http://dx.doi.org/10.3745/KIPSTC.2011.18C.4.227

개방형 IPTV 환경에서의 사용자 인증 및 키 분배 메커니즘

정 지 연[†] · 도 인 실[††] · 채 기 준[†††]

요 약

IPTV는 대표적인 방송통신융합 산업으로 IP망의 양방향성을 이용한 서비스의 차별화를 내세우며 여러 사업자에 의해 서비스가 이루어지고 있다. 최근에는 모바일 환경 등으로 그 영역을 확대하기 위한 연구가 진행되고 있으며 다른 한편으로는 IPTV 서비스를 위한 플랫폼 등을 개방하여 사업자가 아닌 일반인도 IPTV를 통한 방송을 할 수 있는 구조인 개방형 IPTV에 대한 연구가 활발하다. 이러한 개방형 IPTV 환경에서는 다수의 콘텐츠 제공자가 존재하기 때문에 기존 IPTV에서 사용되는 특정 기기 혹은 스마트카드를 통한 사용자 인증 및 키 분배가 어려운 실정이다. 본 논문에서는 기존 분산 네트워크에서의 인증 메커니즘인 Kerberos를 기반으로 하여 분산 환경에서 안전한 사용자 인증과 키 분배를 위한 메커니즘을 제안하였다. 제안 메커니즘은 콘텐츠의 안전한 전송을 보장하며 기존 제안된 IPTV 사용자 인증 관련 연구보다 인증 시간 오버헤드에 있어 우위에 있음을 시뮬레이션을 통해 증명하였고 다양한 관점에서 제안 메커니즘을 다른 관련 연구와 비교하여 개방형 IPTV 환경에서 제안 메커니즘이 갖는 효율성을 증명하였으며 IPTV가 갖는 보안 요구 사항을 제안 메커니즘이 만족한다는 것을 보였다.

키워드 : IPTV, 콘텐츠 보안, 사용자 인증, 키 분배

User Authentication and Key Distribution on Open IPTV System

Jiyeon Jung[†] · Inshil Doh[††] · Kijoon Chae[†††]

ABSTRACT

IPTV(Internet Protocol Television) is one of the typical businesses which are the convergence of Broadcast and Communication. It provides broadcasting service using IP networks. Recently, IPTV service is developed to Mobile IPTV or Open IPTV. Especially, Open IPTV uses open platform so not only service providers but also general users can provide contents to other users. Open IPTV system has many content providers, so existing security solution of IPTV cannot be adopted. In this paper, we suggest user authentication and key distribution mechanism on Open IPTV. Our proposed mechanism is based on Kerberos, so it can support distribution environment such as Open IPTV. We demonstrate that proposed mechanism can guarantee secure transmission of contents and reduce the delay of user authentication on Open IPTV system compared to other authentication mechanisms. We also compare our proposal and other mechanisms in various aspects, and analyze efficiency and safety of proposed mechanism. As a result, we insist that this mechanism satisfies the security requirements for IPTV.

Keywords : IPTV, Contents Protection, User Authentication, Key Distribution

1. 서 론

정보통신 기술의 발달로 인한 전송망의 고도화와 산업의 디지털화에 따른 디지털 비디오 압축 기술의 개발은 광대역 전송망을 통해 고화질의 비디오 전송을 가능하게 하였다. 이에 따라 통신과 방송 각 특징을 모두 지니고 있는 새로운 융합된 서비스가 나타났다. 이러한 통신·방송 융합 서비스로 현재 크게 대두되고 있는 서비스는 IPTV 서비스로 무한한 수의 방송 채널 선택, VoD(Video on Demand), 각종 양방향 응용 서비스 등 고품질의 다양한 방송·통신 융합 서비스를 제공한다.

최근 IPTV는 미디어 서비스 업계에서 새로운 사업 모델로서 주목받고 있다. 그러나 기존 DMB 서비스와의 유사함 때문에 업계에서는 IPTV 사업의 성공을 위해서는 단순히 IP망을 이용한 방송서비스에 그치는 것이 아니라 IP망의 양방향성을 이용한 대화형의 개인화된 서비스를 제공해야 한다는 것에 의견을 모으고 있다[1].

위와 같은 IPTV의 차별화된 발전을 위하여 학계에서는

※ 이 논문은 2009년도 정부(교육과학기술부)의 재원으로 한국학술진흥재단의 지원을 받아 수행된 연구임(NRF-2009-0083985).
† 정 회 원 : LG Electronics 연구원
†† 정 회 원 : 이화여자대학교 컴퓨터공학과 연구교수(교신저자)
††† 종신회원 : 이화여자대학교 컴퓨터공학과 교수
논문접수 : 2011년 3월 28일
수 정 일 : 1차 2011년 5월 31일
심사완료 : 2011년 6월 1일

개방형 IPTV라는 개념을 정의하고 개방형 IPTV 솔루션의 표준화를 진행하고 있다. 개방형 IPTV는 IPTV의 서비스 플랫폼을 공개적으로 개방함으로써 특정 IPTV 서비스 제공자나 네트워크 망 사업자, 단말기 사업자 등에 얽매이지 않고 궁극적으로는 일반인도 IPTV 서비스를 할 수 있는 환경을 말한다. 주요 표준화 단체로는 Open IPTV Forum[2][3]이 존재하며, 이 단체는 managed, 혹은 non-managed network 상에서의 개인화된 IPTV 서비스를 제공하기 위한 End-to-End Solution을 개발하는 것을 목표로 하고 있다.

개방형 IPTV 이외에도 IPTV 서비스를 기존 방송 서비스와 차별화하기 위한 방법 중 하나로 3-Screen 개념이 주목받고 있다. 3-Screen은 2007년 초 미국의 통신사업자 AT&T에 의해 제안된 개념으로 TV, 컴퓨터, 휴대전화 등 3가지 유형의 스크린에 콘텐츠를 제공하는 서비스이다. 이는 네트워크 통합을 통해 콘텐츠를 자유롭게 이동할 뿐 아니라 서로 다른 기기에서 끊임없이 콘텐츠를 이용할 수 있는 환경을 말한다. 이에 따라 IPTV 업계에서는 3-Screen 개념을 IPTV에 적용시켜 다양한 기기에서 끊임없는 IPTV 서비스를 제공하기 위한 기술 개발에 박차를 가하고 있다.

IPTV 시스템이 이용하는 IP 네트워크는 기존의 방송 시스템과 달리 공개되어 있고 누구에게나 접근이 자유롭다는 특징을 가지기 때문에 그에 대한 불법 시청, 불법 복제, 접근 권한 오남용, IPTV 콘텐츠의 위험 등의 우려를 가지고 있다. 따라서 이와 같은 불법적인 접근을 차단하기 위해서 기존 방송 시스템은 CAS, DRM 등의 암호화 시스템을 사용하고 있다[4]. 그러나 기존의 암호화 시스템은 특정 사업자나 특정 기기에 종속되어있으며 특정 서비스 제공자에 의해 콘텐츠가 제공되는 환경에 적합하기 때문에 이를 그대로 개방형 IPTV에 적용시키기 어렵다. 개방형 IPTV 환경에서는 다수의 사용자가 콘텐츠 제공자의 역할을 할 수 있으며 사용자가 요구하는 서비스에 따라 불특정한 콘텐츠 제공자와의 신뢰 관계를 수립해야 하기 때문이다. 또한 기존 IPTV에 사용되는 콘텐츠 보안 시스템은 일반 케이블 TV에 사용되던 콘텐츠 보안 시스템을 그대로 사용하고 있기 때문에 IP 네트워크가 갖는 장점인 양방향성과 높은 대역폭을 충분히 활용하지 못하고 있다. 이와 같이 기존 IPTV 보안 시스템이 갖는 한계는 개방형 IPTV가 가지는 특징을 살리지 못하며 미래 IPTV의 발전 방향으로 꼽히는 3-Screen 개념을 적용하기 어렵다.

