특집 제한수신기술

위성 DMB CAS 소개 및 현황

□ 최주영 : 티유미디어

Ⅰ. 개 요

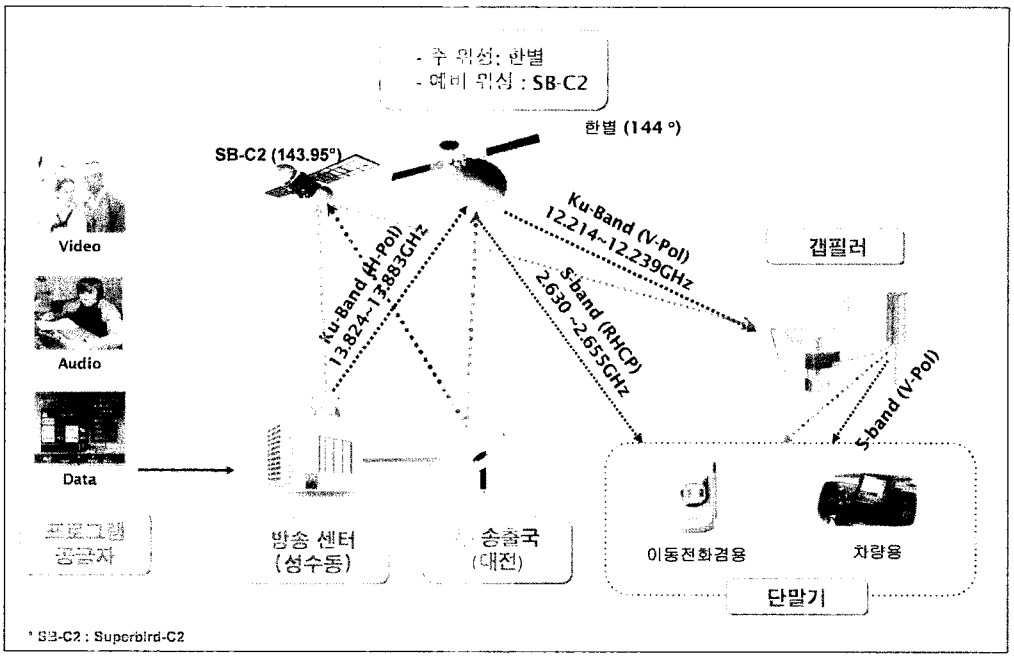
티유 미디어는 2005년 5월 위성 DMB 서비스를 개시한 이후 2008년 11월 현재 약 175만명의 가입자를 확보하고 있으며, 비디오 18 채널, 오디오 19 채널 및 TPEG(Transport Protocol Expert Group, 교통정보 서비스)을 서비스 중이다. 방송 시청을 위해 이동전화 겸용, 전용, 차량용 단말에 이르는 다양한 단말 Lineup을 확보하여 상용 서비스 개시 이래 76종 이상의 단말기를 출시하였다. 위성 DMB는 광고를 주수익원으로 하는 지상파 DMB와 달리 가입자 대상 월정액 유료서비스를 주요 수익원으로 하고 있어 사업 계획 초기 단계부터 CAS(Conditional Access System)을 통한 가입자 관리를 고려하였다. 본 고에서는 티유 미디어의 CAS 기반 유료 서비스 현황과 기술 진화 과정에 대해 설명하고자 한다.

Ⅱ. 위성 DMB 네트워크 및 단말 기술 개요

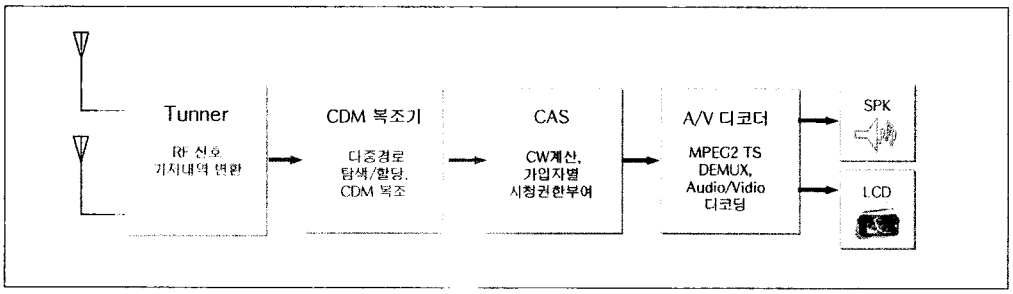
위성 DMB는 음성/영상 등 다양한 멀티미디어 신호를 디지털 방식으로 위성 및 갭필러 네트워크를 통해 이동전화 겸용, 전용, 차량용 단말에 제공하는 서비스이다.<그림 1>

