情 報 保 護 學 會 誌
第19卷 第5號, 2009. 10

CAS와 DRM을 중심으로 한 모바일 IPTV 보안 기술

이 선 영*

요 약

IPTV의 상용화 및 활성화에 따라 향후 언제 어디서든 IPTV 서비스를 제공받고자 하는 요구가 예상되고 있고, 이에 따라 모바일 IPTV에 대한 연구가 활발하게 진행되고 있다. 보안 기술에 있어서도 모바일 IPTV는 고정 IPTV와는 달리 소형 모바일 기기와 무선 환경을 이용하여 서비스를 제공하여야 하므로 이에 맞는 기술이 개발되어야 한다. 본 논문에서는 모바일 IPTV의 개념과 모바일 IPTV 서비스를 위한 보안 요구사항을 살펴 보고, 모바일 IPTV에서 사용되는 보안 기술을 제한수신 시스템(CAS)과 DRM으로 대표되는 서비스 보안 및 콘테츠 보안 기술을 중심으로 살펴 본다.

Ⅰ. 서 론

방송과 통신의 융합 서비스로서 주목 받고 있는 IPTV는 단방향 서비스만을 제공하는 기존의 방송과는 달리 통신의 양방향성을 방송에 결합함으로써 다양한 서비스를 제공할 수 있다[1]. 최근 IPTV의 상용화가 활발하게 진행되고 있는 가운데, IPTV에 대한 기술 연구 및 표준화 활동이 국내외적으로 활발하게 이루어지고 있는 상황이다[2][3]. IPTV 서비스가 활발하게 진행됨에 따라 이동 중에도 이동 단말기를 통하여 IPTV 서비스를 제공할 수 있는 모바일 IPTV에 대한 요구가 증가할 것으로 예상된다. 이에 따라 현재 다양한 표준화 기구에서 모바일 IPTV에 대한 기술 개발 및 표준화 활동이 진행 중에 있다[4].

IPTV와 관련된 기술개발은 QoS가 지원되는 안정된 네트워크 환경에서 충분한 화면크기와 성능을 가진 고정형 IPTV를 통하여 고화질 콘텐츠를 송수신하는 것에 중심을 두고 진행되고 있지만, 단말의 성능이 떨어지는 모바일 IPTV에서의 기술 개발은 IPTV와는 다른 환경을 고려하여 개발되어야 한다. 즉, 단말기의 성능 및 통신 대역의 차이를 극복하고 사용자 요구를 충족시킬 수 있는 기술이 개발되어야 한다. 이러한 모바일 IPTV에 대한 기술 개발 및 연구는 다양한 분야에서 이루어지고 있으나, 본 논문에서는 보안 기술을 중점적으로 다루고자 한다. IPTV에서의 보안은 사용자에게 콘텐츠를 안전하게 전달하기 위한 서비스 보호와 콘텐츠의 관리를 포함한 콘텐츠 보호가 중심을 이루고 있고, 이 목적을 위하여 제한수신 시스템(CAS)과 DRM이 사용되고 있다. 제한수신시스템과 DRM은 모바일 IPTV에서도 변함없이 사용될 것이다. 그러나, 이동성(mobility)이라는 모바일 IPTV의 특성과 소형 이동 단말기의 기능, 통신 대역의 차이 등으로 인하여 고정형 IPTV에서 사용되는 기술과는 차별화되는 부분들이 필요할 것으로 예상된다. 본 논문에서는 IPTV를 위한 보안 기술 중 모바일 IPTV 서비스를 위해 사용될 수 있는 기술로서 서비스 보안과 콘텐츠 보안 기술에 대하여 표준화된 기술을 중심으로 설명하기로 한다. 모바일 IPTV를 위한 보안 기술 요구 사항[5]에 대하여 필요한 기술들을 제한수신시스템과 DRM을 중심으로 살펴보고자 한다.

Ⅱ. 모바일 IPTV

2.1 모바일 IPTV의 정의

모바일 IPTV란 IPTV의 장점과 모바일 TV의 장점을 함께 제공할 수 있는 서비스로서, 무선 구간에서 언제 어디서나 IPTV 서비스를 이용할 수 있는 서비스를 말한다. 사용자는 다른 무선 구간으로 이동하는 경우에도 IPTV 서비스를 지속할 수 있다. 이러한 모바일 IPTV는 구현하는 방법에 따라 다음 세 가지로 분류할 수 있다[4].

