제한수신 기술 및 표준화 동향 분석

정준영* 구한승* 권은정* 권오형**

방송 및 통신 기술이 비약적으로 발달함에 따라 제한수신의 기술도 다양한 어플리케이션을 지원하기 위하여 여러 형태로 발전을 거듭하고 있다. 본 고에서는 최근 부각되고 있는 제한수신 기술들과 현재 시장에 제시된 제한수신 솔루션에 대해 소개하였다. 또한 디지털 방송 표준인 DVB, ATSC, OpenCable 에서 제시된 제한수신 관련 표준내용과 최근 미국의 주요 케이블 방송 사업자들이 주축이 되어 표준화를 준비중인 차세대 네트워크 아키텍처 (NGNA: Next Generation Network Architecture) 에서 제시하는 제한수신 요구사항에 대해 살펴보았다.

목 차

Ⅰ. 서 론

Ⅱ. 제한수신 시스템 개요

Ⅲ. 제한수신 기술 동향

Ⅳ. 제한수신 표준화 현황

Ⅴ. 맺음말

* ETRI 디지털 CATV 시스템연구팀/연구원
** ETRI 디지털 CATV 시스템연구팀/팀장

Ⅰ. 서 론

전 세계적으로 방송의 디지털 전환이 이루어 지고 있으며, 방송 제작과 관련된 기술 및 시스템 개발은 대부분 디지털화가 완료된 상황이다. 또한 방송과 통신이 결합되어 양방향성과 유연성이 증대되는 등 서비스 환경이 변화를 거듭하고 있다. 그러나 디지털 방송이 여러 가지 다양한 장점을 갖는 반면에 극복해야 하는 여러 가지 문제가 대두되고 있다. 그 중 최근 화두가 되고 있는 문제 중 하나는 방송을 통한 디지털 컨텐츠 배포와 관련된 것이다. 즉 디지털 컨텐츠는 아날로그 컨텐츠와 달리 매체의 특성상 완벽한 복제가 가능할 뿐만 아니라 편집 및 배포가 용이하기 때문에 컨텐츠에 대한 접근과 보호가 필수적이며 서비스 면에서 허가된 가입자 만이 해당 컨텐츠에 대해 접근할 수 있도록 허용되

어야 한다. 특히 케이블 또는 위성 방송과 같이 높은 가치의 방송 컨텐츠를 제공하는 유료방송 서비스에서 무단 시청과 불법 복제 및 대량 배포는 사업의 성패를 좌우하는 큰 문제로 전면에 부상될 것이 예상된다.

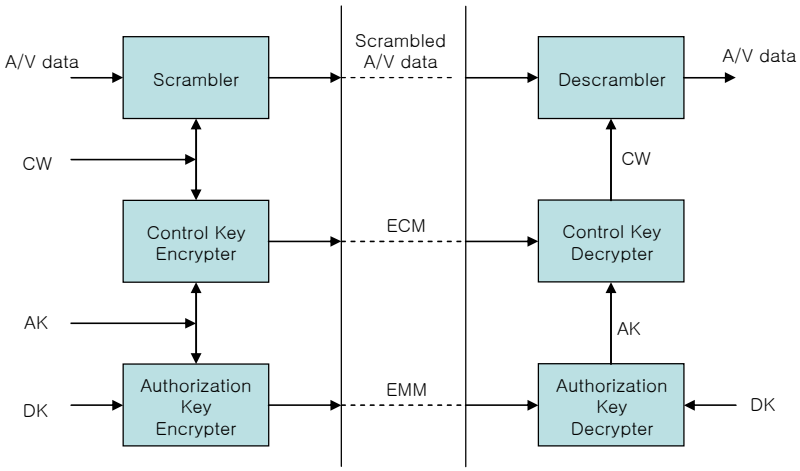
제한수신은 위와 같은 문제를 해결하기 위해 서비스 가입자들로 하여금 특정 프로그램을 시청하고자 할 경우 수신 시스템이 자동으로 수신자를 인식하여 서비스 제공 여부를 판단하여 허가된 가입자 에게만 수신이 가능하도록 처리해 주는 전 과정을 포함한다. 따라서 제한 수신 기술은 방송사들이 전문 프로그램을 상업화하고 이익을 창출하기 위해 필수적인 것이며, 이 제한 수신 기술을 얼마나 효과적으로 운용하는 가에 따라 디지털 유료방송의 미래가 달려있다고 해도 과언은 아닐 것이다.

본 고에서는 제한 수신 기술에 대해 간략하게 살펴보고 제한 수신 기술의 최근 주요 이슈와 동향 및 표준화 현황에 대해 논의하고자 한다.

II. 제한수신 시스템 개요

방송이 디지털화됨에 따라 과거 아날로그 유료방송에서 사용된 단순히 송출된 신호에 왜곡을 발생시켜 이를 수신기에서 복원하는 형태의 제한수신 기술에서 가입자 인증을 기반으로 하여 송출 데이터를 암호화하고 수신기에서 이를 복호화하는 형태의 제한수신 기술이 등장하였다. 제한수신 시스템(CAS: Conditional Access System)은 가입자 관리 시스템(SMS: Subscriber Management System)과 함께 유료방송 서비스를 위해 필수적인 것으로 가입자에게 원하는 프로그램의 제공과 PPV(Pay-Per-View) 및 VOD(Video on Demand) 등과 같은 다양한 부가 서비스를 지원하며 제공되는 서비스의 보안성을 책임지는 시스템이다. 방송 사업자에게는 무자격자의 불법 시청을 방지할 수 있게 하고, 가입자의 시청 성향 등 마케팅 자료를 제공함과 동시에 이를 바탕으로 한 타깃 마케팅을 가능케 한다.

