디지털 CATV 와 IPTV 의 수신제한시스템 비교분석 및 발전방안 연구

신승중*, 박지언**, 곽계달**
*한세대학교 컴퓨터공학과
**한양대학교 컴퓨터공학과
e-mail : expersin@hansei.ac.kr

A Study on Development Plan, Comparison & Analysis of Digital CATV and IPTV

Seung-Jung Shin*, Jiun Park**, Kae-Dal Kwack**
*Dept. of Computer Engineering, Hansei University
**Dept. of Computer Engineering, Hanyang University

요 약

아날로그방송 중단을 앞두고 케이블방송은 디지털 CATV 로 전환하기 위해 노력 중이다. 이를 위해 케이블방송은 단순히 방송의 디지털화 뿐만 아니라, PPV(Pay Per View), PVR(Personal Video Recorder), VOD(Video On Demand) 와 같은 서비스를 가입자에게 제공하기 시작했다. 이와 같은 서비스들은 대부분 유료서비스로 가입자의 수신권한을 확인하기 위해 다양한 종류의 CAS(Conditional Access System)를 사용하고 있다. 2008 년 관련법의 정비와 함께 IPTV(Internet Protocol TV) 시범서비스가 시작 되었는데, IPTV 역시 실시간 방송, VOD 서비스를 기본 서비스로 규정하고 있기 때문에 CAS 의 사용이 필수적이다. 본 논문에서는 디지털 CATV 와 IPTV 에서 사용하는 수신제한시스템을 분석하고, 가입자와 방송사업자 모두에게 도움이 되는 발전방향이 무엇인지 제시하고자 한다.

1. 서론

디지털방송은 다채널을 사용할 수 있기 때문에 가입자의 흥미에 맞는 전용 채널을 구성하여 제공하거나, 또는 고화질/고음질의 영화나 스포츠 방송을 제공하고 있다. 이런 특화된 방송들은 대부분 유료이며, 서비스이용을 선택한 가입자에게만 방송을 볼 수 있는 권한을 부여한다.

<표 1> 방송 제공 형태에 따른 유료화 정책

분류	전송방식	요금체계	특징
지상파 방송	공중파	무료	공익적 차원의 방송
케이블 방송	케이블	기본료+유료채널	저렴한 가격,안정성
위성방송	위성	기본료+유료채널	비싼 가격,다양한 콘텐츠
IPTV 방송	IP	기본료+유료채널	비싼 가격,다양한 콘텐츠

<표 1>은 전송방식에 따른 방송의 요금 체계 및 특징을 보여주는 표로, 지상파 방송을 제외한 대부분의 시스템에서 유료채널을 제공하고 있는 것을 알 수 있다.

디지털 CATV 에서는 이런 유료채널을 제공하기 위해 가입자의 시청권한을 관리할 수 있는 수신제한시스템(Conditional Access System : 이후 CAS 로 줄임)을 사용한다. 최근에는 전 세계적으로 콘텐츠를 제공하는 CP(Content Provider)들이 방송사업자에게 콘텐츠 공급계약을 할 때 CAS 의 적용을 요구하는 추세이다. CAS 를 채택하지 않은 방송사업자에게는 콘텐츠를 공급하지 않기 때문에 CP 가 요구하는 CAS 를 적용하고 있다.

이는 IPTV 역시 마찬가지이며, 특히 IPTV 가 사용하는 IP 망의 보안이 상대적으로 취약하기 때문에 일반적인 의미의 CAS 뿐만 아니라, 개별 콘텐츠에 대한 보안을 강화하는 역할을 하는 DRM(Digital Right Management)도 같이 사용한다.

따라서 본 논문에서는 디지털 CATV 와 IPTV 에서 쓰이는 수신제한시스템을 분석하고, 가입자와 방송사업자 모두에게 도움이 되는 수신제한시스템의 발전방향이 무엇인지 제시하고자 한다.

2. 디지털 CATV 의 수신제한시스템 연구

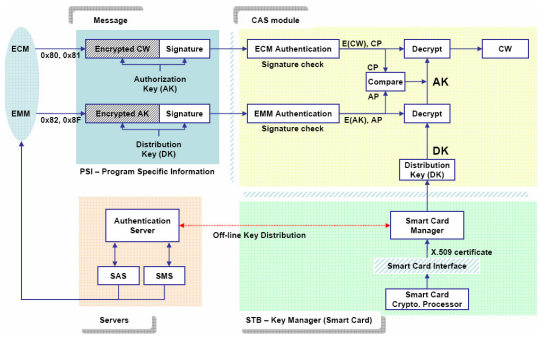
2.1 디지털 CATV 의 CAS

CAS 는 유료 방송 서비스에 대한 가입자의 접근 여부를 제어하는 시스템으로, 가입자의 시청료 납부 현황, 수신지역에 따른 권한, 나이에 따른 수신등급과 같은 것을 판단해서 방송을 시청할 수 있게 한다.