위성 DMB 서비스에 가입한 고객만 방송을 시청할 수 있도록 하기 위해 방송센터에서 송출되는 신호는 CAS를 이용하여 암호화되어 송출되며, 단말은 단말에 저장된 시청권한을 이용하여 암호화된 방송 신호를 복호화하여 방송을 재생한다.<그림 2>

위성 DMB는 ARIB 규격에 따라 30개의 CDM을 이용하여 방송 서비스를 제공한다. 이 CDM중 3개의 채널(Pilot, EPG, CAS)를 시스템 채널로 할당하고 나머지 27개의 채널을 활용하여 비디오, 오디오 및 TPEG 서비스를 제공하고 있다. CAS 채널은 가



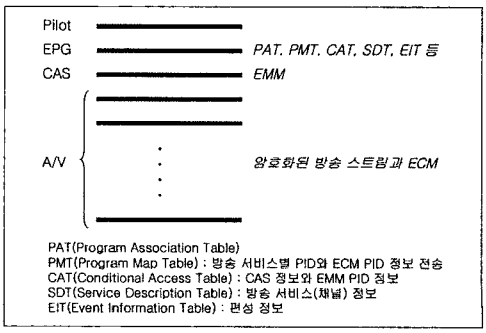
<그림 1> 위성 DMB 네트워크 구성



<그림 2> 단말 수신 절차

입자 관리를 위한 EMM(Entitlement Management Message, 가입자 관리 메시지) 전송에 사용되고 있으며, 비디오, 오디오 및 TPEG 채널은 CAS에서 생성한 CW(Control Word, 암호화키)를 사용하여 암호화되어 전송된다. 해당 채널을 복호화하기 위한 CW는 ECM(Entitlement Control Message)에 포함되어 해당 서비스 채널로 전송된다.<그림 3>

단말은 방송 시청 중 Pilot, EPG, CAS 채널을 항상



<그림 3> 위성 DMB 전송 구성도

백그라운드로 수신하여 방송 재생에 필요한 각종 시스템 정보를 얻게 된다. EPG 채널의 PMT와 CAT에 포함된 ECM, EMM PID를 활용하여 ECM과 EMM을 필터링하게 되고, 이를 활용하여 ECM에 포함된 CW를 추출하게 된다. 단말은 추출된 CW를 이용하여 암호화된 비디오, 오디오 및 TPEG 채널을 복호화하여 가입자에게 DMB 서비스를 제공하게 한다.

위와 같은 CAS의 기능을 기본으로 티유 미디어는 2단계의 진화를 거쳐 현재의 CAS 시스템을 구축하게 되었고, 이를 활용하여 1개 이상의 채널로 구성된 다양한 월정액 상품과 프로그램별 시청이 가능한 PPV 상품으로 가입자에게 유료 서비스를 제공 중이다.

III. CAS 진화 단계

티유 미디어는 <그림 4>와 같이 고객의 서비스 편리성을 증대시키고, 모바일 환경에 적합하도록 CAS를 발전시켜 왔다.

이동전화 겸용 단말에 CAS를 적용하는 최초의 모바일 방송이었기 때문에 각 단계별로 적용된 CAS 기술은 다양한 검토와 시도를 거쳐 개발된 것이었고, 세계 최초로 적용되는 것이어서 모바일 CAS 기술 도입과 발전에 많은 영향을 주었다.

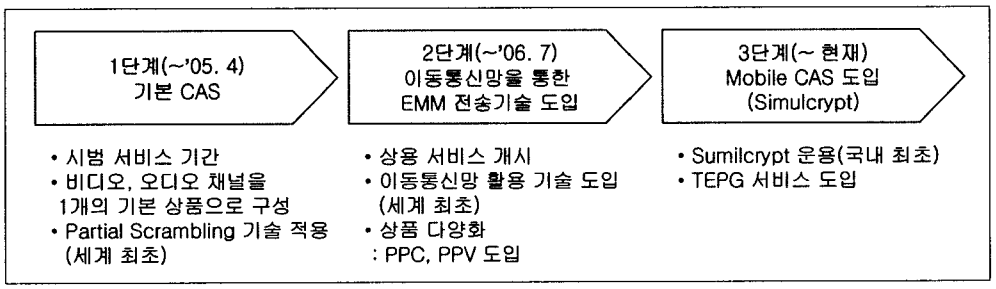
각 단계별로 도입된 기술은 아래와 같다.

