인증 서버를 통한 IPTV의 VOD 콘텐츠 보호 기법

홍석형○, 김대원, 신용태
숭실대학교 컴퓨터학과
{stonehead○, kdwon2002}@cherry.ssu.ac.kr
shin@comp.ssu.ac.kr

A Study on VOD content protection of IPTV techniques to use Certification Server

Sukhyung Hong○, Daewon Kim, Yongtae Shin
Dept. of Computer, Graduate of school, Soongsil University

요 약

본 논문에서는 IPTV의 VOD 콘텐츠를 보호하기 위하여 DRM 시스템을 제안하고, VOD 콘텐츠를 안전하게 전송하기 위하여 콘텐츠 제공자부터 사용자까지의 키 전송에 대한 키 흐름을 제안한다.

따라서, 키를 안전하게 전송하기 위해서 인증서버를 통해 인증 정보를 이용하여 키를 암호화하여 전송하도록 하였다. 상호인증을 통한 콘텐츠 등록 및 획득을 할 수 있도록 제안하였다.

1. 서 론

최근 기술의 발달로 산업간의 경계가 불명확해지고, 고객의 요구사항 고도화 및 사업자의 시장 확대 등에 의해 산업간의 융합화가 발생하고 있다. 특히 이러한 융합화는 BcN의 발전과 일방적인 방송 수신에서 고객이 원하는 고객 맞춤의 방송 및 양방향 방송 요구, 멀티미디어 콘텐츠의 확산 등을 통해 통신과 방송에서 융합화가 더욱 가속화될 전망이다[1].

IPTV에서 콘텐츠 보호를 위한 DRM 기술을 포함하고 있으며 라이센스 기반의 DRM 기술은 라이센스에 복호화 키를 포함하고 있기 때문에 안전하게 전달한다는 보장이 없다. 따라서 IPTV의 개인 맞춤형 서비스인 멀티미디어 데이터인 VOD 콘텐츠를 보호하기 위한 키 관리 기법을 본 논문에서 제안하고자 한다.

2.1절과 2.2 절에서는 IPTV와 DRM의 개념에 대해 설명하고 2.3절에서는 라이센스 기반의 DRM 시스템의 문제점을 설명한 다음에 3장에서는 IPTV의 VOD 콘텐츠를 보호하기 위한 키 관리 기법을 제안하고 4장에서는 결론을 도출하고 향후 연구를 제시한다.

2. 관련 연구

2.1. IPTV(Internet Protocol Television)

IPTV는 협의로는 IP 기반으로 하고, 광의로는 IP 및 혼합된 전달방식을 기반으로 하는 멀티미디어 서비스이다. 또한 IPTV 서비스는 품질과 보안을 보장하고, 양방향 서비스를 제공할 수 있다. 신뢰도가 보장되는 IP 기반의 광대역 네트워크를 통해 다채널 방송, VOD를 비롯한 다양한 유형의 고품질 멀티미디어 서비스를 제공한다[2].

IPTV 서비스 플랫폼은 크게 헤드엔드와 가입자 장치, 백본 네트워크, 액세스 네트워크의 네 가지 요소로 구성이 되며, 이러한 구조에서 IPTV 서비스를 위한 모든 기능은 가입자 단말과 헤드엔드간에 이루어지는 일종의 클라이언트-서버 모델로서 동작한다.

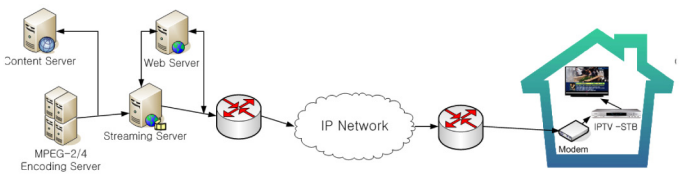

그림 1 IPTV 시스템 구성

IPTV 서비스는 사용자가 원하는 시간에, 원하는 프로그램을, 원하는 장소에서 볼 수 있도록 제어가 가능하다. 또한, IP 망의 다양성으로 인하여 사용자는 멀티미디어 데이터 외에도 영상전화, 메신저, TV 포털,

※ 본 연구는 "서울시 산학연 협력 사업"의 연구비 지원으로 수행되었습니다.
과제번호 : 10581cooperateOrg93111

T-Commerce, T-Banking, 게임 등의 다양한 서비스를 제공받을 수 있을 뿐만 아니라, 개인 방송 등의 공급자가 될 수 있다[3].

