지상파 UHDTV 콘텐츠 보호 기술 표준화 현황

오성흔 (주)디지캡 기술연구소 소장

1. 머리말

ATSC 3.0 표준 기반의 국내 지상파 UHDTV 방송 송수신 정합 표준[1]은 MPEG-2 TS(Transport Stream) 기반이 아닌 IP 기반 전송 시스템으로 방송망과 통신망 결합을 통해 HEVC 기반의 고품질 영상, 실감형 오디오, HTML5 기술 기반의 새로운 런타임 환경, 동적 하이브리드 서비스, 컴패니언 스크린 등 다양한 차세대 방송 서비스를 제공할 수 있는 표준이다. 이 표준은 지상파 방송사에 새로운 기회일 뿐만 아니라 시청자에게도 지금까지 경험하지 못한 보다 새롭고, 풍부한 지상파 방송 서비스 경험을 제공하게 될 것이다.

지상파 UHDTV 서비스를 통해 시청자에게 보다 높은 품질의 영상 콘텐츠 및 서비스를 제공할 수 있는 기회가 생긴 반면 지상파 UHDTV 방송 콘텐츠의 불법 복제물 유통 가능성으로 인해 지상파 방송사의 손실도 더욱 커질 것으로 예상된다. 한국저작권단체연합회에서 발간한 '2016 저작권 보호 연차보고서'[2]에 따르면 불법 복제물 유통에 따른 2015년 합법 저작물 시장 침해 규모 중 방송 콘텐츠가 약 3,073억 원(2014년은 2,066억 원)으로 조사 되었다. 웹 하드를 통한 불법 복제물 유통은 불법 콘텐츠 필터링 기술 적용을 통해 많이 줄어들었으나 최근에는 토렌트 및 모바일 환경, 해외 클라우드 시스템을 통한 불법 복제물 유통이 온라인/오프라인에서 많이 이루어지고 있는 상황이다. 이러한 지상파 UHDTV 방송 콘텐츠의 불법 복제물 유통을 방지하기 위해 국내 지상파 UHDTV 방송 송수신 정합 표준에서는 지상파 UHDTV 방송 콘텐츠 보호를 위한 표준 기술이 포함되어 있다.

본고에서는 국내 지상파 UHDTV 방송 콘텐츠 보호를 위한 표준 기술에 대해 소개한다.

2. 콘텐츠 보호 요구사항

지상파 방송사에서 제공하는 UHDTV 방송 콘텐츠를 합당한 시청 요건을 갖춘 수신 단말기에서만 정상적인 서비스가 되도록 하기 위한 시스템 요구사항으로 ①콘텐츠 스크램블링, ②콘텐츠 보호 관리, ③콘텐츠 사용 제어, ④포렌식 워터마크 삽입 항목으로 구분하고 있다. 각 세부적인 요구사항에 대해서는 표준 문서[1]를 참고하기 바라며, 본고에서

는 각 시스템 요구사항의 이해를 돕기 위해 추가 설명한다.

콘텐츠 스크램블링

- 지상파 UHDTV 방송 콘텐츠의 불법 복제물 유통을 막기 위한 가장 효과적이고 강력한 수단 중 하나는 방송 송출 시 암호화(스크램블링)를 적용하는 것이므로 이를 위해 표준화된 암호화 방식의 표준을 정의하되, 특정 콘텐츠 보호 관리 시스템에 종속적이지 않은 공통된 방식의 암호화 방식 표준화를 해야 한다.

콘텐츠 보호 관리

- 각 방송사는 콘텐츠 보호 관리 시스템(보호된 방송 콘텐츠를 합당한 시청 요건을 갖춘 수신기만 정상적으로 접근할 수 있도록키 관리 등의 접근 제어 메커니즘을 제공하는 시스템)을 도입할수 있어야 하며 방송사는 하나 이상의 콘텐츠 보호 관리 시스템을 동시에 운영할 수 있다.
- 각 방송사가 운영하는 콘텐츠 보호 관리 시스템을 여러 가지 이유로 인해 변경해야 할 경우를 대비하여 방송 서비스 운영 중에도 콘텐츠 보호 관리 시스템을 변경할 수 있는 다운로드 플랫폼을 제공해야 한다. 다운로드 플랫폼은 수신기에 설치되는 콘텐츠보호 관리 시스템의 클라이언트 소프트웨어를 송신 측에서 수신기로 안전하게 다운로드하고 수신기에서 설치, 운영할 수 있는 기술이다.
- 콘텐츠 보호 관리 시스템 변경 시 송신 측에서 신규 콘텐츠 보호 관리 시스템을 손쉽게 추가 운영할 수 있도록 특정 벤더에 종속적이지 않은 송신 측 장비 간 연동 인터페이스 표준이 필요하다.