1. 초기 단계 : 위성 DMB 시범서비스 기간 (~' 05. 4)

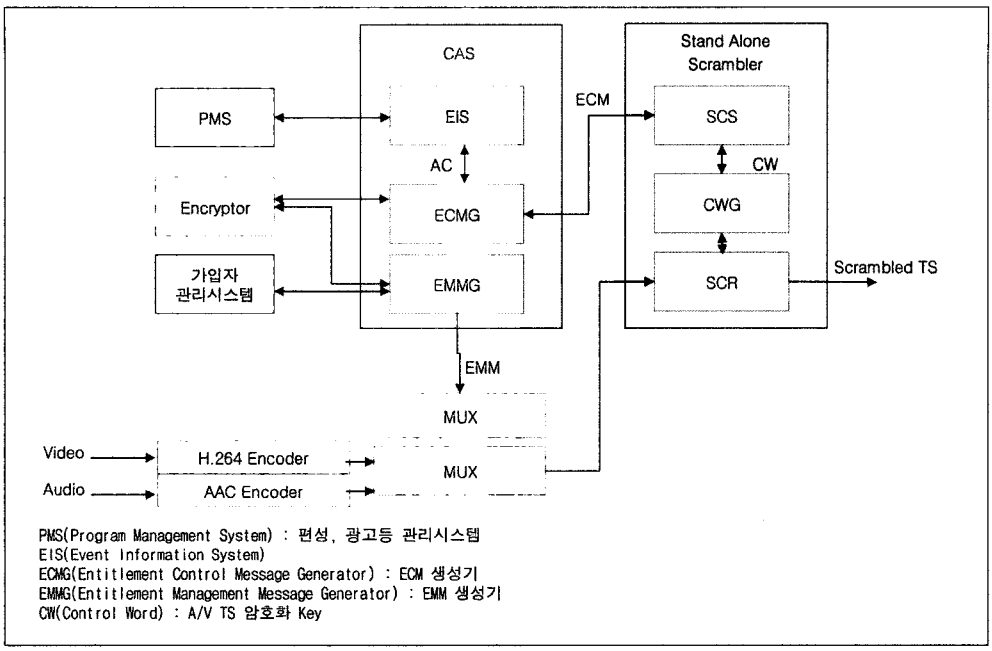
티유 미디어는 사업 계획 단계부터 CAS 사업자를 선정하여 H/E 및 단말 개발에 CAS 기능을 고려하여 설계하였다. 이동전화 겸용 단말에 CAS를 적용하는 최초의 사례였기 때문에 H/E 구성 뿐만 아니라 단말의 성능에 대한 검토도 필요하였다. 초기 단계는 위성 DMB의 가입자 관리 시스템과 방송센터에 CAS를 통합하고<그림 5>, 단말은 EMM 및 ECM을 수신하고 이를 이용하여 암호화된 방송신호를 복호화하여 재생하는 데에 초점을 두었다.

이동전화 겸용 단말의 성능을 고려하여 방송신호의 일부만을 암호화하는 Partial Scrambling 기술을 도입하였다. Partial Scrambling 기술은 H.264 및 AAC 인코딩 특성을 고려하여 일부 패킷에 한해 암호화하여 전송하는 기술이다. 암호화될 패킷은 H.264 Encoder와 AAC Encoder에서 마킹되어 Scrambler로 전달되고 Scrambler는 패킷 헤더에 포함된 암호화 Filed를 참조하여 암호화하게 된다.<그림 6>