2.2. DRM(Digital Right Management)

DRM(Digital Right Management) 기술이란 합법적인 사용 및 사용자로 디지털 콘텐츠의 사용을 한정하고, 디지털 콘텐츠의 사용을 관리하기 위한 기술이다[4].

DRM은 기본적으로 패키징 과정, 유통 과정과 언패키징 과정으로 크게 세 분류로 나눌 수 있다. 패키징 과정은 콘텐츠 제공자가 원본 콘텐츠를 보호하기 위하여 암호화하는 과정이다. 유통 과정은 패키징 된 콘텐츠를 유통 시스템에 의해 콘텐츠를 유통하는 과정을 말한다. 유통 시스템은 사용권리를 포함한 라이센스를 통해 이루어진다. 사용자는 보호된 콘텐츠를 접근하기 위해 유통 시스템을 통해 라이센스를 구매하여 패키징된 콘텐츠를 복호화하여 재생할 수 있다. 즉, 패키징된 콘텐츠를 복호화하는 과정을 언패키징 과정이다[5].

2.3. 라이센스 기반의 DRM 기술의 문제점

라이센스는 DRM 시스템 구조에서 핵심적인 요소이며, 일반적으로 디지털 콘텐츠에 대한 사용 규칙 및 권리를 포함한 허가(grant)를 명확하게 표현하기 위하여 라이센스를 사용한다. 라이센스에는 라이센스 발급자 정보와 허가 정보 등으로 구성되며, 허가 정보는 주체, 자원, 조건, 권리로 구성된다[6].

라이센스를 표현하기 위하여 XrML, ODRL, OMA 등의 권리 표현 언어를 이용하여 허가(grant)를 명확하게 표현한다. 이러한 권리 표현 언어를 이용하는 방식은 불법적인 사용이나 위조를 방지하기 위하여 암호, 전자 서명, 워터마크 등의 보안 기술들로 보호되어야 한다.

VOD 서비스는 콘텐츠별로 암호화하고 복호화 키를 라이센스에 포함하고 있기 때문에, 서명 기술과 암호 기술을 사용을 한다. 하지만 이러한 권리 표현 언어는 XML 형태로 제공되고 있어 라이센스를 신뢰적으로 전달한다는 보장이 없다.

불법적인 콘텐츠 사용을 방지하기 위하여 주체만 제시할 수 있는 패스워드 같은 어떤 비밀을 이용하여 콘텐츠 사용자의 신원 확인 절차를 수행하는 경우, 콘텐츠를 사용할 때마다 신원 확인 절차가 요구하는 비밀을 제공하기 위하여 라이센스 주체의 도움을 받아야 한다. 이러한 경우에는 라이센스에 사용자 정보도 포함되어 있기 때문에 라이센스가 불법적으로 사용될 경우, 사용자의 개인정보도 침해될 우려가 발생한다.

3. IPTV의 VOD 콘텐츠 보호를 위한 키 관리 기법

본 논문에서는 IPTV 환경에서 End-to-End 시스템에서 VOD 콘텐츠를 보호하기 위하여 인증을 통한 콘텐츠 등록 및 라이센스 발급 시스템을 제안한다.

또한, DRM 시스템에서 콘텐츠 등록 과정에서의 키 흐름과 콘텐츠 획득 과정에서의 키 흐름에 대한 키 관리 기법을 제안한다.

3.1. IPTV의 VOD 콘텐츠 보호를 위한 시스템

기존 라이센스 기반 DRM 기술은 라이센스에 콘텐츠를 복호화할 수 있는 키를 포함하고 있어 서명 기술과 암호 기술을 이용하여 라이센스를 사용자에게 전달한다. 이러한 기술은 사용자에게 안전하게 전달한다는 보장을 할 수 없다.

따라서, 인증을 이용한 신뢰할 수 있는 사용자에게 서비스를 제공하는 시스템에서 VOD 콘텐츠를 재생하기 위하여 라이센스에 포함되어 있는 부분키와 콘텐츠 헤더에 포함되어 있는 부분키를 조합하여 복호화 키를 생성하는 방식을 제안한다.

그림 2에서는 제안하는 DRM 시스템 구성을 보여주고 있다. 콘텐츠 제공자와 사용자는 DRM 시스템에서 서비스를 이용하기 위해서는 인증 서버를 통해 먼저 인증이 이루어져야 한다.

