제한수신기술

– 제한수신 기술 개요

□ 신용태, 오성흔* / 숭실대학교, *(주)디지캡

Ⅰ. 서 론

아날로그 신호를 통해 전송되던 AM 방송, FM 방송, 텔레비전 방송 매체들은 디지털 전송 방식의 발달과 디지털화로 인한 장점(고선명 영상, 고품질 음향 등)에 힘입어 급속도로 디지털 방송화 매체로 탈바꿈 되어가고 있다. 위성 디지털 방송 서비스, 디지털 케이블 TV 서비스와 위성 DMB, 지상파 DMB, 그리고 IPTV까지 많은 디지털 방송 매체를 통해 풍부한 디지털 방송 콘텐츠가 시청자에게 제공될 것이다.

보편성과 공익성을 목적으로 하는 지상파 TV 서비스는 주로 광고 수익을 통해 운영을 해왔다. 그러나 고품질, 다채널, 전문 채널 서비스 제공 등 양질의 서비스를 시청자에게 제공하기 위해 기존 광고 수익 구조에서 탈피하여 방송에 가입자(Subscriber) 개념을 도입하게 되었다.

현재 지상파 TV와 지상파 DMB 서비스를 제외한 나머지 디지털 케이블 방송 서비스, 위성 디지털 방송 서비스, 위성 DMB 서비스, IPTV 방송 서비스들은 주로 가입자를 기반으로 하는 유료 방송 형태를 보이고 있다. 가입자에게 양질의 서비스를 제공하는 이러한 유료 방송 서비스가 지속적으로 영위되기 위해서는 합법적 가입자는 증가해야 하고 불법 시청 가입자는 없어야 하며 방송 콘텐츠가 불법적으로 복사/유통되지 않도록 해야 한다. 만일 유료 방송 콘텐츠에 대한 불법적인 시청 접근 또는 불법 복사/유통이 증가하게 된다면 양질의 방송 콘텐츠를 제작하여도 수익이 나지 않는 상황이 발생하기 때문에 양질의 방송 콘텐츠를 제작하는 동기가 사라지고 전반적인 방송 콘텐츠 품질의 경쟁력 약화로 인해 결국 가입자의 손해가 발생하게 되는 결과가 일어날 수 있다.

이러한 불법 시청, 불법 복사/유통을 방지하기 위해 기술적으로 제한 수신 기술(이후 CAS(Conditional

Access System)라 칭함)이라는 기술이 방송 서비스에 적용되고 있다. 본 고에서는 방송 콘텐츠를 보호하는 다양한 기술들을 살펴본 후 CAS 기술에 대해 깊게 살펴본다. 또한 CAS 기술 중 하나인 SimulCrypt 기술에 대해 설명한 후 본 고를 맺는다.

II. 방송 콘텐츠 보호 기술

CAS 기술을 자세히 살펴 보기 이전에 방송 콘텐츠 보호를 위해 적용할 수 있는 기술들을 간단하게 살펴 본다. 방송 콘텐츠 보호 기술을 크게 분류하자면 1) DRM(Digital Rights Management) 기술, 2) CAS(Conditional Access System) 기술, 3) Copy Protection 기술, 4) Watermarking/Fingerprinting 기술로 분류할 수 있다. 본 장에서는 CAS를 제외한 나머지 보호 기술에 대해 간단히 살펴 본다.

1. DRM (Digital Rights Management)

CAS의 마지막 단어가 System인 반면 DRM의 마지막 단어는 Management라는 차이점이 있다. DRM은 콘텐츠의 보호 기술만 제공하는 것이 아니라 디지털 콘텐츠에 대한 내용/특성/저작권/사용/분배에 대한 메타데이터 명세, 과금 및 공정 거래 내역 관리 등의 클리어링 하우스, 디지털 콘텐츠 식별자 체계 등 디지털 콘텐츠 유통 전반에 대한 기술을 포함하고 있다. 최근 뉴스나 산업계에서 언급되고 있는 DRM 기술은 주로 콘텐츠의 불법 사용 및 불법 유통 방지를 위한 보호 기술에만 맞추어 사용되고 있다.

