DRM을 적용한 소규모 제한수신시스템 설계

정회원 정 석 원*

Design of a Small Conditional Access System with DRM

Seok Won Jung* ***Regular Member***

요 약

디지털 방송 서비스는 위성 서비스를 시작으로 지상파와 케이블 방송으로 확산되고 있는 실정이다. 아날로그 방송에서 디지털로 변함에 따라 다채널화, 고품질화, 다기능의 서비스를 가능하게 하고 있으며, 새로운 형태의 비지니스를 창출해 내고 있다. CAS는 디지털 방송 콘텐츠의 불법적인 사용자의 접근을 방지하기 위한 기술로 1990년대 초반부터 유럽 및 미국의 디지털 위성 방송 서비스에 적용되던 것이 국내에서는 2002년에 디지털 위성 방송 서비스에 적용되었다. DRM은 CAS와 달리 디지털 콘텐츠 자체의 지적 자산과 저작권을 보호하는 기술이다. 본 논문은 DRM 기술을 CAS와 별도로 구성하는 것이 아니라 CAS의 기존 체계에 DRM 중 몇 가지 요구사항을 적용한 시스템 설계를 제안한다. 이는 소규모 방송 사업자 용 CAS 시스템에 적용될 수 있을 것이다.

Key Words : Conditional Access System, Digital Rights Management, Digital Video Broadcasting

ABSTRACT

Digital Broadcasting Services get abroad from satellite services to terrestrial services and cable services. As broadcasting services become digital from analog, diverse services such as multi-channel, high quality, time-shift function and so on can be possible. It also generates new digital businesses. The Conditional Access System(CAS) is a technology for providing prevention of illegal access to digital contents. It was applied to digital satellite services at Europe and America from the beginning of 90's. In 2002, a domestic digital satellite service provider adopt a CAS system to their broadcasting services. DRM technologies protect intellectual properties and digital rights of digital contents. This paper suggests a design method to construct a CAS system with DRM which can be applied to a CAS for a small digital broadcasting service.

Ⅰ. 서 론

방송의 디지털화는 아날로그와 달리 한 채널에 한 프로그램을 실어 보내는 대신에 고품질의 여러 프로그램을 실을 수 있게 되었으며, 유료방송, 양방향 서비스 등 이전의 아날로그 방송과는 다른 다양한 서비스를 가능하게 해주고 있다. 디지털 방송 서비스는 지상파 방송이나 케이블 방송에 비해 위성방송에서 먼저 시작하여 서비스 확장에 노력하고 있는 분야이다. 일본의 PerfectTV, 미국의 DirecTV, 유럽의 BskyB와 Canal Satellite 등 많은 방송 서비스 업체들이 비디오/오디오 서비스 이외에 데이터 방송 기술을 이용한 대화형 방송 서비스까지 제공하고 있는 실정이다. 우리나라에서는 한국디지털 위성방송에서 유럽 표준의 DVB(Digital Video Broadcasting)를 바탕으로 대화형 방송 서비스를 제공하고 있다.[1]

최근 국내에서는 통신산업이 IT와 인터넷을 매개로 한 디지털화 및 사회전반의 정보화를 가속화하

※ 본 논문은 2004학년도 목포대학교 신진교수연구비 지원에 의하여 연구되었음.
* 국립목포대학교 정보보호전공(jsw@mokpo.ac.kr)
논문번호 : KICS2007-05-202, 접수일자 : 2007년 5월 2일, 최종논문접수일자 : 2007년 9월 21일

고 있는 가운데 방송과의 융합기술인 DMB(Digital Multimedia Broadcasting) 서비스가 시작되었다. 또한 케이블 방송의 디지털화가 제도적인 정비를 마련하며 다양한 부가 서비스를 제공하려고 준비하고 있는 단계이다.

방송의 디지털화에 따라 고품질과 다기능 제공은 서비스의 유료화를 통한 다양하고 새로운 비지니스 모델을 창출하게 하였고, 이를 위해서는 정당한 가입자에게만 유료 방송을 볼 수 있게 하는 기술이 필요하게 되었다. 이러한 요구사항을 충족하는 기술 중 하나가 제한수신시스템(CAS; Conditional Access System)이며, 1990년대 초반부터 유럽에서 디지털 위성을 중심으로 발전하고 있다. NDS, Irdeto, France Telecom 등 여러 업체가 CAS를 개발하여 상용화하였으며, 현재까지 미들웨어를 통한 양방향 서비스, 데이터 서비스 등 여러 가지 기능을 추가하며 발전을 시키고 있다. 국내에서도 2002년부터 (주)스카이라이프가 디지털 위성방송에 CAS를 적용하여 서비스를 하고 있다.[1]

1997년 미국의 InterTrust 사에 의해 디지털 콘텐츠에 대한 지적 자산 및 저작권을 보호하기 위한 솔루션으로 DRM(Digital Rights Management) 기술이 처음 소개된 이래 InterTrust, ContentGuard, Magex 등 여러 업체에서 DRM 솔루션을 제시하고 있다.[2] 그러나 시장을 확산해 가면서 이들 업체간의 DRM 솔루션의 호환성 결여와 시장 미성숙 등의 요인으로 인해 최근에 MPEG-21, OMA, DVB-CPCM, OpenCable, TV-Anytime, XrML 등에서 국제표준화 작업이 활발히 이루어지고 있는 실정이다.[2]

