OTP를 이용한 IPTV 콘텐츠 보호 및 인증 시스템 설계

Design on Protection and Authentication System of IPTV Contents using OTP

김대진, 최홍섭
대진대학교 전자공학과

Dae-Jin Kim(sampoo00@hanmail.net), Hong-Sub Choi(hschoi@daejin.ac.kr)

요약

광대역 네트워크의 발달과 함께 멀티미디어 산업의 발달은 IPTV와 같은 디지털 콘텐츠 시장의 확산을 가져오고 있다. 이러한 배경 속에서 IPTV 서비스는 일반화, 대중화되었으며, 이 콘텐츠에 대한 보안 및 인증시스템도 강조 되고 있다. 따라서 콘텐츠에 암호화 기능을 수행하여 콘텐츠를 보호하고 사용권한을 제어함으로써 인증된 사용자만이 정당한 서비스를 이용할 수 있는 시스템이 필요하다. 기존의 보안 및 인증 시스템은 수신제한시스템(CAS)과 DRM(Digital Right Management)기술을 같이 접목하여 각각이 가지는 장점을 이용하였으나 비용이 많이 들고, 복잡하며, HW를 동반해야 하는 단점을 가진다. 이러한 단점을 보안하기 위해서 본 논문에서는 OTP(One Time Password)를 이용한 IPTV 콘텐츠 보호 및 인증 시스템을 제안한다. OTP 암호키에 의해서 암호화된 콘텐츠를 데이터 분산기술을 이용하여 전달한다. 이 때 분산서버로부터 전달받을 다른 셋탑박스의 OTP 암호키와 배타적 논리합을 통하여 전달할 셋탑박스의 OTP 암호화된 콘텐츠를 재구성하여 전달한다. 결국 다운로드 받은 콘텐츠는 OTP 암호키로 암호화된 콘텐츠이므로 재배포시 보안에 강점을 가진다. OTP는 이중 인증요소를 이용한 암호화 기법으로 보안성이 뛰어나고 SW적으로 적용 가능하여 비용절감에 효과적이며 구현이 간단하여 개발시간을 단축할 수 있다. 이 논문에서는 IPTV 서비스에 적합한 새로운 콘텐츠 보호 및 인증 시스템 모델을 제안한다.

■ 중심어 : | IPTV | 콘텐츠보호 | 인증 | OTP |

Abstract

While the broadband network and multimedia technologies have been developing, the commercial market of digital contents also has been widely spreading with recently starting IPTV. As the IPTV services are getting to be generalized and popularized, the contents protection and authentication system tends to draw more attentions. So we need a system that can protect contents and allow only authenticated person to use right service by controling user authority and using content encryption. Until now, the conventional protection and authentication system is taking advantages of merits both in CAS and DRM. But the weak point of this system are in high costs, complexity and using HW. For resolving these problems, in this paper, we proposed IPTV contents protection and authentication system using OTP. When we transmit the content encrypted by OTP key using contents delivery technology, we operate XOR with contents using another settop-box's OTP key which was transmitted from distribution server. And contents are reconstructed and transmitted to the settop-box. In the end, downloaded content are encrypted by OTP key and are superior in content protection when contents redistribution. Since OTP use double-authentication elements in encryption process, this method is excellent in content protection. And it is very effective in cost aspect because it could be implemented by SW program. Another benefit is that we can shorten the development time period. In this paper, we propose and find its possibility as a new content protection and authentication method suitable for IPTV services.

■ keyword : | IPTV | Content Protection | Authentication | OTP |

* 본 연구는 2009년도 대진대학교 학술연구비지원에 의한 것임.
접수번호 : #090525-003
접수일자 : 2009년 05월 25일
심사완료일 : 2009년 07월 03일
교신저자 : 최홍섭, e-mail : hschoi@daejin.ac.kr

I. 서 론

컴퓨터와 인터넷의 발달은 정치, 경제, 사회, 문화 등 전 영역에 많은 변화를 가져오고 있다. 이 중에서도 인터넷의 대중화는 수 많은 콘텐츠를 양산하게 되었으며, 이와 관련된 음성 및 영상분야의 기술도 급속도로 발전하고 있다. 특히 IPTV(Internet Protocol TV) 서비스는 TV와 PC의 장점을 융합시켜 멀티미디어 콘텐츠를 보다 쉽고, 편리하게 제공하여 시청자의 미디어에 대한 욕구를 만족시키고 있다. 최근, IPTV 서비스 구현을 위한 노력이 통신사업자, 포탈사업자 및 연구기관 등에서 이루어지고 있으며, VoD(Video On Demand) 및 양방향 중심의 IPTV 서비스가 상용화되고 있다[1-3]. 또한 IPTV 관련 법규가 시행되면 실시간 방송을 포함한 IPTV 서비스가 제공될 예정이다.