지금까지의 DRM 기술(콘텐츠 보호 측면에서)은 주로 유무선 통신망(인터넷, 모바일 등)을 통해 유통되는 음악, 영상, 게임, 문서 등과 같은 불연속적인(Discrete) 디지털 콘텐츠에 대한 보호 기술을 제공해 왔다. DRM 기술은 암호화 기법을 이용하여 콘텐츠의 기밀성(Confidentiality)을 제공하고 콘텐츠의 사용 제어(Permission/Constraints)를 명세할 수 있는 Rights Expression Language를 통해 사용 제어를 가능하도록 한다.

현재까지는 DRM 기술 자체가 상호 작용(Interactivity)이 가능한 네트워크 환경에서 동작하도록 설계되어 있기 때문에 방송 콘텐츠 보호를 위해서 상호 작용이 다소 용이한 IPTV와 같은 환경에서만 제한적으로 적용되고 있다.

2. Copy Protection

Copy Protection 기술은 저장 매체, 인터페이스 신호, 디스플레이 신호에 대한 디지털 콘텐츠 복사 제어 기술이다. D-VHS, PVR 등의 디지털 입출력 규격인 IEEE-1394는 DTCP(Digital Transmission Content Protection), 디스플레이 입출력 방식인 DVI, HDMI에는 HDCP(High-bandwidth Digital Content Protection), Blue-Ray 디스크나 DVD-RW 등 저장매체의 경우 CPRM(Content Protection for Recordable Media) 기술을 적용하여 보호하고 있다.

OpenCable의 CableCARD Copy Protection 기술[1]도 Host와 CableCARD 간 전송되는 방송 콘텐츠에 대한 복사 제어 기술로 볼 수 있다. Copy Protection 기술은 CAS와 DRM과 같이 풍부한 사용권한 제어 기능을 제공하지 않고 주로 제한된 범위 내에서 사용할 수 있는 복사 방지 기술로 볼 수 있다.

3. Watermarking/Fingerprinting

Watermarking 기술과 Fingerprinting 기술은 저작

권자의 권리를 증명하기 위해 가시적으로 또는 비가시적으로 저작권 정보 및 사용자 정보를 삽입하고 검출하는 기술이다. Watermarking은 주로 저작권 주장 또는 복제나 위조 방지를 위해 사용하고 Fingerprinting은 사용자 식별자 정보나 고유 번호를 넣어 콘텐츠 전송 경로의 추적 및 불법 배포자 추적을 위해 이용한다.

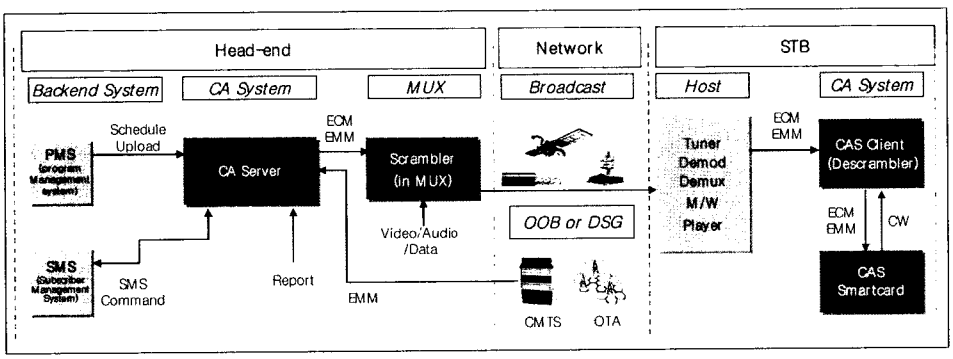
CAS나 DRM은 암호화 기법을 기반으로 접근 제어를 하는 능동적(active) 보호 방식인데 반해 본 기술은 콘텐츠 자체는 암호화 하지 않는 수동적(passive) 보호 방식이라고 볼 수 있다. Watermarking 또는 Fingerprinting Marking을 처리하는 제어 모듈이 없는 이상 불법 복사와 사용 제어의 원천적인 방지는 불가능하다. 본 기술은 P2P, 웹 하드 등에서 불법 콘텐츠의 대량 유통을 방지하기 위한 필터링 기법의 보호 기법을 위해서 이용될 수 있다.

III. 제한 수신 기술 (Conditional Access System)

CAS는 암호화된 방송 프로그램을 위성/케이블/지상파/IP 망과 같은 방송망을 통해서 전송하고 특정 가입자들만이 암호화 된 방송 프로그램을 시청할 수 있도록 하는 방송 보안 시스템이다. 방송 가입자 관리 시스템과 함께 디지털 방송 유료 서비스를 위한 방송 시스템의 핵심 시스템으로 가입자가 원하는 서비스를 정확하고 편리하게 제공받을 수 있도록 하고 방송사업자에게는 불법 시청을 방지하여 수익을 보호하는 시스템이다.

