등록된 IPTV 서비스 가용단말을 들고 댁외로 이동할 경우 서명을 이용하여 네트워크 접속 인증 및 IPTV 서비스 접속 인증을 통합적으로 수행할 수 있도록 제안하여 보안 기술 적용에 따른 통신 오버헤드 및 지연시간을 줄여 댁외에서도 지속적인 IPTV 서비스를 제공받을 수 있도록 하였다.

참 고 문 헌

[1] R. Sharpe, J. Heiles, L. Hong, M. Deschanel, W. Yiyan, J. Maisonneuve, and L. Wei, “An Overview of IPTV Standards Development,” IEEE Transactions on Broadcasting, Vol.55, Issue 2, pp.315-328, Jun. 2009.

[2] ITU-T X.iptvsec-1, “Draft Recommendation X.iptvsec-1: IPTV security aspects,” Apr. 2008.

[3] ITU-T X.iptvsec-2, “The draft Recommendation for X.iptvsec-2: Functional requirements and mechanisms for secure transcodable scheme of IPTV,” Feb. 2009.

[4] ITU-T X.iptvsec-3, “Proposed third draft text on Recommendation X.iptvsec-3 : Key management framework for secure IPTV services,” Feb. 2009.

[5] ITU-T X.iptvsec-4, “Draft Text on X.iptvsec-4: Algorithm selection scheme for SCP descrambling,” Nov. 2008.

[6] ITU-T X.iptvsec-5, “Draft Recommendation X.iptvsec-5, SCP interoperability Scheme,” Feb. 2009.k for secure IPTV services, Feb. 2009.

[7] E. Cruselles, J.L. Melus, and M. Soriano, “An Overview of Security in Eurocrypt Conditional Access System,” Global Telecommunications Conference, Nov. 1993.

[8] B. Rosenblatt, B. Trippe, and S. Mooney,

"Digital Rights Management - Business and Technology," M&T Books, 2002.
〔9〕 우제학, 노창현, 이완복, "IPTV 콘텐츠 보호 기술의 비교 - CAS와 DRM 중심으로," 한국콘텐츠학회논문지, '06, 제6권, 제8호, 2006.
〔10〕 C. P. Schnorr, "Efficient Identification and Signatures for Smart cards," Advances of Cryptology - CRYPTO '89, LNCS, pp. 239-251, January, 1989.
〔11〕 M. Mambo, K. Usuda, and E. Okamoto, "Proxy signatures: Delegation of the power to sign message," IEICE Trans, E79-A, pp.1338-1354, 1996.
〔12〕 Rescorla, E., "Diffie-Hellman Key Agreement Method," RFC 2631, IETF Network Working Group, Jun. 1999.
〔13〕 정윤수, 김용태, 박길철, 이상호, "이동 장비에서 안전한 IPTV 서비스를 사용하기 위한 사용자 인증 메커니즘," 한국통신학회논문지, 제34호, 제4권, 2009.
〔14〕 D. Kwak, J. Ha, H. Lee, H. Kim, and S. Moon, "A WTLS handshake protocol with user anonymity and forward secrecy," CDMA International Conference '02, LNCS Vol.2524, pp.219-30, Springer Verlag, 2002.

노 효 선 (Hyosun Roh) 정회원

2005년 2월 숭실대학교 정보통신전자공학부 학사
2007년 2월 숭실대학교 정보통신전자공학부 석사
2007년 3월~현재 숭실대학교 전자공학과 박사과정
<관심분야> 네트워크 보안, 이동 네트워크 보안, IPTV 보안

정 서 현 (Seohyun Jung) 준회원

2009년 2월 : 숭실대학교 정보통신전자공학부
2009년 3월~현재 : 숭실대학교 전자공학과 석사과정
<관심분야> 네트워크 보안, 차량 보안, IPTV 보안

이 정 현 (Jeonghyun Yi) 정회원

1992년 2월 숭실대학교 전자계산학과 졸업
1995년 2월 숭실대학교 컴퓨터학과 석사
2005년 8월 University of California, Irvine 박사
1995년~2001년 한국전자통신연구원 연구원
2000년~2001년 National Institute of Standards and Technology 객원연구원
2005년~2008년: 삼성종합기술원 수석연구원
2008년~현재: 숭실대학교 컴퓨터학부 조교수
<관심분야> 모바일 보안, 네트워크 보안, 클라우드 보안, 응용보안

정 수 환 (Souhwan Jung) 종신회원

1985년 2월 서울대학교 전자공학과
1987년 2월 서울대학교 전자공학과 석사
1996년 6월 University of Washington 박사
1996년~1997년 Stellar One SW Engineer
1997년~현재 숭실대학교 정보통신전자공학부 부교수
2009년~현재 지식경제부 지식정보보안 PD
<관심분야> 이동 네트워크 보안, 차량 네트워크 보안, VoIP 보안, RFID/USN 보안