情報保護學會論文誌
第17卷 第2號, 2007. 4

방송 콘텐츠를 위한 안전한 유통 시스템 설계 및 구현

이 진 흥,[1†] 이 혜 주,[2] 신 상 욱[1]
[1]부경대학교, [2]모빌리존

Design and Implementation of Secure Distribution System for Broadcasting Contents

Jin-heung Lee,[1†] Hea-ju Lee,[2] Sang-uk Shin[1]
[1]Pukyong National University, [2]MOBILIZONE Inc.

요 약

HDTV용 방송 콘텐츠 보호 시스템은 기존의 DRM 시스템에서 이용하는 파일 암호화 기술을 적용하기에는 상당한 어려움을 가진다. 따라서 TS 등과 같은 방송 콘텐츠 포맷에 대하여 적응적이면서, 효율적인 암호화 기술과 임의 접근 모드가 제공되어야 한다. 또한, 방송 환경에 적합한 키 분배 메커니즘이 제공되어야 한다. 본 논문에서는 기존의 MPEG 시스템을 변경하지 않고 인코더/디코더에 적용 가능한 암호 기법과 브로드캐스트 키 분배 메커니즘을 제안하고 구현하였다.

ABSTRACT

Broadcasting contents protection system for HDTV has many difficult to apply file encryption technology that using the existing DRM systems. Therefore, this system has to be processed as accommodative about broadcasting contents format such as TS and PS and so on. Also, this system must support efficient encryption technology and random access mode. In addition, this system must have suitable key distribution mechanism in broadcasting environment. In this paper, we propose and implement encryption/key distribution scheme applicable to encoder/decoder without changing the existing MPEG system.

Keywords : *MPEG-2 TS security, Broadcasting key distribution, DRM, CTR mode, copyright protection for HDTV*

Ⅰ. 서 론

최근 컴퓨터 기술의 급속한 발전으로 인해 기존의 텍스트 위주의 사용자 환경에서 벗어나 이미지, 그래픽, 오디오 및 비디오 데이터 등을 제공하는 멀티미디어 사용자 환경으로 변환하고 있다.

디지털 기술의 발달과 네트워크 융합으로 인하여 언제 어디에서든지 쉽게 고품질의 방송 프로그램을 전송하고 이용할 수 있게 되었다. 따라서 빠른 인터넷 속도와 양질의 방송 콘텐츠에 의해 디지털 방송 프로그램에 대한 무단 복제와 불법 전송이 더욱 가속화되고, 방송통신 융합시대의 심각한 문제로 제기될 것으로 예상된다. 게다가 디지털TV의 높은 보급률은 많은 이용자가 완벽에 가까운 화질과 음질을 서비스 받을 수 있는 환경을 제공하는 반면, 원본과 동일한 콘텐츠의 복제가 가능한 문제점을 가지고 있다. 또한 이러한 콘텐츠를 위성, 케이블, 공중파 등을 통해 모두 전달 가능하므로 불법 배포는 방송 콘텐츠의 디지털 전환을 더디게 하고 새로운

접수일: 2006년 8월 18일; 채택일: 2006년 12월 4일
* 본 연구는 산업자원부의 지역혁신 인력양성사업의 연구결과로 수행되었습니다.
† 주저자/교신저자, jinhung@hanmail.net

콘텐츠 제작을 위한 사업자들의 투자 및 개발에 걸림돌로 작용할 것이다.

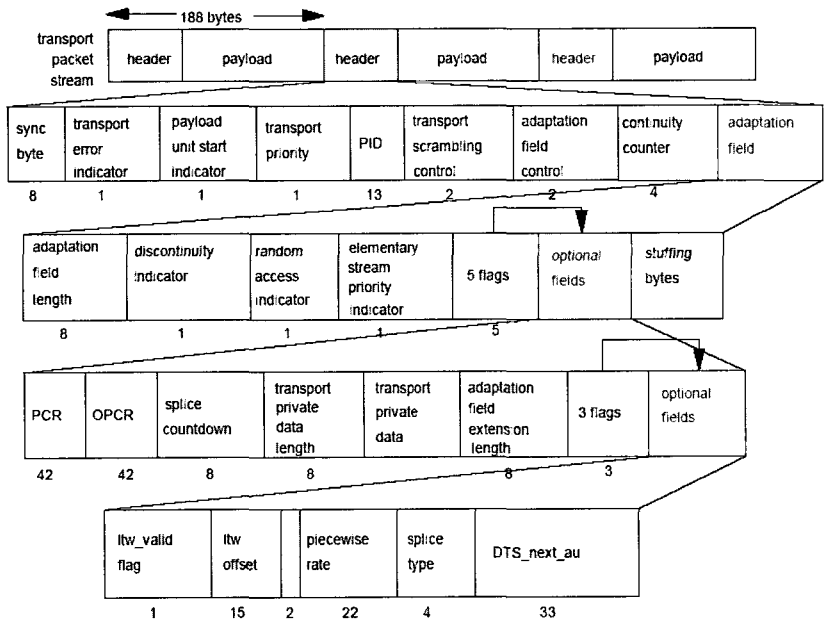
1997년 미국은 FCC(Federal Communications Commission)를 통해서 디지털 TV로의 전환을 선포한 뒤, 2006년에 디지털 전환 완료 시점으로 설정하고 현재 미국의 방송 산업의 입장을 주축으로 FCC에서 콘텐츠 보호 방안들이 논의되고 있다. 콘텐츠 보호와 관련한 이슈는 방송 콘텐츠 서비스의 특성으로 무단 복제 및 잠재적 재전송에 대한 심각한 문제를 안고 있다. 기본적인 원칙은 소비자가 콘텐츠를 녹화하는 것을 제한할 수 없으며, 복제 제한보다 콘텐츠 보호라는 차원에서 더 적절한 형태의 재전송 통제 시스템을 구성해야 한다.