따라서 본 논문에서는 IP 네트워크가 갖는 장점을 살림과 동시에 미래 IPTV의 발전 방향에 알맞도록 개방형 IPTV 환경에서 3-Screen을 지원하는 사용자 인증 및 키 분배 메커니즘을 제안한다. 제안한 메커니즘은 기존에 널리 사용되고 있는 분산 네트워크 환경에서의 인증 메커니즘인 Kerberos를 IPTV 콘텐츠 보호 시스템인 CAS(Conditional Access System)와 접목하여 안전한 사용자 인증 및 키 분배를 통한 안전한 콘텐츠 전송을 할 수 있도록 하였으며 Kerberos를 통해 발급 받은 티켓을 홈 네트워크상의 다른 기기와 공유함으로써 3-Screen 개념을 지원할 수 있도록 하였다.

2. 관련 연구

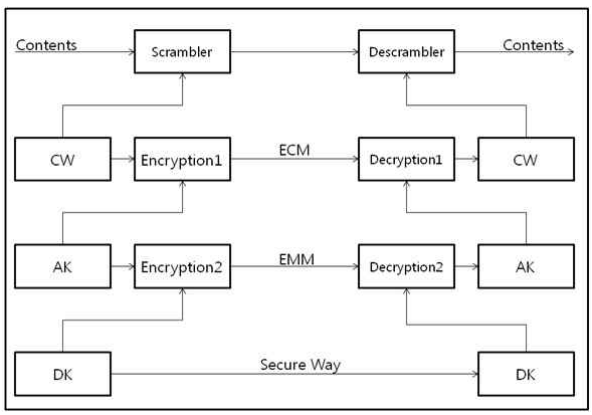
이 장에서는 기존 IPTV 보안 기술에 대해 설명하며 제안 메커니즘의 기술적 기반이 되는 분산 환경에서의 사용자 인증 메커니즘인 Kerberos에 대하여 간략히 설명한다.

2.1 IPTV 보안 기술

IPTV 사용자의 불법적인 시청을 방지하기 위해서 사용자를 인증하고 그의 접근을 적절히 제어할 수 있는 기술이 필요하였고 이를 시스템에 적용하는 방식에 따라 CAS (Conditional Access System) 방식과 DRM(Digital Right Management) 방식으로 분류된다. 이들 기술은 상호 배타적이면서 또 보완적인 특징을 가지고 있다.

2.1.1 CAS (Conditional Access System)[7]

CAS는 각 사용자에게 분배한 개인키를 이용하여 유료 콘텐츠를 적법한 사용자에게 안전하게 전송하기 위한 핵심 기술로서, 기존 디지털 TV 및 위성 방송, IPTV 등에서 콘텐츠 보호를 위해 사용되고 있다.



(그림 1) CAS의 구조

(그림 1)과 같이, CAS는 여러 단계의 키 관리 구조를 가지고 있는데, 이는 스트리밍 서비스에서 잦은 암호화로 인해 발생하는 부담을 분산시킴과 동시에 모든 사용자에게 동일하게 암호화된 콘텐츠를 전송함으로써 사용자 개개인에게 다른 키를 이용하여 암호화 하는 것에 비해 콘텐츠 전송자가 갖는 암호화의 부담을 줄일 수 있게 한다.

CAS의 구체적인 동작 과정은 다음과 같다. 우선 서버에서 전송하는 콘텐츠는 CW에 의해 암호화되어 ECM (Entitled Control Message)과 함께 전송되는데, 이 때 ECM에는 해당 방송의 수신 조건 및 CW의 정보를 담고 있으며 이 정보는 AK에 의해 암호화되어 있다. 이 후 AK는 각 사용자에게 주어진 DK로 암호화되어 EMM(Entitle Management Message)에 담겨 사용자에게 전송된다. 따라서 사용자가 암호화된 콘텐츠를 복호화하기 위해서는 서비스 제공자로부터 분배 받은 DK를 이용하여 EMM과 ECM

을 복호화 해야 한다. 이 복호화를 통해 사용자는 CW를 얻어 암호화된 콘텐츠를 복호화하여 시청할 수 있다.

위와 같은 CAS의 키 관리 구조는 댁내 STB(Set-Top Box)에 삽입되는 스마트카드에 DK를 담아 물리적으로 분배하는 것을 기반으로 하여 그 안전성을 보장한다. 이는 적합한 사용자만이 해당 키를 가지고 있다는 것을 전제로 하여 키 분배뿐 아니라 사용자 인증의 역할도 동시에 수행한다.

그러나 개방형 IPTV 환경에서는 STB와 같은 특정 단말에 귀속된 서비스가 아닌 다양한 기기를 대상으로 하여 서비스를 하는 것을 목표로 하고 있기 때문에 STB에 삽입하는 스마트카드를 이용한 물리적인 키 분배는 적합하지 않다. 또한 개방형 IPTV 환경에서의 콘텐츠 제공은 특정 IPTV 사업자 하나에 의한 것이 아니라 다수의 일반인이 콘텐츠 제공자가 될 수 있기 때문에 다대다(many-to-many) 환경에서의 사용자 인증 및 키 분배 시스템을 적용하는 것이 필요하다.

2.1.2 DRM (Digital Right Management)

DRM이란 디지털 콘텐츠의 생산, 분배, 거래규칙, 과금, 거래내역의 관리, 정산 등 디지털 콘텐츠의 전체 라이프 사이클에 걸쳐 투명성과 신뢰성을 보장하는 유통 체계 전반을 통칭하는 서비스를 말한다.

DRM은 사용자에게 부여된 권한에 따라 디지털 콘텐츠의 사용 권한을 지속적으로 통제하는 방식이다. 이 방식은 콘텐츠의 생명 주기 전체에 걸쳐 원본 추출이 보장되기 때문에 현재 네트워크를 통해 유통되는 많은 디지털 콘텐츠들이 이 기술을 이용하고 있다. 최근의 DRM 기술은 저작권 보호 기술 및 암호 알고리즘을 이용한 콘텐츠의 배포 관리, 워터마킹 기술을 이용한 콘텐츠 관리 기술까지 포함하여 다루고 있다.

이러한 기술을 채용한 DRM은 네트워크 환경에서 영상, 음악, 게임 등의 디지털 콘텐츠를 보호하기 위해 개발된 기술로서 미리 DRM을 적용한 후 콘텐츠를 유통해야 하기 때문에 실시간으로 콘텐츠가 제공되는 방송 서비스에는 적합하지 않은 부분이 있다. 따라서 방송된 이후의 콘텐츠를 보호하기 위해 DRM이 필요함에도 불구하고 방송 서비스에서 활용되지 못하였다. 그러나 주문형 방송과 실시간 방송을 동시에 제공하는 IPTV 서비스에서는 DRM도 이용 가능하다.

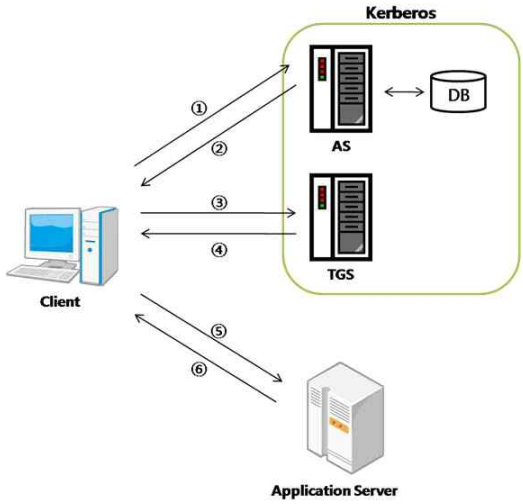
2.2 Kerberos[8]

Kerberos는 개방된 네트워크 환경에서 신뢰 받는 제 3자를 통한 서버와 클라이언트 간의 인증 프로토콜을 말하며 MIT에서 진행된 Project Athena에 의해 개발되었다.