* 순천향대학교 정보보호학과(sunlee@sch.ac.kr)

- 모바일 TV와 IP를 결합한 형태
- IPTV에 모바일 기능을 결합한 형태
- 이동통신에서의 모바일 IPTV 형태

2.1.1 모바일 TV와 IP를 결합한 형태

모바일 TV는 단방향 서비스를 제공하는 모바일 서비스로서 국내의 DMB와 해외의 DVB, MediaFLO 등이 있다. 이들은 IP 기술을 기반으로 개발되지 않았으나 IP를 기반으로 많은 콘텐츠와 IP의 장점을 기술적으로 수용하기 위해 IP 기술을 결합하여 확장하고 있다. 모바일 TV는 단방향 형태로 안정된 무선 방송 전송 방식을 사용하므로 서비스가 안정적이며 양방향 서비스로의 확장을 위해 리턴 채널을 결합하는 형태가 제안되었다. DVB-CBMS가 대표적인 예이며, DVB는 3GPP 기술을 주로 리턴 채널로 사용하는 양방향 IPTV를 연구하고 있다. 국내에서는 모바일 TV기술로 DMB가 널리 사용되고 있으며 수신 자격 관리 정보를 이동통신망을 통해 보내는 방법[6] 및 리턴 채널을 위한 기술로 WiBro를 접목한 양방향 형태의 모바일 IPTV기술을 개발하고 있다[7].

2.1.2 IPTV에 모바일 기능을 결합한 형태

고정형 IPTV는 IP 기반의 다양한 콘텐츠를 IP망을 통하여 사용자에게 전송하는 방식이므로 이를 모바일 IPTV로 확장하기 위해서는 사용자의 환경이 무선이어야 한다. 최근에 광대역 무선접속 기술인 WiMAX(국내에서는 WiBro)를 이용한 모바일 IPTV 기술이 개발되고 있다[7].

2.1.3 이동통신에서의 모바일 IPTV 형태

이동 통신 사업자가 중심이 되어 제공하는 이동 통신상의 멀티미디어 서비스도 초기 모바일 IPTV 서비스라고 할 수 있다. OMA BCAST(BroadCAST)는 이동 통신 영역에서 IPTV 서비스를 원활하게 제공하기 위해 연구되고 있는 가장 대표적인 표준이다.

2.2 모바일 IPTV의 보안 요구 사항

모바일 IPTV의 보안 요구사항은 서비스 보안, 콘텐츠 보안, 단말 보안, 가입자 보안 영역으로 구분할 수 있다. TTA의 표준 문서에서 이들 보안 요구 사항을 ITU-T에서 규정하고 있는 보안 요구 사항들을 수용하면서 기술하고 있다[5].

〔표 1〕 TTA의 모바일IPTV 보안요구사항

보안 분류	번호	내 용
보안 일반	REQ1	보안기술은 모바일 IPTV환경에서 효율적이어야 함.
	REQ2	전송 및 저장 과정에서 콘텐츠가 불법 유출되어서는 안됨
서비스 보안	REQ3	서비스에 대한 접근제어는 이동성을 지원해야 함.
	REQ4	접근제어 모듈은 *device mobility*를 고려한 안전한 변경 및 관리가 가능해야 함.
	REQ5	서비스에 대한 보안레벨의 변경이 가능해야 함.
	REQ6	트랜스코딩이 발생하는 중간 경로에서 서비스의 불법적인 사용/전달/삽입을 방지해야 함.
	REQ7	서비스 중간 경로에 설치된 악의적인 액세스 장치가 사용자의 서비스 자격 관련 데이터의 가로채기/변조/삭제/부정생성 등을 방지해야 함.
콘텐츠 보안	REQ8	콘텐츠 복사방지, 재분배 관리 기능은 이동성을 지원해야 함.
	REQ9	콘텐츠 특성에 따라 차별화된 *usage rule* 및 보안 기능 적용을 지원해야 함.
	REQ10	단말에 대해 불법 콘텐츠 추적이 가능해야 함.
	REQ11	트랜스코딩이 발생하는 중간 경로에서 콘텐츠의 불법적인 사용/전달/삽입을 방지해야 함.
	REQ12	서비스 중간 경로에 설치된 악의적인 액세스 장치가 사용자의 콘텐츠 및 메타데이터의 가로채기/변조/삭제/부정생성 등을 방지해야 함.
단말 보안	REQ13	사용자/단말 이동성 보장을 위한 안전한 소프트웨어 다운로드 및 관리를 지원해야 함.
가입자 보안	REQ14	서비스제공자는 이동성을 가지는 사용자에 대한 인증이 가능해야 함.