콘텐츠 보호 대체 방안의 가장 현실적이면서 기술적인 방안은 방송 콘텐츠에 적합한 암호 알고리즘을 개발하여 암호화된 콘텐츠를 전송하고 정당한 사용자만이 키를 이용하여 복호화 해서 사용하는 방법이다. 미국 차세대 디지털 케이블 방송 규격제정을 위해 미국 케이블랩스에서는 오픈케이블 프로젝트를 운용하고 있으며, ANSI SCTE 41/DVS 301(POD Copy Protection System) 표준[1]을 기반으로 2002년 복제방지 기술에 관한 규격을 발표하였다. 이는 셋톱박스와 수신제한장치 사이에 DES-ECB 방식에 의해 암호화하고, 키 교환을 위해 Diffie-Hellman 알고리즘을 이용한다. 또한 키 정보의 무결성을 위하여 SHA-1을 사용하고 있으며, 키 수열 생성을 위해서 DFAST 알고리즘을 이용하도록 권고하고 있다[2]. DAVIC에서는 기밀성을 위하여 스크램블 기술이 제공되며, 스크램블은 MPEG2 TS에서 수행된다. DAVIC에서 수행되는 스크램블 알고리즘은 ISO, ITU 또는 ETSI에서 표준으로 수용되어야 한다.

본 논문에서는 HDTV용 방송 콘텐츠 보호를 위한 시스템을 새롭게 설계, 구현하여 안전하게 전송하는 방법을 제안한다. 방송 콘텐츠에 대한 암호화 기술은 기존의 파일 암호화 달리 수신측에서 임의 접근하여 복호화될 필요가 있다. 따라서 본 논문에서는 MPEG2 TS를 대상으로 임의 접근 가능한 알고리즘을 설계하고 안전한 방송 콘텐츠 유통을 위하여 브로드캐스트 키 분배 메커니즘을 설계하고 시스템을 구현한다.

Ⅱ. HDTV용 방송 콘텐츠 전송을 위한 MPEG 시스템

MPEG은 동영상 압축/해제 방식의 표준을 가리키며 1991년 디지털 저장 매체용으로 선보인 MPEG1과 1994년 디지털 방송용 MPEG2가 표준규격으로 채택되었다. MPEG2 시스템에는 단일 프로그램을 오류가 없는 채널 환경에서 다중화 하는 프로그램스트림(PS)과



〔그림 1〕 TS 패킷 구성도

오류가 있는 채널 환경에서 복수의 프로그램을 다중화하는 트랜스포트스트림(TS) 두 종료의 다중화 방식이 있다. TS는 일련의 패킷으로 구성되는데 각각의 길이는 188byte로 비교적 짧은 고정길이를 가진다. 이는 MPEG1, MPEG2 및 기타의 방법으로 압축된 엘리먼트 스트림 등을 채널로 전송하기 위하여 정한 일정한 형식을 말한다[3,4,5,6].

MPEG2 TS는 PS와 달리 전송 환경에 적합한 시스템 표준이다. 현재 디지털 방송과 같은 응용분야에 사용되고 있으며 전송 환경에서의 오류를 고려해야 하기 때문에 PS 패킷보다 작은 패킷 크기와 정적인 구조를 요구한다. 일반적인 TS 패킷의 계층 구조는 [그림 1]과 같다. TS 패킷의 헤더는 8비트의 sync_byte (0x47)로 바이트 정렬되어 있다. 따라서 TS 스트림에서 바이트 정렬시켜서 TS 패킷을 추출해 낼 수 있다. 추출된 TS는 일반적으로 4byte의 헤더 정보와 184byte의 유료부하(payload)를 가진다.

시스템 디코더가 TS 스트림 내에 있는 프로그램을 디코딩할 수 있도록 사용자가 정의하는 프로그램 정보를 프로그램 구성정보(PSI, Program Specifica- tion Information)라고 한다. PSI는 프로그램을 구성하고 있는 엘리먼트들에 관한 정보를 갖는 PAT(Program Association Table)와 PMT(Program Map Table), 전송 네트워크에 대한 규정된 값에 해당하는 NIT(Network Information Table), 그리고 조건부 수신에 관한 CAT (Conditional Access Table)로 구성된다. PAT와 PMT에서는 패킷에 대한 PID를 정보를 보내주는데 PID는 TS 패킷 헤더에 있는 패킷 ID를 말한다. 이 PID는 TS 패킷의 소속을 나타내고 있기 때문에 역다중화 과정에서 이 PID 만으로 패킷을 구분하게 된다. NIT는 전송에 관련된 파라메터를 나타내주는 값으로서 FDM (Frequency Division Multiplexing)의 경우 주파수나 트랜스포트 번호 등에 관련된 데이터를 포함한다. PAT에 프로그램 번호가 0인 PMT_PID가 있다면 이 PID를 갖는 TS 패킷은 NIT 정보를 갖고 있게 된다. 그리고 CAT는 시스템 차원에서 전체적인 스크램블을 수행할 때, CA_ descriptor 관련 정보는 PSI 내에 존재해야 한다.

MPEG에서는 최대한 0.7초 이내에 PSI 정보를 전송해야 한다고 규정하고 있다. PID 값이 0인 TS 패킷은 PAT 정보를 갖고 있는 것으로 처음부터 규정하고 있다. 따라서 시스템 디코더는 시스템을 켰을 때 PID가 0인 TS 패킷만을 찾을 것이다.

