디지털 방송에서 안전하고 효율적인 접근 제어 프로토콜

Secure and Efficient Access Control Protocol in Digital Broadcasting System

이지선*, 김효동**
고려대학교*, 아주대학교**

Ji-Seon Lee(jslee702@korea.ac.kr)*, Hyo Kim(hkim@commres.org)**

요약

IPTV(Internet Protocol Television)는 다양한 멀티미디어 콘텐츠를 인터넷을 통하여 TV로 제공하는 방송과 통신이 융합된 기술이다. 방송을 송신하는 측은 멀티캐스트 방식으로 스크램블된 방송콘텐츠를 전송하고, 수신료를 지불한 가입자만이 인증 과정을 거쳐 스크램블된 방송콘텐츠를 디스크램블하여 수신할 수 있어야 한다. 일반적으로, 가입자 인증은 TV에 연결된 셋톱박스 (STB, Set-Top Box)와 스마트카드 기반으로 이루어지는데, 2004년 Jiang *et al.*이 관련 프로토콜을 제안하였고, 이 후에 여러 논문에서 보다 효율적인 프로토콜들이 제안되었다. 하지만, 이 프로토콜들은 모두 메모리와 계산 능력에 제한이 있는 스마트카드에 부담을 주는 모듈라 멱승 계산을 하도록 되어 있다. 본 논문에서는 해쉬함수와 exclusive-or 연산만을 이용한 효율적인 셋톱박스와 스마트 카드 간의 인증 및 키 교환 프로토콜을 제안하고, 제안하는 프로토콜이 다양한 공격에 안전함을 보인다.

■ 중심어 : | 디지털 방송 | IPTV | 상호 인증 | 키 교환 |

Abstract

IPTV is an emerging technology that combines both broadcasting and tele-communication technologies, and provides various multi-media contents to the service subscribers. In general, IPTV broadcasters transmit scrambled signals (multi-media contents) to the paying subscribers, and the users within the acknowledged network descramble the signals using the smart-card. That is, users are verified through communication between STB (Set-Top Box) and smart-card. In 2004, Jiang *et al.* proposed a secure protocol regarding the verification process. The method has been modified and enhanced by several following research works. However, all the methods that have been proposed so far required modular exponentiation operations which may raise the smart-card costs. In this paper, we propose a new efficient mutual authentication and session-key establishment protocol using only hash functions and exclusive-or operations, and show that the proposed protocol is still secure under various security attacks.

■ keyword : | Digital Broadcasting | IPTV | Mutual Authentication | Key Exchange |

접수번호 : #091029-001
접수일자 : 2009년 10월 29일
심사완료일 : 2009년 12월 15일
교신저자 : 김효동, e-mail : hkim@commres.org

I. 서 론

초고속 인터넷의 발달로 IP를 기반으로 한 다양한 융합 서비스가 발전하고 있는데, 이 중에서 특히 주목을 받는 것은 IPTV 서비스이다. IPTV는 방송 콘텐츠의 디지털화와 방송 통신의 융합 환경이 조성됨에 따라 빠르게 일반화되고 있는 서비스 분야이다. 이 기술은 IP를 이용하여 멀티미디어 콘텐츠를 전송하고 TV 단말기(Set-Top Box, STB)를 통해서 이를 수신함으로써 기존의 방송 서비스와 PC 기반의 인터넷 서비스를 동시에 제공할 수 있는 강점을 가지고 있다. 즉, IPTV는 인터넷과 텔레비전 기술이 융합된, 디지털 컨버전스의 한 유형이다. 따라서 컴퓨터에 익숙하지 않은 사람도 TV 모니터와 리모콘을 이용하여 인터넷이 제공하는 여러 서비스들을 제공받을 수 있다.

