디지털 홈네트워킹 환경에서의 DRM 시스템 구축

김종안 류정섭 한평희 김진한
KT 마케팅연구소 디지털미디어개발팀

A study on the implementation of DRM system in digital home networking

Jongan Kim Jungseob Ryu Pyunghee Han Jinhan Kim
KT Marketing & Technology Laboratory

Abstract

Due to the rapid spread of high speed Internet access and the contents digitization, the demand for the copyright protection of digital contents has increased continuously so that the digital rights protection technology becomes one of the inevitable components in the digital content providing services. This paper describes the current trend of DRM(Digital Rights Management) technology and how to implement the system for the protection of digital assets in the digital home networking environment.

Keywords

DRM, Digital Home Networking, Home gateway multimedia securiy

I. 서 론

2005년도 하반기부터는 국내 유선통신사업자들간의 초고속인터넷 속도경쟁이 치열해짐에 따라 100Mbps 상하향속도를 제공받는 가구수가 급속도로 증가할 추세이다. 이에 따라 통신사업자는 가입자 댁내에 홈게이트웨이(네트워크 Hub, VoIP, 카메라 등을 실장한 일종의 IP STB)를 설치함으로서 영상(방송), 음성, 데이터서비스 즉 TPS(Triple Play Service)를 제공할 수 있는 기반을 마련하게 될 것이다. 100Mbps라는 전송속도는 MPEG-2 SD(Standard Definition: 표준 품질로 4 Mbps 대역폭 소요)급 25개 채널 또는 HD(High Definition: 고 품질로 20Mbps 대역폭 소요)급 4개 채널을 수용할 수 있는 용량이다. H.264 등 압축률이 높은 인코딩 방식을 사용한다면 수용 가능한 방송채널 수는 더 늘어 날 수 있다.

데이터 전송망이 디지털화 되고 속도가 빨라짐에 따라 컨텐츠 소유자나 서비스업체는 매출이 정체된 아나로그 시장을 탈피하여 새로운 디지털 시장을 겨냥하여 콘텐츠의 디지털화를 시행하는 추세이다. 디지털 콘텐츠는 아나로그 콘텐츠와는 달리 복사에 비용이 거의 들지 않으며, 복사 후에도 원본과 같은 품질을 지니게 되는 장점이 있으므로 온라인 시장이 강력한 유통경로로 자리를 잡아가고 있다. 그러나 디지털 콘텐츠는 적절한 보호 수단을 갖추지 못한다면 많은 자본과 시간을 투자하여 제작한 콘텐츠가 무한 불법 복제되어 콘텐츠 창작자에게 커다란 경제적 손실을 초래할 가능성이 크다.

디지털 홈네트워킹 환경에서 디지털 콘텐츠 보호 시스템 구축시에는 사용자가 홈게이트웨이(STB)를 이용하여 콘텐츠를 소비하므로 일반 PC 환경과는 달리 몇 가지 고려해야 할 사항이 있다. 본 고에서는 홈네트워킹 환경에서의 DRM 구축방안에 대해서 논하고자 한다.

II. 홈게이트웨이

홈게이트웨이는 홈네트워크(LAN: Local Area Network)와 외부의 네트워크(WAN: Wide Area Network)를 연결하는 지능형 접점 장비이다[1]. 홈게이트웨이는 디지털 네트워킹을 구현하는 핵심 요소로써, 데이터통신을 위한 네트워크 기능, IP 음성통신을 위한 VoIP(Voice over IP) 통신기능, 영상서비스 제공 기능, 그리고 USB 카메라를 이용한 댁내보안서비스 등의 TPS 구현이 가능하도록 가입자 가정에 설치되는 단말장비이다. 홈게이트웨이는 Win CE, Embedded XP, 그리고 리눅스 등의 운영체제, 미디어 플레이어 등의 소프트웨어와 CPU, 메모리, 입출력장치, 오디오/비디오 디코더와 같은 하드웨어로 구현된 일종의 PC와 유사하지만 주요 동작이 TV와 같이 리모컨에 의해 일어나고, 사용자가 임의의 프로그램을 설치/실행할 수 없다는 점에서 PC와 다르다.