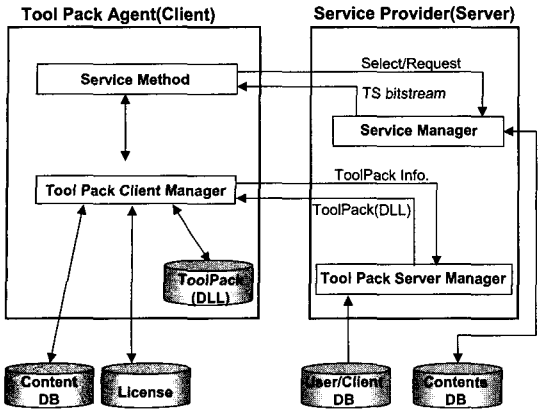
Ⅲ. 안전한 방송 콘텐츠 유통 시스템 설계

2.1 HDTV용 방송 콘텐츠를 위한 보호 툴 설계

콘텐츠 보호를 위하여 많은 DRM 시스템들이 개발되어 왔다. 대부분의 DRM 시스템은 시스템 고유의 요소기술을 이용하여 콘텐츠 보호를 실현하고 있으며, 이러한 시스템은 폐쇄형 DRM 시스템이라고 한다. 이러한 폐쇄형 DRM 시스템은 비공개된 고유의 콘텐츠 보호 알고리즘을 이용하여 충분한 안전성을 제공하고 있지만 앞으로 다가올 개방형 운영체제 장치 하에서 안전하게 콘텐츠를 보호하고, 다양한 DRM 시스템을 이용하려는 소비자의 욕구를 충족시키기 위해서는 개방형 DRM 시스템의 개발이 필수적이다. 개방형 DRM 시스템을 구성하기 위해서는 먼저 시스템간 상호운용성을 지원해야 한다.

DRM 시스템의 상호운용성이란 다양한 DRM 솔루션 또는 타사의 제품이 고객 측의 특별한 노력 없이도 자신의 디바이스에서 DRM 시스템을 적용하는 것이 가능하고, 콘텐츠는 DRM 시스템과 관계없이 제공되는 것을 말한다. DRM 기술의 상호운용성을 지원하기 위한 기존의 방법은 인증, 암호화, 워터마킹 등과 같은 정보보호기술을 모듈화하고, 모듈화된 정보보호 툴에 대한 인덱스(Index) 및 API를 공개하여 툴에 대한 재사용을 가능하게 하는 방식으로 상호운용성을 지원한다. 그러나 IPMP 터미널이 모든 개별 툴의 동작을 제어하는 기존의 구조에서는 개별 툴에 대한 관리와 보호가 쉽지 않기 때문에 특정 서비스 제공자가 사용하는 보호 툴들을 툴 그룹으로 묶고 이에 대한 운용을 툴 에이전트에게 전적으로 일임하는 구조가 요구되었다. 이것을 툴팩이라 하며, 툴팩을 이용하는 경우 툴의 상호운용성 지원을 위한 API를 간소화시키고, 서비스 입장에서 개별 툴에 대한 API 및 툴 정보를 공개할 필요가 없게 됨으로써 보다 안전하게 제공가능하다[7].

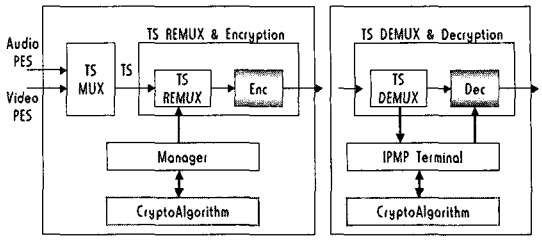
본 논문에서는 [그림 2]와 같이 기존의 툴팩 기반에서 전송되는 콘텐츠를 보호하기 위한 시스템 구조를 제안한다. 제안 시스템은 기존의 방송사가 소유하고 있는 방송콘텐츠에 각 방송사들의 고유한 툴팩으로 다중화하고, 툴팩에 포함된 암호 모듈에 의해 방송 콘텐츠를 암호화하여 콘텐츠를 서비스한다. 이러한 구조는 기존의 MPEG2 IPMP에서 해결해야할 문제점들을 다소 해결할 수 있을 것이다. 첫째, 다중 제어점 사이에서 효율적



〔그림 2〕 툴팩 기반 시스템 구조

인 암호화 툴 적용을 가능하게 한다. 예를 들어 MPEG2 IPMP에서는 역다중화기와 미디어 디코더 사이에 암호화 툴들이 적용될 수 있는 제어점을 마련해 놓고 있으나, 현재 상용화되고 있는 칩셋은 역다중화기와 미디어 디코더가 하나의 칩으로 구현하고 있다. 제안 시스템은 칩셋 사이의 메모리 데이터를 획득하여 툴팩을 적용하는 구조로써 현재 칩셋 사이에서의 암호화 적용 가능한 플랫폼을 제공할 것이다. 둘째, 다양한 보호툴 적용에 의한 계산량 증가를 최소화 한다. 툴팩은 각각의 알고리즘에 따라 독립된 툴팩 라이브러리를 제공한다. 그리고 셋탑박스에서 적용 가능한 알고리즘 및 실시간 접근성을 높임으로써 기존의 하드웨어에서 충분한 처리 성능을 제공할 것이다. 마지막으로 다양한 운영체제 및 효율적인 상호운용성을 지원한다. 제안된 시스템은 셋탑박스 및 IPMP 터미널과 독립적으로 동작 가능한 구조로서 다양한 운영체제를 지원하고 있다. 또한 상호운용을 위한 툴팩 등록 및 갱신 절차를 안전하고 효율적으로 제공할 수 있다.

