최신 DRM 유통 시스템 현황

An Introduction of Recent DRM Systems for Content Distribution

유비쿼터스 시대를 주도할
디지털콘텐츠 기술 특집

황성운 (S.W. Hwang) 콘텐츠유통연구팀 선임연구원
윤기송 (K.S. Yoon) 콘텐츠유통연구팀 팀장

목 차

Ⅰ. 서론
Ⅱ. End-to-End DRM 시스템
Ⅲ. 셋톱박스용 DRM 시스템
Ⅳ. 결론

인터넷의 보급과 더불어 디지털 콘텐츠도 다양한 경로를 통해 보급 및 사용되고 있다. 그러나 디지털 콘텐츠는 속성상 아날로그 콘텐츠와 달리 쉽고, 빠르게 복사할 수 있으며 복제품은 원본에 비해 질적인 저하가 없으며 더 나아가 사용자들의 무료 선호 인식과 더불어 콘텐츠의 불법 복제 및 비정상적인 유통 문제를 야기시키고 있다. DRM은 이러한 디지털 콘텐츠에 대한 불법 복제 및 불법 유통을 방지 또는 억제하기 위한 기술이라고 할 수 있다. 본 논문에서는 두 가지 DRM 유통 시스템을 소개함으로써 최신 DRM 기술 개발 현황을 살펴보고자 한다. 첫번째로 소개되는 End-to-end DRM 시스템은 기존의 유통업자와 소비자 사이에서 콘텐츠가 보호되던 것을 창조자부터 시작하여 최종 소비자까지로 범위를 확대시켰다. 보호 영역의 확대는 보다 더 다양한 콘텐츠 유통 모델을 지원하는 효과를 가져 온다. 두번째로는 인터넷에 연결된 셋톱박스를 이용한 스트리밍 서비스 환경에서 어떻게 DRM이 적용되는지를 살펴보고자 한다.

Ⅰ. 서론

DRM은 인터넷의 보급과 그에 따라 디지털 콘텐츠가 활발히 보급, 사용되면서 나온 새로운 개념이라고 할 수 있다. 디지털 콘텐츠는 아날로그 콘텐츠와 달리 컴퓨터를 이용하여 쉽고, 빠르게 복사할 수 있으며 복제품은 원본에 비해 질적인 저하가 없고 확산 속도가 빠른 속성을 가지고 있다. 이것은 초기 인터넷 상에서 콘텐츠는 무료라는 사용자들의 인식과 더불어 콘텐츠의 불법 복제 및 비정상적인 유통 문제를 야기하고 있다. DRM은 이러한 디지털 콘텐츠에 대한 불법 복제 및 불법 유통을 방지 또는 억제함으로써 디지털 콘텐츠에 연관된 콘텐츠 제작자 또는 저작권자의 권리를 보호하기 위해 등장한 기술이라고 할 수 있다.

DRM은 기본적으로 콘텐츠 원본을 보호된 콘텐츠로 만드는 과정(패키징 모델), 콘텐츠 제공업자가 보호된 콘텐츠를 유통시키는 과정(콘텐츠 유통 모델), 소비자가 보호된 콘텐츠에 접근하고 사용권리를 구매하는 과정(라이선싱 모델), 소비자가 디바이스를 이용하여 보호된 콘텐츠를 소비하는 과정(언패키징 모델)으로 세분화 할 수 있다. 패키징 모델에서는 주로 콘텐츠를 보호하기 위한 메커니즘으로 암호화를 사용하며 이때 콘텐츠를 사용하는 규칙을 명시한다. 이 사용규칙은 보통 최종 소비자 단에서 사용될 규칙을 명시하나 중간 유통 과정을 위한 유통 규칙을 포함할 수도 있다. 패키징 과정을 거쳐 나온 보호된 콘텐츠는 콘텐츠 제공업자 또는 서비스 제공업자가 의도한 유통 모델에 따라 제공되거나 서비스된다. 즉 보호된 콘텐츠는 유통 모델에 따라 다양한 value-chain을 따라 유통되어 중간 유통업자 또는 최종 소비자에게 전달된다. 전달된 보호 콘텐츠를 사용하기 위해서는 중간 유통업자 또는 최종 소비자는 미리 설정된 라이선싱 모델에 따라 라이선스 발급 기관에 돈을 지불하고 콘텐츠를 사용할 수 있는 권리를 얻게 된다. 보통 그 권리를 라이선스라 하며 라이선스는 보호된 콘텐츠에 대한 다양한 접근 권리 및 복호화 키 등의 정보를 포함한다. 최종적으로 소비자는 자신의 컴퓨팅 환경에서 보호된 콘텐츠 및 이에 대한 라이선스를 얻게 된다. 소비자가 구체적으로 콘텐츠를 실행하는 시점에서 언패키징 과정이 발생하며 이를 통해 소비자의 요청이 구매한 라이선스에 포함된 사용 규칙 범위 내에서 허가된다.

위에 기술한 다양한 모델들은 각각 패키저, 유통서버, 클리어링 하우스, DRM 클라이언트 등으로 구현되어 콘텐츠 유통 및 소비 과정에서 사용하게 된다.

DRM 기술은 분류 기준이 명확히 있는 것은 아니지만 설명의 편의상 콘텐츠가 유통되는 환경에 따라 다음과 같이 분류할 수 있다.