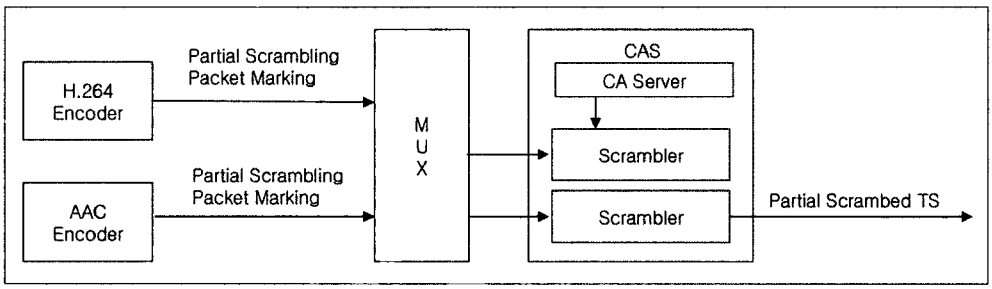
위성 DMB 서비스의 가입자 관리는 가입자 관리 시



<그림 4> 위성 DMB CAS 진화 단계

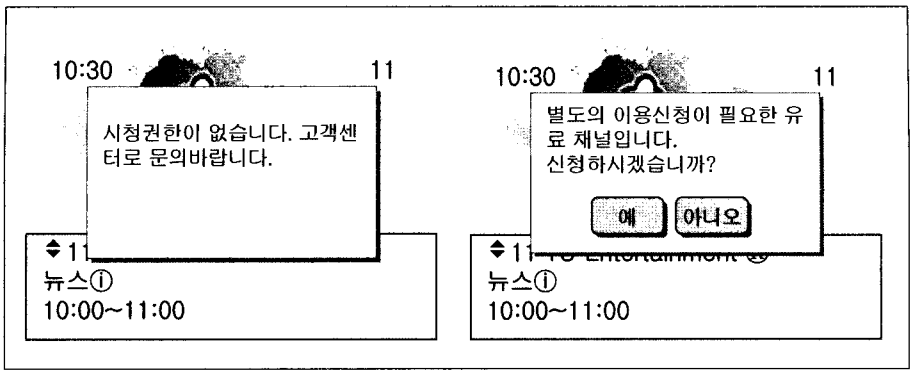


<그림 5> CAS H/E 및 연동 구성도



<그림 6> Partial Scrambling 기술

스템, CAS, 단말의 연동을 통해 수행된다. 위성 DMB 서비스를 가입하면 가입자 관리 시스템에서 보낸 가입 정보가 CAS로 전달되고 CAS는 이에 해당하는 시청권한을 생성하여 해당 가입자의 단말기로 EMM을 전송하게 되고, 단말은 이를 수신하여 단말내의 저장장치에 시청권한을 저장한다. 고객이 단말에서 위성 DMB 방송 서비스를 시작하게 되면 단말내의 CAS Client는 수신된 방송신호에 포함된 정보와 단말 내에 저장된 시청권한을 비교하여 가입된 서비스일 경우에는 방송신호를 복호화하여 재생하게 되고, 가입되지 않은 서비스일 경우에는 <그림 7>과 같이 시청이 불가능함을 알리는 창을 띄우게 된다. 단말로 전송되는 가입을 위한 EMM은 단말에서의 수신을 보장하기 위해 일정 기간동안 반복적으로 전송되고, 시청권한



<그림 7> EPG 상의 가입안내 창

을 관리하기 위한 EMM도 권한 갱신과 보안을 위해 지속적으로 반복 전송되도록 하였다.

그러나, 시스템 통합 작업 단계에서 가입 EMM 수신 시간이 고객에게 불편을 끼칠 수 있다는 문제가 제기되어 이동통신망을 통한 EMM 전송 기술을 검토하게 되었다.

2. 이동통신망을 통한 EMM 전송 기술 도입 단계 : 위성 DMB 상용서비스('05. 5) ~ '06. 7

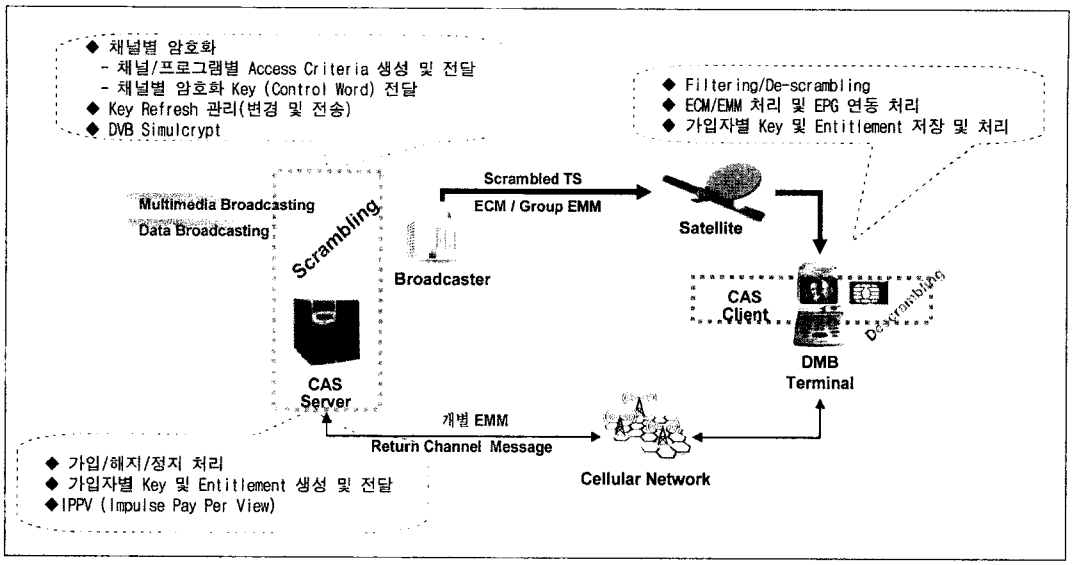
기존 CAS는 대부분 유선 기반의 STB 환경을 대상으로 개발 및 상용화된 제품이어서 모바일 단말(이동전화 겸용 및 차량용 단말)을 대상으로 하는 위성 DMB 서비스에는 적합하지 않은 부분이 있었다. 즉, CAS에서 방송망을 통해 전송하는 EMM은 STB에서의 수신 여부를 확인할 수 없어 일정 기간 동안 주기적으로 반복 전송하는 특징이 존재한다. 그러나, 아래와 같은 환경 차이에 의해 개선점을 모색하게 되었다.