제한수신 시스템이 갖추어야 할 기본적인 기능 요건은 프로그램 및 데이터를 스크램블링하고, 통신 링크상에서 보호되어야 하며, 인증 기능과 접근 제어 기능을 갖추어야 한다. 일반적인 제한수신 시스템의 구성은 (그림 1)에서 보는 바와 같이 송신단에서 데이터를 스크램블링하는 과정과 스크램블링에 사용되는 제어단어(CW: Control Word)를 인증키(AK: Authorization Key)로 암호화하는 과정 그리고 인증키를 분배키(DK: Distribution Key)로 암호화하는 과정으로 나누어 진다 [1]. 수신단에서는 송신단과 동일한 구성을 가지며 역의 과정을 통해 인증키를 분배키로 복호화하고 복호화된 인증키로 다시 제어단어를 획득하며, 획득된 제어단어를 통해 데이터를 디스크램블링하여 시청 가능한 형태의



• CW: Control Word
• AK: Authorization Key
• DK: Distribution Key
• ECM: Entitlement Control Message
• EMM: Entitlement Management Message

(그림 1) 제한수신 시스템 구조

신호를 출력하게 된다. 제한수신 시스템의 주요 기능은 다음과 같다.

스크램블링/디스크램블링 (Scrambling/Descrambling)

수신자격이 없는 수신자는 시청이 불가능하도록 데이터를 암호화한다. 암호화된 방송 컨텐츠의 제어는 제어단어(CW)를 이용하여 암호화 및 복호화를 처리한다. 즉 제어단어는 방송 데이터를 암호화하고 복호화하는 일종의 키로 작용한다. 이 제어단어는 다시 암호화기(Encryptor)에 의해 보호되어 스크램블링된 방송 데이터와 함께 전송되며 수신기의 복호화기(Decryptor)에서 암호화된 제어단어를 복호화하여 방송 데이터 디스크램블링을 수행한다. 이를 위해 송신부와 수신부에는 반드시 같은 비밀키를 공유하여야 하며 이러한 비밀키를 공유하는 과정에서 보안성을 높이기 위해 스마트카드 등을 사용하여 사용자에게 전달한다.

자격 제어 (Entitlement Control)

제어단어(CW)를 인증키로 암호화하고, 이를 ECM(Entitlement Control Message)에 실어서 수신자에게 전송한다. 보안을 위해 제어단어는 주기적으로 전송되며, 그 때마다 제어단어가 새롭게 생성

되고 암호화된다. ECM 에는 암호화된 제어단어 외에 제어변수가 포함되며, 수신기는 전송된 ECM 을 수신할 수는 있지만 수신된 제어변수와 수신기의 인증변수를 비교하여 정당한 사용자로 판단될 경우에만 제어단어를 해독하고, 이를 이용하여 수신된 프로그램을 디스크램블링 한다.

자격 관리 (Entitlement Management)

수신기에 자격을 부여/갱신/관리하는 기능을 하며, 인증키를 분배키로 암호화하여 EMM (Entitlement Management Message)을 생성하고 암호화하여 수신자에게 전송한다. EMM 은 수신기의 제한수신 모듈에 자격을 부여하거나 또는 갱신하는 기능을 한다. 송신부에서는 가입신청을 한 정당한 수신자에게 해당프로그램의 인증키와 수신자격을 전송한다. 인증키는 해당 수신자 고유의 비밀키를 이용하여 암호화한 다음 인증변수와 함께 EMM 에 포함되며 메시지 변조 방지를 위해 전자서명 등이 추가되어 전송된다.

III. 제한수신 기술 동향

방송 및 통신 기술이 비약적으로 발달함에 따라 제한수신의 기술도 다양한 어플리케이션을 지원하기 위해 여러 형태로 발전을 거듭하고 있다. 이 장에서는 최근 부각되고 있는 제한수신 기술들과 현재 시장에 소개된 제한수신 솔루션에 대해 살펴보기로 한다.

CA 응용의 구현 형태에 따른 제한수신 시스템의 유형

제한수신 시스템의 최신 기술 동향을 알아보기 앞서, CA 응용의 구현 형태에 따라 제한수신 시스템의 유형을 나눠보기로 하자 [2]. 여기서 CA 응용은 가입자 수신 단말에 위치해 제한 수신용 키 관리 및 자격 제어를 담당하는 기능 모듈을 의미한다.

첫 번째 CA 응용 구현 유형은 일반 OS 에 클라이언트 형태로 CA 응용을 구현하는 것이다. 이 방식에서는 키 관리와 자격관리 프로그램을 단순히 일반적인 형태의 마이크로 프로세서에 탑재한다. 하지만, 이 방식은 역 엔지니어링 공격에 매우 취약하다.

