실시간 IPTV 서비스를 위한 수신 제한 기술

박종열 | 문진영 | 박민호 | 백의현
한국전자통신연구원

인터넷 사용자의 급속한 증가는 IT 산업 발전에 큰 견인차 역할을 수행해 왔다. 그 중에서 IP 망을 이용한 방송 분배 및 VoD(Video on Demand) 서비스는 네트워크 기술의 발달과 더불어 크게 발전했다. 인터넷을 통한 콘텐츠의 유통은 무료라는 고정 관념과 달리 IPTV[1] 서비스는 실시간 방송의 개념이 추가되어 유료화가 추진되고 있다. 유료 방송 정책은 방송 제공 형태에 따라서 크게 달라지고 서비스를 제공하기 위해 필요한 기술 및 사용하는 자원(Network)에 따라서도 다르다.

〈표 1〉 방송 제공 형태에 따른 유료화 정책

분 류	전송 방식	요금 체계	특 징	비 고
지상파 방송	공중파	무료	공익적 차원의 방송	
케이블 방송	케이블	기본료 + 유료 채널	저렴한 가격, 안정성	저렴한 서비스
위성 방송	위성	기본료 + 유료 채널	비싼 가격, 다양한 콘텐츠	다양한 콘텐츠
IPTV 방송	IP	기본료 + 유료 채널	비싼 가격, 다양한 콘텐츠	인터넷 포함

〈표 1〉은 각각의 방송의 요금 체계 및 특징을 보여주는 표로 IPTV 방송이 다른 방송과 차별화 되는 부분이 없다. 더욱이 IP 망을 이용하기 때문에 케이블이나 위성과 같이 보장된 자원을 사용하지 않고 다른 사용자와 공유하는 IP 망을 이용하기 때문에 서비스 관점에서는 더욱 취약한 특징을 가지고 있는 것이 사실이다.

IPTV 서비스를 다른 방송 서비스와 차별화 하기 위해서는 IP망이 가지는 장점을 최대한 활용해야 한다. 가장 쉽게 생각할 수 있는 방법은 양방향 데이터 방송이다. IP망의 양방향성을 활용하여 인터넷의 지식검색, 시청중인 프로그램의 제작자 정보, 인기 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 위해 전화선(PSTN[2]), 케이블(DOCSIS[3]), 인터넷 모뎀과 같은 반대 방향의 통신 채널(return channel) 확보 하고 있다. 기존의 방송망에서는 양방향 방송을 수신하기 위해서 별도의 통신 채널을 만들어야 하기 때문에 사용자에게 불편함과 추가비용을 부담시킨다.

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 쉽다. 또한 이러한 방송이 특정 사용자에 한정되지 않고 IPTV 가입자라면 누구에게나 사용될 수 있는 개방형 서비스의 특징을 가진다.

IPTV 방송의 차별점은 방송 자체 보다는 연계되는 부가 서비스 적용이 용이하고 그 형태가 매우 다양한 것이다. 이와 같이 유연한 서비스를 제공하기 위해서는 기존의 방송 수신 제어 기술(Conditional Access System : 이후부터 줄여서

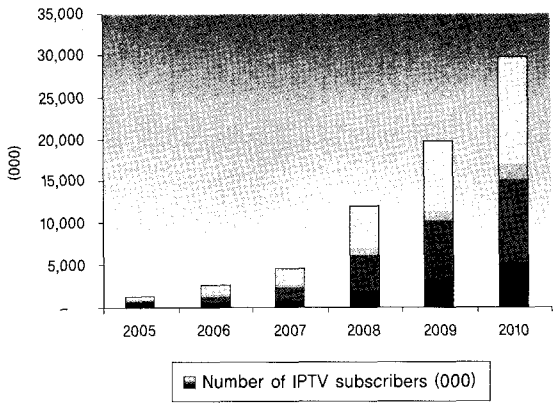
_ IPTV: IP 망을 이용하여 방송 데이터를 실시간 전송하는 일련의 서비스를 의미함
_ PSTN: Public Switched Telephone Network
_ DOCSIS: Data Over Cable Service Interface Specification

CAS)도 변화가 필요하다. 다양한 형태의 방송 수신을 제한할 수 있는 형태로 개발 되어야 한다.

IPTV는 기본적으로 IP라는 공개된 망을 통해서 전송되기 때문에 무한대에 가까운 채널 확장이 가능한 반면 불법적인 시청이 용이한 특징도 있다. CAS 기술이 적용되지 않는다면 옆집에서 시청중인 유료 채널은 같은 서브넷에 연결된 사용자가 네트워크 도청하여 무료로 볼 수 있다. 따라서 콘텐츠 제작자들은 CAS 기술을 통해 사용자의 불법적인 접근을 제어하고 있다.

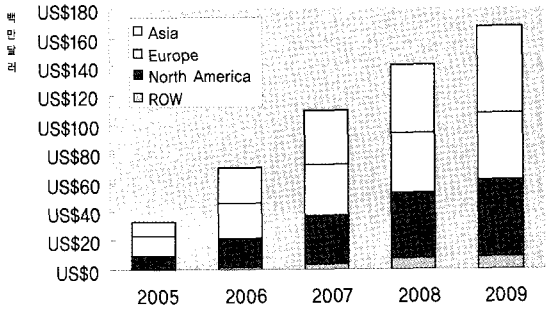
방송 수신 제한(CAS) 기술은 방송의 형태 보다는 사업자의 논리에 따라서 상호 배타적인 기술이 개발되고 있다. 실제 지상파 방송을 위한 ACAP[1], 케이블 방송을 위한 OCAP[2], 위성 방송을 위한 MHP[1]가 표준 기술이지만 방송 수신 제한 기술(CAS)는 이들 표준보다 업체별 제공 기능에 따라 다르기 때문에 개방형 표준 기술의 개발이 필요하다.