STB 환경은 방송 수신만을 목적으로 하고 있으며 유선기반이므로 첫째, EMM 전송이 보장되고 안정적이며 둘째, 전원이 항상 연결되어 있어 백그라운드로 EMM을 받을 수 있어 반복 전송하는 주기를 길게 설정해도 영향이 없고 셋째, EMM 및 ECM 손실의 가능성이 적다는 특징이 있다.

반면 모바일 단말 환경은 이동전화 겸용 단말이 대부분으로 방송수신 외에 통화, 무선인터넷, 카메라, 게임 기능 등을 이용할 수 있으므로 배터리 사용 시간에 제약이 있어 EMM을 백그라운드로 수신할 수 없고 방송시청 중에만 수신할 수 있는 등의 많은 제약이 존재한다. 또한 모바일 환경에서 EMM 전송 성공율을 높이고 빠른 시간 내에 전달하기 위해서는 EMM 전송 주기를 빠르게 해야 하는데 이럴 경우에는 EMM 전송에 많은 리소스가 소요되어 가입자 수용에 한계가 발생한다.

위의 문제를 해결하기 위하여 이동전화 겸용 단말에 한하여 EMM중 일부를 이동통신망을 통해 전송하는 기술을 도입하게 되었다.<그림 8>

즉, 암호화된 방송 신호, ECM , Group별로 전송되는 EMM 및 전용/차량용 단말로전송되는 EMM은 기존대로 방송망을 통해 전송하고 이동전화 겸용 단말의 개별 가입자로 전송되는 EMM은 이동통신망을 통해 전송한다. 이동통신망으로 전송되는 EMM은 이동통신사의 OTA(Over The Air) 또는 SMS를 통해 단말에 전송되는데 가입자의 이동통신사 정보와 이동



<그림 8> 이동통신망을 통한 EMM 전송

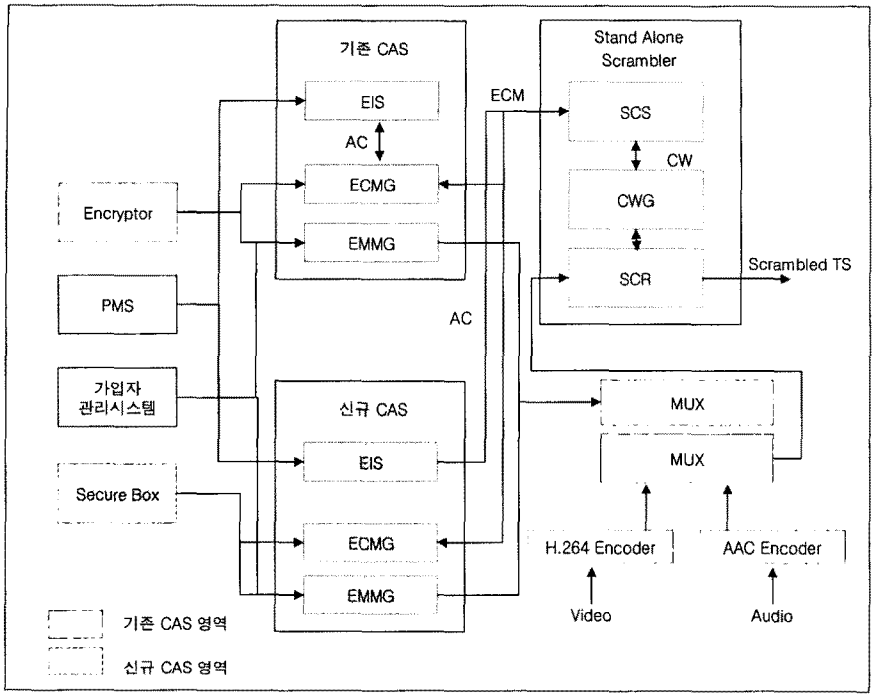
전화 번호를 활용하여 티유 미디어의 CAS에서 생성된 EMM이 전용회선을 통해 이동통신사의 OTA/SMS 서버로 전송되고 이동통신사는 해당 가입자 단말로 OTA/SMS 메시지를 생성하여 전송한다.

