특집

위성방송을 위한 CAS 시스템 및 운용 사례

趙賢淑, 林春植
韓國電子通信研究所

I. 서 론

1994년 미국의 DirecTV에서 약 100만 가입자를 가지고 디지털 위성방송서비스를 시작한 이후, 최근 2~3년 내에 세계의 유수의 방송사들이 앞 다투어 디지털 위성방송을 개시 및 준비하고 있다. 일본의 PerfecTV에서 금년 10월에 JSAT 위성을 이용하여 57개의 채널로 위성방송 서비스에 들어갈 예정에 있고, 우리나라도 무궁화 위성을 이용한 디지털 위성방송의 상용 서비스 개시를 '97년에 실시할 예정에 있어, KBS가 96년 7월 1일부터 2채널에 의해서 현재 디지탈 시험 위성방송을 실시 중에 있다.

이처럼 위성을 이용한 디지털 방송의 다채널 시대에 가입자는 개별화된 전문 채널 서비스를 받을 수 있고, 한편 방송사업자는 기존 지상파에서 광고료 수입에만 의존하던 방송서비스 운영을 CAS (Conditional Access System, 제한수신시스템)을 이용하여 TV 방송에 가입자 개념을 추가하여 정당한 수신료를 지불하는 사람만이 프로그램을 시청할 수 있도록 하고, 전문 방송업자들에 의한 전문 방송 프로그램의 제작을 가능케 하여 다양한 기능의 서비스를 제공할 수 있게 되었다.

가입자 개념 및 전문성을 가지는 상업 방송의 높은 부가가치성에 대한 인식으로 몇몇 선진국에서는 제한 수신에 대한 연구가 상당히 진척되어 있을 뿐 아니라, 유료 채널 가입자에 대한 안전성 연구가 활발히 진행되고 있다.

본 고에서는 디지털 위성방송 시대에 발맞추어 급부상 되고 있는 유료 방송 서비스를 위한 CAS 시스템에 대한 소개와 이용 사례를 기술하고, 국내 위성방송의 유료 채널 서비스에서 사용될 DigiPass에 대해서 기술하고자 한다.

그러나 CAS시스템이 제공하는 기능 및 특성상 이에 관련된 정보를 획득하기는 어려운 상황이며, DVB 및 DAVIC에서도 제한수신 서비스를 위한 기본 frame 및 스크램블링 방식 등만을 표준화로 추진하고, CAS 시스템의 security를 가늠하는 security mechanism과 시스템 구조는 Service provider 및 각국의 재량에 따라 구현하도록 되어있다.

II. CAS 기능 및 구성도

제한수신시스템(CAS)이란 송신기에서 스크램블된 신호를 수신측의 수신 인가를 받은 가입자만이 디스크램블하여 프로그램을 시청할 수 있도록 하는 시스템으로, 이 시스템이 갖추어야 하는 기본적인 요건은 첫째로, 시청료를 지불한 정당한 가입자만이 프로그램을 시청할수 있어야 하고, 둘째, 미가입자의 불법 도시청을 막을수 있는 스크램블링의 강도가 높아야 될 뿐만 아니라, 디스클램블링에 필요한 키를 알아내는 것을 막을 수 있어야 한다.

수신료를 지불한 정당한 가입자에게 안전한 서비스를 제공하기 위한 사용자의 보안서비스에 대한 기능으로는 우선 안전성(security)을 들수 있는데, 시스템의 안전성은 비인가된 사용자가 서비스를 시도할때 마주치게 되는 어려움의 정도로서 여기에는 두가지 양상이 있다. 즉 Access Control과는 상관없이 관련 신호를 디스크램블링하는 것으로 이것은 서비스가 나타내는 성질과 스크램블링에 의한 함수로 고려할 수 있고, 또 하나는 불법적인 방법으로 제어키를 얻는 것으로서, 사용되는 알고리즘의 안전성 문제와 키 관리방법의 문제가 고려 대상이 된다.