제안된 시스템을 적용하기 위해서 먼저 개인 단말기에서는 툴팩의 등록 및 갱신을 수행해야 한다. 단말기는 전송된 콘텐츠를 복호화하기 위해 해당 툴팩을 이용하여 복호화를 시도하게 된다. 이때, 사용된 툴팩이 없는 단말기는 서비스 제공업자로부터 적용된 툴팩을 업데이트하거나 다운로딩 하여 서비스를 제공을 수 있다. 툴팩 업데이트는 시청자의 단말기를 통하여 툴팩 아이디와 툴팩 버전을 서버에 전송하고 필요로 하는 툴팩을 요청한다. 서버는 요청된 툴팩을 확인하고 사용자의 단말기에게 툴팩을 전송한다. 단말기에 툴팩이 설치되면 시청자는 단말기의 툴 에이전트에서 콘텐츠 사용을 위한 라이센스를



〔그림 3〕 MPEG-2 TS 암호화 적용 시스템

요청하게 되고, 요청된 라이센스에 포함된 키로부터 툴팩의 비밀 데이터를 복호화 한다. 이러한 툴팩 비밀 데이터는 콘텐츠 암호화를 위한 알고리즘과 운용모드, 그리고 카운트를 구성할 수 있는 정보 등을 포함한다.

MPEG2 TS를 보호하기 위해 방송 서버와 시청자의 셋톱박스에서는 〔그림 3〕의 형태로 암호 툴이 적용되어야 한다. 방송 서버에서는 A/V가 다중화된 A/V TS에 대해 방송 정보를 재다중화 하고 암호 모듈에 의해 암호화되어 최종적으로 암호화된 TS가 전송될 것이다. 암호화된 TS를 수신한 셋톱박스에서는 방송 정보를 역다중화 하여 IPMP 터미널에 의해 복호화를 요청하고, 복호 모듈은 수신된 TS를 복호화하게 된다.

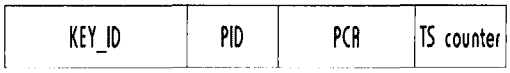
2.2 콘텐츠 암호화를 위한 CTR 모드 설계

HDTV 환경에서의 콘텐츠 유통을 위하여 MPEG2 TS 파일에 대하여 효율적이 암호화 알고리즘을 제공해야한다. TS 파일에 대한 암호화는 188byte의 TS 중에서 유료부하 부분에만 적용되어야 하며, 헤더정보, 적응필드 및 Tail block(64bits 기준으로 유료부하 분할)에는 적용하지 않아야 한다. 따라서 적응필드가 0byte인 경우, 188byte TS 파일 중에서 헤더 부분인 4byte를 제외하면 MPEG2 TS의 유료부하에는 23개의 블록이 DES로 암호화되어 전송하도록 구성되어 있다. 이와 같은 암호화에는 CCI의 내용과 CAS 시스템에서 암호화된 콘텐츠에 대해서 CPS에서의 암호화 적용을 원칙으로 하며, 수신제한장치와 호스트 사이에 암호화 및 키 적용에 관한 규약은 다음과 같다. 여기서 기본은 단일 키 모드이며, 옵션으로 짝수 번째와 홀수 번째로 두 개의 키를 적용하는 듀얼 키 운용 모드도 필요하다. DAVIC 시스템에서는 기밀성을 위하여 스크램블 기술이 제공되며, 스크램블링은 MPEG2 TS에서 수행한다. 스크램블은 부호화된 데이터를 시스템의 비인가된 사용

자가 이용할 수 없도록 정보를 조직적으로 변경하는 메커니즘이다. 스크램블링 메커니즘에서 사용되는 특정 알고리즘은 스니퍼나 해커에 의한 가로채기 공격으로부터 안전해야 한다. 그리고 ISO-13818-1은 TS 패킷 헤더와 적응필드의 암호화를 금하고 있다. 이것은 요구되는 복호화 과정 없이 TS 제어와 역다중화/재다중화를 허락하기 위한 것이다.

국내의 HDTV용 방송 콘텐츠 보호 기술은 초기 워터마킹 시스템을 이용한 저작권 보호 솔루션이 주를 이루다가 현재에는 DRM 솔루션에 의한 암호화 기법이 주류를 이루고 있다. DRM 기술은 AES 암호 알고리즘과 RSA, DH 방식의 키 교환 등 첨단 암호화 알고리즘을 구현하여 안전한 유통 구조를 확립하고 있지만 대부분의 경우 파일로 다운로딩 되는 시스템 상에서 적용 가능한 구조를 가진다. HDTV 방송 콘텐츠를 위한 암호화 기능은 MPEG2 TS 파일을 효율적으로 선택하여 암호화를 수행하고, 사용자 단말기에 복호화할 때에는 유료부하의 암호화된 영역을 복호화해서 부하를 최소화하여 수행해야 한다. 또한 임의의 TS 파일 영역을 선택하여 시청하려고 할때, 실시간적으로 임의 접근 복호화가 가능해야 한다.

