PPI에 기반한 지상파 방송프로그램 보호 기술

*추현곤 이주영 남제호
한국전자통신연구원
hyongonchoo@etri.re.kr

Terrestrial DTV Broadcasting Program Protection based on Program Protection Information(PPI)

*Choo, Hyon-Gon Lee, Jooyong Nam, Jeho
Electronics and Telecommunications Research Institute

요약

지상파DTV 방송프로그램의 온라인 상의 불법적인 배포가 활발하게 일어남에 따라서, 지상파DTV 방송프로그램에 대한 보호를 위한 여러 가지 조치가 시도되고 있다. 국내에서는 TTA를 중심으로 ATSC의 RC 기술자를 기반으로 한 방송프로그램 보호 기술 규격이 제정되었으며, 이를 기반으로 한 수신기에서의 방송프로그램 보호에 대한 표준화가 진행 중이다.

본 논문에서는 방송프로그램 보호신호(Program Protection Information: PPI)에 기반한 지상파 방송프로그램 보호 방법에 대해서 소개한다. 제안하는 방법에서는 방송프로그램에 함께 포함된 PPI 정보의 재배포 조건에 따라, 방송프로그램을 암호화 되어 저장한다. 사용자의 홈도메인을 기반으로 사적복제를 지원하기 위해, 해당 방송프로그램을 복호화 하기 위한 인증 정보는 도메인 정보를 기반으로 방송프로그램과 같이 패키징 된다. 본 논문에서 제안한 지상파 방송프로그램 보호방법은 방송프로그램을 보호할 뿐 아니라, 사용자의 사적이용을 지원하기 위한 홈도메인 기반의 제한적인 배포 기능을 제공한다.

.

1. 서론

방송과 통신기술의 결합 및 컴퓨터, 네트워크 기술의 발달로 인해 방송프로그램의 네트워크을 통한 배포 및 유통을 용이하게 되었다. 그와 더불어 방송프로그램의 인터넷 불법적인 배포가 활발하게 일어남에 따라서, 방송프로그램에 대한 기술적인 보호조치가 요구되고 있는 상황이다. 특히 보호수단이 없는 지상파DTV의 경우, 이에 대한 보호 방책이 시급한 편이다.

지상파 방송프로그램에 대한 보호를 위한 여러 가지 방법이 시도되고 있다[1][2]. 미국에서는 방송프로그램 보호를 위해 'Broadcast Flag:BF' 정보를 삽입하는 방안을 시도했다. BF 방식은 재분배 제어 기술자에 따라, 인증된 기술을 통해서만 방송콘텐츠의 저장 및 재배포를 제어하는 방식이다. 현재 기술은 콜롬비아 연방법원의 '월권' 판정 이후, 효력이 상실된 상태이며, 향후 관련 법제화의 진행 여부 및 시행 시기가 이슈가 될 전망이다[3][4]. 유럽에서는 DVB CPCM 표준을 통해 방송프로그램이 수신된 이후, 홈네트워크 환경에서 저장된 콘텐츠의 사용 제어 및 인터넷을 통한 재배포 제어를 목적으로 한 방송프로그램 보호기술을 정의하고 있다[5]. 일본에서는 디지털 방송의 암호화 및 B-CAS를 이용한 방송프로그램 보호를 시행 중에 있으며, 최근 사용자의 이용범위의 확대를 포함하는 Dub-10 방안으로 개정 시행되고 있다[1]. 국내에서는 TTA를 중심으로 ATSC의 RC 기술자를 기반으로 한 방송프로그램 보호 송수신정합 기술 규격이 제정되었으며. 이를 기반으로 한 수신기에서의 방송프로그램 보호에 대한 표준화가 진행 중이다[6].

본 논문에서는 프로그램보호신호(PPI)에 기반한 지상파DTV 방송프로그램의 저작권 보호 기술 및 시스템에 대해 소개한다. 제안하는 방법은 지상파 DTV 방송프로그램의 PPI 정보에 따라 방송프로그램을 암호화 보호 저장한다. 사용자의 사적이용 기능을 지원하기 위해 홈도메인 기술을 기반으로 한 복사 기능을 제공한다.

