6

IPTV 서비스 보호를 위한 기술 표준화 분석

한국전자통신연구원 ▌박종열 · 문진영 · 백의현*

1. 서 론

IPTV 서비스 상용화는 많은 의미를 가진다. 우선 실시간 멀티미디어 서비스를 전국 규모로 구축했다는 것이다. 지금까지는 VoD(Video on Demand) 서비스나 CDN(Contents Delivery Network) 구축 사업에서 전국적인 서비스망을 구축하려 하였으나, 투자비가 엄청나고 이용료가 비싸 실용화가 어려웠다.

인터넷 사용자의 급속한 증가는 다양한 서비스에 대한 요구를 증대시켰고, IPTV와 같은 훌륭한 인프라는 다양한 융합 서비스를 촉발하는 계기가 될 것이다. 특히, 기존의 인터넷 인프라가 멀티미디어 콘텐트를 전송하는데 제한이 있어 Overlay Multicast나 Download and Play와 같은 방식이 적용되었으나, 넓은 대역폭은 다양한 콘텐트뿐 아니라 서비스까지 전송할 수 있게 되었다.

현재의 IPTV 서비스는 사용자의 성향에 따라 제공하는 맞춤형 방송, 사용자들의 실시간 참여가 가능한 대화형 방송, 다차원 정보를 제공하는 멀티 앵글 방송과 같은 새로운 방송 서비스 적용도 쉬워졌다. 또한 이러한 방송이 특정 사용자에게 한정되지 않고 IPTV 가입자라면 누구에게나 사용될 수 있는 개방형 서비스의 특징을 가진다. 개방형 특징을 가지는 IPTV 서비스는 방송 그 자체 보다는 방송과 연계되는 부가 서비스 개발이 용이하고 다양한 형태의 시스템 개발이 가능한 특징이 다른 방송 시스템과 차별화되는 부분이다. 이와 같이 유연한 서비스를 제공하기 위해서는 기존의 방송 시스템의 보안 기술도 변화가 필요하다.

IP 네트워크는 기존의 방송 시스템과 달리 공개되고 누구에게나 접근이 자유로운 특징을 가지기 때문에, 불법적인 시청이 용이하다. 이와 같은 불법적인 접근을 차단하기 위해서 방송 시스템은 암호화 기술을 이용하고 있다. 실시간 방송에서는 방송 제한 수신 기술(Conditional Access System: CAS)을 비실시간 방송은 저작권 보호 기술(Digital Rights Management: DRM)을 적용하고 있다.

시장에서 방송 제한 수신 기술(CAS)은 방송의 형태보다는 사업자의 논리에 따라서 상호 배타적인 기술로 개발되어 왔다. 실제 지상파 방송을 위한 ACAP[1], 케이블 방송을 위한 OCAP[2], 위성 방송을 위한 MHP[3]가 표준 기술이지만 방송 제한 수신(CAS) 기술은 표준보다는 업체별, 사업자 별 기능을 서로 다르게 정의하고 공개나 호환성 확보를 위한 노력은 하지 않고 있다.

2. IPTV 요구사항 - 보안 측면

IP 망을 이용한 방송 전송 기술은 초고속 인터넷 과 BCN(Broadband Convergence Network), CDN(Contents Distribution Network) 기술의 발전으로 IPTV서비스에 접목이 가능하게 되었다. 특히 사용자의 고품질 방송에 대한 욕구로 인해 HD급 영상의 손실 없는 전송 방법으로 IP 망을 선호하게 되었다. 특히 오래된 도시에서는 낡고 오래된 기존 방송 케이블을 새로 설치하기 보다는 빠른 IP 네트워크망을 설치하는 것이 더욱 효과적이고 경제적이다.

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.

2.1 불법적인 방송 시청 차단

IPTV에서 방송 데이터는 멀티캐스트 방식을 이용해서 전송한다. 멀티캐스트 방식이란 동일 네트워크에 서로 다른 사용자가 있는 경우 하나의 전송으로 여러

* 종신회원

† 본 연구는 한국정보통신기술협회의 IT 표준화 활동 강화 사업의 일환으로 수행하였음 [2009-P1-16-08K83, IPTV 서비스 모델 및 수신제한 표준개발].

사용자가 받아서 볼 수 있는 특징을 제공 한다. 따라서 가입자 정보를 기반으로 채널인증을 하는 경우에는 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 방식의 공격이 가능하다.

기존의 보안 시스템에서도 이와 관련하여 많은 연구 개발이 진행되고 있지만, 새로운 공격 방법이 개발되면 보급되어 있는 모든 단말기(STB)의 관련 기능을 갱신해야 하는 문제점이 있다. 때문에 방송 제한 수신 시스템을 개발하는 많은 회사들이 케이블카드(스마트카드의 일종)에 관련 모듈을 탑재하고 해킹 등의 문제점이 발견되면 케이블카드(POD, 스마트 카드, 메모리)를 교체하는 방식을 취하고 있다.