이러한 조건을 만족하기 위해서 MPEG2 TS 암호화 방식은 다음과 같은 요구사항을 만족해야 한다. 첫째, 암호화된 TS는 셋톱박스에서 실시간으로 복호화가 실행되어야 하므로 셋톱박스의 성능을 고려하여 고속의 복호화가 이루어져야 한다. 둘째, MPEG2 TS는 188byte의 고정된 패킷 길이를 가지고 있으므로 암호화된 TS 패킷은 188byte의 길이를 유지해야 한다. 셋째, TS를 암호화하기 위한 알고리즘은 안전성이 증명되어야 한다. 마지막으로 암호화된 TS 파일에 대한 임의접근 복호화가 가능

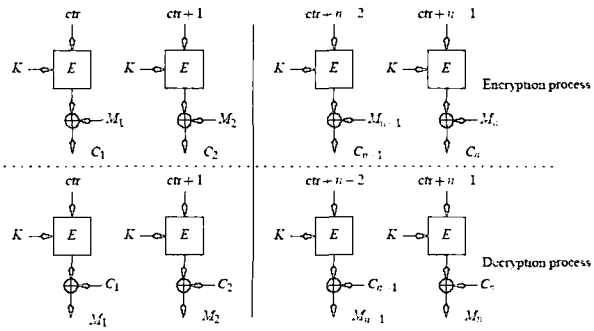


〔그림 5〕 CTR 모드를 위한 카운터 구조

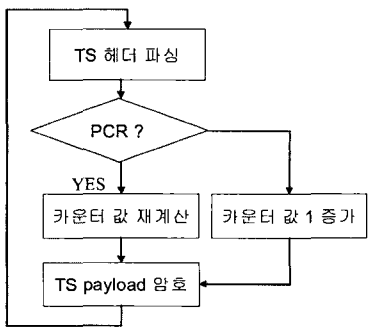
해야 한다.

블록 암호 알고리즘의 카운터(counter, CTR) 모드는 키 K를 이용하여 평문이 아닌 암호화 수행에 대한 카운터 값을 암호화하여 생성된 키스트림을 평문과 EX-OR 연산을 수행함으로써 평문의 암호문을 생성한다. 이러한 카운터 모드를 이용하면 저 사양의 하드웨어 플랫폼 상에서 효율적인 소프트웨어 구현이 가능하고, CBC 모드보다 빠른 하드웨어 처리 속도를 가질 수도 있다. 단일 블록당 단일 암호 알고리즘을 수행하지만 반복되지 않는 카운터 값을 적용하여 ECB 모드보다 좋은 암호학적 안전성을 제공한다. 또 하나의 특징은 암호문에 대한 임의접근이 가능하다. 암호문의 특정 블록의 카운터 값을 알게 되면, 그 위치부터의 복호화를 수행할 수 있다. 또한 기존의 블록암호와는 달리 암호화되는 암호문의 길이는 평문의 길이를 유지할 수 있다. 그리고 암, 복호화 과정에서 기반이 되는 블록 암호의 암호화 함수만을 사용한다. 〔그림 4〕는 CTR 모드를 이용한 암호화와 복호화 과정을 나타낸다[8,9].

카운터모드는 동일한 카운터 값이 사용되는 경우 안전성이 떨어지기 때문에 암호화된 TS 파일 내에서 중복된 카운터 값을 사용하지 않아야 한다. 중복을 피하기 위해 우리는 다음과 같은 카운터 값을 생성한다. 카운터 값은 〔그림 5〕와 같이 TS 패킷에서 추출된 값과 IPMP 터미널로부터 전송 받은 KEY_ID를 이용하여 128bits의 counter_base를 생성한다. KEY_ID 필드는 암호화/복호화 시 사용되는 해당 키에 대한 식



〔그림 4〕 블록 암호의 CTR 모드



〔그림 6〕 카운터의 재계산

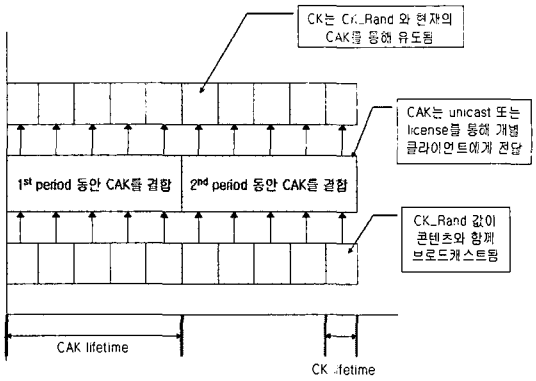
별자로 키를 생성하는데 이용된다. PID 필드는 암호화/복호화 되어지는 해당 TS의 헤더에 있는 패킷 ID로 수신측과 송신측이 암호화/복호화 되는 TS를 구별 가능하도록 카운터를 생성하기 위한 필드로 설정하였다. PCR(Program Clock Reference) 필드는 시스템 인코더에서의 시간을 27MHz 시스템 클럭으로 샘플링한 값으로 주기적으로 TS 다중화 되기 때문에 송신과 수신측의 동기화하기 위하여 이용한다. 마지막 필드인 TS counter는 PCR 값을 수신한 이후에 수신된 TS 패킷을 하나씩 카운트한 값으로 PCR을 새롭게 수신한 경우 카운트는 0으로 재설정된다.

방송의 특성 상 시청자가 TV를 켜는 시점을 알 수 없기 때문에 시청자가 TV를 켜는 순간에 특정 시점을 기준으로 카운터를 재계산해야 한다. 만일 방송 서버가 TS 패킷 T_i를 카운터 c_j로 암호화하여 전송하였을 경우, 셋톱박스에서 수신된 TS 패킷 T_i를 복호할 때와 카운터의 값이 일치하지 않다면 수신측에서의 정확한 복호를 보장할 수 없다. 방송 서버는 PSI와 같은 방송 정보를 주기적으로 보내게 되는데, 그러한 주기정보를 이용하여 카운터를 동기화할 수 있으며, [그림 6]과 같이 PCR 발생 시점을 기준으로 카운터의 동기를 맞출 수 있다.

