방송환경에 적절한 디지털 셋탑박스에서의 녹화 및 재생 제어 방법

최범석 · 이혜주 · 석종원 · 홍진우
한국전자통신연구원

Recording and Playback Control Method Proper in Broadcasting Service Environment

Bum-Suk Choi · Hye-Joo Lee · Jong-Won Suk · Jin-Woo Hong
ETRI
E-mail : [bschoi, hyejoo, jwseok, jwhong]@etri.re.kr

요 약

방송 환경이 디지털화 되면서 기존 방송 단말에서 지원하던 방송 프로그램 녹화 기능이 새로운 저작권 문제를 불러일으키고 있다. 그러나 방송 단말에 저장되는 방송 콘텐츠를 위한 적절한 보호 방안이 마련된다면, 이러한 콘텐츠를 이용한 새로운 비즈니스 모델을 창출해 낼 수 있다. 본 논문에서는 방송 단말에 저장된 콘텐츠를 효과적으로 보호하고 이를 이용한 콘텐츠 유통을 지원할 수 있으며 기존의 방송 서비스 환경에 쉽게 적용될 수 있는 디지털 콘텐츠 보호 방법에 대하여 논한다.

ABSTRACT

As the broadcasting service is digitalized, the copyrighters more concern about permitting users to record broadcasting content. However, the recording is very convenient function for the users to enjoy their favorite program without restriction of broadcasting schedule. In this paper, we will suggest an efficient mechanism to protect recorded content. We will also propose a new business model on the recorded broadcasting content using suggested protection mechanism.

키워드
콘텐츠 보호, 디지털 방송, 셋탑박스, 복사제어

Ⅰ. 서 론

최근 디지털 방송이 본격화되면서 HD 급의 고화질 콘텐츠를 일반 방송채널에서도 시청할 수 있게 되었다. 이러한 서비스는 앞으로 계속 확산될 것이며, 경쟁적으로 차별화를 내세우고 있는 유료 채널서비스에 부응하여, 제공되는 콘텐츠의 질 역시 더욱 고급화 될 것이다. 그러나 아직 콘텐츠 제작자들은 고 품질의 디지털 콘텐츠를 방송 미디어를 통하여 제공하기를 꺼려하고 있는데, 가장 큰 이유 중의 하나는 사용자의 단말에 저장되는 콘텐츠를 안전하게 보호할 수 있는 적절한 방법을 아직 찾지 못하고 있기 때문이다. 기존의 아날로그 신호로 입력되는 방송 프로그램을 아날로그 저장매체에 녹화를 하게 되면 자연히 화질의 열화가 생기게 되어 콘텐츠의 가치를 떨어뜨리게 되므로 복사본에 대한 저작권 보호 문제가 크게 대두되지 않았다. 그러나 디지털 방송 환경으로 변화되면서 복사본은 원본과 전혀 차이가 없게 되었다. 따라서 이러한 디지털 콘텐츠의 특성은 기존에 간과해 왔던 녹화 콘텐츠에 대한 저작권 문제를 다시 불러일으키게 되었다. 그럼에도 불구하고 방송 프로그램 녹화 기능은 방송 서비스가 가지고 있는 일방적인 방송 편성에 따른 단점을 보완시켜줄 수 있는 유일한 방법으로, 대부분의 사용자들에게 없어서는 안될 기능으로 인식되고 있다. 따라서, 본 논문에서는

먼저 녹화 콘텐츠를 이용한 비즈니스 모델을 제안하고 이를 만족시킬 수 있는 효과적인 방송 콘텐츠 보호 방안을 제시한다.[1-2]

II. 녹화콘텐츠를 고려한 비즈니스 모델

사용자가 유료 방송 채널에서 방영되는 프로그램을 방송 단말의 저장장치(이하 PVR: Private Video Recorder)에 마음대로 녹화할 수 있다면, 사용자는 녹화된 프로그램을 언제든지 시청할 수 있고 심지어 녹화된 프로그램을 재배포 할 수도 있을 것이다. 이러한 기능은 사용자에게 편리성을 제공하지만 저작권자의 의도와는 다르게 콘텐츠가 사용될 수 있으므로 이에 대한 적절한 제어가 가능해야 한다.