Kerberos의 원리는 Needham과 Schroeder의 모델에 근거하여 신뢰 받는 제 3자인 중앙 인증 서버가 네트워크 상의 모든 개체와 서로 다른 비밀 키를 공유하고 그 비밀 키를 알고 있는 것으로 실체를 증명한다. 이에 클라이언트는 중앙 인증 서버에 자신의 신원을 증명 해 줄 것을 요청하고 중앙 인증 서버는 클라이언트에게 티켓을 발급 해 줌으로써 클라이언트의 신원을 보증한다. 클라이언트는 이 티켓을 제시하여 서버에게 서비스를 요청하고 서버는 티켓을 이용하여 올바른 클라이언트임을 확인 후 서비스를 제공한다.

Kerberos의 상세 인증 메커니즘은 다음과 같다(그림 2).

① 클라이언트의 ID와 TGS의 ID를 AS에 보내 TGT (Ticket Granting Ticket)을 요청한다.
② AS는 클라이언트와의 공유키를 이용하여 암호화된 정보와 클라이언트가 요청한 TGT를 클라이언트에게 전송한다.
③ 클라이언트는 TGT를 TGS에 전송하여 자신의 신원을 인증하고 SGT(Server Granting Ticket)을 요청한다.
④ TGS는 클라이언트가 전송한 티켓을 통해 클라이언트의 신원을 확인하고 요청한 SGT를 클라이언트에게 전송한다.
⑤ 클라이언트는 SGT를 서비스를 요청하고자 하는 서버에게 전송한다.
⑥ 서버는 SGT를 통해 클라이언트를 확인하고 서비스를 승인한다.



(그림 2) Kerberos의 인증 과정

Kerberos는 패스워드를 네트워크상에 노출시키지 않으며 대칭키 암호화 방식을 채택하여 암호화 과정에서 생기는 오버헤드가 작다는 장점이 있다. 이에 다양한 OS 및 SW에 채택되어 널리 사용되고 있다.

3. 개방형 IPTV 환경에서의 사용자 인증 및 키 분배 메커니즘

본 장에서는 개방형 IPTV가 갖고 있는 다대다 환경에서의 사용자 인증 및 키 분배를 위하여 분산 컴퓨팅 환경에서 사용자 인증을 제공하는 중앙 집중형 인증 방식인 Kerberos를 기반으로 한 제안 시스템을 소개하고 이 과정을 통해 분배된 키를 CAS 시스템에 접목시켜 안전하게 콘텐츠를 전송하는 과정과 사용자 인증 과정에서 발급한 티켓을 안전한 댁내에서 재분배함으로써 사용자가 댁내 다른 기기에서 끊임없는 서비스를 이용하는 과정에 대해 상세히 기술한다.

3.1 가정사항

본 논문에서 사용되는 기호는 <표 1>과 같으며 다음과 같은 가정 사항을 갖는다.

- 서비스 제공자는 사용자 인증을 위한 AS(Authentication Server)와 TGS(Ticket Granting Server)를 가지고 있으며 IPTV 사용자 사이의 서비스 중계 및 중앙 인증 서버 역할을 한다.
- 각 사용자는 서비스 제공자에 위치한 DB에 사전 등록되어 있으며 각 사용자의 ID, 과금 정보, 서비스 정보 등을 알고 있다.
- 각 사용자와 서비스 제공자 내에 위치한 AS와 TGS는 서로의 공유키를 사전에 가지고 있다.
- 홈 네트워크 상의 통신에 대한 보안은 본 논문에서는 다루지 않으며 안전하다고 가정한다.

〈표 1〉 기호 표기법

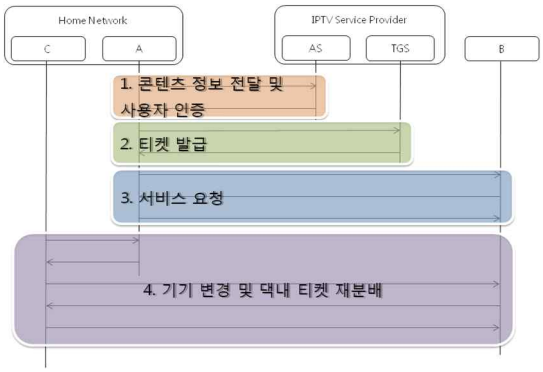
기호	내용
AS	Authentication Server
TGS	Ticket Granting Server
A	사용자
B	콘텐츠 제공자
C	사용자 A의 홈 네트워크 내 다른 기기
ID_N	각 사용자 및 서버 N의 ID
K_N	N과 서비스 제공자의 공유 키
$K_{A,B}$	A와 B사이의 공유키
$Ticket_N$	N에 접근하기 위해 발급된 티켓
$Authenticator_N$	N의 신원을 증명하기 위한 정보
$E(K_N,[M])$	메시지 M을 K_N으로 암호화 한 값
||	concatenation 연산자
Lifetime	각 티켓의 유효 기간

3.2 제안 메커니즘

사용자 A는 AS에게 자신이 제공할 콘텐츠 정보와 함께 인증을 요청한다. A에 대한 인증 및 신원 확인은 AS가 미리 가지고 있던 사용자 정보에 의해 이루어지며 신원 확인 후 TGS에 대한 접근 권한을 부여한다. 이 후 A는 TGS에 접근하여 원하는 콘텐츠 제공자(B)에 대한 접근 권한을 요청하고 TGS는 A의 신원을 확인하고 B에 접근 가능한 티켓을 발급한다. 발급된 티켓은 B에게 서비스 요청 시 함께 전송되어 신원 확인의 매개체가 된다. 이 후 A는 채널 변경(다른 콘텐츠 제공자에 서비스 요청) 시 TGS에 다시 접근하여 다른 콘텐츠 제공자의 서비스를 받을 수 있는 티켓을 요청하며, 홈 네트워크 내 다른 기기에서 서비스를 이어 받고 싶을 경우 홈 네트워크 내 티켓 재분배를 통해 인증 정보를 재이용한다.

3.2.1 콘텐츠 정보 전달 및 사용자 인증

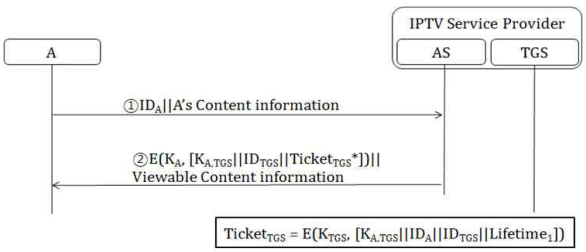
개방형 IPTV 서비스를 이용하고자 하는 사용자(A)는 자신이 제공 가능한 콘텐츠 정보와 함께 서비스 제공자에 위치하는 AS에 접근하여 사용자 인증을 요청한다. A가 전송한 콘텐츠 정보는 서비스 제공자에 저장되어 이 후 다른 사용자가 콘텐츠 정보를 요청할 시 사용된다. AS는 A의 사용



(그림 3) 제안 메커니즘의 구조

자 인증 요청을 확인하고 미리 저장되어 있던 정보를 바탕으로 신원을 확인한다. 이 후 A가 TGS에 접근 가능한 티켓을 생성하여 A와 TGS 사이의 공유키 및 A가 시청 가능한 콘텐츠 정보와 함께 A에게 전송한다. TGS에 접근 가능한 티켓은 A와 TGS의 ID, 티켓의 life time을 담고 있으며 TGS와 AS 간의 공유키로 암호화되어 있어 오직 TGS만 복호화 하여 내용을 확인할 수 있다. 따라서 티켓은 AS가 생성한 A의 신원 보증 매개체가 된다.

각 단계에서 전달되는 값의 상세 정보는 (그림 4)와 같다.



(그림 4) 콘텐츠 정보 전달 및 사용자 인증

① A는 AS에게 자신의 ID(ID_A)와 자신이 제공 가능한 콘텐츠 정보(A's Content info)를 전달하면서 사용자 인증을 요청한다.