IPTV는 인터넷 망을 통하여 멀티캐스트 방식으로 방송 콘텐츠를 전송하는데, 이러한 서비스를 수신하기 위해서는 STB가 필요하다. 멀티캐스트 방식은 하나의 전송으로 동일 네트워크 상의 여러 명이 받아 볼 수 있도록 하는 방식인데, 이 때 가입자 인증으로 동일 네트워크에 가입되어 있지 않은 사용자가 콘텐츠에 접근하는 것을 막을 수 있어야 한다 (이를 walled garden이라고 부른다). 이를 위해서 수신제한시스템 (Conditional Access System, CAS)을 이용한다. CAS는 가입자 수신 STB에 위치해 수신제한용 키와 자격 제어를 담당하는 모듈로 일반적으로 스마트카드를 기반으로 운용된다[1]. 즉, 스마트카드에 정당한 사용자만이 이용할 수 있는 정보를 넣고 TV에 연결된 STB와의 인증 절차를 거친 후에, IP망을 통해서 멀티캐스트되는 스크램블된 콘텐츠 신호를 콘텐츠로 변환하여 TV 스크린에 보여주게 된다. 따라서 STB와 스마트카드 간의 인증은 불법시청을 방지하기 위해 매우 중요하다.

1. 연구 동기

일반적으로 스마트카드 기반의 인증 시스템은 '두 요소 인증 기법 (two-factor user authentication scheme)'이라고 하는데, 이는 사용자가 스마트카드와 패스워드 두 요소를 이용하여 인증을 하는 시스템을 의미한다. 최근에는 다양한 환경에서 보다 효율적인 두 요소 인증 기법이 제안되었는데, 이 기법들은 모두 모듈라 멱승 계산없이 안전하게 인증하려는 기법들이다. 왜냐하면, 모듈라 멱승 계산이 메모리와 계산 능력에 한계가 있는 스마트카드가 담당하려면 카드 단가가 비싸지기 때문이다. 따라서 같은 안전도를 보장하면서 모듈라 멱승 계산이 없는 기법을 제안하는 것은 의미 있는 일이다 [2-6].

2004년에 Jiang *et al.*[7]에 의해서 처음으로 디지털 방송을 위한 셋톱박스와 스마트카드 간의 인증 기법이 제안되었고, 2007년에 Hou *et al.*[8]에 의해 보다 효율적인 기법이 제안되었으며, 최근에 Yoon-Yoo[9]는 Jiang *et al.* 기법의 취약점을 보이고, 보다 안전한 인증 기법을 제안하였다. 하지만 Lee *et al.*[10]이 Yoon-Yoo 기법이 중간자 공격에 안전하지 않음을 보였다. 그러나 Yoon-Yoo가 보인 Jiang *et al.* 기법에 대한 취약점과 Lee *et al.*이 보인 Yoon-Yoo 기법에 대한 취약점은 해쉬함수가 셋톱박스와 스마트카드만이 아는 비밀정보라면 옳지 않은 공격이다. 이 점에 대해서 III장에서 기술하겠다.

제안된 이 모든 기법들은 스마트카드가 모듈라 멱승 계산을 해야 한다. 본 논문의 목적은 모듈라 멱승 계산이 없는 셋톱박스와 스마트카드 간의 인증 기법을 제공하는 것이다. 즉, exclusive-or 연산과 해쉬 함수만을 이용한 효율적인 기법으로 다음과 같은 다양한 공격에 안전한 기법을 제안할 것이다.

(1) 맥코맥핵 공격 (MaCormac Hack Attack) [11]: 스마트카드로부터 셋톱박스로 연결되는 데이터 라인을 같은 종류의 다른 셋톱박스로 전송하여 접근허가를 받으려는 공격.

(2) 스마트카드 복제 공격 (Smart Card Cloning Attack) [11]: 정당한 스마트카드를 복제하여 복제된 카드를 다른 셋톱박스에 넣어서 접근허가를 받으려는 공격.

(3) 재전송 공격 (Replay Attack) : 프로토콜 상에서 유효한 메시지를 골라 저장해 두었다가 나중에 재전송함으로써 정당한 사용자로 가장하는 공격.