2. PPI 기반 방송프로그램 보호 기술

가. 프로그램 보호신호 (Program Protection Information: PPI)

지상파DTV 방송프로그램 보호 송수신 정합에는 방송프로그램의 저작권 보호를 위해, 프로그램보호신호와 프로그램 ID로 구성된 신호를 정의하고 있다. 프로그램보호신호는 지상파 방송프로그램.의 저작권의 보호를 위해 해당 프로그램에 대한 최소한의 재배포 조건을 표현하기 위한 신호를 나타낸다.

프로그램 보호신호의 기술 규격은 <표 1>과 같다. <표 1>에서 redistribution_control_code(RCC)는 방송프로그램 배포 제어 정보로, RCC가 11일 경우 해당 방송프로그램은 자유스럽게 배포가 가능하며, RCC 가 01일 경우 제한적 배포 제어 조건의 범위 내에서의 배포 할 수 있다. RCC 가 00 일 경우, 방송프로그램은 보호된 형태로 사적이용 범위 내에서 저장 관리되어야 한다. redistribution_area 가 0인 경우, 지역정보를 포함하는 저장매체(DVD, HDDVD 등)을 통한 배포 또는 재전송시 한국 지역으로 명시하거나, 해당 지역으로 제한해야 한다.

<표 1> 프로그램 보호 신호

Syntax	Bits	비고
program_protection_information(){		
version	8	시스템 버전
redistribution_control_code	2	재배포제어코드
if (redistribution_control_code ==01){		
redistribution_condition()	8	재배포조건
}		
redistribution_area	1	재배포지역
reserved	5	
ppi_signature	320	디지털서명
}		

방송프로그램의 제한적 재배포 조건은 단말에서 방송프로그램에 대해서 모든 단말에 사용이 가능한 형태(예, 암호화가 없는 AVI파일)로 배포할 경우, 방송프로그램의 제한사항을 의미한다. 재배포 조건은 <표 2>와 같이 구성된다.

<표 2> 프로그램 보호 신호 내의 재배포 조건

Syntax	Bits	비고
redistribution_condition(){		
allowed_max_resolution	2	허용 최대 해상도
holdback_time	3	배포 허용 시점
allowed_length	3	최대 허용 길이
}		

- allowed_max_resolution: 방송프로그램 배포 허용 최대 해상도. 방송프로그램에 대해서 허용 최대 해상도보다 같거나 작은 범위의 화면 해상도 출력으로만 허용한다.
- holdback_time: 방송프로그램 배포 허용 시간. 방송프로그램의 방영 후, 지정된 시간이 지난 후에 배포를 지원한다.
- allowed_length: 방송프로그램 최대 배포 허용 길이. 방송프로그램의 녹화시작에서부터 지정된 시간까지의 길이만 배포를 지원한다.

프로그램 ID는 ATSC A/57b의 Content Labeling Descriptor 규격을 따라 Content Labeling Descriptor의 content_reference_id_byte 내의 ATSC_content_identifier 구조체에 포함되어 전송된다[8]. 전송되는 프로그램 ID의 정의는 <표3>과 같다.

<표 3> 프로그램 ID

Syntax	Bits	비고
Program_identifier(){		
major_channel_number	10	주채널정보
minor_channel_number	10	보조채널정보
reserved	4	
onair_time	32	방영(시작)시간
reserved	4	
length_of_program_code	7	프로그램코드길이
program_code	var	프로그램코드
}		

<표3> 에서 채널 정보 및 방영시간은 기존의 PSIP 프로토콜의 있는 정보와 일치하여야 하며, 프로그램 코드의 경우, 방송사의 자체적으로 사용하는 관리 코드 및 표준 관리 체계 코드(예, UCI 등)를 삽입 가능하다.

프로그램보호신호(PPI)와 프로그램 ID는 지상파방송프로그램의 PMT의 Descriptor 루프 및 EIT 내의 각 이벤트의 Descriptor 루프에 포함되어 전송된다.

