情報保護學會論文誌
第20卷 第4號, 2010. 8

# IPTV 시스템에서의 효과적인 콘텐츠 보호를 위한 일회성 암호와 수신제한시스템을 사용한 보안 모델*

서 기 택,† 김 태 훈, 김 정 제, 임 종 인, 문 종 섭‡
고려대학교 정보경영공학전문대학원

# A Novel Method for Effective Protection of IPTV Contents with One-Time Password and Conditional Access System*

Ki-taek Seo,† Tae-hun Kim, Jung-je Kim, Jong-in Lim, Jong-sub Moon‡
Graduate School of Information Management and Security, Korea University

## 요 약

최근 네트워크의 발전과 인터넷의 대중화로 인하여 IPTV의 서비스가 전 세계적으로 활성화되고 있다. IPTV는 인터넷 프로토콜을 사용하되 방송 특성을 만족해야 하는데 현재는 인터넷 특성상 보안을 제공하지 못하고 있다. 따라서 IPTV에서도 사용자가 요구하는 콘텐츠에 대하여 알맞은 서비스를 제공하는 것이 중요하며 동시에, 콘텐츠의 안전성 및 보안성을 강화해야 할 필요가 있다. 현재 IPTV에서는 콘텐츠를 보호하기 위한 기술로 수신제한시스템(Conditional Access System)과 디지털 저작권 관리(Digital Right Management) 시스템을 도입하고 있지만 한계가 존재한다. 따라서 본 논문에서는 기존의 IPTV에서 사용되고 있는 보안 시스템을 효율적으로 보완하고 안전성을 높일 수 있는 방법을 제안한다. 제안하는 기법은 OTP를 사용하여 콘텐츠를 암/복호화하고 사용자에 관한 권한 관리와 키 관리는 CAS가 수행하는 모델로써 시스템의 부하를 줄일 수 있고 사용자 인증, 콘텐츠 보호, 스트림 데이터 전송의 안전성을 제공할 수 있다.

## ABSTRACT

The evolution of internet have opened the world of IPTV. With internet protocol, IPTV broadcasts contents stream. The IP protocol doesn't provide secure service due to IP characteristics. So, it is important to provide both connect and secure service. Conditional Access System and/or Digital Right Management are being used to protect IPTV contents. However, there exist restrictions in the view of security. In this paper, we analyse existing security technologies for IPTV and propose a novel method to enforce security efficiently. In the proposed method, OTP is used for encryption/decryption contents and CAS controls key for encryption/decryption and the right of user. With this scheme, it reduces the load of the system and provides more security.

**Keywords:** Contents Security, IPTV, CAS, OTP

* 접수일(2010년 3월 22일), 수정일(1차: 2010년 5월 1일, 2차: 2010년 6월 11일, 3차: 2010년 6월 22일), 게재확정일(2010년 7월 30일)
* "이 연구에 참여한 연구자(의 일부)는 '2단계 BK21사업'의 지원비를 받았음"
† 주저자, kitaekseo@korea.ac.kr
‡ 교신저자, jsmoon@korea.ac.kr

## I. 서 론

컴퓨터 네트워크의 발전과 인터넷 사용의 급증으로 인하여, 네트워크를 이용한 정보의 전달 및 공유 비율은 과거와 비교할 수 없을 정도로 증가하였다. 이와 더불어 기존의 전화망, TV망 등에서 주고받던 데이터도 네트워크를 기반으로 제공되고 있다. IPTV(Internet Protocol Television) 서비스는 이러한 흐름에 맞추어 영상 및 음성 미디어 콘텐츠를 네트워크를 이용하여 서비스 하는 것이다[1]. 최근의 IPTV는 QoS가 보장된 광대역 IP 네트워크와 IP 셋탑박스(Set-Top Box), 표준 TV 수상기를 통해서 양방향 TV 서비스를 포함한 디지털 방송 및 통신 융합 서비스를 제공한다[2]. 또한 방송영역에서 제공되던 멀티미디어 콘텐츠를 인터넷 망을 통하여 실시간 전송하는 서비스로 구체화되고 있다[3]. 따라서 IPTV 서비스는 서비스의 원활한 제공 외에도 정당한 사용자를 인증할 수 있는 보안 모델과 디지털 콘텐츠를 보호하고 안전하게 유통시킬 수 있는 기술이 수립되어야 한다. IPTV 서비스를 위한 보안 기술 표준화는 DVB(Digital Video Broadcasting)의 CPCM(Content Protection & Copy Management)을 중심으로 하는 DRM(Digital Right Management)기술 연구와 ATSC(Advanced Television System Committee)나 DVB를 중심으로 하는 수신제한시스템(Conditional Access System: CAS)이 주를 이루고 있다[4][5][6]. 먼저 CAS는 IPTV에서 가장 많이 사용되고 있는 콘텐츠 보안 기술로 정당한 사용자에게 허용된 서비스만을 사용할 수 있도록 제어하는 시스템이며 미디어 데이터 스트림을 암/복호화 하는 기능을 포함한다. DRM기술도 제공되는 콘텐츠에 대하여 제공받는 사용자를 제한하고 콘텐츠에 대한 정당한 사용을 허용해주는 시스템이다. 그러나 이러한 콘텐츠 보안 방식들은 각각 하나의 방식만을 사용하면 보안상의 약점을 내포하게 되며, 여러 개의 보안 모델을 융합하여 적용하게 되면 시스템 구조가 복잡해지고 비용이 많이 드는 단점을 가지고 있다[7]. 그럼에도 불구하고 실제 IPTV 시스템에서는 두 가지 이상의 보안 모델을 융합하여 적용하는 것이 일반적이다. 이는 콘텐츠에 대한 보안성 유지가 그만큼 중요하다는 것을 의미한다. 본 논문에서는 OTP(One-Time Password)의 특성을 적용한 보안 모델을 사용하여 IPTV에서 요구하는 보안 사항을 만족하면서 적은 비용으로 시스템의 안전성을 확보하고 콘텐츠의 보안성을 강화 시킬 수 있는 기법을 제안한다.