콘텐츠 사용 제어

- 수신기에서의 방송 콘텐츠 녹화/재생/이동/복사를 허용하기 위한 이용 제어 정보가 방송 콘텐츠와 함께 시그널링으로 제공되어야 한다. 이는 방송 수신기뿐만 아니라 2차 단말기로의 이동/복사 시에도 제어가 되어야 한다.

포렌식 워터마크

- HDMI(High Definition Multimedia Interface)와 같은 디지털 외부 출력이 있는 경우 HDCP(High-bandwidth Digital Copy Protection) 2.2 이상이 지원되어야 한다. 이는 송출 시스템과 수신기 사이의 스크램블링을 통한 보호, 수신기 내에서의 각종 보호 장치를 적용하더라도 디지털 외부 출력 시 보호되지 않은 상태로 출력되는 것을 방지하기 위한 요구사항이다.
- 암호화 기술을 기반으로 하는 공격적인 접근 방식의 보호 기술을 적용함에도 불구하고 불법 복제물이 유통될 가능성을 대비하여 디지털 외부 출력 시 포렌식 워터마크를 삽입해야 한다. 불법 복제물 유통 시 포렌식 워터마크를 통해 불법 배포의 원천 소스를 추적할 수 있다.

3. 콘텐츠 보호 표준 기술

지상파 UHDTV 방송 콘텐츠 보호 표준은 크게 ①공통 암호화 방식, ②암호화 및 콘텐츠 보호 시스템 시그널링, ③콘텐츠 관리 정보(Content Management Information), ④송신 측에서의 구성 시스템 간 연동 인터페이스, ⑤다운로드 플랫폼, ⑥포렌식 워터마킹으로 구성되어 있다.

3.1 공통 암호화 방식

지상파 UHDTV 방송 송수신 정합 표준에서는 방송 콘텐츠 전송 컨테이너 포맷으로, MMT(MPEG Media Transport) 프로토콜은 ISOBMFF(ISO Base Media File Format) 기반 MPU(Media Processing Unit)를, ROUTE(Real-time Object Delivery over Unidirectional Transport) 프로토콜은 ISOBMFF 기반 DASH(Dynamic Adaptive Streaming over HTTP) 세그먼트를 사용한다[1]. 본 표준에서는 ISOBMFF 기반의 방송 콘텐츠 전송 컨테이너를 암호화하기 위한 방식으로 MPEG CENC(Common Encryption) 표준[3]을 기반으로 한다.

MPEG CENC 표준[3]은 ISOBMFF에 대한 구체적인 암호화 방식(Encryption Method), 키 맵핑 방식, 암호화 메타데이터를 정의한 표준이다. 이 표준은 기존 MPEG-2 TS 시스템 환경에서의 DVB Common Scrambling Algorithm과 유사하게 ISOBMFF 보호에 대한 공통 암호화 기술로 볼 수 있다. 이 표준을 이용하여 콘텐츠를 공통 암호화하면 서로 다른 콘텐츠 보호 관리 기술(예를 들어 CAS(Conditional Access System) 또는 DRM(Digital Rights Management))은 암호화 기능보다는 복호화 키 관리(복호화 키의 안전한 전달/저장, 접근/사용 제어 방식 등) 기능에만 초점을 맞출 수 있다. 그리고 공통 암호화 방식이기 때문에 서로 다른 콘텐츠 보호 관리 기술이 MPEG CENC로 보호

된 하나의 동일한 ISOBMFF 파일에 대한 암/복호화가 가능해진다.