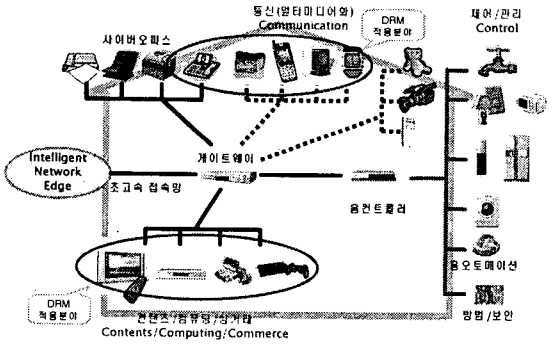


그림 1. 홈네트워크 구성도

홈게이트웨이를 이용한 홈네트워크 구성도는 그림 1과 같다. 홈네트워크 분야는 크게 통신, 콘텐츠/컴퓨팅/상거래, 제어 분야로 나누어지는데 이중 앞의 두 부분이 콘텐츠의 유통/재생과 관련된 부분으로 콘텐츠 보호가 필요한 분야이다.

III. DRM 시스템

1. DRM 기술 개요

DRM(Digital Rights Management: 디지털 저작권 관리)은 암호화 기술을 이용하여 디지털콘텐츠에 대한 지적재산권을 지속적으로 관리하고 보호하는 기술로써[2], 디지털 콘텐츠를 암호화하여, 불법적인 접근을 막고, 적법한 사용자가 라이선스에 포함된 권한과 복호화키를 이용하여 허가된 권한 하에서 콘텐츠를 사용하게 한다. DRM시스템은 일반적으로 그림 2와 같이 DRM 패키저(가), 라이선스서버(나), DRM Agent(다)로 구성된다.

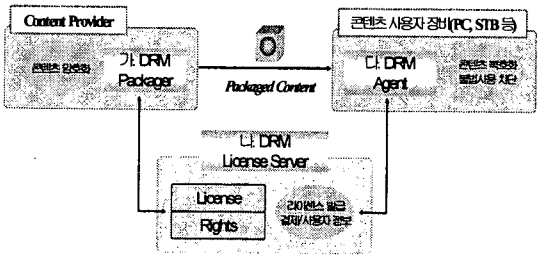


그림 2. DRM 시스템 구성도

패키저는 원본 디지털 콘텐츠를 입력으로 받아들여 암호화 속도가 빠른 AES(Advanced Encryption Standard) 등의 대칭키 암호화 알고리즘을 이용하여 암호화된 DRM 콘텐츠를 출력하게 된다. 패키저를 통해 나온 DRM 콘텐츠는 인터넷환경을 통해 사용자에게 자유롭게 유통된다. 이러한 DRM콘텐츠를 이용하기 위해서는 DRM 라이선스가 필요한데, 라이선스에는 암호화된 DRM 콘텐츠를 복호화에 사용되는 복호키와 콘텐츠의 사용권한을 담고 있다. 라이선스 서버는 이러한 라이선스의 발급과 관리를 담당한다. 마지막으로 DRM Agent는 라이선스 서버에서 발급받은 라이선스에 있는 복호키를 이용하여 암호화된 콘텐츠를 복호화하고 사용권한을 이용하여 콘텐츠의 불법사용 및 차단 기능 등을 수행한다. DRM Agent는 DRM Client, DRM Controller 등 다양한 용어로 불린다.

2. DRM 서비스 흐름도

홈네트워크 환경에서 홈게이트웨이 STB을 이용하여 디지털 콘텐츠 서비스를 할 경우에 DRM 서비스 과정[3]을 그림 3에 나타내어 보았다. DRM 패키징을 마친 후 콘텐츠가 사용자에게 실시간으로 전달되어 소비될 경우에는 실시간 DRM 서비스를 제공하게

되고, 패키징 작업이 완료된 콘텐츠를 콘텐츠 서버에 업로드한 후 사용자의 요청에 의해 제공되는 경우에는 VOD(Video On Demand: 주문형 Video) DRM 서비스를 받게 된다. 먼저 VOD 서비스일 경우에는 CP(Contents Provider: 콘텐츠 제공업체)에게서 받은 원본 디지털콘텐츠를 패키저를 통해 암호화하여(①), 콘텐츠 서버에 업로드 하고, 복호화 키를 등록한다. 사용자의 단말기는 웹사이트에 접속하여, 콘텐츠를 선택, 구매하면(②), 웹서버 사용자 구매정보를 확인한 다음 DRM 라이선스 서버에게 라이선스 발급 요청을 한다.(③). 웹서버는 라이선스 서버에게 라이선스 서버는 사용자의 콘텐츠에 대한 권한정보와 콘텐츠의 복호화 키를 이용하여 라이선스를 발급하여 사용자 홈게이트웨이에 전달한다(④). 콘텐츠 서버(혹은 VOD 서버)는 홈게이트웨이에 사용자가 요청한 콘텐츠를 스트리밍 또는 다운로드 방식으로 제공한다(⑤). 사용자 장비(홈게이트웨이, PC 등)내에 있는 DRM Agent는 라이선스에 포함된 복호화 키를 이용하여 암호화된 콘텐츠를 복호화하고, 재생한다(⑥). 실시간 콘텐츠(방송 콘텐츠)는 디지털 인코딩 과정(①')을 거친 콘텐츠를 실시간 DRM 서버(혹은 Encryptor)에서 패키징작업이 일어난 후 사용자 홈게이트웨이에게 직접 암호화된 스트림이 공급된다는 점에서 VOD 서비스와 다르다.