(그림 1)은 CAS 방식의 수신제한시스템의 블록도이

다. 방송사업자가 비밀번호(Control Word)를 생성하고 생성된 비밀번호를 기반으로 암호화 하여 방송을 전송한다. 이때 CW 는 암호화 되어 ECM(Entitlement Control Message)에 포함하여 전송한다. 수신기는 방송에 함께 전송된 ECM 과 EMM(Entitlement Management Message) 정보를 기반으로 암호화된 정보를 복호화한다. ECM 은 STB 에 권한을 부여하는데 필요한 복호화키와 수신조건을 포함하고, EMM 은 방송서비스에 대한 수신자격정보와 그 수신자격을 받을 사용자 정보를 포함하고 있다.

이렇게 한번 전송된 사용권한은 가입자의 STB 에 연결된 Smartcard 에 기록이 되고, 새로운 ECM 과 EMM 이 수신될 때까지 가입자의 권한을 판단하는 정보로 사용된다.



(그림 1) CAS 방식의 수신제한시스템

2.2 새로운 서비스의 등장

디지털 CATV 의 대표적인 기능이 실시간 방송이라면, 변화된 가입자의 기호와 IPTV 와 같은 신규 방송서비스에 대응하기 위해 새로운 서비스들이 추가 되고 있다. 대표적인 서비스로는 가입자가 원하는 방송을 HDD 에 녹화해서 다시 볼 수 있는 PVR 과 가입자가 원하는 방송을 원하는 시기에 볼 수 있게 하는 VOD 가 있다.

이런 새로운 서비스들의 보안모델은 CAS 에 적합하지 않은 부분이 많아, CAS 와 별개로 DRM 을 도입하거나, CAS 에서 DRM 의 기능을 지원하도록 변경하는 추세이다.

3. IPTV 의 수신제한시스템 연구

3.1 IPTV 의 수신제한시스템 개요

IPTV 는 사용하는 전송방식이 보안에 취약한 IP 망이고, 지원하는 서비스도 단순 실시간 방송뿐만 아니라 콘텐츠 단위의 다양한 서비스를 제공하기 때문에 기존의 CAS 만으로는 대응하기 어려운 부분이 많이 있다.

<표 2> IPTV 보안 모델

보안 항목	내 용
사용자 인증	▪ 사용자 식별 및 권한 부여
디바이스 인증	▪ 사용자 인증과 병행하여 디바이스 식별 및 권한 부여
스트림 접근 제어	▪ 특정 프로그램 또는 채널 스트림에 대한 접근 제어 ▪ 특정 VOD 콘텐츠 스트림에 대한 접근 제어 ▪ PPV/Blackout/Parental Rating 제어
스트림 복사 제어	▪ 모든 콘텐츠 스트림에 대한 불법 복제 방지 – 스트림 통로의 보호 – 불법 저장 방지 – 저장된 콘텐트의 보호 ▪ HDD 저장 콘텐츠의 이용 제어 – 유효 기간 및 플레이 회수 제어 – Watch&Record/Timeshift Recording/PVR – 저장 콘텐츠의 외부 디바이스 전송

<표 2>는 IPTV 의 보안 모델을 나열한 것이다. 다양한 보안항목이 있지만, 본 논문에서는 “스트림접근제어”와 “스트림복사제어”에 관해 다루고 있다. “스트림접근제어”는 방송서비스의 시청권한을 제어하는 것으로 주로 실시간 방송에 사용하며 CAS 가 담당하게 된다. “스트림복사제어”는 실시간 방송의 녹화, VOD 나 기타 저장된 방송의 시청시 단일 콘텐츠에 대한 시청권한과 재생회수와 같은 항목을 제어하게 되며, DRM 이 담당하게 된다.

3.2 IPTV 의 CAS

디지털 CATV 에서 사용하는 CAS 는 단방향 방송에 적합한 구조로, Request/Response 구조가 아닌 폴링 구조를 사용하고 있다. 이로 인해 현재 사용하지 않는 ECM 정보도 스트림에 포함시켜서 전송하여 대역폭의 낭비를 발생한다. EMM 역시 모든 가입자의 권한을 모두 보내는 방식이라 1:1 로 Request/Response 가 가능한 양방향 환경에서는 대역폭을 낭비하게 된다.