: IPTV는 통신 사업자에게 방송을 진출할 수 있는 기회로 방송 사업자에게는 통신 사업에 참여할 수 있는 기회로 여겨지면서, 방송 업계와 통신 업계가 첨예한 대립을 하고 있는 상황이다. 이미 포화 상태에 있는 두 시장에서 새로운 창출로 인식되기 때문이다. IPTV 시장에 대한 많은 자료가 있지만, IT 기술이 빠르게 발전하고 있는 아시아/태평양(일본 제외) 지역의 IPTV 서비스의 2005~2010년 가입자 수 예측은 다음 그래프와 같다. [IDC Research Investments, 2005년 자료 인용]



(그림 1) Asia/Pacific (일본제외) 광대역 망 기반 IPTV 서비스 가입자 수 예측

(그림 1)은 2005년부터 2010년까지의 IPTV 가입자 증가를 예측한 자료로 2010년 일본을 제외하고 아시아/태평양 지역에서 약 3천만명의 가입자를 확보할 것으로 예측하고 있다. 아시아/태평양 지역은 타 지역에 비해서 초고속 인터넷의 보급률이 높으며 새로운 기술의 보급이 상대적으로 빠른 지역이다.



(그림 2) 2005-2009 년도 IPTV 시장 규모 예측 (2005년 MRG 자료입자 수 예측

MRG(Multimedia Research Group)의 IPTV Tracking Service Global Forecast 2005의 자료에 따르면 2005년 세계 IPTV 시장은 8억 8천만 달러(USD)에서 2009년 99억 달러(USD) 규모로 급성장할 것으로 예상되고 있어 빠르게 성장할 것으로 예상된다. 이중에서 수신 제한(CAS) 기술을 포함한 콘텐츠 보호 분야의 기술료 규모는 약 81만불로 매년 약 38%의 높은 성장률이 예상된다.

: IPTV의 유료 서비스를 시작하기 위해서는 요금 체계 및 서비스 접근 제어 기술이 필수적이다. IPTV 시장도 마찬가지로 접근 제어 시스템과 관련 STB 기술이 필요하다. 현재 국내 IPTV 시범 서비스에서는 독자 기술이 아닌 해외 유명 제품과 연계하여 서비스 하고 있다. 선진 외국의 경우 네덜란드계인 이데토액세스(Irdeto Access)에서 개발한 IPTV CAS를 제외하고는 기존의 케이블 방송에서 사용하는 수신 제한 기술을 IP화 하였기 때문에 안전성이 확보되지 못하고 있다.

특히 외국의 선진 기술도 아직 IPTV를 위해서 개발된 것이 아니라 케이블 방송에서 사용되는 기존 방식을 IP화 한 것에 지나지 않아 IPTV 서비스에는 부족한 부분이 많다. 특히 IP 망이 가지는 개방성을 고려할 때 IPTV에 최적화된 CAS 기

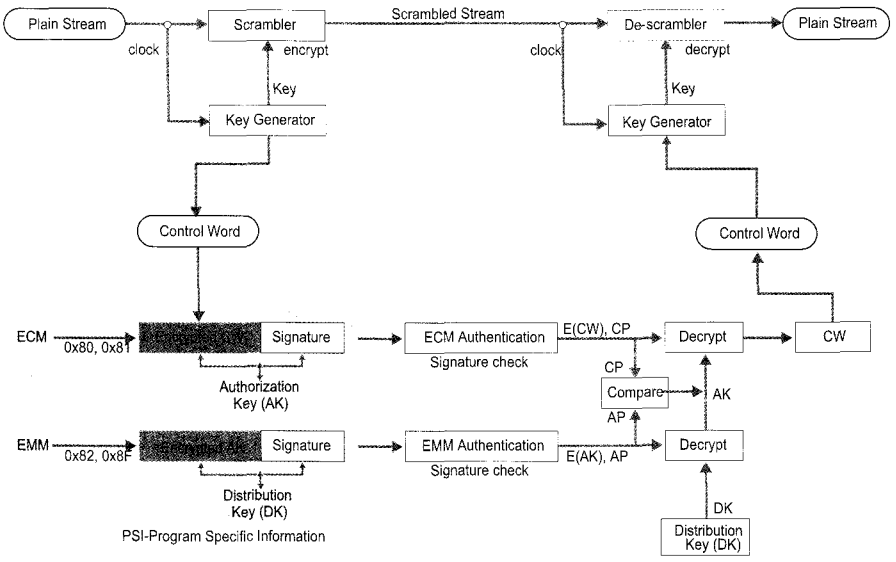
술의 개발이 필요하다. 더불어 IPTV, 케이블 방송, 위성 방송 모두 외국의 기술에 전적으로 의존하고 있어 상대적으로 높은 기술료를 지불하고 있어 자체 기술의 개발이 필요하다.

: 인터넷을 이용한 방송 콘텐츠는 무료라는 인식의 확산으로 IP 기반의 방송 서비스에 대한 사회적 인식이 유료 보다는 무료라는 인식이 깊다. 이는 인터넷을 통해 유통되는 수 많은 콘텐츠들이 쉽게 얻을 수 있기 때문이다. 특히 개인간 파일 공유가 가능해지면서 IP 기반의 방송에 가입하기 보다는 더 빠른 네트워크 서비스에 가입하는 것이 더 현명하다는 생각이 팽배해 있다. 이와 같은 불법적인 방송 콘텐츠의 유출을 막고 서비스에 대한 정당한 지불을 해야 한다는 사회적 인식을 도출하기 위해서는 보다 편리하고 쉽게 방송을 청취할 수 있는 시스템과 더불어 불법적인 방송 콘텐츠의 유출을 방지하는 기술이 필요하다. IPTV 방송 콘텐츠는 그 유출이 쉽고 유출되었을 때 공유되는 형태가 파일이기 때문에 더욱 수신 제한 기술이 필요하다.

