# 디지털 방송 제한 수신 시스템에 관한 연구

김대엽*, 문종섭**, 임종인**

*(주)시큐아이닷컴, 정보보호 연구소

**고려대학교 정보보호 연구소

# A Study on a Conditional Access System for a Digital Broadcasting

Dae-Youb Kim*, Jong-Sub Moon**, Jong-In Lim**

*SECUI.COM, R&D Center

** Center for Information Security Technologies(CIST), Korea University

## 요 약

위성과 케이블 등을 통한 디지털 방송이 보편화됨에 따라, 양질의 방송 프로그램을 제공함으로 서비스의 질을 높이고 발전시킬 필요가 있다. 유료방송은 이와 같은 고급화되고 차별화 된 방송 서비스를 제공하고, 동시에 안정적인 수입구조의 기반이 될 수 있다. 제한 수신 시스템은 이와 같은 유료 서비스를 제공하는데 필요한 시스템으로서 지속적으로 연구 개발되고 있다. 본 논문에서는 현재까지 제안된 제한 수신 시스템의 운영 및 키 관리 방안을 소개하고, 안전하고 효과적인 새로운 제한 수신 시스템의 운영 방안을 제시한다.

## I. 서론

위성과 케이블 등의 방송 매체를 통한 디지털 방송이 보편화됨에 따라, 양질의 방송 서비스를 통한 지속적인 발전이 요구되고 있다. 유료 방송(Pay-TV)은 이와 같은 고급화되고 차별화 된 서비스를 제공하고, 가입자들의 다양한 요구를 충족시키는 동시에 안정적인 수익구조의 기반이 될 수 있다. 유료 방송을 운영하기 위해서는 해당 프로그램에 대한 정당한 시청자격을 가진 수신자만이 해당 프로그램을 시청할 수 있는 시스템이 필요하다. 예를 들어, 채널 또는 프로그램에 대한 시청료를 납부한 가입자, 프로그램의 시청연령 제한에 위배되지 않는 가입자와 같이 방송 사업자가 수신자의 프로그램 시청을 효과적으로 제어할 수 있는 장치가 필요하다. 제한 수신 시스템(Conditional Access System, CAS)은 암호화된 방송 프로그램을 위성이나 케이블망을 통해서 전송하고, 특정 가입자들만이 암호화된 방송 프로그램을 복호화할 수 있도록 하는 시스템을 의미한다[1][2][3]. 그림 1은 CAS에서 디지털 방송 프로그램을 암/복호 하는 과정을 설명한다. 또한 그림 2는 위성을 통한 일반적인 CAS의 구성을 나타낸다.

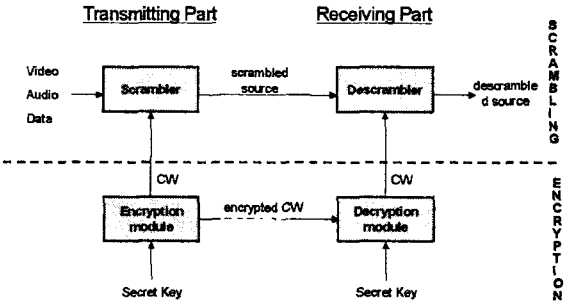


그림 1 : 방송 프로그램의 암/복호.

본 논문에서는 지금까지 연구 발표된 CAS를 소개하고, 그 성능 및 취약점을 살펴본다. 또한, 안전하고 효과적인 새로운 CAS를 제시한다. 본 논문은 다음과 같이 구성된다. 2장 1절에서는 CAS의 기본 구성과 기존에 제안된 운영 방안들을 설명하고, 그 성능 및 취약점 등을 분석한다. 2장 2절에서는 새로운 CAS 운영 방안을 제안하고, 기

존의 운영 방식과 성능을 비교 평가한다.

# II. 디지털 방송 제한 수신 시스템

## 1. CAS의 구성 및 운영

이 절에서 우리는 CAS의 기본 구성과 지금까지 발표된 운영 방안에 관한 연구를 소개한다.