본 논문은 DRM에 대한 표준화가 아직 완전히 이루어지지 않고, 디지털 방송 서비스에 CAS가 적용되고 있는 시점에서 DRM 시스템을 새로이 설치하기에 부담이 있는 소규모 디지털 방송 서비스 업체에게 DRM 기능이 있는 CAS를 제공하려는 데 목적이 있다. 본 논문에서는 소규모 디지털방송 시스템용 CAS를 설계할 때, DRM의 몇 가지 요구사항을 적용하여 구현할 수 있는 EMM(Entitlement Management Message)과 ECM(Entitlement Control Message) 메시지 구조를 제안한다. 그리고 방송사업자와 사용자 사이 또는 사용자 간에 DRM 기능을 제공하기 위한 프로토콜을 제시하고 이의 안전성을 알아본다.

Ⅱ. 제한수신시스템의 구조

디지털방송용 제한수신시스템(Conditional Access System; CAS)은 방송 서비스 제공자가 제공하는 디지털 멀티미디어 방송 프로그램을 정당한 가입자만 시청할 수 있도록 하는 시스템이다. 이와 같은 서비스를 제공하기 위하여 서비스 제공자에 의하여 제공되는 비디오, 오디오, 그리고 데이터 신호들은 스크램블 되어 전송된다. 즉, 정당한 접근 자격을 갖지 못한 사용자가 방송되는 서비스를 임의로 취득했을 때 이 방송 서비스를 시청할 수 없도록 만드는 것이다. 방송 서비스 가입자는 방송되는 서비스에 대한 정당한 접근 자격을 획득한 후 수신한 스크램블된 스트림들을 디스크램블 과정을 거쳐 프로그램을 정상적으로 시청한다.

디지털 멀티미디어 위성방송시스템은 그림1과 같이 인코더, 다중화기, 변조기, 송출기, 수신기, 스마트카드 등으로 구성된다(디지털 케이블 방송시스템도 비슷한 구성을 가지며, 스마트카드 대신에 PCMCIA 모듈을 가지는 경우가 있다). 비디오, 오디오, 데이터 스트림은 인코더를 거쳐 MPEG-1 또는 MPEG-2 기술로 압축이 되고, 전송(Transport Stream; TS) 패킷으로 변환되고 다중화기(MUX; Multiplexer)를 통해 일렬로 재정렬 된다. TS 패킷은 변조기(Modulator)를 통해 전기적인 신호로 변조되고 위성 송출기를 통해 가입자용 수신기로 전달된다. 수신기는 위성을 통해 전달된 TS 패킷들 중 가입자가 선택한 이벤트에 해당하는 비디오와 오디오 스트림을 선택 재생하여 수상기를 통해 시청자에게 보여준다.

방송되는 또는 방송될 이벤트에 대한 정보는 EIS(Event Information System)를 통해 수신기로 전달되고, 이는 특정 채널을 통해 가입자에게 전달되며 방송 스케줄을 알려주는 역할을 한다.

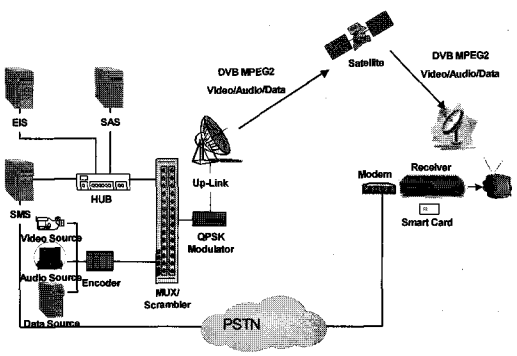


그림 1. 디지털 멀티미디어 위성방송시스템

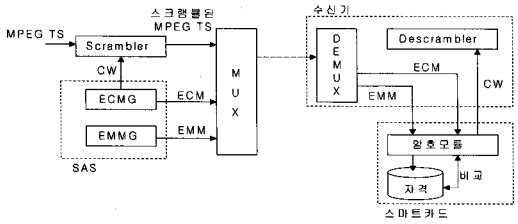


그림 2. CAS 메시지 흐름도

SMS(Subscriber Management System)는 가입자의 기본 정보와 CAS 관련 가입자 정보를 저장하고 이를 SAS로 제공하는 역할을 한다.

SAS(Subscriber Authorization System)는 CAS의 부분 시스템으로 그림 2와 같이 방송 스트림의 스크램블링 제어를 담당하는 ECMG(Entitlement Control Message Generator)와 가입자의 권한 정보를 만드는 EMMG(Entitlement Management Message Generator)로 구성된다. ECMG는 프로그램에 대응하는 제어단어 CW(Control Word)를 만들어 스크램블러에 이를 제공한다. 스크램블러는 제어단어를 스크램블 알고리즘 S의 키로 사용하여 방송스트림을 S_{CW}(방송스트림)로 암호화하여 방송스트림을 자격을 갖지 못한 시청자가 접근할 수 없도록 하는 역할을 담당한다. 또한 ECMG는 이벤트의 접근조건과 제어단어를 키 ECK와 암호 알고리즘 E를 사용하여 E_{ECK}(접근조건, CW)로 암호화하여 ECM 메시지로 만들어 가입자에게 전송하는 역할을 담당한다. EMMG는 가입자가 방송 스트림에 접근할 수 있는 자격에 대한 정보를 키 EMK와 암호 알고리즘 E를 사용하여 E_{EMK}(자격)으로 암호화하여 EMM 메시지에 담아 가입자에게 전송한다. 가입자의 스마트카드는 이를 받아 복호화 알고리즘 D와 키 EMK를 이용하여