: 국내에서 방송되고 있는 영화, 드라마 등이 고가로 해외에 팔리는 사례가 늘고 있다. 하지만 정작 판매된 영상이 상영되기도 전에 이미 일반 사용자들에게 공개되는 경우가 있다. 반대로 해외 이민을 떠나 교민의 경우 멀리서 한국의 드라마를 시청하고자 할 때, 시간 및 공간적 제약을 받지 않고 방송을 수신할 수 있는 방법은 IPTV 밖에 없다. 더불어 불법적인 시청을 방지해야 시간 및 공간을 뛰어 넘는 방송 서비스가 가능하다.

위성 혹은 케이블 방송 시스템에서 유료 채널에 대한 사용자의 불법적인 시청 방지 기술은 사업자의 수익성과 직접적인 관계를 가지고 있기 때문에 중요한 기술로 인식되고 있고, 그 기술은 물론이고 사용되는 알고리즘 자체가 외부에 공개되는 것을 꺼릴 정도로 중요시 여겨지고 있다.

이러한 사용자의 불법적인 시청을 방지하기 위해서는 사용자를 인증하고 그의 접근을 적절히 제어할 수 있는 기술이 필요하였고 이를 시스템에 적용하는 방식에 따라 CAS (Conditional Access System) 방식과 DRM(Digital Right Management) 방식으로 분류 된다. 또는 이 두 가지 기능이 혼합된 암호 이론 기반의 접근 제어 기술에 대한 연구도 최근 활발히 진행되고 있다.



(그림 3) CAS 방식의 수신 제한 시스템

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 스크램블(Scramble)하여 방송을 전송한다.

수신기는 ECM (Entitlement Control Message), EMM (Entitlement Management Message) 정보를 기반으로 스크램블 정보를 복호화(De-scramble)한다. 복호화 과정에서 사용자의 스마트카드(Smart-card)에서 제공하는 복호화 키(Distribution Key)를 이용해서 ECM, EMM 메시지를 다시 CW로 복호화 하는 과정을 거치면 정상적으로 방송을 수신할 수 있다.

(그림 3)은 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 케이블 방송 진영(The National Cable & Telecommunications Association-NCTA)에서는 다음 세대의 방송 기술로 NGNA(Next Generation Network Architecture)를 개발하고 있으며 이는 CAS의 POD(Point of Deploy) 모듈(스마트 카드 형태로 제공)을 대치하는 다운로드형태의 보안 솔루션을 개발하는 것이다.

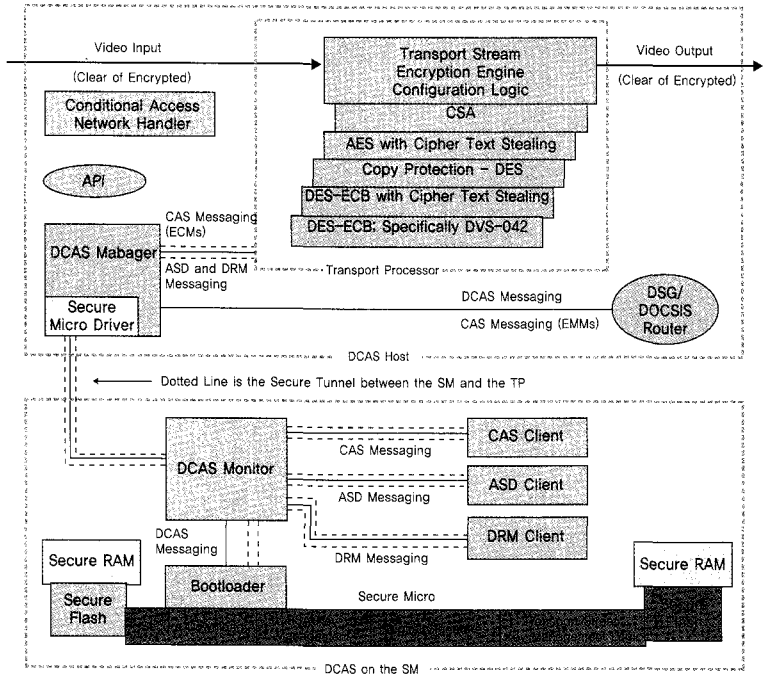
협의적인 의미에서 DRM 기술은 임의의 디지털 정보에 대해서 그 정보의 생성자가 누구이며, 어떤 사람에서 어떤 권리를 부여했는가를 전자적으로 표현하는 기술이다. 멋진 예술 사진이 인터넷에 공개되면 그 그림의 원 저자가 누구이며, 누가 그 정보에 대한 기술적 권리를 가지는가를 가지는 나타내는 기술로 원 저자의 승인 없이 불법적으로 게시 되거나 사용하는 것을 차단하기 위한 기술이다. 광의적인 의미에서 DRM 기술은 불법적인 콘텐츠의 사용과 접근을 방지하기 위한 일련의 기술을 의미한다. DRM 기술은 원 정보에 DRM을 위한 추가적인 정보를 삽입하는 것으로 원 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 암호화 키를 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 많은 비용이 발생하는 문제점을 가지고 있다.