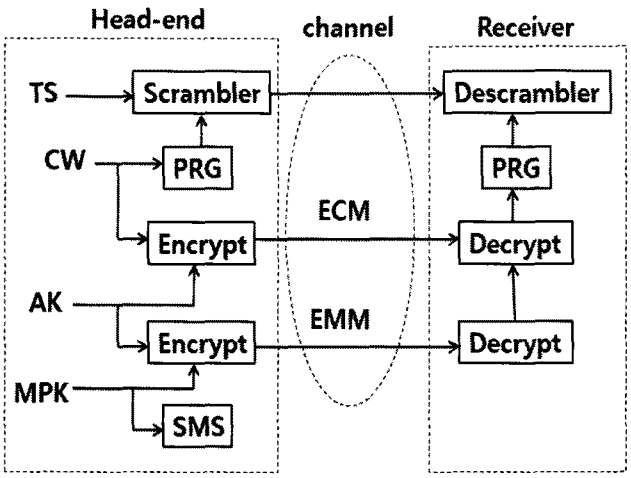


그림 1. 수신 제한 시스템 (CAS)

(4) 중간자 공격 (Man-In-The-Middle Attack) : 셋톱박스와 스마트카드 간의 통신 메세지를 공격자가 중간에서 도청하거나 자신이 변조한 메시지로 통신내용을 바꾸는 공격.

(5) 오프라인 패스워드 추측 공격 (Offline Password Guessing Attack) : 셋톱박스와 스마트카드 간의 통신 메시지들을 가지고 사용자의 패스워드를 획득하는 공격.

최근에는 보안을 위해서 두 요소 인증 프로토콜이 다음의 두 가지 상황에서도 안전해야 한다 [6].

(6) 스마트카드의 내용이 노출된다 하더라고 오프라인 패스워드 추측 공격이 불가능하도록 프로토콜이 구성되어야 한다.

(7) 실수로 패스워드가 노출된다고 하더라고 스마트카드가 없이는 인증이 되지 않도록 해야 한다.

2. 본 논문의 구성

본 논문의 구성은 다음과 같다. 우선 2장에서는 셋톱박스 내의 수신 제한 시스템에 대해 서술하고, 3장에서는 Jiang *et al.*의 기법과 Yoon-Yoo의 기법을 살펴본다. 4장에서는 새로운 인증 기법을 제안하고 5장에서는 제안한 기법의 안전성을 보이고 기존 연구들과 효율성을 비교해 본다. 마지막으로 6장에서는 결론을 맺는다.

II. 수신 제한 시스템 (Conditional Access System, CAS)

수신 제한 시스템은 TV에 연결된 셋톱박스 내에 있는 시스템으로 IPTV 서비스에서 정당한 가입자만이 콘텐츠를 볼 수 있도록 하는 기술이다 [그림1][7][12]. 방송서버 측에서 미디어 콘텐츠를 스크램블링 (scrambling, 암호화)하여 전송하고, 이를 받은 수신자가 셋톱박스 내의 수신 제한 시스템을 이용하여 인증 확인 후 허가되면 디스크램블링(descrambling, 복호화) 과정을 통해 콘텐츠를 볼 수 있도록 한다. 이 때 스크램블링된 자료를 전송 스트림 (Transport Stream, TS)이라 하고 이를 위하여 스크램블링/디스크램블링하기 위한 키로 제어 단어 (Control Word, CW)라고 하는 동일한 키를 사용한다.

헤드엔드에서의 스크램블링 과정을 좀 더 구체적으로 살펴보면 다음과 같다.

1. 제어 단어는 보안을 위하여 암호화한 후 자격 제어 메시지 (Entitlement Control Message, ECM) 형태로 전송된다. 이 때 제어 단어를 암호화하는 키로 인증키 (Authorization Key, AK)를 이용한다.
2. 인증키는 가입자 비밀키 (Master Private Key, MPK)를 사용해서 암호화한 뒤에 자격 관리 메시지 (Entitlement Management Message, EMM)를

통해 전송한다.

