# PIN 코드를 이용한 IPTV 게임 사용자의 개별 인증 프로토콜

정윤수* · 김용태**

## Personal Authentication Protocol of IPTV Game User using PIN Code

Yoon-Su Jeong* · Yong-Tae Kim**

본 연구는 지식경제부 지역혁신센터사업인 민군겸용보안공학연구센터 지원으로 수행되었음.

요 약

IPTV 기술의 발전으로 인하여 사용자는 지리적 위치에 상관없이 멀티미디어 데이터의 서비스를 손쉽게 제공받고 있다. 그러나 가입 가구내 IPTV 게임을 불법적으로 서비스 받으려는 사용자 또한 증가하고 있다. 이 논문에서는 IPTV 서비스를 제공받는 청소년이 청소년이용불가 게임에 쉽게 접근할 수 없도록 PIN코드를 이용한 IPTV 가구내 사용자 개별 인증 프로토콜을 제안한다. 제안 프로토콜은 청소년이 청소년이용불가 게임에 불법적으로 접근하는 것을 예방하기 위해서 PIN 코드를 이용한 일회용 패스워드를 생성하여 IPTV 가구내 주어진 권한 정보를 쌍으로 묶어 인증서버와 셋톱박스에 저장하여 청소년이 강제적으로 게임에 접근하려는 시도를 예방한다.

ABSTRACT

Because of the development of IPTV, user is provided service of multimedia data regardless the location. But the number of users who try to get service of IPTV game illegally is also increasing. In this paper, user authentication protocol in IPTV housing using PIN code not to access easily for teenagers not to access to prohibited games. The proposed protocol combines authority data in IPTV household and creates a disposable password using PIN code to prevent teenagers from accessing illegally to the prohibited games and saves the data in certification server and set-top box to prevent forced accessing.

키워드

IPTV, PIN Code, Authentication, Protocol

Key word

IPTV, PIN Code, Authentication, Protocol

* 정회원 : 한남대학교 산업기술연구소 전임연구원 (제1저자)
** 정회원 : 한남대학교 멀티미디어학부 교수 (교신저자, ky7762@hnu.ac.kr)

접수일자 : 2011. 07. 06
심사완료일자 : 2011. 07. 19

## Ⅰ. 서 론

최근 초고속 인터넷 망의 확산과 디지털 방송의 융합으로 인하여 디지털 컨버전스(Digital Convergence)가 빠르게 진행되면서 동영상 등 대용량의 정보를 편리하게 송·수신할 수 있는 IPTV(Internet Protocol TV) 서비스가 최근 각광을 받고 있다[1,2,3]. IPTV 기술은 기존 초고속 인터넷망을 기반으로 고선명 동영상 서비스를 가정의 TV와 연결하여 제공하는 서비스로 방송용 전파가 아닌 인터넷 프로토콜을 이용하여 인터넷 방송처럼 스트리밍 방식의 방송 프로그램을 시청하는 방송기술을 의미한다[4,5].

IPTV 기술이 본격적으로 사용자들에게 서비스되면서 사용자는 지리적 위치에 상관없이 멀티미디어 데이터의 서비스를 제공받고 있지만 IPTV 서비스는 개인 단위의 미디어 특성을 갖는 것과는 달리 일반적인 TV처럼 가구중심 단위의 미디어 특성을 갖고 있어 사용자 인증 및 결제방식의 문제점을 가지고 있다. 특히, IPTV 게임 서비스는 기존 인터넷 서비스와 유사한 플랫폼 환경으로 제공되기 때문에 IPTV 환경 하에서도 PC 온라인게임 등 다른 플랫폼 기반 게임과 동일한 방법으로 사용자 개별 인증 및 과금 결제가 가능하다.

IPTV 서비스는 사용자 인증 및 결제방식이 개인의 비밀번호 방식이 아닌 가입가구가 공통으로 이용하는 PIN(Personal Identification Number) 코드 형식을 사용한다. IPTV를 통하여 제공되는 유료 게임 서비스의 경우 대부분 PIN 코드 입력방식을 통하여 결제되기 때문에 온라인, 모바일 등 기존 플랫폼에서 지원되고 있는 사용자 개별 인증을 통한 실명 인증 및 개별 전자결제는 제공되지 못하고 있다. 특히, IPTV 게임을 사용하는 청소년이 가정에서 사용하고 있는 PIN 코드를 알고 있다면 부모의 동의없이 청소년이용불가의 게임에 쉽게 접근할 수 있을 뿐만 아니라 유료 청소년이용불가 및 전체이용가 게임의 아이템 등도 쉽게 결제할 수 있는 문제점이 있다.