CAS 기술을 제공하는 업체마다 구조와 명칭이 다를 수 있지만 <그림 1>은 CAS 구성도를 보여 준다. 방송 시스템(보통 Head-end라고 부른다)에는 방송 콘텐츠를 암호화 하는 MUX(Scrambler 기능 포함)와 CAS 서비스를 제공하는 CAS Server, 그리고 방송 운영 정보를 제공하는 가입자 관리 시스템(SMS; Subscriber Management System)과 방송 편성 시스템(PMS; Program Management System) 등으로 구성된다.

방송 수신 장치(STB : Set-top Box)에서는 암호화 된 방송 콘텐츠를 복호화 하는 Descrambling 또는 복호화 기능 그리고 CAS 서비스를 제공하는 CAS 기능으로 구성된다. 보통 CAS는 소프트웨어 수준의 보안 이상의 물리적 수준의 보안 수준에서 동작하기 때문에 서버 측에서는 HSM(Hardware Security Module)을 이용하고 단말기 측에서는



<그림 1> CAS 구성도

Smartcard라는 물리적 보호 장치를 이용한다.

1. CAS 동작을 위한 기반 환경

방송 콘텐츠(비디오/오디오/데이터 등)는 대부분 MPEG-2 System 규격에서 언급하는 Transport Stream(TS) Packet을 통해 전달되며 방송 콘텐츠 보호를 위한 암호화는 보통 MPEG-2 TS 수준에서 적용된다. MPEG-2 System 규격[2]의 Transport Stream Packet Syntax/Semantic에 따르면 TS Packet Header와 Adaptation Field(optional) 부분을 제외한 Payload를 암호화 하도록 규정하고 있다. TS Packet Header 중 transport_scrambling_control field(2 bits)는 해당 TS Packet의 Payload 부분이 암호화 되었는지 아닌지를 표시하기 위해 이용된다.

이 외에도 MPEG-2 System 규격에는 CAS에서 내부적으로 사용하는 ECM(Entitlement Control Message)과 EMM(Entitlement Management Message)이라는 메시지를 전송할 수 있는 체계를 제공한다. 특정 CAS의 ECM/EMM이 어떤 TS Packets의 스트림을 통해 전달되는지 PMT(Program Map Table), CAT(Conditional Access Table)와 Conditional access descriptor라는 것을 통해 시그널링 할 수 있는 체계를 지원한다. MPEG-2 System 규격과 DVB 규격들, OpenCable 규격들에서는 CAS가 동작할 수 있는 환경 체계는 제공하지만 각 CAS가 동작하는 내부 메커니즘(ECM/EMM 포맷, 수신 자격 전달/관리 방식, 다양한 Key 전달/관리 방식 등)은 정의하지 않는다.

차후에 보다 자세하게 설명하겠지만 하나의 방송 시스템에서 두 개 이상의 서로 다른 기술의 CAS가 동시에 운영될 수 있도록 하는 SimulCrypt라는 개념이 존재한다. SimulCrypt 개념은 하나의 방송 사에서 한 개 이상의 CAS가 공존하여 운영할 수 있도록 하되 각 CAS 벤더 기술의 지적 재산권은 보호해야 한다는 배경에 의해 탄생되었다. 이를 위해 탄생한 DVB SimulCrypt 규격[3]은 두 개 이상의 CAS가 상호 운영될 수 있도록 Head-end architecture, Head-end component와 CA component 간의 메시징 인터페이스 구조, 시간 동기화 관계 등을 정의하고 있다.

두 개 이상의 각 CAS가 서로 다른 방식으로 가장 많은 대역폭을 차지하는 방송 콘텐츠를 각각 암호화 해야 한다면 매우 비효율적이기 때문에 공통된 하나의 암호화 알고리즘인 DVB Common Scrambling Algorithm[4]을 정의하여 공통된 암호화 알고리즘으로 암호화 된 하나의 방송 콘텐츠가 송출되도록 하였다. 대신 방송 콘텐츠 암호화 키(이후 Control Word라 한다.)는 각 CAS가 자신 만의 방법으로 안전하고 효율적으로 처리/전달할 수 있도록 자율성을 두었다. SimulCrypt는 각 CAS의 ECM/EMM의 내부 구조와 운영 방식을 노출하지 않은 상태에서 각 CAS 기술의 효율성/안전성에 맞게 ECM/EMM을 생성하고 전달할 수 있는 연동 방식을 제공한다.

