IPTV 정보 보호 기술 동향+

박종열* · 백의현*

*한국전자통신연구원 소셜미디어서비스연구팀

목 차

Ⅰ. 서 론
Ⅱ. 관련연구
Ⅲ. IP 기반 방송의 문제점
Ⅳ. 다운로드 가능한 방송 수신 제어
Ⅴ. 결 론

Ⅰ. 서 론

인터넷 사용자의 급속한 증가는 IT 산업 발전에 큰 견인차 역할을 수행하여 왔다. 그 중에서 IP 망을 이용한 방송 및 VOD(Video on Demand) 서비스는 네트워크 기술의 발달과 더불어 크게 발전하고 있다. 인터넷을 통한 콘텐츠의 유통은 무료라는 고정 관념과 달리 IPTV 서비스는 실시간 방송과 더불어 유료화 되었다. 기존의 유료 방송은 방송 제공 형태에 따라서 크게 달라지고 서비스를 제공하기 위해 필요한 기술 및 사용하는 자원에 따라서도 가격 및 서비스 제공 방법이 달랐다.

IPTV 서비스를 다른 방송 서비스와 차별화하기 위해서는 IP 망이 가지고 있는 장점을 최대한 활용해야 한다. 가장 쉽게 생각할 수 있는 방법은 양방향 데이터 방송이다. IP 망의 양방향성을 활용하여 인터넷의 지식 검색, 시청중인 프로그램의 제작자 정보, 인기 드라마 순위와 같은 정보를 연동하는 것이 가능하다. 이는 단방향인 기존 방송을 양방향으로 진화하는 것으로 데이터 방송이라는 형태로 개발되고 있다. 기존 방송 시스템에서도 이와 같은 기능을 지원하기 위해서 전화선(PSTN)[1], 케이블(DOCSIS), 인터넷 모뎀과 같은 반대 방향의 통신 채널(return channel)을 경쟁적으로 확보하고 있다. 기존의 방송망에서는 양방향 방송을 수신하기 위해서 별도의 통신 채널을 만들어야 하기 때문에 사용자에게 불편함과 추가비용을 요구했다.

IPTV의 경우 이러한 문제점을 쉽게 해결할 수 있다. 또한 사용자의 성향에 따라 제공하는 맞춤형 방송, 사용자들의 실시간 참여가 가능한 대화형 방송 및 다차원 정보를 제공하는 3D TV와 같은 새로운 방송 환경 적응도 쉬운 특징이 있다. 또한 이러한 방송이 특정 사용자에 한정되지 않고 IPTV 가입자라면 누구에게나 사용될 수 있는 개방형 서비스의 특징을 가진다.

IPTV 방송은 방송 그 자체 보다는 방송과 연계되는 부가 서비스의 개발이 용이하고 다양한 형태의 시스템 적용이 가능하다는 특징이 다른 방송과 차별화된다. 이와 같이 유연한 서비스를 제공하기 위해서는 기존의 방송 수신 제어 기술도 변화가 필요하다. 유연하고 융합화된 서비스를 지원하기 위해 다양한 형태의 방송 수신 제한(Conditional Access System: 이후로 줄여서 CAS)이 가능한 기술이 개발 되어야 한다.

IPTV는 기본적으로 IP라는 공개된 망을 통해서 전송되기 때문에 무한대에 가까운 채널 확장이 가능한 반면 불법적인 시청이 용이한 특징도 가지고 있다. CAS 기술이 적용되지 않는다면 옆집에서 시청중인 유료 채널을 같은 서브넷에 연결된 사용자가 네트워크 도청만으로 쉽게 볼 수 있다. 따라서 콘텐츠 제작자들은 방송 수신 제한(CAS) 기술을 통해 사용자의 불법적인 접근을 제어하고 있다.

