IPTV 콘텐츠 보호를 위한 멀티캐스트 DRM 기반의 인증 시스템 설계

정회원 김 재 우*, 김 정 재*, 김 현 철**°, 전 문 석*

Design on Authentication System Based Multicast DRM for Protection of IPTV Contents

Jae-Woo Kim*, Jung-Jae Kim*, Hyun-Chul Kim**°, Moon-Seog Jun* ***Regular Members***

요 약

최근 IPTV는 초고속 통신망을 이용하여 가입자에게 정보 서비스, 동영상 콘텐츠 및 방송 등을 제공하는 서비스로 상용화 및 활성화되며 각광을 받고 있다. 현재 IPTV 시스템은 전송되는 콘텐츠 보호 및 인증을 위하여 CAS와 VOD 콘텐츠용 DRM 시스템을 결합하여 사용하고 있으나 시스템이 복잡하고 구축비용이 높다는 단점을 가지고 있다. 이를 개선하기 위하여 멀티캐스트 방식의 DRM 시스템이 대두되었으나 이 역시 악의적인 사용자에 의해 키가 유출될 경우 시청권한이 없는 사용자가 불법적인 방송시청을 할 수 있다는 문제점이 존재한다. 본 논문에서는 멀티캐스트 DRM 시스템에 사용자 인증 기법을 적용함으로써 악의적인 사용자로부터 콘텐츠를 보호할 수 있는 기법을 제안한다.

Key Words : IPTV, Multicast, DRM, Authentication, CAS

ABSTRACT

Lately, IPTV is in the limelight using a broadband information service to provide video content and broadcast services. Current IPTV system is combining CAS and DRM system for VOD contents to protect transmitting contents and authentication, but it has drawbacks such as system's complexity and high construction costs. Muliticast DRM system emerged as a method to improve them, but, in the multicast DRM system, if the key is intercepted by a malicious user, it can be viewed by an unauthorized user of illegal broadcasting which can be a problem. In this paper, we suggest to protect content from a malicious user by applying the techniques using user authentication in the multicast DRM system.

Ⅰ. 서 론

IPTV(Internet Protocol Television)는 초고속 인터넷 망을 통해 정보나 방송 등을 TV로 제공하는 통신과 방송이 융합된 서비스로 디지털 정보 서비스, 동영상 콘텐트, 다양한 개인 맞춤형 서비스 등을 제공하고 있다. IPTV에 의해 제공되는 콘텐츠들은 전송되기 위해서 모두 디지털화되어야 하는데 디지털화 콘텐츠들은 누구나 컴퓨터를 이용하여 쉽고, 빠르게 복사할 수 있으며, 복사된 콘텐츠는 원본과 동일한 품질로 제공되고 확산 속도가 빠르다는 특징을 가지고 있다. 이에 따라 디지털 콘텐츠에 대한 보안과 저작권보호가 중요한 문제로 대두되고 있다. 현재 콘텐츠에 대한 불법 복제 및 배포를 방지하기 위한 기술들에 대하여 연구가 활발하게 진행되고 있으며, 대표적인 보안 기술로 CAS와 DRM이 있다. CAS는 인증된 가입자에게만

* 숭실대학교 컴퓨터학과 (saypeace, argniss, mjun@ssu.ac.kr),
** 한국과학기술정보연구원 정보화전략팀 (dmzpolice@kisti.re.kr) (° : 교신저자)
논문번호 : KICS2009-12-648, 접수일자 : 2009년 12월 30일, 최종논문접수일자 : 2010년 3월 24일

콘텐츠를 전송할 수 있게 해주지만 사용자에게 콘텐츠를 배포 후 그 콘텐츠에 대해 지속적인 보호가 이루어지지 않아 불법 복제 및 불법 유통이 가능하다. 따라서 현재 IPTV 시스템은 이를 보완하기 위하여 VOD 콘텐츠용 DRM 기술을 CAS와 결합하여 사용하고 있다. 그러나 이러한 시스템은 비용이 많이 들고 복잡하며, 하드웨어를 동반해야 한다는 단점을 가지고 있다.