2. 방송 콘텐츠 암호화 알고리즘

III. 1에서 언급한 바와 같이 MPEG-2 TS Packet을 통해 전달하는 방송 콘텐츠들은 보통 MPEG-2 TS 수준에서의 암호화를 적용한다. 가장 많이 사용되는 암호화 알고리즘은 DVB Common Scrambling Algorithm[4]이며 최근 IPTV에서는 AES(Advanced Encryption Standard)[5] 암호화 알고리즘을 이용하는 추세이다.

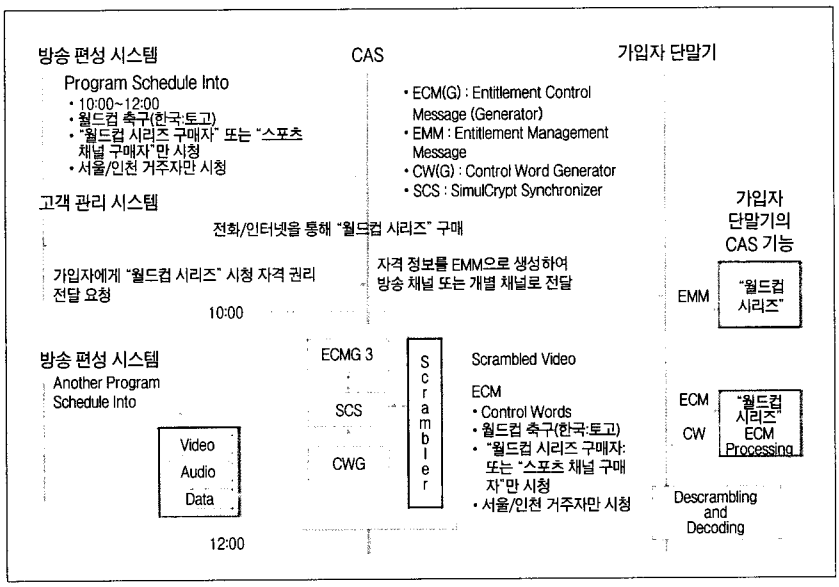
최근 OMA BCAST Service and Content Protection 기술[6], 3GPP MBMS Security 기술

[7], DVB-H IPDC Service Purchase and Protection 기술[8] 등에 따르면 IP Security (IPsec)[9], ISMA Encryption and Authentication(ISMACryp)[10], Secure RTP(SRTP)[11] 수준에서 AES를 통해 암호화와 인증을 수행하는 방식도 존재한다.

3. ECM/EMM

CAS에서 사용하는 메시지는 ECM과 EMM이다. ECM은 보통 CAS가 보호하고자 하는 방송 채널마다 각 CAS 당 하나씩 존재한다. 물론 하나의 채널을 구성하는 구성 요소(비디오, 오디오, 데이터) 마다 서로 다른 Control Word를 적용할 수도 있기 때문에 이런 경우는 채널 당 한 개 이상의 ECM이 존재할 수 있다. EMM은 가입자 관리를 목적으로 생성/전달되는 메시지로써 방송 채널과는 직접적인 관련은 없고 가입자 관리의 다양성에 의해 여러 형태의 EMM들이 존재한다. 앞에서도 설명하였지만 ECM과 EMM의 포맷 및 생성/처리/전달 방식은 어떠한 표준 규격에도 명시되어 있지 않으며 각 CAS 업체마다 다른 기술을 개발, 이용한다.