+ 본 연구는 정보통신 산업원천기술개발사업의 일환으로 수행하였음 [2009-S-003-01, IPTV 기능고도화 및 서비스 확장을 위한 미들웨어 및 보안 플랫폼 기술개발]

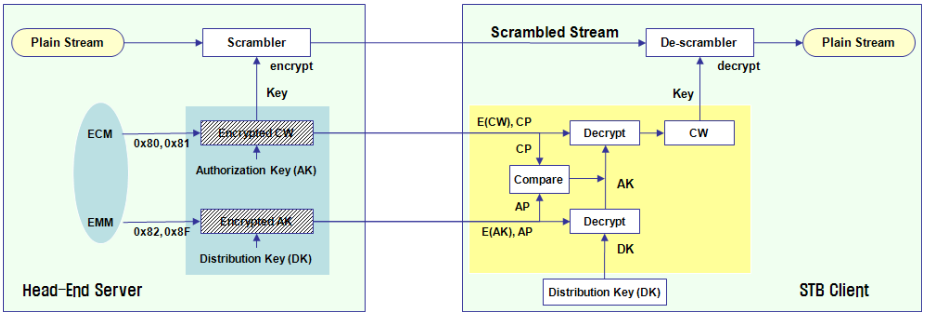

그림 1. CAS 방식의 수신 제한 시스템

지금까지의 방송 수신 제한(CAS) 기술은 방송의 형태 보다는 사업자의 논리에 따라서 상호 배타적인 형태로 개발되어 왔다. 실제 데이터 방송의 경우 지상파 ACAP[1], 케이블 OCAP[2], 위성 MHP[3]의 표준을 따르고 있지만 방송 수신 제한(CAS) 기술은 표준보다는 업체별 제공 기능에 더 의존하고 있는 형상이다.

Ⅱ. 관련연구

유료 방송 서비스에서 방송 수신 제한 기술은 사업자의 수익성과 직접적인 관계를 가지고 있기 때문에 매우 중요한 기술로 인식되고 있다. 때문에 사업자의 선택보다는 보안 제품을 공급하는 회사의 운영 방침을 따르는 경우가 많고, 사용되는 기술뿐 아니라 사용되는 세부 알고리듬 조차도 외부에 공개하지 않는 실정이다.

유료 방송에 대한 사용자의 접근을 제어하는 방법은 기술 적용 방식에 따라 CAS(Conditional Access System) 와 DRM(Digital right Management) 방식으로 분류된다. 또는 이 두 가지 기능을 혼합한 방식이 연구되고 있다. 사용자의 불법적인 접근을 방지하기 위해서는 사용자를 인증하고 그의 접근을 적절하게 제어하는 기술이며, 이때 접근 서비스를 중심으로 하는 경우 CAS 방식, 콘텐츠를 중심으로 하는 경우 DRM 방식으로 구분한다.

1. CAS 기반의 접근 제어 연구

CAS란 전통적인 의미로 조건에 맞게 사용자의 접근을 제한하는 기술로 과거 아날로그 방송에서 사용되는 스크램블(Scramble) 방식을 주로 의미한다. 방송 채널에 대한 접근을 제어 한다는 광의적인 의미에서는 수신 제한을 위한 모든 기술을 의미하기도 한다. CAS는 방송을 전송하는 측에서 비밀번호(Control word)를 생성하고 생성된 비밀번호를 기반으로 영상을 스크램블(Scramble)하여 전송한다. 수신기는 해당 채널의 ECM(Entitlement Control Message), EMM(Entitlement Management Message) 정보를 기반으로 스크램블 정보를 복호화(De-scramble)한다. 복호화 과정에서 사용자는 스마트카드(Smart-card) 혹은 실시간 키 분배를 통해 제공하는 복호화키(Distribution Key)를 이용해서 ECM, EMM 메시지를 다시 CW로 복호화하는 과정을 거치면 정상적으로 방송을 수신할 수 있다.

그림1은 기존 방송의 수신제한 시스템을 보여준다. CW(Control Word)를 이용하여 실시간 복호화(De-scrambling) 과정을 수행하기 때문에 그 과정이 단순하다. 이로 인해 제공되는 제어 방법은 한정된 수준에 그치고 있는 단점이 있다. 최근 연구는 케이블 방송 연합에서 설립한 PolyCipher에서 기존의 CAS POD(point of Deployment) 모듈(스마트카드 형태)을 대치하는 다운로드 형태의 보안 솔루션을 개발하고 기술 시험 중에 있다.