[표 1]에 나타난 모바일 IPTV의 보안 요구 사항 중에는 모바일 IPTV 구현에 있어서 중요한 이슈인 이동성(Mobility)과 트랜스코더빌리티(Transcodability)가 내포되어 있으나, 본 논문에서는 이에 대해서는 다루지 않

고, 서비스 보안과 콘텐츠 보안을 실현하는 기술을 중심으로 살펴보고자 한다.

Ⅲ. 보안 기술

본 장에서는 모바일 IPTV의 보안 요구 사항 중 사용자에게 콘텐츠를 안전하게 전달하기 위한 서비스 보안 기술과 수신된 콘텐츠의 관리를 위한 콘텐츠 보안 기술을 중심으로 살펴보고자 한다. IPTV 방송을 위한 서비스 보안 기술로 제한수신 시스템(CAS)을, 콘텐츠 보안 기술로 DRM을 중심으로 기술하기로 한다.

3.1 제한수신 시스템(Conditional Access System: CAS)

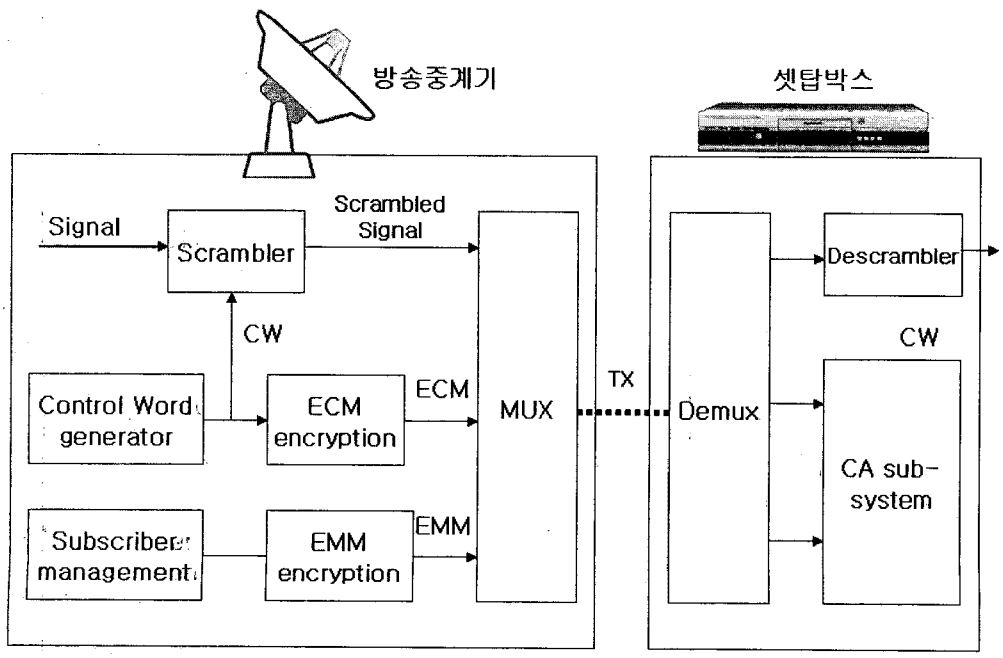
제한수신 시스템은 암호화된 방송 콘텐츠를 유선이나 위성, 인터넷을 통하여 수신자에게 보내고, 시청료를 지불한 수신자에게만 암호를 복호할 수 있는 권한을 부여함으로써 유료 서비스를 가능하게 한다. 제한수신 시스템의 주요 기능은 스크램블링/디스크램블링(srcambling/descrambling) 기능, 자격제어(Entitlement Control) 기능, 자격관리(Entitlement Management) 기능으로 나눌 수 있다[8].

3.1.1 스크램블링/디스크램블링(Scrambling /Descrambling) 기능

수신 자격이 없는 수신자는 시청이 불가능하도록 콘텐츠를 암호화하여 보내며, 제어단어(Control Word: CW)를 이용하여 암호화된 방송 콘텐츠를 암호화 및 복호하게 된다. 스크램블링된 신호와 암호화된 CW가 전송되고, 복호된 CW를 이용하여 디스크램블링을 수행한다. CW를 복호하기 위해 송신부와 수신부는 같은 비밀키를 가지고 있어야만 한다. 비밀키 전송 과정의 보안성 향상을 위해 방송 사업자는 스마트카드 형태로 비밀키를 제공한다.