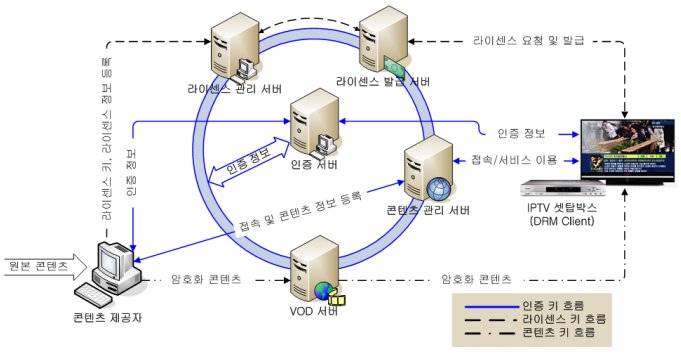

그림 2 IPTV의 VOD 콘텐츠 DRM 시스템 구성

인증 서버는 콘텐츠 제공자나 사용자를 인증하기 위해 사용자 정보를 이용하여 인증키를 생성하고 인증키를 이용하여 사용자를 인증을 수행하고 인증키를 관리한다.

라이센스 관리 서버는 콘텐츠를 복호화 할 수 있는 부

분키인 라이센스 키와 권한 정보를 관리한다. 또한 라이센스 발급 서버로부터 라이센스 발급 요청을 받으면 인증 서버로 통해 사용자 인증이 이루어진 후에 인증 부분키를 이용하여 메시지 인증 코드를 생성하고 공유키를 이용하여 암호화 기능을 수행한다.

라이센스 발급 서버는 라이센스 관리 서버로부터 받은 정보를 이용하여 라이센스를 생성하고 전달한다.

3.2 VOD 콘텐츠 보호를 위한 인증 서버를 통한 인증키 생성 기법

제안하는 DRM 시스템에서의 인증서버는 콘텐츠 제공자나 사용자를 인증하기 위하여 사용자 정보를 이용하여 인증키를 생성한다. 생성된 인증키를 안전하게 전달하기 위해 인증키 부분정보를 전송한다.

콘텐츠 제공자나 사용자가 인증키 부분정보를 수신하면 이를 이용하여 인증키를 생성한다.

인증키와 인증키 부분 정보를 이용하여 DRM 시스템은 콘텐츠 제공자나 사용자를 신뢰적으로 상호인증 할 수 있다.

그림 3은 사용자 정보를 이용하여 인증 서버에서 인증키 부분 정보를 생성하여 사용자에게 안전하게 전달하는 메시지 흐름을 보여준다.

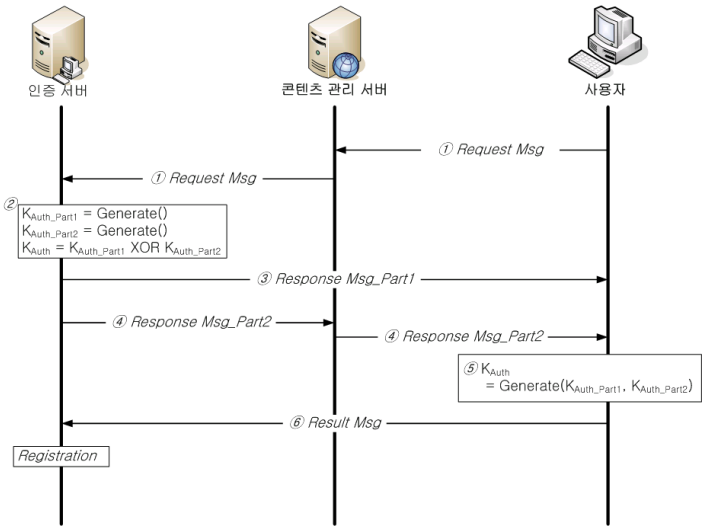

그림 3 인증 키 생성 과정

인증키를 생성하는 과정은 다음과 같다.

① 사용자는 인증키를 생성하기 위한 요청 메시지를 콘텐츠 관리 서버로 전송한다. 요청 메시지에는 ID, 패스워드는 MAC 어드레스 정보를 포함하고, 패스워드와 MAC Address 정보는 공유키(K_S)로 암호화 한다.

$$Request\,Msg = ID \| E(K_S, [Pwd, MACAddress])$$

콘텐츠 관리 서버가 요청 메시지를 수신하면 인증서버로 전달한다.

② 인증 서버가 요청 메시지를 받으면 인증키를 생성한다.