2. DRM 기반의 수신 제한 기술 연구

협의적인 의미에서 DRM 기술은 임의의 디지털 정보에 대해서 그 정보의 생성자가 누구이며, 어떤 사람에게 어떤 권리를 부여하는가를 전자적으로 표현하는 기술이다. 멋진 예술 사진이 인터넷에 공개되면 그 그림의 원 저자가 누구이며, 누가 그 정보에 대한 기술적 권리를 가지는가를 나타내는 기술이다. 또한 권리 표

현과 더불어 저작권자의 승인 없이 불법적으로 게시하거나 사용하는 것을 차단하기 위한 기술이 동반된다. 광의적인 의미에서 DRM 기술은 불법적인 콘텐츠의 사용과 접근을 방지하는 일련의 기술을 의미한다. DRM 기술은 원본 자료에 DRM을 위한 추가적인 정보를 삽입하는 것으로 저자 이외에는 그 정보를 식별하거나 확인할 수 없다.

최근 DRM 기술은 저작권 보호 기술은 물론 암호화 알고리즘을 이용한 콘텐츠의 배포 관리, 워터마킹 기술을 이용한 콘텐츠 관리 기술이 개발되고 있다. 방송 수신 제한 기술을 위해서는 방송 스트림의 암호화키를 표준 DRM의 분배 방식을 따르는 방법이 있다. 암호화 키의 분배가 쉽고 공인 인증서와 연동이 쉬운 장점이 있지만, 다양한 형태의 접근 제어 기술을 수용하기에는 채널 별로 키를 관리해야 하기 때문에 키 분배 및 관리에 문제점이 있다.

3. 암호 이론 기반의 접근 제어 기술 연구

IPTV 방송의 접근 제어를 위해서는 사용자 인증, 시스템 인증, 키 분배, 암호화, 복호화라는 일련의 과정을 거친다. CAS 방식 혹은 DRM 방식은 모두 기존의 서버 시스템과 호환성을 가지는 방식인데 반해 암호 이론 기반의 접근 제어 기법은 다양한 형태로 구성이 가능하다. 하지만 방송 시스템이 가지는 특징을 반영하면 CAS 방식에서 스크램블(Scramble) 방식이나 키 분배를 위한 스마트카드(SmartCard) 인터페이스 부분을 변형하는 연구가 많이 진행되고 있다.

Ⅲ. IP 기반 방송의 문제점

IP 네트워크를 이용한 방송 전송 기술은 초고속 인터넷과 BCN(Broadband Convergence Network), CDN (Contents Distribution Network) 기술의 발전으로 많은 기술적 진보를 이루었다. 특히 사용자의 고품질 방송에 대한 욕구로 인해 HD급 영상의 손실 없는 전송으로 IP 네트워크를 선호하게 되었다. 특히 오래된 도시에서 낡고 오래된 기존 방송 케이블은 새로 케이블을 설치하기 보다는 빠르고 효율성이 뛰어난 IP 네트워크를 설치하는 것이 훨씬 효과적이고 저렴하다.

IP 네트워크를 이용하여 고품질의 영상을 전송하는 경우 다양한 형태의 영상을 전송할 수 있는 장점과 IP 네트워크를 이용한 새로운 서비스의 적용이 쉬운 특징을 가지고 있지만, 공개된 네트워크를 이용하기 때문에 불법적인 시청 및 해킹 가능성이 높아진다. 이와 같은 문제점을 정리하면 다음과 같다.

1. 사용자의 불법적인 방송 시청

IPTV에서 방송 데이터를 멀티캐스트 방식을 이용해서 전송한다. 멀티캐스트 방식이란 동일 네트워크에 다른 사용자가 있는 경우 하나의 전송으로 여러 사용자가 받아서 볼 수 있는 특징을 제공한다. 따라서 가입자 정보를 기반으로 네트워크 인증을 하는 경우는 동일 네트워크의 다른 사용자가 접근 하는 것을 방지 할 수 없다. 또한 사용자의 전송 중간에서 네트워크 가로채기(TCP-hijacking) 기술을 이용해서 연결되어 있는 세션에 대해서 연결을 가로채는 공격도 쉽게 이루어진다.