IPTV 서비스에서 사용되는 PIN코드 방식은 일반적으로 4자리수 값을 가지며 초기값은 0000으로 설정되어 있어 청소년이 쉽게 접근할 수 있으며 청소년이 청소년이용불가 게임에 접근하는 것을 제어할 수 있는 방법이 없어 현재 서비스되고 있는 IPTV의 PIN 코드 방식에 대한 사용자 인증 및 결제 프로토콜에 대한 연구가 필요하다.

이 논문에서는 IPTV 서비스를 제공받는 청소년이 청소년이용불가 게임에 쉽게 접근할 수 없도록 PIN코드를 이용한 IPTV 가구내 사용자 개별 인증 프로토콜을 제안한다. 제안 프로토콜은 청소년이 청소년이용불가 게임에 불법적으로 접근하는 것을 예방하기 위해서 PIN 코드를 이용하여 일회용 패스워드를 생성한 후 IPTV 가구내 주어진 권한 정보와 쌍으로 묶어 인증서버와 셋톱박스에 저장함으로써 청소년이 강제적으로 게임에 접근하려는 시도를 예방한다. 또한, 제안 프로토콜은 청소년이 게임에 접근할 경우 가구내 인증 책임자에게 통보하여 청소년의 게임 접근을 승인하여야만 청소년이 게임을 할 수 있다. 제안 프로토콜은 청소년이 청소년이용불가 게임에 접근할 때마다 인증 서버의 비밀키를 새로 부여받아 PIN 코드와 조합되기 때문에 IPTV 보안 공격에도 안전하다.

이 논문의 구성은 다음과 같다. 2장에서는 IPTV 개념, IPTV 콘텐츠 보안 및 IPTV 보안기술에 대해서 분석한다. 3장에서는 PIN코드 기능을 확장한 IPTV 게임 사용자의 개별 인증 프로토콜를 제시하고, 4장에서는 제안 프로토콜의 보안평가를 분석한다. 마지막으로 5장에서는 이 논문의 결과를 요약하고 향후 연구에 대한 방향을 제시한다.

## Ⅱ. 관련 연구

### 2.1 인증 프로토콜

IPTV(Internet Protocol TV)는 초고속 인터넷망을 활용하여 사용자에 맞는 '개인 맞춤형 서비스'와 '양방향 데이터 서비스'를 TV를 통해 제공하는 대표적인 융합서비스이다[1]. IPTV는 통신사업자 측면에서 기존의 통신서비스 기반 위에 영상 서비스를 제공함으로써 단일 회선망을 통하여 데이터, 음성, 영상을 한꺼번에 묶어 동시에 제공하는 TPS(Triple Play Service) 서비스를 완성하기 위한 서비스이다. 좁은 의미에서는 Walled Garden, VoD 등 초고속 인터넷의 부가서비스로 서비스 제공영역을 PC에서 TV로 확장시킨 개념이지만, 넓은 의미에서는 초고속 인터넷의 가입자 망 구간을 물리

적인 방송매체로 활용하여 A/V(Audio/Video) 형태의 방송채널을 적극적으로 수용하는 것을 포함하는 개념이다.

IPTV는 방송국에서 송출하는 프로그램을 보는 것이 아니라 셋톱박스와 인터넷을 사용하여 원하는 방송을 다운로드 혹은 스트리밍 방식으로 서비스를 제공받는다. 기존 방식의 방송 서비스는 방송사들이 편성한 프로그램을 시청자에게 일방적으로 방송하지만 IPTV 서비스는 시청자가 원하는 방송을 골라 볼 수 있어 실시간 퀴즈, 투표, 상거래 등을 통해 TV 편성에 참여할 수 있는 일종의 개별 맞춤형 TV가 가능하다. IPTV는 소비자가 원하는 서비스의 구현이 가능하고 T-Commerce나 온라인 게임, 채팅, 이메일 등의 양방향 서비스의 이용이 가능한 쌍방향성, Point-to-Point 전달 방식으로 개인화된 채널을 볼 수 있고, 더 나아가 개인의 취향에 따른 개인화된 포털 TV도 등장할 수 있는 개인화, 초고속 인터넷, VoIP, IPTV 등이 결합된 TPS, QPS 등의 제공이 가능하고 그 외 다양성 서비스가 지속적으로 창출될 수 있는 다양성 등의 특징을 가진다.