IPTV 보안 기술은 불법적인 방송 시청을 차단하고 새로운 공격 방법에 대해서 빠르게 대응할 수 있는 유연한 방송 제한 수신 기술의 개발이 필요하다.

2.2 특정 시스템에 종속되지 않는 기술 필요

콘텐트 제공자는 자사의 콘텐트가 불법으로 유출되는 것을 방지하기 위해서 다각도의 노력을 취하고 있다. 콘텐트의 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 유출은 단순히 콘텐트의 유출에 그치지 않고 사업자가 향후 방송 콘텐트를 수급하는데 까지 영향을 미치기 때문에 더욱 중요하고 사업자들이 적극적으로 대응하고 있다.

대부분의 영화사들이 자사의 영화를 방송으로 전송하기 위해서는 일정 수준 이상의 방송 제한 수신 기능을 요구하는 경우가 많다. 심지어 세부적인 적용 기술까지도 점검하고 보안성에 대해서 의견을 제시하는 경우도 많아지고 있다.

특히 방송 제한 수신 시스템 회사와 콘텐트 제작자들 사이의 공조가 강해지면서 세계 적인 기술을 인정받은 몇 개 업체가 전체 시장을 석권하는 문제를 발생시켰다. 특히 선도 기업들은 그 내부의 메커니즘을 공개하지 않아 신규 사업자들의 시장 진출을 막을 뿐만 아니라 새로운 기술 개발도 더디게 하는 결과를 낳았다. 이는 결과적으로 콘텐트 제공자의 요구에 맞는 제한 수신 기술 업체의 기술료는 점점 올라가고, 그 회사의 서버 제품, 그 회사의 방송 제한 수신 모듈을 탑재한 단말(STB), 케이블 카드를 일괄 구입해야 하는 문제점이 있어 이를 극복할 수 있는 기술이 필요하다.

2.3 새로운 접근 제어 기술 보급 용이

방송 제한 수신 기술은 그 기술의 안정성과 보안성이 가장 중요한 요소이다. 따라서 새로운 기술을 적용하기 위해서는 그 기술의 안전성 및 장기간의 시험을 거쳐야 한다. 이것은 그런 과정을 거치지 않으면 새로 개발된 방송 제한 수신 기술의 오류나 보안성에 문제가 있는 경우 관련 기기의 교체뿐만 아니라 모든 단말을 수정해야 하기 때문에 그 비용은 상상하기 힘들 정도로 커지게 된다.

때문에 많은 사업자들은 새로운 기술 적용을 꺼리고 있다. 따라서 새로운 방식의 방송 제한 수신 기술을 적용하기 쉽고 해킹이나 오류가 발생하는 경우 이를 쉽게 대처할 수 있는 기술 개발이 필요하다.

2.4 방송 단말의 상호 호환성 확보

기존의 방송 수신 단말기는 서비스 사업자가 제공하고 있다. 동일 방식의 방송을 제공하고 있더라도 서비스 사업자마다 서로 다른 제한 수신 기술을 적용하고 있기 때문에 '갑'에서 제공 받은 단말기는 '을'에서 사용이 불가능 하다.

케이블 방송의 경우 이와 같은 문제점을 해결하기 위해서 케이블카드 방식으로 제한 수신 기능을 분리(국내에서 분리 의무화, 미국은 2008년 시행)하고 있지만 실질적으로 케이블카드와 방송 수신 단말이 독립적으로 동작하지 않는 경우가 대부분이다. 또한 다운로드 가능한 수신 제한 기술을 도입하고 있으나 시스템을 적용하고 있는 사례는 드물다[2,5].

방송 채널, 프로그램, 장르, 주인공, 횟수 등 다양한 형태의 제한 수신이 가능하고 콘텐트 제공자마다 서로 다른 제한 수신 기술이 동작할 수 있도록 하기 위해서는 특정 제한 수신 기술에 종속되지 않고 동적으로 재구성이 가능한 구조가 필요하다.

3. IPTV 제한 수신 기술

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 위해서 사용자를 인증하고 그의 접근을 적절히 제어할 수 있

는 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.

DRM 기술과 달리 방송 제한 수신 기술은 세부적인 기술이 공개되어 있지 않기 때문에 본 고에서 이념적인 내용을 설명한다. 방송 제한 수신 기술은 하나의 암호화되어 있는 스트림을 다수 사용자에게 전송하고 특정 사업자 집단만 접근을 효율적으로 차단할 수 있는 기술이다.

3.1 방송 제한 수신 기술

CAS란 전통적인 의미로 조건에 맞게 사용자의 접근을 제한하는 기술로 과거 아날로그 방송에서 사용되는 스크램블(Scramble) 방식을 주로 의미 한다. 방송 채널에 대한 접근을 제어 한다는 광의적인 의미에서는 제한 수신을 위한 모든 기술을 의미하기도 한다.