제한 수신을 위한 안전성 메카니즘(security mechanism)으로는 스크램블링/디스크램블링, 의사 난수 발생, 암/복호화, 인증 프로토콜, 키 관리 등이 있다.

1. CAS의 기능 요구사항

디지털 TV 방송에서의 제한수신시스템의 기본 요구조건을 만족시키기 위해 다음의 두가지 기능을 고려해야 한다.

첫째, 프로그램 및 데이타는 스크램블링되고 통신 링크상에서 보호되어야 하며,

둘째, 인증을 위한 가입자 신분 확인(Authentication)기능과 접근 제어(Access Control) 기능이 있어야 한다.

위의 두가지 기능은 결국 자원(프로그램 및 데이타)과 가입자 보호를 위한 것으로, 자원의 보호메카니즘으로는 스크램블링/디스크램블링이 있고, 가입자 보호메카니즘으로는 인가된 가입자들에게 해당 시청 권한을 주는 기술이다. 자격(Entitlement)은 프로그램 및 데이타의 스크램블링에 필요한 관련 키와 수신자의 시청 권리를 말하며 자격통제와 자격관리로 대별할 수 있다.

(1) 스크램블링/디스크램블링 기능
(Scrambling/Descrambling Function)

스크램블링은 원래의 신호에 변형을 가하여 스크램블된 형태의 신호만으로는 수신권한이 없는 수신자는 시청할 수 없도록 하는 것으로 신호의 종류(영상,음성, 데이타) 및 신호의 형태(아날로그, 디지털)에 따라 스크램블링의 방식이 달라진다. 디스크램블링은 스크램블된 프로그램을 원래의 신호대로 복원하는 과정을 말하며, CW를 가진 수신기들에서만 디스크램블된 프로그램의 시청이 가능하다.

(2) 자격통제기능(Entitlement Control Function)

프로그램을 디스크램블하기 위해 필요로한 권한과 관련 키들을 entitlements라 한다. 이 기능은 암호화된 control words와 프로그램을 access하기 위해서 필요로한 요구 조건들을 분배, 즉 난수 발생의 CW를 암호화하고 그 제어 워드를 자격 통제 메시지(Entitlement Control Message : ECM)를 통해 전송한다. 스크램블링의 의사 난수의 규칙성을 찾을 수 없도록 하여 비화도를 높이기 위해 CW를 주기적으로 변경시키고, 자격 통제 메시지내에는 암호화된 CW외에 프로그램 정보와 access parameter도 함께 전송된다. 자격 통제 메시지의 송/수신은 ECM의 주기 계수기(period counter)에 의해 방송될 프로그램과 동기화된다.

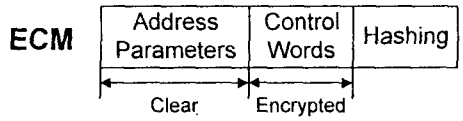
(3) 자격관리기능(Entitlement Management Function)

자격관리기능은 가입자들에게 자격(entitlements)을 전달하는 기능으로 이 데이타는 EMM (Entitlement Managements Messages)라는 메시지에 실어서 보낸다. EMM은 수신기의 보안장치인 스마트 카드내에 자격을 부여하거나 갱신하는 기능을 지원하며, 각 수신자의 주소에 의한 인식 기

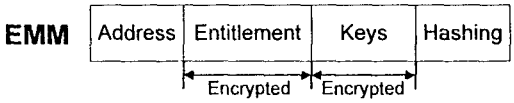
능을 이용하여 수신자의 서비스 키를 바꾸거나 통제하는 통제 취득 기능의 지원도 가능하다