② AS는 A의 ID(ID_A)를 바탕으로 A의 신원을 확인하고 A의 콘텐츠 정보(A's Content info)를 자신의 DB에 저장하여 이 후 다른 사용자의 서비스 요청 시 사용한다. A의 신원 확인이 완료되면 A와 TGS가 사용할 공유키($K_{A,TGS}$)와 A가 TGS에 접근 가능한 티켓($Ticket_{TGS}$)을 생성하고 공유키($K_{A,TGS}$), TGS의 ID(ID_{TGS}), TGS에 접근 가능한 티켓($Ticket_{TGS}$)을 A와의 공유키(K_A)로 암호화 하여 A가 시청 가능한 콘텐츠 정보(Viewable content info)와 함께 전송한다.

3.2.2 티켓 발급

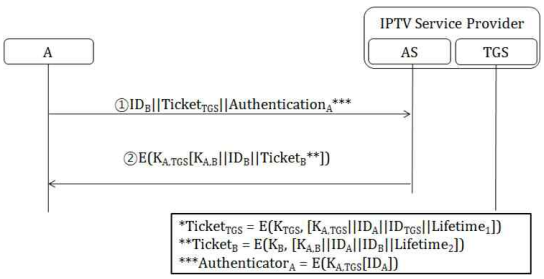
사용자 A는 AS로부터 발급 받은 티켓을 이용하여 TGS에게 자신이 시청하고자 하는 사용자에 대한 접근 권한을 요청한다. 이 때 자신의 신원 정보를 담아 TGS와의 공유키로 암호화 한 Authenticator를 함께 전송한다. 이는 이후

TGS가 A의 신원을 확인하는 매개체로 사용된다. TGS는 A가 전달한 티켓 및 Authenticator를 자신이 가지고 있는 키를 이용하여 복호화 하고 성공적으로 이루어지면 A의 인증을 완료한다. 이 후 A가 요청한 콘텐츠 제공자(B)에 접근할 수 있도록 B에 대한 티켓과 A와 B사이의 공유키를 생성하여 A에게 전송한다.

각 단계에서 전달되는 값의 상세 정보는 다음과 같다.

① A는 자신의 신원을 증명할 Authenticator ($Authenticator_A$)를 생성하여 AS로부터 받은 티켓($Ticket_{TGS}$)과 함께 TGS에게 자신이 시청하고자 하는 콘텐츠 제공자(B)에 대한 접근 권한을 요청한다. 이 때 Authenticator는 A의 신원을 TGS에게 증명하기 위해 사용되며 A와 TGS의 공유키($K_{A,TGS}$)로 암호화되어 TGS만 복호화가 가능한 값이다.

② TGS는 티켓 및 Authenticator를 통해 A의 신원을 확인하고 그 결과 신원이 확실한 경우 A가 요청한 콘텐츠 제공자(B)에 접근할 수 있도록 A와 B사이의 공유키($K_{A,B}$)와 B와 TGS 사이의 공유키(K_B)로 암호화되어 있는 티켓($Ticket_B$)을 생성하여 B의 ID(ID_B)와 함께 A에게 전달한다. 이 때 모든 값은 A와 TGS 사이의 공유키($K_{A,TGS}$)로 암호화되어 있어 A만이 확인 가능하다.



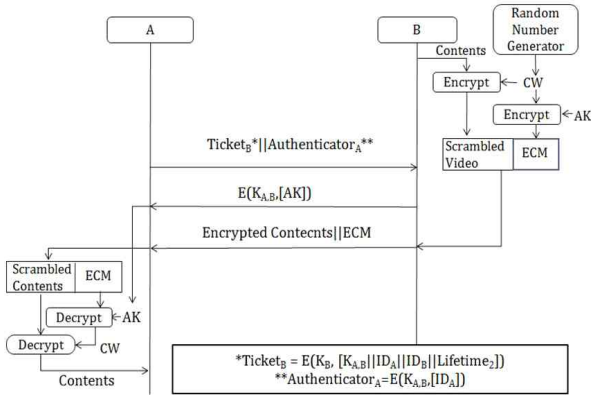
(그림 5) 티켓 발급 절차

3.2.3 서비스 요청

콘텐츠 제공자가 제공하는 콘텐츠는 사전에 CAS를 통해 암호화되어 있으며 사용자 A는 이 콘텐츠를 시청하기 위해 TGS에게 전달받은 티켓과 자신의 신원을 인증 할 Authenticator를 생성하여 B에게 전달하며 서비스를 요청한다. B는 TGS와의 공유키로 티켓을 복호화 하여 확인하고 A와의 공유키로 Authenticator를 복호화 하여 A의 신원을 확인한다. A의 신원 확인이 끝나면 B는 A가 자신의 콘텐츠를 시청할 수 있도록 콘텐츠를 복호화 할 수 있는 키인 AK를 A와의 공유키로 암호화 하여 A에게 전달한다. 이 후 AK는 사용자 A가 B가 전송하는 콘텐츠를 복호화 하는데 사용되어 A는 B의 콘텐츠를 시청할 수 있다.

각 단계에서 전달되는 값의 상세 정보는 (그림 6)과 같다.

① B는 사전에 자신이 제공할 콘텐츠를 CAS(Conditonal Access System)를 통하여 암호화한다. 본 논문에서 사용되는 CAS는 제안 메커니즘에 의해 기존 3단계 암호화에서 2단계 암호화로 간소화되었으며 콘텐츠를 CW(Control Word)로 암호화 하고 다시 CW를 AK(Authentication Key)로 암호화 하여 ECM(Entitled Control Message)을 생성, 암호화된 콘텐츠와 함께 전송된다.



(그림 6) 서비스 요청

② 사용자 A는 TGS로부터 발급받은 티켓($Ticket_B$)과 자신의 신원을 알리는 Authenticator($Authenticator_A$)를 생성하여 전달함으로써 서비스를 요청한다. Authenticator는 A의 ID(ID_A) 정보를 담고 있으며 A와 B의 공유키($K_{A,B}$)로 암호화되어 있다.

③ B는 A가 전송한 티켓($Ticket_B$)을 자신과 TGS의 공유키(K_B)로 복호화 하여 확인하고, Authenticator를 티켓으로부터 얻은 자신과 A의 공유키($K_{A,B}$)로 복호화 하여 A의 신원을 확인한다. A가 올바른 사용자임이 판명되면 A가 자신의 콘텐츠를 복호화 하여 시청할 수 있도록 AK를 자신과 A의 공유키로 암호화 하여 전송한다.

④ 이 후 B는 자신의 암호화된 콘텐츠와 ECM를 전달하는 멀티캐스팅 그룹에 A를 포함시킨다.

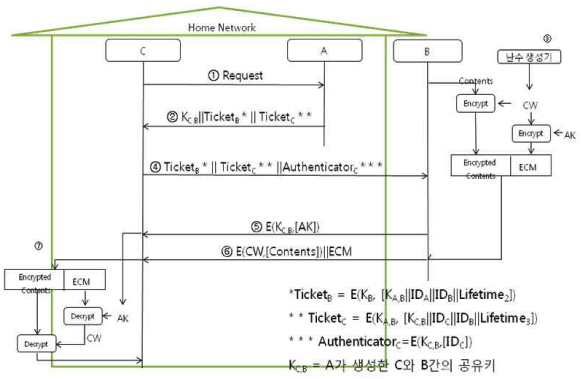
⑤ A는 ③에서 받은 AK를 이용하여 B로부터 받은 ECM을 복호화 하여 CW를 얻고 CW를 이용하여 암호화된 콘텐츠를 복호화 하여 시청한다.

3.2.4 기기 변경 및 댁내 티켓 재분배

제안 메커니즘은 단일 사용자의 단일기기 인증뿐 아니라 해당 사용자가 다른 기기에서 끊김 없는 서비스를 받을 수 있도록 댁내 티켓 재분배를 통해 간소화된 인증 방법을 포함한다.