2. 콘텐츠 제공자에 종속적인 수신제한 기술의 보급

콘텐츠 제공자는 자사의 콘텐츠가 불법적으로 유출되는 것을 방지하기 위해서 다각도의 노력을 취한다. 콘텐츠의 불법 유출은 “영화→비디오→방송”으로 이어지는 자사의 수익 모델에 큰 영향을 미칠 뿐만 아니라 기존 유료 이용자들의 이탈을 조장할 수 있기 때문에 매우 중요하다. 최근에는 불법적인 유출뿐 아니라 유통에 대해서도 처벌을 하는 등 그 대응이 더욱 적극적이다. 특히 영화에 대해서는 더욱 적극적이다. 대부분의 영화사들이 자사의 영화를 공중파 방송(지상파, 케이블, 위성)에서 유료로 송출하기 위해서는 일정 수준 이상의 수신 제한 기술을 요구하는 경우가 많다. 실제 허리우드 영화사에서는 텔코디아(구 벨연구소)에서의 안전성 검증을 요구하는 사례가 늘고 있다.

보안성 관련 이슈로 방송 수신 제어 기술을 가지고 있는 회사와 콘텐츠 제작사들 사이의 공조가 강해지면서 세계적인 기술을 인정받는 몇 개 업체가 전체 시장을 석권하는 문제점을 발생시켰다. 이로 인해 선도 기업들은 타 기술과 연동하는 기술도 공개 하지 않아 신규 사업자의 시장 진출을 막을 뿐만 아니라 새로운 기술 개발도 더디게 하는 결과를 낳았다. 결과적으로 콘

텐츠 제공자의 요구에 맞는 수신 제한 기술 업체의 기술료는 올라가고, 그 회사의 서버 제품, 그 회사의 방송 수신 제어 모듈을 탑재한 단말(STB), 케이블 카드를 일괄 구입해야 했다.

3. 방송 수신 제어를 위한 새로운 기술 적용 어려움

방송 수신 제어 기술은 그 기술의 안전성이 가장 중요한 요소이다. 따라서 새로운 기술을 적용하기 위해서는 그 기술의 안전성 및 장기간의 시험을 거쳐야 한다. 이것은 그런 과정을 거치지 않으면 새로 개발된 방송 수신 제어 기술의 오류가 발생하는 경우 관련 기기의 교체 비용이 상상하기 힘들 정도로 크기 때문이다. 따라서 많은 사업자들이 새로운 기술 적용을 꺼리게 된다. 새로운 방식의 방송 수신 제한 기술을 적용하기 쉽게 해킹이나 오류가 발생하는 경우 이를 쉽게 대처할 수 있는 기술 개발이 필요하다.

4. 사용자 맞춤형 시청 지원 부재

사용자 맞춤형 시청이란 사용자의 취향 및 과거 시청 내역을 기반으로 사용자의 선호 채널을 선택해서 보여주는 기술이다. TV-Anytime Forum[4]에서는 이와 관련된 방송 메타 정보 처리를 위한 기술 개발이 활발하게 진행되고 있다. 디지털 방송과 더불어 SI (System Information) 정보를 가공한 EPG(Electronic Program Guide) 서비스는 사용자에게 방송 안내를 위한 기술로 방송 메타 정보를 처리한 것이다. 이것을 사용자의 선호에 따라 가공하는 것이 맞춤형 시청 기능이다.

맞춤형 시청을 하기 위해서는 SI 정보를 처리하는 기술도 중요하지만 사용자의 요구에 따른 다양한 형태의 유료 방송을 제공하는 것도 중요하다. PPV(Pay Per View)의 경우 사용자가 보고 싶은 프로그램 대금을 지불 하고 시청하고 있지만 대금 청구나 사용자 인증을 위해서 별도의 전화망 연결(상담원 연결)이나 전용 단말기를 이용해야만 하는 단점이 있다.

PPV에서 전용 단말기가 필요한 것은 PPV를 제공하기 위해 필요한 인증 및 대금 지불 과정이 추가되기 때문이다. IPTV의 맞춤형 방송이 활성화 된다면 일방적인 방송 가입(기본 채널 가입)보다는 사용자가 선호하는 채널 혹은 프로그램에 대해서만 지불하는 등 다양한 형태의 방송 시청이 가능하다. 특히 VOD 나 PPV와 같은 유료 콘텐츠에 대해서는 해당 서비스를 받는 동안 수행되는 방송 수신 기술의 실행이 필요하다. IPTV에서 VOD 서비스가 일반화되어 있어서 실시간 방송과 VOD 서비스에 적용되는 각각의 보안 기능이 유기적으로 연동 되어야 한다. 또한 IPTV 서비스에서 제공되는 다른 보안 서비스(금융, 결제, 인증)도 서로 연계되고 동적으로 구성이 가능해야 맞춤형 방송을 효과적으로 지원할 수 있다.

