특집 제한수신기술

MCAS 개요 및 현황

□ 최주영*, 김종호** / *티유미디어 방송기술팀, **SK 텔레콤 C&I기술원

Ⅰ. 개 요

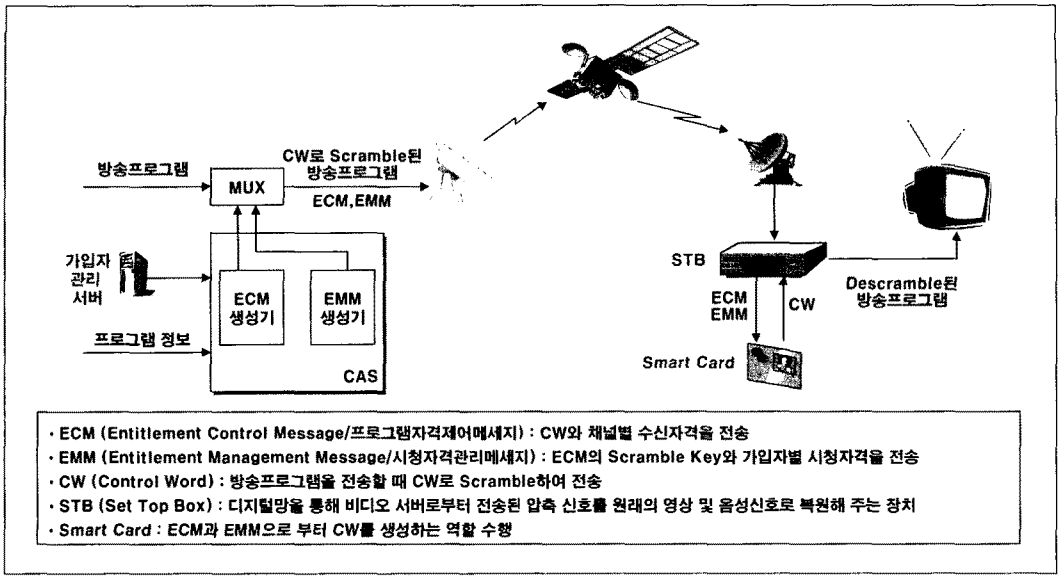
모바일 CAS는 모바일 방송(DMB, DVB-H 등)이 활성화됨에 따라 기존 유선방송용 CAS를 기반으로 하여 모바일 방송(DMB, DVB-H 등)에 적합하도록 개발된 수신 제한 시스템을 통칭하는 용어로 사용된다. 모바일 방송 초기에는 기존 CAS를 모바일 방송 환경에 그대로 도입하였으나, 모바일 방송 사업자의 개선 요구 사항이 발생하고 모바일 방송 활성화에 따른 신규 방송 사업자의 필요성에 따라 CAS 업체들이 모바일 환경에 특화된 CAS를 개발하여 상품화하게 되었다.

본 고에서는 티유 미디어와 SK Telecom이 공동으로 개발하여 위성 DMB에 적용한 모바일 CAS(이하 MCAS)를 소개하고자 한다.

Ⅱ. CAS의 기본 동작 원리와 MCAS 도입 배경

1. CAS의 기본 동작 원리

CAS(Conditional Access System)은 유료 방송 사업자가 방송 서비스 관리를 위해 정당한 시청권한을 가진 가입자만이 프로그램을 수신할 수 있도록 하는 시스템이다. CAS는 방송 사업자 측에 구축되는 서버와 STB(Set Top Box)에 구현되는 Client solution으로 구성된다. CA 서버 Part에서는 Control Word를 생성하여 비디오, 오디오, 데이터 등의 방송 신호를 암호화하여 전송한다. 이와 함께 가입자의 시청 권한 관리를 위한 EMM(Entitlement Management Message)와 암호화된 방송 신호를 복호화하기 위한 CW(Control Word)가 포함된 ECM(Entitlement Control Message)를 함께 전송한다. 단말은 방송 신



<그림 1> CAS 개요

호를 수신하여 ECM과 EMM을 추출하여 STB내의 CA Client에 전달하고 저장된 시청권한과 비교하여 시청 가능할 경우 ECM내에서 CW를 추출하여 방송 신호를 복호화하여 재생한다.<그림 1>