단말은 OTA/SMS를 통해 전송받은 EMM을 단말 내 저장장치에 저장하여 위성 DMB 서비스를 이용할 수 있도록 지원한다. 본 기능의 도입을 통해 방송 시청 환경과 무관하게 EMM을 수신할 수 있게 되어 고객의 가입후 위성 DMB 시청이 편리하게 되었으며, 방송망으로 전송되는 EMM의 상당부분을 이동통신망을 통해 전송하게 되어 제한된 방송 리소스를 절감하게 되었다.

3. 모바일 CAS 개발 및 Simulcrypt 적용 단계 : '06. 8 ~ 현재

이동통신망을 통한 EMM 전송 기술이 안정적으로 동작하게 되면서 CAS를 모바일 환경에 최적화하는 방안에 대해 검토가 시작되었다. 기존 CAS를 분석한 결과 보안성을 높이기 위해 도입된 다단계의 Key 전송 방식을 변경할 수 있으면 방송망으로 전송되는 EMM을 최소화할 수 있을 것으로 검토되었다. 그러나 기존 CAS를 수정할 경우 이미 서비스에 가입된 단말에 역호환성을 보장하기 어려워 신규 CAS를 개발하여 2개의 CAS를 Simulcrypt로 운영하는 것으로 결정하였다. 신규 CAS는 설계 단계부터 모바일 환경을 Target으로 하여 SK Telecom과 티유 미디어가 공동으로 개발하여 '06년 8월 상용화에 성공하였다.

모바일 CAS는 기존 CAS와의 서비스 연계 및 Simulcrypt 구성이 필수적이었기 때문에 개발과 동시에 PMS, 가입자 관리 시스템과 Scrambler와의 연동 특히 ECM 생성을 위한 CW 연동에 초점을 맞추었다.<그림 9> 출시된 단말이 복수의 CAS 정보를 수신할 경우 발생할 수 있는 오류에 대비하기 위해 Testbed 시험 및 시험 채널 운용 단계를 거쳐 신규 CAS를 도입하게 되었다. 신규 CAS 도입 후



〈그림 9〉 신규 CAS 도입후 Simulcrypt 구성도

Simulcrypt 적용으로 EMM, ECM은 CAS별로 분리되어 송출되고, 단말은 해당 단말에 적용된 CAS에 따라 EMM, ECM을 선별 수신하여 고객에게 서비스를 제공한다. CW는 기존 CAS와 신규 CAS가 공유하여 비디오, 오디오 채널의 암호화는 기존 방식대로 진행되며, 공유된 CW는 개별 CAS의 ECM 규격에 맞추어 전송된다.

티유 미디어 모바일 CAS의 특징은 아래와 같다.

첫째, 기존 CAS는 Key 방식을 채택하였으나, Key와 알고리즘 방식을 통합한 CAS 기술로 개발하였다.

둘째, 이동전화 겸용 단말기로 전송하는 대부분의 EMM은 이동통신망(대역외 채널)을 통해 전송하도록 하여 방송망 리소스 사용을 최소화 하였다. 기존 CAS에 대비하여 방송망으로 전송되는 EMM의 비율이 20% 수준으로 이동전화 겸용 단말의 가입자 증가가 방송망 리소스 사용에 미치는 영향은 미미하다.

세째, 모바일 환경의 특성상 수신 중 발생할 수 있는 EMM 및 ECM의 손실에 대비하여 단말에서의 EMM, ECM 손실 검출 절차를 강화하여 단말에서의 에러 발생을 최소화하였다.

넷째, 단말의 특성을 고려하여 이동전화 겸용 단말과 차량용 단말의 EMM 종류와 전송 방식를 달리 적용하였고, 추가의 리소스 절감이 가능하도록 하였다.

다섯째, 향후 DRM 서비스와의 통합을 고려하였고, 선불권 등 다양한 Pay TV Model에 대한 지원이 가능하다.

티유 미디어는 모바일 CAS 적용을 통해 기존의 CAS 리소스에서 1,000만명 이상의 가입자를 수용할 수 있게 되었다.