이러한 배경 속에서 IPTV는 다양한 적용 분야에서 연구 되고 있다. 그러나 이러한 콘텐츠 서비스는 보안에 대한 표준이나 모델이 정립되지 않아 여러 가지 다양한 기술들이 적용되고 있다. 그 대표적인 콘텐츠 보안 기술로는 DRM(Digital Right Management)과 수신제한시스템(CAS : Conditional Access System)이 있다. Yingjiu Guo[4] 등은 IPTV 시스템에 DRM 프로토콜(Protocol)을 정의하고 적용하였으며, Tianpu Jiang[5] 등은 디지털 방송에서 수신제한시스템을 적용할 때 키(Key) 분배시 계층적 접근을 이용한 효율적인 암호화 구조를 설계하였다. Zhang Hua[6] 등은 IPTV 시스템에 DRM과 수신제한시스템 각각 적용하였을 때 구현 원칙을 설명하고 비교 정리하였다. 그러나 이러한 방식들은 각각 한가지씩만 사용하였을 때 약점을 드러내고 있고, 같이 적용 시에는 시스템 구현 시 복잡하고 비용이 많이 드는 단점을 가지고 있다. 따라서 본 논문에서는 OTP(One Time Password) 기술을 이용하여 다운로드 기반의 IPTV 시스템에 적합한 새로운 인증 기법을 제안한다. 논문의 구성은 2장에서 다운로드 기반의 IPTV 시스템 모델인 사용자 맞춤형 채널관리 IPTV에 대하여 설명하고 기존의 콘텐츠 보안기술 및 IPTV의 적용을 알아본다. 3장에서는 OTP를 이용한 새로운 콘텐츠 보안 및 인증 기술을 알아보고 IPTV 시스템에 적용해 본다. 4장에서는 OTP를 이용한 IPTV 시스템 구현 결과를 설명하고 기존 보안 및 인증 기법과의 성능비교를 하였으며, 마지막으로 5장에서 결론을 맺었다.

II. 기존의 IPTV 시스템과 콘텐츠 보안기술 적용

1. 사용자 맞춤형 채널관리 IPTV

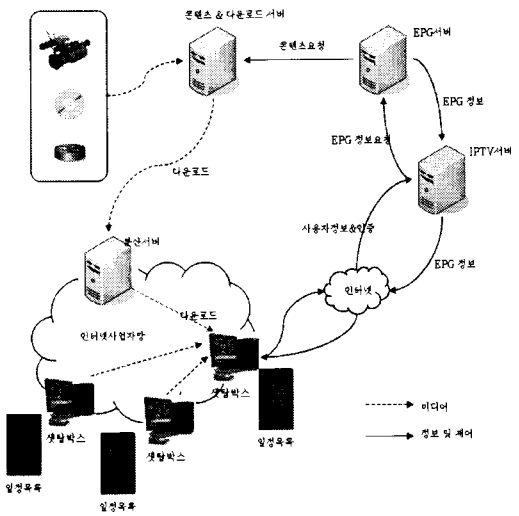


그림 1. 사용자 맞춤형 채널관리를 이용한 IPTV 시스템

10Mbps 이상의 HD급의 고화질 콘텐츠가 풍부해지고 다양한 콘텐츠 서비스를 요구하는 업체들이 점점 많아짐에 따라 실시간 서비스를 하기에는 비용 면에서나 자원 면에서 중소업체에게 부담으로 작용한다. 또한 네트워크를 통하여 10Mbps이상의 콘텐츠를 재생한다면 로컬에 있는 콘텐츠를 재생하는 것보다 높은 사양의 셋탑박스가 필요하다. 이것도 서비스 업체에게 비용 부담을 준다. 만약 적은 규모의 기반시설을 이용하여 HD 서비스를 한다면 서비스 안정도가 떨어지고 방송이 끊기는 등의 방송사고가 일어날 수 있다.

사용자 맞춤형 채널관리를 이용한 IPTV 시스템은 [그림 1]에서 보는 바와 같이 인코딩이나 이미 만들어진 디지털 콘텐츠를 콘텐츠 채널 서버에 등록을 하고

표 1. 수신제한시스템과 DRM 비교분석[2]