ECM은 관련 방송 채널(또는 채널의 구성 요소)에 대한 시청 가능 조건을 명시한 것으로써 암호화된 Control Word와 접근 기준(Access Criteria) 정보가 표시되어 있다. 접근 기준 정보는 각 CAS 업체가 제공하는 CAS 서비스 및 기술마다 다를 수 있지만 보통 해당 방송 채널을 시청하기 위해 어떠한 자격 정보(Entitlements)가 필요한지, 시청을 위한 나이 제한이 있는지, 지역적 제한이 있는지 등의 조건 정보가 기술되어 있다. EMM은 전화 또는 인터넷 등 다양한 방식을 통해 가입자가 방송 프로그램 또는 채널을 가입/구매하였을 때 구매한 채널/프로그램을 시청하기 위한 자격 정보를 전달하기 위해 이용한다. 이 외에 Text Messaging, CA 운영을 위한 Key 정보들, PIN Reset/Change 등의 다양한 CA 서



<그림 2> CAS 동작 방식의 예

비스를 지원하기 위해 이용되기도 한다. ECM은 보통 암호화 된 방송 콘텐츠와 함께 방송 채널로 전송되지만 EMM은 보통 방송 채널 또는 개별 채널(디지털 케이블 방송의 경우 OOB 또는 DSG Tunnel을 통해, 위성 DMB인 경우 OTA를 통해, IPTV인 경우 Unicast IP를 통해)로 전달된다.

<그림 2>는 CAS 동작 방식을 쉽게 설명하기 위해 월드컵 축구 게임에 대한 프로그램을 구매하여 시청하는 순간까지의 시나리오 예를 보여 준다.

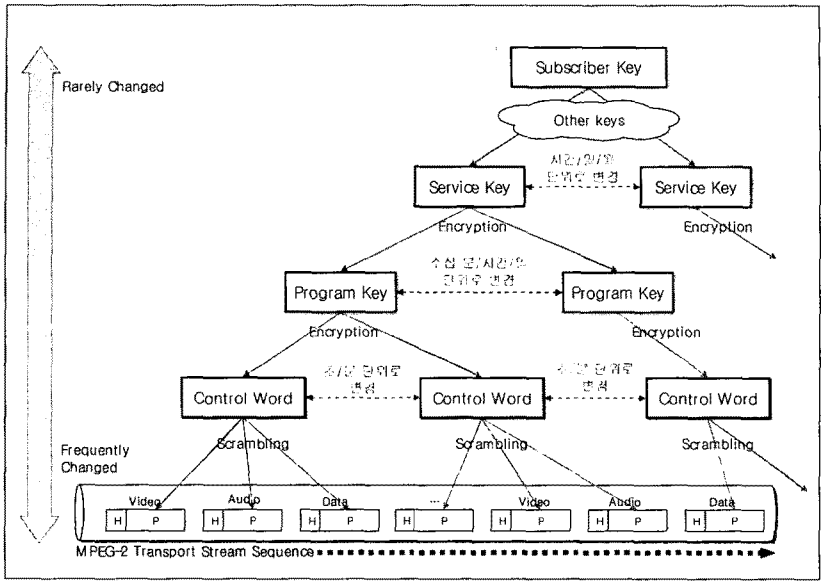
방송사의 방송 편성 시스템은 방송 채널 운영에 대한 기본적인 정보와 접근 기준 정보를 CAS 또는 내부 EIS(Event Information Scheduler)에게 제공한다. 가입자는 월드컵 축구 게임을 시청하기 위해 전화 또는 인터넷을 통해 구매를 한다. 가입자 관리 시스템은 CAS에게 가입자가 월드컵 축구 게임을 시청할 수 있도록 EMM을 통해 자격 정보를 전달해 줄 것을 요청한다. CAS는 EMM을 생성하여 방송 채널 또는 개별 채널을 통해 EMM을 전달하고 가입자 단말기에 있는 CAS 기능은 EMM을 처리하여 가입자가 월드컵 축구 시청을 위한 자격이 있음을 기록한다. 10시부터 12시까지에는 월드컵 축구 방송이 암호화되어 전송되며 암호화된 Control Word와 방송 편성 시스템이 명시했던 접근 기준 정보가 ECM을 통해 전달된다. 암호화 된 방송 콘텐츠와 ECM을 수신한 가입자 단말기의 CAS 기능은 축구 방송을 시청하기 위해 ECM 내에 기술된 접근 기준 조건을 만족하는 자격을 가지고 있는지 확인한다. 이미 EMM을 통해 월드컵 축구를 시청할 수 있는 자격을 가지고 있기 때문에 CAS에서 운영하는 Key들을 통해 최종적으로 ECM에 있는 암호화 된 Control Word를 복호화 할 수 있고 복호화 된 Control Word를 이용하여 암호화 된 방송 콘텐츠를 복호화하여 최종적으로 시청하게 된다.