MPEG CENC 표준은 AES(Advanced Encryption Standard) 128 bits 암호화 알고리즘을 이용하여 ISOBMFF 파일에 있는 각 샘플들을 암호화한다. 이때 사용하는 암호화 알고리즘 식별자, 각 샘플들의 암호화 여부 및 암호화된 부분에 대한 위치 정보, 복호화 키 식별자, 초기화 벡터(Initialization Vector) 값이 ISOBMFF 파일에 같이 포함된다. 그리고 각 콘텐츠 보호 관리 기술의 데이터(예를 들어 CAS 기술의 경우 ECM(Entitlement Control Message) 또는 EMM(Entitlement Management Message)을, DRM 기술인 경우 라이선스 자체 또는 라이선스 발급 정보)를 Protection System Specific Header box('pssh')로 구성하여 ISOBMFF 파일에 추가할 수 있다. 각 'pssh'에는 콘텐츠 보호 관리 시스템의 식별자와 해당 시스템의 데이터가 포함되며 ISOBMFF 파일에는 하나 이상의 콘텐츠 보호 관리 시스템의 'pssh'가 포함될 수 있다.

콘텐츠 보호 표준에서는 MPEG CENC 표준을 도입함에 있어 다음과 같은 몇 가지 규칙에 대해 기술하고 있다.

- 'cenc' Protection Scheme(AES 128 bits Counter Mode) 이용할 것을 권고
- DASH의 경우, 같은 Adaptation Set 내 모든 Representation은 같은 암호화 키와 권한으로 보호할 것을 권고
- 트랙 내 모든 샘플은 동일한 암호화 키를 이용하여 암호화하도록 권고
- 암호화 키를 주기적으로 변경하도록 Key Rotation 적용 권고

3.2 암호화 및 콘텐츠 보호 시스템 시그널링

콘텐츠 보호 시그널링은 ①3.2절에서 설명한 MPEG CENC 암호화 시그널링과 ②콘텐츠 보호 관리 시스템과 3.6절에서 설명할 다운로드 플랫폼 시스템의 데이터 전달 프로토콜 및 전달 위치에 대한 시그널링으로 구성된다. 본 절에서는 후자에 대해서만 설명한다.

우선 콘텐츠 보호 관리 시스템과 다운로드 플랫폼 시스템을 유일하게 식별하기 위한 식별자 체계는 MPEG CENC 표준에서의 System ID 체계에 따라 16bytes 크기의 UUID(Universally Unique Identifier) 체계를 이용한다. 기존 DVB 계열의 2bytes CA_System_ID 체계와 다른 점이다.

각 콘텐츠 보호 관리 시스템의 데이터 중 콘텐츠 복호화를 위한 제어 정보가 포함되어 있는 데이터(예를 들어 CAS의 경우 ECM, DRM의 경우 라이선스 발급 정보 등)는 3.2절에서 설명한 바와 같이 암호화된 ISOBMFF 파일 내 Protection System Specific Header Box ('pssh')에 포함되어 전달한다. 수신기에서는 암호화된 ISOBMFF 파일을 수신한 후 암호화가 되어 있는 경우 복호화 키를 얻기 위해 수신기에 설치되어 있는 콘텐츠 보호 관리 시스템 클라이언트에 해당하는 'pssh'를 전달한다. 콘텐츠 보호 관리 시스템 클라이언트는 합당한 시청 요건 확인 및 추출한 복호화 키를 CENC 복호화 기능으로 전달하여 최종적으로 암호화 ISOBMFF 파일을 복호화한다.

각 콘텐츠 보호 관리 시스템의 EMM/라이선스 데이터는 ROUTE 프로토콜과 MMT 프로토콜을 통해 방송망으로 전달할 수 있다. ROUTE 프로토콜로 전송하는 경우는 각 콘텐츠 보호 관리 시스템별로 ROUTE LCT(Layered Coding Transport) 채널을 할당하여 데이터를 전달하고, MMT 프로토콜로 전송하는 경우는 MPEG MMT 2nd 규격에서 정의한 라이선스 시그널링 메시지 LS_messsage()를 통해 전달한다. 그리고 이 데이터들이 전달되는 위치에 대한 시그널링 정보는 CPT(Content Protection Table)이라는 XML 문서를 통해 정의하고 있으며 이 CPT는 저수준 시그널링(Low Level Signaling)