2. MCAS 도입 배경

기존 유선환경 기반의 CAS는 데이터 수신이 안정적이고 전원이 항상 공급되는 환경을 기반으로 하였기 때문에 가입자 관리를 위한 EMM을 일정 주기로 반복적으로 전송하여 가입, 해지를 처리하고 시청권한을 관리하였다. CAS에서 방송망을 통해 전송하는 EMM은 STB에서의 수신 여부를 확인할 수 없어 가입 및 해지 상태와 무관하게 반복 전송되었다. 유선환경 기반의 CAS가 적용된 기기는 대부분 STB 형태였는데, STB은 방송 수신만을 목적으로 하고 있어 EMM 수신이 보장되고, 전원이 항상 연결되어 있어 가입자의 방송 시청여부와 무관하게 EMM을 백그라운드로 수신할 수 있다는 특징이 있다. 이러한 특징으로 인해 EMM의 반복 전송 주기를 길게 관리하여도 수신에 큰 문제가 없었다.

그러나, 모바일 방송의 경우 모바일 단말(이동전화 겸용, 전용 및 차량용)의 특성상 방송수신 외에 다양한 기능을 사용할 수 있고, 전원 공급을 배터리에 의존하여 사용 시간에 제약이 있어 EMM을 백그라운드로 수신하기 어렵다는 문제가 발생한다. 즉, EMM을 백그라운드로 수신할 경우 배터리가 소모되어 타 기능 사용에 제약을 주게 된다. 그래서, EMM을 방송 시청 중에만 수신하도록 단말이 개발되는데 모바일 방송의 시청 패턴을 고려해 볼 경우 1회 시청시간이 짧아 EMM 수신이 쉽지 않다. EMM 전송 성공율을 높이고 빠른 시간 내에 단말에 전달하기 위해서는 EMM 전송 주기를 짧게 운영하여야 하는데 이럴 경우 EMM 전송에 많은 리소스가 소요되어 가입자 수용에 한계가 발생한다.

위의 환경 및 기기의 차이에 의한 문제를 극복하고자

도입된 것이 MCAS이며, 아래와 같은 단말 및 이동방송 환경에 대한 분석을 통해 세부 기능이 개발되었다.

1) 단말

단말은 이동전화 겸용, 전용 및 차량용 단말로 분류가 되는데 이동전화 겸용 단말이 대부분을 차지한다. 이동전화 겸용 단말은 이동통신망을 활용하여 EMM을 전송하고 EMM 수신에 대한 확인이 가능하여 반복 전송에 따른 부담을 줄일 수 있다.

2) 방송 환경 및 CAS

모바일 방송 환경은 리소스가 한정되어 있어 EMM에 소요되는 리소스를 최소화하는 것이 필수적이다. 이에 반해 단말은 EMM의 빠른 전송을 필요로 하고 있어 기존 STB 환경보다 CAS 운용 조건이 더욱 열악하다. 따라서 기존 CAS의 Key 관리 방식을 개선 검토하였다. 즉, 보안을 강화하기 위해 다단계로 전송되는 Key방식을 개선하여 전송되는 Key는 최소화하면서 내부의 기능으로 Key를 계속하여 생성하도록 할 경우 EMM에 소요되는 리소스를 절감할 수 있다.

III. MCAS 구조 및 특징

1. 기술 및 서비스 요구사항

MCAS는 아래와 같은 요구사항과 2절에서 언급한 모바일 방송 환경 분석에 기반하여 개발된 시스템이다.