본 논문에서는 CAS를 이용하지 않고 멀티캐스트 DRM 시스템에 사용자 인증 기법을 적용하여 악의적인 사용자로부터 콘텐츠를 보호할 수 있는 시스템을 제안한다. 논문의 구성은 다음과 같다. 2장에서 CAS, DRM 등 IPTV 환경에서 사용되는 관련 기술들에 대하여 알아보고, 3장에서 제안하는 시스템의 구성 및 특성을 설명한다. 4장에서는 제안하는 시스템의 구현 및 기존 인증 기법과 비교 분석을 하고 마지막으로 5장에서 결론을 맺는다.

Ⅱ. 관련연구

2.1 CAS(Conditional Access System)

CAS는 기존의 아날로그 방송 때부터 사용되어 온 시스템으로 유료 방송 서비스에 대한 접근제어를 하는 기본 시스템으로 사용 되었다[4]. CAS는 방송시스템에 가입한 가입자만이 특정 프로그램을 수신할 수 있도록 하는 시스템으로, 유료 방송 사업자의 비즈니스 수익을 보호하는 것이 목적이다. 시스템의 주요 기능은 스크램블링/디스크램블링(scrambling/descrambling), 자격제어(Entitlement Control), 자격관리(Entitlement Management)로 나눌 수 있으며, CAS시스템의 구성도는 그림 1과 같다[6].

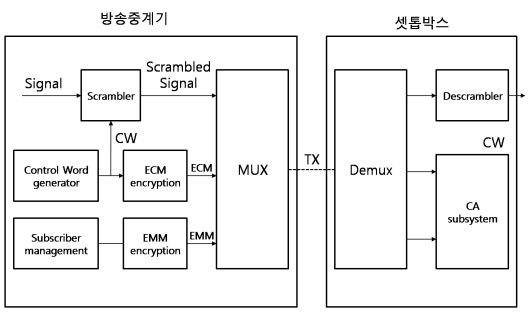

그림 1. CAS 시스템 구성도

2.1.1 스크램블링/디스크램블링

스크램블링은 비인가된 수신자는 시청할 수 없도록 원래의 TV 신호형태를 변형시키는 것으로 TV 프로그램 형태(오디오/비디오/데이터)와 신호형태(아날로그/디지털)에 따라 그 방식이 다르다. 디스크램블링은 디스크램블링 키인 CW(Control Word)를 가질 수 있는 수신기에서만 수행된다. DVB 프로젝트에서, EP-DVB 응용에 적용되는 스크램블링 방식은 장기간 외부 공격의 가능성을 최소화하기 위해서 설계하여 왔다. 따라서, 스크램블링 방식은 고도의 암호 메카니즘으로 구성된다.

2.1.2 자격제어(Entitlement Control)

송신측에서 수신측으로 전송하기 전에 제어단어를 이용하여 인증키를 암호화하고 제어단어는 ECM(Entitlement Control Message)에 포함되어 전송된다. CW는 주기적으로 생성되며 암호화되어 전송된다. 또 ECM에는 제어변수가 포함되어 있으며, 모든 수신기는 전송된 제어변수와 수신기의 인증변수와 비교하여 올바른 사용자일 경우 스마트카드 내의 비밀키로 CW를 복호화하고 수신된 콘텐츠를 디스크램블링 한다.

2.1.3 자격관리(Entitlement Management)

수신기의 자격을 관리하는 기능으로 분배키를 이용하여 인증키를 암호화하고 EMM(Entitlement Management Message)을 생성하며 수신측에 전송한다. 전송된 EMM은 수신측에 있는 스마트카드에 자격을 부여하거나 갱신하는 역할을 한다.

2.2 DRM(Digital Right Management)

DRM은 인터넷 환경에서 디지털 콘텐츠에 대한 생산에서부터 디지털 콘텐츠의 전체 사이클에 걸쳐 지적 재산권을 관리하고 제어하기 위해 사용되는 기술이다. DRM을 이용하면 디지털 콘텐츠의 데이터를 암호화하여 유통하고, 사용자 인증 및 단말기에 대해 라이선스를 발급함으로써 콘텐츠의 불법 복제를 방지할 수 있다[5]. DRM 시스템은 디지털 콘텐츠를 암호화하는 DRM 패키저와 라이선스를 발급 및 관리하는 클리어링 하우스, 발급받은 라이선스를 이용하여 사용하는 DRM 클라이언트로 구성되어 있다. 라이선스는 콘텐츠에 대한 사용권한과 복호화 키를 포함하고 있는데, 사용 권한에 대한 제한 조건과 비교하여 조건에 맞는 경우에만 복호화를 수행할 수 있다. 이러한 전체 과정을 위조 방지(Tamper Resistance)기술을 통해 보호함으로써 해커나 불법 사용자에 의한 콘텐츠불법 유출을 차단할 수 있다[4]. 스트리밍 DRM 시스템은 VOD 콘텐츠용 DRM과 멀티캐스트 콘텐츠용 DRM으로 분류되어지고 두 가지 방식의 차이점은 표 1과 같다.