3. 전송 스트림(TS), 자격 제어 메시지(ECM), 자격 관리 메시지(EMM)가 같이 전송된다.

이 때 가입자 관리 시스템(Subscriber Management System, SMS)이 가입자 비밀키와 스마트카드를 관리한다. 일반적으로 가입자 비밀키는 가입자가 최초로 가입하는 시점에 가입자 관리 시스템에 의해 관련 비밀 정보들과 함께 스마트 카드 안에 내장되어 가입자에게 배포된다.

수신측에서 전송 스트림, 자격 제어 메시지와 자격 관리 메시지를 받으면 다음의 디스크램블링 과정을 거친다.

1. 수신측에서는 스마트카드에 저장된 가입자 비밀키를 이용하여 자격관리 메시지를 복호화하여 인증키를 알아낸다.
2. 복호화한 인증키를 이용하여 자격제어 메시지를 복호화하고 제어단어를 알아낸다.
3. 이 과정에서 스마트카드와 셋톱박스는 안전하게 제어 단어를 주고받기 위하여 공유키를 생성하고, 스마트카드는 제어 단어를 생성한 공유키로 암호화하여 셋톱박스로 보낸다. 암호화된 제어 단어를 받은 셋톱박스는 공유키로 복호하여 전송스트림을 디스크램블링하고 콘텐츠를 가입자에게 보여준다.

따라서 정당한 가입자만이 콘텐츠를 볼 수 있도록 하기 위해서는 스마트카드와 셋톱박스 간의 상호 인증이 필요하고, 제어 단어를 안전하게 전달하기 위하여 공유키를 생성하는 것이 중요하다.

III. 관련 연구들

이번 장에서는 2004년에 Jiang *et al.*이 제안한 프로토콜과 2008년에 Yoon-Yoo에 의해 제안된 프로토콜을 살펴 보겠다. 스마트카드와 셋톱박스가 상호 인증과 키 교환을 하고 제어 단어를 안전하게 전달하기 위해서 다음과 같이 5단계가 필요하다.

(1) 등록 단계 : IPTV에 가입하기 위하여 처음으로 등록하는 단계로 SMS는 스마트카드에 사용자 관련 정보와 인증을 위한 정보들을 입력한다.

(2) 로그인 단계 : 정당한 사용자는 가입한 프로그램을 받아 보기 위하여 스마트카드를 이용하여 셋톱박스에 로그인한다.

(3) 상호인증 단계 : 스마트카드와 셋톱박스 사이에 인증이 이루어진다.

(4) 세션 키 계산 단계 : 상호 인증 후에 스마트카드와 셋톱박스는 세션키를 공유한다.

(5) CW 전송 단계 : 공유한 세션키를 이용하여 대칭키 알고리즘을 통해 CW를 안전하게 전달한다.

기존 연구들과 본 논문에서 제안하는 기법을 보이기 위하여 다음과 같이 용어들을 정리한다.

- ID_C / PW : 사용자의 스마트카드 아이디/암호
- ID_S : 셋톱박스의 고유 일련 번호 (아이디). 셋톱박스의 고유 번호는 요금계정을 위해서 필요하며 서비스 제공업체에서 관리한다. 따라서 이 번호는 셋톱박스만이 알고 있는 비밀값이다.
- x_S : 셋톱박스의 비밀키
- p, q : 512비트, 140비트인 소수 공개값 ($q|p-1$)
- $h(\bullet)$: 일방향 해쉬 함수, 셋톱박스와 스마트카드만이 알고 있다.
- $E(\bullet)/E^{-1}(\bullet)$: 대칭키 암호 알고리즘
- $\oplus$: exclusive-or 연산자
- $\|$: concatenation 연산자

1. Jiang *et al.* 기법 [7]

2004년에 제안된 Jiang *et al.*의 프로토콜은 다음과 같다.

1.1 등록단계

사용자는 등록을 위해서 자신의 스마트카드 아이디 ID_C와 암호 PW를 SMS에 보내고 SMS는 R을 다음과 같이 계산한다.