5. 방송 수신 단말 사이의 상호 호환성 부재

기존의 방송 수신 단말기는 서비스 사업자가 제공하고 있다. 동일 방식의 방송을 제공하고 있더라도 서비스 사업자마다 서로 다른 수신 제한 기술을 적용하고 있기 때문에 '갑'에서 제공받은 단말기를 '을'에서 사용하는 것이 불가능 하다.

케이블 방송의 경우 이와 같은 문제점을 해결하기 위해서 케이블카드 방식으로 수신 제한 기능을 분리하고 있지만 실질적으로 케이블카드와 방송 수신 단말이 독립적으로 동작하지 않는 경우가 대부분이다.

방송 채널, 프로그램, 장르, 주인공, 횟수 등 다양한 형태의 수신 제한이 가능하고 콘텐츠 제공자마다 서로 다른 수신 제한 기술이 동작할 수 있도록 하기 위해서는 특정 수신 제한 기술에 종속되지 않고 동적으로 재구성이 가능한 구조가 필요하다. 따라서 이러한 요구사항을 만족하기 위해서는 동적 재구성이 가능하며 다운로드가 가능한 수신 제한 기술이 필요하다.

Ⅳ. 다운로드 가능한 방송 수신 제어

다운로드 가능한 방송 수신 제어 기술은 다운로드 받은 프로그램을 구동하는 방식에 따라서 하드웨어 기반, 가상머신(Virtual Machine) 기반, 소프트웨어 기반으로 구분된다. 다운로드를 위한 공통 기능은 하드웨어 및 시스템에서 공통으로 사용되는 기본 기능을 정의하고 관련 소프트웨어 연동 및 프로그램 다운로드를 위한 일련의 과정을 정형화하여 정의하고 구현하는 것이다. 다음은 수신 제한 기능을 다운로드 하기 위해서 일반적 기능을 정의한다.

- 수신 제어를 위한 소프트웨어 및 하드웨어 기능의 분리 및 연동 인터페이스 정의
- 동적으로 프로그램을 바인딩(Binding) 하고 언바인딩(Un-binding) 하는 프로그램 제어 기능
- 수신 제어 프로그램의 다운로드, 설치, 실행, 제어하는 관리 기능
- 다운로드 프로그램의 인증 및 안전성 검증 기능

위의 내용과 별도로 수신 제어 기능의 다운로드 및 설치 과정에서 IPTV 방송 수신에 영향을 미치지 않도록 하는 프로세스 분리 기능(Process Isolation)도 서비스를 위해서는 중요한 부분이다.

본 논문에서 다운로드 가능한 방송 수신 제한 기술의 기술 범위는 방송 가입자의 인증, 접근 제어 모듈의 전송, 접근 제어 모듈의 단말기 설치의 과정으로 이루어진다. 이 과정을 좀 더 상세하게 기술하면 다음과 같다.

- **방송 가입자의 인증**: 유료 방송은 가입자(혹은 세대 단위)의 가입정보에 따라서 방송의 수신 여부가 결정된다. 또는 가입자의 선택에 따라서 대금 결제 후 시간 단위 혹은 방송 단위의 시청이 가능하기 때문에, 방송 가입자의 인증 과정이 가장 먼저 이루어진다.

- **방송 채널의 Control Word(CW) 생성**: 유료 방송 채널은 기본적으로 암호화(혹은 Scrambling) 하여 전송하기 때문에 방송을 수신하기 위해서는 채널에 대한 Control Word(CW)를 상호 교환하는 과정이 필요하다. 다운로드 가능한 수신 제한 기술은 특정 암호 알고리즘에 종속되지 않으며, 셋톱박스에서 관련된 기능 및 알고리즘을 지원해야 한다.

- **접근 제어 모듈의 생성**: Control Word는 방송 채널을 보호하기 위한 일련의 정보이지만, 접근 제어 모듈은 Control Word와 연동하여 암호화된 방송을 수신하여 원래의 신호를 복원(복조)하는 과정에 관여한다. 이 부분은 사업자마다 혹은 방송사마다 서로 다른 방식이 사용될 수 있다. 특히 방송 수신용 Control Word와 내부에서 사용되는 암호화키의 구조는 업체별로 약간씩 변형하여 운영하고 있다.