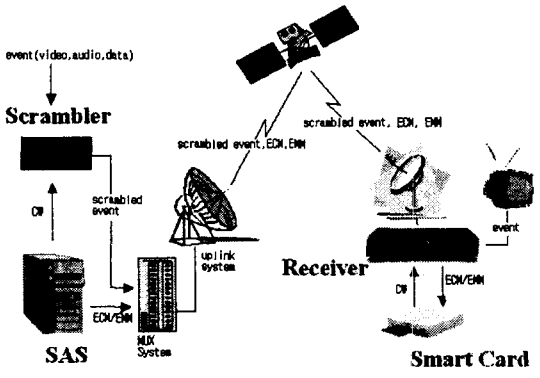


그림 2 : 위성방송 CAS 구성도.

그림 2에서와 같이 일반적인 CAS는 가입자의 자격을 관리하고 제어하는 인증 서버(Subscriber Authentication Sever, SAS)와 방송 프로그램을 암호화하는 스크램블러(Scrambler), 방송 프로그램을 수신하는 수신기, 그리고 CAS의 각종 제어 메시지를 처리하고 시청자격이나 암/복호에 사용되는 키와 같은 데이터를 저장하는 가입자 스마트카드(Smart Card)로 구성된다. 특히, 수신기에는 암호화된 방송 프로그램을 복호화 하는 디스크램블러(Descrambler)가 내장되어 있다. 또한, 가입자의 프로그램 시청을 효과적으로 제어하기 위하여 자격 제어 메시지(Entitlement Control Message, ECM)와 가입자의 시청자격을 제어하기 위한 자격 관리 메시지(Entitlement Management Message, EMM)를 사용한다.

비디오, 오디오, 그리고 데이터와 같은 방송신호는 제어단어(Control Word, CW)를 키로 사용하여 암호화 된 후 전송된다. 이와 같은 암호화 과정을 스크램블(Scramble)이라 정의하고, 스크램블러를 통해서 수행된다. 스크램블 된 방송을 시청하기 위해서, 수신기는 스크램블에 사용한 CW와 동일한 CW를 사용하여 복호화 작업을 수행해야 된다. 이 복호화 작업을 디스크램블(Descramble)이라 정의하고, 수신기에 내장된 디스크램블러를 통해서 수행된다. 그러므로, CW는 해당 프로그램에 대한 시청자격이 있는 가입자만 획득할 수 있어야 한다. ECM은 채널별로 관리되며, CW와 해당 프로그램의 시청자격(entitlement)을 전송하기 위하여 사용된다. 프로그램의 시청을 제어하고, 안전하게 전송하기 위하여 ECM은 암호화된 상태로 전송된다.

$$ECM = E_{key\,1}(CW, \text{시청자격})$$
$$EMM = E_{key\,2}(key\ 1, \text{가입자 시청자격}) \quad (1)$$

일반적으로, ECM의 암호화에 사용된 key1을 채널키(Channel Key)라 부르고, EMM을 통해서 암호화된 상태로 가입자에게 전송된다. 이 때 사용되는 키, key2는 가입자 스마트카드 발급 시, 발급 프로그램에 의해 제공된 키를 사용하거나, 또 다른 EMM을 통해서 가입자에게 전송된다. 또한, EMM은 가입자가 신청한 시청자격을 포함할 수 있다. 일반적으로, ECM은 모든 가입자가 수신 할 수 있고, EMM은 그 종류에 따라 수신자를 선별해서 전송한다.

수신기는 가입자에게 전송된 EMM을 수신하여 스마트카드로 전달한다. 스마트카드는 키/시청자격 등을 안전하게 EEPROM과 같은 내부 메모리에 저장한다. 가입자가 채널을 선택하면, 수신기는 해당 채널의 ECM을 수신해서 스마트카드로 전달한다. 스마트카드는 저장영역을 검사하여 key1이 저장되어 있으면, ECM을 복호화 한다. ECM의 시청자격과 가입자 스마트카드에 저장되어 있는 가입자 시청자격을 비교하여 동일한 자격이 있으면, CW를 수신기로 전달한다. 수신기는 전달된 CW를 사용하여 디스크램블 작업을 수행해서 정상적인 방송 프로그램을 TV와 같은 디스플레이 매체로 전달함으로써 가입자로 하여금 시청할 수 있게 한다.