1) 필수 요구사항

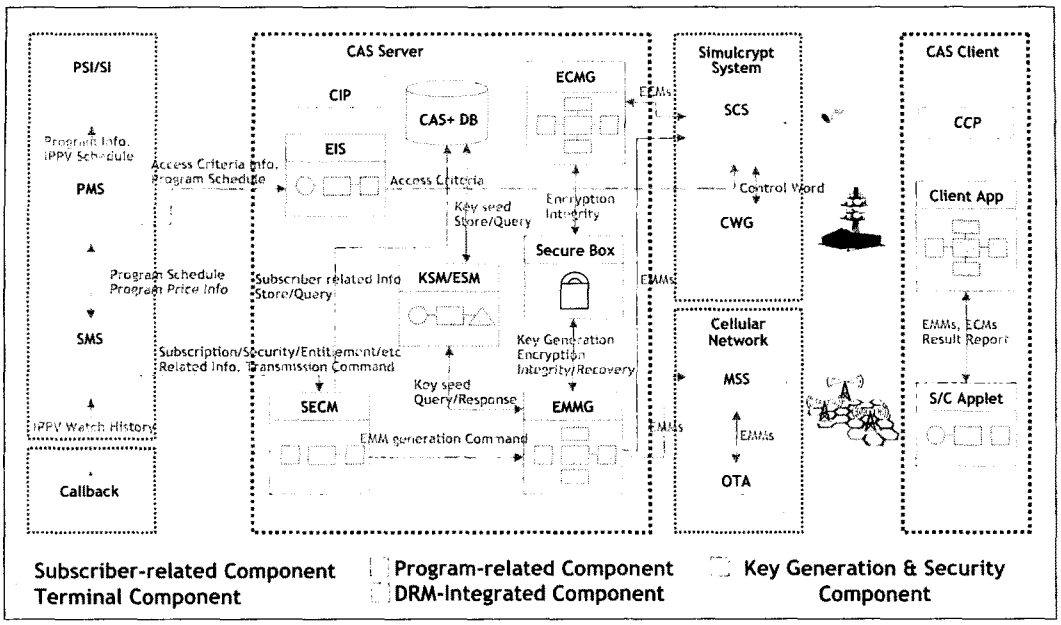
- 기 구축된 CAS와의 호환성을 위해 DVB Simulcrypt를 보장해야 한다.
- 이동통신망을 활용하여 방송망으로 전송되는 가입자 관리를 위한 EMM을 최소화한다.
- 이동통신망과의 연결이 불가능한 전용, 차량용 단말에 전송되는 EMM도 관리 방식을 개선하여 EMM 전송을 최소화한다.
- 채널별, 프로그램별 시청을 제어할 수 있어야 한다.
- 모바일 방송 환경의 특성상 발생할 수 있는 EMM, ECM 데이터 손실에 대비하여 단말은 데이터 손실 발생시에도 시청중 오류를 발생시키지 않아야 한다.

2) 부가 기능

- DRM(Digital Rights Management) 기술과의 결합을 통해 콘텐츠에 대한 접속 제어(Access Control) 및 사용 제어(Usage Control)가 지원되어야 한다. 또한 외장 메모리 및 타 기기로 저장된 콘텐츠 전송이 가능해야 하며, 이 경우 DRM에 의해 엄격히 사용이 제한되어야 한다.
- 선불권(시간, 기간 등)에 대한 서비스가 가능해야 한다.

2. 시스템 구조

MCAS는 방송 프로그램 스케쥴 등록 및 관리 시스템(PMS, Program Management System), EPG를 위한 정보 송출 시스템(PSI/SI), 가입자 관리 및 과금 시스템과 연동되어 채널 및 프로그램별 시청 권한을 설정하고 가입자 관리 및 시청 권한을 위한 EMM을 송출한다. 전체 시스템 구성은 <그림 2>와 같으며, CAS를 구성하는 각 모듈별 기능은 아래와 같다.



<그림 2> MCAS 시스템 구성도

1) EMMG(Entitlement Menagement Message Generator)

가입자에게 전달되는 방송 콘텐츠의 수신 자격 정보와 Smartcard 적용 정보 및 암호화 Key를 관리하며, 가입자의 시청 권한 및 Key에 대한 전송 스케쥴을 관리한다.

2) ECMG(Entitlement Control Message Generator)

CW(Control Word)와 AC(Access Criteria) 정보를 Smartcard에 안전하게 전달하도록 하는 메시지를 생성한다. ECMG는 SAS(Stand-Alone Scrambler)의 SCS와 DVB Simulcrypt ECM Protocol을 지원한다. ECMG는 SCS(Simulcrypt Synchronize)로부터 보내지는 CW와 AC를 수신하고 수신된 CW, AC를 이용하여 ECM을 생성한다. 생성된 ECM은 Secure Box를 통해 암호화 된 후 SCS로 반환된다. AC 정보는 MCAS Database 내부에서 직접 추출하여 ECM 생성에 사용될 수 있다.

3) EIS(Event Information System)

PMS로부터 AC를 수신하고 이를 활용하여 채널 및 프로그램별로 ECM내에 AC 정보가 포함되도록 한다.

4) SECM(Subscriber Entitlement Command Manager)

가입자 관리 시스템으로부터 전달되는 가입, 해지 등의 명령어를 EMMG에 전달하는 기능을 수행한다.