논문의 구성은 다음과 같다. 2장에서 OTP를 사용하는 인증 방법과 IPTV에서 사용되고 있는 CAS 기술, DRM 기술에 대한 관련 연구들을 분석하고, 3장에서는 본 논문에서 제안하는 일회성 암호를 이용한 수신제한시스템 보안 모델을 제안한다. 4장에서는 제안하는 기법에 대하여 효율성 및 안전성을 검증하고 마지막으로 5장에서 결론 및 향후 연구에 대해서 설명한다.

## II. 관련 연구

### 2.1 OTP를 이용한 보안 기술

OTP 사용자 인증을 위한 OTP기술은 매번 새로운 비밀번호를 생성하여 상호 인증하는 기술로, 해쉬함수(Hash function)를 사용하기 때문에 간단하고 어떤 정보도 호스트에 남지 않는 안전한 기술이다[8]. 해쉬 함수는 주로 MD4, MD5 또는 SHA1이 사용되는데 이러한 해쉬 함수는 불가역적인 성질을 가지고 있어 해쉬값을 알고 있더라도, 원래의 입력값을 알아내기 힘들며, 또한 같은 해쉬값을 갖는 새로운 입력값을 찾아내는 것도 힘든 특징을 가지고 있다[9]. 따라서 공격자가 네트워크상에서 해쉬함수로 생성한 비밀번호를 알아낸다 하더라도 그 해쉬값을 갖는 원문 비밀번호를 알아내거나 새로운 비밀번호를 만들어내기 어렵다. 근래의 OTP기술은 방식에 따라 시도/응답(Challenge/Response) 방식, 시간 동기화(Time Synchronous) 방식, 이벤트 동기화(Event Synchronous) 방식으로 크게 세 가지로 분류된다[10][11][12]. 각각의 생성원리를 살펴보면, 시도/응답 방식은 인증 서버에서 난수발생기를 이용하여 생성한 난수를 사용자에게 안전하게 전송하고, 사용자는 이 난수를 이용하여 OTP를 생성한다. 그렇게 되면 서버와 사용자는 OTP생성을 위한 시드를 공유하게 되어 같은 OTP를 생성하고 상호 인증 할 수 있는 방식이다. 시간 동기화 방식은 사용자의 고유값과 시각정보를 이용하여 OTP를 생성하는 방식으로 인증서버와의 시간동기를 통하여 같은 시간값을 시드로 OTP를 생성하는 방식이다. 마지막으로 이벤트 동기화 방식은 시간 정보 대신에 인증서버와 인증 횟수(Counter) 기록을 공유하고 인증 횟수를 일회용 패스워드 생성 시 시드로 사용한다. 이러한 OTP기술은 방식에서는 차이가 있지만, 수행하는 역할은 동일하

다. 즉, 사용자가 필요로 하는 서비스를 이용하기 위하여 인증 절차를 수행할 때, 일회성 패스워드를 생성하여 상호 인증하는 것이다[13]. 최초에 생성되는 OTP 는 해쉬함수 의 입력값으로, 사용자의 고유값와 시드값 token을 이용하여 생성된다.

$$P_0 = f(s\,,\ token) \tag{1}$$

이후 생성되는 은 이전에 생성된 에 같은 함수를 한 번 더 적용하여 생성한다.

$$P_1 = f(P_0\,,\ (token+1)) \tag{2}$$

이와 같은 과정을 일반적으로 나타내면 다음과 같다.

$$P_i = f^i(P_{i-1}\,,\ (token+i))\ \text{(단, } i \geq 1) \tag{3}$$

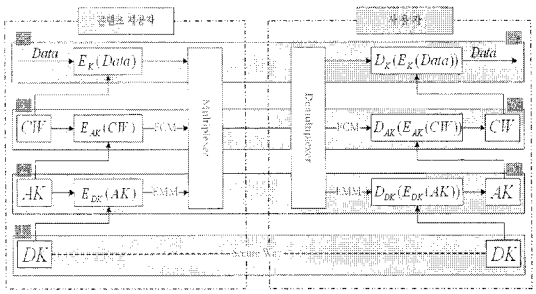
위의 수식에 따라 OTP는 의 값을 알지 못하면 생성할 수 없고, token이 매번 갱신되어 시드로 이용되므로 임의로 을 생성할 수 없다. 이는 키의 노출이나 재사용 문제에 대하여 높은 보안성을 유지할 수 있는 장점이 있다.

## 2.2 IPTV와 수신제한시스템(CAS)

CAS는 CAS는 콘텐츠 보호를 위한 보안 기술로 사용자에게 부여되는 수신자격(Entitlement)을 판단하고 수신자격을 갖춘 사용자에게 허용된 서비스만을 사용할 수 있도록 제어하는 시스템이다. 또한 CAS는 스크램블링(Scrambling)/디스크램블링(De-Scrambling) 알고리즘을 이용하여 미디어 데이터 스트림을 암/복호화 하는 기능을 포함한다[14][15]. 스크램블링 알고리즘은 콘텐츠 제공자가 생성한 제어단어(Control Word: CW)를 사용하여 사용자에게 전송되는 스트림 데이터를 암호화하여 전송하면 권한이 있는 수신자는 수신자 단말기의 프로세스를 통하여 얻은 CW를 사용하여 암호화된 스트림 데이터를 복호화함으로써 전송된 콘텐츠를 안전하게 수신할 수 있는 암호화 알고리즘이다. 또한 CAS에서는 계층적 키 구조를 사용하여 CW를 ECM(Entitlement Control Message)으로 전송하고 수신자 정보를 EMM(Entitlement Management Message)에 포함시켜 전달한다[16]. [그림 1]은 CAS에서 사용되는 계층적 키 구조를 자세히 나타낸 것이다.