표 1. 스트리밍 DRM 비교

	VOD 콘텐츠용 DRM	멀티캐스트 콘텐츠용 DRM
암호화	pre-encryption 파일별로 암호화	live encryption 채널별로 암호화
키 전달	키를 라이선스에 넣어 단말기에 전달	스트림에 키를 직접 삽입
키 갱신	리패키징이 필요하므로 어려움	주기적인 업데이트 기능
응용	소규모 사용자 사용	대규모 사용자 사용

2.2.1 VOD 콘텐츠용 DRM

VOD 서비스는 가입자 관리 서버, 스트리밍 서버, 패키저, 라이선스 발급 서버, 콘텐츠 서비스 서버, 클라이언트 서버로 구성된다. 패키저와 라이선스 발급 서버에 의해 콘텐츠를 보호하고 패키저는 콘텐츠 암호화, 콘텐츠 관리 및 라이선스 발급에 필요한 정보를 입력하여 메타 데이터를 생성한다. 또 패키징 된 콘텐츠 및 메타데이터를 VOD 서비스 서버에 전송하는 역할을 한다. 서버 측에서는 패키징 과정을 통해 콘텐츠 및 메타데이터를 콘텐츠에 삽입하고 보호된 형태로 스트리밍이 가능하게 하고, 수신측에서는 언패키징을 통해 콘텐츠를 사용할 수 있게 된다.

2.2.2 멀티캐스트 콘텐츠용 DRM

멀티캐스트 서비스를 위한 DRM 시스템은 가입자 관리 서버, 스트리밍 서버, DRM 멀티캐스터, 키 관리 서버, 콘텐츠 서비스 서버, 클라이언트로 구성되며, DRM 멀티캐스터와 키 관리 서버에 의해 콘텐츠 보호가 이루어진다. DRM 멀티캐스터와 스트리밍 서버로부터 송출된 멀티캐스트 콘텐츠는 키 관리 서버로부터 받은 키로 채널별로 암호화하여 멀티캐스트 서버로 재전송 된다. 클라이언트는 DRM 멀티캐스트 서버에서 암호화 된 방송을 수신하며, 키 관리 서버는 콘텐츠를 암호화 할 키를 생성하고 관리한다. 키 관리 서버는 멀티캐스트 서비스를 위한 DRM 시스템의 핵심 요소로서 멀티캐스트 그룹의 구성원들이 공유할 수 있는 키를 제공하고 관리함으로써 그룹원들이 동일한 데이터를 안전하게 수신하도록 한다[11].

2.3 캐스팅 기술

일반적인 데이터 전송 방식은 브로드캐스트(Broadcast), 멀티캐스트(Multicast), 유니캐스트(Unicast)로 나눠진다. 브로드캐스트는 하나의 송신자가 불특정 다수에게 데이터를 동시에 수신하는 것이고, 멀티캐스트는 하나의 송신자가 어떤 특정된 다수 및 특정 그룹에 대해 데이터를 동시에 수신하는 것이며, 유니캐스트 방식은 하나의 송신자가 특정 한 수신자에게 데이터를 전송하는 방식이다. IPTV에서는 실시간 방송을 위한 효과적인 전송과 네트워크의 품질 및 대역폭을 확보하기 위해 멀티캐스트 기술, 그리고 VoD 서비스 제공을 위한 유니캐스트 기술을 사용한다. 유니캐스트와 멀티캐스트의 데이터 전송 방식을 비교하여 보면 그림 2와 같다.