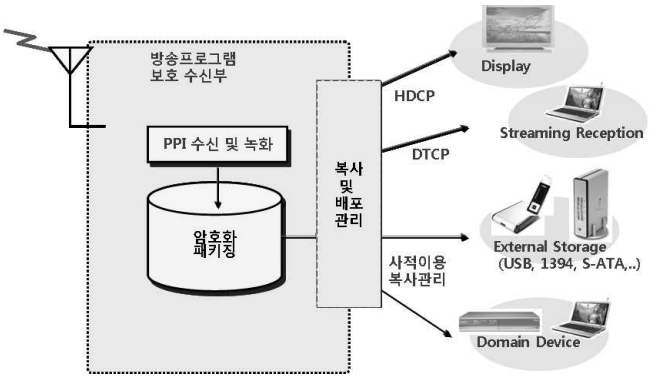
나. 방송프로그램 보호 기술 요구사항

지상파DTV 방송프로그램의 경우, 다른 콘텐츠와 달리 저작권을 위한 보호 외에, 사용자의 사적 이용에 대해서 일정한 범위 내에서 지원이 가능해야 한다. 이를 고려한 PPI 기반 방송프로그램의 보호 기술적 요구사항은 다음과 같다.

- 방송프로그램의 무단 배포 방지할 수 있어야 한다.
- 수신단말은 PPI를 수신, 해석 할 수 있어야 한다.
- 수신단말은 PPI를 수정하거나 누락시키지 말아야 한다.
- 수신단말은 PPI에 따라 방송프로그램을 보호할 수 있어야 한다.
- 수신단말은 방송프로그램을 녹화할 경우 프로그램과 함께 PPI를 저장 및 관리하여야 한다.
- 수신단말은 방송프로그램을 복사 및 배포할 경우, 방송프로그램의 PPI를 유지하여야 한다.
- 수신단말은 PPI가 포함된 방송프로그램을 복사할 경우, 상호호환적 전송 규격을 지원해야 한다.

다. 방송프로그램 보호 기술 구성

PPI를 포함한 방송프로그램에 대한 보호는 수신 단말에서 지원된다. <그림 1>은 수신단말을 통한 지상파DTV 방송프로그램 보호 기술의 구성을 나타낸다.



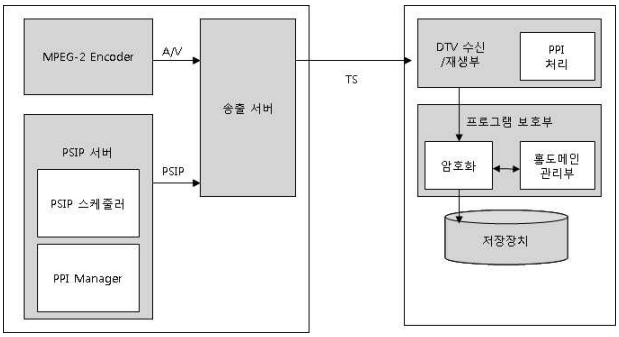
<그림 1> 방송프로그램 보호 기술 구성

지상파DTV 방송프로그램의 보호 기술에는 가장 먼저 PPI 신호를 추출 해석하고, 이를 바탕으로 녹화 시에 암호화 및 패키징을 한 다음, 사용자의 사적이용 범위 내에서의 방송프로그램에 대한 복사 및 배포 지원 기술을 그 범위로 한다. 다음에서 지상파DTV 방송프로그램에 대한 보호 기술에 대한 구현 방안에 대해서 소개한다.

3. PPI 기반 방송프로그램 보호 시스템

가. 시스템 구성

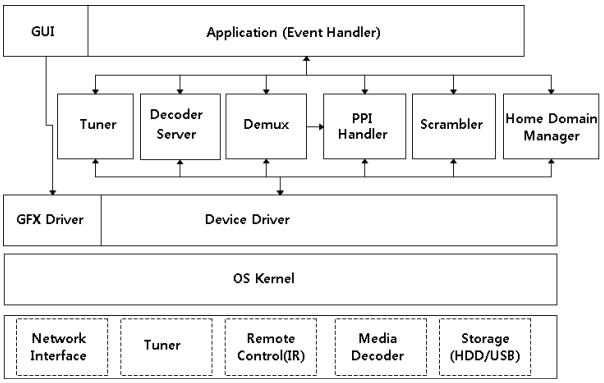
방송프로그램 보호 시스템은 방송프로그램에 PPI 및 프로그램 ID를 방송프로그램에 재다중화하여 전송하는 송출서브시스템과 이를 수신하여, 녹화/배포 시에 제어를 실행하는 수신서브시스템(이하 수신단말)로 구성된다. 본 논문에서 소개하는 지상파DTV 방송프로그램 보호를 위한 시스템 구성은 <그림 2>와 같다.