그러므로, 유료 방송 시스템을 운영하기 위해서는 가입자 시청자격과 ECM/EMM의 암/복호에 사용되는 키를 안정적이고 효과적으로 운영할 수 있는 방안이 제시되어야 한다.

현재까지 제안된 CAS는 특정 채널의 ECM을 복호화 할 수 있는 채널키가 가입자의 스마트카드에 저장되어 있으면, 가입자가 해당 채널에 대한 시청자격을 갖고 있는 것으로 간주한다 [4][5][6].

[4]와 [5]에서는 4개의 암/복호키(MPK, GK, DEK, CW)로 구성된 CAS가 제안되었다. 각각의 키들은 그 다음에 명시된 키를 암호화하기 위하여 사용된다. MPK는 가입자 스마트카드마다 유일하게 할당되는 키를 의미하며, GK의 암/복호를 위하여 사용된다. GK는 서비스 채널의 그룹에 할당되는 그룹키를 의미한다. $t$ 개의 서비스 채널이 존

재하고 $s$ 명의 가입자가 서비스를 이용한다고 가정하면, $1 \le n \le \min(2^t, s)$개의 채널 그룹이 존재할 수 있다. GK는 해당 그룹에 속한 채널의 채널키(DEK)의 암/복호화에 사용된다. DEK는 각 서비스 채널에 할당된 채널키를 의미하며, 해당 채널의 프로그램의 암/복호에 사용된 CW를 암/복호화하기 위하여 사용된다. GK와 DEK는 주기적으로 갱신되며, EMM을 통해서 가입자에게 전송된다. 또한 CW도 주기적으로 변경되고, ECM을 통해서 전송된다. $s$ 명의 서비스 가입자는 $n$ 개의 채널 그룹 중 하나에 속한다. 정상적인 서비스를 제공받기 위해서 가입자는 자신이 속한 채널 그룹의 새로운 GK를 전송 받아야 한다. 또한 전송된 GK는 해당 채널 그룹에 속한 가입자만이 획득할 수 있어야 한다. 이를 위하여, GK 갱신에 필요한 EMM 패킷은 해당 그룹에 속한 가입자의 PK로 암호화된다. 그러므로 서비스에 사용된 모든 GK를 갱신하기 위해서는 $s$ 개의 패킷이 필요하다. 또한 DEK가 변경되면, 해당 채널을 포함하는 그룹별로 패킷을 생성/전송하면 되므로 $n$ 개의 EMM 패킷이 필요하다. 키 갱신을 위한 EMM의 경우, 가입자가 언제 수신했는지 알 수 없으므로, 주기적으로 계속 생성/전송해야 된다. 따라서, DEK의 갱신 주기가 1일이라고 가정하면, 키 갱신을 위해 필요한 패킷은 1일 기준으로 $n+s$ 개가 필요하다. 또한 실제 운영에서 가입자의 시청자격 변경을 고려해야 된다. 시청자격 변경이 한 가입자당 평균 한 달에 한번씩 발생한다면, 이에 필요한 패킷의 수는 1일 기준으로 $s/30$이 된다. 이와 같은 자격 변경 EMM도 일정시간 동안 주기적으로 전송해야 된다. 그러므로, CAS를 정상적으로 운영하기 위해서는 1일 기준으로 평균 $n+s+s/30$개의 EMM 패킷을 생성해야 하고, 이를 주기적으로 계속 전송해야 된다. 가입자 수가 많은 경우, 이와 같은 패킷의 생성 및 전송은 SAS 뿐만 아니라 Uplink System에도 큰 무리가 된다. 또한, 가입자가 선택하는 채널 그룹의 종류도 제한적으로 제공될 수밖에 없다. 그리고, GK 또는 DEK가 곧 시청 자격이 되기 때문에, 프로그램 단위의 시청 자격 제한이나 Pay per View와 같은 다양한 서비스를 제공할 수 없다.