두 번째 유형은 보안이 강화된 소프트웨어 형태로 CA 응용을 구현하는 것이다. 이때 CA 응용은 프로그램 내 키 관리와 자격관리 부분이 해커에 의해 역 엔지니어링 공격을 당하는 것을 방지하기 위한 보안 메커니즘을 포함하게 된다. 또한, 이 방식은 양방향 네트워크를 통해 CA 응용에 대한 인증을 실시함으로써 응용 복제(cloning)와 같은 공격을 막을 수 있다. Iredeto 의

SoftClent 솔루션이 두 번째 유형의 한 예가 된다 [5].

세 번째 유형은 셋탑박스 내 SoC 칩에 CA 응용을 구현하는 것이다. 셋탑박스에서 사용되는 일반적인 SoC 를 디자인할 때 부가적으로 키 관리와 자격관리 기능을 추가하여 구현하게 된다. 칩 자체는 스마트카드에서 사용된 칩 수준의 보안을 제공하지는 않지만, 소프트웨어 만으로 구현된 것 보다는 안전하다.

네 번째 유형은 셋탑박스에 내장된 형태의 소프트웨어와 독립된 모듈인 스마트 카드를 함께 사용해 CA 응용을 구현하는 것이다. 이 유형에서 소프트웨어는 스마트카드가 생성한 제어단어(Control Word)를 보호하고 스마트카드로 향하는 메시지 흐름을 제어하는 역할을 수행한다. 이 형태는 보안의 핵심적인 기능을 스마트 카드가 처리하고, 소프트웨어는 부가적인 기능을 구현하는 형태이다. 하지만, 셋탑박스 내 소프트웨어는 해커에 의한 역 엔지니어링 공격에 취약하기 때문에 제어단어를 안전하게 보호할 수는 없다.

다섯 번째 유형은 셋탑박스에 내장된 보안 칩과 스마트 카드를 함께 사용해 CA 응용을 구현하는 것이다. 셋탑박스에 내장된 보안 칩은 스마트 카드와 셋탑박스 사이에 보안 채널을 형성한다. 그리고, 스마트 카드는 암호화된 제어단어를 셋탑박스로 출력하고, 셋탑박스는 내장된 보안 칩을 사용해 암호화된 제어단어를 복호화 한다. 이 방식에서는 키(key)나 자격정보와 같이 매우 중요한 정보는 스마트 카드에 저장되기 때문에 셋탑박스 내 보안칩의 보안 수준은 높지 않아도 된다.

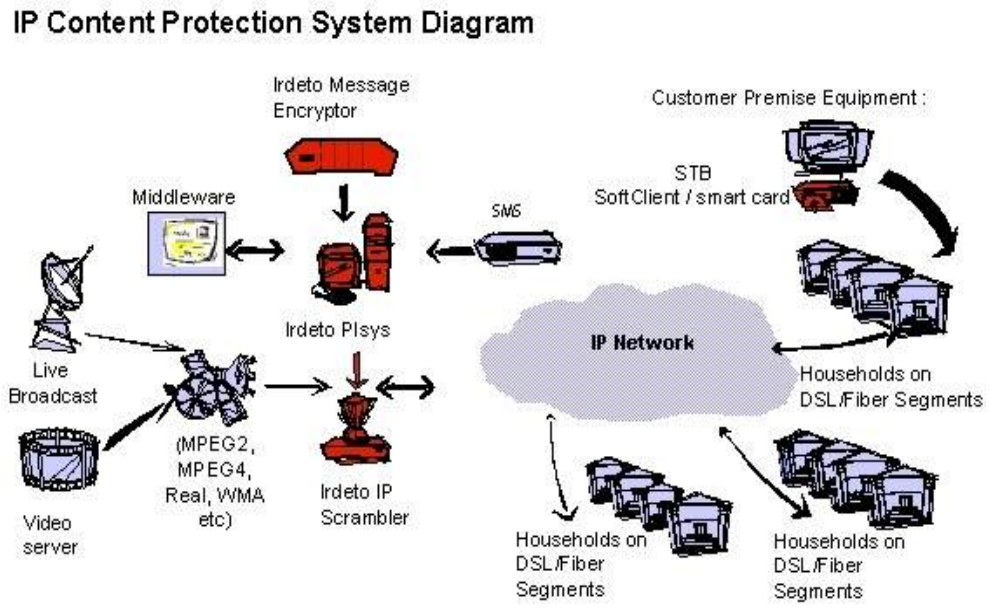
마지막으로 여섯 번째 유형은 셋탑박스에 보안 칩 만을 내장해 CA 응용을 구현하는 것이다. 이 유형에서는 셋탑박스 마더보드에 보안칩을 내장한다. 칩이 키(key)나 자격 정보와 같이 중요한 정보를 저장해야 하기 때문에, 다섯 번째 유형에 사용된 보안 칩 보다는 높은 레벨의 물리적 보안이 요구된다. 하지만, 이 유형은 단 방향 네트워크 상에서 보안의 결합으로 인해 키 관리 및 자격관리 알고리즘 갱신이 요구될 때 셋탑박스 자체를 교환해야 하기 때문에 스마트 카드를 사용한 방식 보다 유연한 운용을 할 수 없다. 물론, 양방향 네트워크 상에서는 안전한 소프트웨어 다운로드 방식을 이용해 CA 응용을 갱신할 수 있다. 참고로, 이 방식은 추후에 자세히 설명하게 될 NGNA 제한수신 표준과 동일한 개념의 구조다.