- **방송 콘텐츠에 수신 제한 모듈 및 Control Word 정보 결합**: 방송 콘텐츠를 정상적으로 수신하고 시청하기 위해서는 적절한 수신 제한 모듈이 설치되어 방송 콘텐츠에 포함되어 있는 제어 정보(EMM/ECM)를 바탕으로 Control Word를 만들어 내야 한다. 내부적으로 수신 제한 모듈이 제어 정보(EMM/ECM)를 어떻게 처리하는가는 하는 부분은 사업자별로 정의하고 있는 부분이기 때문에 그 내용이 수신 제한 모듈 속에 포함되어야 한다.

- **수신 제한 모듈의 전송, 인증 및 방송 수신기 하드웨어의 인증**: 방송이 전송되는 인터넷은 공유되는 네트워크 환경이기 때문에 불법 도청, 감청이 쉽고 변형된 코드의 수신이 가능하다. 따라서 적용되는 수신 제한 모듈이 변형되지 않고 전송 되었는가 검증하는 기능과 당 모듈을 수신한 하드웨어 셋톱박스가 인증된 놈인가 확인하는 과정이 필요하다.

- **수신 제한 모듈의 단말기 설치 및 실**행: 수신 제한 모듈은 동적으로 설치되고 재 기동하여 방송 수신을 제어한다. 이 과정이 방송 시청 중에 발생하면, 새로운 프로그램을 설치하고 구동하기 위해서 사용자가 많은 시간을 기다려야 하는 문제점이 있다. 이 과정을 극복하기 위해서 실시간으로 메모리 적재 및 실행하는 기술의 개발이 필요하다.

- **접근 제어 모듈을 통한 방송 수신**: 실행중인 수신 제한 모듈은 해당 방송을 수신하고 방송에서 수신 제한 관련 메시지 EMM, ECM을 추출하여 권한에 따라 방송 프로그램을 복호화하고 미디어를 디코더에게 전송하여 출력한다.

다운로드 수신 제한 기술을 적용하기 위한 단말기의 기능은 하드웨어 인증, 사용자 인증, Control Word 생성, CA 이미지의 동적 바인딩이 유기적으로 연동된다. 다음은 각각 기능에 대한 세부적인 설명이다.

1. 다운로드 수신 제한을 위한 셋톱박스

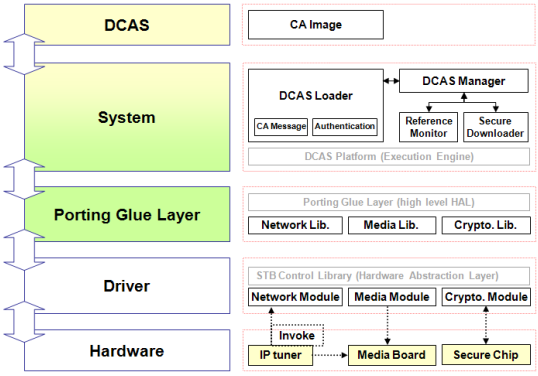

그림 2. 다운로드 수신 제한을 위한 셋톱박스 계층도

방송 수신 제한 기술을 다운로드 하기 위해서는 코드를 다운로드 하는 기술과 더불어 다운로드한 코드를 수행하는 방법이 중요하다. 그림 2는 셋톱박스의 시스템 계층도를 보여준다. 총 5개의 계층(Layer)로 구성이 되며 하드웨어, 드라이버, PGL (Porting Glue Layer), 시스템, 다운로드 CAS가 그것이다. 각각은 다음과 같다.

- **하드웨어**: 망에서 방송 데이터를 수신하고 실시간 해석하여 필요한 정보(SI/PSIP)를 미들웨어 전송하는 역할을 수행한다. 또한 CAS에서는 복호화(Decrypt, Descrambling) 역할을 수행한다.

- **드라이버**: 하드웨어를 제어하는 기능으로, 새로운 기능의 적용이나 하드웨어와 관련된 기능을 수행한다. 보통은 하드웨어 제작 업체에서 기능을 제공하지만, CAS나 미들웨어에서 필요한 기능을 이 수준에서 수정하기도 한다.