### 2.2 인증 프로토콜 보안 기술

최근 IPTV와 관련된 기술은 계층적 레벨에 따라 키를 부여하는 방법과 권한에 따라 키를 부여하는 방법으로 구분하여 연구되고 있다[2,3,4].

Tu. et. al 기법[6]은 Schnorr 디지털 서명과 일방향 함수를 사용하여 키 동의를 수행하는 프로토콜을 제안하였다. 이 프로토콜은 McCormac Hack 문제와 스마트 카드 복제에 강하다고 주장하였지만 Huang. et al.[7]에서는 [6]기법이 완전한 전방향 안정성을 보장하지 못하여 가장 공격에 취약한 문제점을 개선한 기법을 제안하였다.

Jiang. et al.[8]은 [7]이 여전히 가장 공격에 취약하고 상호 인증을 제공하지 못하는 것을 증명하였고 Jiang. et. al[9]은 [6] 기법에서 연산량 측면이 비효율적인 것을 개선하였으며 Yoon. et. al.[10]에서는 [9]의 프로토콜이 위장 공격 및 메시지 변조 공격에 취약한 것을 개선한 프로토콜을 제안하였다. 그러나 이 기법은 지수연산을 사용하지 않으며 일방향 함수와 대칭키 알고리즘을 사용하였다.

Lee. et. al.[11] 기법은 IPTV 환경에서 사용되는 키를 2레벨과 3 레벨을 실행할 수 없도록 분류하는 것을 보완하기 위해 2개의 4 레벨 키 관리 기법을 제안하였다. [11] 기법은 4 레벨 키 관리 기법을 단순화하면서 가입자 개개인을 구분하기 위해서 서비스 수신 그룹과 그룹 가입자 채널의 개념을 사용하였다. IPTV의 모든 서비스 수신 그룹은 수신 그룹 키(RGP, Receiving Group Key)을 소유하며 수신 그룹 키를 이용하여 가입자의 서비스를 구분한다.

Hou. et. al.[12] 기법은 가입자에게 레벨을 부여하여 인증 서버가 가입자의 채널과 가입자의 그룹화를 위해 가입자의 레벨에 맞는 키 분배 기법을 제안하였다 [2,3,4]. [12]의 키 분배 기법은 모든 가입자가 가입자의 가입 레벨에 맞는 단일 분배키만을 사용하는 특징이 있다.

Kim. et. al.[13] 기법은 IPTV 서비스를 제공받는 사용자를 인증하기 위해서 디지털 시그너처 프로토콜과 일방향 해쉬 함수를 기반한 RSA 암호화를 사용한다. [13] 기법은 계층적 액세스 제어 구조를 형성하기 위해서 채널을 여러 그룹으로 나누었으며 가입자가 채널 그룹의 단일 수신 그룹 키를 사용하는 특징이 있다.

## Ⅲ. PIN 코드를 이용한 IPTV 가구내 사용자 개별 인증 프로토콜

이 절에서는 IPTV 게임을 서비스받는 청소년이 청소년이용불가 게임에 쉽게 접근할 수 없도록 PIN코드를 이용한 IPTV 가구내 사용자 개별 인증 프로토콜을 제안한다. 제안 프로토콜은 청소년이 청소년이용불가 게임에 불법적으로 접근하는 것을 예방하기 위해서 PIN 코드와 개별 비밀번호를 조합하여 생성한 키 값 즉 일회용 패스워드를 IPTV 가구내 주어진 권한 정보와 쌍으로 묶어 셋톱박스에 등록하여 사용자에게 서비스를 제공한다.

### 3.1 개요

IPTV 게임을 서비스 받는 청소년은 사용자 인증 및 결제방식이 개인의 비밀번호 방식이 아닌 가입가구가 공통으로 이용하는 PIN코드 형식을 이용한다. 그러나 PIN 코드 방식은 PIN코드를 청소년이 알고 있다면 부모의 동의없이 청소년이용불가의 게임에 쉽게 접근할 수 있을 뿐만 아니라 유료 청소년이용불가 및 전체 이

용가 게임의 아이템 등도 쉽게 결제할 수 있는 문제점이 있다.