[5]에서는 4개의 키(MPK, GK, DEK, CW)로 구성된 또 다른 CAS를 제안하고 있다. 제안된 CAS에서 MPK, DEK, CW는 앞서 설명한 것과 동일하나, GK는 그 의미가 다르다. 제안된 CAS는 채널그룹 RG와 가입그룹 CG를 운영한다. 채널그룹은 앞에서 설명한 것과 동일하다. 가입그룹은 가입자를 서비스 신청 시점을 기준으로 묶는 것을 의미한다. $n$ 개의 채널그룹과 $m$ 개의 가입그룹이 존재한다고 하면, 다음과 같은 $n \times m$ 개의 가입자 그룹이 존재하고, 각각의 가입자는 이 중 하나에 속하게 된다.

$$U = \begin{pmatrix} U_{11} & U_{12} & \cdots & U_{1n} \\ U_{21} & U_{22} & \cdots & U_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ U_{m1} & U_{m2} & \cdots & U_{mn} \end{pmatrix} \quad (2)$$

여기서, $U_{ij}$는 $i$ 시점에 채널 그룹 $RG_j$를 신청한 가입자 그룹을 의미한다. 각각의 $U_{ij}$에는 그룹키 $GK_{ij}$가 할당되어 DEK의 갱신에 사용된다. 그러므로, DEK의 갱신을 위해서는 $n \times m$ 개의 패킷이 필요하며, GK의 갱신을 위해서는 $s$ 개의 패킷이 필요하다. 그러므로 키 갱신을 위해 생성해야 될 EMM 패킷의 수는 $n \times m + s$이 된다. 또한, 앞에서 설명한 것과 같이 시청 자격 변경을 요구하는 가입자를 처리하기 위한 EMM 패킷을 고려하면 $n \times m + s + s/30$개의 패킷을 생성해야 된다. 이 경우도 앞에서 설명한 경우와 같은 취약점을 동일하게 갖고 있다.

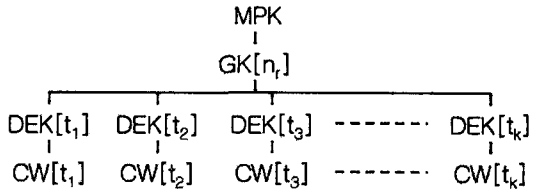


그림 3 : CAS 키 구조.

[6]에서는 스마트카드를 사용하지 않고 SAS와 수신기가 키를 공유하는 CAS를 제안했다. 제안된 CAS는 CW와 채널키 AK의 키 구조를 갖는다. 또한 AK는 위성망을 사용하지 않고, 일반적인 유선 네트웍망과 password-based protocol을 사용해서 공유한다[7][8]. 즉, 방송 신호를 CW로 암호화하여 전송하고, AK로 암호화된 CW는 ECM 형태로 위성망을 이용해서 전송한다. 그리고, 해당 채널의 시청을 원하는 가입자는 유선 네트웍망으로 자신의 id를 SAS로 전송하면, SAS는 데이터베이스에 저장되어 있는 가입자의 id와 password를 기본 값으로 password-based protocol을 사용하여 수신기와 session key를 생성/공유한다. 생성된 session key로 해당 채널의 AK를 암호화하여 가입자에게 네트웍망을 이용하여 전송한다. 수신기