$D_{EMK}[E_{EMK}(\text{자격})] = \text{자격}$

으로 복호화 한다. 복호화된 이벤트 접근 자격은 스마트카드의 내부에 저장을 한다. 가입자가 수신기를 통해 스크램블된 이벤트에 접근을 시도하면, 수신기는 이벤트에 해당하는 ECM 메시지를 스마트카드로 보낸다. 스마트카드는 ECM 메시지를 복호화 알고리즘 D와 키 ECK를 이용하여

$D_{ECK}[E_{ECK}(\text{접근조건, CW})] = \text{접근조건, CW}$

으로 복호화 한다. 복호화한 후 얻은 접근 조건과 스마트카드 내부에 저장된 자격권한을 비교하여 이 벤트에 접근할 수 있는가를 먼저 판단한다. 이벤트에 접근을 할 수 있는 자격이 있는 경우 ECM의 복호화에서 얻은 제어단어 CW를 수신기의 디스크램블러로 전송한다. 수신기는 제어단어를 디스크램블링 알고리즘 T의 키로 제공하여 방송 스트림을

$T_{CW}[S_{CW}(\text{방송스트림})] = \text{방송스트림}$.

으로 복호화 하고, 복호화 된 방송 스트림을 디코딩하여 텔레비전 수상기로 보여준다.

Ⅲ. 저작권보호 기술

90년대 말, 인터넷을 통한 디지털 콘텐츠 유통산업의 발달과 더불어 디지털 콘텐츠의 불법복제로 인한 저작권 침해를 방지하기 위한 DRM 기술이 여러 회사들에 의해 독자적으로 발표되었다. 그러나 2000년을 전후로 DRM 기술에 대한 상호 호환성 보장에 대한 문제가 제기되어 OeBF(Open e-Book Forum), DVD 포럼, MPEG-21 등 다양한 표준화 단체들이 이러한 문제를 해결하기 위해 현재까지 노력 중 이다. 또한 디지털 방송 콘텐츠의 보호를 위해 ATSC(Advanced Television Systems Committee), CableLabs, DVB 등에서도 MPEG-2 TS 기반의 CAS 규격과 셋톱박스의 복제방지를 위한 기술 규격을 마련하였다. 셋톱박스로 수신된 방송콘텐츠를 DVD 녹화기 또는 PVR과 같은 기록장치를 통해 불법 복제하는 것을 방지하기 위해 4C Entity에서는 CPPM/CPRM 기술을 내놓았다.[5][6]

DRM은 콘텐츠의 정보를 허가되지 않은 사용자로부터 보호하기 위해서 암호화 기술을 사용하며, 정당한 사용자가 암호화된 콘텐츠를 복호화할 수 있도록 키를 생성하고 분배하는 등의 키 관리 기술이 필요하다. 또한 디지털 콘텐츠의 유통 및 관리가 지엽적인 범위에서만 국한되지 않고 범용적인 도메인에서 적용 가능하기 위해서 표준적인 콘텐츠 식별체계를 갖출 필요가 있다.

콘텐츠의 사용권한은 재생, 보기, 출력 등 사용자에게 콘텐츠가 표현되고 이용되는 권리 형태를 정의하는 표시 권한(Render Permission)이 있고 복사, 이동, 대여 등 사용자들 사이에 권리의 교환이 이루어지는 권리형태를 정의한 전이 권한(Transport Permission)이 있다. 그리고 추출, 수정, 추가 등 콘텐츠의 내용 자체를 변형할 수 있는 권한을 정의하는 변형 권한(Derivative Permission)이 있다. 콘텐츠의 사용조건으로는 사용기간, 사용회수, 사용 내역 추적, 사용 지역 등이 있을 수 있다.

콘텐츠에 대한 권리는 사용권한과 사용조건의 조합으로 구성되며, 기계가 인식할 수 있는 형태로 기

술되어 사용자에게 전달되게 된다. 이때 권리표현 방식은 XML 기반이나 파라미터 형태로 구성된다. XML 기반은 확장성이 우수한 반면 구현이 어려운 점이 있고, 파라미터 방식은 구현이 간단하나 확장성이 없는 특징이 있다.

최근 모바일 시장의 급속한 성장과 셋톱박스 기반의 VOD 서비스, 디지털 방송, 디지털 홈 서비스 등 광대역 기반의 멀티미디어 콘텐츠에 대한 DRM 기술의 요구 증대로 OMA(Open Mobile Alliance), MPEG-21 등의 표준화 활동이 두드러지고 있는 실정이다.