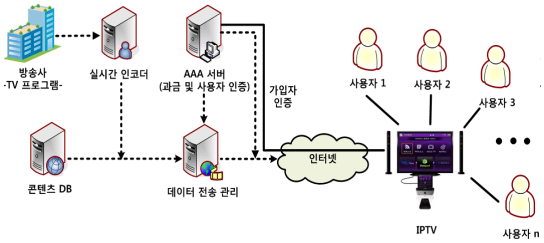


그림 1. 제안 프로토콜의 개요
Fig. 1 Concept of Proposed Protocol

제안 프로토콜은 (그림 1)와 같이 사용자가 IPTV 서비스를 제공받기 위해 가입자 인증 기술을 사용하여 가입자와 인증 서버간의 상호인증을 제공한다.

### 3.2 제안 인증 프로토콜 용어 정의

제안 프로토콜에서 사용하는 주요 용어를 정의하면 표 1과 같다.

### 3.3 PIN 코드를 이용한 사용자 인증 프로토콜

이 절에서는 청소년이 불법적으로 게임에 접근하는 것을 막기위해서 가구내 할당된 PIN 코드와 권한 정보를 이용하여 청소년이 IPTV 게임을 합법적인으로 인증하여 사용할 수 있는 방법을 기술한다.

#### 3.3.1 등록 과정

등록과정은 IPTV 게임을 제공받기 원하는 가구내 사용자가 인증서버에게 서비스를 요청하기 전에 사용자 정보를 사전에 등록하는 과정으로써 서비스를 제공받기 위해서는 사용자의 인식자 $ID_U$와 패스워드 $PW_U$가 필수적이다.

• **단계 1 :** 단계 1에서는 사용자가 IPTV 서비스를 제공받기 전에 인증 서버에 사용자 정보를 전달하는 단계로써 사용자 $U$는 인증 서버 $AS$에게 사용자 $U$의 정보 중 인식자 $KU_U$(=$ID_U$)와 패스워드 $KR_U$(=$KU_U \cdot g^{CW}$)를 해쉬 함수 $H(\cdot)$에 적용하여 권한 정보 $I_U$= $H(KU_U, KR_U)$를 생성한다. 권한 정보가 생성된 후에는 사용자 $U$가 생성한 임의의 랜덤수 $r_U$, 게임 채널 정보 $Ch$와 함께 사용자의 서비스 등록 시간 정보 $T_U$를 식 (1)처럼 인증 서버에게 전달하여 등록한다.

$$E_{KR_U}(KU_U, T_U), E_{KU_{AS}}(I_U, r_U, Ch) \quad \text{(식 1)}$$

표 1. 용어 정의
Table. 1 Notaion

| 용 어 | 정 의 |
|---|---|
| * | 각각의 개체(U : 사용자자, AS : 인증서버) |
| $ID_*$ | * 의 아이디 |
| $SID$ | 보안 인식자 |
| $OTP$ | 일회용 패스워드 |
| $PIN$ | 가입자의 일련번호 |
| $CT$ | $OTP$ 입력 값으로 동기화 되어 있는 카운터 |
| $g$ | 곱셈군 $Z_n^*$ 의 생성자 |
| $I_*$ | *의 권한정보 |
| $r_*$ | * 가 생성한 랜덤수 |
| $T_*$ | * 의 서비스 등록 시간 정보 |
| $Ch$ | 채널 정보 |
| $H()$ | 안전한 일방향 해쉬 함수 |
| $E_*[\,]$ | *의 키로 암호화 |
| $KS$ | 가입자와 인증서버가 사전에 공유한 대칭키 |
| $KU_*/KR_*$ | *의 ID기반 공개키/개인키 |
| $ECM$ | Entitlement Control Message |
| $EMM$ | Entitlement Management Message |
| $CW$ | Control Word |

• **단계 2 :** 단계 2에서는 인증서버가 사용자로부터 전달받은 정보를 복호화하여 사용자의 정보를 가공하는 단계로써 인증서버는 사용자의 공개키 정보 $KU_U$와 인증서버 $AS$가 생성한 비밀키 $X_{AS}$를 해쉬 함수 $H(\cdot)$에 적용한 후 사용자에게 전달받은 $I_U$와 exclusive-OR 하여 $SI$로 대체한다.

$$SI = I_U \oplus H(KU_U, X_{AS}) \quad \text{(식 2)}$$

• **단계 3 :** 단계 3에서는 인증서버가 생성한 $SI$를 사용자에게 전달하는 단계로써 인증서버는 $SI$와 함께 사용자 인식자 $ID_U$를 해쉬 함수 $H(\bullet)$에 적용한 후 보안 인식자 $SID_U$(=$I_U \oplus Ch \oplus ID_U$)를 사용자가 생성한 임의의 랜덤수 $R_U$로 암호화하여 사용자에게 전달한다.

$$E_{R_U}(SID_U, H(SI, ID_U)) \quad \text{(식 3)}$$

• **단계 4 :** 단계 4에서는 사용자가 인증서버로부터 전달받은 정보를 복호화하여 $SI$ 정보를 확인 한 후 정보를 데이터베이스에 저장한다.