는 공유한 session key를 사용하여 전송된 AK의 복호화를 수행한다. 제안한 CAS은 스마트카드를 사용하지 않기 때문에 비용절감 등의 효과가 있을 수 있다. 그러나, 가입자가 자신의 id와 password를 다른 여러 사람과 공유한다면, 이를 제어할 수 없다. 또한 수신기에 AK를 안전하게 저장할 수 있는 물리적인 영역이 없이 EEPROM과 같은 일반적인 저장영역을 사용한다면, 쉽게 AK를 복사/배포할 수 있다. CAS의 운영 목적은 정당한 시청자격을 가진 사람만이 정상적으로 방송 프로그램을 시청할 수 있도록 제어하는 것이다. 그러므로, [6]에서 제안한 CAS는 기본적인 CAS의 요구조건을 만족시키지 못한다. 또한 기존의 유선 네트웍망을 이용한 AK의 전송은 많은 시청자가 동시에 시청하는 프로그램의 경우, 시청자의 요청을 처리하기 위해서 그 만큼의 대용량 시스템과 처리 방안이 필요하기 때문에 비효과적이다.

## 2. CAS 운영에 관한 제안

[4],[5], 그리고 [6]에서 제안한 CAS는 앞에서 언급한 것처럼 채널키 또는 그룹키를 시청자격으로 이용하기 때문에, 가입자의 다양한 서비스 요구를 만족시킬 수 없다. 이 절에서 우리는 효과적이고 안전한 제한 수신 시스템의 운영에 관한 방안을 제안한다. 제한하는 CAS는 SAS, 스크램블러, 디스크램블러가 내장된 수신기, 그리고 가입자 스마트카드로 구성된다. 또한 안전한 메시지 전송을 위하여 세 종류의 키-PK, BK, CK-와 CW를 사용한다. 그리고, 효과적인 운영을 위하여 두 종류의 EMM을 사용한다:

- EMM_B : 키의 갱신을 위한 EMM.
- EMM_P : 가입자 자격 갱신을 위한 EMM.

또한, 시청자격으로는 채널 id, 프로그램 id, 토큰 등을 다양하게 사용할 수 있다.

### 1) 키 구조

제안하는 CAS는 네 종류의 키 PK, BK, CK, CW를 사용한다. PK는 가입자 스마트 카드마다 유일하게 제공되는 키를 의미한다. PK는 EMM_P 생성을 위해 사용되며, 경우에 따라 EMM_B 생성에 사용되기도 한다. BK는 BK와 CK의 갱신을 위한 EMM_B 메시지를 생성하기 위해 사용된다. CK는 채널키로, CW를 전송하는 ECM을 생성하기 위해 사용된다. 제안하는 CAS에서 CK는 채널에 하나씩 할당되지 않고, 모든 채널에 동일하게 사용된다. 단, 안전성을 위해서 복수개의 CK가 존재할 수 있다. 여기서는 $n$개의 CK가 존재한다고 가정하고, 이를 CK1, ... ,CKn으로 표시하고, Key id로 구분한다. SAS는 ECM을 생성할 때, $n$ 개의 CK 중에서 하나를 선택하여 사용하며, 해당 Key id를 ECM에 명시한다.

### 2) 자격 종류

제안하는 CAS의 시청자격은 다양하게 구성할 수 있다. 본 논문에서는 채널, 프로그램, 그리고 PPV 서비스를 위한 토큰만을 정의한다.

- channel id : 서비스 채널에 할당된 id로, 15비트의 실제 채널 id와 1비트의 AD flag로 구성된다. ECM에서 사용할 경우 AD flag는 항상 '0'으로 설정되며, EMM_P에서 사용될 경우, '1'이면 해당 channel 자격을 스마트카드에서 삭제하고, '0'이면 스마트카드에 저장한다.
- program id : 서비스 프로그램에 할당된 id로, 15비트의 실제 프로그램 id와 1비트의 AD flag로 구성된다.
- token : 방송 프로그램에 할당된 PPV를 위한 프로그램의 가격을 의미한다. 해당 프로그램에 대한 채널과 프로그램 시청자격이 없는 가입자가 프로그램을 시청하고 싶을 때, 스마트카드에 저장되어 있는 token으로 해당 값을 지불하고 프로그램을 시청한다.