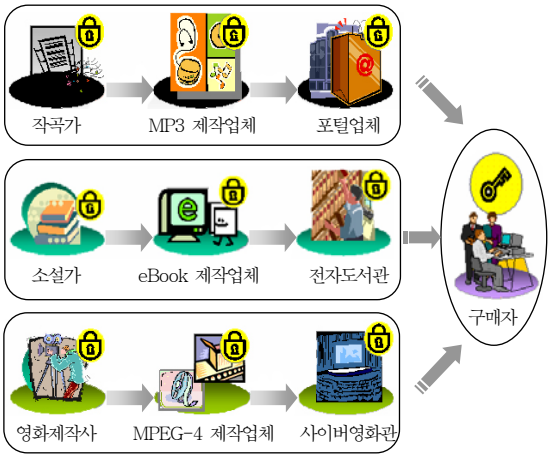
- 인터넷 DRM – 인터넷을 통하여 콘텐츠 유통이 이루어지고 주로 PC를 통하여 소비되는 형태
- 셋톱박스 DRM – 인터넷, 케이블 또는 위성망을 통하여 콘텐츠가 전달되고 TV에 연결된 셋톱박스를 통하여 소비되는 형태
- 무선 DRM – 무선망을 통하여 콘텐츠가 전달되고 단말기(폰, PDA 등)를 통해 소비되는 형태

본 논문에서는 인터넷 DRM과 셋톱박스 DRM을 중심으로 현재 ETRI에서 개발된 DRM 시스템들을 소개하고자 한다.

Ⅱ. End-to-End DRM 시스템

1. 개발 배경

End-to-end DRM 시스템은 콘텐츠에 대해 최초로 패키징을 한 유통업체로부터 다양한 중간 유통업체(신디케이터, 배급자)에 의해 재패키징 되고 유통되는 과정을 반복하여 최종 소비자에 이르기까지의 모든 유통 단계에서 콘텐츠의 원본과 저작권을 보호할 수 있는 DRM 시스템이다. 이것은 현재 실물 유통 비즈니스 모델과 마찬가지로, 디지털 콘텐츠가 도매업자, 소매업자를 비롯한 여러 가지 유통 경로를 통해 유통될 수 있도록 지원하기 위해 나온 시스템이다. 이를 위해 유통 각 단계마다 서로 다른 유통



(그림 1) End-to-End DRM 시스템 개념도

정책 및 사용 범위를 적용할 수 있으면서, 서로 다른 이해 관계인 유통 주체의 권리를 보호할 수 있는 기술 개발이 필요하다. (그림 1)은 End-to-end DRM 시스템 개념도를 나타낸 것이다. 콘텐츠가 여러 단계의 유통 업자를 거치면서 사용 권리가 변경되거나 새로운 형태의 콘텐츠로 합쳐지는 과정을 나타내고 있다.

2. 요구사항 분석

DRM이 적용된 콘텐츠는 패키징 과정에서 미리 설정된 사용 규칙 및 소비자가 구매한 권한에 따라 적절하게 사용되어야 한다. 다음은 End-to-end DRM 시스템이 만족해야 할 주요 요구사항을 나열한 것이다.

- 다단계 패키징 – 상위 단계에서 허용된 유통 규칙 및 사용 규칙의 범위 내에서 콘텐츠의 보호 메커니즘이 적용되어야 한다.
- 다단계 라이선싱 – 상위 단계에서 허용된 유통 규칙 및 사용 규칙의 범위 내에서 콘텐츠에 대한 사용 요청이 허가되어야 한다.
- 복합 콘텐츠 지원 – 기존의 여러 유통업체가 만든 다양한 사용 규칙과 유통 규칙이 적용된 패키징된 콘텐츠들로부터 새로운 콘텐츠를 재구성할 수 있어야 한다.

3. 시스템 구성

End-to-end DRM 시스템은 인터넷 기반의 PC 환경을 대상으로 개발되었다. 세부적으로 End-to-end DRM 시스템은 패키저, 유통 서버, 라이선스 서버, DRM 클라이언트로 구성된다.

패키저는 원본 콘텐츠를 패키징하여 보호된 콘텐츠를 생성하거나 보호된 콘텐츠를 재패키징하여 새로운 보호된 콘텐츠를 생성한다. 또한 보호된 콘텐츠를 생성하면서 함께 생성된 암호화키와 메타데이터를 라이선스 서버와 유통 서버에 제공한다. 패키저는 세부적으로 콘텐츠를 등록하는 부분(콘텐츠, 라이선스, 키정보, 메타데이터 등록/삭제/갱신), 패키징을 담당하는 부분(패키징, 라이선스 정보 등록), 콘텐츠 정보를 관리하는 부분(보호된 콘텐츠 리스트 관리 및 갱신)으로 나뉘어진다.

패키저에 의해 생성 보호된 콘텐츠는 보통 secure container라고 불리는 파일 구조체 형태로 콘텐츠 유통 체인을 거쳐 최종 소비자에게 전달된다. Secure container는 배포될 콘텐츠의 다양한 메타데이터를 표현하기 위해 MPEG-21 DID[1] 규격을 따른다. MPEG-21 DID는 콘텐츠의 유통을 위해 필요한 식별자, 유통업체, 그리고 콘텐츠의 메타데이터들이 체계적으로 기술될 수 있는 표현 언어를 제공하고 있다. (그림 2)는 secure container의 구조를 나타낸다. Secure container는 크게 헤더, DIDL block, resource block으로 구성된다. 헤더는 컨테이너 식별정보, 포맷 버전, DIDL과 리소스에 대한 위치정보를 포함한다. DIDL block은 유통되는 콘텐츠의 메타데이터 정보를 포함하며, MPEG-21 DIDL 규격을 이용하여 기술한다. Resource block은 원본 콘텐츠(리소스)가 암호화되어 저장되는 부분으로, 복수 개의 리소스가 저장될 수 있다. 각각의 리소스 위치 정보는 DIDL 내의 RP에 의해서 명시적으로 기술된다.