5) Secure Box

ECM과 EMM에 대한 암호화 및 메시지 인증을 수행한다. 별도의 하드웨어를 추가로 구성하여 Secure Box 자체에 대한 보안을 강화한다.

3. 기술 특징 및 장점

MCAS의 가장 큰 특징은 이동통신망을 통한 EMM 전송과 Key와 Algorithm을 결합한 보안 기술이다. 또한 일종의 EMM 압축 방식을 적용하여 전체적으로 기존 CAS 대비 EMM 전송에 소요되는 리소스를 평균 50% 이상 절감하였다. 특히, 이동전화 겸용단말의 경우 80%이상 리소스 절감이 가능하다.

1) Key + Algorithm Based CAS

Key만을 기반으로 하는 CAS의 경우 보통 다단계 Key 방식을 적용하여 EMM 전송에 리소스가 많이 소요되고, Algorithm만을 기반으로 하는 CAS의 경우 Piracy에 의한 복구에 많은 어려움이 있다. 이 두 가지 방식의 단점을 보완한 것이 Key & Algorithm 방식의 CAS이다. EMM내에 포함된 Key는 일종의 Seed Key 역할을 하며, 이 Key를 수신한 단말 내부적으로 ECM내의 CW를 얻기 위한 Key가 재생산된다.

2) 이동통신망을 통한 EMM 전송

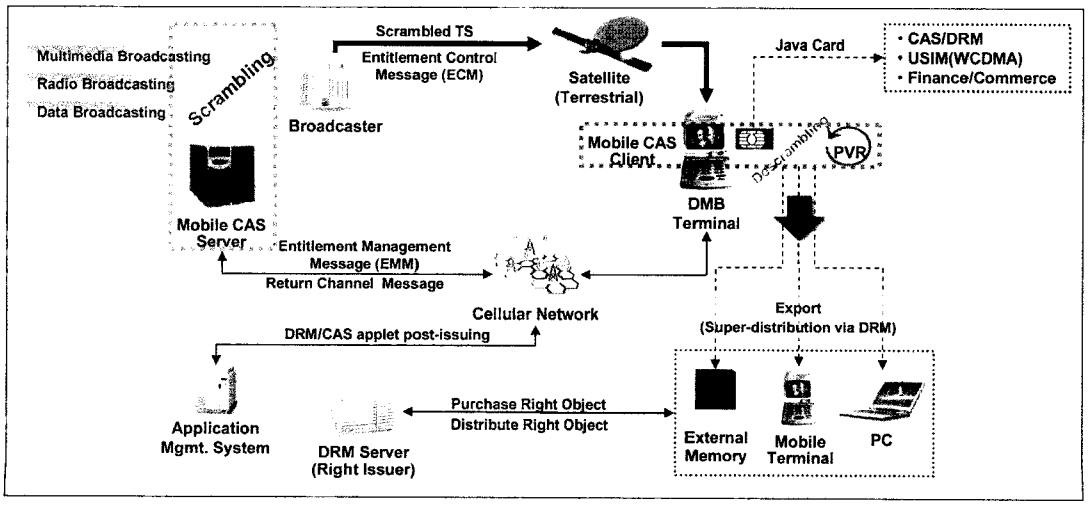
이동전화 겸용 단말의 경우 이동통신망을 통해 EMM을 수신한다. 단말은 EMM 수신 후에 성공 여부를 이동통신망을 통해 Return 한다. CA Server Part에서는 실패한 경우에 한하여 EMM을 이동통신망을 통해 재송신하게 된다.

3) 다양한 Pay TV Model

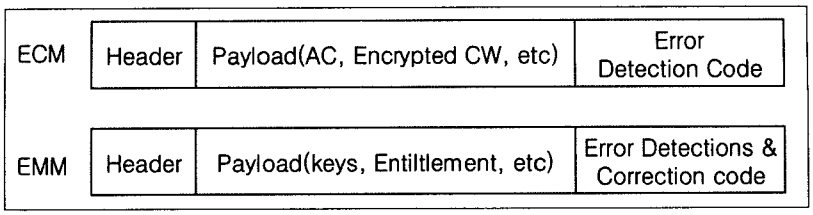
채널별 월정액 상품 및 PPV(Pay Per View) 뿐만 아니라 선불권 상품, 이동통신망을 통한 후불제 상품 등의 구성이 가능하다. 선불권의 경우 유효 기간 기준, 시청 시간 기준, 프로그램 시청 기준 등 다양한 기준을 설정하여 운영할 수 있다.