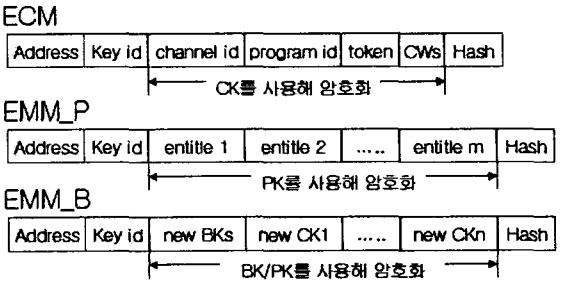


그림 4 : ECM/EMM 구조.

앞에서 정의한 자격 이외에, 몇 개의 채널을 묶어서 하나의 자격으로 제공하는 패키지 서비스, 스포츠나 드라마와 같은 프로그램 종류를 묶어서 하나의 자격으로 제공하는 Theme 서비스, 시청연령 제어와 같은 Level 서비스, 특정 지역 또는 특정 가입자 그룹에 대한 시청 제어와 같은 Black Out/In 서비스 등 다양한 자격을 정의/제공할 수 있어, 가입자에게 다양한 서비스를 제공할 수 있다.

### 3) EMM/ECM 메시지

그림 4는 제안하는 CAS에서 사용되는 ECM과

EMM의 기본적인 구조를 설명한다. Address는 전송되는 메시지를 수신할 대상을 나타내며, '0'인 경우 모든 가입자가 수신할 수 있고, 그 외의 값인 경우 특정 대상자만 수신하게 된다. Key id는 해당 메시지의 암호화에 사용된 키를 구분하기 위해 사용되며, Hash는 메시지의 무결성을 보장하기 위하여 사용된다.

ECM은 채널별로 구성되며, 해당 채널의 프로그램 암호에 사용된 CW와 시청할 수 있는 시청 자격인 채널 id, 프로그램 id, 그리고 PPV 서비스를 위한 프로그램 가격인 토큰을 포함한다. 만약, 시스템을 확장하여 다른 자격들을 제공한다면, 프로그램을 시청하기 위한 자격들을 추가로 명시한다. Address는 '0'으로 설정되고, Key id는 암호에 사용된 CK의 Key id를 명시한다.

EMM_P는 서비스 가입자가 신청한 자격을 해당 가입자에게 전송하기 위하여 사용된다. 전송되는 자격은 새로 신청한 채널 또는 프로그램의 id와 취소한 채널 또는 프로그램의 id, 그리고 신청한 token의 개수 등이 포함된다. 메시지는 가입자의 PK를 사용해서 암호화되어 전송되고, Address는 해당 가입자에게 할당된 Address 값으로 설정되며, Key id는 PK의 id로 설정된다.

EMM_B는 CK와 BK를 갱신하기 위하여 사용된다. Address를 '0'으로 설정하면, BK를 사용하여 암호화한다. 이 메시지는 모든 가입자들에게 전송된다. 예외적인 경우로, 오랜 기간 동안 서비스를 이용하지 않은 가입자는 주기적으로 갱신된 키를 전송 받지 못했기 때문에, EMM_B에 사용된 BK와 스마트카드에 저장된 BK가 다를 수 있다. 이러한 경우, EMM_B를 정상적으로 처리할 수 없기 때문에, 사용중인 채널키를 획득할 수 없다. 이 때, 가입자는 SAS에 키 갱신을 요청한다. SAS는 Address를 해당 가입자의 Address로 설정하고, 메시지를 해당 가입자의 PK로 암호화한 EMM_B를 생성/전송하고, 가입자 수신기는 이를 처리한다.