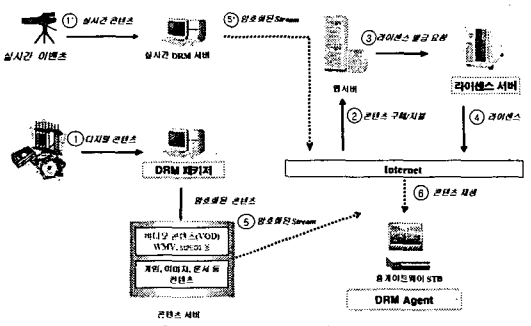


그림 3. DRM 서비스 흐름도

3. 홈네트워킹 DRM 시스템의 특성

홈네트워킹 DRM 시스템은 DRM Agent가동작되는 홈게이트웨이의 하드웨어 및 소프트웨어적 특성으로 인하여 일반 PC용 DRM 시스템 설계시와는 달리 고려해야 할 사항에 대하여 살펴보기로 하자. 홈네트워킹 DRM 시스템은 홈게이트웨이의 구조적인 폐쇄성(Embedded XP, WinCE, Linux 등의 OS를 서비스 특성에 맞게 Customization하여 일반인이 홈게이트웨이 OS 등 기타환경에 접근하기 어려움)으로 보안성이 높은 DRM 시스템을 구축할 수 있는 장점이 있다. 한편 홈게이트웨이는 일반 PC보다 저성능 하드웨어(CPU, 메모리 용량 등)를 가지고 있기 때문에 높은 강도의 보안 알고리즘, 소프트웨어적인 디코더 구현 등 연산이 많은 작업을 수행할 수 없는 단점 등 많은 제약을 가지게 된다. 아울러 홈게이트웨이는 네트워크 기능, 가전 제어, 디지털 영상서비스 등의 기능을 동시에 하나 이상 수행해야 하므로 어느 특정 서비스가 하드웨어 자원을 독점할 수 없다는 점도 DRM 서비스 구축시 고려하여야 한다. 또한 DRM 구축 업체와 홈게이트웨이 제조업체가 동일 사업자가 아닐 확률이 크기 때문에 DRM Agent를 홈게이트웨이에서 동작시키기 위해서는 홈게이트웨이 제조업체의 협조가 DRM 시스템의 구축에 또 다른 변수로 작용할 수 있다.

홈게이트웨이 기반 VOD 서비스의 파일 포맷으로는 현재 MPEG2/WMT(Windows Media Technology) 가 널리 사용되고 있으나, 홈게이트웨이의 성능이 향상됨에 따라 향후에 MPEG4/H.264 코덱을 지원하는 홈게이트웨이가 VOD 서비스에 많이 채택될 전망이다. MPEG4/H.264 코덱은 MPEG-2에 비해 압축 효율이 높아 제한된 전송 대역폭을 이용하여 IPTV(IP 방송서비스) 사업자에게는 상당히 매력적이나, 현재까지는 H.264 디코더 칩셋이 양산되지 못하여 빠른 시일내에 가입자에게 널리 보급되기에는 어려움이 있을 것으로 판단된다.

4. 홈네트워킹 DRM 시스템 구조

홈게이트웨이용 DRM시스템은 크게 CA(Certificate Authority) 서버, DRM Packager, License 서버, 홈게이트웨이용 DRM Agent의 4개 모듈로 나눠질 수 있다 (그림 4 참조). 본 고에서는 DRM 구성요소간의 정보 교환에는 비대칭키 방식인 PKI(Public Key Infrastructure)를 이용하고, VOD 시스템[3]에서 사용자(홈게이트웨이)에게 제공하는 디지털 콘텐츠의 암호화에는 대칭키 방식인 AES (Advanced Encryption Standard) 암호화

알고리즘을 사용할 것을 제안한다. AES 방식은 전 세계적으로 그 강인성이 인정받고 있으며, 암/복호화 속도가 PKI 방식에 비해 빨라 홈게이트웨이 기반의 콘텐츠 암/복호화에 널리 사용되고 있다.