4. CAS의 보안성

불연속적인(Discrete) 콘텐츠를 주로 보호하는 DRM은 보통 하나의 콘텐츠에 대해서 하나의 암호화 키를 적용하지만 방송 서비스와 같이 연속적인(Continuous) 콘텐츠 형태를 갖는 방송 채널을 하나의 암호화 키를 이용하여 변경하지 않고 계속 사용한다는 것은 보안 상 위험이 될 수 있다. 그래서 CAS는 보통 하나의 채널을 보호하는 Control Word를 일정 주기(보통 수십 초에서 수십 분)마다 계속 변경하도록 운영하는 Renewable Security를 제공하고 있다.

III. 3에서 언급한 바와 같이 Control Word는 오직 시청 자격이 있는 가입자의 단말기에서만 최종적으로 가질 수 있도록 해야 하므로 Control Word는 또 다른 특정한 Key로 암호화 되어 ECM 내에 포함된다. 이 특정한 Key 또한 오직 시청 자격이 있는 가입자의 단말기에서만 가질 수 있도록 해야 하며 Renewable Security를 위해 이 특별한 Key 또한 주기적으로 변경되어야 한다. 이러한 Key들 간의 관계를 Key Hierarchy라고 부르는데 각 CAS 업체마다 Renewable Security를 위한 Key Hierarchy가 다르며 이를 운용하는 관리/전달 메커니즘이 다르다.

<그림 3>은 간단한 CAS Key Hierarchy를 보여준다. 방송 프로그램은 Control Word로 암호화 되고 Control Word는 Program Key로 암호화된다. Program Key는 또 다른 Service Key로 암호화 되는 형태로 이루어진다. 하위에 있는 Key일수록 변경 주기가 잦아지며 상위에 있는 Key 일수록 변경이 거의 이루어지지 않는다. <그림 3>은 이해를 돕기 위해 임의적으로 구성한 것으로써 전혀 다른 Key Hierarchy를 제공하는 CAS 기술도 있을 수 있다.



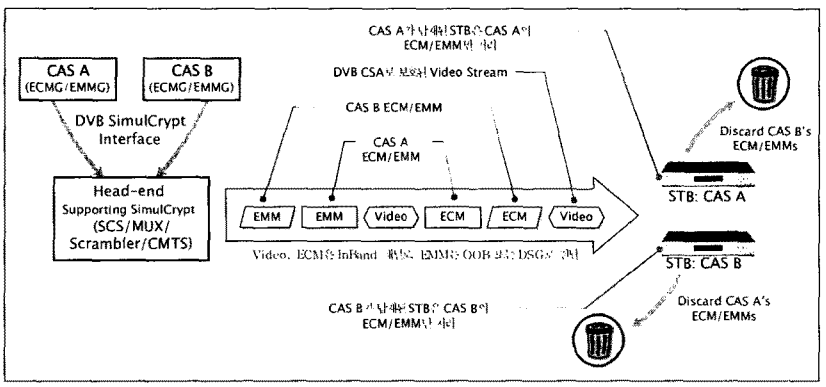
<그림 3> 간단한 CAS Key Hierarchy

IV. SimulCrypt 기술

1. SimulCrypt 개념

CAS 측면에서 SimulCrypt는 하나의 방송 시스템에서 하나 이상의 CA Systems이 동시에 운영될 수 있도록 Head-end 시스템 컴포넌트 간의 인터페이스를 정의한 것이다.

<그림 4>는 SimulCrypt 개념을 보여 준다. SimulCrypt를 지원하는 Head-end는 방송 콘텐츠를 암호화하여 전송하는 것 뿐만 아니라 CAS A와 CAS B의 ECM과 EMM을 동시에 전송하는 것 또한 가능하다. 보통 MUX에 있는 SCS(SimulCrypt Synchronizer) 기능이 하나 이상의 CA System (ECMG