소프트웨어 기반 제한 수신 시스템

최근, 이슈로 부각되고 있는 제한수신 시스템의 유형은 스마트 카드를 배제한 소프트웨어 기반의 제한수신 시스템이다 [2, 3]. 소프트웨어 기반의 제한수신 시스템이 관심을 끄는 첫 번째

이유는 스마트 카드 또는 OpenCable™의 CableCARD 등과 같은 하드웨어 기반의 제한수신 모듈을 사용했을 경우 모듈에 대한 발급 및 갱신 비용이 방송 사업자들에게 큰 부담으로 한다는 것이다. 특히, OpenCable™방식에서 요구하는 PCMCIA 형태의 CableCARD 는 스마트 카드보다 많은 운영 비용을 요구한다. 두 번째 이유는 예전의 단 방향 방송 네트워크가 양방향 네트워크로 변하는 점을 들 수 있다. 단 방향 네트워크에서의 제한수신 시스템은 사용자와 동일 시 되는 스마트카드 또는 CableCARD 가 없으면 실체 인증이 불가능했다. 하지만, IPTV 와 같이 양방향 방송이 점차 가시화 되고 있는 현재는 스마트카드와 같은 하드웨어를 통한 실체인증이 반드시 필요하지 않게 되었다. (그림 2 참조) 이러한 이유들 때문에 양방향 네트워크 상에서 소프트웨어 기반 제한수신 시스템이 시장에 소개되고 있는 것이다. 특히, 소프트웨어 기반 제한수신 시스템은 200,000 ~ 300,000 명의 가입자 수를 갖는 소규모 네트워크에서는 매우 유리한 위치를 차지할 것으로 예상되고 있다.

소프트웨어 기반의 제한수신 시스템이 운용비용 절감이라는 측면에서 큰 매력을 가지고 있지만, 보안 측면에서는 아직까지 하드웨어 기반의 제한수신 시스템이 우세하다. 왜냐하면, 단순히 플래쉬 메모리에 CA 응용 코드를 저장하는 소프트웨어 방식은 보안 칩을 사용한 스마트 카드 보다 역 엔지니어링과 같은 물리적 공격에 매우 취약하기 때문이다. 하지만, 소프트웨어 기반



(그림 2) IP 컨텐츠 보호 시스템 예

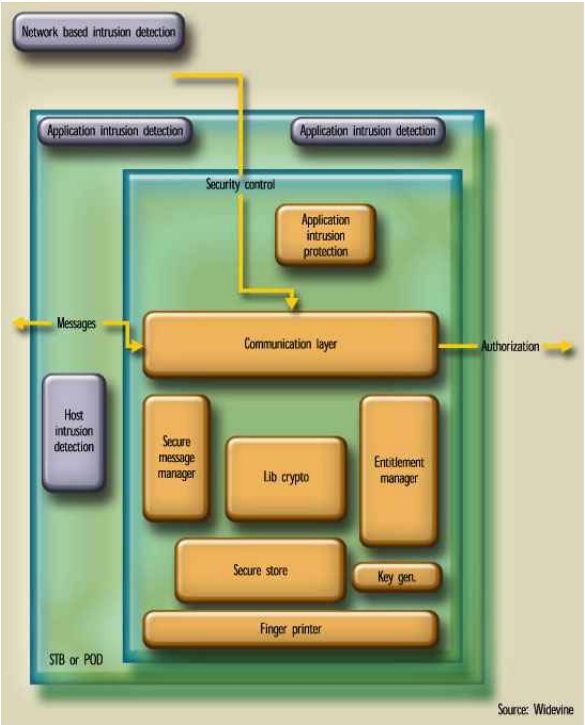
의 제한수신 시스템을 주장하는 측은 소프트웨어 기반의 제한 수신 시스템 솔루션이 하드웨어 기반의 제한수신 시스템 보다 훨씬 빠르게 CA 응용을 갱신할 수 있기 때문에 보안적인 측면에서 문제될 것이 없다고 말한다 [3]. 왜냐하면, 제한수신 시스템에 치명적 보안 결함이 발생했을 때 소프트웨어 기반의 제한수신 시스템은 단순히 새로운 CA 응용을 다운로드 하면 되기 때문이다.

현재까지 시장에 소개된 소프트웨어 기반 제한수신 시스템에는 Latens Systems 사의 Latens 제한수신 시스템이 채택한 Widevine Technologies 사의 Cyper VSC(Virtual SmartCard) 솔루션, Iredeto 사에서 IPTV 용 제한수신 시스템으로 개발한 SoftClient 솔루션, 그리고 NDS 사가 개발한 VGS(VideoGuard Security Server)솔루션 등이 있다. Cyper VSC 솔루션과 VGS 에 대한 보다 구체적인 내용은 다음과 같다.

- Cyper VSC

VSC 의 구성은 (그림 3)과 같으며, 주요 구성요소에 대한 설명은 다음과 같다 [4, 6].