멀티캐스트는 방송프로그램과 같은 멀티미디어 콘텐츠를 송신하기 위해 고안된 전송 방식으로 네트워크 설비와 서버 증설의 부담을 최소화 해준다. 주로 원격 회의나 채팅 등에 응용되고 있으며, 초고속 인터넷을 적용하면 IPTV에서 수많은 채널을 지원할 수 있게 된다. FTTH(Fiber To The Home)같은 광가입자망이 아니라 xDSL(ADSL 또는 VDSL 등)망에서도 멀티캐스트 기술과 H.264와 같은 동영상 압축기술 등을 이용하면 SD급 화면을 채널당 약 2Mbps 이내로 전송 가능하다. 또한, 멀티캐스트 방식의 IPTV는 동일한 데이터가 일단의 수신자 그룹에 속하는 각 수용자들에게 동시에 전달되기 때문에 송신해야 할 데이터량은 수신자 수와 관계가 없게 된다[3].

그러나 평상시 멀티캐스트는 네트워크 장비까지만 전송하고, 하위에 있는 시청자까지는 전달되지 않게 된다. 따라서 멀티캐스트를 지원하기 위해서는 모든 네트워크 장비는 멀티캐스트를 지원해주는 장비로 구성되어 있어야 한다.

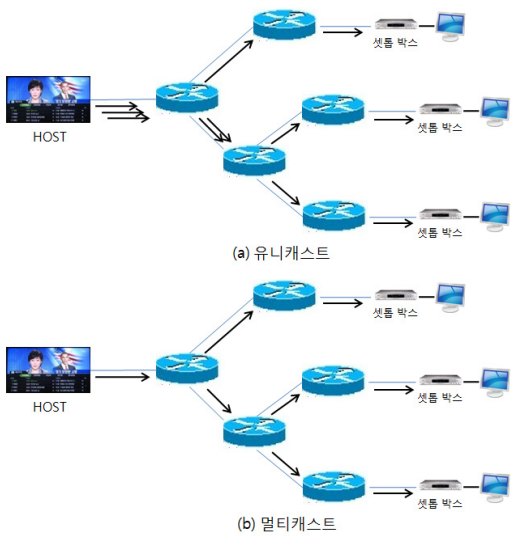

그림 2. 데이터 전송 방식

Ⅲ. 제안하는 시스템

제안하는 시스템은 양방향 통신이 가능하다는 IPTV의 장점을 이용하여 그림 3과 같이 멀티캐스트 DRM 시스템에 상태정보서버를 두고 실시간으로 사용자 정보와 채널 정보를 인증하는 방식을 사용해 시청권한이 없는 사용자의 불법적인 방송시청 문제를 해결하였다.

사용자는 셋톱박스를 이용하여 실시간방송을 보기 위해 콘텐츠 서비스 서버(CSS)에 접속하고 가입자 관리서버(UMS)에서 사용자 권한 검증을 상태정보서버(SIS)에게 요청하고 이상이 없을 시 사용자 정보를 키 관리 서버(KMS)에게 보낸다. 키 관리 서버에서 채널키 추출에 필요한 그룹키를 사용자 공개키로 암호화하여 보내고 콘텐츠 암호화에 필요한 채널키와 그룹키를 DRM 멀티캐스터에 보낸다. 실시간 방송은 스트리밍 서버를 거쳐 스트리밍화 되고 DRM 멀티캐스터를 거쳐 콘텐츠는 암호화되고 멀티캐스팅 된다. 콘텐츠는 DRM 멀티캐스터를 거쳐 그룹키로 암호화된 채널키와 함께 셋톱박스로 보내진다. 셋톱박스에서는 키 관리 서버에서 받은 그룹키를 사용하여 채널키를 얻고 암호화 된 콘텐츠를 복호화하여 안전하게 방송을 시청할 수 있다.

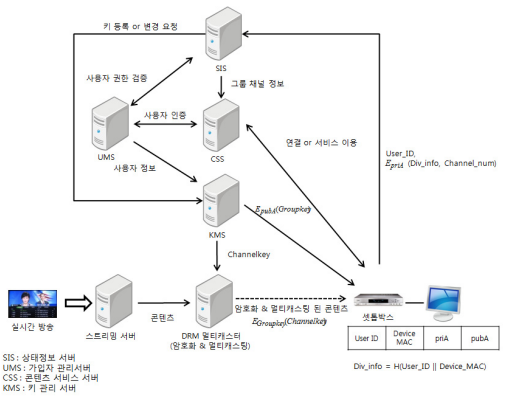

그림 3. 제안하는 시스템 구성도

3.1 상태정보 생성

제안하는 시스템의 상태정보는 미디어 복호화 모듈에서 암호화된 콘텐츠를 복호화하기 위해 채널키가 사용될 때 인증 모듈에서 생성된다. 상태정보 생성과정은 그림 4와 같다. 미디어 복호화 모듈이 DRM 멀티캐스터에서 보낸 암호화와 멀티캐스팅 된 콘텐츠를 받으면 미디어 복호화 모듈에서는 콘텐츠에 삽입된