<그림 4> SimulCrypt 개념

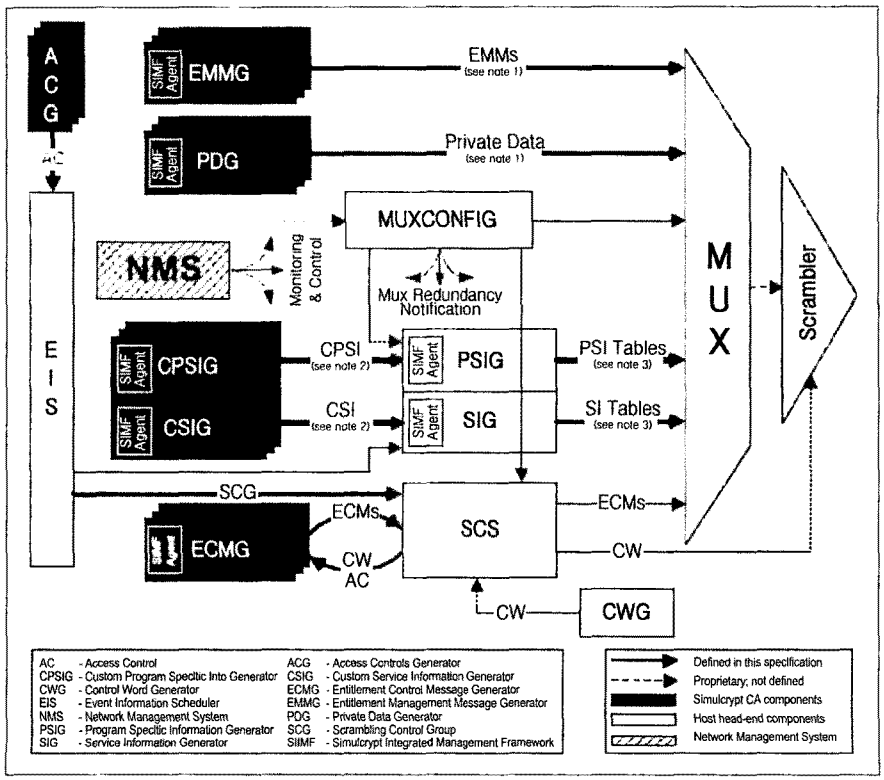
부분)과 연동을 하여 각 CA System의 ECM을 송출하며 각 CA System의 EMMG는 MUX와 연동하거나 CMTS, OTA를 통해 자신의 EMM을 송출한다.

CAS A가 탑재된 STB는 CAS A의 ECM과 EMM만 처리하고 CAS B의 ECM과 EMM은 처리하지 않는다. 반대로 CAS B가 탑재된 STB는 CAS B의 ECM과 EMM만 처리하고 CAS A의 ECM과 EMM은 처리하지 않는다. 방송 콘텐츠는 CAS A와 CAS B가 공통적으로 사용해야 하는 DVB Common Scrambling Algorithm으로 보호되기 때문에 각 CAS가 탑재된 STB는 자신의 ECM/EMM을 이용하여 암호화 된 방송 콘텐츠를 복호화 할 수 있다.

2. SimulCrypt 규격

기술 측면에서 SimulCrypt를 보다 정확하게 기술하자면 SimulCrypt 기술은 DVB(Digital Video Broadcasting) 조직에서 정의한 Head-end 시스템 컴포넌트 간의 인터페이스 규격[3]을 준수하는 기술이다. DVB SimulCrypt 규격은 현재 공식적으로 V1.4.1 버전까지 존재하며 IP DataCasting over DVB-H가 추가된 V1.5.1 버전이 DVB BlueBook 형태로 존재한다.

DVB SimulCrypt 규격에서는 EIS(Event Information Scheduler), SCS(SimulCrypt Synchronizer), ECMG(ECM Generator), EMMG(EMM Genera-



<그림 5> DVB SimulCrypt System Architecture (ETSI TS 103 197 규격에서 발췌)

tor), SIG(Service Information Generator), PSIG(Program Specific Information Generator), MUX(Multiplexer), SCR(Scrambler), CWG (Control Word Generator) 등과 같은 Head-end 시스템 컴포넌트와 이들 간의 인터페이스 규격을 정의하고 있다.

CA System과 관련한 주요 인터페이스는 ECMG <=> SCS 인터페이스와 EMMG <=> MUX 인터페이스, ACG <=> EIS 인터페이스가 있다. 이 인터페이스에는 연동하는 시스템 컴포넌트 간의 Channel 관리, Stream 관리, 메시지 전달과 응답에 대한 프로토콜, 메시지 송출 정책이 정의되어 있다. 예를 들어 ECMG <=> SCS 인터페이스에서는 SCS가 CWG를 통해 얻은 Control Word를 ECMG에게 전달하는 메시지와 ECMG가 Control Word를 이용하여 ECM을 생성한 후 다시 SCS로 전달하는 메시지 등을 정의하고 있다.