- **PGL(Porting Glue Layer)**: 하드웨어 기능을 추상화한 계층으로 데이터 방송 미들웨어를 위해 정의한다. 데이터 방송은 자바 언어로 되어 있고, 드라이버 이하는 C언어로 개발되어 있기 때문에 이 수준에서는 언어 변환(JNI: Java Native Interface) 기능을 수행한다.

- **시스템**: 수신 제한 시스템(CAS)에 필요한 공통 기능과 다운로드 CAS 코드를 실행시켜주는 기능을 수행한다. 실제 다운로드 CAS 코드가 작성되어 있는 형태에 따라서 C 코드 혹은 자바의 클래스 형태로 동작이 가능하며, 동적으로 프로그램을 실행시키고 관리하는 기능을 수행한다.

- **다운로드된 CA 프로그램**: 방송 시청과 동시에 방송 서버에서 해당 방송에 대한 CA 프로그램을 전송하고 이를 수신한다. 다운로드 CA 프로그램은 방송 수신 제한(CAS)을 실행하기 위해 필요한 핵심 코드인 키 관리 기능을 포함하고 있다. CA 코드를 다운로드하여 동적으로 바인딩 하기 위해서는 다운로드 코드 이외의 기능에 대해서는 표준 인터페이스를 제공해야만 한다.

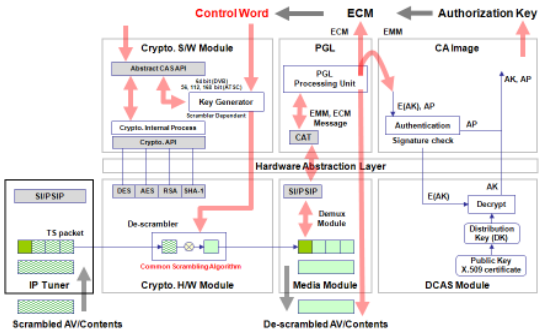

그림 3. 수신 제한 시스템의 정보 흐름도

방송 수신 제한 기술(CAS)은 방송 데이터로부터 복호화키를 뽑아내고 방송 콘텐츠를 복원하는 기능을 담당한다. 그림 3은 암호화된 콘텐츠(Scrambled Contents)로부터 원래의 콘텐츠로 복원하기까지의 구성을 보여주고 있으며 각 모듈 사이에 EMM, ECM 메시지를 Control Word로 만들어 가는 과정을 보여준다. 이 과정에 키 관리자가 다운로드 CA 프로그램의 코드가 된다.

2. 키 매니저를 통한 Control Word의 공유

CAS 기능은 Head-End 서버와 셋톱박스가 동일한 키를 공유하여 콘텐츠를 보호하는 역할을 수행한다. 이 과정에서 방송 콘텐츠 전체를 암/복호화해야 하기 때문에 빠른 연산을 할 수 있는 암호 연산을 사용하게 된다. 따라서 전체 시스템의 보안 강도를 낮추지 않고 빠른 연산을 하기 위해서는 사용되는 키를 주기적으로

갱신하는 방법을 사용한다.

이와 같이 키를 주기적으로 갱신하기 위해서 EMM, ECM 메시지를 방송 콘텐츠와 함께 주기적으로 보내고 있다. EMM은 가입자 그룹에 따라 적용하는 권한으로 동일 그룹에 속한 사용자는 동일 EMM 메시지를 수신한다. ECM 메시지는 최종적으로 사용되는 키 Control Word의 정보를 포함하고 있으며, 매우 짧은 갱신 주기를 가지고 있다. 반면 EMM 상대적으로 긴 수명을 가지며 각기 다른 그룹은 다른 메시지로 전송하기 때문에 많은 종류의 EMM 메시지가 전송된다.