본 논문에서 제시하는 비즈니스 모델은 방송사(또는 저작권자)가 허용하는 조건 하에서 방송 프로그램에 대한 녹화를 가능하도록 하고 녹화된 프로그램을 사용자가 재배포할 수도 있도록 하되, 일단 녹화된 프로그램을 재사용 하기 위해서는 반드시 유통 시스템을 거치도록 하여 이익을 창출하는데 그 목적이 있다. 이를 가능하게 하기 위해서는, 먼저 방영되는 각 콘텐츠에 대하여 저장제어가 가능해야 하며, PVR에 저장되는 콘텐츠에 대하여는 안전한 보호 관리가 이루어져야 한다. 다양한 비즈니스 모델을 지원하기 위하여 다양한 시청 조건이 적용 가능해야 하며, 시청자들 간의 자유로운 콘텐츠 공유를 지원하기 위하여 콘텐츠와 이를 시청하기 위하여 필요한 라이센스가 독립적으로 관리되어야 한다. 마지막으로, 과금처리 및 키를 전송하기 위한 각각 다른 수많은 PVR 시스템에 저장되는 콘텐츠들을 효율적으로 관리하기 위한 키 관리 방안이 적용되어야 한다.

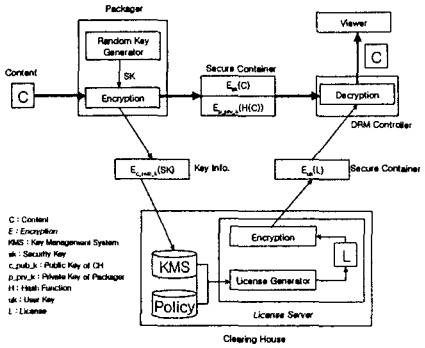
III. CAS의 범위

CAS(Conditional Access System)란 유료방송 서비스를 위하여 서비스를 신청한 가입자만이 방송 시청이 가능하도록 제한하는 시스템이다. 유료방송을 시청하려면 시청자는 TV, 셋탑박스(이하 STB, Set Top Box)와 STB에서의 사용자 인증을 위한 스마트카드를 가지고 있어야 한다. 여기서 스마트 카드는 시청 자격, 시청자의 정보, 시청 기록 등을 저장하고 있으며, STB는 스마트 카드에 저장된 시청자의 정보에 따라 인코딩된 디지털 신호를 적절한 출력 형태로 변환시키거나 제한할 수 있게 된다.[3-4]

CAS는 이미 유료 아날로그 방송에서부터 적용되어 왔으며, 현재의 디지털 유료 방송 서비스에서도 가장 일반적으로 사용되고 있는 방법이다. 그러나 CAS의 개념은 최초에 STB에 수신되는 프로그램에 대한 접근 제한(conditional access)을 주된 목적으로 하고 있으며, PVR에 저장되는 콘텐츠에 대한 보호를 보장하지는 않는다.

IV. DRM과 방송환경의 고려사항

DRM(Digital Rights Management) 시스템은 인터넷 환경에서 콘텐츠 유통을 위한 보호 메커니즘을 가리킨다. 기존의 DRM 시스템은 일반적으로 서버 상에서 콘텐츠가 보호처리(packaging process)되어 PC에 전달되고, 이를 소비하기 위해서는 라이센스를 독립적으로 다운받아야 하는 프레임워크를 가지고 있다. <그림 1>은 가장 일반적인 DRM 시스템의 구조를 나타낸다.[5]



<그림 1> 일반적인 DRM 시스템 구조

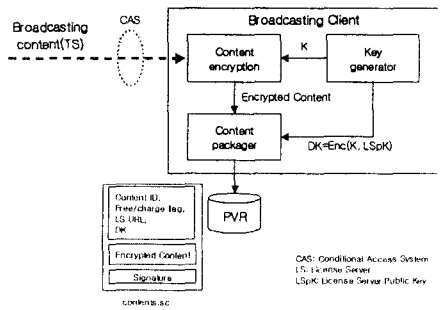
콘텐츠 소비 환경의 관점에서, 방송 환경에 있어서 PVR에 저장되는 콘텐츠는 일단 사용자의 단말에 저장된 후 소비된다는 점에서 인터넷 환경에서 다운로딩(downloading) 후 시청할 수 있는 콘텐츠와 그 개념이 유사하다. 따라서 기존의 인터넷 콘텐츠에 대한 DRM 시스템이 PVR에 저장되는 방송 콘텐츠에도 유사하게 적용될 수 있다. 즉 방송 서버측에서 콘텐츠를 암호화하고 STB에서는 암호화된 상태로 PVR에 저장하도록 한 후, 리턴채널(return channel)을 통하여 저장된 콘텐츠에 대한 라이센스를 전송 받도록 할 수도 있다.