<그림 5>는 DVB SimulCrypt 규격에서 발췌한 DVB SimulCrypt System Architecture를 보여 준다.

VI. 맺음말

CAS와 DRM은 기본적으로 콘텐츠 보호와 접근/사용 제어라는 동일한 목적을 가짐에도 불구하고 기술 탄생의 배경이 달라 아직까지는 하나의 기술로 통합되어 적용되고 있지는 않다. 현재는 이 두 기술이 적용되는 위치가 달라 실시간 방송 프로그램을 보호하기 위해서는 CAS 기술이, VoD 콘텐츠 또는 방송 프로그램의 안전한 녹화 보호에 대해서는 DRM 기술이 적용되고 있는 상태이다. 최근 ITU-T IPTV FG의 Security 진행 부분과 OMA BCAST Service and Content Protection[6], DVB-H IPDC Service Purchase and Protection[8] 등에서 CAS 측면과 DRM 측면을 모두 통합 고려한 Service and Content Protection 기술이 표준화 되고 있는 상황이다.

방송 사업자가 CAS 솔루션을 선택하는 기준은 보통 안정성, 상용화 경험, 가격 요소라고 한다. 국내 CAS 기술 개발의 부단한 노력과 많은 발전으로 인해 기술적, 운영적 안정성은 해외 CAS 기술과 비슷한 수준이라고 보고 있고 가격 경쟁력은 해외 CAS 기술보다는 다소 높은 것으로 예상된다. 최근 국내 CAS 기술의 해외 수출 사례가 증가하고 있어 상용화 경험이 전무하다고 볼 수는 없지만 아직 해외 CAS 기술에 비해 상용화 경험이 적은 것은 사실이다. 국내 CAS 기술이 보다 발전하기 위해서는 방송 사업자의 국내 CAS 기술에 대한 적극적인 검토/고려도 필요하고 현실 서비스의 기술적/운영적 요구사항이 반영된 기술로 계속 발전할 수 있도록 방송사와 CAS 기술 벤더와의 전략적인 협력 또한 필요하다고 본다.

참 고 문 헌

[1] OpenCable, "CableCARD Copy Protection 2.0 Specification," OC-SP-CCCP2.0-I04-060803

[2] ISO/IEC 13818-1, "Information technology - Generic coding of moving pictures and associated audio information: Systems"

[3] ETSI TS 103 197 V1.3.1, "Digital Video Broadcasting (DVB); Head-end implementation of DVB SimulCrypt"

[4] ETSI Technical Report 289, "Support for use of scrambling and Conditional Access within digital broadcasting system," 1996

[5] FIPS PUB 197, "Advanced Encryption Standard (AES)," 2001

[6] OMA BCAST Technical Specification, "Service and Content Protection for Mobile Broadcast Services"

[7] 3GPP Technical Specification Group Services and System Aspects, 3GPP 33.246, "3G Security; Security of Multimedia Broadcast/Multicast Service (Release 7)"

[8] ETSI TS 102 474 V1.1.1, "DVB Video Broadcasting (DVB); IP Datacast over DVB-H: Service Purchase and Protection," 2007

[9] IETF RFC 4301, "Security Architecture for the Internet Protocol," S. Kent, K. Seo, December 2005

[10] ISMA, "ISMA 1.0 Encryption and Authentication, Version 1.1"

[11] IETF RFC 3711, "The Secure Real-time Transport Protocol (SRTP)," M. Baugher, D. McGrew, M. Naslund, E. Carrara, K. Norrman, March 2004

필 자 소 개

신 용 태

- 한양대학교 산업공학(학사)
- Univ. of Iowa 전산학(석사)
- Univ. of Iowa 전산학(박사)
- Univ. of Iowa 전산학과 객원교수
- Michigan State Univ. 전산학과 객원교수
- 현재 : 숭실대학교 컴퓨터학부 교수
- 주관심분야: CAS/DRM, 멀티캐스트 통신, 그룹통신, 모바일 IP 등

오 성 흔

- 인천대학교 정보통신공학(학사)
- 숭실대학교 컴퓨터학과(석사)
- 숭실대학교 컴퓨터학과(박사)
- 현재 : (주)디지캡 기술연구소 연구소장
- 주관심분야 : CAS/DRM, 암호학, 실시간 시스템, 멀티미디어 시스템 등