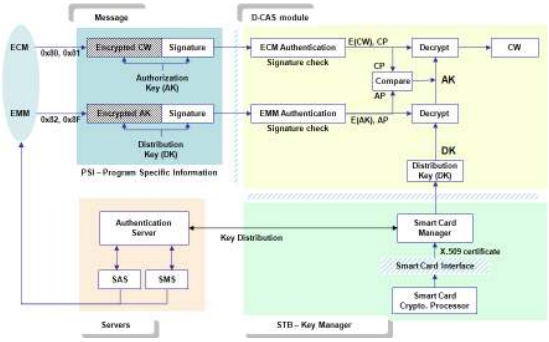

그림 4. 단말에서 CA 메시지 처리

그림 4는 셋톱박스에서 EMM, ECM, CW를 생성하고 소비하는 과정을 보여주고 있다. 기존의 CAS 기술은 EMM 메시지를 복호화하기 위해서 스마트카드 혹은 중간 단계의 키를 사용한다. 이는 스마트카드에 발급된 키를 교체할 수 없기 때문에 더 오래 키를 사용하기 위한 방법이었다. 하지만 IP 망은 양방향의 특징을 가지고 있고 실시간으로 사용자 키를 분배하고 갱신하는 것이 가능하기 때문에 온라인 인증을 통해서 사용자 키를 분배하는 것이 가능하며, 스마트카드에 내장되어 있는 키는 사용자 키 분배과정의 사용자 인증 및 서명을 위해서 사용된다. 또한 보안 강도를 높이기 위해서 더 많은 단계의 ECM, EMM을 추가하여 시스템을 구성하는 경우도 있다.

V. 결 론

IPTV 서비스를 위한 보안 기술은 인터넷이 가지고 있는 양방향성과 방송이 가지고 있는 일방향성의 특징을 모두 활용해야 한다. 특히 다운로드 가능한 방송 수신 제어 기술은 사용자 혹은 서비스 제공자마다 필요로 하는 수신 제한 기술을 달리 적용할 수 있는 기술로 특정 수신 제한 기술에 종속되지 않는 특징을 가지고 있다. 이들 특징을 반영한 기술이 CAS 와 DRM 기술이다. 이들 기술은 상호 배타적이면서 또 보완적인 특징을 가지고 있다. DVB의 경우는 CAS 기술과 DRM 기술의 영역을 구분하여 상호 보완적인 구조를 가지도록 연구가 진행 중[5]에 있다. 북미의 ATIS 경우는 실시간 방송을 위해서는 CAS 기술을 적용하고 요구불(On Demand) 서비스에 대해서는 DRM 기술을 적용[6]하고 있다. 이는 CAS와 DRM 기술이 상호 배타적이거나 경쟁적인 기술이 아닌 상호 보완적 기능을 수행하기 때문이다.

따라서 IPTV 환경에서 다양한 서비스와 연계 및 사용자의 요구에 맞게 기술을 발전하기 위해서는 DRM, CAS 기술을 접목하고 또한 새로운 보안 서비스들을 수용할 수 있는 개방형 보안 기술에 대한 연구가 필요하다. 특히 전통적인 보안 서비스인 금융, 결제, 신원확인 등의 기능을 포함하는 포괄적 의미의 보안 플랫폼 개발이 필요하다.

참고문헌

[1] Advanced Common Application Platform, ATSC Standard, http://www.atsc.org/standards/

[2] The OpenCable Application Platform, CableLabs Standard, http://www.opencable.com/ocap/

[3] Multimedia Home Platform, DVB project office, http://www.mhp.org/

[4] The global TV-Anytime Forum, http://www.tv-anytime.org/

[5] DVB, "Content Protection and Copy Management Specification; Part 4: CPCM Specification", TS 102 825-4 V1.2.1, 2008

[6] ATIS, “IIF Default Scrambling Algorithm(IDSA) IPTV Interoperability Specification,” ATIS-0800006, 2007.

저자소개

박종열(Jongyoul Park)

1996년 충남대학교 컴퓨터공학 학사
1999년 광주과학기술원 정보통신 석사
2001년 U. of Utah, 객원 연구원
2004년 광주과학기술원 정보통신 박사
2004년 ~ 현재 한국전자통신연구원 소셜미디어서비스 연구팀 선임

※관심분야 : 방송 수신 제한, 전자지불, 이동코드, 인증시스템, 분산 시스템 등

백의현(Euihyun Paik)

1984년 숭실대학교 전자계산 학사
1987년 숭실대학교 전자계산 석사
1997년 숭실대학교 전자계산 박사
1987년 ~ 현재 한국전자통신연구원 소셜미디어서비스 연구팀 팀장

※관심분야 : IPTV, 방송 수신 제한, 개방형 홈네트워크, 상황인지 등