CAS는 방송을 전송하는 측에서 비밀번호(control word)를 생성하고 생성된 비밀번호를 기반으로 스크램블(Scramble) 하여 방송을 전송 한다. 수신기는ECM (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 복호화하는 과정을 거치면 정상적으로 방송을 수신할 수 있다[1].

그림 1은 기존 방송의 기본적인 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(스마트카드 형태로 제공)을 대치하는 다운로드형태의 보안 솔루션을 개발하는 것이다[2].

3.2 그룹 기반의 사용자 접근 제어 기술

방송 제한 수신 기능은 다단계의 키를 공유함으로 하여 적법한 사용자만이 방송을 수신하는 기술이다. 키를 공유하는 사용자는 방송을 수신하고 키를 공유하지 못하는 사용자는 방송을 수신할 수 없다. 이를 위해서 방송 제한 수신 시스템은 사용자를 그룹으로 정의하고 그룹에 따라서 키를 공유하고 분배하는 기술을 제공한다.

그림 2는 방송 제한 수신 기술에서 사용하는 그룹 기반의 접근 제어 기술을 그림으로 보여주고 있다. ECM 메시지는 방송 스트림을 암호화하고 이를 공통화시키는 역할을 수행하며, EMM 메시지는 그룹을 기반으로 권한을 주고 빼는 역할을 수행한다. 그림 2에서 Key Generator는 3단계로 제공된다. 이 중간 과정에서 사용자를 그룹 지워주고 권한을 설정하게 된다.

저작권 보호 기술이 개인별로 권한을 할당하고 방

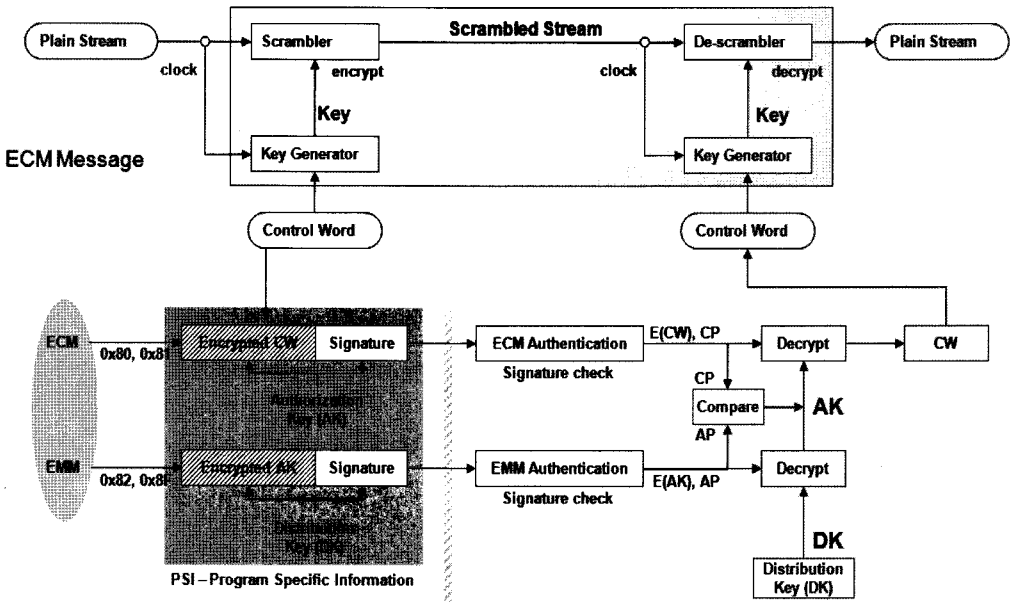


그림 1 제한 수신 기능 개념도

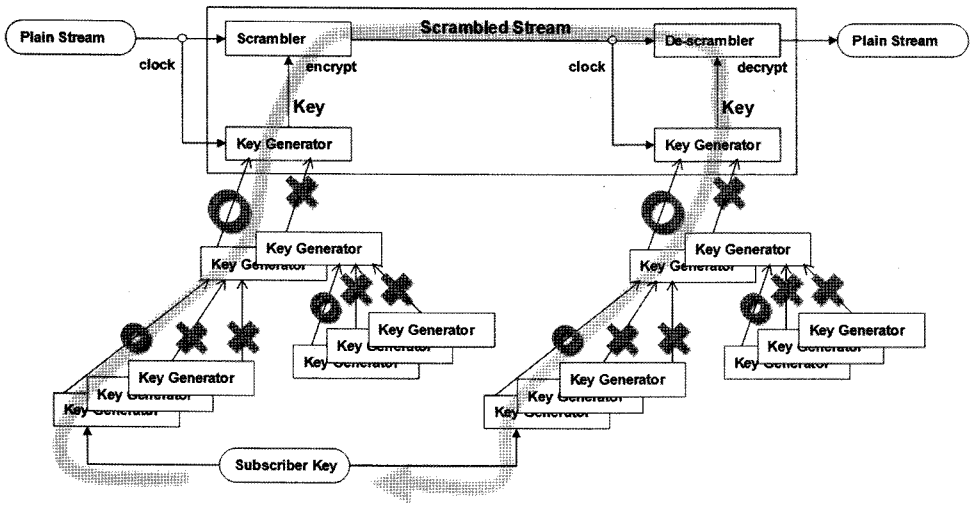


그림 2 그룹 기반의 접근 제어 기술

송 스트림을 암호화하는 것과는 달리 모든 스트림을 한번 암호화하고 키를 다단계로 공유하여 접근을 제어한다. 일반적으로 방송 제한 수신 기술을 보유한 업체는 EMM 기능을 사설화하고 가입자 그룹을 제어하는 방법을 공개하지 않으므로 해서 보안성을 확보하고 있다.