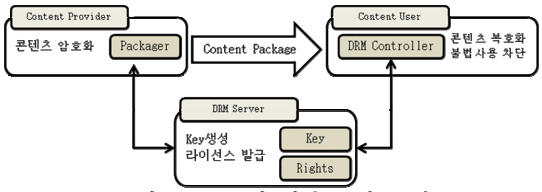
CAS 는 콘텐츠에 대해 보안을 적용하는 기술이 아니라 채널이라 불리는 콘텐츠의 전송경로 자체에 접근을 제어하는 방식이다. 그러므로 전송경로 자체의 유동성이 강하고, 콘텐츠 자체가 별도의 사용권한을 가져야 하는 IPTV 환경에서는 기존의 CAS 를 그대로 적용하기가 어려운 부분이 많다.

이런 이유로 IPTV 에서는 수신제한시스템으로 CAS 만을 사용하지 않고 다음으로 소개하는 DRM 과 함께 사용하여 상호 보완작용을 하게 구성한다.

3.3 IPTV 의 DRM

DRM 은 인터넷 기반의 콘텐츠 유통 환경에서 발전한 기술로 콘텐츠의 불법 복제 방지를 기본 목적으로

한다. DRM 을 이용하면 저장된 콘텐츠에 대한 암호화 및 권한 관리가 용이해지며, IPTV 의 VOD, PVR 또는 각종 멀티미디어 재생에 사용하기 적합하다.



(그림 2) DRM 의 기본 동작 모델

IPTV 에서의 DRM 은 디지털 콘텐츠의 데이터를 암호화하여 무단 복제를 방지하고, 인증된 사용자 및 단말기에 대해서만 라이센스를 발급하며, 라이센스에 포함된 Rights 및 Key 를 이용하여 복호화를 수행하는 기능을 한다.

(그림 2)는 DRM 이 동작하는 기본 모습을 보여준다. 우선 Content Provider 의 Packager 가 콘텐츠를 패키징하는데, 이 과정에 해당 콘텐츠의 정보가 DRM Server 에 등록된다. 이렇게 해서 생성된 Content Package 가 사용자에게 전달이 된다. 사용자는 해당 콘텐츠를 이용하기 위해 DRM Server 로부터 라이선스라 받아 해당 콘텐츠를 복호화 하여 사용하게 된다.

4. 디지털 CATV 와 IPTV 의 수신제한시스템 비교 분석

4.1 채택하고 있는 수신제한시스템 비교

기본적인 디지털 CATV 에서는 CAS 만으로 충분히 수신제한시스템을 구현할 수 있었다. 하지만 PVR 을 이용해서 특정 프로그램을 저장하거나, 원하는 프로그램을 원하는 시간에 보기 위해 VOD 서비스를 이용하는 것과 같이 개별 콘텐츠에 대한 서비스를 도입할수록 기존의 CAS 만으로는 이에 대응하기가 어려워지고 있다. 이런 부족한 부분은 DRM 을 도입하여 해결하려는 시도가 이루어지고 있다. 기존에 사용하던 CAS 와는 완전 별개의 DRM 을 도입하는 경우도 있고, CAS 에서 DRM 의 기능을 흡수하여 CAS 가 모든 보안 모델을 담당하게 하는 형태의 개발도 이루어지고 있다.

이와는 반대로 IPTV 는 국제규격의 표준화가 늦어지면서, 실시간 방송을 제외하고 VOD 가 중심이 된 IPTV 가 먼저 시범실시가 되었다. VOD 의 보안모델은 DRM 으로 충분하므로 초기에는 DRM 만 적용한 사례가 대부분이지만, 디지털 CATV 와 같은 실시간방송이 실시가 되면 기존의 DRM 만으로는 대응이 힘든 점이 있다. 그러므로 IPTV 도 디지털 CATV 와 같은 방식의 CAS 를 도입하는게 가장 쉽게 수신제한시스템을 구축하는 방법이다. 하지만 국내에서는 DRM 이 IPTV 의 수신제한시스템을 선점했기 때문에, 실시간 방송에 대한 보안 모델 역시 DRM 을 콘텐츠 단위에서 Live Streaming 으로 확장하여, DRM 이 CAS 의 역할까지 담당하게 하는 시도도 이루어지고 있다.