(4) 메시지 구조

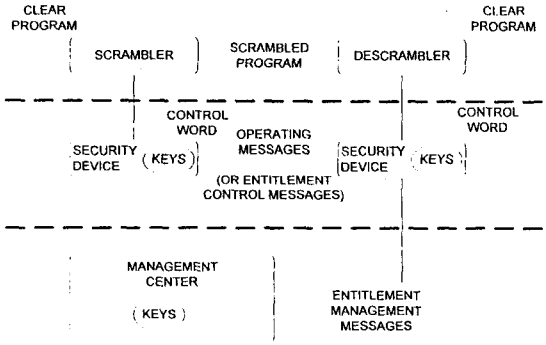
o ECM(Entitlement Control Messages)



o EMM(Entitlement Management Messages)



2. CAS의 기능 구성도



〈CAS 시스템의 기능 블럭도〉

III. CAS 시스템

CAS시스템의 1980년 초에 유럽에서 Cable TV 서비스가 본격화되면서 주로 유럽에서 CAS 시스템들이 경쟁적으로 연구개발되어 유럽의 거의 모든 나라에서 CAS시스템을 개발하였다. 미국의 DirecTV의 CAS시스템인VideoCrypt도 이스라엘의 NewsDataCom사가 개발한 제품이다.

유럽의 대표적인 CAS 시스템을 VideoCrypt, EuroCrypt, NagraVision, Luxcrypt와 B-MAC을 들 수 있고, 최근들어 네덜란드의 IRDETO가 개발한 시스템이 유럽 , 아프리카, 호주 시장에서 서비스되고 있다. VideoCrypt는 크게 두가지(VC I, VC II) 형태가 있으며, VC1은 영국과 아일랜드에서 사용되고 그밖의 유럽에서는 VC II가 사용된다.

EuroCrypt 역시 EurioCrypt-M, EuroCrypt-S, EuroCrypt-S2, EuroCrypt-S＊의 여러 형태의 시스템이 나와 있었으나, EuroCrypt-M이 가장 대표적으로 사용된 시스템이다. 이들 각각에 대해서 간단히 살펴보면 다음과 같다. 여기서 언급되는 CAS 시스템들은 초기에 아날로그 방식의 스크램블링을 지원하였고, 최근에는 디지탈 스크램블링 방식을 지원한다. 그러나 CAS 시스템의 기능중 안전성(security)을 처리하는 즉, 안전한 key 전송을 위한 부분은 스크램블링 방식(아날로그/디지털)과는 무관한 처리 과정이므로 디지털 방송시대에 쉽게 접근할수 있는 시스템들이다.

1. VideoCrypt

Thomson Consumer Electronics와 News Datacom에 의해서 개발되었으며, 1994년부터 디지탈 방송을 처음 개시한 DirecTV에서 100만 가입자를 가지고 서비스를 시작하여 '96년 현재 160만 이상의 Pay-TV 가입자를 두고 있다. VideoCrypt는 Multi-standard encryption system (for PAL, NTSC and SECAM)으로서 어느 시스템에 쉽게 접목할수 있는 융통성을 가지고 있다. 제공되는 서비스는,

- Single or Multiple Subscriptions with many tier levels in one channel
- Pay Per View(PPV) and Impulse Purchasing
- Thematic selection(enable all arts programming)
- Geographic Limitation(restrict to a country/area)
- Single-Event(Throwaway cards)
- Parental control(reception with card only)
- Pre-Determined time period

유럽에서는 BSkyB channels이 VideoCrypt를 처음 사용하였고, Sky Movies는 90년5월2일에 VideoCrypt에 의해서 처음으로 암호화한 서비스를

Service Provider	Country	입자수	CA채널수	시스템
TV3, TV1000, FilMax	Sweden	70,000	4	ASTRA
FilmNet	Sweden	00,000	5	ASTRA, Tele-X
CANAL+	France	60,000	2	Telecom2, TDF1/2
BBC World Service TV	Europe	7,000	1	Intelsat
PV Plus	N'lands	11,200	1	Eutelsat
Business TV(FT, Maxat)	Europe	4,100	2	Entelsat, TC2
KalbelKanal	Gernany	620	1	Eutelsat

하였으며, 최근에는 DVB Common Scrambling 방식 사용한 시스템이 개발되어 있다.