4) DRM 확장성

녹화/녹음에 대한 제어와 이후 저장된 콘텐츠에 대한 관리를 위해 DRM과의 결합이 가능하다.<그림 3> 저장된 콘텐츠는 DRM이 적용되어 있어 저장된 기기에 한해서만 재생이 가능하며, 적법한 절차에



<그림 3> CAS, DRM 결합 구성도



<그림 4> ECM, EMM 구조

의해 DRM이 적용된 콘텐츠를 복사한 사용자는 Rights 구매를 통해 파일 재생을 할 수 있다. CAS와 DRM 기술의 결합을 통해 녹화/녹음 서비스도 가입자 개념을 도입하여 상품화가 가능하다.

5) EMM, ECM 손실 보완

모바일 방송의 특성상 발생할 수 있는 데이터 손실을 처리하기 위해 EMM과 ECM 영역에 MAC과 Hash영역을 두어 수신 과정에서 문제가 발생할 경우 EMM은 복원, ECM은 discard 할 수 있도록 했다.<그림 4> ECM의 경우, 전송 주기가 짧아 discard 하더라도 시청에는 문제가 없어 복원 기능을 두지 않았다.

IV. 향후 계획 및 과제

CAS는 유료 방송에서의 핵심 기술로 MCAS는 모바일 환경에 적합하도록 진화된 첫번째 사례이다. 즉, EMM을 이동통신망이라는 대역외 채널(방송망 이외 채널)로 전송하고 모바일 환경에 적합하도록 전송되는 EMM 자체를 최소화 하였다.

또한 국내 기술로 모바일 CAS를 해외사업자에 비해 이른 시기에 개발하여 적용함으로써 향후 해외 사업을 펼칠 수 있는 좋은 Reference 확보라는 성과를 이루어냈다. 또한 그 동안 모바일 방송에 적합하지 않은 CAS를 가진 해외 Major CAS 업체에 비해 기술적인 우위를 점함으로써 향후 기술 Trend를 이끌어갈 수 있는 계기 또한 마련할 수 있었다.

이를 바탕으로 그동안 해외업체의 CAS가 장악하고 있던 국내 CAS 시장에 새로운 전기를 마련하여, 서서히 국내 CAS로 대체되는 흐름을 만들어낼 수 있었다. 현재 MCAS는 위성DMB에 적용된 것을 바탕으로 국내 지상파DMB 사업자의 양방향 데이터방송 서비스 적용을 계획하고 있으며, 국내 실시간 IPTV(SK브로드밴드 borad&TV) 서비스에 적용될 예정이다.

해외 사업도 활발히 전개하고 있는데, 중국 Mobile TV 표준인 CMMB향 CAS 개발 및 이에 따른 적용과 함께 태국 MCOT 사와 DVB-H향 CAS를 통한 Trial 서비스를 진행하고 있다. 그 외에도 중동 S2M 사업자를 대상으로 Mobile CAS 적용을 협의 중에 있다.

CAS는 유료방송의 핵심 기술로서, 기술적인 우수성 뿐만 아니라 안정성의 검증에 대해 방송사업자들이 요구하고 있는 실정이다. 따라서 30년 이상 전통적인 CAS를 개발하고 사업화한 노하우가 있는 해외 사업자와 경쟁하기 위해서는 기술적인 우수성은 물론, 국내의 Reference 확보 및 이에 따른 검증 등을 통해 경쟁력을 키워나가는 것이 중요할 것으로 생각된다.

필 자 소 개

최 주 영

- 1995년 2월 : 이화여자대학교 전자계산학과 졸
- 1997년 2월 : 한국과학기술원 전산학과 졸
- 1997년 2월 ~ 2003년 9월 : SBS 기술연구소
- 2003년 9월 ~ 2003년 12월 : SKTelecom PMSB 사업추진단
- 2004년 1월 ~ 현재 : 티유미디어 방송기술팀

김 종 호

- 1999년 8월 : 서울대학교 전기공학부 졸
- 1999년 12월 ~ 2003년 3월 : KL-Net㈜
- 2003년 6월 ~ 2004년 8월 : LG CNS㈜
- 2004년 9월 ~ 현재 : SK텔레콤 C&I기술원