1. DK(Distribution Key)는 콘텐츠 제공자와 사용자간에 안전한 경로를 통하여 사전에 분배한다.
2. 콘텐츠 제공자와 사용자가 안전한 방법으로 분배된 대칭키인 DK를 이용하여 AK(Authorization Key)를 암호화하고 수신자의 자격을 부여하고 관리하는 메시지인 EMM을 통하여 수신자에게 전송된다.
3. AK로 암호화된 CW를 포함한 ECM은 수신자에게 전달되어 정당한 사용자가 CW를 얻을 수 있도록 한다.
4. CW를 사용하여 스트림 데이터를 암호화하고 사용자에게 전송한다.
5. 사용자측에서는 전달받은 EMM을 복호화하여 AK얻고 정당한 사용자임을 확인한다.
6. 전송받은 ECM를 복호화하여 데이터 복호화에 필요한 CW를 얻는다.
7. CW를 사용하여 전송받는 데이터를 복화화한다.

CAS에서 ECM은 키 갱신 스케줄에 따라 CW를 전송하기 위하여 스트림 데이터 사이에 삽입되어 주기적으로 전송되며, 스트림 데이터의 갱신 주기에 맞추어 지속적으로 전달되어야 한다. 따라서 CAS에서 사용하는 계층적 암호화 방식은 여러 번의 암호화와 키 생성이 수반되어야 하는 단점이 있으며, 셋탑박스에서의 복호화 과정도 복잡하여 실시간 스트림 데이터에 대한 처리에 시간이 소요된다. 또한 CAS는 사용자 요청에 의한 응답을 요구하는 요청/응답(Request/Response) 구조가 아닌 폴링 방식[17]으로 필요하지 않는 ECM을 주기적으로 전송하면서 스트림 대역폭을 낭비하는 문제를 근본적으로 가지고 있다.




[그림 1] CAS에서의 암/복호화 과정

### 2.3 IPTV와 DRM-CAS 모델

IPTV에서는 DRM의 콘텐츠 보호 기술과 CAS의 수신제한기술을 접목하여 사용할 수 있다. CAS와 DRM이 융합된 형태의 콘텐츠 보안 모델은 CAS 중심의 구현모델로 기존에 구축되어 있는 CAS기능을 그대로 유지하면서 DRM을 추가 구현하는 모델이다[18]. 즉, 접근제어는 CAS가 담당을 하고, DRM은 콘텐츠의 저장 및 외부 유출 방지 기능을 담당함으로써 CAS의 보안 취약성을 해결하는 모델이라고 할 수 있다. 하지만 CAS와 DRM을 융합한 모델은 DRM 구현 시 추가의 트래픽이 발생하는 문제가 있다. 또한 CAS내에서 DRM을 적용하게 되면 DRM 라이센스를 발급하는 시기의 문제와 CAS와 연동되어 콘텐츠에 DRM 암호화가 적용되는 시기의 문제를 고려하지 않을 수 없다. 따라서 두 가지 기술을 접목함으로 인해 시스템 구현이 복잡해지고 비용이 많이 드는 단점을 가지고 있다.

### 2.4 IPTV에서 OTP 기술을 사용한 기존 연구

기존의 OTP를 이용한 IPTV 시스템에 대한 연구는 IPTV의 실시간 서비스를 고려하지 않은 다운로드 환경에서 OTP 기술을 적용한 연구이다. 즉 기존 연구에서 사용하는 기법은 콘텐츠 다운로드 서버 및 채널 서버를 구축하고 사용자가 요구하는 콘텐츠에 대하여 콘텐츠 제공자로부터 다운로드 받은 콘텐츠를 사용자가 요구하는 채널에 대하여 분배하고 사용자에게 콘텐츠를 제공하는 방식이다. 이때 셋탑박스에서는 OTP를 생성하여 OTP 인증 서버에 인증을 요청하고, 이후 인증이 완료되면 사용자는 콘텐츠를 분산서버로부터 다운로드 받아 복호화하여 이용하게 된다[19]. 하지만 현재 IPTV는 실시간 방송 서비스가 활발하게 보급되고 있으며 이러한 요구에 적절하게 대응할 수 있는 실시간 기반의 IPTV 서비스를 제공하여야만 한다. 따라서 기존의 OTP를 이용한 다운로드 기반의 IPTV 시스템으로는 적절하게 대응하기 어렵다. 또한 기존의 연구는 CAS를 사용하지 않고 OTP 기술을 단독적으로 사용하고자 하는 모델이지만 OTP가 단독으로 IPTV 시스템에 적용되기에는 문제가 있다. 우선 콘텐츠 이용에 필요한 콘텐츠 접근 정보와 사용자에 관한 그룹정보 및 채널정보를 OTP기술만으로는 해결할 수 없어 추가적인 콘텐츠 채널 관리 서버와 콘텐츠 다운로드 서버 및 분산서버를 구축하여야 한다. 그리고 이러한 서버들을 통하여 콘텐츠 사용에 따른 요금 문제를 명확히 해결하여야 한다. 따라서 기존의 연구에서는 따로 구축하고 관리해야 하는 서버가 오히려 늘어나는 단점이 있다. 이는 현재 IPTV 시스템에 적용될 경우 추가 비용이 발생하는 문제를 가지고 있다. 따라서 현재 IPTV 서비스에서 적용하기 위해서는 기존의 연구와 같이 추가적인 채널 서버 및 콘텐츠 관리 서버, OTP 인증 서버를 구축하는 것 보다는 현재의 시스템에 적용가능하면서 콘텐츠의 보안성을 높이고 실시간 서비스가 가능하며 비용을 줄일 수 있는 연구가 진행되어야 한다.