$R = h(ID_C \oplus x_S) \oplus h(PW)$.

SMS는 스마트카드의 비밀키 x_C를 선택하고 대응되는 공개키 $y_C = g^{-x_C} \bmod p$를 계산한다. SMS는 $\{R, g, ID_C, ID_S, h(\cdot), E(\cdot), MPK\}$를 스마트카드에 입력하여 사용자에게 보낸다.

1.2 로그인 단계

사용자는 자신이 원하는 프로그램을 받아 보기를 원할 때, 자신의 스마트카드를 셋톱박스에 넣고, 자신의 아이디와 암호를 입력한다. 아이디 ID_C와 암호 PW를 입력받은 스마트카드는 다음의 순서로 로그인 단계를 수행한다.

(1) 두 개의 임의의 난수 $t, r \in Z_q^*$를 선택한 후 다음과 같이 T, Y, X를 계산한다.

$T = g^t \bmod p$

$Y = h(T \| ID_C \| ID_S)$

$X = R \oplus h(PW)$

(2) 스마트카드는 셋톱박스로 로그인 요청 메시지 $\{X, Y, r, ID_C\}$를 보낸다.

1.3 상호인증 단계

로그인 요청 메시지 $\{X, Y, r, ID_C\}$를 받은 셋톱박스는 다음과 같이 상호 인증 단계를 수행한다.

(1) 셋톱박스는 사용자의 아이디 ID_C가 옳은지 검사하고, 옳다면 다음의 등식이 성립하는지 확인한다.