구 분	수신제한시스템			DRM		비고
적용분야		과거(199x~)	현재	과거(199x~)	현재	IPTV 콘텐츠 보호영역에 접전
	전송망	방송망(위성,케이블,지상파)	방송/인터넷 망	인터넷 망	인터넷/방송 망	
	서비스	방송형 채널서비스 VoD서비스	양방향서비스 분야에 진출	VoD 등 각종 디지털 서비스(문서 등...)	방송형 채널서비스 분야에 진출	
콘텐츠 보호방식	- 콘텐츠 보호 : 스크램블링/디스크램블링 - ECM/Verifier/SC : HW와 SW 기반 암/복호화 - AES 128 bit 사용 - 업데이트 주기에 따라 계속 다른 라이센스 키 사용			- 콘텐츠 보호 : 암호화/복호화 - 라이센스 보호 : S/W 기반 암/복호화 - AES 128 bit 사용 - 1개의 라이센스 키로 암/복호화		암호알고리즘은 동일하나, 구현방식 차이
사용권한 전송방식	암호화된 콘텐츠를 사용권한 및 복호키와 함께 멀티케스트 전송하여 Verifier와 스마트카드에 의해 복호화			사용자의 콘텐츠 재생시점에 사용권한 및 복호키 전송		
제공가능	- 보안기법을 통한 콘텐츠 보호 및 사용자 수신제한 - 가입자 시청 자격관리(권한부여/갱신/삭제 등) - 패키지 상품구성 가능 및 과금, 시청이력 조회용이 - 녹화방지, 수신기 제어 등 관련 부가기능 풍부			- 보안기법을 통한 콘텐츠 보호 - 시스템 자체 제공 가능한 부가기능 미약		
장점	- 다양한 비즈니스 모델 수용가능 - H/W 및 S/W 기반 구현으로 콘텐츠 보안성 우수 - 검증된 보안시스템으로 디지털 콘텐츠 확보용이 - DVB 및 ATSC 표준 준수로 타 시스템과 연동 우수			- 인터넷에 최적화된 암/복호화 방식 - S/W 구현방식으로 해킹 시 신속히 대처 - 자체 솔루션 확보로 기술종속 탈피 및 다양한 BM(PVR, 다운로드 형 VoD 등)에 적용		
단점	- DRM에 비해 시스템구축 가격이 고가(로열티 및 스마트카드 비용 등) - 스마트카드 해킹시 카드 교체 및 배송 비용 증가			- S/W 방식의 단말 암호화로 보안성 취약 - 표준 DRM 솔루션 부재로 호환성 부족 - 실시간 방송 콘텐츠의 보안성 미흡		
적용사례	DirectTV, BskyB, Skylife/ Cox, TWE/BBTV, VNL 타 매체, 국내 위성, 케이블, MegaTV 사례 등. 2. 콘텐츠 보안기술의 필요성			유무선 콘텐츠 서비스 보안에 다수 적용 (MegaTV, KTF 도시락, SKT 멜론 등)		

개인이나 사업자가 EPG(Electronic Program Guide) 서버를 통해서 사업장에 맞는 사용자 맞춤채널을 구성한다. 그 후 채널에 해당하는 콘텐츠를 셋탑박스에 다운로드 받는다. 파일 다운로드는 그리드 분산(Grid Delivery)이나 P2P(Peer to Peer)분산과 같은 데이터 전송시스템을 이용하여 네트워크 자원을 최소화 할 수 있다. 또한 사용자 맞춤채널에 등록된 다운로드 콘텐츠는 일정에 맞추어 각 사업장에 맞는 서비스를 할 수 있다. 결국 사업장에 원하는 HD급의 콘텐츠를 원하는 시간에 서비스를 함으로써 고객의 만족도를 좀 더 높일 수 있다[7].

2. 콘텐츠 보안기술의 필요성

채널관리 IPTV는 사용자가 원하는 콘텐츠를 원하는 시간에 원하는 프로그램을 시청할 수 있는 사용자 맞춤형 시스템이다. 그러나 콘텐츠 보안, 사용자 인증, 콘텐츠 재배포, 과금 등에 문제점을 가지고 있다. 서버의 콘텐츠는 방화벽 등에 의해서 어느 정도 보안이 이루어질 수 있으나, 아이디/비밀번호 노출시 개인 정보의 노출 및 불법사용에 문제점이 생기고, 셋탑박스내에 있는 콘텐츠에 대해서는 불법유통과 같은 문제점이 노출된다. 따라서 이러한 약점을 해결하기 위한 콘텐츠 보안기술이 필요하다.

3. 기존의 콘텐츠 보안기술

3.1 수신제한시스템(CAS)

수신제한시스템은 암호화 기술을 이용하여 콘텐츠에 대하여 스크램블을 걸고 스마트카드나 케이블 카드를 이용하여 해당 가입자만이 사용할 수 있도록 만든 콘텐츠 보안 기술이다. 콘텐츠 보호방식에 있어서는 업데이트 주기마다 다른 라이센스 키를 제공하여 다양한 라이센스 키를 적용할 수 있다. 또한 스마트카드를 적용하여 다단계 암호화 구조를 사용할 수 있다. 따라서 보안기법을 통한 콘텐츠 보호 및 사용자 수신을 제한 할 수 있고 여러 가지 부가 기능이 가능하다. 예를 들면 가입자에 대한 시청 자격관리를 통하여 가입자 마다 시청할 수 있는 채널 구분이 가능하고 이를 상품화하여 패키지 상품구성이 가능하다. 또한 녹화방지 및 수신기 제어 등 관련 부가기능이 다양하다. 이러한 기능 이외에도 다양한 비즈니스 모델 수용이 가능하고 H/W 및 S/W기반의 구현으로 콘텐츠 보안성이 우수하여 콘텐츠 수급이 용이하다. 그러나 DRM에 비해 라이센스 가