$K_{AuthPart1}$ = *Generate(ID, Pwd, Nonce)*
$K_{AuthPart2}$ = *Generate(MAC Address, Pwd, Nonce)*
K_{Auth} = *Generate*($K_{AuthPart1}$, $K_{AuthPart2}$)

③ 인증키를 안전하게 사용자에게 전달하기 위해서는 사용자가 인증키를 생성할 수 있는 부분키로 제공한다. *Response_Msg1*는 인증 부분키($K_{AuthPart1}$)와 생성된 인증키(K_{Auth})의 해쉬를 포함한다.

$$Msg = E(K_S, [MAC(Pwd, K_{AuthPart1}) \| K_{AuthPart1}])$$
$$Response\_Msg1 = Msg \| h(K_{Auth})$$

④ 또 다른 인증 부분키($K_{AuthPart2}$)를 포함하는 *Response_Msg2*는 콘텐츠 관리 서버를 통해 사용자에게 전달된다.

$$Response\_Msg2 = E(K_S, [MAC(Pwd, K_{AuthPart2}) \| K_{AuthPart2}])$$

⑤ 사용자가 인증키 부분키를 모두 수신하면 인증키(K_{Auth})를 생성한다.

⑥ 사용자가 생성한 인증키를 해쉬 함수를 이용하여 해쉬값을 생성하고 *Response_Msg1*에 포함된 인증키 해쉬값과 비교하여 결과를 인증서버로 전송한다.

DRM 시스템에 접속하여 서비스를 이용하려면 접속 시에 ID와 인증키(K_{Auth})를 포함하는 인증 메시지($Auth_{Msg}$)를 콘텐츠 관리 서버에 전송하고 인증 서버를 통해 인증을 받아야 한다.

$$Auth_{Msg} = ID \| E(K_S, K_{Auth})$$

또한, 콘텐츠 등록 및 콘텐츠 획득하는 과정에서 인증정보로 사용된다.

3.3 VOD 콘텐츠 보호를 위한 키 관리 기법

그림 4는 콘텐츠 제공자로부터 DRM 시스템까지의 VOD 콘텐츠를 등록하는 과정에 대한 메시지 흐름을 나타낸다.

콘텐츠 제공자가 VOD 콘텐츠를 패키저를 통해 패키징하여 DRM 시스템에 패키징된 콘텐츠, 콘텐츠 정보와 권한 정보를 등록을 한다. 등록하는 과정은 다음과 같다.

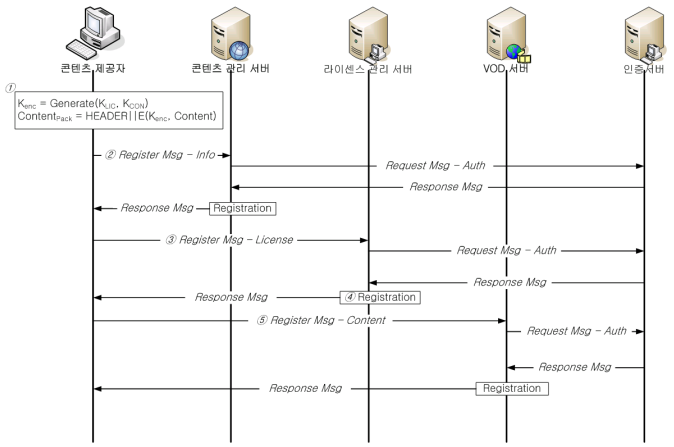

그림 4 VOD 콘텐츠 등록 과정

① 콘텐츠 제공자는 원본 VOD 콘텐츠를 패키저를 이용하여 패키징을 한다. 패키징은 원본 콘텐츠를 암호화 알고리즘을 이용하여 암호화는 과정으로서 암호화하기 위해서는 키가 필요하다.

콘텐츠를 암호화할 수 있는 키를 생성하기 위해 라이센스에 포함되는 라이센스 키(K_{LIC})와 콘텐츠 헤더에 포함되는 콘텐츠 키(K_{CON})를 생성한다. 이 키들을 이용하여 암호화 키(K_{Enc})를 생성한다.

$$K_{LIC} = Generate(ConID,\ ConName,\ Nonce)$$
$$K_{CON} = Generate(ID,\ K_{Auth},\ Nonce)$$
$$K_{ENC} = Generate(K_{LIC},\ K_{CON})$$

암호화키(K_{ENC})가 생성이 되면 콘텐츠를 패키저를 통해 암호화를 수행한다. 콘텐츠 헤더에 포함되는 콘텐츠 키(K_{CON})는 공유키(K_S)를 이용하여 메시지 인증 코드를 생성하고 라이센스 키(K_{LIC})를 이용하여 암호화한다.

$$Header = ConID \| E(K_{LIC}, [MAC(K_S, K_{CON}) \| K_{CON}])$$
$$Content_{PACK} = Header \| E(K_{Enc}, Content)$$

② VOD 콘텐츠가 패키징이 완료되면 콘텐츠 관리 서버로 등록 요청 메시지를 전송한다. 등록 요청 메시지에는 인증 정보($Auth_{Msg}$)와 콘텐츠 정보가 포함된다.