3.1.2 자격제어(Entitlement Control) 기능

CW를 인증키로 암호화하여 ECM (Entitlement Control Message)에 실어 수신자에게 전송한다. CW는 주기적으로 전송되며, 그 때마다 새로운 CW가 생성되고 암호화되어 전달된다. ECM에는 암호화된 CW외에 제어 변수(Control parameter)가 포함되며, 모든 수신기



〔그림 1〕 CAS의 시스템 모델

는 수신된 제어 변수와 수신기의 인증 변수(authentication parameter)를 비교하여 정당한 사용자로 판단될 경우에만 스마트 카드 내의 비밀키를 이용하여 CW를 복호하고, 수신된 콘텐츠를 디스크램블링 한다.

3.1.3 자격관리(Entitlement Management) 기능

수신기에 자격을 부여/갱신/관리 하는 기능으로, 인증키를 분배키로 암호화하여 EMM(Entitlement Management Message)을 생성하고 암호화하여 수신측으로 전송한다. EMM은 수신기의 보안 장치인 스마트 카드에 자격을 부여하거나 갱신하는 기능을 한다. 송신부에서는 가입 신청을 한 정당한 수신자에게 해당 프로그램의 인증키와 수신 자격을 전송한다. 인증키는 수신자 고유의 비밀키를 이용하여 암호화한 다음 인증 변수와 함께 EMM을 생성한 후 메시지의 변조 방지를 위해 전자 서명을 추가하여 전송한다.

제한수신 시스템의 시스템 모델은 [그림 1]과 같다. 제한수신 기술을 사용하기 위해서는 디지털 방송 표준인 DVB(Digital Video Broadcasting), ATSC (Advanced Television System Committee), OpenCable에서 정한 인터페이스 및 콘텐츠 보호 규격을 만족해야 한다. 각 방송 규격에서 요구하는 제한수신 시스템에 대하여 간략하게 살펴보도록 한다.

3.1.3.1 DVB 제한수신 시스템

DVB는 세부적인 수신 제한 기능보다는 전체적인 시스템에서 사업자 간의 동등한 접근을 보장하는 것을 목적으로 하고 있다. 이를 위해 DVB에서는 MultiCrypt와 SimulCrypt 기술을 개발하였다[9]. MultiCrypt는 하나의 수신기에서 하나 이상의 제한수신 프로그램을 수용하도록 규정한다. SimulCrypt는 서로 다른 업체에서 하나의 공통 암호 알고리즘을 사용하여 스크램블링 하되, 접근제어와 관련된 자격 관리 메시지(EMM)와 자격 제어 메시지(ECM)는 제한수신 시스템별로 각자의 방법으로 생성하여 전송하는 시스템이다.

MultiCrypt와 SimulCrypt는 하나의 방송 채널에 대해서 다수의 보안 업체가 동시에 서비스를 제공하기 위한 기술을 정의하고 있으며, 여러 제한수신 모듈 공급자를 수용하기 위하여 가입자의 수신기에서 디스크램블링과 암호화 기능을 분리하였다. 디스크램블링 방식은 DVB-CSA (Common Scrambling Algorithm)라는 기술을 사용하도록 하고 있다.