격이나 스마트카드 비용 등 가격이 높은 단점을 가진다. 수신제한시스템은 콘텐츠의 관점에서 보면 강점을 가지고 있으나 개인정보에 대해서는 약점을 가지고 있다. 셋탑박스는 콘텐츠 인증을 위해 개인정보를 이용하는데 이때 개인정보에 대한 보안성이 취약하다. 셋탑박스를 통하여 개인정보가 누출될 가능성이 있다. 따라서 서비스 업체에서는 콘텐츠 보호뿐만 아니라 개인정보에 대한 보안이 더욱 요구되어 진다.

3.2 DRM

DRM은 양방향 통신이 가능한 인터넷 기반의 기술로서 디지털 콘텐츠의 데이터를 암호화해 인증된 사용자 및 단말기에서만 풀 수 있도록 한다. 콘텐츠의 자유로운 복제는 허용하되 불법 사용은 철저히 막는 것이 DRM의 목적이다. DRM은 단일 라이센스 키를 이용한 S/W 기반의 암호화 기술이며 콘텐츠 재생 시점에 사용권한 및 복호키를 전송한다. 콘텐츠 접근 및 배포에 대한 제어가 용이하고 S/W 기반의 기술이기 때문에 비용이 적고 해킹 시 신속히 대처할 수 있으나 수신제한시스템에 비해서는 보안성이 약하다. 현재 다양한 표준 규격이 혼재하고 있으며 DRM 표준 제정이 어려운 상태다. [표 1]은 수신제한시스템과 DRM을 비교 분석한 것이다[2].

4. 기존의 콘텐츠 보안기술의 적용

IPTV 서비스가 활성화됨에 따라 디지털 콘텐츠의 불법적인 유통이 더욱 활성화 될 것이고 다양한 멀티미디어 디바이스(PMP, MP3, PDA, 컴퓨터 등)의 일반화는 콘텐츠를 아무런 제약 없이 사용할 수 있게 할 수 있다. 따라서 콘텐츠에 암호화 기능을 수행하여 콘텐츠를 보호하고 사용권한을 제어함으로써 인증된 사용자만이 정당한 서비스를 이용할 수 있는 시스템이 필요하며, 이를 위해 수신제한시스템과 DRM 기술이 적용된다.

초기에는 이들 방식이 콘텐츠 각각에 대한 보호 시스템으로 사용하였으나 다음과 같은 취약점을 가지고 있다. 수신제한시스템은 이미 다운로드 받은 콘텐츠에 대해서는 저작권 보호가 이루어지지 못하고, 또한 DRM은 실시간 방송 시 과금이 어렵기 때문에 이들 각각의 단점을 보안하고자 두 방법을 함께 사용하였다. IPTV로 콘텐츠를 다운로드 받거나 사용하려고 할 때 수신제한시스템을 통하여 인증 절차를 수행하고, 터미널 내에 있는 콘텐츠를 다른 디바이스로 이동할 때는 DRM을 사용하는 인증시스템을 만드는 것이다.

III. 제안하는 OTP를 이용한 IPTV 콘텐츠 보호 및 인증 시스템

1. OTP(One Time Password)

컴퓨터나 네트워크를 통하여 유통되는 정보 및 주요 데이터를 보호하는 정보 보안의 가장 기초적인 요소는 인증이다. 인증 방법으로는 사용자 아이디/비밀번호, 복잡한 질의응답, 생체 인식, 스마트카드 이용 등 다양한 방법들이 존재한다. 그 중에서도 최근에 가장 주목받고 있는 솔루션이 OTP 시스템이다. OTP를 정의하면 사용자가 인증을 받고자 할 때마다 매번 새로운 비밀번호가 자동으로 생성되는 보안 시스템으로, 한번 사용하고 버리는 일회용 비밀번호를 말한다. 최근 고도화되고 있는 해킹, 패스워드 유출과 같은 위험의 증가로 정보보호 기능이 위험에 노출되고 있다. 키로깅(Key-Logging), 스니핑(Sniffing), 피싱(Phishing) 등 비밀번호 탈취를 위한 여러 방법들이 존재하고 있고 이를 방어하기 위한 방화벽 등 네트워크 보안이 이루어지고 있으나 아이디와 비밀번호가 노출되면 결국은 인증의 실패를 가져오게 된다. 따라서 OTP 시스템은 인증 방식으로 더욱 부각되고 있다.