3.3.2 상호인증 과정

상호인증 과정은 IPTV 서비스를 제공받기 원하는 사용자 $U$가 사용자 인증 유·무를 수행하는 과정으로써 이 과정은 사용자 $U$가 보유하고 있는 인증 정보를 통해 인증서버와 상호인증이 이루어진다.

• **단계 1 :** 사용자가 IPTV 게임에 대한 서비스를 제공받기 원한다면 사용자는 사전에 인증서버 $AS$에 등록한 인식자 $KU_U$와 패스워드 $KR_U$를 입력하여 사용유·무를 확인한 후 제어문자 $CW$, 시간동기화 값 $T_U$, 카운트 $CT$, 핀정보 $PIN$를 이용하여 일회용 패스워드를 생성한다.

$$OTP = g^{CW} \oplus PIN \oplus T_U \oplus CT \oplus ID_{AS} \quad \text{(식 4)}$$

• **단계 2 :** 사용자는 자신이 생성한 일회용 패스워드 $OTP$를 보안 인식자 $SID_U$와 함께 인증서버의 공개키로 암호화하여 인증서버에게 전달한다.

$$E_{KU_{AS}}(OTP, SID_U) \quad \text{(식 5)}$$

• **단계 3 :** 인증서버는 사용자로부터 전달된 정보 중 $SID_U$을 데이터베이스에 저장된 사용자 정보와 일치하는지 검색한다. 검색된 정보가 일치하지 않으면 서비스는 종료되고 일치하면 전달된 사용자 정보를 이용하여 $OTP'$ 를 생성한다. 서버는 생성된 $OTP'$와 사용자가 전달한 $OTP$를 비교하여 사용자를 검증한다.

$$OTP' \stackrel{?}{=} OTP \quad \text{(식 6)}$$

• **단계 4 :** 사용자 검증이 끝나면 인증서버 $AS$는 $OTP$와 $SID$의 사용자 정보를 기반으로 $ECM$과 $EMM$을 생성한다. 이 메시지는 인증서버가 사용자를 인증하는 정보로써 $EMM$ 메시지는 티켓으로 구성하여 사용자 권한 및 접근제어를 관리하게 된다.

$$ECM = CW \bullet g^{SID_U} \quad \text{(식 7)}$$
$$EMM = E_{SID_U}(CW, I_U, KU_U) \quad \text{(식 8)}$$

• **단계 5 :** 인증서버는 $ECM$와 $EMM$을 사용자의 공개키 $KU_U$로 암호화한 후 사용자에게 전송한다.

$$E_{KU_U}(ECM, EMM) \quad \text{(식 9)}$$

• **단계 6 :** 사용자는 인증서버로부터 받은 메시지를 사용자의 개인키 $KR_U$로 복호화한 후 $ECM$과 $EMM$을 검증한다. 검증이 완료되면 사용자는 인증서버에게 확인 메시지를 전달하고 검증이 완료되지 않으면 인증을 다시 요청한다.

$$D_{KR_U}(ECM, EMM) \quad \text{(식 10)}$$
$$Check \ \ ECM \text{ and } EMM \quad \text{(식 11)}$$

• **단계 7 :** 사용자로부터 $ECM$과 $EMM$의 검증 확인 메시지를 전달받은 인증서버는 (식 12)와 같은 과정을 통해 세션키 $SK$를 생성하여 사용자에게 전달한다. 생성된 세션키 $SK$는 사용자의 보안 인식자 $SID_U$로 암호화하여 사용자에게 전달한다.

$$\text{Generate } SK = H(OTP, ID_U, h(ID_{AS})) \quad \text{(식 12)}$$

$$Transfer \quad E_{SID_U}(SK) \qquad \text{(식 13)}$$

• **단계 8 :** 사용자는 서버로부터 전달받은 세션키 $SK$를 복호화하고 세션키 $SK'$를 식 (14)처럼 생성하여 비교한다. 사용자는 세션키 $SK$을 이용하여 제어문자(Control Word, CW)와 사용자 권한 정보 $I_U$를 암호화하여 인증서버에게 전달한 후 인증서버는 전달된 $E_{SK}(CW, I_U)$를 복호화하여 사용자 인증을 수행한다.