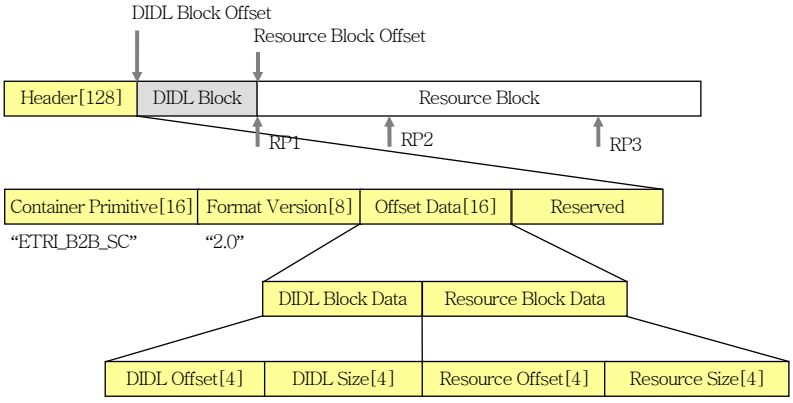
라이선스 서버는 패키저로부터 보호된 콘텐츠에 대한 라이선스 발급에 필요한 정보를 등록 받고 이들 데이터를 관리하며 구매자(유통업자 또는 최종

소비자)에게 라이선스를 발급한다. 또한 라이선스 발급 시 이전 유통단계에서 설정한 라이선스 발급 범위 내에서 라이선스가 발급될 수 있도록 한다. 이를 위해서는 패키저로부터 전달된 정보의 전자서명 확인, 라이선스를 파싱해서 권한 정보 추출 및 관리, 라이선스 발행에 필요한 정보 갱신, 라이선스 갱신(기 발행된 라이선스의 권한 및 조건을 추가, 삭제, 변경) 등의 기능을 수행한다.

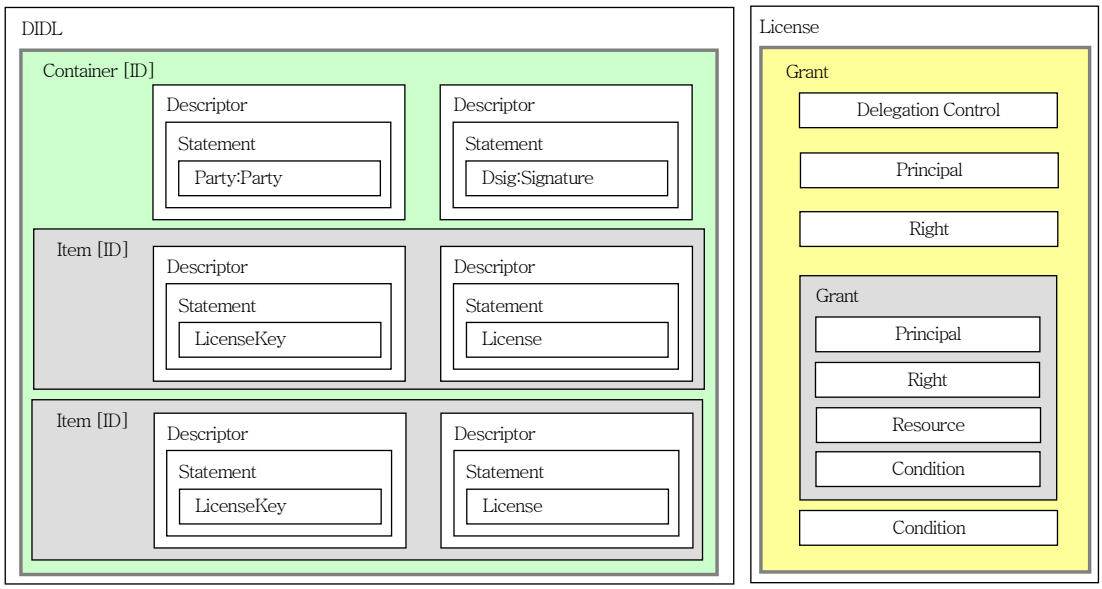
라이선스 서버에 의해 생성된 라이선스는 유통 과정에서 사용 권한을 통제하기 위하여 사용되고 MPEG-21 Part5의 REL[2]를 이용하여 표현되며, secure container처럼 MPEG-21 DIDL을 전송 컨테이너로 사용한다. (그림 3)은 라이선스의 구조를 나타낸다.

유통 서버는 구매자에게 판매 조건과 보호된 콘텐츠를 제공하며 구매자에게 라이선스를 발급하도록 요청한다.