OTP의 특성을 살펴보면 이중요소 인증수단, 동적(dynamic) 비밀번호, OTP 생성매체 이다. 이중요소 인증수단은 이용자 본인이 가지고 있는 OTP 생성매체에 의하여 생성된 비밀번호로 사용자를 인증하는 이중요소 인증(Two-Factor Authentication)방식을 말한다. "알고 있는 것(Something you know)"과 "갖고 있는 것(Something you have)"를 동시에 사용하는 방식으로 정적인 비밀번호와 같이 한 가지 요소만으로 인증 받는 단일요소인증에 비해 높은 수준의 보안을 유지할 수 있다. 동적 비밀번호는 OTP 생성기를 통하여 필요한 시

점에 발생되고 매번 다른 번호를 생성하는 것을 말하며 한번 생성되면 다시 사용할 수 없기 때문에 높은 보안성을 유지할 수 있다. OTP 생성매체는 OTP를 생성할 수 있는 기능을 가진 장치를 말하며, 흔히 OTP 토큰(Token)이라고 한다. 별도의 OTP 토큰을 통해서만 비밀번호가 생성되며, 기기에 대한 복제 및 오용이 불가하다. 현재 사용되고 있는 OTP를 이용한 일반적인 인증 절차는 [그림 2]에 나타낸다.

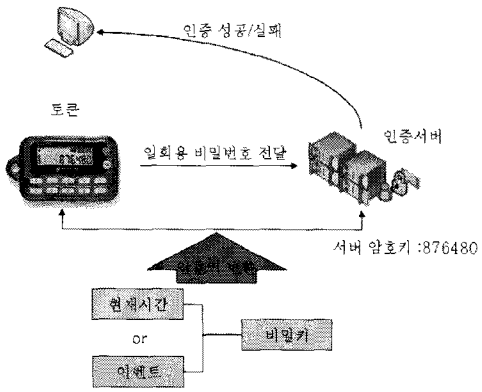


그림 2. OTP를 이용한 인증 절차

OTP를 이용한 인증방식에는 시간동기화 방식과 이벤트 방식이 있다. 시간동기화 방식의 경우 토큰과 인증 서버 사이에 특정 비밀키를 공유하고 이 비밀키와 현재 시간을 조합하여 새로운 암호키로 변환한다. 특정한 시점에 OTP 토큰과 서버 내에서 동일한 키와 시간을 이용하여 동일한 일회용 비밀번호를 생성하여 사용자 인증에 사용한다. 이벤트 방식의 경우 시간을 이용하지 않고 인증을 한 횟수를 이용하여 일회용 비밀번호를 생성하는 점에서 차이가 있다. 마찬가지로 한번 인증에 사용한 일회용 비밀번호가 다시 사용할 수 없도록 제약한다.

2. OTP를 이용한 IPTV 시스템

기존의 IPTV의 인증시스템으로 DRM과 수신제한시스템을 이용하였다. 본 논문에서는 두 방법 이외에 IPTV 시스템에 적용할 수 있는 OTP를 이용한 새로운 인증 시나리오를 제안하고자 한다. DRM은 S/W 방식의 단일 암호화로 보완성이 취약하고 수신제한 시스템은 시스템 구축 시 로열티 및 스마트 카드비용 등으로 비용이 증가되는 단점을 보인다. 그러나 OTP를 이용한

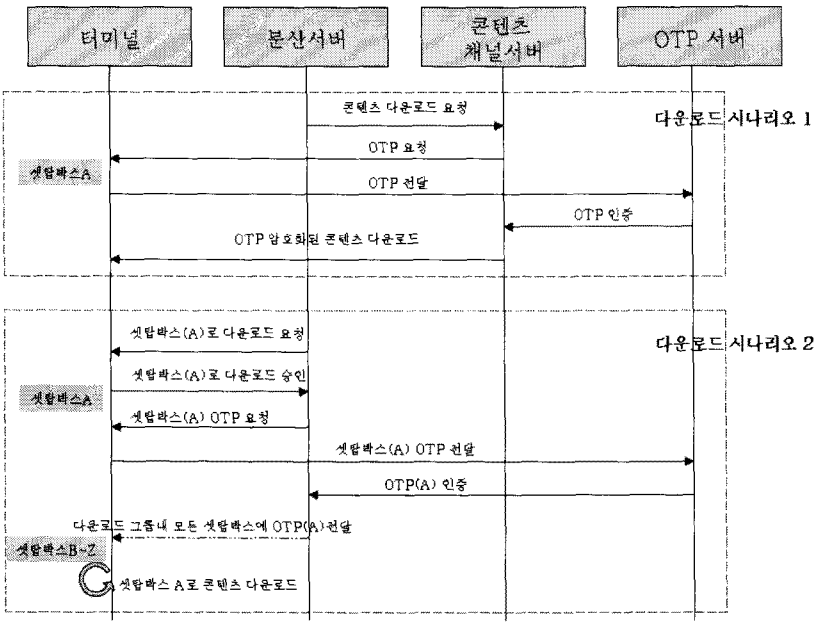


그림 3. OTP 암호화를 이용한 IPTV 시스템 데이터 흐름도

IPTV 시스템은 기존 인증시스템의 단점을 보완 할 수 있다. OTP는 이중인증요소를 이용한 암호화 기법으로 보안성이 뛰어나고 셋탑박스에 OTP S/W를 탑제함으로써 비용절감 효과가 있다.