4.1 DRM 패키저(Packager)

패키저는 원본 디지털 콘텐츠를 암호화 하고 그 암호화된 콘텐츠를 VOD 서버로 전송하고, 서비스화면에 게시될 관련 메타데이터 정보와 라이선스 서버가 라이선스를 발급하기 위해 필요한 정보를 입력하는 하는 기능 수행을 수행한다.

콘텐츠 암호화 방식으로는 AES 방식을 사용하는데, AES는 DES(Digital Encryption Standard)를 대체할 차세대 표준 알고리즘으로 미국 NIST (National Institute of Standards and Technology)에서 선정한 암호화 알고리즘으로 홈게이트웨이 하드웨어 성능을 고려하여 128bit 길이의 블록 암호화 기법을 사용한다.

실시간 DRM 시스템의 경우에는 여러 방송 채널을 동시에 받아들여 실시간으로 암호화를 수행하는 Realtime Encryptor가 DRM 패키저를 대신한다.

4.2 라이선스 서버

암호화된 콘텐츠를 재생하기 위한 복호화 키의 관리와 사용권한 및 조건을 명시하고 있는 객체인 라이선스의 설정 값들은 관리하는 시스템으로, DRM 패키저(실시간 Encryptor)를 통해 입력된 정보를 이용하여 라이선스를 생성하고 사용자에게 전달하는 기능을 수행한다.

라이선스 서버는 DB서버를 이용하여 암복호화키, 라이선스 발급 정보 등을 기록한다. DB(Database) 서버는 라이선스 발급 성능(초당 라이선스 발급 건수) 향상을 위해 통상 라이선스 서버와 분리하여 구현하며, DRM 시스템 안정성을 위해 SAN(Storage Area Network) 스위치를 이용하여 이중화를 구현한다.

실시간 DRM 시스템의 경우에는 방송 콘텐츠를 복호할 수 있는 Key를 발생하는 Key 분배서버를 구현하여야 한다.

4.3 CA 서버

PKI 기반 인증서와 CRL(Certificate Revocation List, 인증서 폐기 목록)을 발급 관리하여 객체를 인증하고, 인증된 객체와 PKI 기반의 암호화 송수신을 수행하여 신뢰성을 확보하기 위한 서버이다. 여기서 객체란 각 모듈이나 시스템, 사용자, 그리고 라이선스 등 PKI 인증서가 적용되는 모든 것을 포함한다. 인증서 검증을 통해 해당 시스템(또는 사용자)은 전체 시스템 관리자가 인증한 적법한 시스템(또는 사용자)으로 신뢰할 수 있으며 그 유효성을 검증하기 위해 루트 CA부터 최종사용자 인증서로의 경로 검증과 폐기 목록의 검증, 유효 시간의 검증 등을 수행한다. DRM 시스템에서의 주 역할은 DRM 객체(패키저, 라이선스 서버, 홈게이트웨이 등)의 인증서의 발급/관리를 담당하게 된다.

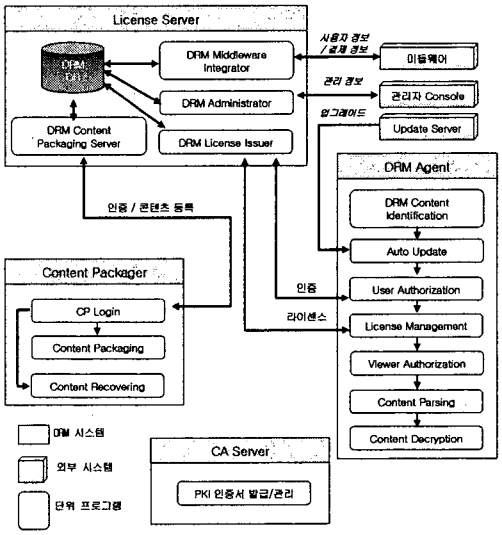


그림 4. 홈네트워킹 DRM 시스템 구성도

4.4 DRM Agent

홈게이트웨이의 플레이어 내부에서 DRM 기능을 처리하는 모듈로써 사용자 인증, 라이선스 발급 요청, 발급된 라이선스의 관리, 라이선스 서버와의 암호화 메시지 송수신(인증서에 있는 공개키를 이용), 콘텐츠 복호화 및 재생, 콘텐츠 사용권한 조사 등의 기능을 수행한다.