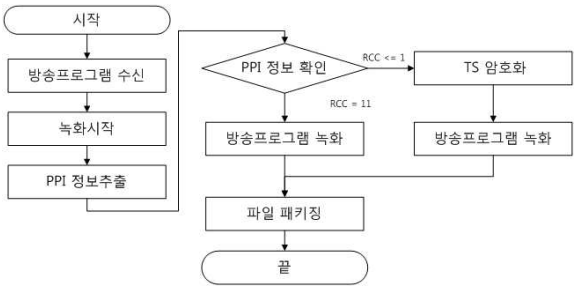
<그림 2> 지상파DTV 방송프로그램 보호 시스템 구성

송출서브시스템에서는 방송프로그램 보호를 위한 프로그램 ID와 보호에 대한 배포 범위를 입력하여 전송하고, 이에 따라 수신 단말에서 PPI 정보에 따라 방송프로그램을 저장, 배포 관리한다.

<그림 3>은 임베디드 기반의 수신단말의 구성의 예를 보여준다. 기존의 지상파DTV 수신기의 구성인 DTV 튜너, 역다중화기(Demux), 비디오 및 오디오에 대한 디코더 모듈 및 이를 통해 외부 출력을 보유하고 있으며, 역다중화기에서 PSI/PSIP 정보를 입력받아 프로그램보호신호 및 방송프로그램 ID 정보를 추출하는 PPI 처리기와 보호된 상태로 방송프로그램을 녹화하기 위한 Scramber와 사적 복제를 지원하기 위한 홈도메인 관리기로 구성된다.



<그림 3> 방송프로그램 보호 수신 단말 구성



<그림 4> 지상파방송프로그램 보호 녹화 처리 과정

다. 프로그램 보호신호에 따른 보호 기능 동작

방송프로그램 보호과정은 두 가지로 구성된다. 방송프로그램의 PPI를 해석하여 보호된 상태로 녹화 저장하는 단계와 보호된 방송프로그램을 사용자의 수신기기에서 이용하기 위해 홈도메인 기술을 이용한 배포를 관리하는 단계이다. 아래에서 각 단계에 대해서 설명한다.

- 방송프로그램 녹화 관리

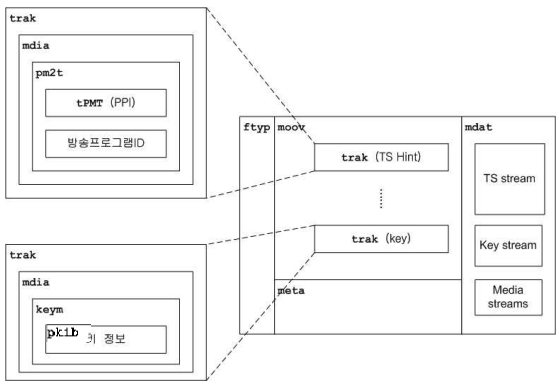
<그림 4>는 PPI에 따른 방송프로그램 보호 녹화과정을 나타낸다. 수신단말에서 방송프로그램의 보호는 지상파DTV를 통해 전송되는 방송프로그램으로부터 프로그램보호신호(PPI)를 추출 및 해석하는 단계, 프로그램보호신호에 따라 방송프로그램을 암호화 저장 및 패키징 단계로 구성된다.