최근의 기술 동향은 저작권 보호 기술과 방송 제한 수신 기술을 접목하는 기술이 개발되고 있으며, 특히 사용자의 다양한 보안 서비스를 서로 연동하기 위한 연구가 개발 중에 있다.

4. IPTV 보안 기술 표준화 동향

IPTV 서비스를 위한 보안 서비스는 DVB의 CPCP을 중심으로 하는 DRM 기술 연구와 ATIS나 DVB를 중심으로 하는 CAS(방송 제한 수신 기술)이 주를 이루고 있다. 전통적인 관점에서 IPTV 서비스는 주문형(VoD) 방송과 실시간(Linear) 방송으로 구분되며 주문형 방송은 DRM 기술을 중심으로 발전하여 왔고, 실시간 방송은 CAS 기술을 중심으로 발전하여 왔다. 최근의 연구는 DRM 기반의 실시간 방송 수신 처리 기능이나 반대로 CAS 기반의 DRM 연구도 진행이 되고 있다.

다음은 IPTV 위한 보안 기술의 대표적인 표준화 기술인 OpenCable DCAS, DVB CPCM, ATIS IIF에 대해서 기술하고 각각이 가지고 있는 특징을 정리한다.

4.1 다운로드 제한 수신 기술 연구

그림 3은 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

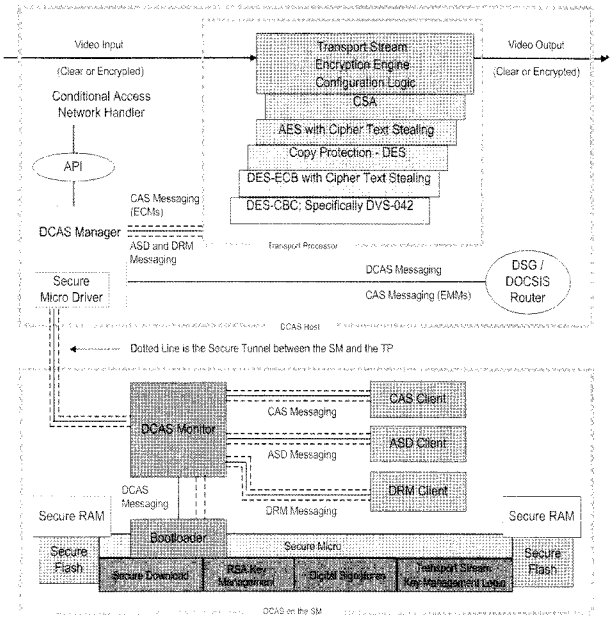


그림 3 OpenCable DCAS 구성도[2]

수 있도록 설계하였다. 여기서 암호화된 콘텐트를 복호화하는 기능은 TP(Transport Processor)에서 담당을 하며, CAS Client(다운로드 CAS 코드)에서 전송하는 Control Word를 통해 실시간 복호화하는 과정을 가진다.

기술 개발을 주도하고 있는 PolyCipher는 자사 제품의 출시를 미루고 있는데, 이를 두고 2가지의 소문이 무성하다. 하나는 SM 칩의 보안성에 문제가 있는 것이 아닌가 하는 부분이고 다른 하나는 SM 칩이 개당 US$ 20 정도의 고가로 인해 내부 딜레마에 빠져 있다는 소문이다. 현재는 Infineon 등의 호환 칩을 통해 일부 업체가 상용화하고 있다.

4.2 DVB-CPCM 기술 연구

DVB 측은 방송 제한 수신 기술에서 사업자가 동등

한 접근성을 보장하기 위해 많은 표준화를 시도하였다. 세부적인 제한 수신 기능보다는 전체적인 시스템에서 사업 간의 동등 접근을 보장하는 기술로 Multi-Crypt, SimulCrypt 이 대표적인 기술이다.

MultiCrypt는 다수의 방송 제한 수신 프로그램을 동시에 구동되는 특징을 가진다. SimulCrypt는 서로 다른 보안 업체에서 하나의 공통 암호화 알고리즘을 사용하고 업체별로 메시지(EMM, ECM)를 생성하여 전송하는 시스템이다. 이 기술은 하나의 방송 채널에 대해서 다수의 보안 업체가 동시에 서비스를 제공하기 위한 기술로 최근 KLabs(한국디지털케이블연구원)에서 케이블 방송에 도입을 추진하고 있다.