### 4) 스마트 카드

CAS에서 사용되는 스마트 카드는 ISO/IEC 7816 - part3과 part4에서 제공하는 명령어 이외에 CAS에서 필요한 명령을 처리할 수 있도록 설계되어야 한다. 또한 키와 자격을 저장할 EF가 발급 시 생성되어야 한다. 키를 저장하는 EF를 key_EF라 하고, 채널, 프로그램, 토큰을 저장하는 EF를 각각 channel_EF, program_EF, 그리고 token_EF라 하자. key_EF는 외부 명령으로는 접근이 불가능하도록 설정되어야만 하고, 오직 스마트 카드 내부 프로그램에 의해서만 접근할 수 있어야 한다. 즉, 스마트카드 명령에 의한 key_EF의 읽기/쓰기는 금지되도록 설정되어야 한다. 그리고, 자격에 관한 EF의 경우는 읽기 명령만이 허용된다[9].

### 5) CAS 운영

새로운 가입자가 등록하면, SAS는 스마트카드 발급 절차를 통해 PK, BKs, CKs와 Address등이 입력된 카드를 해당 가입자에게 발급한다.

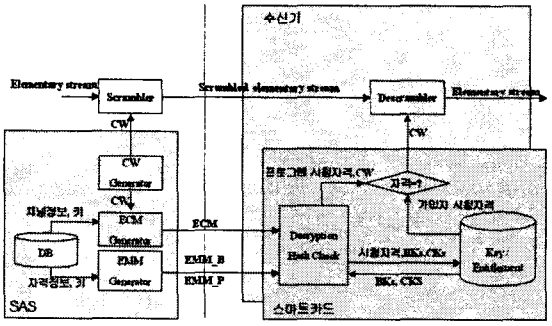


그림 5 : CAS 운영도.

가입자가 신청한 채널, 프로그램, 토큰과 같은 자격은 EMM_P로 만들어져 가입자에게 전송된다. 수신기는 EMM_P를 스마트카드에 전달하고, 스마트카드는 복호화 및 메시지 무결성을 점검한 후, AD_flag에 따라 각각의 자격들을 channel_EF, program_EF, token_EF에 각각 저장 또는 삭제한다.

수신기에 전원이 공급되면, 수신기는 EMM_B를 수신해서, BK와 CK의 갱신을 시도한다. 수신된 EMM_B는 스마트카드로 입력되고, 스마트카드는 입력된 EMM_B를 복호화 하고, 메시지 무결성을 검증한 후, key_EF에 각 키와 키 id를 저장한다.

가입자가 채널을 선택하면, 수신기는 해당 채널의 ECM을 수신한다. 수신된 ECM은 스마트카드에 전달된다. 스마트카드는 입력된 ECM의 복호화와 메시지 무결성을 검증한다. 또한 ECM의 channel id가 channel_EF에 저장되어 있는 id와 동일한가를 검증한다. 동일한 channel id가 존재하면, CW를 수신기로 전달한다. 만약 동일한 id가 없으면, program_EF를 확인하여 ECM의 program id와 동일한 id가 있으면, 해당 CW를 전달한다. 적당한 channel / program id를 자격으로 갖고 있지 않다면, token_EF에 저장되어 있는 token의 수를 확인한다. 저장되어 있는 token의 수가 ECM에 있는 token의 수와 같거나 많으면, 가입자의 PPV

의향을 묻는 출력 값을 수신기에 전달한다. 가입자가 PPV를 선택하면, 수신기는 PPV 명령과 ECM을 스마트카드에 전송한다. 스마트카드는 ECM의 token 수만큼 token_EF의 token을 감소시킨 후, CW를 수신기로 전송한다.

수신기는 전송된 CW와 디스크램블러를 사용하여 전송된 방송신호의 복호화 작업을 수행하고, 결과를 TV나 PC를 통해 가입자에게 보여준다.