- Secure Store: VSC 에서 가장 중요한 구성요소가 바로 secure store 이다. 다른 보안 모듈들이 그렇듯이, VSC 에서도 제한수신 시스템에서 사용되는 보안 정보들을 가장 안전하게 저장하는 것이 그 시스템의 안전도를 결정하는 중요한 요소가 된다. Secure store 는 키(key)정보나 자격 정보 등 해커로부터 안전하게 보호되어야 할 정보들을 저장하며, 여기에 저장된 정보들은 finger printing 프로세스를 통해 셋탑박스와 같은 호스만이 볼 수 있다.
- Finger printer: finger printer 모듈은 클라이언트 또는 서버에게 고유한 식별 정보를 제공한다. 이 finger printer 는 숫자 또는 고유 인자들로 구성되며, finger printer 를 구성하는 고유 인자들을 'ridge'라고 부른다. 'ridge'의 예로는 하드웨어 시리얼 넘버, 운영체제 버전 넘버, 인터넷 프로토콜 주소, 또는 물리적 메모리 크기 등이 된다. 이러한 finger printer 는 여럿이 모여 hand printer 를 구성하며, 시스템 내에 존재하는 개인용 컴퓨터, 서버, 셋탑박스등을 식별하는 고유한 값이 된다. 특히, 각 finger printer 그룹의 배열이나, 각각의 'ridge'들은 finger print 또는 hand print 결과에 영향을 주도록 되어 있어, 각 사용자들이 우연히 같은 'ridge'을 갖게 된다 하더라고 결과적으로 서로 다른 finger print 와 hand print 를 갖게 된다.



(그림 3) Cyper VSC 구성 모듈

- Secure message manager: 이 모듈은 서로 다른 상대방과 메시지를 주고 받을 때 상대방에 대한 인증 및 메시지 자체에 대한 프라이버시를 제공한다.
- Entitlement management: 이 모듈은 사용자의 시청자격을 관리한다. 여기서 말하는 시청자격은 컨텐츠에 대한 저장권한, 복사권한, 단순 시청권한등을 의미한다.
- Key generation: 이 모듈은 제한수신 시스템이 요구하는 다양한 키(key)들을 생성하는 역할을 한다.
- Digital copy protection: 응용계층에서 컨텐츠 보호를 하는 기능을 부여한다. 예를 들어 소프트웨어 또는 하드웨어에 차원에서의 칩임 감지 및 응답 메커니즘과 같은 강력한 컨텐츠 보호 메커니즘을 지원한다.

● VGS

NDS 의 소프트웨어 기반 제한수신 시스템 솔루션인 VGS 는 셋탑박스내 플래쉬 메모리에 중요한 사용자 인증 정보를 저장하지 않고, 원격으로 떨어진 보안 서버에 사용자 인증정보를 저

장한다. 이때 사용자 단말과 같은 네트워크 상에 위치한 보안 서버는 높은 데이터 전송률을 갖는 DOCSIS 나 DAVIC 과 같은 리턴 채널을 통해 연결되어야 한다. 이런 시스템 구성을 통해 해커들에 의해 쉽게 그 내용이 노출될 수 있는 사용자 단말 내 저장장소를 인증정보 저장장소로 사용하지 않아도 되는 장점이 있다. 이때 보안 서버로 사용되는 것이 바로 VGS(VideoGurard Security Server)이다. VGS 솔루션에 의하면, 사용자 단말은 수 초마다, 인증 정보를 다운로드 받을 수 있는지 물어보며, VGS 는 0.5 초 이내에 이에 대한 응답을 해야 한다 [7].

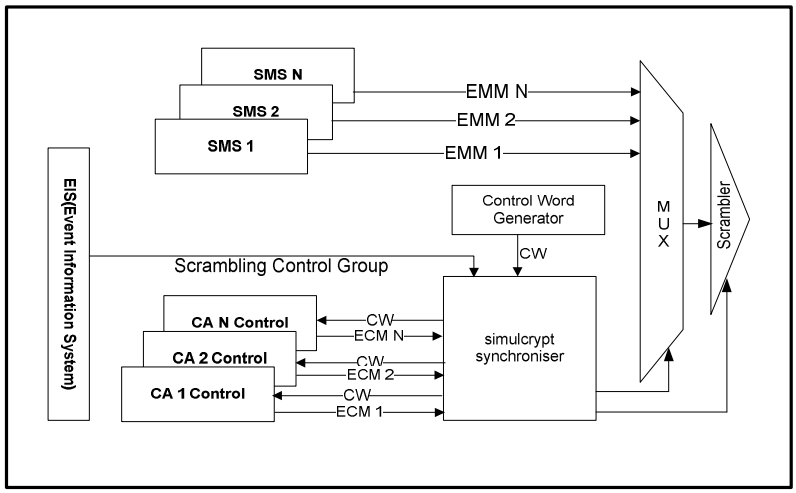
Ⅳ. 제한수신 표준화 현황

앞에서 최근 부각되고 있는 제한수신 기술들에 대해 살펴보았다. 이 장에서는 디지털 방송 표준인 DVB, ATSC, OpenCable 에서 제시된 제한수신 관련 내용과 최근 미국의 주요 케이블 방송 사업자(MSO)들이 주축이 되어 표준화를 준비중인 차세대 네트워크 아키텍처 (NGNA: Next Generation Network Architecture)에서 제시하는 제한수신 요구사항에 대해 살펴보도록 한다.