IPTV 방송의 접근 제어를 위해서는 사용자 인증, 시스템 인증, 키 분배, 암호화, 복호화 라는 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 위해 스마트카드(SmartCard) 인터페이스 부분에서 변형되는 방식이 연구되고 있다.

(그림 8)은 OpenCable 측에서 연구 개발 중에 있는 DCAS 구성도를 보여주고 있다. 먼저 OpenCable 측은 전용 칩을 사용한다. 이 전용 칩은 CAS(Conditional Access System), DRM(Digital Right Management), ASD(Authorized Service Domain) 클라이언트를 다운로드 받을 수 있도록 설계 하였다. 여기서 암호화된 콘텐츠를 복호화 하는 기능은 TP(Transport Processor) 에서 담당을 하며, CAS Client(다운로드 CAS 코드)에서 전송하는 Control Word를 통해 실시간 복호화하는 과정을 가진다.

이와 같은 접근 제어 연구는 사용자의 불법적인 접근을 차단하기 위한 메커니즘으로 서비스 제공자 혹은 콘텐츠를 제공하는 사업자의 요구 및 사업 모델에 따라서 많이 달라질 수 있다. 하지만 기존의 제공 메커니즘의 방법은 외부에 개



(그림 4) OpenCable DCAS 구성도[3]

방되지 않고 사업자별로 독립적인 플랫폼에서 동작하는 문제점을 가지고 있다.

IP 망을 이용한 방송 전송 기술은 초고속 인터넷 과 BcN (Broadband Convergence Network), CDN(Contents Distribution Network) 기술의 발전으로 서비스가 가능하게 되었다. 특히 사용자의 고품질 방송에 대한 욕구로 인해 HD 급 영상의 손실 없는 전송 방식으로 IP 망을 선호하게 되었다. 특히 오래된 도시에서는 낡고 오래된 기존 방송 케이블을 새로 설치하기 보다는 빠른 IP 네트워크 망을 설치하는 것이 더욱 효과적이고 저렴하다.

IP 망을 이용하여 고품질의 영상을 전송하는 경우 손실 없는 영상을 전송할 수 있는 장점과 IP 망을 이용한 새로운 서비스의 적용이 쉬운 특징을 가지고 있지만, 공개된 네트워크인 IP를 이용하기 때문에 불법적인 시청 가능성이 높다. 이와 같은 문제점을 정리하면 다음과 같다.

IPTV에서 방송 데이터는 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 채널인증을 하는 경우에는 동일 네트워크의 다른 사용자가 접근 하는 것을 방지 할 수 있다. 또한 사용자의 전송 중간에서 네트워크 가로채기(TCP-hijacking) 기술을 이용해서 연결되어 있는 세션에 대해서 연결을 가로채는 방식의 공격이 가능하다.

기존 시스템에서도 이와 관련하여 많은 연구 개발이 진행되고 있지만 새로운 공격 방법으로 인해 시스템이 피해를 입는 경우 모든 셋톱박스(STB)의 관련 기능을 갱신해야 하는 문제점이 있다. 때문에 수신 제한 시스템을 개발하는 많은 회사들이 케이블카드(스마트카드의 일종)에 관련 모듈을 탑재하고 해킹 등의 문제점이 발견되면 케이블카드를 교체하는 방식을 취하고 있다.

콘텐츠 제공자는 자사의 콘텐츠가 불법으로 유출되는 것을 방지하기 위해서 다각도의 노력을 취하고 있다. 콘텐츠의 불법 유출은 "영화 -> 비디오 -> 방송"으로 이어지는 자사의 수익 모델에 큰 영향을 미치기 때문이다. 최근에는 불법적인 유출뿐 아니라 유통에 대해서도 처벌을 하는 등 그 대응이 더욱 적극적이다. 특히 유료 방송의 경우 불법 유출에 대해서 더욱 적극적이다. 대부분의 영화사들이 자사의 영화를 방송으로 전송하기 위해서는 일정 수준 이상의 수신 제한 기술을 요구하는 경우가 많아 지고 있다.

특히 방송 수신 제어 기술을 가지고 있는 회사와 콘텐츠 제작사들 사이의 공조가 강해지면서 세계적인 기술을 인정받은 몇 개 업체가 전체 시장을 석권하는 문제점이 발생시켰다. 특히 선도 기업들은 그 내부의 메커니즘을 공개하지 않아 신규 사업자들의 시장 진출을 막을 뿐만 아니라 새로운 기술 개발도 더디게 하는 결과를 낳았다. 결과적으로 콘텐츠 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 한다.

방송 수신 제어 기술은 그 기술의 안정성이 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 비용은 상상하기 힘들 정도로 커지기 때문이다. 때문에 많은 사업자들이 새로운 기술 적용을 꺼리게 되는 것이다. 따라서 새로운 방식의 방송 수신 제한 기술을 적용하기 쉽고 해킹이나 오류가 발생하는 경우 이를 쉽게 대치할 수 있는 기술의 개발이 필요하다.

사용자 맞춤형 시청이란 사용자의 취향 및 과거 시청 내역을 기반으로 사용자의 선호 채널을 선택해서 보여주는 방식이다. TV-Anytime Forum[5]에서는 이와 관련된 방송 메타정보 처리를 위한 기술 개발이 활발하게 진행되고 있다. 디지털 방송과 더불어 SI(System Information) 정보를 가공한 EPG(전자 프로그램 가이드) 서비스는 사용자에게 방송에 대한 안내를 하는 것으로 방송 메타 정보를 처리한 것이다. 이것을 사용자의 선호에 따라서 가공하는 것이 맞춤형 시청 기능이다.