[그림 3]에서는 OTP 암호화를 이용한 IPTV 시스템 데이터 흐름도를 나타낸다. 기존 방식에서 사용자 맞춤형 채널정보를 요청 및 전달한 후에 다운로드하는 방식에 OTP 콘텐츠 보안이 추가된다. 우선 해당 콘텐츠를 가지고 있는 셋탑박스의 그룹을 다운로드 그룹이라 정의한다. OTP를 이용한 다운로드에서는 다운로드 그룹 내에 이미 다운로드를 받은 콘텐츠가 없는 경우 다운로드 시나리오1을 따른다. 분산서버는 콘텐츠 채널서버에 다운로드를 요청하고 채널서버는 셋탑박스에 OTP를 요청한다. 셋탑박스는 OTP 서버에서 생성한 OTP를 전달하고 인증을 거쳐서 채널서버는 OTP 암호화된 콘텐츠를 다운로드 한다. OTP 키를 이용한 암호화 방식은 배타적 논리합(XOR)을 이용한다. 배타적 논리합은 똑같은 키값을 이용하여 연산을 두 번하면 원본 값을 그대로 가지는 특성을 가지고 있다. 예를 들어 원본이 0011 이고 암호키가 0110인 경우 배타적 논리합을 하면 0101이 나오고 또다시 같은 암호키로 배타적 논리합을 수행하면 원본인 0011을 가지기 때문에 이러한 특징을 OTP 키와 같이 사용하면 콘텐츠 보안시스템에 적용가능하다. [그림 4] 에서는 이러한 특징을 이용한 동영상 스트림 전달과정을 나타낸다.

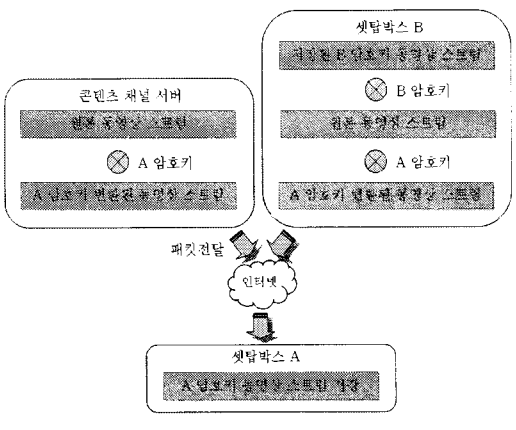


그림 4. 동영상 스트림 전달 과정

다운로드 시나리오2에서는 다운로드 그룹내에 이미 다운로드 받은 콘텐츠가 존재하는 경우이다. 이 콘텐츠는 이미 생성된 OTP 암호키에 의해서 암호화되어 있다. 따라서 다른 셋탑박스로 콘텐츠를 전달하기 위해서는 먼저 저장해놓은 OTP 암호키로 배타적 논리합을 수행하여 원본 동영상 스트림 버퍼를 가지고 셋탑박스 내에 임시 보관한다. 그 후 분산서버로부터 콘텐츠를 전달할 셋탑박스의 OTP 암호키로 다시 배타적 논리합을 통하여 전달할 셋탑박스에 맞는 OTP 암호화된 콘텐츠로 재구성한다. 이와 같은 과정을 통해서 모든 셋탑박스에 암호화된 콘텐츠를 저장하고 재생 시 해당 암호키로 복호화하여 시청할 수 있다. 셋탑박스내에 저장된 콘텐츠는 암호화 되어 있고 OTP 암호키는 셋탑박스 내에서 메모리 관리를 하기 때문에 콘텐츠 재배포시에도 보안에 강점을 가진다.

IV. 구현결과

1. 시스템 구현 환경

IPTV 시스템 구성을 위하여 셋탑박스는 OS (Operation System)로 윈도우즈 비스타(Windows Vista)를, 미디어기술은 WMT(Windows Media Technology)를 이용하였으며, 셋탑박스의 재생기는 다이렉트쇼(DirectShow)를 이용하여 필터(Filter)기반으로 개발하였다. 또한 랜더링의 성능 향상을 위해 VMR9(Video Mixer Render9)를 사용하였다. 재생기 구성시 다양한 압축포멧을 지원하기 위해 코덱필터(CODEC Filter)는 FFDShow 오픈소스를 이용하였으며, Guliverkli 오픈소스를 이용하여 파서필터(Parser Filter)로 사용하였다. 또한 고화질 IPTV 시스템을 구성하기 위하여 720p의 HD 콘텐츠를 사용하였다. 테스트시 비디오는 H.264, 오디오는 MP3 형식의 콘텐츠를 사용하였다. 서버 구성은 분산서버/IPTV 서버/EPG 서버/콘텐츠 채널 서버로 구성되며 테스트 시 각각 PC 한 대씩 각각의 서버 역할을 수행 하였고, 서버간 통신 및 셋탑박스와 통신은 TCP 프로토콜을 이용하여 소켓(Socket) 통신을 하였다. 또한 콘텐츠 채널서버에서 분