## III. 제안하는 방법

본 논문에서 제안하는 모델은 현 IPTV 시스템에서 사용되고 있는 CAS와 OTP를 접목시킴으로써 CAS가 가지고 있는 문제점을 보완하고 성능을 향상시킬 수 있는 기법이다. 또한 OTP를 이용하여 데이터를 암/복호화함으로써 시스템의 속도를 향상시키고 비용을 절감시킬 수 있는 모델이다. 사용하는 OTP기술은 시도/응답 방식과 시간 동기화 방식을 접목시킨 방식으로 최초에 서버의 시간값을 token으로 사용자에게 전달하면 그 시간값을 이용하여 상호간에 시간을 동기화 시키고 자체적으로 시간값을 증가시키면서 OTP를 위한 시드를 생성하는 방식이다.

### 3.1 제안하는 기법의 동작 메커니즘

CAS에서 사용되고 있는 계층적 키를 이용한 암호화 알고리즘은 콘텐츠 스트림 데이터를 전송할 때마다 CW를 이용하여 데이터를 암호화하고, CW에 대한 정보를 AK를 이용하여 암호화하며 이 AK를 다시 DK로 암호화는 구조를 사용하고 있다. 또한 CW가 포함된 ECM 메시지는 사용자의 방송 채널 전환 요구에 바로 대응할 수 있기 위하여 초단위의 빠른 주기로 계속해서 전송될 필요가 있다. 제안하는 기법인 OTP-CAS 모델은 CAS가 수신자의 권한 설정 및 OTP 키 생성에 필요한 시드생성을 담당하고 OTP가 사용자 인증 및 암/복호화 키와 데이터 암/복호화 부분을 담당하는 모델이다. 따라서 CAS와 같이 계층적 암호화가 필요하지 않으며 키 생성에 필요한 시드를 한번만 교환함으로써 데이터의 교환이 지속적으로 자주 발생하는 스트림 데이터를 암호화하는데 적합한 모델이다. OTP를 키로 이용하여 데이터를 암/복호화함

으로써 CW와 ECM의 역할이 불필요해진다. 즉, CW를 포함한 ECM을 전송할 필요 없이 OTP 생성을 위한 Server-Time을 한번만 전송함으로써 CW과 ECM이 생성되고 전송되는 단계를 생략 할 수 있다. 또한 암/복호화 시 배타적 논리합(exclusive-OR)연산을 사용하므로 속도가 빠르다.

### 3.2 IPTV 적용방안

IPTV 시스템은 크게 콘텐츠 제공자(Contents Provider)와 서비스 제공자(Service Provider), 그리고 사용자(Client)로 구성된다. 콘텐츠 제공자와 사용자는 서비스 제공자에게 인증과정을 거치고 암호화에 사용될 OTP 생성에 관한 정보를 교환한다. 이후 실제 데이터의 전송은 콘텐츠 제공자와 사용자가 OTP를 사용하여 암호화된 데이터를 교환함으로써 이루어진다.

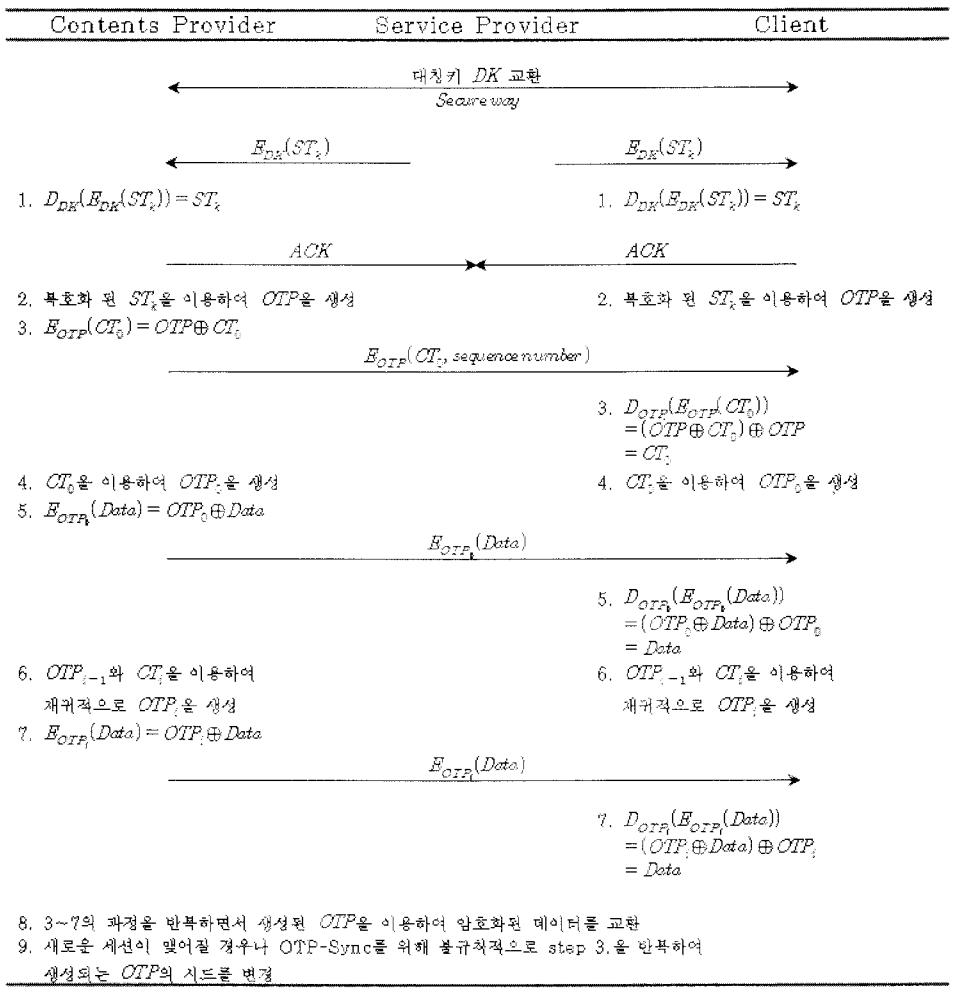
- 콘텐츠 제공자(Contents Provider: CP): 콘텐츠 제공자는 방송을 하는 실제 콘텐츠를 관리하며 서비스 제공자에서 관리되는 OTP 생성 정보를 수신하여 스트림 데이터에 대한 암호화를 수행한다.
- 서비스 제공자(Service Provider: SP): 서비스 제공자는 콘텐츠 제공자와 사용자의 인증을 담당하며, 콘텐츠 암호화에 사용되는 OTP 생성 과정을 관리한다.
- 사용자(Client): 보호된 콘텐츠를 받아 해독한다. 해독된 정보는 사용자 셋탑박스에 내장된 디코더를 통해 수신기로 전송된다.