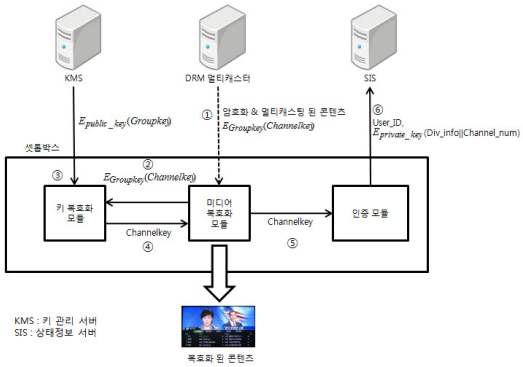

그림 4. 상태정보 생성 과정

$E_{Groupkey}(Channelkey)$를 키 복호화 모듈로 보낸다. 키 복호화 모듈에서는 가지고 있던 그룹키나 키 관리 서버에서 보내온 그룹키를 이용하여 암호화 된 채널키를 복호화하여 채널키를 다시 미디어 복호화 모듈로 보낸다. 채널키를 받은 미디어 복호화 모듈에서 암호화된 콘텐츠를 채널키로 복호화 하면서 인증모듈에 채널키 사용함을 알리면 인증모듈은 상태정보를 생성한다.

인증을 위한 상태정보는 사용자 ID(User_ID), 특정 사용자의 셋톱박스를 한정시키기 위한 정보(Div_info), 채널키를 사용하는 채널 번호(Channel_num)로 구성되어있다. User_ID는 처음 IPTV 서비스에 가입하였을 때 발급받는 ID로서 각 사용자를 식별할 수 있는 정보로서 중복이 없어야 한다. Div_info는 사용자의 특정 장치 ID로 사용자와 셋톱박스를 바인딩하기 위해 생성된 값이다.

Div_info는 User_ID와 셋톱박스 MAC 어드레스의 해쉬값으로 이루어진다. Channel_num은 현재 채널키를 사용하여 복호화하고 있는 채널의 번호로서 사용자가 채널에 대한 사용가능 여부를 판단한다.

상태정보를 상태정보서버로 보낼 때는 User_ID는 평문으로, Div_info와 Channel_num은 사용자의 개인키로 암호화하여 보낸다.

3.2 인증과정

상태정보서버의 주요한 역할은 두 가지로 나뉠 수 있다. 하나는 사용자에 대한 디바이스 인증이고 다른 하나는 사용자에 대한 채널을 시청할 수 있는 권한 인증이다. 상태정보서버는 이 두 가지 인증을 하기 위해 각 그룹별 채널 정보를 유지 및 관리해야 한다. 각 그룹별 채널 정보를 유지함으로써 상태정보서버는 셋톱박스에서 보내오는 현재 채널에 그룹을 알 수 있고 사

용자가 가입한 그룹과 비교하여 채널에 대한 인증을 할 수 있다. 또한 상태정보서버는 각 그룹별 채널 관리를 담당하면서 콘텐츠 서비스 서버에게는 서비스 이용을 위한 각 그룹별 채널정보를 보내고 키 관리 서버에게는 키(채널키, 그룹키) 등록 및 변경을 요청하게 된다.

두 가지 인증에 대한 동작 절차는 그림 5와 같다.

①~③ 셋톱박스는 Div_info와 Channel_num을 전자서명하여 User_ID와 함께 상태정보서버로 보낸다.

④ 상태정보서버는 User_ID를 이용 가입자 관리 서버에게 사용자의 공개키를 받는다.

⑤ 전자서명 된 Div_info를 사용자의 공개키를 이용하여 복호화 한다.

⑥ 상태정보서버는 User_ID를 이용 가입자 관리 서버에게 Div_info ′ 를 받는다.

⑦ 복호화하여 얻은 Div_info와 가입자 관리 서버에 저장되어 있던 Div_info ′ 를 비교하여 사용자에 대한 디바이스에 대해 인증한다.

⑧ 전자서명된 Channel_num를 사용자의 공개키를 이용하여 복호화 한다.