DVB 의 제한수신

DVB 는 1993 년 제한수신에 대한 논의를 시작하면서 방송 사업자의 상업적인 요구 사항을 바탕으로 제한수신에 대한 기술적인 표준화를 추진하였다. DVB 는 제한수신에 대한 개방적인 국제 표준을 제시하기 위하여 가입자 단말기(Set-top Box)의 사용과 배포에 관한 것 등에 관심을 두었다. 특히 유료방송 서비스가 임의의 제한수신 시스템 사업자에 의하여 시장이 독점되는 것을 방지하는 것에 중점을 두었으며 이를 위해 Simulcrypt 기술을 표준화 하였다. 이 기술은 여러 제한수신 공급자를 수용하기 위하여 가입자의 수신기(Set-Top Box)에서 디스크램블링과 암호화 처리를 담당하는 부분을 모듈로 분리한 방식이다. 또한 모듈에서 동작하는 디스크램블링과 암호화 기능을 분리하여 디스크램블링 방식은 Common Scrambling 알고리즘인 DVB-CSA(Common Scrambling Algorithm)을 사용하도록 하고, 암호화 방법은 각 제한수신 시스템마다 다르게 사용하도록 하여 가입자 수신기는 서로 다른 제한수신 시스템을 갖는 보안 모듈을 수용할 수 있도록 하였다 [8].

(그림 4)는 Simulcrypt 의 개념도를 설명하고 있다 [9]. 제어단어(CW: Control Word)의 생성은 한 곳에서 이루어지며 Simulcrypt Synchroniser 을 통해 제어단어 생성 주기 마다 TCP/IP 통신을 통해 스크램블러 제어단어를 전송하고 제한수신 시스템으로 제어단어를 전송한



(그림 4) Simulcrypt 개념도

다. 이에 따라 제한수신 시스템은 Simulcrypt Synchroniser 을 통해 여러 개의 제한수신 시스템으로부터 생성되는 ECM 을 재다중화기로 전송하기 할 수 있으며 SMS 는 가입자 별로 ECM 을 해석하기 위한 EMM 을 생성하여 재다중화기로 전송 할 수 있도록 하였다.

Common Scrambling 기술에 대한 표준의 내용은 스크램블링 알고리즘, CA 와 관련된 메시지가 MPEG2-TS 패킷에서의 다중화 되는 방법 그리고 제어단어를 생성하고 스크램블러로 전송하기 위한 메커니즘 등에 관련된 것이다. 이와 관련하여 MPEG 시스템 ISO/IEC 13818-1 에 제한수신 시스템으로부터 생성되는 메시지에 대하여 Table ID 값에 대한 정의를 추가하고 모듈에서 다수의 제한수신 시스템을 구별하기 위해서 CA_descriptor 를 정의하는 방법을 규정하였다. 이 표준은 ETSI(European Telecommunications Standards Institute)를 통해 NDA(non-disclosure)를 체결한 기관들에 배포될 수 있도록 하였다.

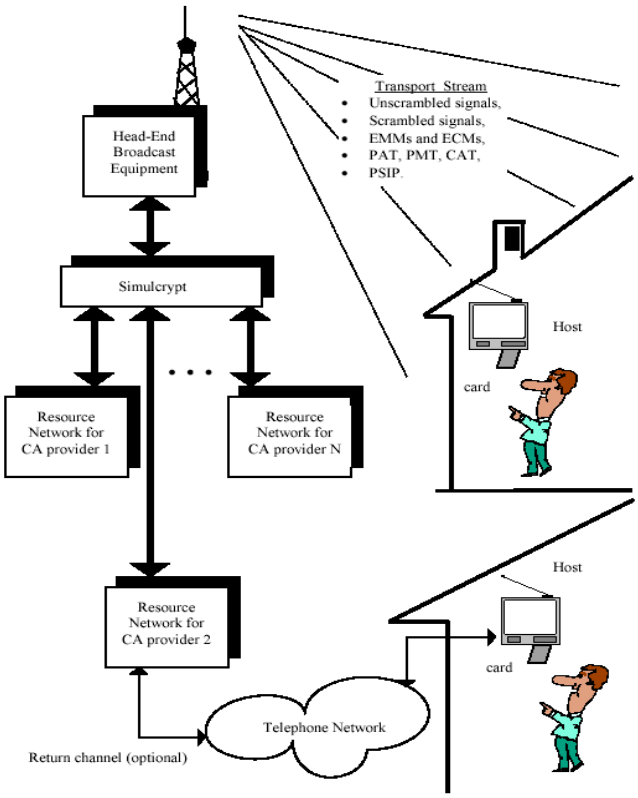
Common Interface 는 방송 스트림이 호스트에 수신되면 Common Interface 를 통해 모듈로 스크램블된 신호를 전송하고 모듈의 암호화 처리를 담당하는 제한수신 시스템 및 디스크램블러에 의해 디스크램블된 신호를 다시 호스트로 전송하는 방식을 제공한다. 특징적인 것은 모듈이 호스트의 리소스와 통신하기 위한 방법으로 모듈이 MMI(Man Machine Interface)를 통해 호스트로 간단한 디스플레이 명령을 보냄으로써 호스트에 대한 정보를 획득하거나 IEEE 1394 와 같은 입출력 포트를 통해 PC 나 VCR 로 데이터를 전송할 수 도 있다는 점이다. 이 표준은 향후 DAVIC(Digital Audio Video Council)규격의 security part 및 미국의 NRSS(National Renuwable Security Standard)의 규격의 기반을 제공하였다.