[그림 2]는 OTP를 생성하고 암호화된 데이터를 교환하는 일련의 절차를 나타낸다. 다음은 제안하는 기법에서 사용되는 계수이다.

- $DK$(Distribution Key) : 콘텐츠 제공자와 사용자 간에 안전한 경로를 통하여 사전에 분배된 대칭키
- $E_K()/D_K()$ : 임의의 키 $K$을 사용하는 암/복호화 알고리즘
- $ST_k$ : 서비스 제공자에서 선택된 임의의 시각정보. $k$는 콘텐츠 채널을 나타낸다.
- $OTP$ : One-Time Password
- $\oplus$(exclusive-OR) : 배타적 논리합 연산
- $CT_0$ : 콘텐츠 제공자에서 선택된 초기 시각 정보
- $OTP_0$ : $CT_0$에 의하여 생성된 최초의$OTP$
- $Data$ : 오디오 및 비디오 정보를 담고 있는 실제 스트림 데이터
- $CT_i$: $i$번째 생성된 $CT$
- $OTP_i$ : $OTP_0$을 이용하여 생성된 $i$번째 $OTP$

제안하는 프로토콜은 총 9단계로 이루어지며 각 단계는 초기값 설정, OTP생성, 데이터 암호화의 단계로 이루어진다. 서비스 제공자는 사전에 이미 안전하게 분배되어 있는 콘텐츠 제공자와 사용자의 대칭키($DK$)로 서비스 제공자의 시각($ST$)을 암호화하여 전송한다. 이때 전송되는 $ST$는 채널별로 생성되어 전송되며 이를 통하여 사용자의 수신자격을 결정하는 $AK$의 역할을 한다. 따라서 해당 채널에 대한 수신자격을 갖춘 가입자(사용자)만이 $ST$을 수신할 수 있으며 이를 통한 사용자 권한 관리가 이루어진다. 또한 $ST$는 사용자가 콘텐츠를 이용하기 위하여 채널을 요구하는 시간보다 앞선 시간에 분배되어 콘텐츠가 방송될 때에는 사용자들이 이미 초기 OTP를 생성할 수 있는 충분한 시간을 제공한다.

- Step 1. 콘텐츠 제공자와 사용자는 서비스 제공자로부터 전송받은 암호화된 데이터를 복호화하여 $ST_k$을 얻는다. 이때 사용자와 콘텐츠 제공자는 $ST_k$을 정상적으로 수신했다는 $ACK$을 보내고 서비스 제공자는 $ACK$을 수신 할 때까지 지속적으로 $ST_k$을 전송한다. $ST_k$을 송신하고 $ACK$을 수신하는 부분은 TCP환경에서 동작되므로 모든 사용자들은 $ST_k$을 수신하게 되었을 경우 이에 대한 $ACK$을 송신하게 된다. $ACK$가 전송되지 않은 사용자들에 한하여 지속적으로 $ST_k$을 전송하고, 사용자들에게 $ACK$을 수신하면 $ST_k$의 전송을 중단한다. 암호화된 데이터 $E_{DK}(ST_k)$는 사전에 이미 안전하게 분배되어 있던 $DK$로 암호화되어 있으므로 대칭키 알고리즘에 의하여 복호화하는 것에는 문제가 없다. 또한 $ST_k$는 $DK$에 의하여 암호화되어 전송되었으므로 노출에 대하여 안전하다.
- Step 2. 복호화된 데이터인 $ST_k$을 이용하여 초기 $OTP$을 생성하는 과정이다. 초기 $OTP$는 이후에 전송되는 $CT_0$을 암호화하는 키로 사용되며, 전체 절차에서 최초에 한번만 사용된다.




〔그림 2〕 OTP 생성 및 데이터 암/복호화 과정

- Step 3. 콘텐츠 제공자는 초기 *OTP*을 이용하여 $CT_0$과 sequence number을 암호화하고 사용자에게 전달한다. $CT_0$는 콘텐츠 제공자가 선정하는 임의의 시각값으로 *OTP* 생성 시 시드로 사용되는 중요한 정보이다. 또한 sequence number은 OTP 갱신 주기 정보이며 $OTP_i$ 생성 시 양측의 생성 시점을 동일하게 조절하는 역할을 하고, 만약 $CT_i$에 대한 수신이 불안정한 경우에도 그 시점에서 생성되는 $OTP_i$에 대한 생성 시점 정보를 제공하여 OTP-Sync가 이루어진다. 이 데이터는 안전성을 위하여 초기에 안전하게 생성된 *OTP*로 암호화하여 전송한다. 사용자는 전송받은 암호 데이터를 초기 *OTP*로 복호화하여 $CT_0$과 sequence number을 얻는다. 초기 *OTP*는 같은 *ST*값을 사용하여 생성하였으므로 같은 값을 가지며, 한번 사용된 *OTP*는 재사용되지 않으므로 노출에 안전하다.
- Step 4. 콘텐츠 제공자와 사용자는 같은 $CT_0$을 공유하게 되었으며, 이를 이용하여 실제 *Data*을 암호화 하게 될 $OTP_0$을 생성한다. 또한 갱신 주기에 의하여 $CT_i$을 생성함으로써 이후에 생성될 $OTP_i$의 초기값을 결정한다.
- Step 5. 생성된 $OTP_0$을 이용하여 실제 스트림 데이터를 암호화하여 전송한다. 사용자는 전송된 암호 데이터를 $OTP_0$을 이용하여 복호화하여 스트림 데이터를 얻을 수 있다.
- Step 6. 앞서 생성된 $OTP_{i-1}$와 $CT_i$을 이용하여 이후에 사용하게 될 $OTP_i$을 재귀적으로 생성

한다.