Ⅳ. DRM을 위한 CAS 메시지 구조 및 보안 프로토콜 제안

CAS는 정당한 자격을 가진 가입자만 방송을 시청할 수 있도록 하는 목적을 가지고 있다. 따라서 정당한 자격을 가진 사람은 디지털 멀티미디어 스트림들을 개인용 저장장치인 PVR(Personal Video Recorder)에 저장해 두었다가 재시청을 할 수 있으며 법에 규정되어 있지 않으면 이는 불법이 된다.

본 장에서는 수신기로부터 SAS로 시청내역을 전송하는 리턴 채널이 없는 소규모 CAS가 적용된 방송시스템에서 DRM의 일부 기능을 구현하는 방법에 대해서 알아본다. 소규모 방송 사업자에게는 부당한 사용자의 방송시청과 정당한 사용자 또는 부당한 사용자의 디지털콘텐츠의 불법복제가 큰 문제를 가져올 수 있다. 따라서 정당한 사용자만 시청이 가능하도록 하는 CAS 시스템의 도입과 저작권을 보호하기 위한 DRM의 도입을 고려해야 한다. 그러나 소규모 가입자와 적은 채널 수를 가지고 몇 가지 간단한 방송 서비스를 제공하는 방송사업자가 CAS와 DRM 두 시스템을 각각 구입하는 것은 무리가 있다. 본 논문은 이런 여건의 방송 사업자에게 CAS과 DRM을 동시에 제공하려고 하는데 목적이 있다. 방송사업자는 수신기로부터 SAS로 시청내역을 전송하는 리턴 채널이 없는 소규모 CAS를 원하거나 이러한 CAS를 가졌다고 가정하자. 그리고 수신기는 스트림을 저장할 수 있는 개인용 저장장치와 ECM과 EMM 메시지를 분석할 수 있는 스마트카드를 가지고 있다고 하자.

4.1 DRM 조건을 가진 ECM 구조

ECM 메시지는 일반적으로 그림 3과 같은 내용을 갖는 구조를 내부에 가지고 있다.

이벤트ID	접근조건	evenCW|| oddCW	해쉬값

그림 3. 일반적인 ECM 메시지 구조

이벤트 ID는 각 이벤트의 식별자이고, 접근조건은 CAS의 제공 서비스의 종류에 따라 그 값이 결정된다. 예를 들어 CAS가 프로그램 패키지 서비스를 하고, 이벤트 당 PPV(Pay-per-view) 서비스를 제공한다면 프로그램 패키지의 식별자와 이벤트의 가격이 접근조건이 된다. 제어단어는 수신기에서의 동기화를 위해서 evenCW와 oddCW 두 쌍씩 전달되어야 한다. 그리고 해쉬값을 포함하여 전달되는 ECM 메시지는 무결성을 확보한다. 또한 제공되는 접근조건과 제어단어는 이벤트에 대한 접근 자격이 없는 시청자가 알 수 없도록 암호화를 하여 전달되어야 한다. 이때 사용되는 암호화키를 ECK(Entitlement Control Key)라 한다. 제어단어는 보안상의 이유로 5~10초에 한 번씩 바뀌어 전송되고, ECK는 방송 서비스 제공자가 원하는 시점에 바꿀 수 있어야 한다.

수신기로 전송되어오는 방송 스트림 중 스크램블된 스트림은 Demux를 거쳐 비디오, 오디오, 데이터, PSI/SI 테이블 정보, ECM, EMM 데이터로 나누어진다. 이 중 ECM은 스크램블된 스트림을 디스크램블할 수 있는 제어단어를 가지고 있다. 따라서 스크램블된 스트림을 저장장치에 저장하여 두었다가 재생해서 보려고 한다면, 스크램블된 스트림들과 ECM 메시지를 전송되어 오는 순서대로 저장하여 두면 된다. 그러나 스마트카드 내에서 ECM 메시지를 복호화하기 위해서는 ECM 메시지를 암호화할 때 사용된 ECK를 사용해야 하는데 ECK는 위에서 설명했듯이 변경될 수 있다. 이 경우 저장된 스크램블된 스트림을 재생하기 위해 저장되어 있는 ECM 메시지를 스마트카드로 보내면 스마트카드 내의 ECK가 기존의 ECK와 다르기 때문에 제어단어를 복호화하는데 실패하게 된다. 따라서 저장된 스크램블된 스트림을 재생하기 위해서는 그림 4와 같이 ECM 메시지 내에 DRM에 관한 조건을 가지는 영역이 필요하다. DRM의 조건에는 현재 스크램블에 사용되고 있는 제어단어의 회수, 이벤트 전체에 사용되는 제어단어의 개수, 이벤트에 사용되고 있는 ECK에 대한 식별자 등을 포함한다. DRM 조건은 암호화하지 않는다. 또한 스마트카드는 이벤트에 대한 ECK를 식별자와 함께 저장하고 있어야 하며 새로운 ECK를 저장할 때 이전의 ECK를 지워서는 안 된다. 그림 4의 접근조건과 제어단어는 ECK를 이용하여 암호화한다.