DRM 클라이언트는 라이선스 서버로부터 발급된 라이선스에 포함된 사용권한 및 조건에 따라 구매자가 콘텐츠를 이용할 수 있도록 한다. 즉, DRM 클라이언트는 일반 구매자측 PC에 설치되어 권한에 따라 콘텐츠가 올바르게 사용될 수 있도록 제어하는 프로그램이다. DRM 클라이언트의 주요 기능은 라이선스 관리, SC 처리, 메타데이터 분석, 복호화, 외부 애플리케이션 제어, DRM 관련 데이터의 안전한 관리 등이다. DRM 클라이언트는 DRM 제어부, secure DB, 플러그인 등으로 구성된다.



(그림 2) Secure Container 구조



(그림 3) 라이선스 구조

〈표 1〉 운영 플랫폼 및 지원 미디어

운영 플랫폼		지원 미디어	
패키저	Linux, Windows	오디오	MP3, WMA
유통서버	Linux, Windows	비디오	MPG, AVI, WMV
라이선스 서버	Linux, Windows	문서	HWP, DOC, PDF
클라이언트	Windows	복합 콘텐츠	MPEG-21 DIDL 기반 복합 콘텐츠

DRM 제어부는 외부 시스템과의 통신, SC 처리, 플러그인 제어, secure DB 접근 등의 기능을 한다. Secure DB는 라이선스, 사용 이력, 클라이언트 공개키쌍 등 사용자에 의해 임의로 변경되어서는 안되는 정보를 안전하게 저장 관리하는 기능을 한다. 플러그인은 외부 애플리케이션에 삽입되어 복호화된 데이터를 제공하고 외부 애플리케이션의 동작을 제어하는 기능을 한다.

<표 1>은 End-to-end DRM 시스템의 개발 환경 및 지원 미디어를 나타낸다.

4. 기존 방식과의 차별점

<표 2>는 기존 DRM 시스템과 End-to-end DRM 시스템의 특성을 비교한 것이다. 주요 특징으로 다단계 패키징 및 라이선싱 개념을 도입함으로써 비즈니스 모델 지원 범위 및 콘텐츠 보호 범위를 기존의 배포자와 구매자 구간에서 콘텐츠 유통 전 구간으로 확대했다는 점이다. 본 시스템은 사용규칙 및 메타데이터 등 요소 기술에서 국제 표준을 준수하고 있다. 특히 복합 패키징을 지원함으로써 여러 콘텐츠의 복합화 과정에서 발생할 수 있는 각 저작권자의 권리 침해를 방지하면서 콘텐츠 유통을 지원하는 점이 큰 특징이다. 또한 본 시스템의 DRM 클라이언트는 뷰어에 독립적인 플러그인 아키텍처를 사용함으로써 다양한 뷰어에 DRM을 손쉽게 적용할 수 있다.

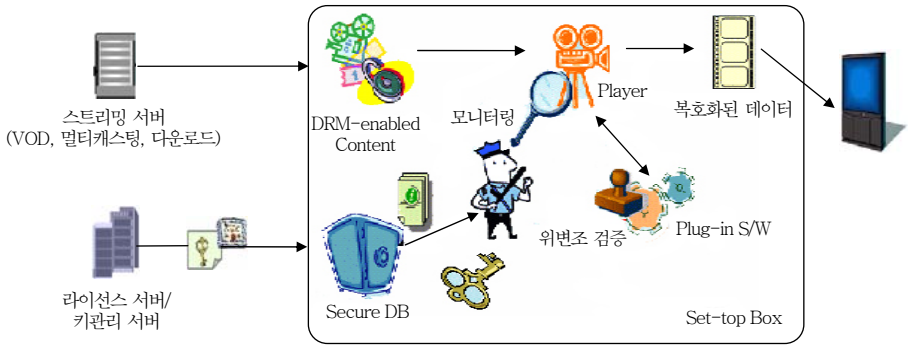
〈표 2〉 기존 시스템과 End-to-End ERM 시스템의 비교

	기존 시스템	End-to-end DRM 시스템
비즈니스 모델 지원 범위	• 배포자~구매자 범위 지원	• 창조자~구매자 범위 지원
End-to-end 콘텐츠 보호	• 지원 못함	• 지원
사용 규칙	• XrML[3] • ODRL[4]	• MPEG-21 REL
메타데이터	• 임의 방식	• MPEG-21 DID
콘텐츠 패키징	• 단일 패키징	• 복합 패키징
뷰어 및 플레이어	• 특정 뷰어에 종속	• 뷰어 독립

Ⅲ. 셋톱박스용 DRM 시스템

1. 개발 배경

기존의 동영상 콘텐츠에 대한 DRM 시스템은 대부분 콘텐츠를 암호화하여 사용자 시스템에 콘텐츠 전체를 다운로드 하여 콘텐츠를 재생할 때 메모리상에서 특정 크기의 블록만큼씩 복호화하여 이 복호화된 콘텐츠가 재생되는 형태이다(이를 다운로드 서비스라 칭한다). 그러나 영화와 같은 동영상 콘텐츠의 경우, 대부분 대용량이기 때문에 다운로드 방식은 비효율적이다. 따라서, 대용량 동영상 콘텐츠의 경우 다운로드에 많은 시간이 소요되므로, 주문형 비디오(VOD)와 같은 방식으로 스트리밍을 통하여 서비스를 하는 것이 보편적이다. 하지만, 근래 스트리밍을 통하여 서비스되는 동영상을 저장할 수 있는 프로그램이 속속 등장하면서 스트리밍을 통하여 서비스되는 동영상에 대한 보호 방안이 필요하게 되었다. 가장 통상적인 유형의 스트리밍 방식은 유니캐스트(unicast) 통신이다. 유니캐스트 방식에서는 하나의 송신자가 다수의 수신자들에게 데이터를 전송하기 위해서는 각각의 수신자들에게 동일한 데이터를 반복적으로 보내야 하기 때문에 송신자 노드의 자원과 네트워크 대역폭의 낭비를 초래한다. 이러한 문제점을 해결하기 위해 등장한 기술이 IP 멀티캐스트이다. 최근에 광대역통합망(BcN)의 킬러 애플리케이션으로 대두되고 있는 IPTV(인터넷 TV)가 바로 멀티캐스트를 이용한 방송이다. IPTV는 케이