ATSC 의 제한수신

ATSC 에서 제시하고 있는 제한수신 관련 표준의 주요 특징은 Simulcrypt 방식을 채택했다는 것이다. 즉 하나의 프로그램에 대해 여러 개의 제한 수신 시스템이 동시에 적용될 수 있는 구조를 가지고 있다. ATSC 에서 규정한 Simulcrypt 방식은 앞에서 설명한 DVB 표준에서 제시된 Simulcrypt 규격을 그대로 준용하고 있다. (그림 5)는 ATSC 제한수신 시스템의 주요 구성 요소들을 간략하게 보여준다 [10].

Simulcrypt 방식을 위해 요구되는 Common Scrambling 규격은 DVB 에서 규정한 스크램블링 알고리즘과 다르다. ATSC 에서 규정한 스크램블링 알고리즘은 8 바이트 블록을 입력 받아 8 바이트 블록을 출력하는 CBC(Cipher Block Chaining) 모드의 Triple-DES 를 정의하고 있으며 MPEG TS 패킷 레벨에서만 스크램블이 가능하다.

또한 수신 측에서 Replaceable 제한수신 모듈(이하 제한수신 모듈)의 사용을 규정하고 있다. 즉



(그림 5) ATSC 제한수신 시스템 구성 요소

스크렘블링된 방송 데이터에 대한 디스크렘블링은 제한수신 모듈이 담당하게 된다. 제한수신 모듈의 기술로 NRSS-A(스마트 카드)와 NRSS-B(PCMCIA)의 두 가지 종류를 허용한다. 즉 제한수신을 지원하는 DTV 수신기는 NRSS-A 또는 NRSS-B, 또는 둘 다를 처리하기 위한 하드웨어 및 소프트웨어를 포함해야만 한다. 수신기와 제한수신 모듈간의 통신 규격에 대한 별도의 규정은 하지 않지만 대신 NRSS 의 사용을 의무화하고 있다.

OpenCable 의 제한수신

1996 년 12 월 미국의 통신 위원회인 FCC(Federal Communication Commission)는 방송통신융합법인 Telecom Act 를 통과시키면서 디지털 케이블 방송에 대비하여 수신기(Set-Top Box)에서 제한수신 모듈의 분리를 제시하였다. 1998 년 9 월에는 FCC 에서 NRSS 표준규격을 제정하여 수신기(Set-Top Box)와 제한수신 모듈의 분리를 명시하였으며, 최초 2005 년 1 월부터 분리를 의무화하였다. 하지만 현재 케이블 방송 산업계와 FCC 간의 대립으로 인해 분리의 의무화 시점이 2007 년 7 월 이후가 되었다. OpenCable 표준은 이와 같은 FCC 의 요구사항을 만족하기 위해 CableLabs[1]에서 규격화한 것으로 일부 수신기 업체의 독점공급을 막고, 서비스 업체 및 서비스 지역에 상관없이 케이블 방송 서비스를 제공하고자 하는 목적으로 추진되었다.

OpenCable 에서 제시하고 있는 제한수신 관련 표준의 주요 특징은 (그림 6)와 같은 PCMPIA 카드 타입의 분리형 제한수신 모듈(CableCARD)의 사용이다 [11]. DVB 와 ATSC 에서 규정한 Simulcrypt 방식과 같은 송신부에 관련된 부분은 표준에서 언급하고 있지 않다. 따라서 Common Scrambling 과 같은 규격이 이 표준에서는 포함되지 않고 제한수신 모듈이 디스크램블링에 대한 모든 책임을 가진다. 따라서 DVB 와 ATSC 표준에 비해 제한수신 시스템의 적용이 더 자유롭다고 볼 수 있고 보안의 측면에서도 더 강화되었다고 말할 수 있다. 하지만 송신부 장비들간의 호환성에는 그다지 좋지 않다.

(그림 6) 분리형 제한수신 모듈

즉 OpenCable 에서는 수신기와 제한수신 모듈간의 인터페이스만을 규정하고 있다. 이 인터페이스 규격은 기본적으로 NRSS 의 규정을 따르며, 응

[1] CableLabs: 1988 년 북미 케이블방송 산업계의 멤버들로 구성된 비영리 표준화 단체

용을 위해 다른 요소들이 추가로 정의되었다. 수신기와 제한수신 모듈간의 인터페이스에는 인증서(X.509)기반의 상호 인증을 기초로 하고 있으며, 이 인터페이스에서 제한수신 모듈을 통해 디스크램블링된 방송데이터를 수신기로 전달할 때 발생할 수 있는 불법 복제를 막기 위해 별도의 복제방지 규격을 규정하고 있다 [12].

NGNA 의 제한수신

NGNA 는 최근 미국의 주요 케이블 방송 서비스 업체인 컴캐스트, 타임워너, COX 커뮤니케이션을 주축으로 하여 기존 케이블 TV 망인 HFC 인프라에 추가적인 투자 없이 비용 효율적으로 통신 및 멀티미디어 서비스를 포함하는 통합 멀티미디어 구조를 구현할 수 있도록 하는 것을 목표로 하고 CableLabs 를 통해 표준화 작업을 진행 중에 있다 [13].