3.1.3.2 ATSC 제한수신 시스템

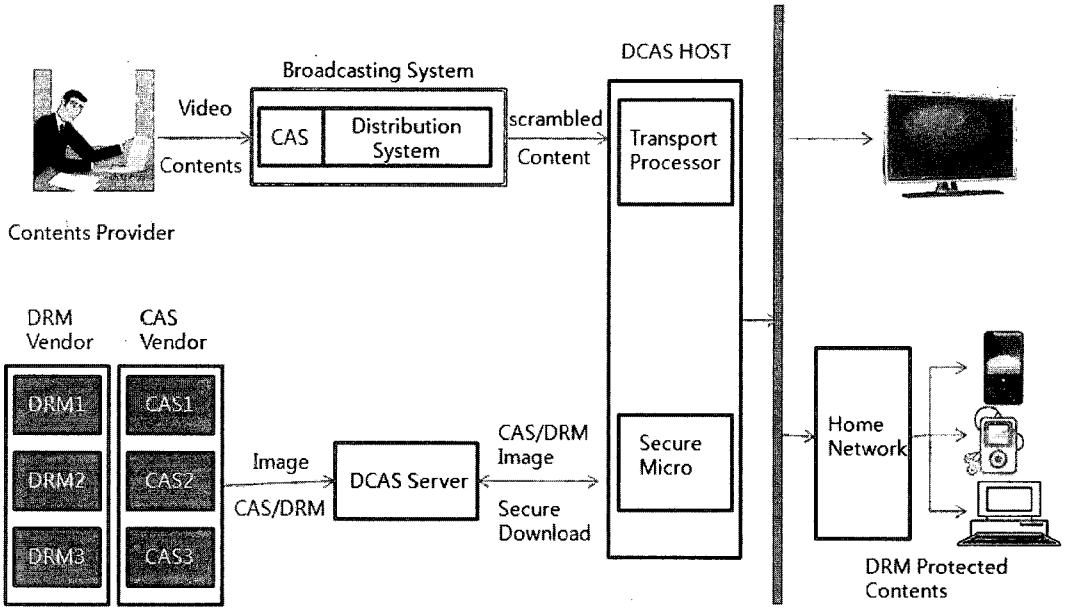
ATSC에서는 하나의 프로그램에 여러 개의 제한수신 모듈이 동시에 적용될 수 있는 있는 SimulCrypt방식을 채택하고 있다, 콘텐츠를 암호화하는데 사용되는 스크램블링 알고리즘은 168비트의 키를 가진 CBC(Cipher Block Chaining) 모드의 Triple-DES가 규격화 되어 있다. 수신부에서 사용되는 보안 인터페이스 모듈에 대한 규격은 스마트카드 타입의 NRSS(National Renewable Security Standard)-A, PCMCIA 타입의 NRSS-B 두 가지가 허용되고 있다. 수신기와 보안 모듈간의 통신 규정은 없지만 NRSS 사용을 의무화하고 있다[10].

3.1.3.3 OpenCable 제한수신 시스템

OpenCable의 제한수신 시스템은 송신부의 시스템과 수신부의 호스와 분리된 POD(Point Of Deployment)로 구성되어 있다. 기존의 디지털 방송 수신 장치 시스템에서는 암호화된 콘텐츠를 수신하여 복원하는 기능이 수신기에 내장되어 있었으나 POD에서는 수신기로부터 분리한 별도의 보안 모듈로 정의하고 있다. OpenCable에서는 DVB나 ATSC와 같이 특정 암호 알고리즘을 표준으로 규정하지 않고, 수신기와 보안 모듈 간의 인터페이스만을 규정하고 있다[11].

3.1.3.4 다운로드형 제한수신 시스템

기존의 유료 방송 시스템에서는 단말기와 수신 제어 기능이 독립적으로 동작하지 않는 경우가 대부분이다. 다양한 형태의 제한수신이 가능하고 콘텐츠의 제공자마다 서로 다른 제한수신 기술이 동작할 수 있도록 하기 위해서는 특정 제한수신 기술에 종속되지 않고 동적으로 재구성이 가능한 구조가 필요하다. 이를 위하여 다운로드형 제한수신 시스템(Downloadable CAS; DCAS)이 제안되었다[12][13][14]. 소프트웨어 기반의 DCAS는 상대적으로 낮은 셋탑박스 가격과 높은 개방형 구조로 인해 DRM등의 추가적인 보안 모듈을 쉽게 적용할 수 있으며, SimulCrypt의 구현이 용이하다. 또한 보안 침해 사고가 발생하였을 때, 새로운 제한수신 시스템을 소프트웨어 다운로드함으로써 침해에 대해 빠르고 효율적으



〔그림 2〕 DCAS 시스템 구성도[13]

로 대응할 수 있다.

DCAS는 셋탑 박스에 제한수신 모듈(CAS)이 미리 설치되어 있는 것이 아니라 방송수신을 제어하는 기능을 다운로드 가능한 형태로 구현하는 것을 말한다. DCAS는 SM(Secure Micro)이라는 전용 칩을 사용하는데, 이 칩은 CAS, DRM, ASD(Authorized Service Domain) 클라이언트를 다운로드 받을 수 있도록 설계하였다. 암호화하는 기능은 TP(Transport Processor)에서 담당하고, CAS 클라이언트에서 전송하는 CW를 통해 실시간 복호하게 된다. [그림 2]는 DCAS 구성도이다.