사용자 A는 자신과 같은 홈 네트워크상에 존재하는 다른 기기(C)에서 서비스를 이어 받을 수 있도록 C에서 A로 요청을 한다. A는 자신의 이용하던 콘텐츠를 C에서도 이어 사용할 수 있도록 자신이 가지고 있던 콘텐츠 제공자(B)에 대한 인증 정보를 C에게 넘겨준다. 즉 기존에 인증 과정을 거쳐 자신이 가지고 있던 티켓을 C에게 넘겨주고, 스스로가 인증 주체가 되어 C의 신원을 B에게 보장한다. 이러한 과정을 통해 C는 새롭게 서비스 제공자에 접근하지 않아도 A가 사용 중 이었던 서비스를 이어 받을 수 있고, 이는 기기 변경 시 생길 수 있는 인증에 의한 지연을 줄일 수 있도록 한다.

각 단계에서 전달되는 값의 상세 정보는 (그림 7) 과 같다.



(그림 7) 기기 변경 및 댁내 티켓 재분배

① A와 같은 홈 네트워크상에 존재하는 다른 기기인 C는 기존 인증 과정을 거쳐 서비스를 사용 중인 A에게 서비스를 이어 받고자 요청 메시지를 보낸다.

② A는 C가 자신과 같은 홈 네트워크에 존재하는 안전한 사용자임을 B에게 알려주기 위해 자신이 가지고 있던 인증 정보인 티켓($Ticket_B$)을 전달하고 동시에 C와 B 사이에 사용될 공유키($K_{C,B}$), 그리고 C의 신원을 B에게 알려주기 위한 새로운 티켓($Ticket_C$)을 생성하여 C에게 전달한다.

③ B는 사전에 자신이 제공할 콘텐츠를 CAS를 통하여 암호화한다.

④ C는 A로부터 받은 두 개의 티켓($Ticket_B$, $Ticket_C$)과 자신의 신원을 알릴 Authenticator($Authenticator_C$)를 생성하여 B에게 전달함으로써 B에게 서비스를 요청한다.

⑤ B는 $Ticket_B$를 TGS와의 공유키(K_B)로 복호화 하여 A의 정당성을 확인하고 $Ticket_C$를 A와의 공유키($K_{A,B}$)로 복호화 하여 내용을 확인함으로써 C의 정당성을 확인한다. 이 과정을 통해 B는 C의 신원을 확인하고 자신과 C 사이에 사용할 공유키($K_{C,B}$)를 얻는다. 이 후 C가 자신의 콘텐츠를 복호화 하여 시청할 수 있도록 AK를 자신과 C의 공유키($K_{C,B}$)로 암호화 하여 전송한다.

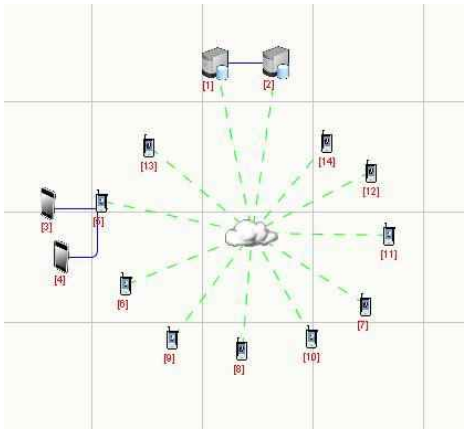
⑥ 이 후 B는 자신의 암호화된 콘텐츠와 ECM를 전달하는 멀티캐스팅 그룹에 C를 포함시킨다.

⑦ C는 ⑤에서 받은 AK를 이용하여 B로부터 받은 ECM을 복호화 하여 CW를 얻고 CW를 이용하여 암호화된 콘텐츠를 복호화 하여 시청한다.

4. 제안 메커니즘 실험 및 분석

4.1 시뮬레이션 환경

본 논문에서 제안한 개방형 IPTV 환경에서 사용자 인증 및 키 분배 메커니즘의 성능을 분석하기 위하여 (그림 8)과 같이 네트워크 환경을 구성하였다. 서비스 제공자에는 AS와 TGS 서버가 위치하여 중앙 인증 서버의 역할을 하며 그 외 총 10명의 콘텐츠 제공자의 역할을 하는 사용자를 배치하였다. 사용자의 일부는 홈 네트워크를 구성하여 제안한 티켓 재분배 메커니즘을 실험할 수 있도록 하였다. 각 사용자가



(그림 8) 시뮬레이션 환경

서비스를 사용하기 위해서는 서비스 제공자에 위치한 AS 및 TGS 서버에 접속하고 권한을 얻은 후 IP 망을 통하여 다른 사용자와 통신하여 서비스를 제공받도록 하였다.

시뮬레이션은 QualNet 4.5 버전을 사용하였다. QualNet은 가상의 네트워크 기반에서 다양한 프로토콜을 설계·분석·검증하며 네트워크 어플리케이션 등을 실제로 구축하기 전에 가상의 공간에 구축하여 문제점을 분석하고 예측할 수 있는 소프트웨어이다. Sensor Network를 비롯하여, WLAN, Mobile Ad hoc Network, Wired LAN, Cellular Network, Satellite Network에 대한 기본적인 라이브러리를 가지고 있으며 사용자가 이 프로토콜을 수정하여 확장 사용할 수 있는 장점이 있다.

본 논문에서는 QualNet을 사용하여 기존 IPTV 사용자 인증 메커니즘과 제안 메커니즘의 인증 소요 시간을 다양한 각도에서 비교·분석하였고 제안 메커니즘의 효율성 및 안전성을 여러 면에서 분석·기술하였다.

<표 2>는 상세 시뮬레이션 환경 및 시뮬레이션 시 사용된 제안 메커니즘 및 비교 대상 메커니즘의 암호화 기법을 요약 한 것이다.

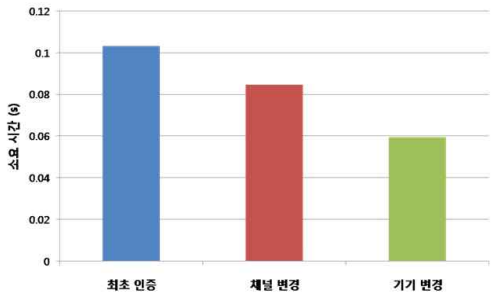
〈표 2〉 시뮬레이션 환경

시뮬레이션 툴	Qualnet 4.5		
기기 사양	CPU	Intel Core2Duo 2.93GHz	
	RAM	3.00GB	
네트워크 구성	중앙 인증 서버(AS, TGS)와 10명의 사용자		
시뮬레이션 방법	각 사용자가 순차적으로 인증 및 서비스 요청 전체 평균값으로 인증 시간 측정		
암호화 기법	제안 메커니즘	자바카드 기반	OTP 기반
	56bit DES	56bit DES	ExclusiveOR연산

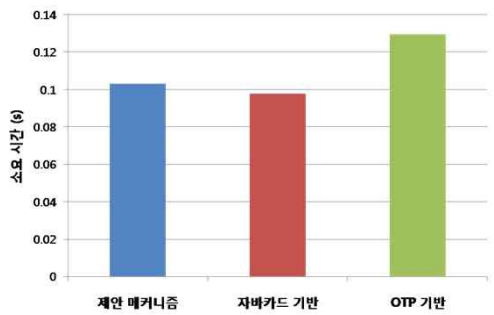
4.2 인증 소요 시간 실험 및 분석

(그림 9)은 제안 메커니즘의 상황별 인증 소요 시간을 측정한 것이다. 제안 메커니즘에 의해 사용자가 처음 인증 과정을 거쳤을 경우 소요되는 시간에 비해 이 후 채널을 변경하거나 홈 네트워크 상에서 기기변경을 할 때 소요되는 인

증 시간이 각각 0.02초와 0.04초 줄어든 것을 볼 수 있다. 이는 제안 메커니즘이 SSO (Single-Sign-On)를 지원하여 최초 인증 후 서비스를 받는 대상을 바꾸고자 할 경우 인증 과정을 처음부터 다시 진행하지 않아도 서비스를 요청할 수 있기 때문이다. 즉 한 번의 로그인으로 다수의 서버로부터 서비스를 받을 수 있기 때문에 개방형 IPTV처럼 다수의 사용자로부터 콘텐츠를 받는 환경에 적합하다고 할 수 있다. 또한 중앙 인증 서버로부터 발급 받은 티켓을 안전한 홈 네트워크에서 재분배하는 티켓 재분배 방법은 최초 인증 소요 시간에 비해 기기 변경 시 소요되는 인증 시간을 0.04초 줄이는 결과를 얻었다. 이는 사용자가 홈 네트워크 상의 다른 기기에서 이어 서비스를 받고자 할 때 생기는 지연시간을 줄여 사용자의 편의성을 높이는 결과를 가져올 수 있다.