맞춤형 시청을 하기 위해서는 SI(System Information)정보를 처리하는 기술도 중요하지만 사용자의 요구에 따른 다양한 형태의 유료 방송 서비스가 필요하다. PPV(Pay Per View)의 경우 사용자가 보고 싶은 프로그램의 대금을 지불하고 시청할 수 있다. 위성 방송에서는 이미 상용 서비스가 되고 있는 것으로 사용자는 기본 채널 이외에 상황에 따라 보고 싶은 채널을 시청할 수 있다. PPV 시청의 경우 사용자의 대금 청구나 사용자의 인증을 위해서 별도의 전화망 연결(상담원 연결)이나 전용 단말기를 필요로 하고 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 제한 기술의 실행이 필요하다. 특히 콘텐츠 제공 사업자마다 서로 다른 수신 제한 기술을 요구하는 경우에 동적 재구성이 가능한 수신 제한 기술이 필요하다.

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 단말기는 '을' 에서 사용이 불가능 했다.

케이블 방송의 경우 이와 같은 문제점을 해결하기 위해서 케이블카드 방식으로 수신 제한 기능을 분리(국내에서 분리 의무화, 미국은 2007년 7월로 연기)하고 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 본 논문에서는 동적 재구성이 가능하며 다운로드가 가능한 수신 제한 기술을 제안한다.

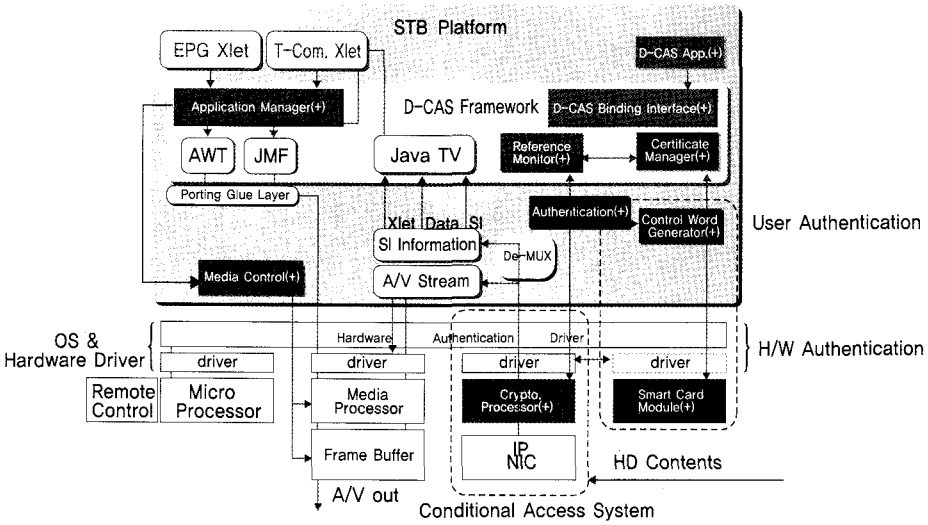
방송 수신을 제어하는 기능을 다운로드 가능한 형태로 만든다는 것은 H/W에서 공통으로 사용되는 기본 기능을 정의하고 관련 S/W 및 다운로드 하기 위한 일련의 과정을 정의하고 구현하는 것이다. 다음은 수신 제한 기능을 다운로드 하기 위해서 필요한 기능이다.

- 수신 제어를 위한 기본적인 S/W와 H/W 기능의 분리
- 동적으로 S/W를 바인딩(Binding) 하고 언바인딩(Unbinding) 하는 기능
- 수신 제어 메커니즘 S/W의 다운로드, 설치, 실행, 관리하는 기능

위의 내용과 별도로 수신 제어 기능의 다운로드 및 설치 과정에서 방송 자체의 수신에 영향을 미치지 않도록 하는 프로세스 분리 기능(Process Isolation)도 서비스를 위해서는 중요한 부분이지만, 본 고에서는 방송 수신 제어 기능 자체에 대해서 기술하는 것으로 관련된 내용은 언급하지 않는다.

본 고에서 다운로드 가능한 방송 수신 제한 기술은 크게 방송 가입자의 인증, 접근 제어 모듈의 전송, 접근 제어 모듈의 단말기 설치의 과정을 진행하게 된다. 이 과정을 좀더 상세하게 기술하면 다음과 같다.

- : 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 과정은 가장 중요한 부분이다.
- : 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 기능은 특정 암호 알고리즘에 종속되지 않으며, 셋톱박스에서 지원해야 하는 알고리즘을 정의해야 한다.
- : 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 암호화 키의 구조는 업체별로 약간씩 변형하여 운영하고 있다.
- : 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 모듈속에 포함되어야 한다.
- : 방송이 전송되는 IP 망은 공유되는 네트워크 환경이기 때문에 불법 도, 감청이 쉽고 변형된 코드의 수신이 가능하다. 따라서 적용되는 수신 제한 모듈이 변형되지 않고 전송되었는가 검증하는 기능과 당 모듈을 수신한 하드웨어 셋톱박스가 인증된 놈인가 확인하는 과정이 필요하다.
- : 수신 제한 모듈은 동적으로 설치되고 재 기동하여 방송을 수신한다. 이 과정은 새로운 프로그램을 설치하고 구동하는 과정으로 방송 중에 발생하면, 사용자가 많은 시간을 기다려야 하는 문제점이 있다. 이 과정을 극복하기 위해서 실시간으로 메모리 적재 및 실행하는 기술의 개발이 필요하다.
- : 실행중인 수신 제한 모듈은 해당 방송을 수신하고 방송에서 SI(System Information) 정보를 추출하여 방송 미들웨어에 전송하고 AV를 출력한다.