- Step 7. 생성된 $OTP_i$을 이용하여 스트림 데이터를 암호화하여 전송한다. 사용자는 전송된 암호 데이터를 $OTP_i$을 이용하여 복호화하여 스트림 데이터를 얻을 수 있다.
- Step 8. Step 3.~Step 7.까지의 과정을 반복하면서 전송되는 스트림 데이터의 암/복호화를 수행한다.
- Step 9. 사용자가 요구한 콘텐츠에 대한 전송 이외에 다른 콘텐츠에 대한 요구가 있을 때나 OTP 동기화를 요구할 때에는 불규칙적으로 $CT_j$을 교환함으로써 새로운 OTP를 생성하기 위한 시드를 교환한다. 여기서 $CT_j$의 교환은 Step 3.과 같은 절차를 수행한다.

IPTV는 콘텐츠 제공자 혹은 사용자에 의하여 빈번한 스트림 데이터의 전송을 요구하며, 브로드캐스팅을 통하여 데이터를 전송하므로 정당한 사용자에 의한 정당한 콘텐츠의 제공이 가장 중요한 문제이다. 그러므로 OTP를 이용한 데이터의 암호화는 IPTV 시스템에서 보안적 측면을 강화하기에 적합한 암호 알고리즘이다.

## IV. 제안하는 기법의 분석 및 검증

### 4.1 제안하는 기법의 효율성

제안하는 기법은 IPTV에서 스트림 데이터를 전송할 때, 기존에 사용되던 콘텐츠 보호 기술을 효율적으로 개선하는 모델로 OTP를 사용하여 데이터를 암/복호화하고 ECM과 CW를 사용하지 않음으로써 시스템의 부하를 줄일 수 있는 방법이다. 기존의 CAS 같은 경우에는 초기에 설계될 때부터 Three-level key distribution scheme[16]을 적용하였으며, 이로 인하여 스트림 데이터를 얻기 위해서는 세 번에 걸친 암/복호화 과정을 거쳐야 한다. 또한 CAS는 처음에 단방향 방송에 적합한 구조로 개발되었기 때문에 필요하지 않은 ECM을 계속 전송하는 문제를 근본적으로 가지고 있다. 즉, CAS는 일정한 주기에 따라 ECM을 콘텐츠 스트림 데이터에 끼워서 전송하는데 이것은 네트워크 대역폭의 낭비를 초래하게 된다. 이는 실시간 데이터 전송을 주로 하는 IPTV 시스템의 특성상 사용자의 요구에 적절히 대응하지 못하는 문제가 발생된다.

본 논문에서 제안하는 OTP-CAS 모델을 사용하는 시스템의 콘텐츠 보안은 이러한 IPTV 요구에 적합한 콘텐츠 보호 기술을 제공한다.

첫째로, 제안하는 기법에서는 암호 알고리즘의 적용횟수가 기존의 CAS보다 적게 연산되므로 암/복호화에 있어서 빠른 처리가 가능하다. 또한 CW를 안전하게 전송하기 위하여 사용되는 계층적 키 구조를 생략시킴으로써 ECM의 생성 및 전송이 배제된다. ECM은 CW가 암호화된 메시지이므로 본 논문에서 사용되는 OTP를 이용하면 ECM의 전송이 배제되어도 서비스 제공에는 문제가 없다. 게다가 제안하는 기법에서는 배타적 논리합 연산을 사용함으로써 기존에 사용되는 대칭키 암호화 알고리즘보다 연산속도가 빨라진다. 이는 배타적 논리합 연산이 기계 수준(Machine level)에서 수행되기 때문이다.

둘째로, 초기 OTP의 시드로 사용되는 $ST$는 채널별로 생성되어 전송되며 이를 통하여 사용자의 수신자격을 결정하는 $AK$의 역할을 한다. 또한 생성되는 OTP는 같은 채널을 시청하는 사용자들에 한하여 같은 OTP를 보유하게 되어 다수의 사용자들에 대한 키를 효율적으로 관리할 수 있다. 이를 기반으로 생성된 OTP는 랜덤하게 생성되어 재전송 공격 및 키 노출의 위험으로부터 안전하다. 따라서 브로드캐스팅 환경에서 다수의 사용자들의 수신자격을 결정하기 용이하다.

셋째로, 기존에 CAS에서 사용되는 CW를 사용하지 않고 최초에 교환되는 Server-Time을 한번만 이용함으로써 스트림 데이터 전송 시 CW가 주기적으로 생성되는 비효율성을 제거할 수 있으며 CW를 암호화하고 복호화하는 시간을 단축시킬 수 있다.

넷째로, 제안하는 기법에서는 데이터 스트림에 ECM을 포함하여 전송할 필요가 없으므로 트래픽 관리 및 대역폭 관리가 용이하다. CAS에서 ECM을 스트림 데이터에 포함시켜 전송할 때 발생되는 데이터그램의 낭비를 줄임으로 데이터의 효율성을 향상시킬 수 있으며, 같은 크기의 패킷에 보다 많은 용량의 콘텐츠 데이터를 전송할 수 있으므로 고화질의 콘텐츠를 보다 적은 시간에 전송하는 것이 가능하다.