⑨ 상태정보서버는 User_ID를 이용 가입자 관리 서버에게 사용자가 가입한 Group ′ 를 받는다.

⑩ 복호화하여 얻은 Channel_num이 속한 Group을 구한다.

⑪ Group과 가입자 관리 서버에 저장되어 있던 사용자가 가입한 Group ′ 비교해 채널에 대해 인증한다.

상태 정보 서버는 각 인증 과정에 실패를 하게 되면 키 관리 서버에게 키(채널키, 그룹키) 변경 요청을 하게 된다.

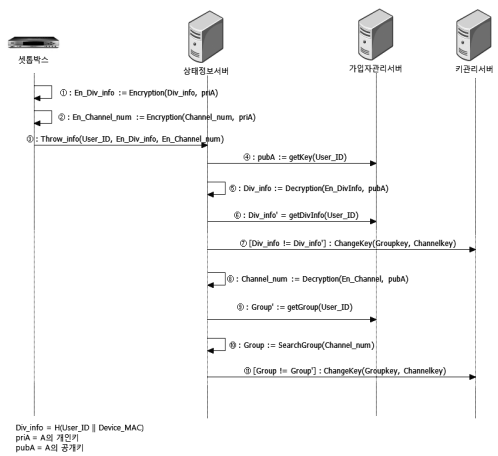

그림 5. 인증에 대한 동작 절차

Ⅳ. 시스템 구현 및 분석

4.1 시스템 구현

구현한 시스템은 크게 서버와 클라이언트로 구성된다. 간략한 구현을 위해 서버부분은 송출부와 상태관리 부분으로 구현하였고 실시간 방송을 대신하여 실시간 웹캠을 사용하였다. 모든 구현은 Windows XP 운영체제 상에서 C#을 사용하여 구현하였다. 시스템에서 전송되는 패킷의 암·복호화는 AES와 RSA 알고리즘을 사용하였으며, 해쉬연산은 SHA-512를 사용하여 구현하였다.

제안하는 시스템의 서버 송출부 화면은 그림 6과 같이 구현하였다. DRM 서버는 채널키를 사용하여 암호화되고 멀티캐스팅 된 웹캠 이미지와 그룹키로 암호화된 채널키를 송신한다.

그림 7은 클라이언트에서 서버에 접속하고 암호화된 컨텐츠를 복호화 과정을 나타낸다. 클라이언트는 먼저 그룹키를 입력하여 서버로부터 받은 그룹키로 암호화된 채널키를 복호화하고 복호화하여 얻은 채널키를 이용하여 암호화된 컨텐츠를 복호화한다. 클라이언트는 채널키를 사용하여 복호화할 때 사용자 식별 ID(User_ID), Div_info, 채널번호(Channel_num)로 이루어진 상태정보를 생성하여 서버로 전송한다. Div_info는 User_ID와 MAX 어드레스의 해쉬값으로 이루어진다.

클라이언트로부터 수신한 상태정보를 관리 및 인증하는 상태관리부는 그림 8과 같다. DRM 서버는 클라이언트로 User_ID와 클라이언트의 개인키로 암호화

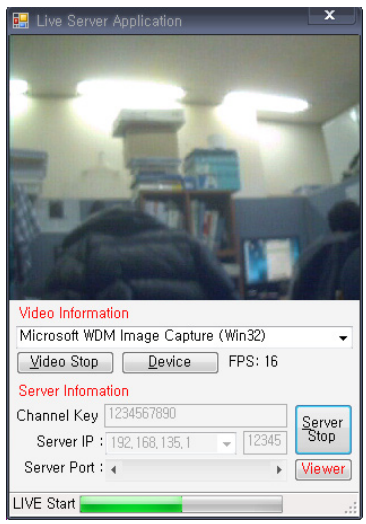

그림 6. 서버 송출부

된 상태정보를 수신하여 상태정보에 들어있는 Div_info와 채널번호(Channel_num)를 이용 디바이스 인증과 채널 인증과정을 거쳐 정당한 사용자인지 확인한다. 만약 불법적인 사용자일 경우 그림 9와 같이 채널키와 그룹키를 변경하게 된다.