그림 4는 DVB의 CPCM 기술을 보여주고 있다. DVB는 댁내로 전달되는 네트워크와 홈 내에서 소비되는 네트워크를 분리하여 정리하고 있다. 그림에서 AP는 실제 방송 스트림을 수신하여 CPCM 콘텐트로 변환하는 역할을 수행한다. DVB 측에서는 기존의 방송 영역과 별도로 홈 안에서 유통되는 모델을 정의하고 있는 것이다. 즉 홈 내에서는 모든 콘텐트를 CPCM 콘텐트로 변환하여 유통하고 외부로 전송하는 경우에만 다시 변환하는 절차를 거치게 된다.

4.3 ATIS IIF(IPTV Interoperability Forum)

ATIS IIF는 IPTV 서비스의 상호 호환성을 확보하기 위해서 북미 통신 사업자 연합이 설립한 기구이다. 특히 보안 기술의 상호 호환성을 확보하기 위해서 IDSA(IIF Default Scrambling Algorithm)를 제시하고 있다. IDSA는 실시간 방송은 CAS 기술을 이용하고 비실시간 방송(On Demand) 방식은 DRM 기술을 이용하는 것이다.

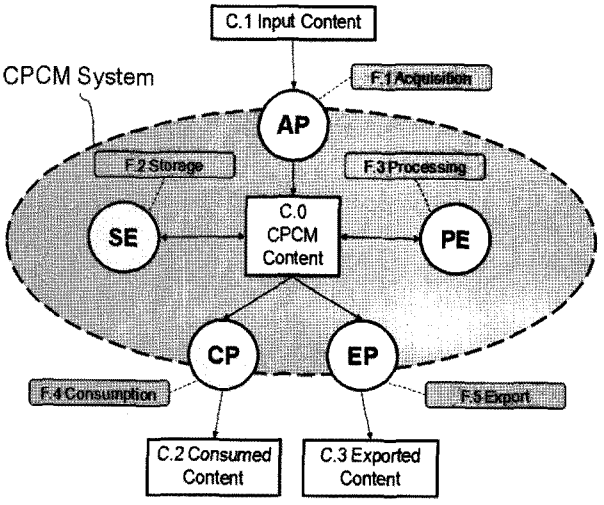


그림 4 DVB-CPCM 기술[3]

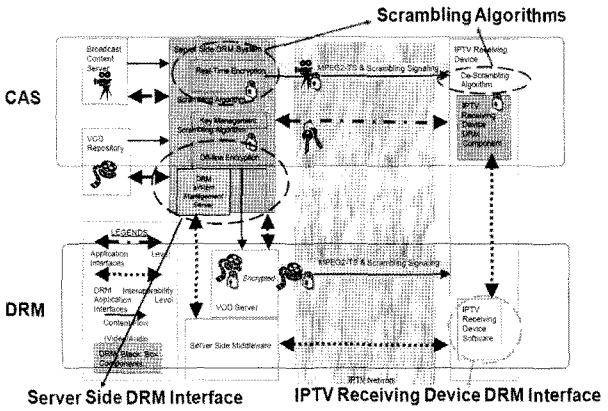


그림 5 ATIS IIF의 IPTV 보안 기술[4]

그림 5는 ATIS IIF에서 정의하고 있는 구조를 보여준다. 그림에서 상단부는 실시간 방송 서비스에 대한 기술로 Real-Time Encryption이 이루어지고 키 분배 과정을 모두 포함한다.

즉 전통적인 CAS 기술을 그대로 수용하고 있다. 반면 하단부는 사용자의 요구에 의해서 제공되는 VoD 서비스로 미리 암호화된 콘텐트를 이용하여 전송한다.

5. ITU-T IPTV 보안 기술 표준화 동향

ITU-T는 FG-IPTV를 통해 IPTV 표준화 요구사항을 도출하고, IPTV-GSI를 거치면서 세부적인 표준화 기술을 정리하고 있다. 각각의 요구사항은 해당 연구반(Study Group)에 전달되어 세부적인 표준화가 진행 중이다. 이 중에서 IPTV 보안 기술은 SG17(Study Group 17)의 Q6(Question 6)에서 5가지 문서로 표준화가 개발 중에 있다.

ITU-T Q6/SG17에서 개발 중인 문서는 "X.iptvsec-1: Functional requirements and architecture for IPTV security aspects", "X.iptvsec-2: Functional requirements and mechanisms for secure transcodable scheme of IPTV", "X.iptvsec-3: Key management framework for secure IPTV service", "X.iptvsec-4: Algorithms selection scheme for SCP descrambling", "X.iptvsec-5: SCP interoperability scheme"이며, 각각은 다음과 같다.