그러나 방송 콘텐츠의 소비 환경은 인터넷 콘텐츠 소비 환경과 몇 가지 다른 특징을 가지고 있다. 방송 환경의 가장 큰 특징은 방송 서비스가 일 대 일로 제공되는 서비스가 아닌 일 대 다의 무차별적으로 제공되는 서비스라는 점이다. 따라서 방송국 측에서는 특정 셋톱박스에만 선별적으로 콘텐츠를 전송할 수 없으며, 콘텐츠에의 접근을 제어하기 위한 유일한 방법은 셋톱박스를 통해서만 가능하다. 또한 일반적으로 유료 방송 채널의 경우 CAS를 적용하여 가입자만이 시청을 가능하도록 하고 있으며, 채널 가입자는 각 콘텐츠의 저장 허가 유무에 상관없이 현재 해당 채널을 통하여 방송되고 있는 콘텐츠를 시청할 수 있는 권리를 가진다. 즉, 가입된 채널에 대하여 일단 방송 시간에 방영되는 프로그램은 시청 가능 하여야 하므로 어떠한 방식으로

든 암호화된 콘텐츠를 복호화 할 수 있는 키 정보를 프로그램과 함께(또는 미리) 셋탑박스에 전달시켜 주어야 한다. 이는 앞 절에서 언급한 CAS에서 사용되고 있는 복잡한 키 관리 시스템(ECM, EMM)을 다시 적용할 것을 요구하게 된다. 이는 매우 비효율적인 보호 방법이다. 마지막으로 현재 디지털 방송 콘텐츠의 전송 포맷은 MPEG-2 전송 규격을 따르고 있으며, PVR에서는 기본적으로 trick play를 위한 random access 기능을 지원하고 있다. 따라서 PVR에 저장된 방송 콘텐츠를 보호하는 방법은 위에서 언급한 방송 환경 및 방송 콘텐츠의 특성이 모두 고려되어야 한다.

V. 녹화 콘텐츠 보호 방법

여기서는 기존의 방송 시스템을 그대로 사용하면서도 DRM 기술을 접목시킬 수 있는 방법을 제시한다. <그림 2>는 STB와 PVR 상에서 콘텐츠 보호 방법을 나타낸다.



<그림 2> 녹화 콘텐츠 보호 방법

방송 스트림(TS)이 전송되어 STB에 수신되면 일단 CAS를 통하여 채널에 대한 가입 여부를 확인하게 된다. 채널 가입자임이 확인되면 스마트카드에 저장된 복호키를 통하여 스크램블된 스트림이 역스크램블이 되어 사용자에게 디스플레이된다. 만일 사용자가 전송 스트림에 대한 녹화(또는 예약녹화)를 선택하게 되면, 역스크램블된 스트림은 STB 내에서 자체적인 암호화 과정을 거치게 된다. 스트림에 대한 암호화에 있어서 고려해야 할 점은 PVR에서 지원할 수 있는 다양한 플레이 모드를 제한하지 말아야 한다는 것이다. 특히, 랜덤 액세스 플레이 모드를 지원하기 위해서는 TS 패킷 중 PSI 정보를 담고 있는 패킷과 데이터 패킷의 헤더 부분은 암호화에서 제외시켜야 한다.[6]