다섯째로, IPTV에서는 스트림 데이터를 지속적으로 전송하므로 암호화 키의 업데이트가 빈번하게 이루어져야 하는데 OTP 시스템의 경우 이러한 요구에 맞게 키 생성 시 매번 다른 키가 생성되므로 키의 안전성에서도 효과적이며 배타적 논리합이라는 연산의 단점을 보완하는 것이 가능하다.

### 4.2 제안하는 기법의 안전성

IPTV 시스템이 갖추어야 하는 근본적인 보안 요소들은 사용자의 인증과 스트림 데이터에 대한 제어이다[20]. 본 논문에서 제안하는 기법에 대한 안전성은 IPTV에서 요구하는 보안사항과 밀접한 연관이 있으며 안전성에 대한 검토는 다음과 같다.

• 사용자 인증(User Authentication)

IPTV 시스템에서 사용자 인증이란, 전체 서비스에 대한 사용자를 식별하고 콘텐츠에 대한 사용권한을 부여하는 과정을 의미한다. OTP를 적용한 CAS의 경우 초기 OTP를 생성하기 위한 시드값을 콘텐츠 제공자와 사용자간의 안전한 방법에 의해 교환된 대칭키를 이용하여 암호화함으로써, 쌍방에 같은 키 값 $D_{DK}(E_{DK}(ST)) = ST$을 소유할 수 있으며, 정당한 사용자가 아니라면 이후 스트림 암호화에서 사용되는 키를 생성할 수 없다. 따라서 사용자에 대한 인증은 OTP를 생성하여 키 값을 소유한 사용자에 대하여 $CT_0$을 이용하여 배타적 논리합 연산을 수행하면 검증할 수 있다.

• 접근 제어(Access Control)

정당하지 않은 사용자는 콘텐츠에 대한 접근 권한이 없어야 한다. 정당하게 인증을 받은 사용자만이 스트림 데이터를 복호화 할 수 있기 때문에 정당하지 않은 사용자나 악의적인 목적으로 스트림 데이터를 획득한 공격자는 해당 콘텐츠에 대한 사용권한을 얻을 수 없다. 제안하는 기법은 OTP를 사용하므로 불법적으로 콘텐츠를 소유한다하여도 OTP 시스템의 특성상 복호화 할 수 없다. 이는 OTP 알고리즘이 이벤트 발생 시 한번 생성되고 이후에는 소멸되는 특성을 가지고 있기 때문이며, OTP 키 값은 $CT$에 의하여 랜덤하게 생성되므로 키값의 복원이 어렵다.

• 스트림 데이터 제어(Stream data Control)

OTP를 이용한 암/복호화 기술은 시스템 내에서 소프트웨어적으로 적용되어 사용될 수 있다. 따라서 스트림 데이터에 대한 암/복호화 비용을 절감할 수 있으며 OTP Generator 모듈도 시스템 내부에 존재하므로 스트림 데이터에 대한 암/복호화 제어가 용이하다. 더불어 전송 시 스트림 데이터에 대한 손실이 발생하였을 경우, 두 가지 방법으로 손실 유무 및 복구가 가능한데, 첫째, 콘텐츠 제공자와 사용자는 일시적으로 서로 보유하고 있는 키가 다르므로($OTP \neq OTP'$) 데이터의 손실 여부를 파악할 수 있으며 서비스 제공자에게 요청하여 새로운 $ST$을 공유하고 OTP를 생성함으로써 전송되는 콘텐츠의 복원 시점을 알 수 있다. 둘째로는 데이터 전송 시 스트림의 시퀀스 번호(4byte 크기)를 포함하여 전송하는 방식을 사용하게 되면 패킷 로스(Packet loss) 발생 시점을 파악하고 데이터를 복구하기 용이하다.

## V. 결 론

최근의 IPTV 서비스는 특정사용자에게 한정되어 콘텐츠 서비스를 제공하는 것이 아니라 서비스를 원하는 사용자는 인터넷망을 통하여 누구나 쉽게 접할 수 있는 특징을 가진다. 이는 서비스의 개발이 용이하고 다양한 형태의 유연한 서비스를 제공할 수 있는 개방형 서비스의 형태이며, 제공되는 콘텐츠 및 서비스의 대중화를 가능하게 한다. 하지만 기존의 IPTV 서비스는 개발에 많은 비용이 들고 시스템의 구조도 복잡하여 많은 사용자의 요구에 적절히 대응하지 못하는 문제를 가지고 있다. 또한 아직까지 IPTV 서비스에 대한 명확한 표준 모델이 수립되어 있지 못하여 시스템의 안전성과 콘텐츠의 보안성에 대한 근본적인 문제를 가지고 있다. 그리고 IPTV 보안성을 강화시키기 위하여 적용하는 CAS나 DRM 등은 하나의 모델만을 적용시켰을 경우 얻을 수 있는 안전성에 한계가 존재한다. 따라서 이러한 특징에 맞추어 보안 기술의 변화가 필요하며, 안전성에 대한 효율적인 대책을 강구하여야 한다.

본 논문에서 제시하는 OTP-CAS 모델은 이러한 보안적 사항에 초점을 맞추어 정당한 사용자를 위한 안전한 콘텐츠 전송을 가능하게 한다. OTP-CAS 모델은 사용자 인증, 콘텐츠 보호, 스트림 데이터 전송의 안전성을 제공하여 IPTV 서비스의 기본적인 보안사항을 충족시키며, 모델 적용이 용이하고 적용 비용을 절감시키는 효과가 있다. 따라서 OTP-CAS 모델은 사용자가 증가하고 있는 근래의 IPTV 서비스에 적합한 모델이다. 향후 연구로는 IPTV뿐만 아니라 VoIP등 근래에 사용자가 늘어나고 있는 스트림 데이터를 이용한 서비스의 효과적인 암호화 알고리즘에 관하여 연구함으로써 통합된 스트리밍 암호화 기법의 연구가 필요할 것이다.