NGNA 에서는 제한수신과 관련하여 다운로드 가능한 제한수신 (Downloadable CA)을 제시하였다. 이는 수신기와 제한수신 모듈(e.g. CableCARD)간의 하드웨어적인 분리 대신, 수신기에 제한수신 어플리케이션을 다운로드하는 방식의 소프트웨어적인 분리를 의미한다. 즉, 제한수신 어플리케이션을 동작시키기 위한 표준화된 제한수신 프로세서를 수신기에 내장하여 원격으로 제한수신 방식을 구성하거나 재설정할 수 있도록 한다.

즉 NGNA 에서 표준화하고자 하는 대상은 다운로드 가능한 제한수신을 지원할 수 있는 제한수신 프로세서의 기능 및 구조이다. 이 제한수신 프로세서는 여러 개의 디스크램블링 알고리즘들을 처리할 수 있는 유연한 복호화 엔진(Flexible Decryption Engine)과 제한수신 키 관리를 위한 키 관리 어플리케이션 등으로 구성된다.

유연한 복호화 엔진은 서비스 운영자가 선택할 수 있는 제한수신 시스템에 많은 자유를 허락해준다. 이를 위해 유연한 복호화 엔진은 적어도 아래에 제시된 디스크램블링 알고리즘을 처리할 수 있어야 한다 [14].

- Data Encryption Standard (DES)
- Triple DES
- Advanced Encryption Standard (AES)
- DVB-Common Scrambling Algorithm
- MediaCipher (Motorola®)
- PowerKey (Scientific Atlanta®)

그리고 송신부와 제한수신 프로세서간에 제한수신 어플리케이션을 안전하게 다운로드 받을 수 있도록 하기 위해 인증 매커니즘 및 데이터 암호화 등을 포함하는 안전한 다운로드 (Secure Download) 방식이 지원되어야 할 것이다.

향후 다운로드 가능한 제한수신 기술은 단순한 제한수신 제공에 그치지 않고 홈 네트워크와 연동하여 DRM (Digital Rights Management)의 요소기술로의 사용이 기대된다.

V. 맺음말

지금까지 최근 부각되고 있는 제한수신 기술들과 현재 시장에 소개된 제한수신 솔루션에 대해 살펴보았으며, 디지털 방송 표준인 DVB, ATSC, OpenCable 에서 제시된 제한수신 관련 내용과 표준화를 준비중인 차세대 네트워크 아키텍처 (NGNA)에서 제시하는 제한수신 요구사항에 대해 간략히 알아보았다. 그리고 제한수신 기술 및 표준의 동향이 방송과 통신 기술의 비약적인 발전에 힘입어 소프트웨어 기반의 형태로 진화하고 있음을 알 수 있었다. 소프트웨어 기반의 제한수신 기술은 방송 서비스 운영자에게 좀 더 유연한 제한수신 솔루션을 제공해 줄 뿐만 아니라 운용비용 절감이라는 측면에서 큰 매력을 가지고 있다. 하지만, 보안의 입장에서는 하드웨어 기반의 방식보다 취약한 면이 존재하며, 여기에 대한 기술 연구가 좀 더 보강될 필요가 있다.

앞에서도 언급한 바가 있지만, 디지털 컨텐츠는 그 특성상 접근, 조작, 목제, 저장, 배포가 용의하고 오류정정 기술을 통한 원본과 동일한 완벽한 품질을 유지할 수 있기 때문에, 이러한 컨텐츠에 대한 무단 접근과 복제 배포는 디지털 유료방송의 성패를 좌우할 뿐만 아니라 디지털로의 전환 노력에 대한 의미를 퇴색시키기에 충분하다. 하지만 이러한 문제를 해결할 수 있는 제한수신에 대한 국내 기술과 연구는 아직 미진하다. 이러한 시점에서 방송 선진국들의 기술 동향과 표준화 현황을 짚어봄으로써 우리의 위치를 파악하고 인식을 새롭게 해야 할 것이다.

<참 고 문 헌>

[1] EBU Project Group B/CA “Functional Model of a Conditional Access System” EBU Technical Review Winter 1995.

[2] “Software versus hardware: the great CA debate,” Cable & Satellite International, jan-feb 2004.

[3] “Smartcard-less CA: now it’s being taken seriously,” Cable & Satellite International, sept-oct

2004.
[4] “The application of virtual smart card technology to interactive TV,” CED, Aug. 2003.
[5] http://www.irdetoaccess.com
[6] http://www.widevine.com
[7] http://www.nds.com
[8] David J.Cutts.” DVB conditional access,” ELECTRONICS & COMMUNICATION ENGINEERING JOURNAL," Feb.1997
[9] ETSI TS 103 197 V1.4.1,” Digital Video Broadcasting(DVB) Head-end implementation of DVB SimulCrypt,” ETSI, Dec.2004
[10] ATSC Standard A/70A: Conditional Access System for Terrestrial Broadcast, Revision A
[11] OpenCable Specification OC-SP-MC-IF-C01-050331: OpenCable CableCARD Interface Specification
[12] OpenCable Specification OC-SP-CCCP-IF-C01-050331: OpenCable CableCARD Copy Protection System Interface Specification
[13] "NGNA: A sneak-peek at cable's battle plan for the future” CED, May. 2004.
[14] "Downloadable Conditional Access Picks Up Steam” Cable Digital News, Jun. 2005.