5.1 X.iptvsec-1: 요구사항 및 구조

ITU-T의 보안 표준안은 "콘텐트", "서비스", "네트워크", "단말", "사용자"로 구분되어 있다. 이 중에서 표준화 대상은 콘텐트와 서비스로 한정한다. 네트워크 보안 기능은 네트워크의 기반 기능으로 IPTV 서비스에 특화되지 않기 때문에 대상이 되지 않는다. 단말 및 사용자 보호 기술은 타 기술과 연동에서 고려

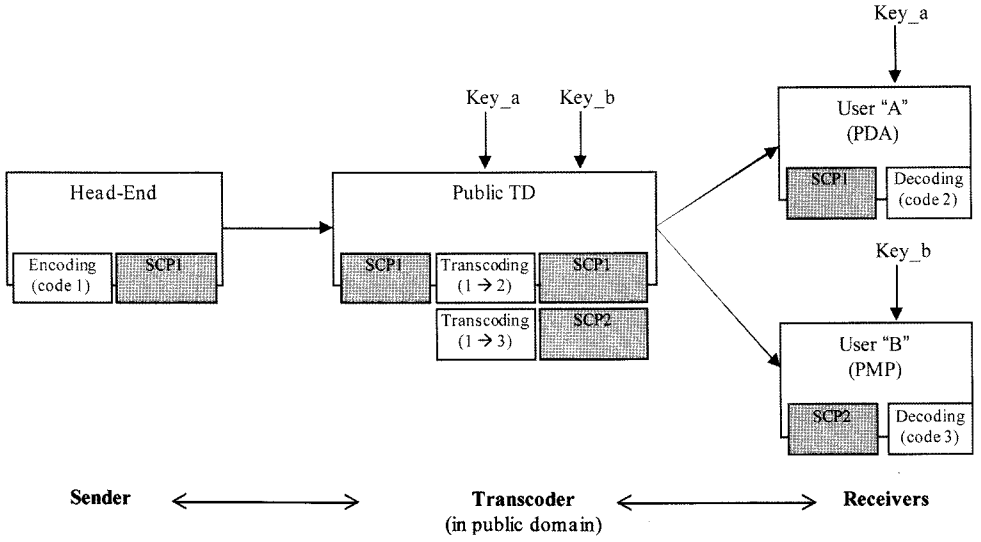


그림 6 트랜스코딩 개념

될 부분으로 직접적인 표준화 대상이 되지 못한다.

콘텐트 보호 기술은 전통적인 DRM 기술과 연계되어 있는 기술로 콘텐트 자체에 대하여 보안 기술을 적용한 것이다. 콘텐트 보호 기술은 콘텐트 제작자를 중심으로 표준화하고 있으며, 중국과 일본을 중심으로 자국 DRM 기술의 표준 반영에 집중하고 있다.

FG-IPTV 난 IPTV-GSI와 달리 SG17에서의 콘텐트 보호 기술에 대한 표준화 활동은 미미한 편이며, 국내에서 제안한 키 관리, 암호화, SCP 변환 기술이 활발하게 표준화 진행 중이다.

5.2 X.iptvsec-2: 트랜스코딩 가능한 보안 기술

X.iptvsec-2는 별도의 복호화 과정을 거치지 않고 트랜스코딩이 가능한 기술을 표준화 하고 있다. 모바일 단말기를 위해 별도의 스트림을 제작하지 않고, 기존의 스트림을 암호화된 상태로 다운 사이징하는 기술이다.

그림 7은 트랜스코딩 가능한 보안 기술의 간략한 시나리오를 보여준다. SCP(Service and Contents Protection) 기술은 트랜스코더에서 SCP1이 변하지 않고 PDA 용으로 다운사이징하는 경우와 완전 다른 SCP2로 변환하는 경우다.

전자는 H.264 SVC와 같이 별도의 디코딩하고 인코딩하는 것이 아니라 암호화된어 있는 상태로 변환하는 기술을 보여주는 것이다. 실제 SCP1에서 SCP2로 변환하는 과정은 X.iptvsec-5에서 기술하고 있으며 본 문서에서는 SCP가 변하지 않는 경우를 가정한다.

5.3 X.iptvsec-3: 키 관리 기술

IPTV 서비스의 키 관리 기술은 그림 8과 같이 3단계(TEK, SEK, URK)의 키를 정의한다. 방송 수신 제한 기술에서 사용하고 있는 다단계 키 관리 기술과 비교하여 보면 그림 1의 CW, AK, DK와 매칭된다. 현재의 문서는 멀티캐스트 프로토콜(실시간 방송)에 대해서만 그림 8과 같이 정의하고 있으며, 비실시간 방송에 대해서는 작업 진행 중에 있다.

본 표준화 문서는 IETF의 MIKEY를 기본으로 하고 있으며, DVB와 ATIS 문서를 참고하여 작성하고 있다. 실시간 방송에 대해서는 3단계 키 구조를 취하고 비실시간 방송에 대해서는 2단계로 낮추고 키를 발급 받는 과정에서 인증하고 권한을 설정하는 방식으로 추진되고 있다.