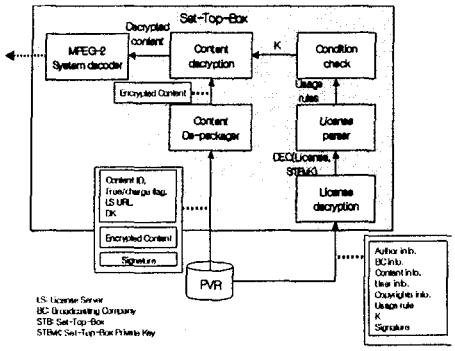
암호화에 사용되는 (대칭)키는 STB 내에서 랜덤하게 생성되며 선택된 스트림에 대한 암호화 과정을 마치면 자동적으로 삭제되게 된다. 암호화된 스트림은 DRM 시스템과의 연결을 위한 메타데이터와 함께 하나의 파일 형태(secure container)로 PVR에 저장되게 된다. 이러한 파일 안에는 암호화된 스트림과 더불어 콘텐츠 ID, 유료 콘텐츠임을 나타내는 flag, 라이센스를 발급하는 기관의 URL, 암호화된 스트림을 복호화할 수 있는 키 정보, 그리고 암호화된 스트림과 메타데이터의 무결성 확인을 위한 서명 등이 포함된다. 여기서 키 정보(DK)는 암호화 키(K)를 라이센스 발급기관의 공개키로 암호화한 값이 된다.

저장된 콘텐츠를 사용자가 재생 선택하면, STB는 먼저 저장된 파일이 유료 콘텐츠(free_charge flag)인가를 확인하게 된다. 만일 선택한 파일이 유료 콘텐츠일 경우, 리턴채널을 통하여 메타데이터에 기술된 라이센스 서버의 URL로 접속하게 된다.

STB가 라이센스 서버에 라이센스 요청을 하면, 라이센스 서버는 먼저 라이센스를 요청한 STB를 인증하고 요구한 콘텐츠(content ID)에 대한 권리 선택(time, number of time to play, etc…)을 위한 웹페이지를 전송한다. 사용자가 라이센스에 포함될 권리를 모두 선택하고 나면, 결재처리를 위한 과정으로 넘어가고 결재처리를 완료하면 요청한 라이센스를 생성한다. 라이센스 안에는 라이센스 발급 기관에 대한 정보, 라이센스 유효 기간, 사용자가 선택한 권리 정보, 암호화된 콘텐츠를 복호화할 수 있는 키 정보, 및 라이센스에 대한 서명이 포함된다. 특히 암호화된 콘텐츠를 복호화 할 수 있는 키 정보는 STB로부터 전달받은 키 정보(DK)를 라이센스 서버의 개인키로 복호화 한 값(K)이 된다. 마지막으로, 라이센스는 오직 해당 라이센스를 요청한 STB에서만 사용할 수 있도록 라이센스를 요청한 STB의 공개키로 암호화되어 전송되게 된다.[7]

STB는 다운로드된 라이센스 파일을 먼저 STB의 개인키로 복호화하고 파싱 된 정보로부터 해당 라이센스가 정당한 라이센스인지를 확인한다. 또한 라이센스에 기술된 권리 정보를 검사하여 요청한 명령에 대한 권리 내용을 포함하고 있는지를 확인한다. 마지막으로, 다운로드 된 라이센스에 해당되는 콘텐츠 파일은 라이센스 파일로부터 추출된 복호화 키정보를 사용하여 암호화된 스트림을 복호화 하게 된다. <그림 3>은 STB에서 라이센스를 이용한 콘텐츠 재생과정을 나타낸다.

STB는 다운로드 된 라이센스 파일을 먼저 STB의 개인키로 복호화하고 파싱 된 정보로부터 해당 라이센스가 정당한 라이센스인지를 확인한다. 또한 라이센스에 기술된 권리 정보를 검사하여 요청한 명령에 대한 권리 내용을 포함하고 있는지를 확인한다. 마지막으로, 다운로드 된 라이센스에 해당되는 콘텐츠 파일은 라이센스 파일로부터 추출된 복호화 키정보를 사용하여 암호화된 스트림을 복호화하게 된다.