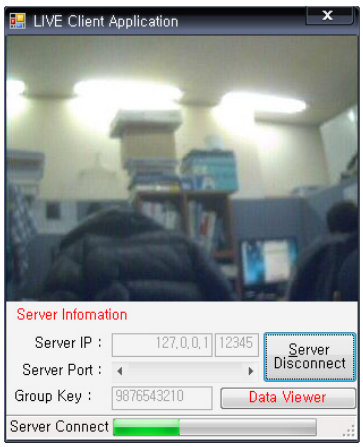

그림 7. 클라이언트

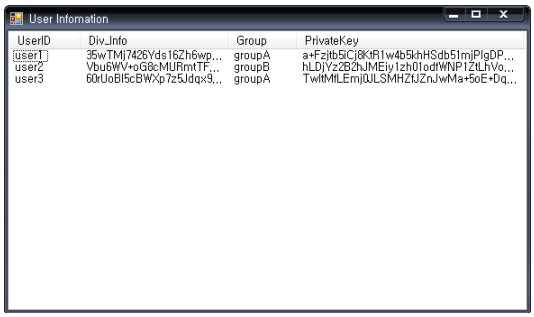

그림 8. DRM 서버 상태관리부

그림 9. 채널키, 그룹키 변경

4.2 시스템 분석

기존의 콘텐츠 보호 및 인증 시스템은 CAS와 VOD 콘텐츠용 DRM 두 가지 기술을 결합하여 각각이 가진 단점을 보안하는 방법을 사용하여 왔다. 기존의 시스템과 제안하는 시스템을 비교하여 보면 표 2와 같다.

표 2. 기존 시스템과의 비교

	CAS	VOD 콘텐츠용 DRM	제안하는 시스템
콘텐츠복제	가능	불가능	불가능
실시간방송	지원	미지원	지원
전송방식	단방향	양방향	양방향
키 전달	키스트림에 키 삽입	키+라이선스	스트림에 키 삽입
키 갱신	주기적 업데이트	리패키징	주기적 업데이트
비용	높음	낮음	낮음

제안하는 시스템에서 사용자에게 전송되는 콘텐츠는 채널키 및 그룹키로 암호화되어 전송되기 때문에 콘텐츠복제가 불가능하며, 멀티캐스트 DRM 방식을 사용하기 때문에 실시간 방송을 지원한다. 또한 사용자 정보와 채널정보를 인증할 수 있도록 양방향 전송 방식을 지원하도록 시스템을 설계하였으며, 키 전달 및 갱신은 스트림에 키를 삽입하여 주기적으로 업데이트 할 수 있도록 설계하였다. 비용적인 측면에서도 CAS를 이용하여 시스템을 구축할 경우 고가의 하드웨어를 사용하여야 하기 때문에 구축비용이 높은 반면에 제안하는 시스템은 구현하여 실측해 본 결과 기존 시스템에 비하여 매우 낮은 비용으로 구축이 가능하다.

제안하는 시스템에서는 기존의 CAS 시스템이 가지는 다운로드 된 콘텐츠에 대하여 지속적인 보호가 어렵다는 문제와 VOD 콘텐츠용 DRM의 단점인 실시간 방송에 적합하기 않다는 문제를 해결하였다. 또한 기존 시스템은 두 가지 기술을 접속하여 시스템을 구성하기 때문에 두 기술 간의 호환성을 고려하여야 하지만 제안하는 시스템에서는 고려할 필요가 없다.

V. 결 론

최근 초고속 인터넷 망을 통해 정보나 방송 등을 TV로 제공하는 할 수 있는 IPTV 서비스가 상용화및 활성화되어 각광을 받고 있다. 그러나 콘텐츠의 디지털화로 인해 콘텐츠 보호 및 인증에 관한 많은 문제가 발생하였다. 이러한 문제를 해결하기 위하여 CAS와 VOD 콘텐츠용 DRM 기술을 결합한 시스템이 고안되었지만 시스템이 복잡해지고 비용이 많이 든다는 단점이 존재한다.

또한 기존의 멀티캐스트 DRM 시스템은 단방향 방송에 적합한 구조를 바탕으로 도입된 CAS의 문제를 해결 할 수 있지만, 키 유출시 불법적인 방송시청을 막을 수가 없다는 문제점을 가지고 있다.

본 논문에서는 멀티캐스트 DRM 시스템에 인증기법을 적용함으로써 기존 시스템의 모든 기능을 사용하면서도 저비용의 구축할 수 있는 시스템을 제안하였다. 제안한 시스템은 양방향 통신이 가능하다는 IPTV의 장점을 이용하여 상태정보서버를 두고 두 가지 요소 인증을 통해 콘텐츠의 보호 및 인증을 모두 처리할 수 있도록 설계되었다.