5.4 X.iptvsec-4: 복호화(Descrambling) 선택 기술

실시간 IPTV 방송 기술은 업체별로 서로 다른 암-복호화 기술을 사용하고 있기 때문에, 이들간의 호환성을 확보하기 위해서는 공통 복호화 부분을 정의하해야 한다. 본 문서는 공통 복호화 기술을 위해서 기존에 사용하고 있는 복호화 알고리즘을 선택하고 사용할 수 있도록 하는 문서이다.

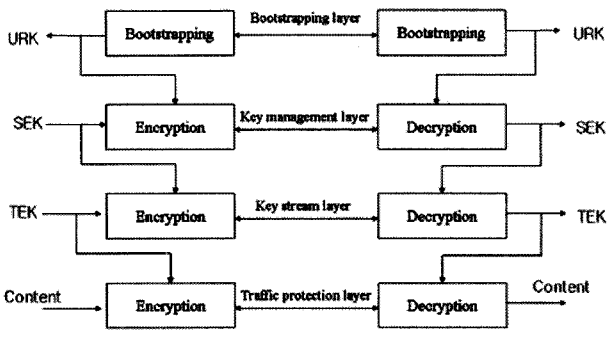


그림 7 다단계 키 관리 기술

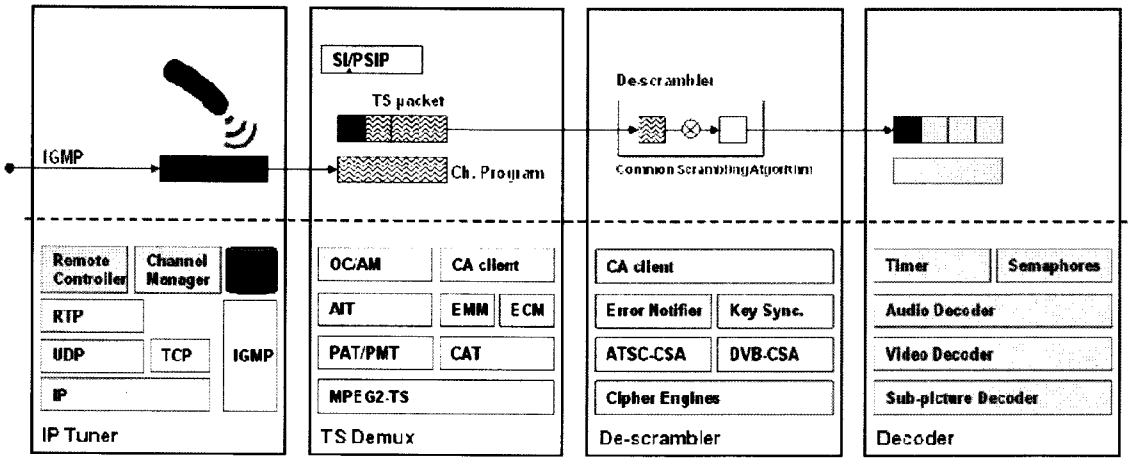


그림 8 복호화(Descrambling) 선택 기술

그림 9는 단말의 일반적인 작업 순서를 보여준다. 제한 수신 프로그램에서 해석한 키를 복호화기(Descrambler)로 전송하면, 복호화기는 방송 콘텐츠를 주어진 키로 복호화 한다. 기존의 제한 수신 제품들이 이 기능을 독점 혹은 사설화하여 차별화 했던 부분이다.

본 표준화 문서에서는 현재까지 제공되고 있는 다양한 알고리즘을 포함하여 암호화 기능을 선택적으로 사용할 수 있도록 하여, 단말기의 특정 사업자 종속 문제를 해결하는 것이다.

5.5 X.iptvsec-5: 보안 기술 상호호환 기술

본 문서는 서로 다른 보안 기술의 상호호환성을 확보하기 위해 표준화 진행하고 있는 문서이다. PVR 혹은 Service Roaming과 같이 서로 다른 보안 서비스를 변환해야 하는 경우에 대해서 표준화 되어 있는 형식을 이용하여 보안 기술을 적극적으로 변환할 수 있는 기술을 정의한다.

그림 10은 SCP1을 SCP2로 변환하는 내용으로 Content, Usage Rights, Metadata를 표준화되어 있는 중간 형식을 이용하여 변환하는 기술이다. 변환 과정에서 IPTV 서비스 사업자, PVR 제공 사업자, 보안 서비스 제공 사업자들의 정책에 따라서 진행한다.