$$\text{Generate } SK' = H(OTP, ID_U, h(ID_{AS})) \qquad \text{(식 14)}$$

$$Compare \; SK \stackrel{?}{=} SK' \qquad \text{(식 15)}$$

$$E_{SK}(CW, I_U) \qquad \text{(식 16)}$$

$$\text{Decrypt } E_{SK}(CW, I_U) \qquad \text{(식 17)}$$

3.3.3 패스워드 변경 과정

사용자는 IPTV 게임 서비스를 제공받는 과정 중에 등록과정에서 입력한 패스워드 $KR_U$를 변경할 수 있다. 유지보수 과정은 서비스를 제공받는 사용자가 임의 시간에 패스워드를 변경하는 과정으로써 사용자의 패스워드를 변경하는 과정은 식 (18)와 같다. 식 (18)에서 사용자는 $SI'$를 계산한 후 인증서버와 셋톱박스에 저장되어 있는 $SI$를 $SI'$로 변경한다.

$$SI = I_U \oplus H(KU_U, X_{AS}) \qquad \text{(식 18)}$$

## Ⅳ. 평가

제안 프로토콜의 상호 인증과정을 통해 생성된 세션키 $SK$는 인증서버와 사용자만이 알고 있어 제 3자는 알 수 없다. 인증과정에서 생성한 $OTP$는 각 사용자가 서비스를 요청할 때 사용자가 소유하고 있는 제어문자 $CW$, 시간동기화 값 $T_U$, 카운트 $CT$, $PIN$ 정보를 이용하여 생성하기 때문에 제 3자가 시도하는 악의적인 공격 중 replay 공격과 impersonation 공격을 예방하는 역할을 수행한다. 제안 프로토콜에서는 매 통신마다 서로 다른 세션키 $SK$가 생성되며 생성된 세션키 $SK$는 EMM의 제어 문자 $CW$를 암호화하여 전달하기 때문에 제어문자 $CW$를 얻으려는 평문(plaintext) 공격의 암호 알고리즘 공격을 예방하고 있다.

제안 프로토콜은 IPTV 환경에서 발생하기 쉬운 cloning 문제를 해결하기 위해 사용자의 인식자 $KU_U$(=$ID_U$)와 패스워드 $KR_U$(=$KU_U \bullet g^{CW}$)를 해쉬 함수 $H(\bullet)$에 적용하여 권한 정보 $I_U$=$H(KU_U, KR_U)$를 생성함으로써 예방한다. 제안 프로토콜에서 생성되는 사용자의 보안 인식자 $SID_U$는 수신기마다 서로 다른 보안 인식자 $SID_U$를 사용하기 때문에 제 3자가 복제된 자신의 정보를 다른 수신기에 적용할 경우 수신기가 사용자를 인식하지 못하도록 하고 있다.

표 2. 프로토콜 비교 분석
Table. 2 Compare Analysis of Protocol

| 구분 | 스마트카드 복제방지 | McCommac Hack 방지 | 다중 STB 지원 | 완전한 전방향 안전성 | 암호 프리미티브 | 가장 공격 |
|---|---|---|---|---|---|---|
| Jiang[9] | ○ | × | × | × | 지수연산 | ○ |
| Yoon[10] | ○ | × | × | ○ | 지수연산 | ○ |
| Lee[11] | ○ | | × | ○ | 지수연산 | × |
| Hou[12] | ○ | × | × | × | 지수연산 | ○ |
| Kim[13] | ○ | × | × | × | 대칭키 기반 연산 | ○ |
| 제안 프로토콜 | ○ | ○ | ○ | ○ | 지수연산과 대칭키 기반 연산 | × |

이러한 방법은 수신기에 등록된 사용자의 인식자와 수신기가 해쉬함수에 의해 생성된 인식자 값이 서로 달라 cloning 문제를 예방하고 있다. 따라서, 복제된 스마트카드를 사용하는 사용자는 제안 프로토콜의 해쉬 함수에 의해 생성되는 인식자를 판별하기 어려워 제 3자가 자신의 스마트카드를 가지고 다른 수신기를 사용하는 것은 사실상 불가능하다.