<표 1> 배포 제어 정보 구성

정보 항목		설 명
Redistribution Control Code		제한적 배포, 자유로운 배포
Redistribution Condition		제한적 배포의 경우
	Holdback Time	배포 허용 시점: 1일, 2일, 1주일, 4주일, 또는 제한 없음
	Allowed Max Resolution	배포 허용 최대 해상도: SD(720x480), FHD(1920x1080), 또는 제한 없음
	Allowed Copy	최대 허용 복사 회수: 복사 불가, 9회, 제한 없음
Redistribution Area		한국 또는 제한 없음
Signature		CMI 정보 무결성을 위한 Signature

을 통해 전달한다.

3.3 콘텐츠 관리 정보

콘텐츠 관리 정보는 수신기에서 방송 콘텐츠 녹화/재생/이동/복사를 허용하기 위한 배포 제어(Redistribution Control) 정보이다. 콘텐츠 관리 정보는 콘텐츠 보호 관리 시스템을 통해 전달하는 경우에는 이진 형식(Binary Format)으로, ATSC 3.0에서 정의한 서비스 시그널링 또는 서비스 어나운스먼트(Service Announcement) 서비스를 통해서 전달된 경우에는 XML 형식으로 표현된다. 정의된 배포 제어 정보는 〈표 1〉과 같다.

배포 제어 정보는 서비스 수준, 콘텐츠 수준에서 지정할 수 있다. 서비스 수준에서 지정하는 경우 이 정보는 서비스 수준 시그널링(Service Layer Signaling)의 User Service Bundle Description에서 〈ContentManagementInfo〉 요소로 정의되고, 콘텐츠 수준에서 지정하는 경우 서비스 어나운스먼트의 콘텐츠 프래그먼트(Content Fragment)에서 〈ContentManagementInfo〉 요소로 정의된다.

3.4 구성 시스템 간 연동 인터페이스

콘텐츠 보호 시스템 요구사항에서 언급한 바와 같이 지상파 방송사는 하나 이상의 콘텐츠 보호 관리 시스템을 동시에 운영할 수 있어야 하며 필요 시 콘텐츠 보호 관리 시스템을 운영 중에라도 변경할 수 있어야 한다. 송신 측 헤드엔드(Head-end) 시스템에서 콘텐츠 보호 시스템과 CENC 스크램블러 시스템 간 인터페이스 또는 기술 종속성이 있다면 변경이 매우 어렵기 때문에 이를 위해 구성 시스템 간 연동 인터페이스를 표준화하였다. 연동 인터페이스 표준은 DVB SimulCrypt 표준[4] 기술을 기반하여 MPEG CENC를 지원하도록 규격 확장하였다. 참고로, DVB SimulCrypt 표준은 하나의 방송 시스템에서 하나 이상의 콘텐츠 보호 관리 시스템이 동시에 운영될 수 있도록 헤드엔드 시스템 컴포넌트 간의 연동 인터페이스 및 동기화 방식을 정의한 것이다.

본 표준에서 확장한 주요 내용은 다음과 같다.

- CENC Protection System UUID(16 bytes) 체계 지원을 위한 신규 파라미터 정의
- ECMG(ECM Generator) SCS 인터페이스에서 AES 128 bits 키 크기와 UUID 체계의 키 식별자를 위한 CP_CW_Combination 파라미터의 구체적 정의
- Protection System Specific Header ('pssh') 데이터의 다양한 시그널링 위치를 지원하기 위한 파라미터 확장
- 추가/확장된 상기 파라미터를 활용하는 관련 시스템 컴포넌트 간 채널/스트림 전용 메시지(Channel/Stream specific Message) 확장

3.5 다운로드 플랫폼

콘텐츠 보호 시스템 요구사항에서 언급한 바와

같이 지상파 방송사는 운영 중에라도 콘텐츠 보호 관리 시스템을 교체할 수 있도록 하기 위해 본 표준에서는 다운로드 플랫폼(Download Platform) 기술을 정의하였다. 다운로드 플랫폼은 지상파 UHDTV 방송 콘텐츠 보호를 위해 운영 중인 콘텐츠 보호 관리 시스템에 대한 버전 관리를 수행하며 필요한 경우 수신기에 설치되어 있는 콘텐츠 보호 관리 시스템의 클라이언트 업데이트 또는 신규 설치를 수행한다. 본 표준은 콘텐츠 보호 관리 시스템의 클라이언트 교체뿐만 아니라 수신기에서 다운로드 플랫폼을 구현하는 DP(Download Platform) 매니저 자체도 교체할 수 있도록 되어 있다.