DRM Agent는 향후 홈게이트웨이의 새로운 코덱 등을 수용할 수 있는 유연한 확장 구조를 가지도록 설계하여야 한다.

IV. 결 론

홈네트워킹 환경에서 디지털 콘텐츠 서비스 제공하는 데 필수 구성요소인 DRM시스템은 현재까지 다양한 분야에 활발히 연구되어 적용되고 있다. 홈게이트웨이에 사용되는 DRM 솔루션은 그 시스템 특성으로 인해 PC보다 안정된 보안환경을 제공하지만 제한된 하드웨어 성능으로 인하여 하드웨어 자원을 효율적으로 사용할 수 있도록 DRM 시스템을 설계하여야 한다. 본 고에서는 이를 위해 DRM 구성요소(패키저, 라이선스 서버, STB)간 정보 교환에는 PKI 인증서를 이용한 비밀통신 사용을, 디지털 콘텐츠 보안에는 AES 대칭키 암호화 알고리즘을 사용할 것을 제시하였다.

DRM 기술은 CP(Contents Provider)의 디지털 콘텐츠를 암호화하여 유무선 인터넷 유통환경을 이용하여 사용자의 단말기(STB, PC, 휴대폰 등)에 전달하기 때문에 현재까지는 디지털 콘텐츠 보호수단으로 각광을 받고 있다. 하지만 DRM 기술의 치명적인 결함은 단말기내에서 DRM 콘텐츠가 복호된 이후의 디지털콘텐츠의 보호에 대한 대책이 미흡하다는 것이다. 이를 보완하기 위해서는 오디오 칩셋이나 비디오 칩셋 제조회사와 협력하여 DRM 기술을 디바이스 드라이버 수준까지 적용하여야 한다. 또한 DTV 시대에 대비하여 홈게이트웨이의 아나로그 TV 출력단자(composite, YCbCr 등)를 디지털 출력단자(DVI 등)로 교체한 후, 홈게이트이와 DTV간에 HDCP(DVI, HDMI 등의 디지털 인터페이스를 통해 디지털 디스플레이로 전송되는 디지털 신호의 불법복제 방지기술) 등의 링크 암호화기술을 적용하여야 DRM은 보다 완벽한 디지털 콘텐츠 보호 솔루션으로 그 가치를 인정받을 수 있을 것이다.

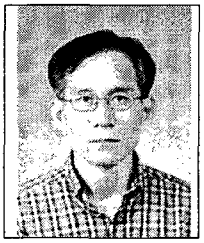
[참 고 문 헌]

[1] 이해영 외 3인, "홈게이트웨이 동향 및 전망", KT 정보통신연구지, 제15권 1호, pp3-10, 2001.3

[2] "DRM 최신 국제표준 기술사양 분석 및 세계유명제품 동향과 전망에 과한연구" 소프트웨어 진흥원

[3] 박훈규 외 2인, "홈게이트웨이를 이용한 디지털 컨텐츠 서비스 제공에 관한 연구", Comsw2004, 2004.7

Biography



김 종 안

1984년 고려대학교 전기공학과 졸업

1988년 고려대학교 대학원 전자공학과(공학석사)

1988년~현재 KT 마케팅연구소 책임연구원

<주관심분야> DRM, CAS, 디지털 시네마, Wibro

<이메일> joankim@kt.co.kr

류 정 섭

1994년 충남대학교 전산과 졸업

1996년 충남대학교 대학원 전산과(공학석사)

1996년~현재 KT 마케팅연구소 책임연구원

<주관심분야> DRM, CRM, CAS

<이메일> subi@kt.co.kr

한 평 희

1987년 숭실대학교 전자공학과 졸업

1989년 한국과학기술원 전기전자공학과(공학석사)

1989년~현재 KT마케팅연구소 수석연구원

<주관심분야> 통방융합서비스, 디지털컨텐츠보호, 디지털신호처리

<이메일> phhan@kt.co.kr

김 진 한

1986년 고려대학교 전자공학과 졸업

1988년 한국과학기술원 전기및전자공학과(공학석사)

1992년 한국과학기술원 전기및전자공(공학박사)

1992년~현재 KT 마케팅연구소 디지털미디어개발팀장

<주관심분야> DRM, IP-TV, On-Demand 서비스, 디지털컨텐츠, WiBro 등

<이메일> jinhan@kt.co.kr