즉, 그림에서와 같이 처리하고자 하는 TS 패킷의 헤더를 파싱하여 PCR 값이 존재하는 TS 패킷인 경우 새로운 카운터 값을 생성하고 그렇지 않은 경우 원래의 카운터 값을 1증가시켜 TS 유료부화를 암호화하거나 복호화한다.

2.3 브로드캐스트 키 분배 메커니즘 설계

방송 콘텐츠는 무료로 제공되고, 임의의 사용자들은 콘텐츠가 제공되는 채널에 액세스한 뒤 사용할 수 있다. 이러한 채널 액세스는 가입(subscription) 기반으로 가입하지 않은 사용자들은 콘텐츠를 이용할 수 없어야 한다. 이를 위해 사용자를 인증하고 안전한 방법으로 콘텐츠를 전달할 수 있는 보안 서비스가 필요하다. 방송 서비스에서 개별 사용자를 인증하기 위해서는 point-to-point 서비스에서 사용한 것과 동일한 절차를 이용하는 것이 가능하다. 그러나 사용자 그룹에게 키를 전달하기 위해서는 독자적인 키 관리와 분배 메커니즘이 요구된다[10]. 키 분배 기법은 브로드캐스트 키 전송을 보호하기 위해 point-to-point 기밀성에 의존할 수 있으며, 데이터 보호는 별도의 메커니즘을 요구한다. 본 논문에서 우리는 3GPP2의 브로드캐스트/멀티캐스트 보안 프레임워크[11]에 기술된 키 관리 기법을 기반으로 한 HDTV용 방송 콘텐츠 유통 시스템을 위한 키 분배 메커니즘을 제안한다.



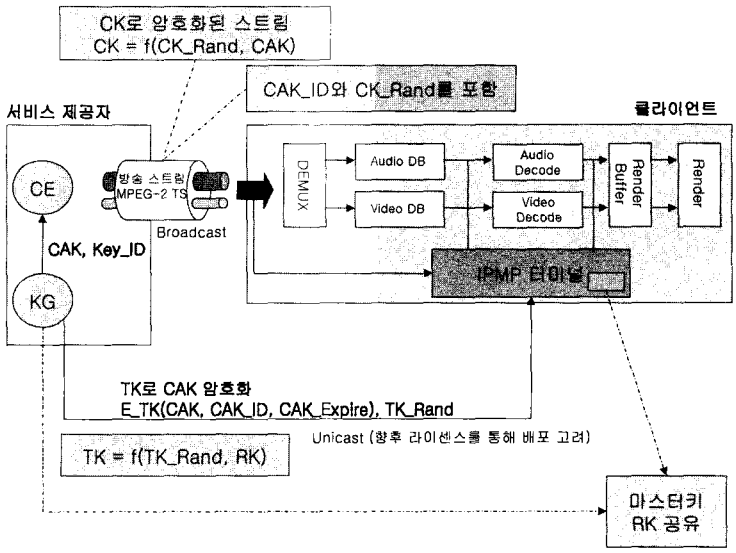
[그림 7] 콘텐츠 키 관리 개요

이를 위해 우리는 사용자의 클라이언트는 내부에 안전한 저장 공간을 가지는 신뢰된 장치로 간주하고, 방송 서비스를 위한 사용자 인증과 권한 부여뿐만 아니라 네트워크 보안은 고려하지 않는다. 방송 콘텐츠를 위한 브로드캐스트 보안에서는 다음의 신뢰 모델을 가정한다. 모든 네트워크 개체들은 그들이 통신하는 다른 네트워크 개체를 신뢰한다고 가정한다. 그리고 네트워크 개체들 간의 통신은 안전하고 모든 네트워크 개체들은 자신의 작업을 정확히 수행한다고 가정한다.

방송 콘텐츠 서비스에서 다루는 주요 위협은 사용자가 특정 콘텐츠 스트림에 대해 허가되지 않고 그 스트림의 내용에 접근하는 것이다. 이 위협을 방지하기 위해 콘텐츠는 클라이언트에게 암호화되어 전달되고 복호화 키는 방송 콘텐츠를 수신하는 것이 허가된(가입된) 클라이언트들에게만 제공된다. 여기서의 주요 초점은 권한 부여를 요구하는 콘텐츠 스트림에 대한 키 관리 기법이다.

콘텐츠는 유일하고 빈번하게 변경되는 CK (Content Key)를 사용하여 암호화된다. 클라이언트들은 동일한 CK를 사용하여 콘텐츠를 복호화 한다. CK는 허가되지 않은 클라이언트들과 CK를 공유하는 "rogue shell"의 영향을 최소화하기 위해 빈번하게 변경되어야 한다. CK는 무선 상으로 전달되지 않으며, CAK(Channel Access Key)와 암호화된 콘텐츠와 함께 브로드캐스트 되는 난수로부터 클라이언트에 의해 유도된다.