향후, 본 시스템은 키 변경 과정에서 키 관리 서버와 셋톱박스 사이의 동기화 및 채널 zapping 등에 대해서도 고려하여 연구 되어져야 할 것이다.

참 고 문 헌

〔1〕 박지현, 정연정, 윤기송, “DRM 기술 동향”, 전자통신동향분석, 제22권 제4호, pp.118-132, 2007. 8

〔2〕 이선영, “IPTV를 위한 콘텐츠보호 기술”, 한국 인터넷 정보학회, 제8권 제1호, pp.29-35, 2007. 3

〔3〕 이해창, 김덕넌, 김한수, “IPTV의 활용기술과 기술의 진화방향 분석”, 한국 인터넷 정보학회, 제8권 제3호, pp.38-48, 2007. 9

〔4〕 Ahmet M. Eskicioglu, ″Protecting Intellectual Property in Digital Mulltimedia Networs″, IEEE Computer, Vol.36, pp.39-45, July, 2003

〔5〕 B. Rosenblatt, B. Tripple, And S. Mooney, Digital Rights Management - Business and Technology, M&T Books, 2002

〔6〕 EBU, Functional Model of a Conditional Access system, EBU Project Group B/CA, October, 1995

〔7〕 W. Kanjanarin and T. Amornraksa, “Scrambling and key distribution scheme for digital television”. IEEE International Conference on Networks, pp.140-145 Oct. 2001

〔8〕 Baofeng Liu, Wenjun Zhang, Tianpu jiang, “A scalable key distribution scheme for conditional access system in digital pay-TV system” Consumer Electonics, IEEE Transactions on, Vol.20, No.2, pp.632-637, May, 2007

〔9〕 Shigue Lian, “Digital Rights Managements for the Home TV Based on Scalable Vidio Coding”, IEEE Trans. on Consumer Electronics, Vol.54, 2008

〔10〕 S. Transter, “An Overview of Digital Broadcasting”, NDS Training, 2001

〔11〕 박종열, 문진영, 백의현, “IPTV 융합 서비스를 위한 보안 기술 동향”, 전자통신동향분석, 제 23권, 제5호, pp.40-48, 2008. 10

〔12〕 이선영, “CAS와 DRM을 중심으로 한 모바일 IPTV 보안 기술”, 정보보호학회지, 제19권 제5호, pp.73-80, 2009. 10

〔13〕 윤장우, 이현우, 류 원, 김봉태, “IPTV 서비스 및 기술 진화 방향”, 한국통신학회지(정보와 통신), 제25권 제8호, pp.3-11, 2008. 7

〔14〕 박종봉, “IPTV 서비스, 국내외 현황과 향후 발전 모습”, TTA Journal, No. 122, pp. 62-67, 2009. 4

김 재 우 (Jae-Woo Kim) 정회원

2007년 2월 서울산업대학교 컴퓨터공학과

2009년 2월 숭실대학교 컴퓨터학과 석사

2009년 3월~현재 숭실대학교 컴퓨터학과 박사과정

<관심분야> 전자문서 보안, DRM, 무선통신 보안

김 정 재 (Jung-Jae Kim) 정회원

1999년 2월 영동대학교 컴퓨터공학과

2001년 2월 숭실대학교 컴퓨터학과 석사

2005년 8월 숭실대학교 컴퓨터학과 공학박사

<관심분야> RFID, DRM, 멀티미디어 보안

김 현 철 (Hyun-Chul Kim) 정회원

2003년 2월 인제대학교 정보컴퓨터학부

2005년 2월 경원대학교 전자계산학과 석사

2009년 8월 숭실대학교 컴퓨터학과 공학박사

2009년 5월~현재 한국과학기술정보연구원 정보화전략팀 선임연구원

<관심분야> 공전소, DRM, 보안 정책 및 전략

전 문 석 (Moon-Seog Jun) 정회원

1981년 2월 숭실대학교 전자계산학과

1986년 2월 University of Maryland 전산학 석사

1989년 2월 University of Maryland 전산학 박사

1989년 9월~1991년 2월 New Mexico State University Physical Science Lab. 책임연구원

1991년 3월~현재 숭실대학교 컴퓨터학과 교수

<관심분야> Network Security, 정보보호, DRM