콘텐츠 관리 서버는 등록 요청 메시지를 수신하면 인증 정보($Auth_{Msg}$)를 인증서버로 전달한다. 그리고 인증서버로부터 인증 결과에 따라 콘텐츠 정보를 등록한다.

③ 콘텐츠 정보가 등록이 되면 라이센스 관리 서버에 라이센스 등록 요청 메시지를 전송한다. 등록 요청 메시지는 인증정보($Auth_{Msg}$), 라이센스 키(K_{LIC})와 권한 정보가 포함된다. 콘텐츠 관리 서버가 콘텐츠 제공자로부터 콘텐츠 등록 메시지를 수신하면 등록 요청 메시지에 포함되어 있는 인증 정보를 인증서버로 전송한다.

$$K_{LICENSE} = E(K_S, [MAC(K_{AuthPart2}, K_{LIC}) \| K_{LIC}])$$

④ 라이센스 관리 서버는 인증서버로부터 인증 결과와 함께 인증 부분키($K_{AuthPart2}$)를 수신하면 공유키(K_S)로 복호화하고 인증 부분키($K_{AuthPart2}$)로 메시지를 인증하여 라이센스 키를 등록한다.

$$Auth = D(K_S, K_{AuthPart2})$$
$$K_{LIC} = D(K_S, [MAC(Auth, K_{LIC}) \| K_{LIC}])$$

⑤ 콘텐츠 등록 정보들이 정상적으로 등록이 되면 패키징된 콘텐츠를 VOD 서버에 등록을 수행한다.

위의 과정이 끝나면 사용자는 콘텐츠를 이용할 수 있으며, 사용자가 콘텐츠를 획득하여 사용하기 위해서는 그림 5에서 제안하는 콘텐츠 획득 과정에 따라 이루어진다.

IPTV의 VOD 서비스를 이용하기 위해 사용자는 콘텐츠 관리 서버에 인증정보($Auth_{Msg}$)를 전송한다. 인증 서버를 통해 인증이 이루어진 후에 콘텐츠 관리 서버는 사용자에게 VOD 서비스를 이용할 수 있는 VOD 콘텐츠 정보를 전송한다.

사용자가 VOD 콘텐츠를 선택하면 VOD 서버로부터 선택한 VOD 콘텐츠를 다운로드한다.

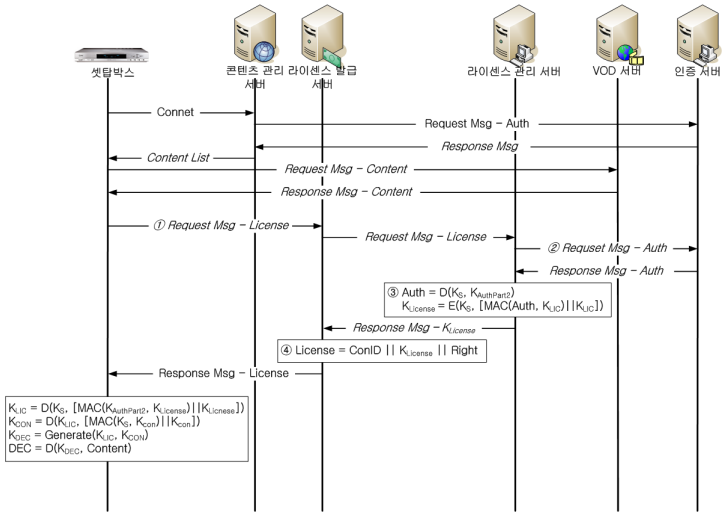

그림 5 콘텐츠 획득 과정

VOD 콘텐츠를 재생하기 위해서는 콘텐츠 헤더에 포함된 복호화 부분 키(K_{CON})와 라이센스에 포함되어 있는 복호화 부분 키(K_{LIC}) 조합으로 복호화 키를 생성해야 한다.