제안 프로토콜은 네트워크를 통해 전송되는 메시지는 ID 기반 공개키/개인키쌍을 이용하여 제공하며 가입자와 인증서버간에는 상호인증이 제공되기 때문에 가입자는 $OTP$로 검증하고 인증서버는 ECM, EMM을 통해 검증할 수 있다. 불법적인 제3자가 가입자의 인증 정보 및 개인정보를 획득하려고 시도하더라도 제안 프로토콜에서는 메시지를 중간에 가로채더라도 인증서버와 사용자사이에 공유된 세션키 $SK$을 모르기 때문에 CW를 획득할 수 없어 개인정보 유출을 방지한다.

또한 제안 프로토콜은 공격자가 세션을 하이재킹하더라도 $OTP$를 사용하기 때문에 메시지를 재사용할 수 없으며, ID기반 공개키/개인키쌍을 통해 하이재킹으로부터 원천적으로 봉쇄가 가능하다.

표 2는 IPTV 보안 기술과 관련된 최근 연구들과 스마트 카드 복제방지, McCommac Hack, 다중 STB 지원, 완전한 전방향 안정성, 암호프리미티브, 가장 공격 등에 대해서 제안 프로토콜과 비교분석하고 있다.

표 2에서 기존 기법들은 모두 스마트카드에 사용가능한 단일 STB를 등록해 둠으로써 스마트카드의 불법 복제를 방지하였지만 이들은 다중 STB 환경을 지원하지 못한다. 또한 기존기법은 $CW$를 상호인증을 통해 생성한 세션키 $SK$를 이용하여 암호화 전송하는 방법으로 단순 도청을 막을 수 있지만 중간자 공격과 같은 가장 공격으로 $SK$를 획득할 수 있고 이를 통해 $CW$를 확보할 수 있기 때문에 $McCormac\ Hack$ 공격이 가능하다.

그러나 제안된 프로토콜은 cloning 문제이외에 McCormac Hack 문제 또한 예방하고 있다. McCormac 문제는 제3자가 소유하고 있는 스마트카드를 이용하여 다른 스마트카드가 전송한 메시지를 다른 수신기에게 전달하도록 하는 방법으로써 제안 프로토콜에서는 이 공격을 예방하기 위해 스마트카드와 수신기사이에서 생성된 세션키 정보를 다른 위치에 위치하는 수신기가 알지 못하도록 해쉬 함수와 서명키 기반의 암호 알고리즘을 사용하고 있다.

만일 스마트카드와 수신기 사이의 통신 과정 중에 발생되는 임의의 통신 메시지를 공격자가 스마트카드에 저장하더라도 제안 프로토콜의 세션키 $SK$는 매 통신마다 서로 다른 세션키가 생성되어 공격자의 스마트카드와 일치하지 않게 된다. 수신기는 공격자가 가지고 있는 스마트카드내에 저장되어 있는 메시지를 복호화할 수 없게 되어 서비스를 제공받지 못하게 된다.

## Ⅴ. 결론

이 논문에서는 IPTV 서비스를 제공받는 청소년이 청소년이용불가 게임에 쉽게 접근할 수 없도록 PIN코드를 이용한 IPTV 가구내 사용자 개별 인증 프로토콜을 제안하였다.

제안 프로토콜은 청소년이 청소년이용불가 게임에 불법적으로 접근하는 것을 예방하기 위해서 PIN 코드와 개별 비밀번호를 조합하여 생성한 키 값과 IPTV 가구내 주어진 권한 정보를 쌍으로 묶어 인증서버와 셋톱박스에 저장하여 청소년이 강제적으로 게임에 접근하려는 시도를 예방하였다.

제안 프로토콜은 청소년이 청소년이용불가 게임에 접근할 때마다 인증 서버로부터 비밀키를 새로 부여받아 PIN 코드와 조합되기 때문에 청소년의 불법적인 게임 사용을 예방하였다.

제안 프로토콜은 기존 프로토콜에 비해 해쉬함수를 이용하여 사용자가 지불하는 채널에 대한 수신자격을 올바르게 판별할 수 있도록 하였으며 스마트카드에서 발생되기 쉬운 cloning 문제와 McCormac 문제를 해결하기 위해서 세션키 $SK$를 상호 인증 과정에서 생성하였다. 세션키 $SK$는 EMM을 암호화하도록 하여 제 3자가 인식자를 판별하지 못하도록 하여 서비스를 이용할 수 없도록 하였다.