산서버로의 데이터 전달에는 ftp 프로토콜을 사용하였으며, 사용자 데이터베이스 구축을 위해 MS-SQL2005를 사용하였다.

표 2. 시스템 구현 환경

시스템 환경	상세내역
OS	-. 윈도우즈 비스타
개발 SDK	-. 다이렉트쇼 -. Platform SDK
기반 기술	-. 다이렉트쇼 필터 -. VMR9
참고소스	-. 파서필터 : Guliverkli -. 코덱필터 : FFDShow
콘텐츠	-. 크기 : 1920x1080 -. 비디오 코덱 : H.264 -. 오디오 코덱 : MP3
컴파일러	-. Microsoft Visual Studio 2008
프로토콜	-. 서버/셋탑박스 통신 : TCP -. 다운로드 : FTP
DB	-. MS-SQL2005

2. 시스템 프로토타입

본 장에서는 Windows 환경 아래서 OTP를 이용한 IPTV 인증시스템을 구현하였다.

OTP는 이중요소 인증을 사용하기 때문에 두 가지 인증요소가 필요하다. 그중에 "알고 있는 것"은 현재시간, "갖고 있는 것"은 셋탑박스의 고유 아이디를 사용한다. 본 생성기에서는 셋탑박스의 고유 아이디와 현재 시간의 덧셈 연산을 통하여 랜덤함수의 시드(Seed)값 구성한다. 이 시드값을 통하여 동일 시점에 셋탑박스마다 고유의 OTP값을 생성할 수 있다.

이러한 과정을 통해서 생성된 셋탑박스의 OTP값은 다운로드 받기 전 암호키로 사용된다. 전송할 콘텐츠 패킷스트림과 OTP 암호키의 배타적 논리합을 통하여 암호화된 새로운 콘텐츠 스트림을 구성한다. OTP 암호키로 변환된 콘텐츠 스트림을 콘텐츠 채널서버나 다른 셋탑박스에 전송하게 된다. 다운로드 완료 후에는 셋탑박스 내에 OTP 암호키로 변환된 콘텐츠가 존재하게 된다. 이 콘텐츠를 IPTV 서비스에 이용하기 위해서는 OTP 복호키를 이용한다. OTP 복호키는 배타적 논리합을 이용하기 때문에 OTP 암호키와 동일하다. 배타적 논리합은 두 번 연산을 통해서 원형의 데이터를 얻을 수 있기 때문이다. 또한 이 콘텐츠는 그 셋탑박스 내에서만 사용 가능하고 다른 멀티미디어 디바이스에 이동되었을 경우에도 OTP 복호키를 알 수 없기 때문에 콘텐츠 유통에 의한 인증관리 면에서 우수하다.

[그림 5]은 지금까지 설명했던 방법을 이용한 셋탑박스 및 IPTV 시스템 구현 화면으로, 현재 재생 화면과 EPG 정보를 같이 나타내어 사용자 편의성을 고려한 UI(User Interface)를 제공한다. 테스트 영상으로는 영화 "우리 생애 최고의 순간"의 한 장면을 사용하였다.

그림 5. 셋탑박스 및 IPTV 재생화면

3. 시스템 성능비교

표 3. 콘텐츠 보안 및 인증 기술의 비교

	DRM + CAS	OTP
보안	128bit 암/복호화	이중인증
보호방식	SW / HW	SW
디바이스	필요(스마트카드 등)	불필요
비용	고비용	저비용
시스템설계	복잡	단순

기존의 콘텐츠 보안 및 인증 기술은 수신제한시스템과 DRM을 결합하여 각각이 가지는 단점을 보안하는 방법을 사용하였다. 그러나 본 시스템은 IPTV 시스템에 OTP를 적용함으로써 하드웨어를 적용하지 않으면서 수신제한시스템과 DRM의 역할이 가능하기 때문에

저비용, 고효율의 보안 및 인증 서비스가 가능하다. 또한 단순히 소프트웨어 서비스 로직을 이용하기 때문에 기존서비스 보다 단순화 할 수 있다. [표 3]에서는 기존의 콘텐츠 보안 및 인증 기술과 제안하는 OTP 방식을 비교하였다.