2. EuroCrypt

EuroCrypt는 France Telecom의 재원에 의해서 CCETT 가 개발한 CAS시스템으로 CABLE서비스를 위한 CAS 시스템을 비롯하여 아날로그 방식의 스크램블링 및 1994년부터는 DVB Common Scrambling알고리즘을 사용한 CAS 시스템을 개발 착수하여 현재 프랑스의CANAL +에서 1채널에 의해서 시험방송되고 있다. 다음표는 유럽에서 EuroCrypt를 사용하여 CAS서비스를 하고 있는 것을 나타낸 것으로 1994년 통계치이므로 현재는 이보다 훨씬 많은 수요가 있으리라 생각된다.

이외에도 네덜란드의 PTT등 다른 방송사들이 EuroCrypt를 가지고 서비스를 개시할 준비를 하고 있다.

3. NagraVision

NagraVision은 스위스에서 개발된 시스템으로 Syster와 Nagra로서 알려져 있고, 프랑스, 스페인, 터어키와 독일 등지에서 사용되고 있다. 다른 CAS 시스템들과는 달리 디코더 박스를 판매가 아닌 사업자가 임대하는 형식으로 운영되고 있는 것이 특이 할만하다.

4. IRDETO

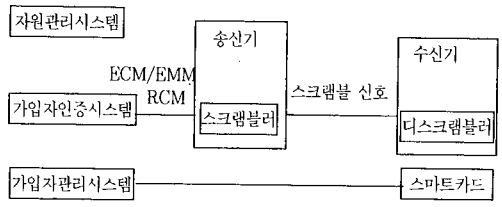
다른 CAS시스템들과 마찬가지로 Turn-key base로 운영되는 시스템으로 Object-Oriented 개념과 Modular Control방식으로 설계되어 있어 융통성을 향상시킨 시스템으로 소개되고있다. 아날로그 CA 방식으로 525line vs 625 line 시스템을 지원하고, 디지털 CA방식으로 DVB/DAVIC의 표준에 따르고 있다. 현재 태국, 남아프리카, 호주 및 이탈리아 등지에서 4개의 MPEG2/DVB 시스템으로 운영되고 있다.

5. DigiPass

국내에서 디지털 위성방송에서의 제한수신 서비스를 위해 ETRI가 개발한 Conditional Access System이다. 시스템의 기능 및 제공 가능한 서비스를 들에 대해서 살펴보고 국내에서 개발해야만 하는 타당성에 대해서는 결론에서 언급하고자 한다.

DigiPass의 특징으로는 MPEG-2/DVB complaint한 시스템이며 해외 시장 진출을 고려하여 DVB common scrambling을 사용하였고, 시스템의 안전성을 강화하기 위해 다단계 키관리 메카니즘으로 처리되었으며, 국내 사정을 고려한 암호 알고리즘을 사용하여 설계된 시스템으로 500백만 가입자까지 처리할수 있다.

무궁화위성방송에서는 DigiPass 시스템의 기능



〈DigPass 기능 블럭도〉

	ideo Crypt 1	Video Crypt 2	D2-MAC Euro Crypt-M	Nagra Syster	Lux Crypt	B-MAC
TV 신호	PAL	PAL	D2-MAC	PAL	PAL	B-MAC
스크램블링방식 ● Video ● Audio	- Line Cut and Rotate - Non-scrambling	- Line Cut and Rotate - Non-scranbkubg	- Line Cut and Rotate on Chroma/Luma - Encrypted digital	- Line Shuffle - Spectrum Inversion	- Frame/Averae Peak Level Inversion - digital PCM	Line Delay DES-like
Smart Card	미 보유	보유	보유	보유	미 보유	미 보유
사용자	BSkyB Multichannels, Adult Channels, urotica, JSTV	Discovery, FilmNet	FilmNet TV1000, TV3, Canal+	Premiere, Canal+	RTL-4 Veronique	AFRTS SIS Racing Channel

이용하여 다음과 같은 방송서비스를 제공할 수 있다.