(그림 4) 셋톱박스용 DRM 개념도

블·위성·육상 네트워크 대신 인터넷 광대역 망으로 프로그램을 전송한다. 따라서 유니캐스트 방식의 VOD 콘텐츠 및 멀티캐스트 방식의 방송 콘텐츠를 보호할 필요성이 대두되고 있다. 본 기술은 ADSL, VDSL 또는 Ethernet 등과 같은 IP 네트워크를 통해 스트리밍 서버에 연결된 리눅스가 내장된 셋톱박스 환경에서 스트리밍 서비스에 DRM을 적용하는데 필요한 기술을 말한다. (그림 4)는 셋톱박스용 DRM 시스템의 개념도를 나타낸다.

2. 요구사항 분석

다음은 셋톱박스용 DRM 시스템이 만족해야 할 주요 요구사항을 나열한 것이다.

- 스트리밍 서버 독립성 – DRM 시스템은 기존 스트리밍 서버나 관련 모듈의 변경에 대한 요구 없이 적용되는 것이 바람직하다.
- 스트리밍 표준 지원 – 표준 동영상 포맷인 MPEG-2 TS[5], MP4[6]를 지원하고 표준 스트리밍 프로토콜인 RTP[7], RTSP[8]를 지원해야 한다.
- DRM이 적용되지 않은 서비스와 구별 불가능 – 최종사용자의 관점에서 볼 때, DRM이 적용된 서비스는 DRM이 적용되지 않은 서비스와 구별 불가능해야 한다. 이를 위해 DRM 적용으로 인한 가시적인 성능 저하나 지연, 화면의 열화 등이 발생하지 않아야 한다. 또한 VCR 유사기능 – 되감기, 빨리감기, 일시중지, 중지 등의 기능을 동일하게 지원해야 한다.
- 다운로드 서비스도 지원 – 본 기술의 주요 대상은 스트리밍 콘텐츠에 DRM을 적용하는 것이나, 스트리밍에 부적합한 네트워크 환경이나 최종 사용자 요구가 발생하는 경우(예를 들어, EBS 수능 방송)에는 다운로드 콘텐츠에 대해서도 DRM을 적용할 수 있어야 한다. DRM이 적용된 스트리밍 콘텐츠를 포맷 변경 없이 그대로 사용자 로컬 시스템에 다운로드해서 사용할 수 있도록 하는 것이 바람직하다.
- 대규모 사용자 환경 고려 – 셋톱박스용 DRM 시스템은 대규모 사용자가 특정 시간대에 접속하여 서비스를 요구하는 경우에도 수용할 수 있도록 성능을 고려하여 설계되어야 한다.

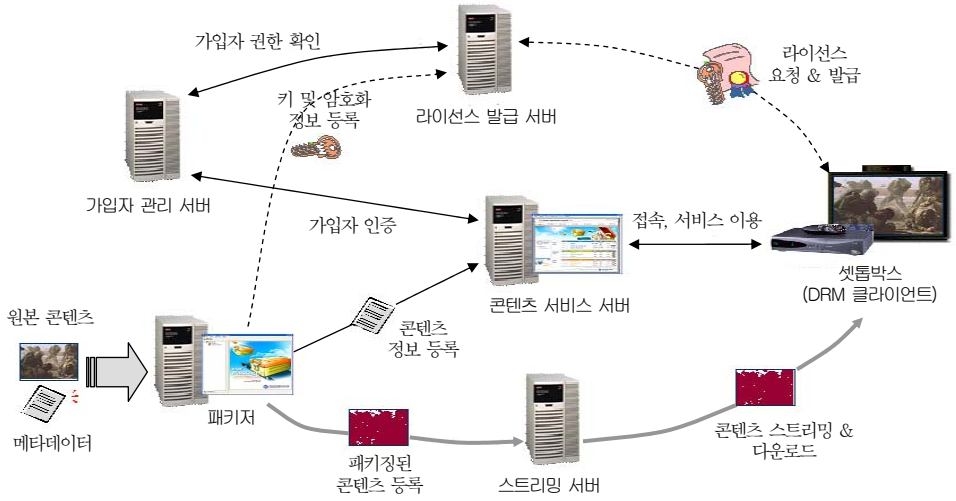
3. 시스템 구성

셋톱박스용 DRM 시스템은 크게 MPEG-2/4 VOD 스트리밍 DRM 시스템과 MPEG-2 멀티캐스트 DRM 시스템으로 구분할 수 있다. (그림 5)와 같이 MPEG-2/4 VOD 스트리밍 DRM 시스템을 먼저 설명하면 다음과 같다. 스트리밍 서비스업자는 콘텐츠를 패키저를 이용하여 패키징하는데 그 과정에서 발생된 패키징된 콘텐츠는 스트리밍 서버에 업로드되고 관련 키 정보는 라이선스 서버에 등록된다(초기에 사용자가 서비스에 가입 및 지불을 완료한 상태를 가정한다). 사용자는 셋톱박스를 통하여 콘텐츠 서비스 서버에 접속하여 콘텐츠를 요청한다. 콘텐츠 서비스 서버는 이 요청을 라이선스 서버로 넘