## 참고문헌


[1] K. Kerpez, "IPTV service assurance," IEEE Communications Magazine, vol. 44, no. 9, pp. 166-172, Sep. 2006

[2] Ken Kerpez, Dave Waring, George Lapiotis, J. Bryan Lyles, and Ravi Vaidyanathan, "IPTV Service Assurance," IEEE Communications Magazine, vol. 44, no. 9, pp. 166-72, Sep. 2006.

[3] M. Pagani, Multimedia and Interactive Digital TV: Managing the Opportunities Created by Digital Convergence, IRM Press, Apr. 2003.

[4] Digital Video Broadcasting(DVB), "Support For Use of Scrambling and Conditional Access Within Digital Broadcasting Systems," DVB Document A007, Feb. 1997.

[5] Digital Video Broadcasting(DVB), "Content Protection & Copy Management," DVB Document A094, Nov. 2005.

[6] Advanced Television System Committee (ATSC), "Conditional Access System for Terrestrial Brodcast," A/70A, Jul. 2004.

[7] S. Hwang, "Content and service protection for IPTV," IEEE Transactions on Broadcasting, vol. 55, no. 2, Jun. 2009.

[8] T. Tsuji and A. Shimizu, "An impersonation attack on one-time password authentication protocol OSPA," IEICE Transactions on Communications, vol. E86-B, no. 7, pp. 2182-2185, Jul. 2003.

[9] N.M. Haller, "The s/key one-time password system," Proceedings of the 1994 Symposium on Network and Distributed Systems Security, pp. 151-157, Feb. 1994.

[10] MRaihi, "TOTP: Time-based One-time Password Algorithm," Internet Draft Informational, Sep. 2010.

[11] Leslie Lamport, "Password Authentication with Insecure Communication," Communications of the ACM, vol.24, no.11, pp. 770-772, Nov. 1981.

[12] MRaihi, "OCRA: OATH challenge Response Algorithm," Internet Draft Informational, Sep. 2010.

[13] N. Haller, C. Metz, P. Nesser and M. Straw, "A One-Time Password System", RFC 2289, Feb. 1998.

[14] Advanced Television System Committee (ATSC), "Digital Television System," A/53, Aug. 2009.

[15] Digital Video Broadcasting(DVB), "Frame structure channel coding and modulation for a second generation digital terrestrial television broadcasting system(DVB-T2)," ETSI EN 302 755, Sep. 2009.

[16] M. Zhu1, M. Zhang1, X. Chen1, D. Zhang1 and Z. Huang1, "A Hierarchical Key Distribution Scheme for Conditional Access System in DTV Broadcasting," Lecture Notes in Computer Science, vol 4456/2007, pp. 839-846, Sep. 2007.

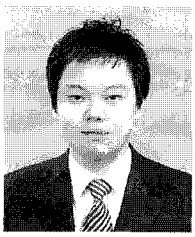
[17] F. Kamperman, B. van Rijnsoever, "Conditional access system interoperability through software downloading," IEEE Transactions on Consumer Electronics, vol. 47, no. 1, pp. 47-54, Feb. 2001.

[18] ATIS, "ATIS Releases Default Scrambling Algorithm for IPTV," ATIS-0800006, Mar. 2007.

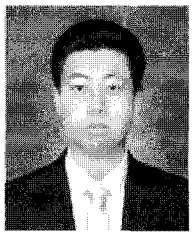
[19] 김대진, 최홍섭, "OTP를 이용한 IPTV 콘텐츠 보호 및 인증 시스템 설계," 한국콘텐츠학회논문지, 9(8), pp. 129-137, 2009년 8월.

[20] David H. Ramirez, IPTV Security: Protecting High-Value Digital Contents, Wiley Publishing, 2008.

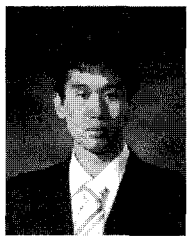
## 〈著者紹介〉

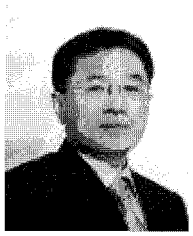
서 기 택 (Ki-taek Seo) 학생회원
2008년 2월: 강남대학교 컴퓨터미디어공학부 컴퓨터공학과 졸업
2008년 3월~현재: 고려대학교 정보경영공학전문대학원 정보경영공학과 석사과정
〈관심분야〉 패턴인식, 네트워크 보안, 스트리밍 암호화, 콘텐츠 보안



김 태 훈 (Tae-hun Kim) 학생회원
2008년 2월: 고려대학교 전산학과 졸업
2008년 3월~현재: 고려대학교 정보경영공학전문대학원 정보경영공학과 석사과정
〈관심분야〉 침입탐지, 악성코드, 데이터 마이닝



김 정 제 (Jung-je Kim) 학생회원
2009년 2월: 중앙대학교 컴퓨터공학과 졸업
2009년 8월~현재: 고려대학교 정보경영공학전문대학원 정보경영공학과 석사과정
〈관심분야〉 침입탐지, 네트워크 보안, VoIP 보안



임 종 인 (Jong-in Lim) 종신회원
1986년 2월: 고려대학교 대학원 수학과 박사(암호학)
2000년 8월: 고려대학교 정보보호대학원/CIST 원장(센터장)
2004년 1월: 국가정보원 정보보호정책 자문위원
2005년 7월: 대통령 자문 전자정부 특별위원
2005년 12월: 국회 과기정위원회 정보통신 정책 자문위원
〈관심분야〉 정보보호기술, 정보보호정책, PET, 컴퓨터 포렌식

문 종 섭 (Jong-sub Moon) 종신회원
1981년~1985년: 금성 통신 연구소 연구원
1991년: Illinois Institute of technology 전산학 박사 졸업
1993년~현재: 고려대학교 전자 및 정보공학부 교수
〈관심분야〉 생체인식, 침입탐지, 네트워크 보안, 운영체제, 시스템 보안