이벤트ID	DRM 조건	접근조건	제어단어	해쉬값

그림 4. DRM 조건을 갖는 ECM 구조

저장된 스크램블된 스트림을 재생하기 위해서는 저장하고 있는 ECM 내의 접근조건과 스마트카드 내에 저장되어 있는 자격이 일치해야만 제어단어의 복원이 가능하다. 재생하는 시점이 이벤트를 방송하던 시점과 달라져 있으므로 스마트카드에 저장되어 있는 이벤트에 대한 자격조건이 달라져 있을 수 있다. 따라서 스마트카드는 사용자의 자격조건이 새로 갱신될 때 이전의 자격조건을 지우지 않고 저장해 두어야 한다. 그러면 저장된 스트림을 재생하여 보려고 할 때 스마트카드에 저장되어 있는 자격조건들을 비교하여 만족할 때 디스크램블이 되고 그렇지 않은 경우에는 디스크램블이 되지 않는다. 스마트카드 내의 자격조건은 DRM 권한의 기한 동안 저장해 둔다.

4.2 EMM 내의 DRM 자격

CAS의 서비스는 일반적으로 패키지가입(subscription per class), 주제와 등급별 가입(subscription per theme and level), 예약 PPV(pre-booked pay-per-view), PPV(pay-per-view), IPPV(impulse pay-per-view) 등으로 나눌 수 있다(서비스에 대해 일반적으로 사용되는 용어는 없다). CAS는 가입자에게 이러한 서비스를 제공하기 위해서 EMM 메시지로 이벤트에 접근할 수 있는 자격을 개인별 또는 가입자 그룹별로 전송한다.

기존의 CAS는 스마트카드에 저장된 자격이 없어지지 않는 한 이벤트를 저장하여 두었다가 계속해서 볼 수도 있으며, 저장한 스트림을 같은 자격을 소유한 다른 이에게 재분배 할 수도 있다. 즉, 디지털 스트림에 대한 소유권리가 방송 서비스 제공자로부터 완전히 가입자에게 이양되어 저작권의 침해가 될 수 있음을 뜻한다.

우리는 기존의 CAS의 기능에 다음과 같은 내용의 저작권 관리 요구사항을 추가한다.

- 이벤트를 지정한 회수만큼 보기
- 이벤트의 재분배(한 번 보기)

이들에 대한 서비스제공은 가입자가 서비스를 신청할 때 가입자가 설정할 수 있도록 하고, 이에 대한 자격을 EMM 메시지로 전송하여 준다. 일반적으로 EMM 메시지 내의 자격들은 TLV(tag-length-value) 형태로 전달되므로 위와 같은 서비스를 추가하기 위한 자격 역시 TLV 형태로 정의를 하면 쉽게 기존의 CAS를 확장할 수 있다.

4.3 이벤트 지정한 회수만큼 보기

이벤트를 못 보게 하는 것은 이벤트의 접근 자격을 갖지 못하게 하면 볼 수 없는데 이는 CAS의 고유 기능 중 하나이다. 이벤트를 보는 자격은 CAS 서비스를 신청하면 얻을 수 있다. 자격을 얻은 가입자는 이벤트를 최소한 한 번은 볼 수 있게 된다.

1) 한 번 보기 DRM 자격을 가진 경우

가입자가 DRM 자격으로 한 번만 보기를 선택하여 스마트카드 내에 이 DRM 자격을 가지고 있다고 하자. 이 경우 가입자는 이벤트를 보면서 동시에 스크램블된 이벤트를 PVR에 저장할 수 있다. 이때 이벤트를 보았다는 것을 확인하지 않으면 PVR에 저장된 이벤트를 다시 볼 수 있게 된다. 일반적으로 이벤트를 보았다는 것은 이벤트의 마지막까지 보았다는 것을 뜻할 것이다. 그런데 이벤트의 마지막 스트림을 보았을 때를 한 번 본 것으로 확인한다면 악의적인 의도를 가진 가입자는 맨 마지막 스트림을 보기 전에 방송 보기를 취소하여 한 번 본 것에 대한 것을 확인할 수 없을 것이다. 그래서 ECM 내 DRM 조건에

- 현재 스트림을 스크램블하고 있는 제어단어의 회수 numberInDrm
- 전체 사용되는 제어단어의 개수

를 넣어 보내고, 스마트카드는 ECM에서 제어단어를 복원해낼 때 마다 현재까지 본 제어단어의 회수 numberInS = numberInDrm을 갱신하여 저장하고 이 값을 이용하여 이벤트를 다 보았는가를 확인할 수 있다. 스마트카드 내의 EEPROM에 이를 저장해야 하는데 회수의 갱신은 상당히 많은 EEPROM 쓰기 행위가 이루어지므로 같은 메모리 번지에 계속 쓰게 해서는 안된다.

이벤트를 끝까지 다 본 경우 스마트카드는 이벤트 식별자 eventIDInS, ECK 식별자 ECKIDInS, 본 제어단어의 회수 numberInS, 본 회수 countInS에 대한 자료를 저장한다.

가) 한 번 끝까지 다 본 경우

저장되어 있는 이벤트를 다시 보려고 할 경우의 절차는 다음과 같다.

단계 1) 수신기는 이벤트에 해당하는 첫 번째 ECM 메시지를 스마트카드에 전달한다.