(그림 9) 제안 메커니즘의 상황별 인증 소요 시간

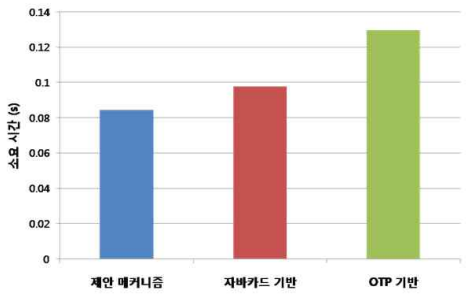


(그림 10) 메커니즘 간 인증 소요 시간 비교

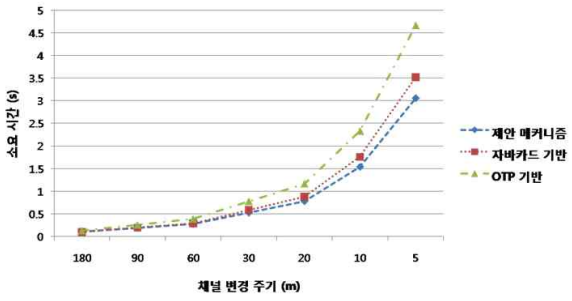
(그림 10)은 기존 논문에서 제안된 IPTV 사용자 인증 메커니즘의 인증 소요 시간을 제안 메커니즘과 비교 한 것이다. 각 인증 소요 시간은 사용자 1인이 서비스를 요청하여 인증 과정을 거쳐 서비스를 받을 수 있을 때까지의 시간을 측정 한 것이며 각각 자바카드[6]와 OTP[5]를 기반으로 제안한 기존의 메커니즘과 비교하였다. 그 결과 제안 메커니즘은 자바카드 기반의 메커니즘에 비해서 0.01초 정도 더 소요되는 것으로 나타났지만 OTP 기반의 메커니즘에 비해서는 0.02초 정도 빠른 것으로 나타났다. 이는 제안 메커니즘에서는 DES를 사용하여 암호화된 티켓을 생성하는 작업을 여러 번 하는 반면 자바카드 기반의 메커니즘은 자바카드를 이용하여 각 사용자에 대한 개인키를 분배하고 이를 이용하여 새로운 키를 분배 받는 방식이기 때문인 것으로 보인다. 반면 OTP 기반의 메커니즘은 각 사용자간 OTP를 수립하기 위해 여러 번의 통신을 거쳐야 하는 것에 비해 제안 메커니즘은 비교적 적은 횟수의 통신을 하기 때문에 OTP 기반 메커니즘과 비교해서는 더 빠른 인증 시간을 보였다.

4.3 채널 변경 시 인증 소요 시간 실험 및 분석

최초 인증 시 소요 시간에서 제안 메커니즘이 자바카드 기반의 메커니즘보다 더 긴 시간을 사용한 것에 비해서 (그림 11)의 채널 변경 시 인증 소요 시간에서는 제안 메커니즘이 가장 짧은 시간을 사용한다는 결과가 나온 것을 볼 수 있다. 이는 기존의 자바카드와 OTP 기반의 메커니즘이 채널 변경 상황을 고려하지 않았기 때문에 사용자가 채널 변경 시, 즉 다른 사용자로부터 콘텐츠를 제공받고자 할 경우 각각 제안한 인증 절차를 다시 거쳐야 하기 때문이다. 반면 제안 메커니즘은 SSO를 제공하여 다른 사용자로부터 콘텐츠를 받고자 할 때 인증 절차의 처음부터 반복하는 것이 아니라 일부분만 반복함으로써 다른 콘텐츠 제공자에 대한 권한을 얻을 수 있다. 그 결과 제안 메커니즘은 자바카드 기반, OTP 기반 메커니즘에 비해 각각 약 0.02초, 0.04초의 시간을 단축한 결과를 얻을 수 있었다. 채널 변경 시 생기는 지연시간은 Channel Zapping Time이라고 불리며 사용자가 직접적으로 느끼는 민감한 지연시간으로 이를 줄이기 위해 다양한 연구가 진행되고 있다.



(그림 11) 채널 변경 시 인증 소요 시간 비교



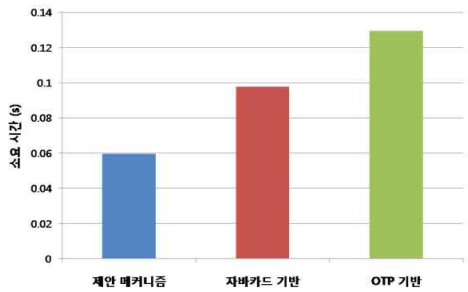
(그림 12) 채널 변경 주기에 따른 인증 누적 시간 비교

채널 변경 시 생기는 인증 시간의 차이는 채널 변경 주기에 따라 더욱 크게 나타난다. (그림 12)는 사용자가 총 3시간 동안 IPTV를 시청 한 경우 채널 변경 주기에 따른 총 인증 소요 시간을 측정 한 것이다. 그 결과 3시간 동안 채널 변경을 1번 했을 경우는 세 메커니즘 간에 큰 차이를 보

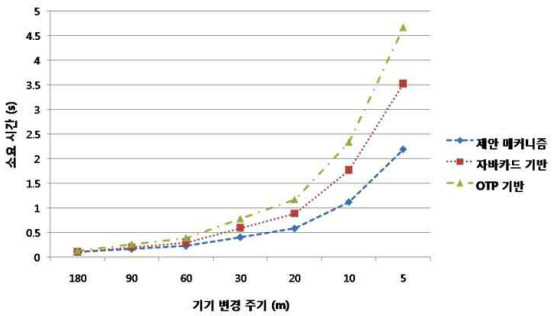
이지 않지만 채널 변경을 자주 할수록 그 차이가 벌어지는 것을 볼 수 있다. 특히 최초 인증에서는 제안 메커니즘보다 빠른 결과를 보였던 자바카드 기반의 메커니즘도 채널 변경 빈도수가 높아질수록 제안 메커니즘보다 더 많은 인증 시간을 소모하는 것으로 나타났다.

4.4 댁내 기기 변경 시 인증 소요 시간 실험 및 분석

(그림 13)은 사용자가 홈 네트워크 상에서 기기를 변경하여 서비스를 이어 받고자 할 경우 생기는 인증 소요 시간을 측정 한 것이다. 홈 네트워크 상의 끊임없는 서비스는 차세대 IPTV의 목표 서비스 중 하나인 3-Screen이 지향하는 것으로 기기 변경 시 생기는 지연 시간을 단축시키기 위해 인증 메커니즘에서의 고려도 필요하다. 그러한 점에서 제안



(그림 13) 기기 변경 시 인증 소요 시간 비교



(그림 14) 기기 변경 주기에 따른 인증 누적 시간 비교

메커니즘은 사용자의 인증 과정에서 발급된 티켓을 홈 네트워크 상에서 재분배하여 다른 기기에서 사용함으로써 다른 기기의 인증 과정에서는 중앙 인증 서버에 다시 접근하지 않을 수 있도록 하였기 때문에 이에 대한 고려를 하지 않은 자바카드 기반이나 OTP 기반의 메커니즘에 비해 인증 소요 시간을 각각 약 0.04초, 0.06초씩 단축 한 결과를 얻었다. 이는 (그림 14)과 같이 기기 변경 주기에 따라 생기는 총 인증 시간을 비교할 때 더욱 큰 차이를 내는 것을 볼 수 있다.