프로그램보호신호(PPI) 추출은 수신되는 방송프로그램의 PSIP/PSI 정보를 이용한다. Demux에서 PSIP/PSI 정보를 PPI 처리기로 전달하면, PPI 처리기에서는 RC Descriptor의 존재 유무를 확인한 후, PPI 정보를 해석하여, redistribution_control_code의 값을 통해 다음과 같이 암호화 필드를 설정한다.

bEncryption = if(redistribution_control_code <= 1)? 1:0;

PPI정보에서 암호화 필드가 설정이 되는 경우, 사용자가 방송프로그램의 녹화할 때, 프로그램은 암호화가 적용되어 저장된다. 제안하는 시스템에서는 프로그램의 암호화를 위해 AES128 CTR를 사용한다. 임베디드 환경에서의 암호화하여 저장하는 부담을 덜기 위해, 암호화는 패킷단위에서 TSID를 기준으로 Video 또는 Audio/Video 데이터를 선택적으로 암호화하며, TS의 Sync를 위하여 TS 패킷의 헤더 및 adaptation 필드를 제외한 페이로드만 암호화를 진행한다. 암호화에 사용된 키(CW)는 임의의 값으로, 도메인 또는 기기의 고유키로 다시 암호화 된 후 방송프로그램과 함께 패키징 저장관리 된다.

패키징 파일은 ISO Media File Format/DVB File Format 기반의 파일 포맷을 이용한다[8][9]. <그림5>는 패키징 파일 포맷의 구성의 예를 나타낸다.

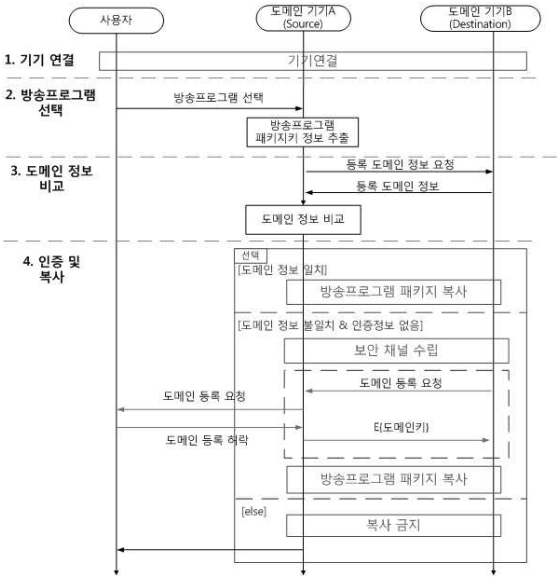


<그림 5> 방송프로그램 보호 공유 파일 포맷

TS 형태의 방송프로그램을 저장하기 위해 MPEG-2 Protected Transport Stream Reception Hint Track을 이용하며, PPI 및 Program ID 정보를 저장하기 위해 MPEG2TSSampleEntry 박스 내의 PMT Table을 이용한다. 암호화에 사용된 키정보는 키트랙으로 저장하고 KeyMessageReceptionSampleEntry를 통해 부가 정보를 저장하는 방식으로 지원한다.

- 홈도메인 관리

사용자가 다른 장치를 통해 녹화된 방송프로그램을 이용하려 할 경우, 기기 간 도메인 등록 절차를 통한 도메인 키 공유를 통해 가능하다. <그림 6>은 방송프로그램 복사 과정에서 도메인 등록을 통한 프로그램 복사의 예를 보여준다. 제안하는 시스템에서는 <그림 6>과 같이 복사 대상 기기가 방송프로그램의 복사를 위해 연결될 때, 등록 정보의 비교를 통해 복사와 등록 과정을 동시에 수행하도록 처리한다. 장치간의 보안채널 수립은 Diffie-Hellman 알고리즘을 사용한다.

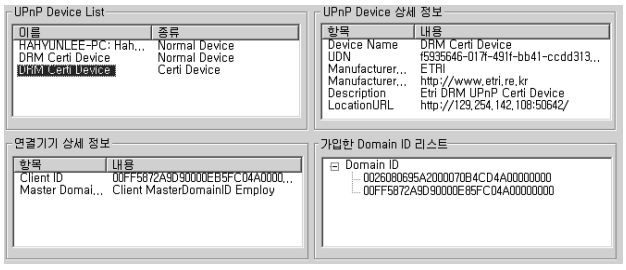


<그림 6> 홈도메인 관리 기능을 통한 방송프로그램 복사

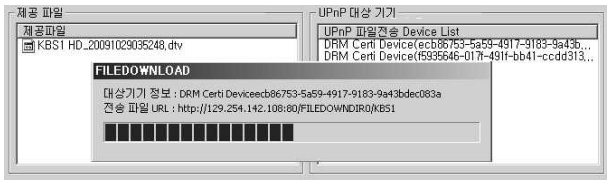
4. 구현 결과

제안하는 방송프로그램 보호관리 시스템은 STB 및 PC 형태의 수신단말 형태로 구현되었다. <그림 7>은 STB으로 구현된 수신단말기에서 전송되는 PPI에 대한 모니터링 정보에 대한 출력 기능에 대한 예이다.