단계 2) 스마트카드는 ECM 내 DRM 조건에 있는 ECK 식별자 ECKID를 보고 스마트카드 내에 저장되어 있는 복호화 키를 ECK를 찾는다. DRM 조건에 ECK의 식별자를 두는 것은 1절에서 설명했듯이 공중파나 위성을 통해 방송되고 있는 이벤트

의 ECM을 암호화하는데 사용하는 키와 재생해서 보려고 하는 저장하고 있는 스트림의 ECM을 암호화할 때 사용했던 키가 다를 수 있기 때문이다.

단계 3) ECM 내에는 암호화된 E_{ECK}(접근조건, CW)를 복호화하여

$D_{ECK}[E_{ECK}$(접근조건, CW)]=접근조건, CW

를 얻는다.

단계 4) 스마트카드는 ECM 내 DRM 조건과 저장되어 있는 DRM 자격 그리고 이벤트를 본 이력을 비교해본다.

단계 5) 본 회수 countInS=1로 되어있기 때문에 볼 수 없음이라는 메시지를 수신기에게 보낸다.

단계 6) 수신기는 가입자에게 한 번 보았기 때문에 더 이상 볼 수 없음을 알려준다.

나) 한 번 끝까지 다 못 본 경우

이벤트의 끝까지 다 못 보고 저장해 둔 스트림을 재생해서 보려고 하는 경우의 절차는 다음과 같다.

단계 1) 수신기는 이벤트에 해당하는 첫 번째 ECM 메시지를 스마트카드에 전달한다.

단계 2) 스마트카드는 ECM의 eventID의 값으로 저장하고 있는 본 회수 countInS를 확인한다. 이벤트를 다 안 보았기 때문에 count=0 이다.

단계 3) 스마트카드는 ECM 내의 DRM 조건 중 제어단어의 회수 numberInDrm=1의 값과 스마트카드 내 저장하고 있는 본 제어단어 회수 numberInS를 비교한다.(numberInS ≥numberInDrm 이다.)

단계 4) 스마트카드는 numberInS를 수신기로 보낸다.

단계 5) 수신기는 저장되어 있는 ECM의 DRM 조건을 보고 numberInDrm의 값이 numberInS 인 ECM을 찾는다.

단계 6) 수신기는 찾은 ECM을 스마트카드로 보내고, ECM에 해당하는 스트림을 찾아 디스크램블러로 보낸다.

단계 7) 스마트카드는 ECM 내 DRM 조건에 있는 ECK 식별자 ECKID를 보고 스마트카드 내에 저장되어 있는 복호화 키를 ECK를 찾는다.

단계 8) ECM 내에는 암호화된 E_{ECK}(접근조건, CW)를 복호화하여

$D_{ECK}[E_{ECK}$(접근조건, CW)]=접근조건, CW

를 얻는다.

단계 9) 복호화한 접근조건과 스마트카드 내 ECMID와 같이 저장된 자격을 비교한다.

단계 10) 제어단어 CW를 수신기로 보낸다.

2) 여러 번 보기 DRM 자격을 가진 경우

지금까지는 한 번만 보기 DRM 자격일 때 시스템의 동작을 설명하였다. 이를 확장하면 다음과 같이 여러 번 보기도 가능하다. 스마트카드 내에 DRM 자격으로 여러 번 보기 회수가 저장되어 있다고 가정하자. 위에서 설명한 한 번 보기처럼 이벤트를 볼 때마다 제어단어의 회수와 본 회수를 저장해 둔다. 위에서 설명한 방법에 따르면 보지 못한 나머지 부분을 보아야만 다시 처음부터 볼 수 있게 되는데 만약 가입자가 처음부터 보기를 원한다면 수신기에 맨 처음부터 보기라는 명령을 내리고, 수신기는 보지 못한 이벤트 스트림의 마지막에 해당하는 ECM을 전송하여 스마트카드 내의 보기 회수를 증가시키고 제어단어의 회수를 초기화시킨다. 그리고 다시 맨 처음 스트림과 ECM을 가지고 이벤트를 볼 수 있도록 한다. 만약 보기 회수를 넘어 이벤트 보기를 시도하는 경우 스마트카드는 새로 받은 ECM과 저장되어 있는 DRM 자격을 비교하여 더 이상 볼 수 없음을 판다하고 이 사실을 가입자에게 알려준다.

4.4 이벤트의 재분배

저장되어 있는 스크램블된 이벤트를 다른 이에게 재분배를 하려고 하면 가입자가 재분배에 대한 자격을 가지고 있어야 한다. 그리고 받으려고 하는 가입자는 그 이벤트를 볼 자격을 가지고 있지 않은 경우일 것이다. PVR에 저장되어 있는 스크램블된 자료들은 언제든지 아무에게나 복사하여 보내줄 수 있다. 그러나 스크램블된 이벤트를 보려고 하면 ECM을 복호화하여야 하고, 이벤트를 볼 수 있는 자격을 가지고 있어야 한다. 그래서 이벤트의 재분배를 위해서는

- 재분배하려는 가입자의 스마트카드 인증,
- 이벤트 보기 자격 전송,
- ECK 키 전송,
- 방송 스트림 전송

이 필요하다.