다운로드 플랫폼 표준은 TTA 'IPTV용 교환 가능한 CAS(iCAS)' 표준[5]을 기반으로 하고 있다. iCAS 표준은 기본적으로 양방향을 기반으로 하고 있기 때문에 단방향 속성의 방송망 환경을 지원하기 위해 DP Message 정의, 방송망을 통한 DP 시스템 데이터 전달 방식에 대해 표준 확장이 이루어졌다.

DP Message는 현재 운영하고 있는 콘텐츠 보호 관리 시스템과 다운로드 플랫폼 시스템 식별자 및 버전 정보를 포함하는 메시지로 방송망을 통해 전송한다. 이 외 CA Token, CA Token Revocation List, 콘텐츠 보호 관리 시스템의 클라이언트 소프트웨어 이미지, 다운로드 플랫폼 시스템의 DP 매니저 소프트웨어 이미지가 전달되는 단방향/양방향 전달 위치 정보를 포함한다. DP Message가 전달되는 위치 정보는 3.3절에서 언급한 CPT를 통해 시그널링 된다. 다운로드 플랫폼 시스템의 데이터는 ROUTE 프로토콜을 통해 방송망으로 전달한다.

3.6 포렌식 워터마킹

지상파 UHDTV 송수신 정합 표준에서는 특정한 포렌식 워터마킹 알고리즘에 대해서는 명시하고 있지 않으나 포렌식 워터마킹에 포함되어야 할 정보(제조사 인덱스, 디바이스 모델 이름, 워터마크 식별자)를 정의하고 있으며 부록을 통해 포렌식 워터마킹 기술 도입 시 성능 평가 항목 및 방법에 대해 기술하고 있다.

4. 맺음말

본고에서는 지상파 UHDTV 송수신 정합 표준에 포함되어 있는 콘텐츠 보호 표준 기술을 살펴보았다. 추가로 언급할 것은 본 표준에서는 콘텐츠 보호 관리 시스템 자체에 대해서는 표준화를 하지 않았다는 점이다. CAS 또는 DRM 기술로 대표되는 콘텐츠 보호 관리 시스템을 단일 표준화하는 경우 표준화로 인한 장점도 있겠지만 기술 차별화가 어렵고, 하나의 잘못된 구현이 표준을 준수한 다른 구현물에 위협이 될 수 있고(global breakdown), 표준화가 잘못된 경우 대체/갱신하는 절차가 어렵다는 단점이 있다. 반대로 비표준화 접근은 특정 벤더에 얽매이거나(Lock-in) 특정 벤더의 지원이 끊기면 대체 벤더를 찾기 어려운 단점이 있다. 본 표준에서는 콘텐츠 보호 관리 시스템을 변경할 수 있는 다운로드 플랫폼 기술을 표준화하여 비표준화 접근 방식의 단점을 다소 해결할 수 있도록 하였다.

[참고문헌]

[1] TTA, '지상파 UHDTV 방송 송수신 정합 (TTAK.KO-07.0127)', 2016년 6월 24일

[2] 한국저작권단체연합회, '2016 저작권 보호 연차보고서', 2016년 5월

[3] ISO/IEC 23001-7 Information technology – MPEG systems technologies – Part 7: Common encryption in ISO base media file format files (2nd Edition)

[4] ETSI TS 103 197 V1.5.1 (2008-10) Digital Video Broadcasting (DVB); Head-end implementation of DVB SimulCrypt

[5] TTA, , 'IPTV 용 교환 가능한 CAS (iCAS) (TTAK.08-0023/R2)', 2011년 9월 28일