Ⅳ. CAS 기반 서비스

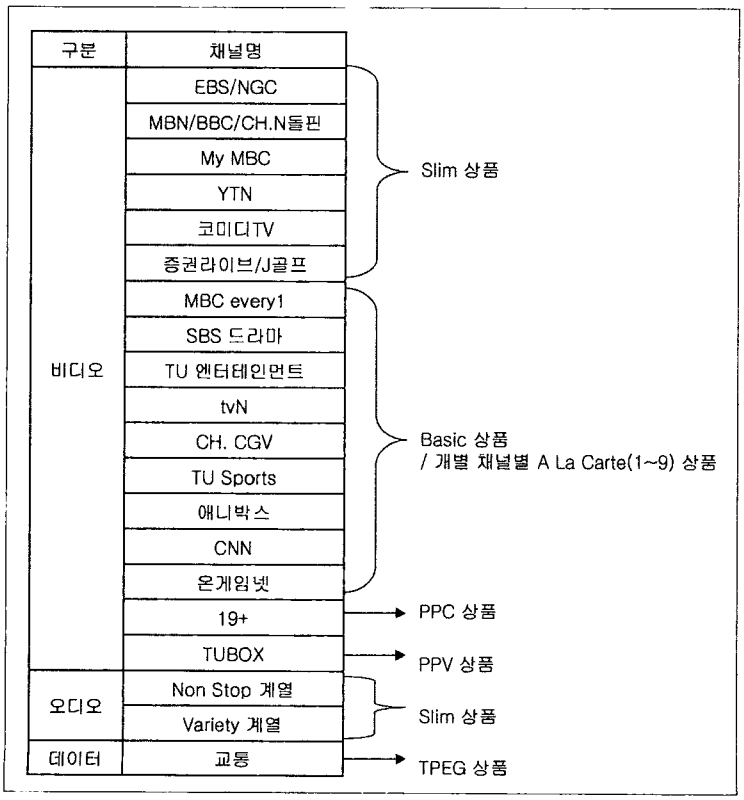
1. 월정액 서비스

티유 미디어는 <그림 10>과 같이 월정액 상품을 구성하여 고객에게 다양한 상품 선택권을 제공하고 있다. 가장 기본이 되는 것은 비디오 채널 일부와 오디오 채널 전체를 포함한 Slim 상품으로 Slim 상품에 가입한 고객은 Basic 상품, Basic 상품 구성채널을 개별적으로 재구성한 A La Carte 상품, PPC, PPV 상품 등에 추가 가입할 수 있다.

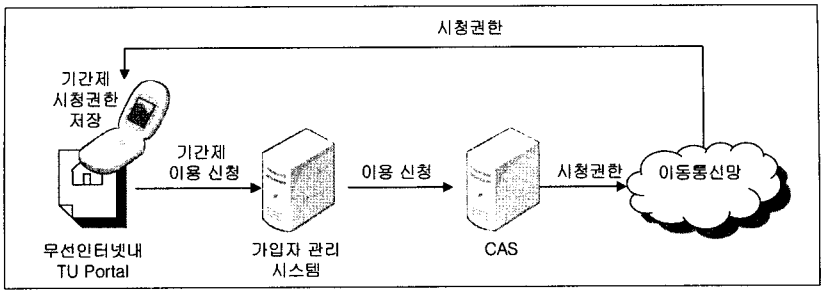
월정액 서비스를 위한 상품 정보는 ECM에 포함되어 전송되며, 단말은 ECM에 포함된 상품정보와 시청권한을 비교하여 해당 채널을 재생한다.

2. 기간제 이용 서비스(Pay Per Day 변형 모델)

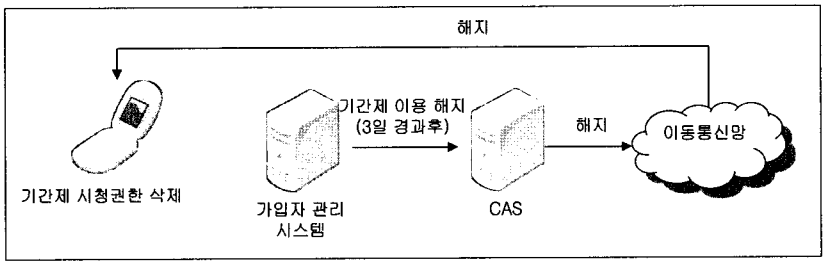
Slim 상품에 가입한 고객은 19+ 서비스 채널을 월정액이 아닌 기간제로 이용할 수 있다. 기간제 이용 서비스는 현재 3일 이용권으로 제공되어 이용 신청 후 3일까지 19+ 서비스 채널을 시청할 수 있다. 이용 신청은 무선인터넷상의 TU 홈페이지를 통해 가능하며 이용 신청시 해당 서비스 채널의 시청권한이 EMM으로 단말에 전송되어 저장되고, 고객은 수