- 주제별/프로그램 서비스 등급별 가입
- 다수의 프로그램 서비스 등급 및 주제에 대한 동시 가입
- Pre-Booked Pay-Per-View(PPV)
- Impulse Pay-Per-View
- 위성을 통한 시청자격 제어 및 관리
- 수신권리 부여기간의 제한
- PPV 수요촉진을 위한 Pay Free Time
- 스마트 카드를 이용한 가입자 보호관리 및 사용통계 데이타관리

이상 유럽 및 국내의 CAS 시스템들을 살펴보았으며 아래 표는 유럽의 CAS 시스템의 특성을 살펴본 것이다.

IV. 결 론

CAS 시스템은 위성을 이용한 디지털 위성방송에서 뿐만 아니라 CATV(Cable TV)에도 적용할 수 있다. 최근 방송 추세는 채널마다 전문성을 지니며 다른 방송과 구별이 되는 전문 방송채널의 확대 및 방송 사업자의 수입을 광고료에 의존하지 않고 가입자의 시청료에 의존하여 방송 내용의 질적 차별화를 추구하고 있다.

또한, 데이타의 전송 방식에 있어서도 기존의 아날로그 방식에서 탈피해 디지털화로 나아가고 있으며, HDTV등 보다 나은 화질과 음질등 고 품질의 서비스 제공을 추구하고 있다. 이런 추세에 직접위성방송과 CATV 같은 방송 기술 및 제한 수신 기능의 지원을 위한 기술은 필수적이며 잠재적으로 매우 높은 부가 가치를 지니고 있다.

그러나 이와 관계된 기술은 유럽을 비롯한 선진국들의 점유물로 되어 있어 기술 보유국들의 기술에 대한 횡포 또한 만만하지 않은 상황이고, CAS 시스템이 가지는 시스템 특성상 기술 도입시 막대한 기술료와 매월 지불 해야만 하는 security fee는 국민 경제에 막대한 영향 뿐 아니라 유료 방송 실시에 있어 초기 시스템 도입에 따라 기술의 종속성은 영영 탈피하기 어려운 상황이 예상되었다.

이와 같은 점을 고려하여 한국전자통신연구소에서는 디지털 위성방송에서의 유료 방송을 위한 CAS 시스템인 DigiPass를 1994년말부터 DigiPass 개발에 착수하여 96년 말에는 국내에서 유료 방송 서비스의 시험방송을 할 수 있을 것으로 기대된다.

참 고 문 헌

〔1〕 Information processing system-Open Systems Interconnection-Basic Reference Model-Part 2 : Security Architecture, ISO 7498-2.

〔2〕 General characteristics of a conditional access broadcasting system-Report CCIR 1079-1.

〔3〕 조현숙,임춘식,"DigiPass : KoreaSat DBS의 Conditional Access System" 전자공학회지, VOL. 22 NO.7, 1995

〔4〕 John McCormac "European Scrambling Systems" April,1996.

〔5〕 CCETT Presentation 자료

〔6〕 IRDETO Presentation 자료

저 자 소 개

趙 賢 淑

1957年 12月 28日生
1980年 2月 전남대학교 수학과(학사)
1991年 8月 충북대학교 전산학과(석사)

1982年 3月～한국전자통신연구소
1996年 현재 한국전자통신연구소 지상 SW연구실장

林 春 植

1952年 4月 3日
1975年 2月 한국항공대학 통신공학과(학사)
1986年 2月 한국항공대학 대학원 석사과정(통신전공)
1992年 3月 일본요코하마 국립대학 전자정보공학박사과정 (전자정보)수료

1978年 3月 군복무(공군 ROTC)
1980年 6月 국방과학연구소(연구원)
1996年 현재 한국전자통신연구소 위성통신단 지상시스템연구부 부장

주관심분야 : 정보이론(채널 코딩), 디지털 이동통신, 대역확산통신, 위성통신망 및 신호처리 기술