제안하는 CAS의 경우, 키 갱신을 위해 필요한 패킷은 1일 기준으로 1개이며, 동일한 EMM_B를 모든 가입자가 수신한다. 가입자가 한 달에 평균 한번 시청자격 변경을 신청할 경우, 하루에 생성해야될 패킷의 경우는 평균 $1+s/30$이 된다. 1만명의 가입자를 확보한 방송사업자가 30개의 유료방송 채널을 운영한다고 가정하자. CW와 채널키의 갱신 주기를 각각 15초와 하루라 하고, 한 달에 한번씩 가입자는 자신의 시청자격을 변경한다고 하자. 또한 [4]와 [5]에서 그룹키는 한 달을 주기로 변경한다고 가정하자. 그리고, [5]에서 가입자 그룹은 한 달을 기준으로 하루를 동일한 그룹으로 가정하면, 표 1은 하루에 생성해야 되는 EMM 메시지의 개수를 나타낸다. 이 경우 채널그룹의 수 $n$은 최대 $2^{30}$이 될 수 있다.

표 1 : ECM/EMM 패킷 수.

| | [4], [5]안 | [5]안 | 제안 안 |
|---|---|---|---|
| EMM 수 | 10334+ $n$ | 10334+(30 × $n$) | 335 |
| ECM 수 | 172,800 | | |

## III. 결론

위성 TV와 케이블 TV의 보급으로 디지털 방송은 급속하게 성장하고 있다. 그러나 이와 같은 성장을 유지하기 위해서는 기본적으로 유료방송을 통한 안정적인 수익구조가 제공되어야 한다. 제한수신 시스템은 유료 방송 서비스를 가능하게 해주는 시스템으로 많은 연구가 진행되고 있으며, 상용화되고 있다. 본 논문에서는 지금까지 제안된 CAS의 연구결과를 소개하고, 그 특성과 취약점등을 설명했다. 또한, 지금까지 제안된 CAS의 특징이 암/복호키를 시청자격으로 사용했기 때문에 그로 인해 발생되는 서비스의 제한과 많은 패킷 생성의 문제를 해결하기 위하여, 시청자격과 암/복호키를 분리해서 운영하는 새로운 CAS를 제시했다. 제시된 CAS는 사용되는 키의 갱신을 위한 패킷의 수가 1개이므로, 앞서 소개된 CAS의 키 갱신을 위해 필요한 패킷이 가입자의 수에 비례해서 증가하는 것과 비교하여 볼 때 효과적으로 패킷을 운영할 수 있으며, 다양한 방송 서비스를 제공할 수 있도록 설계되었다.

## 참고문헌


[1] EBU Project Group B/CA, "Functional model of conditional access sytem", EBU Technical Review, pp. 64-77, winter 1995.

[2] Francoise Coutrot, Vincent Michon,"A Single Conditional Access System for Sattellite -Cable and Terrestrial TV", *IEEE Trans. on Consumer Electronics*, vol. 35, no. 3, pp464-468, Aug. 1989.

[3] Didier Angebaud, Jean-Luc Giachetti, "Conditional Access Mechanisms for All-Digital Broadcast Signals", *IEEE Trans. on Consumer Electronics*, vol. 38, no. 3, pp188-194, Aug. 1992.

[4] H.S.Cho, C.S.Lim, "Digipass : Conditional Access System of Koreasat DBS", *Journal of Electronics*, vol. 22, no. 7, pp. 768-775, July 1995.

[5] Fu-Kuan Tu, Chi-Sung Laih, and Hsu-Hung Tung, "On Key Distributin Management for Conditional Access System on Pay-TV System", *IEEE Trans. on Consumer Electronics*, vol. 45, no. 1, pp, 151-158, February 1999.

[6] Youngsoo Kim, Joonsuk Yu, and Donho Won, "An Efficient Satellite CAS using Password-Based Protocol", The association for intelligent machinery, 2000.3.3. Proc. of CS&I'2000 ; International Conference on Computer Science and Informatics, pp.607-610, 2000.3.

[7] D.P.Jablon, "Strong Password-only Authenticated Key Exchange", ACM Computer Communications Review, 1996.

[8] R.Perlman, C.Kaufman, "Secure Password -Based Protocol for Downloading a Private Key", Proc. of the 1999 Network and Distributed System Security(NDSS), 1999.

[9] ISO/IEC7816-4 : Interindustry commands for interchange, 9. 1995.