라이센스에는 콘텐츠를 복호화 할 수 있는 부분키(K_{LIC})가 포함되어 있기 때문에 인증을 통한 라이센스 발급이 이루어져야 하고 라이센스 키(K_{LIC})를 인증정보를 이용하여 메시지 인증코드로 작성한 다음에 암호화하여 전송되어야 한다. 라이센스 발급하는 과정은 다음과 같다.

① 사용자는 콘텐츠 ID와 인증 정보가 포함된 라이센스 발급 요청 메시지를 라이센스 발급 서버로 전송한다.

라이센스 발급 서버가 라이센스 발급 요청 메시지를 수신하면 라이센스 관리 서버로 전달한다.

② 라이센스 관리 서버는 인증정보를 인증서버에 전송하여 라이센스의 메시지 인증 코드의 키로 사용할 인증 부분 키($K_{AuthPart2}$)를 함께 인증 결과를 수신한다.

③ 라이센스 관리 서버는 인증서버로 받은 정보를 공유키(K_S)를 이용하여 복호화하여 라이센스 키를 메시지 인증 코드로 생성하고 공유키로 다시 암호화하여 라이센스 발급 서버로 전송한다.

$$K_{License} = E(K_S, [MAC(K_{AuthPart2}, K_{LIC}) \| K_{LIC}])$$

④ 라이센스 발급 서버는 콘텐츠 ID, 라이센스 키, 권한 정보를 이용하여 라이센스를 생성하여 사용자에게 전송한다.

사용자는 라이센스를 획득하면은 라이센스에 포함되어 있는 라이센스 키(K_{LIC})를 복호화하고 콘텐츠 헤더에 있는 콘텐츠 키(K_{CON})를 이용하여 복호화 키를 생성한다.

복호화 키(K_{Dec})를 이용하여 콘텐츠를 복호화하여 재생을 할 수 있다.

4. 결론 및 향후 연구

IPTV의 VOD 콘텐츠를 보호하기 위하여 인증 서버를 이용한 사용자 인증을 할 수 있는 DRM 시스템에서 인증을 위해 인증서버에서 생성된 인증키를 안전하게 사용자에게 전달하기 위한 부분키로 전송을 제안하였다.

또한 콘텐츠를 복호화 할 수 있는 부분키들을 안전하게 전송하기 위하여 공유키를 이용하여 콘텐츠키를 메시지인증코드로 생성하고 라이센스키로 암호화하여 콘텐츠 헤더에 포함시켰고, 라이센스에는 사용자 인증 부분키를 이용하여 라이센스 키를 메시지인증코드로 생성하고 공유키로 암호화하여 포함시켰다.

따라서, VOD 콘텐츠를 보호하기 위하여 복호화 키를 생성하기 위한 부분정보를 콘텐츠 헤더와 라이센스에 나누어 전송함으로써 복호화 키를 안전하게 전송할 수 있고 키들을 안전하게 전송하기 위해 인증서버에서는 인증정보를 이용하여 키를 암호화하여 전송하도록 하였다. 상호 인증을 통한 콘텐츠 등록 및 획득을 할 수 있도록 제안하였다.

향후 논문에서 제안하고 있는 인증서버를 통한 VOD 콘텐츠 보호 기법에 대한 효율성과 VOD 콘텐츠를 안전하게 보호할 수 있도록 구현을 통한 성능평가를 하고자 한다.

참고문헌

[1] 성정식, 이성용, 송호영, 김봉태, "IPTV 서비스 및 표준화 동향“, 전자통신동향분석 제21권 제 3호, 123~136, 2006.6

[2] 이병탁, 오승훈, 심재찬, 송호영, “FTTH 기반 IPTV 서비스 및 기술 동향”, 전자통신동향분석 제 21권 제 6호, 104~112, 2006년 12월

[3] 황성운, 윤기송, “최신 DRM 유통 시스템 현황”, 전자통신동향분석 제20권 제 4호, 2005년 8월

[4] Rob H. Koenen, Jack Lacy, Michael Mackay, Steve Mitchell, "The Long March to Interoperable Digital Rights Management", Proceedings of the IEEE Vol. 92, No. 6, 2004. 6

[5] Yeonjeong Jeong, Kisong Yoon, and Jaecheol Ryou, "A Trusted Key Management Scheme for Digital Rights Management", ETRI Journal, Volume 27, Number 1, 2005.2

[6] 장혜진, “DRM 기술로 보호된 컨텐츠의 융통성 있는 공유를 위한 멤버/그룹 라이센스 메커니즘”, 정보처리학회 논문지 C 제 11-C권 제 6호, 2004. 12