DCAS 시스템은 크게 DCAS 서버, DCAS 호스트, TA(Trusted Authority)로 구성된다. DCAS 서버는 DCAS를 수행하기 위한 정책, 이미지 정보, 배포하는 기능을 하고, DCAS 호스트는 DCAS 서비스를 지원하는 단말로 방송 신호 및 데이터 신호를 수신하는 기능을 가지며 SM, TP 구조를 갖는다. TP는 암호화 모듈/디스크램블링 모듈이고, SM은 DCAS 호스트에 내장되는 보안 칩으로서 DCAS 서버, TP와 통신하여 콘텐츠 보호 서비스를 제공한다. TA 시스템은 DCAS 호스트를 위한 SM, TP의 인증서를 발행하고, 기타 인증과 관련된 정보를 전달하는 역할을 수행한다.

DCAS 호스트에서 SM은 보안상 중요한 역할을 한다. 이 SM에는 여러 가지 특허 기술이 사용되고 있으므로 시스템의 비용 등을 생각하면 . SM과 같은 전용칩을 사용하지 않고 모든 것을 소프트웨어로 구현하는 것이 바람직하다. 특히, 소프트웨어로만 구현된 제한수신 시스템은 모바일 기기 및 모바일 환경에 적합할 것으로 생각되어 많은 연구가 진행되고 있다.

3.2 DRM

제한수신 시스템은 인가된 사용자가 암호화된 콘텐츠를 복호하여 원본 콘텐츠를 획득한 후의 사용에 대해서는 관여하지 않으므로 사용자가 획득한 콘텐츠를 불법 복제 및 불법 유통할 경우에는 콘텐츠에 대한 지속적인 보호가 이루어지지 않는다. 따라서, 통신과 방송의 특성을 함께 가지는 IPTV에서는 제한수신 시스템만으로는 콘텐츠를 보호할 수 없고 DRM을 병용하여야 한다.

DRM이란 디지털 콘텐츠의 생산, 분배, 거래규칙, 과금, 거래내역의 관리, 정산 등 디지털 콘텐츠의 전체 라이프 사이클에 걸쳐 투명성과 신뢰성을 보장하는 유통체계 전반을 통칭하는 서비스를 말한다. DRM 시스템은 DRM 패키저와 클리어링 하우스, DRM 클라이언트로 구성된다. DRM 패키저는DRM을 적용한 콘텐츠를 만들고 공급하고, 클리어링 하우스는 라이선스를 발급하고 관리한다. DRM 클라이언트는 라이선스에 따라

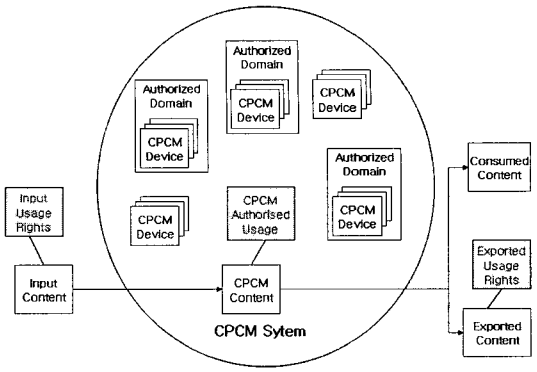
사용을 통제하는 역할을 한다. DRM은 사용자에게 부여된 권한에 따라 디지털 콘텐츠의 사용 권한을 지속적으로 통제하는 방식이다. 이 방식은 콘텐츠의 생명 주기 전체에 걸쳐 원본 추출이 보장되기 때문에 현재 네트워크를 통해 유통되는 많은 디지털 콘텐츠들이 이 기술을 이용하고 있다. 최근의 DRM 기술은 저작권 보호 기술 및 암호 알고리즘을 이용한 콘텐츠의 배포 관리, 워터마킹 기술을 이용한 콘텐츠 관리 기술까지 포함하여 다루고 있다. 이러한 기술을 채용한 DRM은 네트워크 환경에서 영상, 음악, 게임 등의 디지털 콘텐츠를 보호하기 위해 개발된 기술로서 미리 DRM을 적용한 후 콘텐츠를 유통해야 하기 때문에 실시간으로 콘텐츠가 제공되는 방송 서비스에는 적합하지 않은 부분이 있다. 따라서, 방송된 이후의 콘텐츠를 보호하기 위해 DRM이 필요함에도 불구하고 방송 서비스에서 활용되지 못하였다. 그러나 주문형 방송과 실시간 방송을 제공하는 IPTV 서비스에서는 DRM도 이용가능하다. 현재 IPTV 서비스는 주문형 방송과 실시간 방송으로 구분되며 주문주문형 방송은 DRM 기술을 중심으로 발전하여 왔고, 실시간 방송은 제한수신 기술을 중심으로 발전하여 왔다. 최근의 연구는 DRM 기반의 실시간 방송 수신처리 기능이나 반대로 CAS 기반의 DRM 연구도 진행되고 있다. 또 3.1.4절의 DCAS를 사용할 경우에는 DRM 모듈을 다운로드하여 사용할 수 있다.