클라이언트는 필요한 CAK 값을 복호화하기 위해 서비스 제공자와 마스터 키 RK(Registration Key)를 사전



〔그림 8〕 브로드캐스트 키 분배 흐름도

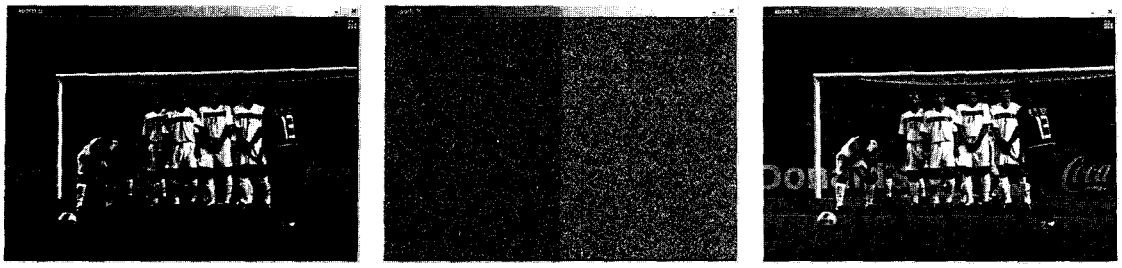
에 공유해야 한다. TK(Temporary Key)는 서비스 제공자에 의해 RK로부터 유도되고 CAK를 암/복호화하기 위해 사용된다. CAK는 서비스 제공자에 의해 암호화되어 클라이언트에게 전달된다. 이것은 서비스 제공자와 클라이언트간의 안전한 유니캐스트 전송에 의해 전달될 수도 있고, 또는 클라이언트가 라이센스를 획득함으로써 얻을 수 있다. 이것은 서비스 제공 시나리오에 따라 달라질 수 있다. 동일한 CAK가 특정 채널에 가입한 모든 사용자에게 제공되고, 미리 정의된 시간동안 유효하다. 클라이언트가 암호화된 CAK를 획득하면, CAK를 복구하여 콘텐츠 스트림을 복호화하기 위해 필요한 CK를 계산한다. 미리 제공된 정확한 RK를 가진 클라이언트만이 CAK를 복구할 수 있다.

〔그림 8〕은 HDTV용 방송 콘텐츠 유통을 위한 제안된 키 분배 메커니즘의 간략한 흐름도를 나타낸다. 먼저 서비스 제공자와 클라이언트는 RK를 공유하고 있다고 가정한다. RK의 공유는 CAS의 스마트카드를 이용한 비밀키 전송 등을 활용한다. 서비스 제공자의 KG(Key Generator) 모듈이 CAK를 생성하고, 식별자 CAK_ID와 만료 시간 CAK_Expire를 관련시킨다. KG 모듈은 CE(Content Encryptor) 모듈에게 CAK와 CAK_ID, CAK_Expire를 전달한다.

CE는 CK_Rand를 랜덤하게 생성한 후 유사랜덤함수(pseudo-random function) f를 이용하여 CK=f(CK_Rand, CAK)를 유도한다. CE는 CK를 사용하여 콘텐츠를 암호화하여 클라이언트에게 전송한다. 이때 CE는 암호화된 콘텐츠와 함께 CAK_ID와 CK_Rand를 전달한다. 클라이언트는 암호화된 콘텐츠를 수신하면 다음과 같이 동작한다. 먼저 암호화된 콘텐츠와 함께 전달된 CAK_ID를 확인하여 이전에 수신된 콘텐츠로부터 변경되지 않았다면 해당되는 CAK를 계속 사용한다. 클라이언트는 콘텐츠와 함께 전송된 CK_Rand와 CAK를 이용하여 CK를 유도한 후, 콘텐츠를 복호화 한다.

만약 CAK_ID가 변경되었다면 클라이언트는 서비스 제공자로부터 CAK를 새로 전송받아야 한다. 이 과정은 클라이언트와 서비스 제공자의 KG 사이에 안전한 유니캐스트 전송을 통해 이루어질 수 있고, 또는 클라이언트가 DRM의 라이센스 서버에 접속하여 새로운 CAK를 포함한 라이센스를 획득할 수도 있다. CAK는 정당한 클라이언트 외의 다른 개체에 의해 수신되는 것을 방지하기 위해 암호화되어야 한다. KG에 의해 생성된 임시 키 TK를 요구한다. 유니캐스트 전송을 이용하는 경우, 클라이언트가 KG에게 CAK Request를 하며, KG는 CAK를 암호화하여 E_{TK}(CAK,CAK_ID, CAK_Expire), TK_Rand를 클라이언트에게 전송한다. 여기서 TK는 KG가 랜덤하게 생성한 TK_Rand와 RK를 이용하여 유도된다.(TK=f(TK_Rand, RK)) CAK Request는 마스터 키 RK에 의존하는 인증 정보를 포함할 수도 있다.

제안된 키 분배 메커니즘은 기존의 IPMP 터미널 구조를 그대로 활용하여 콘텐츠 키를 브로드캐스팅할 수



(a) 원본 데이터 (b) 암호화된 데이터 (c) 복호화된 데이터

〔그림 9〕 MPEG-2 TS 파일에 대한 시뮬레이션

있는 구조이다. 현재 방송 서비스에서 콘텐츠의 불법 시청을 막고 유료 채널 수신 서비스를 제어하기 위하여 방송 콘텐츠를 스크램블링 하여 전송하고 방송 단말에서는 스마트카드의 키 정보를 이용하여 디스크램블링을 수행하는 CAS 시스템으로 충분하다. 그러나 방송 콘텐츠가 디지털화 되면서 하드디스크를 이용한 콘텐츠 저장, 인터넷 접속, 그리고 인터액티브 방송 서비스 등 다양한 방송 서비스가 제공될 것으로 예상된다. 그러므로 현재의 CAS 만으로는 이를 충분히 제어하기에 역부족이다. 또한 기존의 IPMP 터미널과 CAS 시스템 상에서의 상호운용성을 보장해야 한다. 이러한 환경에서 제안 알고리즘은 HDTV용 방송 콘텐츠 키 분배를 효율적으로 제공하고 기존의 셋톱박스에 적용된 IPMP 터미널간의 상호호환성을 제공한다.