4.5 효율성 분석

본 장은 IPTV 사용자 인증 및 콘텐츠 보호에 관한 기존 연구와의 비교를 통해 제안한 메커니즘의 효율성을 설명한다.

개방형 IPTV 환경에서의 사용자 인증 메커니즘은 모든 사용자가 콘텐츠 제공자가 될 수 있다는 가능성을 고려하여 그에 따른 인증 방법을 제공해야 한다. 제안 메커니즘의 경우 서비스 제공자의 위치에 중앙 인증 서버를 도입하여 각 사용자 간의 사용자 인증을 담당하게 함으로써 기존 메커니즘이 콘텐츠 제공자와 사용자가 서비스 이용 전에 물리적인 방법 혹은 그 외의 안전한 방법으로 공유키를 미리 저장해 두는 것과는 달리 매 세션 안전한 인증 과정을 통해 서로의 공유키를 생성할 수 있도록 하였다. 이는 기존의 메커니즘에서의 콘텐츠 제공자가 모든 사용자에 대해 공유키를 각각 저장해두어야 함에 있어 발생하는 저장 공간의 오버헤드를 줄일 수 있다는 장점을 가지고 있다. 또한 기존 메커니즘이 스마트카드, 자바카드 등 물리적인 방법으로 공유키를 전달하기 때문에 한번 전달된 공유키는 하드웨어를 변경하지 않는 한 변경되지 않는다는 단점이 존재하는 반면, 제안 메커니즘은 매 세션 인증 과정을 통해 새로운 키를 발급 받기 때문에 키를 유추하기 어렵고 공격당하더라도 새로운 키 생성으로 빠르게 복구할 수 있다는 장점이 있다.

개방형 IPTV는 플랫폼을 개방함으로써 기존 단말기 혹은 네트워크 망에 대한 종속에서 탈피하여 사용자 모두가 자유롭게 콘텐츠를 제공하는 것을 목표로 한다. 따라서 기존 메커니즘이 스마트카드, 자바카드 등의 하드웨어에 의존하여 키를 분배한다는 점은 사용자로 하여금 하드웨어에 종

〈표 3〉 효율성 비교

	CAS[7]	자바카드 기반[6]	OTP 기반[5]	제안 메커니즘
사용자 인증 방법	스마트카드를 통한 물리적인 방법으로 키 전달	자바카드 내에 공유키를 저장하여 전달	인증 전 인증 서버, 사용자, 콘텐츠 제공자 사이에 공유키 설립	중앙 인증 서버를 통해 티켓 및 공유키 발급
콘텐츠 제공자의 키 저장 오버헤드	N개 (모든 사용자와의 공유키)	N개 (모든 사용자와의 공유키)	N개 (모든 사용자와의 공유키)	1개 (중앙 인증 서버와의 공유키)
키 변경 주기	변경 불가능	변경 불가능	필요에 따라 변경	매 세션마다 변경
콘텐츠 보호	3단계 키 구조를 통해 콘텐츠 암/복호화	고려하지 않음	생성한 OTP를 이용하여 콘텐츠 암/복호화	메커니즘을 통해 생성한 공유키를 이용하여 2단계 키 구조를 통해 콘텐츠 암/복호화
하드웨어독립성	X	X	O	O
기기 변경 지원 여부	X	X	X	O
추가 H/W 장치	스마트카드, STB	자바카드	필요 없음	필요 없음

속되게 하여 개방형 IPTV에 알맞지 않다. 그러나 제안 메커니즘은 특정 하드웨어가 필요 하지 않기 때문에 사용자 누구나 다른 사용자와의 인증 과정을 거쳐 콘텐츠를 제공하는 것이 가능하다. 또한 이러한 기기에 종속되지 않는다는 장점은 사용자로 하여금 다른 기기와 인증 정보를 공유함으로써 홈 네트워크 내의 다른 기기에서도 서비스를 이어 받을 수 있도록 한다. 이는 차세대 IPTV가 목표로 하는 3-Screen에 부합하며 특히 제안 메커니즘은 티켓 재분배를 통해 인증 과정을 단축시킴으로써 기기 변경에 의해 생길 수 있는 지연 시간을 줄이는 결과를 얻었다.

<표 3>은 제안 메커니즘을 기존 IPTV 콘텐츠 보안 기술인 CAS 및 기존 IPTV 사용자 인증 관련 연구와 다양한 각도에서 비교한 것이다.

4.6 안전성 분석

4.6.1 사용자 인증 (User Authentication)

IPTV 시스템에서 사용자 인증은 서비스를 요청하는 사용자를 식별하고 사용자의 가입 정보에 따라 콘텐츠의 사용 권한을 부여하는 것을 의미한다. 본 논문의 사용자 인증 메커니즘은 각 사용자가 서비스 가입 시 부여 받은 AS와의 개인키(KA)를 통해 본인 스스로를 인증하며 AS는 사용자의 ID를 바탕으로 AS에 저장되어 있는 DB를 검색하여 사용자의 가입 정보를 확인하고 서비스에 대한 접근 권한을 티켓의 형태로 부여한다. 특히 본 메커니즘을 통해 수립되는 사용자와 TGS, 사용자와 콘텐츠 제공자의 공유키를 이용하여 사용자는 자신의 신원을 증명하는 Authenticator를 생성하여 서비스를 요청함과 동시에 본인의 신원을 증명할 수 있다.

4.6.2 접근 제어 (Access Control)

정당하지 않은 사용자는 콘텐츠에 대한 접근 권한을 부여받지 않아야 한다. 본 논문에서 제안하는 메커니즘은 콘텐츠에 대한 사용자의 접근 권한을 티켓의 형태로 부여한다. 정당한 사용자에게만 주어지는 티켓은 사용자와 TGS, 사용자와 콘텐츠 제공자 사이의 공유키를 담고 있으며 각각 AS와 TGS, AS와 콘텐츠 제공자 사이의 공유키로 암호화되어 있어 TGS와 콘텐츠 제공자만이 티켓의 내용을 복호화 하여 확인할 수 있다. 따라서 올바른 사용자는 AS로부터 콘텐츠에 대한 접근 권한으로써 티켓을 부여 받고 이를 근거로 TGS와 콘텐츠 제공자에게 접근할 수 있게된다. 각 티켓은 올바른 사용자의 신원 정보를 담고 있으며 사용자 스스로를 증명하는 Authenticator와 함께 전달되므로 TGS와 콘텐츠 제공자는 사용자에 대한 접근 제어가 가능하다. 또한 Replay Attack을 막기 위해 각 티켓은 Life time 값을 담고 있으며 이를 이용하여 티켓이 Life time에 의해 정해진 시간 이상으로 재사용되는 것을 방지할 수 있다.

4.6.3 콘텐츠 보호 (Contents Protection)

IPTV 시스템에서는 올바른 사용자 인증 후 전달되는 콘텐츠 보호 또한 고려해야 한다. 본 메커니즘은 제안한 인증 메커니즘을 통해 생성되는 사용자와 콘텐츠 제공자 사이의 공유키(KA,B)와 CAS 시스템을 이용하여 콘텐츠 제공자는 전송하는 콘텐츠를 암호화 하여 전달하고 사용자는 생성된 공유키를 통해 전달받은 콘텐츠를 복호화 할 수 있도록 한다. 이를 통하여 콘텐츠 제공자와 키를 생성한 사용자 외에는 콘텐츠 제공자가 전달하는 콘텐츠를 시청할 수 없도록 한다. 특히 본 메커니즘은 기존 3단계 키 관리 시스템을 사용했던 CAS 시스템을 수정, 보완하여 2단계 키 관리 시스템으로 단축시킴으로써 기존 3단계 키 관리 시스템에 의해 발생했던 추가적인 통신 오버헤드 및 계산 오버헤드를 줄임과 동시에 보안 강도도 유지할 수 있도록 하였다. 특히 현재 IPTV의 콘텐츠 보안을 위해 널리 사용되고 있는 CAS를 수정하여 사용함으로써 새로운 시스템 적용 시 발생할 수 있는 비용을 절감할 수 있다는 점에서 의의를 갖는다.