<그림 7> 방송프로그램보호신호 모니터링



(a) 도메인 관리



(b)방송프로그램 복사제어

<그림 8> UPnP 네트워크를 이용한 도메인 관리 및 파일 복사

시스템의 수신단말에서 도메인 관리 기능은 UPnP 네트워크를 이용하여 구현되었다. <그림 8>은 UPnP 네트워크를 통해 관리되는 기기 간에 UPnP 기기 정보 및 이를 통해 관리되는 도메인 정보 관리 및 방송프로그램을 복사 제어 기능에 대해 보여 주는 예이다. 그림 8에서의 예에서와 같이 제안하는 도메인 관리 기술은 UPnP 프로토콜과 같은 홈네트워크 프로토콜과 쉽게 연동할 수 있으며, 파일 복사와 도메인 관리를 동시에 처리할 수 있는 장점을 가지고 있다.

5. 결 론

본 논문에서는 방송프로그램 보호신호(Program Protection Information: PPI)에 기반한 지상파 방송프로그램 보호 방법에 대해서 소개하였다. 제안하는 방법에서는 방송프로그램에 함께 포함된 PPI 정보의 재배포 조건에 따라, 방송프로그램을 암호화 되어 저장한다. 사용자의 홈도메인을 기반으로 사적복제를 지원하기 위해, 인증 정보는 도메인 정보를 기반으로 방송프로그램과 같이 패키징 된다. 방송프로그램의 복사 및 공유 기능은 홈도메인 등록 절차를 통해 제공된다. 실험결과로서 STB 및 PC 형태의 수신단말에서의 방송프로그램에서의 PPI 추출 및 도메인 기반의 복사 제어 기능을 UPnP 네트워크를 통해 보였다.

본 논문에서 제안한 지상파 방송프로그램 보호방법은 방송프로그램의 저작권을 보호할 뿐 아니라, 다른 기기에서의 공유를 지원함에 따라 사용자의 사적이용을 지원할 수 있는 장점을 가진다.

Acknowlegment

본 연구는 방송통신위원회, 지식경제부 및 한국산업기술평가관리원의 IT신성장동력핵심기술개발사업의 일환으로 수행하였음. [과제관리번호: 2007-S-003-03, 지상파DTV 방송프로그램 보호 기술개발]

참 고 문 헌

[1] Williams, Jim C., "Preserving the Viability of Broadcast TV," Asia Pacific Technical Review Journal, Jul-Aug., Asia Pacific Broadcasting Union (ABU), 2005.

[2] 추현곤, 남제호, 김준섭, "지상파DTV 방송프로그램 보호기술 특허 동향분석", 전자통신동향분석, 제22권 6호, 2007년 12월.

[3] The Broadcast Flag: What Now, In-stat Inc., 2005. 06.

[4] 방건, 추현곤, 남제호, "DTV 방송콘텐츠 저작권 보호를 위한 Broadcast Flag 기술 동향", 전자통신동향분석, 제21권 4호, 2006년 8월.

[5] DVB Bluebook A094R2, DVB Content Protection and Copy Management – A094r2 contains the complete set of core normative elements of the CPCM specification, Feb. 2008.

[6] 정보통신단체표준 , TTAK.KO-07.0068, 지상파 DTV 방송프로그램 보호신호 송수신정합, 2008.12.

[7] ATSC Standard A/65C: Program and System Information Protocol for Terrestrial Broadcast and Cable (Revision C) with Amendment No. 1, Oct. 2006.

[8] ATSC Standard A/57B: Content Identification and Labeling for ATSC Transport. May 2008.

[9] DVB Bluebook A121, File Format Specification for the Storage and Playback of DVB Services, June 2008.