향후 연구에서는 수신제한시스템을 기반으로 DRM의 기능을 결합하여 가입자의 권한 접근 및 레벨을 부여한 인증 메커니즘을 연구 수행할 계획이다.

## 참고문헌


[ 1 ] Gartner Group, “An Introduction to IPTV (Television via Internet Protocol),” Oct. 2005.

[ 2 ] Y. S. Jeong, Y. T. Kim, Y. S. Jung, G. C. Park and S. H. Lee, “A Mutual Authentication Protocol based on Hash Function for Efficient Verification of User Entitlement in IPTV Service”, Journal of KIISE : Informatio Networking, Vol. 37, No. 3, pp. 187-197, Jun. 2010.

[ 3 ] Y. S. Jeong, Y. S. Jung, Y. T. Kim, G. C. Park and S. H. Lee, “A Security Model Analysis Adopt to Authentication State Information in IPTV Environment”, The Journal of Korea Information and Communication Society, Vol. 35, No. 3, pp. 421-430, Mar. 2010.

[ 4 ] Y. S. Jeong, Y. T. Kim, G. C. Park and S. H. Lee, “User Authentication Mechanism for using a Secure IPTV Service in Mobile Device”, The Journal of Korea Information and Communication Society, Vol. 34, No. 4, pp. 377-386, Apr. 2009.

[ 5 ] Y. S. Jeong, Y. T. Kim, G. C. Park and S. H. Lee, “A Low-weight Authentication Protocol using RFID for IPTV User”, Journal of The Korea Institute of Information Security and Cryptology, Vol. 19, No. 2, pp. 105-116, Apr. 2009.

[ 6 ] F. K. Tu, C. S. Laih, and H. H. Tung, “On Key Distribution Management for Conditional Access System on Pay-TV System,” IEEE Trans. On Consumer Electronics, vol. 45, pp. 151-158, February 1999.

[ 7 ] Y. L. Huang, S.P. Shieh, and J.C. Wang, “Practical Key Distribution Scheme for Channel Protection,” IEEE Twenty-Fourth Annual International Computer Software&Applications Conference, 2000.

[ 8 ] T. Jiang, S. Zheng, and B. Liu, “Key Distribution Based on Hierarchical Access Control for Conditional Access System in DTV Broadcast,” IEEE Trans. On Consumer Electronics, Vol.50, No. 1, pp.225-230, 2004.

[ 9 ] T. Jiang. Y. Hou, and S. Zheng, “Secure Communicatio between Set-Top Box and Smart Card in DTV Broadcasting”, IEEE Transaction on Consumer Electronics, Vol 50(3), pp. 882-886, 2004.

[10] E. Yoon and K. Yoo, “A New Secure Key Exchange Protocol between STB and Smart card in DTV broadcasting”, Proc. of the Intelligence and Security Informations(ISI), Vol. 3917, LNCS, pp. 139-150, 2009.

[11] S. Lee, N. Park,S. Kim, and J. Choi, “Cryptanalysis of secure key exchange protocol between STB and smart card in IPTV broadcasting”, Proc. of the Advances in Information Security and Assurance(AISA), Vol 5576, LNCS, pp. 797-803, 2009.

[12] T. Hou, J. Lai and C. Yen, “Based on Cryptosystem Secure Communication between Set-Top Box and Smart Card in DTV Broadcasting”, Proc of the TENCON07, pp. 1-5, 2007.

[13] H. Kim, “Secure Communication in Digital TV Broadcasting”, International Journal of Computer Science and Network Security(IJCSNS), vol.8(9), pp.1-5, 2008.


## 저자소개


**정윤수(Yoon-Su Jeong)**

1998. 청주대학교 전자계산학과 학사
2000. 충북대학교 대학원 전자계산학과 석사
2008. 충북대학교 대학원 전자계산학과 박사
2009. 9 ~ 현재 한남대 산업기술연구소 전임연구원
※관심분야 : 센서 보안, 암호이론, 정보보호, 네트워크 통신, 이동통신보안

**김용태(Yong-Tae Kim)**

1984. 한남대학교 계산통계학과 학사.
1988. 숭실대학교 전자계산학과 석사.
2008. 충북대학교 전자계산학과 박사.
2002. 12. ~2006.2 (주)가림정보기술 이사
2010. 8 ~ 현재 한남대학교 멀티미디어 학부 교수
※관심분야 : 모바일 웹서비스, 정보보호, 센서 웹, 모바일 통신보안