일반적인 두 가입자가 위에 나열한 조건을 주고받으려면 두 가입자가 공유하고 있는 키를 바탕으로 해야 한다. 여기에서는 두 사람이 같은 방송사업자가 운영하는 서비스에 가입하고 있다고 가정하자. 다만 한 가입자가 이벤트에 대한 접근권한이 없는 경우이다(이미 방송된 이벤트를 보고 싶을 때 방송사업자로부터 권한을 받고 이벤트를 보내달라고 하는 것은 비용이 비싸기도 하고 방송 운용상 어려움이 있다. 따라서 이벤트를 방송사업자로부터 받아볼 수 없을 때 이벤트를 저장하고 있는 다른 가입자로

부터 전송받아 보려는 경우를 생각할 수 있다).

자격을 보내는 스마트카드 SC1과 자격을 받는 스마트카드 SC2는 같은 멀티미디어 방송서비스를 받고 있고 있기 때문에 EMM 메시지를 암호화 또는 복호화할 때 사용하는 EMK(Entitlement Management Key) 키를 공통적으로 가지고 있다. 이 키를 기반으로 세션키를 만들어 두 스마트카드를 인증하고 자격을 담은 EMM을 생성하여 주고받는다.

그림 5와 같이 권리를 받으려는 SC2는 자신만이 받을 수 있는 EMM 메시지를 위해서 가입자의 개인 주소인 SC2_ADDR과 세션키를 만들 때 사용할 난수 R1을 만들고, 이들을 두 스마트카드가 공통적으로 가지고 있는 EMK로 암호화하여 SC1으로 E_{EMK}(SC2_ADDR, R1)을 전송한다. SC1은 EMK로 $D_{EMK}E_{EMK}$(SC2_ADDR, R1) = SC2_ADDR, R1을 복호화하고 SC2_ADDR은 나중에 SC2에게 보낼 EMM을 만들기 위해서 저장한다. SC1은 난수 R2를 생성한 후 세션키 SK를 R1과 R2의 배타적논리합(XOR)으로 만든다. SC1은 자신이 정당한 스마트카드라는 것을 알리기 위해 SC2로부터 받은 SC2_ADDR을 EMK로 암호화하고, SC2가 세션키를 만들 수 있도록 자신이 만든 난수 R2를 암호화하여 E_{EMK}(SC2_ADDR, R2)를 보낸다. SC2는 받은 메시지를 EMK를 이용하여

$D_{EMK}E_{EMK}$(SC2_ADDR, R2) = SC2_ADDR, R2

로 복호화한다. SC2_ADDR 값으로 SC1을 인증하고, 복원한 R2와 자신이 만든 난수 R1을 가지고 세션키 SK를 만든다. SC1은 이벤트에 대한 보기 자격을 세션키 SK로 암호화하여 EMM 메시지를 만든다. 이때 SC2 만이 받아볼 수 있도록 EMM 메시지 내에 SC2_ADDR을 넣어 만든다.

SC2는 SC1으로부터 전달받은 스크램블된 이벤트를 볼 자격이 없었으므로 SC2 내에는 ECM을 복호화할 ECK를 가지고 있지 않다. 따라서 SC2로 전달되는 EMM은 스크램블된 스트림을 복호화할 때 사용하는 ECK를 포함하고 있어야 한다. 따라서 EMM 메시지의 형식은 대략 다음과 같다.

EMM = E_{SK}(SC_ADDR, 자격, ECK, 해쉬값)

SC2는 세션키 SK로 EMM을 복호화한 후 스마트카드 내에 볼 자격과 ECK를 저장한다. 이벤트를 볼 권리를 이양 받은 SC2는 스크램블된 스트림을 3절에서 설명한 방법으로 볼 수 있게 된다.

스마트카드 SC1 내의 자격이 SC2로 이전이 되고나면 SC1 내의 DRM 자격은 없어져야 한다. DRM 자격은 EMM을 만든 후 SC1 내에서 없어지고 난 후 EMM 자격이 전송되어야 한다. 자격을 SC2로 보냈다는 로그를 이벤트 식별자 eventID와 SC2_ADDR과 함께 남기는 것이 좋다.

정당하지 않은 스마트카드 SC2는 EMK를 가지고 있지 않기 때문에 세션키 SK를 만들 수 없고, 자격이 담긴 EMM을 복호화할 수 없어 저장된 이벤트의 재생을 할 수 없다.

그림 5의 프로토콜은 SC2에 대한 인증은 포함하고 있지 않다. 즉, 정당하지 않은 가입자가 스마트카드 SC2를 위장하여 임의의 값을 정당한 스마트카드 SC1으로 전송한다. 이 경우, SC1은 임의의 값을 EMK로 복호화한 후 개인주소에 해당하는 값 SC2_ADDR을 만들지만 이는 정당한 가입자의 개인주소가 아니다. 수신기는 SC2의 개인주소를 얻어오고, 이 값을 위의 복원값과 비교하여 SC2의 인증을 시도한다. 이 방법을 사용하면 위장 SC2에 의해 정당한 스마트카드 SC1 내의 자격이 없어지는 일은 없다.

스마트카드 SC1에서 DRM 자격이 없어지고 EMM 메시지를 스마트카드 SC2로 보내었으나, 통신상의 장애로 인해 SC2가 이벤트를 재생할 수 있는 자격을 얻지 못한 경우가 있을 수 있다. 이 경우는 서비스 업체가 SC1의 로그를 분석하고 자격을 보내는 시도를 했음을 확인하고 SC2 스마트카드에 이벤트에 대한 재생 자격을 직접 넣어줘야 한다.