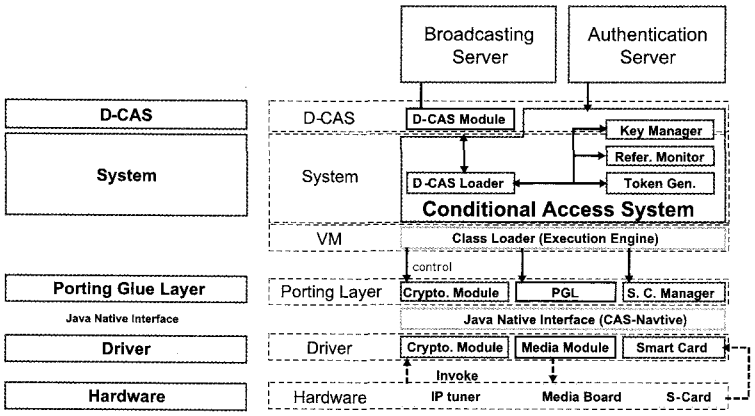


(그림 5) 다운로드 가능한 수신 제한 시스템의 셋톱박스 구조도

(그림 4)는 다운로드 수신 제한 기술을 적용하기 위한 셋톱박스의 기능을 보여주고 있다. 하드웨어 인증, 사용자 인증, Control Word 생성, D-CAS 모듈의 동적 바인딩이 유기적으로 연동된다. 다음은 각각의 기능에 대한 세부적인 설명이다.

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

- : 망에서 방송 데이터를 수신하고 실시간 해석하여 필요한 정보(SI/PSIP)를 미들웨어 전송하는 역할을 수행한다. 또한 CAS에서 제공되는 키를 기반으로 복호화(Decrypt, Descrambling)하는 역할을 수행한다.



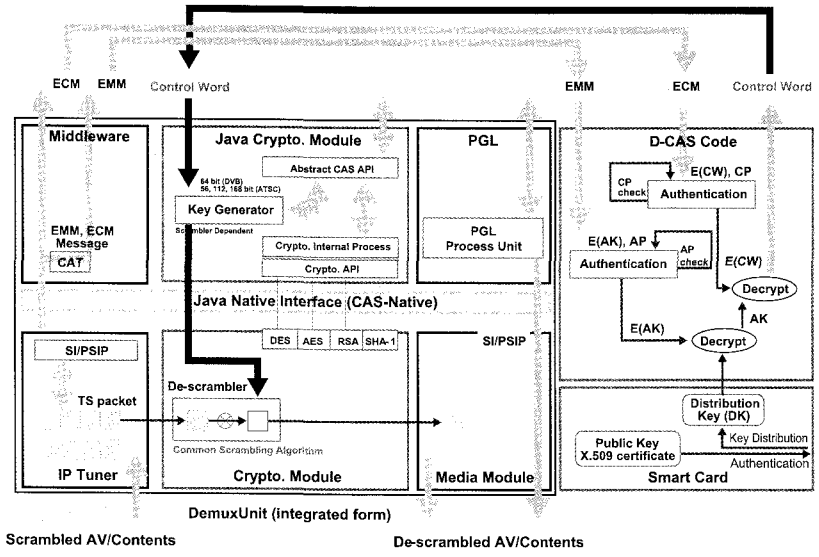
(그림 6) 다운로드 수신 제한을 위한 셋톱박스 계층도

- : 하드웨어를 제어하는 기능으로, 새로운 기능의 적용이나 하드웨어와 관련된 기능을 수행한다. 보통은 하드웨어 제작 업체에서 기능을 제공하지만, CAS나 미들웨어에서 필요한 기능을 이 수준에서 수정하기도 한다.
- : 하드웨어 기능을 추상화한 계층으로 방송 미들웨어를 위해서 정의한다. 방송 미들웨어는 자바 언어로 되어 있고, 드라이버 이하는 C언어로 개발되어 있기 때문에 이 수준에서는 언어 변환(JNI: Java Native Interface) 기능을 수행한다.
- : 수신 제한 시스템(Conditional Access System - CAS)에 필요한 공통 기능과 다운로드 CAS 코드를 실행시켜주는 기능을 수행한다. 실제 D-CAS 코드가 작성되어 있는 형태에 따라서 C 코드 혹은 자바의 클래스 형태로 동작이 가능하며, 동적으로 프로그램을 실행시키고 관리하는 기능을 수행한다.
- : 방송 시청과 동시에 방송 서버에서 해당 방송에 대한 CAS를 전송하고 이를 수신한다. 다운로드 CAS는 방송 수신 제한(CAS)를 실행하기 위한 핵심 코드를 주로 키 관리 기능을 포함하고 있다. CAS 코드를 다운로드하여 동적으로 바인딩 하기 위해서는 다운로드 코드 이외의 기능에 대해서는 표준 인터페이스를 제공해야만 한다.

방송 수신 제한 기술(CAS)는 방송 데이터로부터 복호화 키를 뽑아내고 방송 콘텐츠를 복원하는 기능을 담당한다. 그림 6은 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 관리자이자 다운로드 CAS의 코드가 된다.

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 됩니다. 따라서 전체 시스템의 보안 강도를 낮추지 않고 빠른 연산을 하기 위해서는 사용되는 키를 주기적으로 갱신하는 방법을 사용합니다.