<그림 3> 녹화 콘텐츠 재생 방법

VI. 일반적 고려사항

셋탑박스는 PC만큼 사용자에게 다양한 제어 수단을 허용하지 않기 때문에 보안적인 측면에서 PC보다 안전하다고 할 수 있으나 여전히 내부적인 처리를 수행하는 소프트웨어 모듈과 중요한 데이터가 일시적으로 저장되는 메모리 부분에 대한 보호가 필요하다. 예를 들어서, CAS를 통하여 역스크램블된 스트림이 암호화 모듈을 가장한 소프트웨어 모듈에 의하여 캡쳐될 수도 있으므로 스트림 데이터를 주고받기 전에 반드시 수신 모듈과 암호화 모듈 사이에 인증이 이루어져야 하며, 스트림 데이터 처리중 발생하는 임시 데이터 버퍼에 불법적인 접근을 막기 위하여 TRS(Temper Resistant Software) 기술이 필요하다. 또한 암호화에 사용되는 키정보가 셋탑박스 내부에서 생성되므로 스트림 암호화가 종료되기까지 이러한 키정보를 안전하게 유지할 필요가 있다.

라이센스 다운로딩을 위하여 셋탑박스에서 리턴채널을 통하여 라이센스 서버와 통신을 할 때, 사용자 정보 및 라이센스를 안전하게 전송하기 위하여 보안 프로토콜(IPSEC, SSL, etc.)을 사용할 수 있어야 한다.

V. 결 론

인터넷 환경에서의 디지털 콘텐츠 서비스는 그 역사가 짧지만 다양한 비즈니스 모델과 유통 프레임워크가 이미 개발되어 실제 서비스에 적용하고 있다. 그러나, 방송 서비스는 상대적으로 긴 역사에도 불구하고 초기 방송 모델에서 서비스의 다양성을 크게 넓히지 못하고 있다. 이는 그동안 방송의 개념이 무차별적이며 일방적인 서비스이어 왔기 때문일 것이다. 그러나 차세대 셋탑박스에서는 디지털 콘텐츠와 메타데이터를 처리할 수 있는 능력을 갖게 되며 기본적으로 리턴채널을 통하여 인터넷에 얼마든지 접속할 수 있는 환경이 갖추어지게 된다. 따라서 아직까지는 방송 채널을 통해서만 실시간으로 제공이 가능한 고품질의 디지털 콘텐츠와 메타데이터를 이용한 편리한 사용자 환경, 그리고 리턴채널을 통한 서버와의 사용자 인터액티버티에 힘입어 앞으로의 방송 서비스는 현재 인터넷에서의 콘텐츠 제공서비스를 능가하게 될 것이다. 그러나 이러한 서비스도 인터넷 환경의 DRM과 같은 방송 환경에 적합한 방송 콘텐츠 보호 방안이 제공되어야만 가능하다. 본 논문에서는 방송 환경의 특징과 기존 방송 서비스 형태 및 방송 콘텐츠의 포맷 등을 고려한 방송 콘텐츠에 대한 보호 방법을 제안하였다. 이러한 방송 콘텐츠 보호 방법은 CAS의 보호 범위 밖에 있는 콘텐츠 저장 시점에서부터 시작되며, 기존의 방송 프레임워크에 크게 영향을 주지 않는다. 또한 본 보호 방법을 적용하여 저장된 방송 콘텐츠는 다른 사용자와 공유가 가능하므로 P-to-P를 이용한 비즈니스 모델에 적용이 가능하다. 따라서 본 방송 콘텐츠 보호 메커니즘을 적용한다면, 그 동안 광고 수입 또는 채널 가입에 따른 수익에만 의존하던 방송사에게 새로운 수익모델을 제시할 수 있을 것으로 기대한다.

참고 문헌

[1] TALISMAN final report, ACTS Project Number AC019, Sept. 1995.

[2] OPIMA, 2000. OPIMA Specification Version 1.1.

[3] Digital Video Broadcasting(DVB): Support for use of scrambling and Conditional Access(CA) within digital broadcast systems, ETSI(Informative), ETR289ed.1, Oct. 1996.

[4] Digital Video Broadcasting(DVB): DVB SimulCrypt;Part1;Head-end architecture and synchronization, TS101 197-1 v1.1.1, Jun, 1997.

[5] Kang hogap, Fasoo.com presentation document, pp.23, 2003

[6] ISO/IEC JTC1 SC29 WG11 N4701, ISO/IEC 13818-1:2000 PAMD2, March, 2002.

[7] The Electronic Media Management System from IBM, http:// www-3.ibm.com/ software /data/cm/attach/emms_v2_1_4_ brochure.pdf