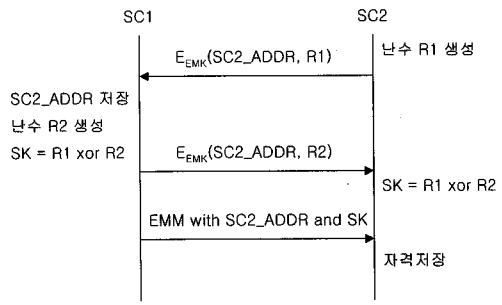


그림 5. 스마트카드 인증과 자격전송 프로토콜

V. 결 론

이상에서 우리는 수신기로부터 SAS로 시청내역을 전송하는 리턴 채널이 없는 소규모 CAS를 가정하고, 수신기는 스마트카드를 통해 ECM과 EMM 메시지를 분석하고, 스트림을 저장할 수 있는 개인

용 저장장치를 가지고 있다고 가정했다.

이러한 가정 하에 ECM 메시지 내에 DRM 조건 영역을 두고 ECK 식별자, 제어단어 회수, 전체 제어단어 개수를 포함시킨다. EMM 메시지는 자격을 TLV 형태로 담아 나르므로 DRM 자격인 이벤트 보기 회수, 재분배 가능에 대한 것을 TLV 형태로 가입자에게 보낸다. 스마트카드는 DRM의 기능을 수행하기 위해서 DRM에 대한 자격을 저장해야 하고, ECM을 복호화하여 제어단어를 획득하여 이벤트를 보려고 할 때 다른 자격보다 먼저 DRM 자격을 확인하여 가입자에게 보여줄 것을 확인하여야 한다. 스마트카드는 이벤트의 재생을 위해서 ECM을 복호화할 때 사용했던 ECK의 식별자와 ECK를 저장하고, 이벤트를 보았다는 것을 확인하기 위해 제어단어의 회수를 볼 때마다 갱신한다.

저장된 스크램블된 스트림을 다른 가입자에게 전송해주고 볼 수 있는 자격을 이양하는 프로토콜을 두 스마트카드가 공통으로 가지고 있는 EMM을 만들 때 사용하는 EMK를 바탕으로 제안되었다.

본 논문에서 제안된 방법은 CAS를 적용하여 디지털방송 서비스를 제공하고 있거나, 새로이 디지털 방송 서비스를 개시하는 사업자가 DRM과 CAS를 별개로 운영하지 않고 한 시스템으로 운영하려고 할 때 적용될 수 있는 방법이다. 기존의 시스템에 제안하는 기능을 추가하기 위해서는 다음과 같은 부분이 수정되어야 한다. ECM을 만드는 ECMG와 ECM을 만들 때, DRM 조건을 갖는 구조로 바뀌어야 한다. ECM 메시지 내의 접근조건들이 TLV 형식으로 많이 구현되고 있으니 DRM 조건에 태그를 부여하여 구현하면 된다. EMM 메시지를 만드는 EMMG 역시 DRM 자격을 포함할 수 있도록 수정 구현되어야 하나 이 역시 태그를 부여하여 구현할 수 있다. 수신기는 디지털 스트림을 저장할 수 있는 하드웨어와 기능을 가지고 있어야 하며, 스마트카드와의 DRM 관련 기능을 처리할 수 있는 명령어들이 구현되어야 한다. 스마트카드는 이벤트 식별자별로 자격과 그 때 사용되었던 ECK를 저장하고 있어야 하며, DRM 관련 기능을 수행하기 위한 명령어들을 처리할 수 있어야 한다.

본 논문에서 제안한 모델이 DRM의 모든 기능을 구현하지는 못하지만 어느 정도 디지털 콘텐츠에 대한 저작권을 보호하기 위한 최소한의 요구사항을 만족시키는 방법일 것으로 생각된다.

참 고 문 헌

[1] 스카이라이프, http://www.skylife.co.kr

[2] 한국정보처리학회, "DRM 최신 국제표준 기술 사양 분석 및 세계 유명제품 동향과 전망에 관한 연구", *한국소프트웨어진흥원*, 2004.

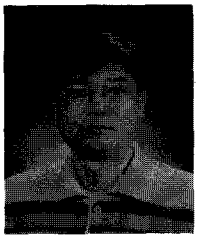
[3] ETSI, "Digital Video Broadcasting(DVB); Support for use of scrambling and Conditional Access(CA) within digital broadcasting systems", *ETR 289*, 1996.

[4] DVB, http://www.dvb.org

[5] 4C Entity, "Content Protection for Recordable Media Specification Revision 1.0", 2003.

[6] 4C Entity, "Content Protection for Prerecorded Media Specification Revision 1.0", 2003.

정 석 원(Seok Won Jung) 정회원



1991년 2월 고려대학교 이과대학 수학과 졸업

1993년 2월 고려대학교 일반대학원 수학과 석사

1997년 2월 고려대학교 일반대학원 수학과박사

2004년 3월~현재 목포대학교 정보보호전공 조교수

<관심분야> 공개키 암호 알고리즘, 방송보안, 스마트카드보안, 암호칩 설계