즉, 기존의 콘텐츠 보안 및 인증 기술은 IPTV에 적용하기 위해서는 수신제한시스템과 DRM를 같이 사용해야만 서로가 가지는 단점을 보안해 줄 수 있지만 OTP 방식에서는 소프트웨어 방식의 고효율, 저비용의 인증 시스템이 가능하다.

V. 결론

IPTV는 TV와 PC의 장점을 융합시켜 멀티미디어 콘텐츠를 보다 쉽고, 편리하게 제공하여 여러 서비스를 상용화하고 있으며, 방송국뿐만 아니라 수많은 콘텐츠 사업자도 IPTV를 이용한 서비스 공급을 원하고 있다. 이러한 환경 속에서 IPTV는 시장에서 점점 보편화, 일반화 되어가고 있다. 또한 상용 서비스에서 IPTV가 제 역할을 하기 위해서는 콘텐츠 보안 및 인증 시스템의 도입이 중요하다. 기존에는 수신제한시스템과 DRM과 같은 보안 및 인증시스템을 사용하였다. 수신제한시스템은 이미 다운로드 받은 콘텐츠에 대해서는 저작권 보호가 이루어지지 못하고, DRM은 실시간 방송 시 과금이 어렵기 때문에 이들 각각의 단점을 보안하고자 두 방법을 함께 사용하였다. 그러나 이 방법은 하드웨어를 동반해야 하기 때문에 비용이 많이 들고 시스템이 복잡하게 된다. 따라서 본 논문에서는 이와같은 단점을 극복할 수 있는 OTP를 이용한 콘텐츠 보호 및 인증 시스템을 제안하였다. OTP 인증시스템은 이중인증요소를 사용하기 때문에 보안성이 뛰어나고 로열티나 스마트카드와 같은 부분을 사용하지 않기 때문에 비용절감에 효과가 있다. 따라서 IPTV 서비스 환경에서 고효율, 저비용의 콘텐츠 보호 및 인증시스템으로 적용할 수 있다.

참 고 문 헌

[1] 홍인화, 이석필, "IPTV의 기술동향", IT Soc Magazine, 제17권, pp.26-34, 2007(3).

[2] 최락권, 송치양, "IPTV 서비스 구현을 위한 핵심 기술 연구", 전자공학회지, 제35권, 제3호, 2008(3).

[3] 김대진, 최홍섭, "휴대용 멀티미디어 디바이스를 위한 TPO(Time, Place, Occasion)-Shift 시스템 설계에 대한 연구", 한국컴퓨터정보학회논문지, 제14권, 제2호, pp.9-16, 2009(2).

[4] G. Yingjiu, L. Chuang, Y. Hao, and Z. Zhang, "Design and Analysis of IPTV Digital Copyright Management Security Protocol," ISPACS, pp.554-557, 2007(11).

[5] J. Tianpu, Z. Shibao, and L. Baofeng, "Key Distribution Based on Hierarchical Access Control for Conditional Access System in DTV Broadcast," IEEE Transactions on Consumer Electronics, Vol.50, No.1, 2004(2).

[6] H. Zhang, C. Chen, L. Zhao, S. Yang, and L. Zhou, "Content Protection for IPTV-current state of the art and challenges," IMACS, pp.1680-1685, 2006(10).

[7] 김대진, 최홍섭, "사용자 맞춤형 채널 관리를 이용한 다운로드 기반의 IPTV 시스템 제안", 한국디지털콘텐츠학회논문지, 제10권, 제1호, pp.61-71, 2009(3).

저 자 소 개

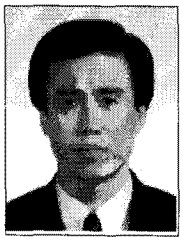
김 대 진(Dae-Jin Kim) 정회원

- 1998년 2월 : 대진대학교 전자공학과 졸업(공학사)
- 2000년 2월 : 동국대학교 전자공학과 졸업(공학석사)
- 2008년 2월 : 대진대학교 전자공학과 수료(공학박사)

- 2000년 ~ 2003년 : 한빛소프트 주임연구원
- 2003년 ~ 2007년 : 모토로라 코리아 전임연구원
- 2007년 ~ 2008년 : 아이비인터넷 부장
- 2008년 ~ 현재 : 피어컴(미디어웹) 선임연구원

<관심분야> : 저작권 보호, 멀티미디어 시스템, 디지털 콘텐츠, 멀티미디어 검색, IPTV

최 홍 섭(Hong-Sub Choi) **정회원**



- 1985년 2월 : 서울대학교 전자공학과 졸업(공학사)
- 1987년 2월 : 서울대학교 전자공학과 졸업(공학석사)
- 1994년 2월 : 서울대학교 전자공학과 졸업(공학박사)
- 1995년 ~ 현재 : 대진대학교 전자공학과 정교수

<관심분야> : 통신 및 신호처리, 음성인식, 멀티미디어 시스템, IPTV