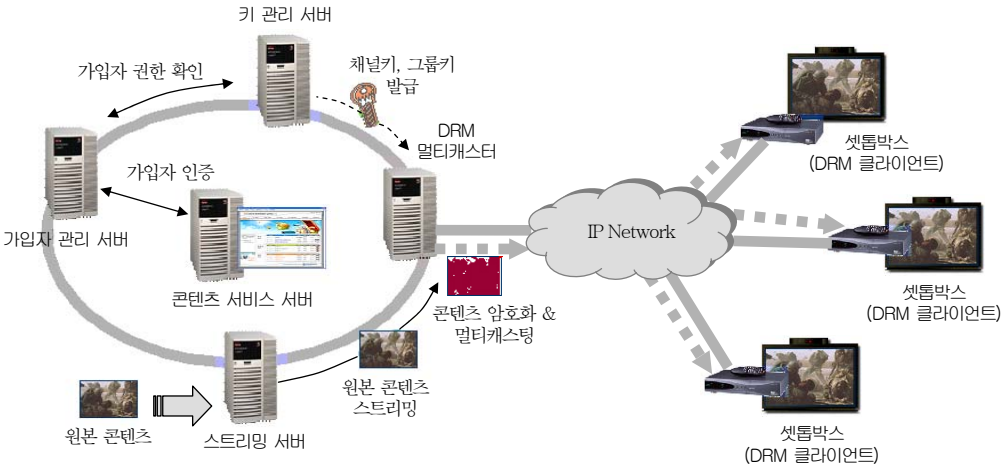
기고, 라이선스 서버는 가입자 관리 서버에 문의하여 해당 콘텐츠에 대한 사용 권한이 있는지를 확인한 후 라이선스를 해당 사용자의 셋톱박스 내에 있는 DRM 클라이언트로 별도의 키전송 채널을 통해 전달한다. 라이선스 발행과 동시에 스트리밍 서버로부터 패키징된 콘텐츠가 스트리밍 채널을 셋톱박스로 전송하고 DRM 클라이언트는 이를 라이선스에 들어 있는 키정보를 이용하여 실시간 복호화하여 렌더링하게 된다.

(그림 6)과 같이 멀티캐스트 DRM 시스템은 VOD 스트리밍 DRM 시스템과 공통적으로 스트리밍 서버, DRM 클라이언트, 콘텐츠 서비스 서버, 가입자 관리 서버를 사용한다.

그러나 두 시스템은 다음과 같은 점에서 차이가 있다. 이 차이점은 물론 멀티캐스트와 유니캐스트라는 두 스트리밍 방식의 차이점으로부터 출발한다. 멀티캐스트 스트리밍 시스템은 기본적으로 클라이언트의 요청과 관계없이 서버에서 일방적으로 방송을 날리고 사용자는 이 중에서 원하는 채널에 접속하여 서비스를 받는 방송 시스템이라고 생각하면 이

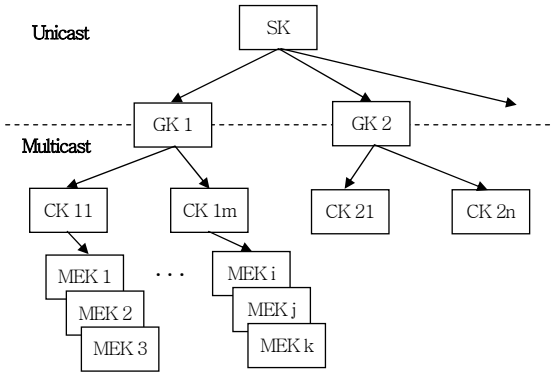


(그림 5) MPEG-2/4 VOD 스트리밍 DRM 시스템



(그림 6) MPEG-2 멀티캐스트 DRM 시스템

해가 쉽다. 방송은 기본적으로 채널 단위로 서비스되며 대규모 동시 사용자 환경에서 녹화 방송뿐만 아니라 생방송도 지원해야 한다는 특징이 있다. 이 때문에 VOD DRM 시스템이 파일별로 암호화(pre-encryption)하고 복호화 키를 라이선스에 담아 개별적으로 사용자에게 전달하면 되나, 멀티캐스트 DRM 시스템은 채널별로 암호화하고(real-time encryption) 대규모 사용자 환경에 유연하게 키 전달 및 갱신이 이루어져야 한다. 따라서 멀티캐스트 DRM 시스템에서는 패키저 대신에 DRM 멀티캐스터라는 장비를 두어, 스트리밍 서버로부터 받은 실시간 미디어 스트림을 암호화하여 외부 멀티캐스트 주소로 방송하는 형태를 취하게 된다. DRM 멀티캐스터에서는 미디어키(MEK)를 발생하여 스트림을 암호화한다. 멀티캐스트 DRM 시스템에서는 VOD와 달리 기본적으로 사용자 규모가 크고 채널 및 프로그램 전환으로 인하여 특정 시간대에 키요청이 집중되므로 기존 라이선스 방식을 사용하게 되는 경우 라이선스 서버에 급격한 성능 저하가 예상된다. 이 문제를 해결하기 위하여 키관리 시스템을 두고 있다. 키관리 시스템은 대규모 사용자 집단에 효율적으로 채널키를 전달하고 갱신하기 위한 시스템이다. 먼저 사용자들은 가입한 서비스 그룹별로 나뉘어 그룹키(GK)를 부여 받는다. 그룹키는 서비스 가입 시점에 해당 셋톱박스만이 풀 수 있는 비밀키(SK)로 암호화 되어 셋톱박스에 전달된다. 각 채널마다 DRM 멀티캐스터로부터 전송되는 멀티캐스트 스트림을 채널별로 암호화하기 위한 채널키(CK)가 부여된다. 이렇게 키관리 시스템은 미디어키, 채널키, 그룹키와 같은 3단계 키계층 구조를 관리하는 시스템이다. (그림 7)은 키계층 구조를 나타낸다.