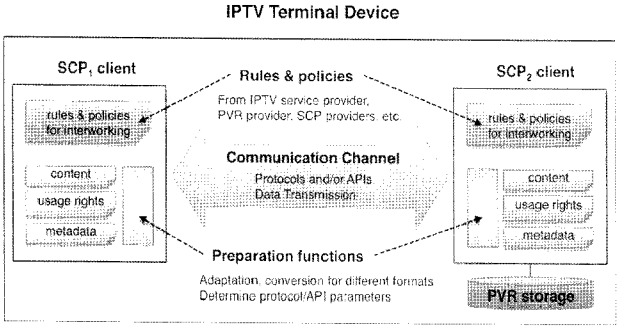


그림 9 보안 기술 상호 연동 기술

형식의 변환을 위해서는 SCP1이 중간 형식으로 변환하는 과정을 수행하고, 이를 다시 SCP2가 중간 형식을 SCP2에 맞는 보안 형식으로 변환하는 과정을 수행한다. 향후 변환 중간 형식에 대한 세부적인 기술을 정의해 나갈 예정이다.

5. 결 론

IPTV 서비스 보호 기술은 인터넷이 가지고 있는 양방향성과 방송이 가지고 있는 대중성을 기반으로 하고 있다. 특히 다운로드 가능한 방송 제한 수신 기술은 사용자 혹은 서비스 제공자마다 필요로 하는 제한 수신 기술을 달리 적용할 수 있는 기술로 특정 제한 수신 기술에 종속되지 않는 특징을 가지고 있다.

이들 특징을 그대로 반영한 기술이 제한 수신 기술(CAS)와 저작권 보호 기술(DRM) 이다. 이들 기술은 상호 배타적이면서 또 보완적인 특징을 가지고 있다. DVB의 경우는 CAS 기술과 DRM 기술의 영역을 구분하여 상호 보완적인 구조를 가지도록 연구가 진행 중에 있다. 북미의 ATSC 경우는 실시간 방송을 위해서는 CAS 기술을 적용하고 VoD(Video On Demand) 서비스에 대해서는 DRM 기술을 적용하고 있다. 이는 CAS와 DRM 기술이 상호 배타적이거나 경쟁적인 기술이 아닌 상호 보완적 기능을 수행하기 때문이다. ITU-T는 키 관리 기술, 암호화 기술, 보안 기술 호환성 확보 기술을 표준화하고 있어 II 장의 보안 요구사항을 만족하는 표준을 개발하고 있다.

따라서 IPTV와 같이 양방향 특징을 가지는 방송 서비스에서는 제공하는 방송의 형태에 따라서 CAS와 DRM 기술이 동시 제공되거나 통합하는 보안 기술이 요구된다. 이와 더불어 다양한 보안 기술들 사이의 호환성 확보를 위한 기술 개발이 요구된다.

참고문헌

[1] ATSC Standard, "Conditional Access System for Terrestrial Broadcast Revision A," 2004.

[2] Opencable, "DCASTM System Overview Technical Report", OC-TR-DCAS-D01-06-2-6, OpenCable™

[3] DVB, "Support For Use of Scrambling and Conditional Access Within Digital Broadcasting Systems," DVB Document A007, 1997.

[4] ATIS, "IIF Default Scrambling Algorithm(IDSA) IPTV Interoperability Specification," ATIS-0800006, 2007.

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

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

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

[8] DVB, "Multimedia Home Platform", http://www.mhp.org/

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

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

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

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

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

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

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

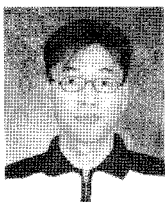
[16] Jae Hoon Nah, "The draft Recommendation for X.iptvsec-2: Functional requirements and mechanisms for secure transcodable scheme of IPTV", ITU-T SG17 Q6, 2009.

[17] Heung Youl Youm, "Proposed third draft text on Recommendation X.iptvsec-3: Key Management framework for secure IPTV services", ITU-T SG17 Q6, 2009.

[18] Jongyoul Park, "Draft Text on X.iptvsec-4: Algorithm selection scheme for SCP descrambling", ITU-T SG17 Q9, 2008.

[19] Kisong Yoon, Y.Jeong, D. Nam, "Draft Recommendation X.iptvsec-5, SCP interoperability scheme", ITU-T SG17 Q6, 2009.

[20] Heung Youl Youm, "X.1191, X.iptvsec-1: Functional requirements and architecture for IPTV security aspects", ITU-T SG17 Q9, 2008.



박 종 열

1996 충남대학교 학사
1999 광주과학기술원 석사
2004 광주과학기술원 박사
2001 U. of Utah, 객원 연구원
2004~현재 ETRI 선임연구원
관심분야 : 방송 수신 제한 시스템, 전자지불, 인증, 분산시스템 등
E-mail : jongyoul@etri.re.kr

문 진 영

2000 경북대학교 학사
2002 한국과학기술원 석사
2002~현재 ETRI 선임연구원
관심분야 : 방송 수신 제한 시스템, 자바카드, 메타데이타 기술 등
E-mail : jymoon@etri.re.kr

백 의 현

1984 숭실대학교 학사
1987 숭실대학교 석사
1997 숭실대학교 박사
1987~현재 ETRI 책임연구원
관심분야 : IPTV, 방송 제한 수신, 개방형 홈네트워크, 상황인지 등
E-mail : ehpaik@etri.re.kr