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 메시



(그림 7) 수신 제한 기능이 적용된 셋톱박스의 정보 흐름도

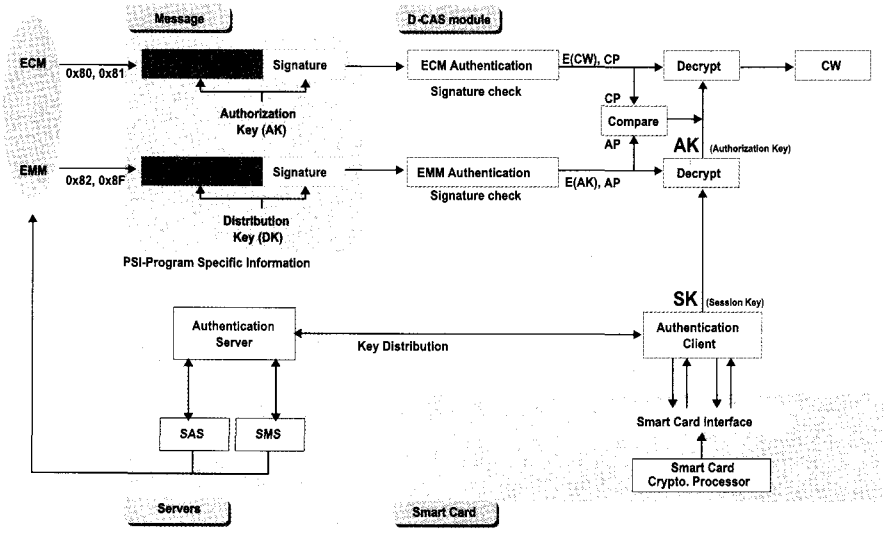
지는 최종적으로 사용되는 키 Control Word의 정보를 포함하고 있으며, 매우 짧은 갱신 주기를 가지고 있다. 반면 EMM 상대적으로 긴 수명을 가지며 각기 다른 그룹은 다른 메시지로 전송하기 때문에 많은 종류의 EMM 메시지가 전송된다.

(그림 7)은 셋톱박스에서 EMM, ECM, CW를 생성하는 과정을 보여주고 있다. 기존의 CAS 기술은 EMM 메시지를 복호화 하기 위해서 스마트 카드 혹은 중간 단계의 키를 사용한다. 이는 스마트 카드에 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, 스마트 카드에 내장되어 있는 키는 사용자 키 분배과정의 사용자 인증 및 서명을 위해서 사용된다.

영상 미디어 산업은 불법 복제에 민감하며 국제적으로 검증된 보안 시스템을 갖추었을 때 메이저 업체의 콘텐츠가 보급되고 있다. 이 같은 이유로 현재의 수신 제한 시스템은 NDS와 Nagravision과 같은 일부 업체에 의해 전체 시장을 독점되고 있으며 메이저 영상 미디어 업체와 이들이 밀접한 관계를 유지하여 국제 영상 미디어 산업을 좌지우지 하고 있다. 하지만 다운로드 가능한 접근 제어 기술의 개발은 기존의 기술을 대변하기 보다는 새로운 기술의 적용을 쉽고 빠르게 하여 관련 산업 활성화에 큰 영향을 미칠 것이다. 특히 다운로드 기술의 적용으로 독자 개발한 수신 제한 기술의 국제적 검증이 가능하여 국내 영상 산업의 자생력과 국제 경쟁력 증대에 기여할 것이다.

다운로드 가능한 수신 제한 기술은 방송 콘텐츠 보호 및 수신 제한 시스템에 대한 해외 기술료 지급 기술을 확보하여 기술 종속을 탈피하고 IPTV 시장의 활성화에 기대할 것으로 예상된다. 특히 본 연구를 통해 관련 핵심 기술을 확보하여 국내 다운로드 수신 제한 기술의 국제표준 및 상용 서비스에 적용 가능할 것이다.

저장된 디지털 콘텐츠에 디지털 방송 콘텐츠 저작권 보호



(그림 8) 셋톱박스에서 다운로드 모듈 (DCAS Module)

관리 기술을 적용하기 위해서는 관련된 기능을 셋톱박스 혹은 시스템에 설치해야 한다. 현실적으로 모든 디지털 기기에 관련 기능을 설치하는 것은 쉽지 않다. 하지만 다운로드 가능한 수신 제한 기술에서는 새로운 기능의 설치뿐 아니라 기존의 CAS 기능에 다른 제품의 DRM 과 연동하는 것도 가능하다. 즉 새로운 기술의 적용이나 새로운 기능의 추가가 용이하여 새로운 공격 기법이나 해킹 기법이 발견되었을 때 적극적인 대응이 가능해 진다. 따라서 디지털 방송 콘텐츠 제작에 있어서 저작권 보호 기술을 적용한 고품질 콘텐츠 제작 및 보급이 활발해질 것이다.

특정 하드웨어 기기 기반의 접근 제이 기술이 아닌 하드웨어 기기와 연동된 암호화 이론을 기반으로 하고 있어, 전자상거래용 응용 프로그램과 연동하여 개인 정보 보호 기술로 활용이 가능하다.

방송 콘텐츠의 댁내 재분배에서 필요한 콘텐츠 보호 기술은 암호학적 이론을 기반으로 하고 있어, 호환성 있는 암호 시스템 연동이 필요하다. 따라서 본 연구의 다운로드 가능한 수신 제어 기술은 댁내 콘텐츠 재분배를 위한 보안 기술로 활용이 가능하다.

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. 방송 수신 제한 기술에 대한 특정 해외 유명 업체의 독점적 지위로 인해서 서비스의 조기 도입 및 국내 독자 기술 개발의 어려움을 해소하기 위해서는 다운로드 가능한 수신 제한 기술의 개발은 그 의미가 크다. 또한 다운로드 되는 수신 제한 메커니즘이 단말기의 기능과 분리가 가능하기 때문에 다양한 형태의 프로그램을 연동하는 것이 가능하다. 특히 데이터 방송용 응용 프로그램과 연동하면 새로운 형태의 서비스가 가능하다. 즉 사용자의 입력을 유도하거나 방송을 따라 하는 등의 방송 서비스의 형태의 변화도 가능하다. 이 기술은 IPTV 환경을 고려하여 개발 중에 있지만 DMB, NGNA, DTV 등의 모든 디지털 방송 기술에 적용이 가능하다.