Ⅳ. 시스템 구현

본 시스템은 Windows XP 환경에서 C++, MFC, DirectX를 이용하여 구현하였다. TS 패킷은 TS 헤더와 유료부하로 구성되고, 유료부하에는 PES 패킷이 포함된다. TS의 시작은 sync_byte '0x47'로 시작하므로 이것을 파싱한 뒤, 해당 PID를 이용하여 원하는 채널 정보를 추출한다. 추출된 정보는 3장에서 정의된 시스템의 형태로 복호화해서 플레이어 모듈로 전송하게 된다. 이때 복호화 되어 전송되는 시점은 기존의 IPMP 터미널에서 전송 받은 제어지점(control point)으로 설정되므로 안전한 콘텐츠의 이용 및 불법 복제 방지를 가능하게 한다. 그리고 키 분배를 위하여 RK는 사전에 콘텐츠 전송 서버와 플레이어 간에 안전하게 공유된 정보를 이용한다. 공유된 RK로부터 콘텐츠와 함께 전송된 CK_Rand와 추출된 CAK를 이용하여 암호화된 콘텐츠를 복호화 하였다. 키 공유를 위한 CAK 정보는 향후 라이센스 서버에서 라이센스 파일로서 전송 가능할 것이다. 〔그림 9〕는 제안한 CTR 모드를 이용하여 TS를 암호화한 후 복호되어 재생되는 화면을 나타내고 있다.

Ⅴ. 결 론

본 논문에서는 최근 이슈가 되고 있는 디지털방송 콘텐츠와 관련하여 저작권 보호를 위한 암호화 툴팩에 관한 시스템 및 적용 가능한 암호 메커니즘을 제안하였다. 본 연구는 기존의 IPMP 터미널이 적용된 수신기에서 다양한 콘텐츠를 안전하게 이용하고, 사용자 환경에서 다양한 제어 포인트를 가지도록 구성하면서 쉽게 이용할 수 있도록 적응적이고 유효한 알고리즘 및 기술을 제안한다. 또한 제안된 툴팩은 MPEG 시스템을 변경하지 않고 인코더/디코더에 적용될 수 있으므로 다양한 애플리케이션에 이용 가능할 것이다. 향후 연구계획으로는 현재 MPEG2 TS에 대하여 제한적으로 지원되는 시스템을 ES와 PS로 확장하여 완전한 방송 콘텐츠 저작권 보호 시스템 연구가 진행되어야 할 것이다.

참고문헌

〔1〕 OpenCableTM POP Copy Protection System, Cable Television Lab., 2001

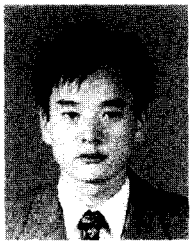
〔2〕 OpenCableTM Interface Speifications: OC-SP-CCCP-IP-C01-050331, http://www.opencable.com/downloads/specs/OC-SP-CCCP-IF-C01-050331.pdf

〔3〕 유시룡 외, MPEG 시스템, 대영사, 2002.

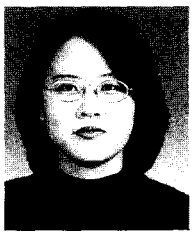
〔4〕 Michael Orzessek, Peter Sommer, ATM & MPEG-2: integrating digital video into broadband networks, Prentice-Hall, Inc., Upper

Saddle River, NJ, 1997
[5] H.Sun et. al., Digital Video Transcoding for Transmission and Storeage, CRC Press, 2005
[6] Digital Transmission Content Protection Specification Vol.1, 5C, 2004
[7] Digital Media Project(DMP), http://www.chiariglione.org/
[8] H. Lipmaa, P. Rogaway, D. Wagner, "Comments to NIST concerning AES Modes of Operation: CTR-Mode Encryption" Symmetric Key Block Cipher Modes of Operation Workshop, 2000, http://csrc.nist.gov/CryptoToolkit/modes/workshop1/papers/lipmaa-ctr.pdf
[9] J. Daemen and V. Rijmen. The Design of Rijndael: AES —- the Advanced Encryption Standard. Springer-Verlag, 2002. ISBN: 3540425802
[10] Amos Fiat and Moni Naor, "Broadcast Encryption", Advances in Cryptology: CRYPTO 1993 (LNCS 773), pp. 480-491, 1993
[11] 3GPP2 S.P0083 Version 1.0, "Broadcast-Multicast Service Security Framework", 16 October, 2003

〈著者紹介〉



이 진 흥 (Jin-heung Lee) 정회원
1998년 2월: 동서대학교 정보통신공학과 졸업
2000년 2월: 부경대학교 전자계산학과 석사
2002년 3월~현재: 부경대학교 정보보호협동과정 박사과정
2004년 9월~현재: 모빌리존 대표
<관심분야> DRM, Digital Fingerprinting, 정보보호응용



이 혜 주 (Ju-hye Lee) 정회원
1994년 2월: 부경대학교 전자계산학과 졸업
1997년 2월: 부경대학교 전자계산학과 석사
2000년 2월 : 부경대학교 전자계산학과 박사
2000년~2001년: 한국정보통신대학교 박사후 연구과정
2001년~2005년: 한국전자통신연구원 디지털방송연구단 선임연구원
2005년~2006년: 경성대학교 초빙교수
2006년 10월~현재: 모빌리존 개발팀장
<관심분야> 디지털 콘텐츠 보호 및 관리, 워터마킹, 멀티미디어 처리 기술

신 상 욱 (Sang-uk Shin) 정회원
1995년 2월부경대학교 전자계산학과 졸업
1997년 2월부경대학교 전자계산학과 석사
2000년 2월부경대학교 전자계산학과 박사
2000년 4월~2003년 8월한국전자통신연구원 선임연구원
2003년 9월~현재부경대학교 전자컴퓨터정보통신공학부 조교수
<관심분야> 암호 이론, 이동/모바일네트워크 정보보호, 멀티미디어콘텐츠보호