<그림 10> 티유미디어 월정액 상품 구성 현황



<그림 11> 기간제 이용권 신청 및 시청 절차



<그림 12> 기간제 이용권 해지 절차

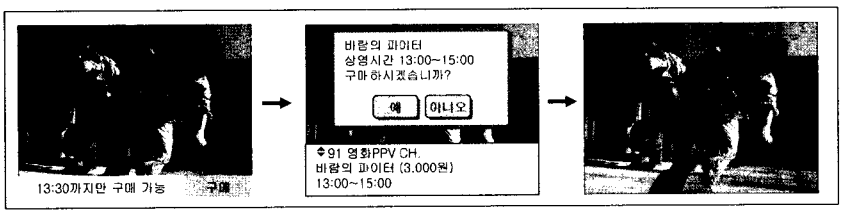
분 내로 해당 서비스 채널을 시청할 수 있다.<그림 11> 3일 경과 후에는 가입자 관리 시스템에서 자동으로 시청권한을 해지시키며, 해지 EMM이 단말로 전송되어 시청권한이 삭제된다.<그림 12>

기간제 이용 서비스는 '09년에 이용 가능한 채널을 확대할 예정이다.

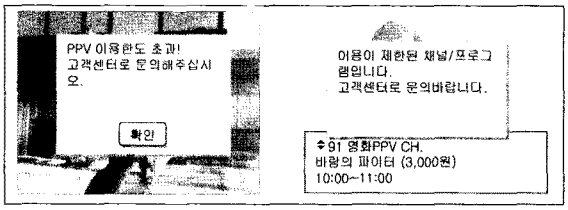
3. PPV(Pay Per View)

PPV 서비스는 프로그램 별로 시청을 신청하고 과금이 되는 서비스이다.<그림 13> 프로그램 시작 초기에 미리보기 시간을 두어 일정시간 시청한 후 전편 시청을 원할 경우 프로그램 구매 신청을 하게 되면 단말에 PPV 신청 이력이 저장되고 단말의 CAS 기능을 통하여 시청이 가능하도록 한다. 단말의 PPV 신청 이력은 이동통신망을 통해 PPV 이력 관리서버로 전송되어 월 이용료와 함께 이용요금이 청구된다.

PPV의 무분별한 신청 및 청소년 가입자 보호를 위해 단말에 월 이용한도 및 청소년 시청 제한 기능



<그림 13> PPV 신청 및 시청 절차



<그림 14> PPV 이용한도 관리 및 이용제한 기능

을 설정하여 월 이용한도를 초과할 경우 PPV 신청이 처리되지 않도록 하였으며 청소년 시청 불가 프로그램일 경우 프로그램 미리보기 기능부터 제한하게 된다.<그림 14>

V. 향후 계획 및 과제

CAS는 유료 방송에서의 핵심 기술로 위성 DMB 서비스의 CAS는 모바일 환경에 적합하도록 진화된 첫번째 사례이며, EMM을 이동통신망이라는 대역외 채널(방송망 이외 채널)로 전송하는 획기적인 진화를 이루었다. 또한 국내 기술로 모바일 CAS를 개발하여 적용함으로써 국내에서 많은 업체들이 CAS를 개발하고 해외 시장에 진출하게 하는 시발점이 되게 하였다. 국내 기술로 CAS를 개발하여 위성 DMB 수신 기능과 CAS 기능을 결합한 Chip도 다양하게 개발되었고, 서비스 확장 측면에 있어서도 신속성과 융통성을 가지게 되었다.

티유 미디어도 가입자에게 보다 다양한 서비스를 제공하고, 편리하게 이용할 수 있도록 CAS 기능을 확장하고 있으며, 모바일 CAS의 특화 영역에서 기술 우위를 점할 수 있도록 계속하여 신규 기술을 적용할 예정이다.

특히 DRM 기술과의 결합을 통해 녹화 기능을 확대하여 언제, 어디서나 시청이 가능한 모바일 방송의 장점을 배가시킬 예정이며, 기간제 이용권 확대 등을 통해 고객이 선택할 수 있는 상품을 다양하게 할 계획이다.

필자소개

최주영

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