참 고 문 헌

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

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

[3] "DCASTM System Overview Technical Report", OC-TR-DCAS-D01-06-2-6, OpenCableTM

[4] "The Digital Video Broadcasting Project(DVB)", http://www.dvb.org/

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

[6] " Open Services Gateway Initiative Alliace" , http://www.osgi.org/

[7 "Multimedia Home Platform", http://www.mhp.org/

[8] "DVB IPTV 표준화 동향 분석", IITA 주간기술동향, 2005.5.18

[9] "IPTV 기술 및 시장동향 분석", 전자부품연구원 EIC 전자정보센터, 2004. 11

[10] "The S/KEY One-Time Password System," Neil M Haller,; Proceedings of the ISOC Symposium on Network and Distributed System Security, San Diego, CA, February 1994

[11] "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," R.L Rivest,; A. Sharmir,; L. Adleman,; Communications of the ACM, Vol. 21, No. 2, pp120-126, Feb. 1978

[12] "An overview of security in Eurocrypt conditional access system," Cruselles, E.; Melus, J.L.; Soriano, M.; Global Telecommunications Conference, 1993, IEEE in Houston. GLOBECOM '93., IEEE Nov. 1993, pp. 188-193

[13] "A scalable key distribution scheme for conditional access system in digital pay-TV system," Baofeng Liu; Wenjun Zhang; Tianpu Jiang; Consumer Electronics, IEEE Transactions on, Vol.50, No.2, May 2004, pp. 632-637

[14] "Key distribution based on hierarchical access control for conditional access system in DTV broadcast," Tianpu Jiang; Shibao Zheng; Baofeng Liu; Consumer Electronics, IEEE Transactions on, Vol.50, No.1, Feb 2004, pp. 225-230

[15] "Implementation conditional access system for pay TV based on Java card," Prasertsatid, N.; Computational Electromagnetics and Its Applications, 2004. Proceedings. ICCEA 2004. pp.533-536

[16] "A secure conditional access system using digital signature and encryption," Noore, A.; Consumer Electronics, IEEE Conference, June 2003, pp.220-221

[17] "On key distribution management for conditional access system on pay-TV system," Fu-Kuan Tu; Chi-Sung Laih; Hsu-Hung Tung; Consumer Electronics, IEEE Transactions on, Vol.45, No.1, Feb.1999, pp.151-158

[18] "Implementation conditional access system for pay TV based on Java card," Prasertsatid, N.; Sookchareonphol, D.; Kosalwit, S.; TENCON 2004. 2004 IEEE Region 10 Conference, Vol.2, 21-24 Nov. 2004, pp.399-402

[19] "Scrambling and controlling access to an all-digital broadcast programme," Angebaud, D.; Giachetti, J.L.; Broadcasting Convention, 1992. IBC., International, 3-7 Jul 1992, pp.224-228

[20] "Conditional access system interoperability through software downloading," Kamperman, F.; van Rijnsoever, B.; Consumer Electronics, IEEE Transactions on, Vol.47, No.1, Feb. 2001, pp.47-54

[21] "A key transport protocol based on secret sharing applications to information security," Eskicioglu, A.M.; Delp, E.J.; Consumer Electronics, IEEE Transactions on, Vol.48, No.4, Nov 2002, pp.816-824

[22] "Design WDRM in digital TV," Hongtao Wu; Bocheng Zhu; Communications and Information Technology, 2005. ISCIT 2005. IEEE International Symposium on, Vol.2, 12-14 Oct. 2005, pp.910-913

[23] "Cryptography theory and practice", Douglas R. Stinson, CRC press, 1995, pp233

박 종 열

1996년 충남대학교 컴퓨터공학과 졸업(학사)
1999년 광주과학기술원 정보통신공학과 졸업(석사)
2001년 ~ 2002년 University of Utah, school of computing 객원 연구원
2004년 광주과학기술원 정보통신공학과 졸업(박사)
2004년 ~ 현재 한국전자통신연구원 유비쿼터스홈서비스연구팀 선임연구원
관심분야 : 방송 수신 제한, 전자지불, 이동코드, 인증시스템, 분산시스템 등

문 진 영

1996년 대구과학고등학교 졸업
2000년 경북대학교 컴퓨터공학과 졸업(학사)
2002년 한국과학기술원 전산학과 졸업(석사)
2002년 ~ 현재 한국전자통신연구원 유비쿼터스홈서비스연구팀 연구원
관심분야 : 방송 수신 제한, 자바카드, 메타데이타 기술 및 검색, 비즈니스 프로세스 관리 등

박 민 호

2002년 동국대학교 정보통신공학 졸업(학사)
2004년 한국정보통신대학교 정보통신공학 졸업(석사)
2004년 ~ 현재 한국전자통신연구원 유비쿼터스홈서비스연구팀 연구원
관심분야 : 무선 멀티미디어 전송, 무선 메쉬 네트워크, IPv6, 홈네트워크 등

백 의 현

1984년 숭실대학교 전자계산 졸업(학사)
1987년 숭실대학교 전자계산 졸업(석사)
1997년 숭실대학교 전자계산 졸업(박사)
1987년 ~ 현재 한국전자통신연구원 유비쿼터스홈서비스연구팀 팀장(책임연구원)
관심분야 : IPTV, 방송 수신 제한, 개방형 홈네트워크, 상황인지 등