IPTV 서비스를 위한 DRM으로서 DVB의 CPCM이 대표적이고, 제한수신 시스템과 함께 DRM을 이용하는 ATIS IIF가 있다. 이 기술들은 모바일 IPTV에서도 사용될 것이다.

3.2.1 DVB CPCM

CPCM(Content Protection & Copy Management) 시스템은 불법복제를 방지하기 위한 방법이 아니라 사용자가 콘텐츠를 복사하여 어떻게 사용하는지를 제어하며[15], 상업적인 콘텐츠의 보호와 관리를 위하여 상호호환적 플랫폼을 제공한다. DVB는 댁내로 전달되는 네트워크와 홈 내에서 소비되는 네트워크를 분리하여 정리하고 있다. 사용자가 획득한 콘텐츠는 브로드캐스트, 케이블, 위성, 인터넷 등 다양한 방법으로 인가된 도메인 내의 각 장치에 전송되어 사용될 수 있다. [그림 3]은 CPCM 시스템의 개념을 나타내고 있다.

입력 콘텐츠가 CPCM 시스템에 입력되면 CPCM 디



〔그림 3〕 CPCM의 개념도

바이스에 의해 구현되는 AP(Aquistion Point)에서 CPCM 콘텐츠로 된다. CPCM 콘텐츠는 저장, 처리될 수 있으며, 사용자에 의해 사용되거나 다른 시스템으로 수출되어 CPCM 시스템을 떠날 수 있다. DVB에서는 기존의 방송 서비스 영역과 별도로 홈 안에서 유통되는 모델을 정의하고 있다. 홈 내에서는 모든 콘텐츠를 CPCM 콘텐츠로 변환하여 유통하고 외부로 전송하는 경우에만 다시 변환하는 절차를 거치게 된다. CPCM 시스템의 구성 요소는 다음과 같다.

(1) CPCM Device: CPCM 함수를 수행하는 장치
(2) CPCM Authorised Domain: 한 가정내에 속하는 모든 CPCM 디바이스의 국소적 그룹
(3) CPCM Content Usage Rules: 콘텐츠 서비스 제공자에 의해 정해짐
(4) CPCM Content: CPCM 시스템에 의해 관리되는 콘텐츠

DVB CPCM을 준수하는 장치에서는 복사본의 수를 제한하지 않은 상태에서 인터넷 무단 재배포는 허용하지 않는다. 그러나, 사용자의 사적 이용을 보장하기 위해 홈 내의 기기 및 모바일 기기 등 사용자의 여러 단말에서의 방송 프로그램의 이용을 지원한다.

3.2.2 ATIS IIF

ATIS IIF는 IPTV 서비스의 상호 호환성을 확보하기 위해서 북미 통신 사업자 연합이 설립한 기구로서, 보안 기술의 상호 호환성을 확보하기 위하여 IDSA를 제시하고 있다[16]. IDSA는 실시간 방송에서는 제한수신 기술

을 이용하고, 주문형 방송에서는 DRM 기술을 이용하는 방식이다.

Ⅳ. 결 론

IPTV의 기술 개발과 표준화가 빠른 속도로 진행되고 있는 가운데, 언제 어디서든 방송 서비스를 제공받을 수 있는 모바일 IPTV의 수요가 예상되고 있다. 모바일 IPTV의 실제 구현에서 중요한 이슈가 되는 것은 이동성(mobility)과 트랜스코더빌리티(Transcodability)이다. 이동성은 서비스를 받고 있는 도중 다른 지역으로 이동되더라도 서비스가 지속되어야 하는 것이고, 트랜스코더빌리티는 사용하는 디바이스의 능력에 따라 화면의 질, 전송속도, 보안 레벨 등이 변경 가능한 특성이다. 이 두 가지 특성이 만족되어야만 완전한 모바일 IPTV 서비스가 제공될 것으로 예상된다. ITU-T 및 TTA의 모바일 IPTV 보안 요구사항에도 두 가지 특성이 모두 포함되어 있다. 그러나, 본 논문에서는 이 특성들에 대해서는 다루지 않고, 서비스 보안 및 콘텐츠 보안 기술 자체에 대해서만 기술하였다.