4.6.4 기밀성 (Confidentiality)

IPTV는 IP망의 양방향성을 이용한 다양한 응용 프로그램을 서비스 할 수 있다. 이러한 응용 프로그램은 사용자의 결제 정보 등의 민감한 데이터를 전송하는 경우도 있기 때문에 사용자와 콘텐츠 제공자 사이에 전송되는 데이터에 대한 기밀성을 유지하는 것이 중요하다. 따라서 본 메커니즘에 의해 생성되는 사용자와 콘텐츠 제공자 사이의 공유키(KA,B)는 이 후 사용자와 콘텐츠 제공자 사이에 전송되는 데이터를 암호화하기 위한 키로 사용될 수 있으며 이를 통하여 사용자와 콘텐츠 제공자 사이에 전달되는 데이터에 대한 기밀성을 지킬 수 있다. 또한 이 키는 사용자가 서비스를 요청할 때 마다 새로 TGS에 의해 생성되는 키로써 키의 재생성을 통해 키 유추에 의한 공격에 대해 빠르게 대응할 수 있다는 장점이 있다.

4.6.5 무결성 (Integrity)

사용자가 콘텐츠 제공자에게 서비스를 요청하기 위해 전달하는 티켓은 해당 콘텐츠 제공자만이 알고 있는 키(KB)에 의해 암호화되어 있기 때문에 공격자에 의한 위장(impersonation) 공격이 불가능하다. 또한 사용자 스스로의 신원을 인증하기 위해 생성하는 Authenticator는 TGS에 의해 생성된 해당 세션을 위한 공유키(KA,B)로 암호화되어 있기 때문에 공유키를 알지 못하는 공격자가 임의로 생성하거나 해당 메시지를 수정하는 것은 불가능하다.

5. 결 론

개방형 IPTV는 아직 그 연구가 초기 단계에 있지만 스마트폰의 어플리케이션, 위키피디아, 유튜브 등 개방된 환경에서 일반인의 참여를 통해 큰 창출 효과를 얻은 사례를 생각할 때 개방형 IPTV가 갖는 가능성은 무궁무진 할 것이라 예상할 수 있다. 그러나 개방된 환경에서는 그만큼 보안상의 허점을 가질 수 있는 만큼 효과적으로 적용될 수 있는 안전한 메커니즘의 개발이 필요하다.

본 논문은 개방형 IPTV에서 안전한 콘텐츠 전송을 위해 사용자와 콘텐츠 제공자 사이에 신뢰 관계를 쌓기 위한 사용자 인증 메커니즘을 제안하였으며 제안한 메커니즘을 통해 사용자와 콘텐츠 제공자 사이에 설립된 공유키를 기존 콘텐츠 보호 기술인 CAS에 접목시켜 안전한 콘텐츠 전송이 가능하도록 하였다. 또한 제안한 인증 메커니즘을 통해 생성한 티켓을 안전한 홈 네트워크 내에 재분배함으로써 사용자로 하여금 안전한 홈 네트워크 내에서 기기 변경을 통해 IPTV 서비스를 이어서 시청할 수 있도록 하였다.

제안 메커니즘은 Qualnet 시뮬레이터를 이용하여 IPTV 사용자 인증에 관한 기존 연구와 다양한 상황에서의 인증 소요 시간을 비교함으로써 제안 메커니즘이 개방형 IPTV 환경에서 더욱 빠른 시간에 인증을 완료하는 것을 보였다. 또한 기존 연구와 다양한 시각에서 효율성을 비교 분석하여 제안 메커니즘이 개방형 IPTV 환경에서 기존 연구에 비해 갖는 장점에 대해 보였다. 특히 제안 메커니즘이 IPTV 서비스가 요구하는 여러 보안 요구사항을 만족한다는 것을 증명하였다.

개방형 IPTV는 다양한 기기에 적용 가능한 오픈 플랫폼을 기반으로 한 서비스를 목표로 하고 있기 때문에 기술적으로 적합한 웹 기반의 플랫폼이 특히 주목받고 있다. 이러한 환경에서 이미 웹 보안 서비스로서 충분히 안전성을 검증 받아 온 Kerberos를 개방형 IPTV에 적용하는 것은 효과적이라고 볼 수 있다.

또한 기존 IPTV에서 사용된 스마트카드를 이용한 물리적인 키 분배 방법 대신 Kerberos 인증 메커니즘을 이용한 안전한 키 분배 방법을 사용함으로써 스마트카드를 읽을 수 없는 일반 PC, 모바일 기기 등에서도 CAS를 적용하기 위한 키 분배를 할 수 있다. 이는 기기에 구애 받지 않고 서비스를 하고자 하는 개방형 IPTV의 목적에 알맞다.

향후에는 중앙 인증 서버에 발생할 수 있는 과도한 사용량을 줄이고 다수의 사용자에 대해 제안 메커니즘을 적용할 수 있도록 분산 인증 시스템을 적용시켜 연구를 진행 할 예정이다.

참 고 문 헌

[1] 류원, 엄태원, 이현구, 황승구, “차세대 IPTV 기술개발 동향,” TTA Journal, No.122, 2009.

[2] M. Cedervall, U. Horn, Y. Hu, I. M. Lvars and T. Nasstrom, "Open IPTV Forum - Toward an Open IPTV Standard," Ericsson Review, No.3, 2007.

[3] Open IPTV Forum, “Functional Architecture V2.0,” http://www.openiptvforum.org (Available at 12.13.2010)

[4] S. O. Hwang, "Content and Service Protection for IPTV," IEEE Transactions on Broadcasting, Vol.55, No.2, June, 2009.

[5] 서기택, 김태훈, 김정제, 임종인, 문종섭, “IPTV 시스템에서의 효과적인 콘텐츠 보호를 위한 일회성 암호화 수신제한시스템을 사용한 보안 모델,” 한국정보처리학회논문지, 20권, 4호, 2008년 8월.

[6] J. Moon, J. Park and E. Paik, "JavaCard-based Two-Level User Key Management for IP Conditional Access Systems," IEEE International Conference on Network (ICON), Nov., 2007.

[7] F. K. Tu, C. S. Laih and H. H. Tung, “On Key Distubution Management for Conditional Access System On Pay-TV System,” IEEE Transactions on Consumer Electronics, Vol.45, No.1, Feb., 1999.

[8] B. C. Neuman and T. Ts'o, "Kerberos: an Authentication Service for Computer Networks," IEEE Communication Magazine, Vol.32, No.9, Sep., 2004.

정 지 연

e-mail : jiyeon.jung@lge.com

2009년 이화여자대학교 컴퓨터학과(학사)

2011년 이화여자대학교 컴퓨터공학과(석사)

2011년～현 재 LG Electronics 연구원

관심분야 : 네트워크 보안, IPTV 보안, 정보보안

도 인 실

e-mail : isdoh@ewhain.net

1993년, 1995년 이화여자대학교 전자계산학과(학사, 석사)

1995년～1998년 삼성 SDS

2002년～2007년 이화여자대학교 컴퓨터공학과(박사)

2007년～2008년 서울대학교 박사후연구원

2008년～현 재 이화여자대학교 컴퓨터공학과 연구교수

관심분야 : 네트워크 보안, 무선통신망, 센서네트워크 보안, 홈네트워크 보안

채 기 준

e-mail : kjchae@ewha.ac.kr

1982년 연세대학교 수학과(학사)

1984년 미국 Syracuse University 컴퓨터학과(석사)

1990년 미국 NorthCarolina State University 컴퓨터공학과(박사)

1990년～1992년 미국 해군사관학교 컴퓨터학과 조교수

1992년～현 재 이화여자대학교 컴퓨터공학과 교수

관심분야 : 네트워크 보안, 센서 네트워크, 네트워크 프로토콜 설계 및 성능분석