(그림 7) 계층적 키 구조

VOD DRM 시스템에서는 각 사용자별로 라이선스 전송 채널을 열고 라이선스를 전달했으나, 대규모 사용자 환경에서는 성능 측면에서 바람직하지 않다. 따라서 멀티캐스트 DRM 시스템에서는 멀티캐스트 스트리밍 채널 속에 직접 키 패킷(미디어키, 채널키, 그룹키)을 삽입하여 전달하는 방식을 취한다.

<표 3>은 셋톱박스용 DRM 시스템의 개발 환경 및 지원 미디어를 나타낸다.

4. 기존 방식과의 차별점

<표 4>는 기존 DRM 시스템과 셋톱박스용 DRM 시스템의 특성을 비교한 것이다. 무엇보다도 큰 특징은 기존 스트리밍 시스템 즉, 기존 스트리밍 서버 및 스트리밍 플레이어, 코덱 등에 대한 변경 없이 DRM을 적용할 수 있다는 점이다. MPEG-2 멀티캐

〈표 3〉 운영 플랫폼 및 지원 미디어

운영 플랫폼	
MPEG-2 VOD DRM Toolkit	Linux, Windows
MPEG-4 ISMA/ISMACryp DRM Toolkit	Linux, Windows
MPEG-2 DRM Multicaster	Windows
MPEG-2 Multicast Key Management Server	Windows

지원 미디어	
VOD DRM	MPEG-2 TS(Transport Stream) MP4(MPEG-4 ISO File Format) MPEG-4 ISMACryp
Multicast DRM	MPEG-2 TS

〈표 4〉 기존 시스템과 셋톱박스용 DRM 시스템의 비교

	기존 시스템	ETRI 셋톱박스용 DRM 시스템
MPEG-2 VOD	• 스트리밍 서버 의존적 • 스트리밍 지원	• 스트리밍 서버 비의존적 • 스트리밍/다운로드 서비스 동시 지원
MPEG-2 Multicast	• 라이선스 방식의 실시간 암호화	• 키패킷 삽입 방식의 실시간 암호화
MPEG-4 ISMA	• 실시간 암호화의 경우, 다운로드 지원 못함	• ISMA[9] • 패킷단위 복호화 지원
MPEG-4 ISMACryp	• 지원하는 제품 없음	• ISMACryp[10] 지원
Selective Encryption	• 전체 데이터 암호화 • I Frame 암호화	• 오디오/비디오/전체/프레임별로 지원 • 프레임 내 부분 암호화

스트 DRM 시스템은 기존 라이선스 방식의 실시간 암호화의 문제점 즉, 라이선스 발급 서버에 대한 부하 집중, 복호화 시 콘텐츠와 라이선스의 싱크 문제, 갑작스런 프로그램 변경 대응의 어려움 등을 해결하기 위해 키패킷 삽입 방식의 실시간 암호화 기법을 새로 적용하였다. 그 결과, 서버 부하 집중 문제 및 복호화 시 싱크 문제가 발생하지 않으며 갑작스런 프로그램 변경에도 쉽게 대응할 수 있다. 또한 본 시스템은 콘텐츠의 보안 요구사항 및 성능 사이에 균형(trade-off)을 제공하기 위해 다양한 레벨의 선택적 암호화(selective encryption) 기법을 제공하고 있다. 즉, 성능이 중요한 콘텐츠의 경우에는 암호화 부분을 줄이고 보안이 요구되는 콘텐츠의 경우에는 전체 데이터 또는 오디오/비디오별로 암호화를 할 수 있다.

Ⅳ. 결론

지금까지의 대부분의 DRM 시스템 및 유통 모델은 오직 B2C 거래만을 지원하였으나 본 논문에서 소개된 End-to-end DRM 시스템은 B2C 뿐만 아니라 B2B 거래까지 지원하는 것이 특징이다. 유일하게 B2B 및 B2C를 동시에 지원하는 프로토콜이 ICE[11]인데, 이 프로토콜은 가격 및 콘텐츠 보호와 같은 조건들을 다루지 못한다. End-to-end DRM 시스템은 유통업자들 사이에서 유통 규칙 및 사용 규칙을 제어하고 강제함으로써 현재 또는 미래에 가능한 보다 더 다양한 유통 모델(예, 신디케이션, e-marketplace)을 지원할 수 있다는 데서 큰 의미가 있다. e-marketplace에서는 콘텐츠 유통 주체들이 접근해서 자신의 콘텐츠를 불법 복제로부터 안전한 상태 하에 올리고 이 콘텐츠에 다양한 유통 주체들이 참여함으로써 콘텐츠 유통 네트워크를 형성한다. 미래에는 e-marketplace와 같은 다양한 유통 모델이 발전할 것이고 이를 지원할 수 있는 End-to-end DRM 시스템의 필요성은 더욱 증가하리라 본다.