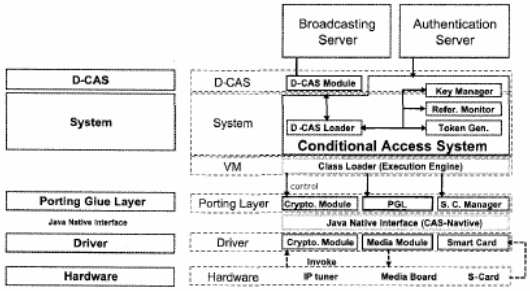
결국 CAS 와 DRM 은 방송서비스가 고도화 되면서 둘 모두 수신제한시스템에 꼭 필요한 구성 요소가 되고 있다.

4.2 향후 발전방향

CAS 는 사용자의 단말인 STB 에 해당 CAS 의 복호 시스템을 구현하고, Smartcard 에 복호에 필요한 기본 정보를 담게 된다. 이 경우 CAS 자체를 바꾸어야 하거나 Smartcard 를 새로운 암호화 방식으로 변경해야 할 경우 가입자의 STB 와 Smartcard 를 모두 교체해야 하는 불편함이 발생한다.

이에 대한 보완 방법의 하나로 D-CAS(Download CAS)의 개발이 유력하다. D-CAS 는 수신을 제어하는 기능을 다운로드 가능한 형태로 만들어, 필요할 경우 가입자의 수신제한시스템을 즉시 변경할 수 있도록 하는 시스템이다. (그림 3)은 D-CAS 를 이용한 STB 의 계층도를 나타낸 그림이다. 이를 가능하게 하기 위해서는 다음과 같은 기능구현이 필요하다.

- 수신 제어를 위한 H/W 기본 기능 정의 및 S/W 와 H/W 기능의 분리
- 동적으로 S/W 를 바인딩(Binding)/언바인딩(Unbinding)하는 기능
- 수신제한시스템 S/W 를 다운로드,설치,실행,관리하는 기능



(그림 3) D-CAS 를 이용한 STB 계층도

디지털 CATV 에서는 NGNA(Next Generation Network Architecture)를 통해 CAS 의 POD(Point of Deploy) 모듈을 완전히 다운로드 가능한 S/W 형태의 솔루션으로 변경하는 작업을 진행하고 있다.

5 결론

디지털 CATV 는 PVR, VOD 와 같은 새로운 서비스를 실시하면서 기존에 사용해 오던 CAS 뿐만 아니라 DRM 역시 필요로 한다. 반면 IPTV 는 VOD 위주의 서비스 뿐만 아니라 실시간 방송도 시작하면서 CAS

의 사용을 필요로 한다. 결국 디지털 CATV 와 IPTV 는 사용하는 전송망의 차이는 있지만 가입자에게 제공하는 서비스가 서로 유사해 지면서, 수신제한시스템도 CAS 와 DRM 을 모두 사용해야 하는 유사한 환경으로 발전하고 있다.

수신제한시스템의 사용범위가 넓어지면 해킹에 대한 가능성도 더 커지게 된다. 해킹이 발생하면 방송사업자는 수신제한시스템을 교체하기 위해 방송사업자측의 Headend 시스템과 가입자측의 STB 및 Smartcard 를 모두 교체해야 한다. 이렇게 되면 결국 방송사업자와 가입자 모두 금전적 손실과 불편함을 겪게 된다. 이를 최소화 하기 D-CAS 의 사용이 활발히 이루어질 것으로 예상된다. 해킹이 발생하면 D-CAS 를 이용해 새로운 CAS 를 STB 에 설치하여 사용할 수 있으므로 STB 를 교체할 필요가 없고, 해킹발생시 가장 빠르게 대체할 수 있다. 그리고 D-CAS 는 Smartcard 를 사용하지 않기 때문에, Smartcard 의 발행 및 배송과 같은 비용부담의 필요성도 없어진다.

참고문헌

[1] 우제학, “IPTV 서비스의 보안 기술”, 한국정보처리학회 IT21 컨퍼런스, 2008.6

[2] 박종열, “IPTV Security 표준동향 및 사업 전략”, IPTV 표준기술 워크숍, 2006.11

[3] ETRI, “IPTV 기술 및 서비스”, 2007

[4] ETRI, “실시간 IPTV 서비스를 위한 수신제한기술”, 2007

[5] 한국정보보호진흥원, “Security for Multicast of IPTV Service”, 2007.6

[6] 한국콘텐츠학회, “IPTV 콘텐츠 보호 기술의 비교-CAS 와 DRM 중심으로”, 2006

[7] 한국방송영상산업진흥원, “디지털케이블방송과 IPTV 서비스의 동향과 분석”, 2007