서비스 보안은 사용자에게 콘텐츠를 안전하게 전달하기 위한 보안 기술을 의미하고, 콘텐츠 보안 기술은 안전하게 수신된 콘텐츠의 사용, 복제 및 배포 등 콘텐츠의 관리를 위한 보안 기술을 의미한다. 서비스 보안 기술로서 IPTV에서 사용하기 위해 표준화되고 있는 여러 표준 기구의 제한수신 시스템을 설명하였다. 이들 제한수신 시스템이 그대로 모바일 IPTV에 적용될 수 있으나, 대역폭에 제한이 있는 모바일 환경과 고정 IPTV에 비해 성능이 낮은 디바이스의 기능을 생각하면 다운로드형 제한수신 시스템(DCAS)이 적합할 것으로 생각된다. 다운로드형 제한수신 시스템에 대해서는 현재 많은 연구가 진행되고 있다. 콘텐츠 보안 기술로서 다양한 DRM 기술이 개발되어 있으나, 특히 방송에 맞도록 표준화되고 있는 DRM 기술로서 DVB CPCM과 ATIS IIF를 소개하였다. 주문형 방송과 실시간 방송이라는 방송 형태에 따라 제한수신 시스템과 DRM을 병행하여 사용하는 ATIS IIF에서 제시한 IDSA는 매우 유용한 기술이다. IPTV에서 제한수신 기술과 DRM기술은 상호 보완적으로 사용되므로, 향후에도 이 두가지 기술을 이용하는 방법에 대한 연구가 계속되어야 할 것이다. 또한, 모바일 IPTV의 활성화를 위해 본 논문에서 소개한 기술들을 바탕으로 한 많은 새로운 기술들이 연구 개발되어야 할 것이다.

참고문헌

[1] 윤장우, 이현우, 류 원, 김봉태, "IPTV 서비스 및 기술 진화 방향", 한국통신학회지(정보와 통신) 제25권 제8호, pp. 3-11, 2008년 7월.

[2] 최락권, "IPTV 서비스 구현을 위한 핵심 기술 연구", 대한전자공학회지, 제35권 제3호, pp. 29-43, 2008년 3월.

[3] 박종봉, "IPTV 서비스, 국내외 현황과 향후 발전 모습", TTA Journal, No. 122, pp. 62-67, 2009년 4월.

[4] 박수홍, "Mobile IPTV 기술 및 국내외 표준화 동향", HN Focus, Vol. 20, pp. 48-54.

[5] TTA, "Non-NGN 기반 Mobile IPTV 요구사항", TTAK. KO-08.0021, 2009년 6월.

[6] 최영주, "위성 DMB CAS 소개 및 현황", 방송공학회지, 제 13권 제 4호, pp. 44-53, 2008년 12월.

[7] 이진호, "Mobile IPTV를 위한 DCAS 기술", 모바일 IPTV 보안 심층 세미나, pp. 141-158, 2009년 6월.

[8] EBU, Functional Model of Conditional Access system, EBU Project Group B/CA, October, 1995.

[9] ETSI, DVB Head-end Implementation of DVB Simulcrypt, ETSI TS 103 197 V1.4.1, December, 2004.

[10] ATSC, ATSC Standard: Conditional Access System for Terrestrial Broadcast, Revision A, with Amendment No.1, Doc. A/70A, July, 2004.

[11] CableLabs, CableCARD Copy Protection system. Interface Specification, OC-SP-CCCP-IF-C01-050331, March, 2005.

[12] 박종열, 문진영, 박민호, 백의현, "실시간 IPTV 서비스를 위한 수신 제한 기술", 한국통신학회, 제24권, 제2호, pp. 13-24, 2007.

[13] 김영모, 고병수, "다운로드형 제한수신시스템 기술 동향", 한국방송공학회지, 제13권 제 4호, pp. 54-64, 2008년 12월.

[14] 정영호, 정준영, 구한승, 조용성, 유응식, 권오형,

"다운로더블 제한수신 시스템 기술", 전자공학회지, 제35권 제 9호, pp. 975-984, 2008년 9월.

[15] DVB, Digital Video Broadcasting (DVB); Content Protection & Copy Management, DVB Document A094, November 2005.

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

〈著者紹介〉

이 선 영 (Sun-Young Lee)

종신회원

1993년: 부경대학교 전자계산학과 이학사

1995년: 부경대학교 전자계산학과 이학석사

2001년: 일본 동경대학교 전자정보공학과 공학박사

2004년~현재: 순천향대학교 정보보호학과 교수

<관심분야> 암호이론, 정보이론, 콘텐츠 보안, 정보보호