본 논문에서 소개된 셋톱박스용 DRM 시스템은 VOD 방식뿐만 아니라 멀티캐스트 방식의 스트리밍 서비스에도 DRM 기능을 지원한다는 측면에서 큰 의미가 있다. 아직까지 국내 DRM 업체 몇 곳을 제외하고 세계적으로 상용화된 형태의 멀티캐스트용 DRM 시스템을 개발한 곳은 보고되지 않고 있다. 또한 상기 개발한 국내 업체들의 경우 라이선스 방식으로 설계되어 있어 본 논문에서 제시한 키 패킷 삽입 방식의 시스템과는 구조적인 측면에서 차이가 있다. 특히 MPEG-2 멀티캐스트 DRM 시스템은 향후 도래할 IPTV 환경에서의 콘텐츠 보호 메커니즘으로 활용성이 증가할 것으로 본다. 뉴스위크 한국판(2005.6.15.)은 “텔레비전의 대변혁과 미래”라는 칼럼에서 IPTV는 일본에서는 이미 많이 이용되고 있으며 다른 나라에서도 인기라고 소개하고 있다. 특히 디지털 비디오 리코더(DVR)는 좋아하는 프로그램을 녹화해 원할 때 보고, 광고 방송을 건너뛰게 해준다. 2010년에는 불법 복제와 시청자들의 광고 건너뛰기로 미디어 회사의 자본이 1600억 달러나 감소하리라고 예상되는 가운데 마이크로소프트, 디즈니 등 여러 회사들은 서둘러 새로운 DRM 시스템 개발에 나섰다고 한다. 특히 마이크로소프트, 소니, 노키아, 삼성, 필립스 등 장치 제조업자들도 IPTV에 큰 기대를 걸고 있는데 그것은 IPTV가 여러 장치(X박스, 플레이스테이션, 휴대폰 등)를 넘나들며 콘

텐츠를 주고 받으리라 예상하기 때문이다. 국내에서도 IPTV는 KT나 하나로텔레콤 등 유선통신 사업자들이 차세대 홈네트워크 사업의 핵심 프로젝트로 추진하고 있는 서비스로, 전문가들은 IPTV가 안방 혁명을 가져올 킬러 서비스가 될 것으로 보고 있다. 국내에서는 IPTV가 2006년 상반기에 상용화될 예정이다. 앞으로 대역폭의 확대와 더불어 고화질 고품질의 디지털 콘텐츠에 대한 서비스 수요가 증가할 것으로 보이며 이에 따라 VOD 및 멀티캐스트용 DRM 시스템의 수요 또한 비례해서 증가할 것으로 예상된다.

약어 정리

ADSL	Asymmetric Digital Subscriber Line
B2B	Business to Business
B2C	Business to Consumer
BcN	Broadband convergence Network
CK	Channel Key
DID	Digital Item Declaration
DIDL	Digital Item Declaration Language
DRM	Digital Rights Management
DVR	Digital Video Recorder
GK	Group Key
ICE	Information and Content Exchange
IP	Internet Protocol
ISMA	Internet Streaming Media Alliance
ISMACryp	ISMA Encryption and Authentication specification
MEK	Media Encryption Key
MPEG	Moving Picture Experts Group
ODRL	Open Digital Rights Language
REL	Rights Expression Language
RP	Resource Pointer
RTP	Real-time Transport Protocol
RTSP	Real Time Streaming Protocol
SC	Secure Container
SK	Secret Key
TS	Transport Stream
VCR	Video Cassette Recorder
VDSL	Very-high-data-rate Digital Subscriber Line
XrML	eXtensible rights Markup Language

참 고 문 헌

[1] MPEG-21 DID, Digital Item Declaration, ISO/IEC 21000-2 FDIS Digital Item Declaration(N4813), May 2003.

[2] MPEG-21 REL, Rights Expression Language, Ad Hoc Group on MPEG-21 Rights Expression Language(N5190), Oct. 2002.

[3] ContentGuard, "eXtensible Rights Markup Language, Version 2.0," Available at http://www.xrml.org.

[4] Open Digital Rights Language, Version 1.1, Available at http://odrl.net.

[5] Generic coding of moving pictures and associate audio information, Part 1: System, Part 2: Video, Part 3: Audio, CD 13818, ISO/IEC JTC 1/SC 29/WG 11, May 1995.

[6] 14496-1:2001/Amd.1:2001 (E) Information Technology - Coding of audio-visual objects - Part 1: Systems, 2001.

[7] H. Schulzrinne et al., "RTP: A Transport Protocol for Real-Time Applications," July 2003.

[8] H. Schulzrinne, A. Rao, and R. Lanphier, "Real Time Streaming Protocol(RTSP)," Apr. 1998.

[9] ISMA, Internet Streaming Media Alliance Implementation Specification Version 1.0., Aug. 2001.

[10] ISMACryp, Internet Streaming Media Alliance Encryption and Authentication Specification Version 1.0., Feb. 2004.

[11] The Information and Content Exchange(ICE) Protocol Version 1.1., Available at http://www.ices-tandard.org.