$X = h(ID_C \oplus x_S)$

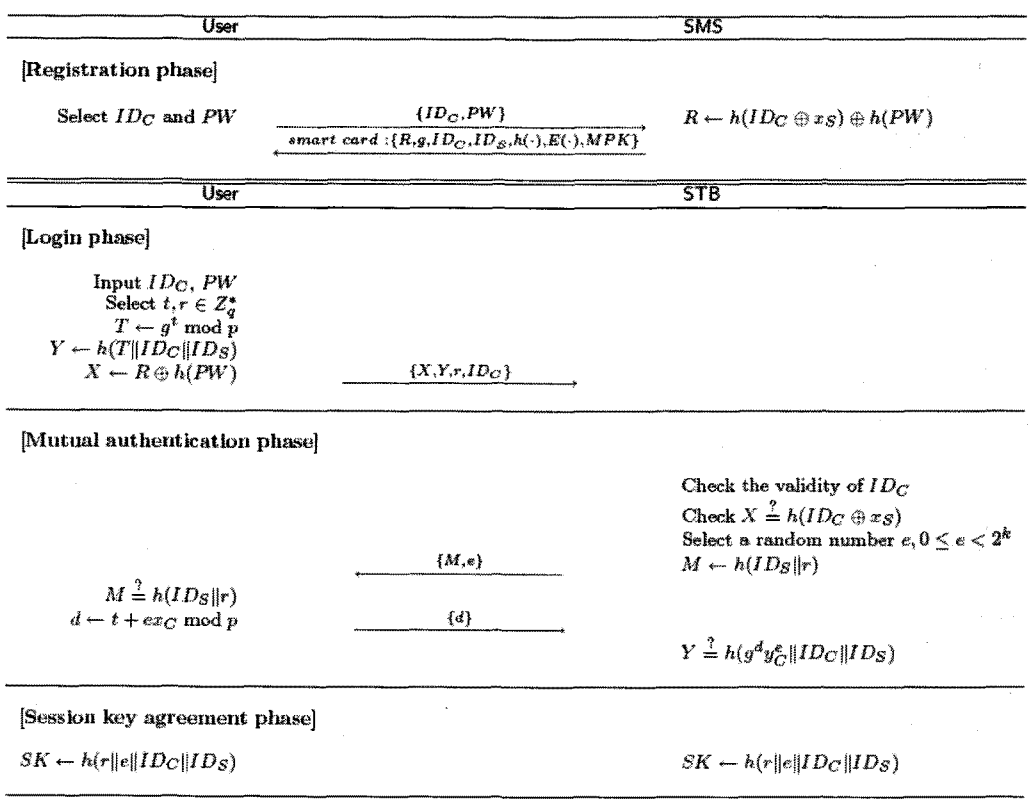


그림 2. Jiang *et al.*'s Protocol

(2) 위의 등식이 성립하면, 셋톱박스는 임의의 난수 $e, 0 \le e < 2^k$,를 M을 계산하여 $\{M,e\}$를 스마트카드로 보낸다.

$$M = h(ID_S \| r)$$

(3) $\{M,e\}$를 받은 스마트카드는 받은 M이 옳은 값이라면, 셋톱박스를 인증한다.

(4) 셋톱박스를 인증한 스마트카드는 다음과 같이 $\{d\}$를 계산하여 셋톱박스로 보낸다.

$$d = t + ex_C \bmod p$$

(5) 셋톱박스는 다음의 등식이 성립하는지 확인한다.

$$Y = h(g^d y_C^e \| ID_C \| ID_S)$$

(4) 위의 등식이 성립하면 셋톱박스는 스마트카드를 인증하고, 결국 상호 인증이 성립된다.

1.4 세션키 생성 단계

상호인증 단계가 성공적으로 이루어졌으면, 셋톱박스와 스마트카드는 각자 다음의 세션키를 계산하여 공유하게 된다.

$$SK = h(r \| e \| ID_C \| ID_S)$$

1.5 CW 전송 단계

스마트카드는 MPK를 이용하여 암호화되어 전송된 CW를 복호화한 후, SK를 이용하여 CW를 암호화하여 $CW_e = E_{SK}(CW)$를 구하고 셋톱박스로 보낸다. 셋톱박스는 $CW = E_{SK}^{-1}(CW_e)$를 통해 CW_e 를 복호화하여 CW를 구하고 프로그램을 디스크램블하여 사용자가 콘텐츠를 볼 수 있도록 한다.

Yoon과 Yoo는 자신들의 논문에서 Jiang *et al.*의 기법이 셋톱박스의 아이디 ID_S가 노출된다면 사용자 가장 공격 (impersonation attack)에 취약하다고 하였는데, 이는 옳지 않다. 왜냐하면, Jiang *et al.*은 자신들의 논문에서 해쉬 함수 $h(\cdot)$는 오직 셋톱박스와 스마트카드만이 안다고 했기 때문에 셋톱박스와 스마트카드 간에 주고받는 모든 메시지들 $\{X, Y, r, ID_C\}$, $\{M,e\}$, $\{d\}$와 ID_S를 안다고 하여도 $h(\cdot)$를 모른다면 $SK = h(r \| e \| ID_C \| ID_S)$를 계산할 수 없다. 또한 Yoon과 Yoo는 Jiang *et al.*의 기법이 전방향 안전성을 보장하지 못한다고 하였는데, 이 역시 옳지 않다. 왜냐하면, 같은 이유로, 즉, $h(\cdot)$를 모른다면 x_S를 안다고 하더라도 $SK = h(r \| e \| ID_C \| ID_S)$를 구할 수 없기 때문이다.

오히려 Jiang *et al.*의 기법에 문제가 되는 것은 스마트카드의 내용을 제 3자가 알게 되는 경우이다. 앞에서 기술했듯이 두 요소 인증 기법에서는 스마트카드 내용이 유출되는 경우에서도 안전하기를 요구한다. 하지만 Jiang *et al.*의 기법에서는 스마트카드 내용을 안다면 해쉬함수가 노출되기 때문에 Yoon과 Yoo가 얘기했던 사용자 가장 공격이 가능해 진다.

2. Yoon-Yoo 기법

2008년에 Yoon-Yoo는 다음의 기법을 제안하였다.

2.1 등록단계

사용자는 아이디 ID_C와 암호 PW를 SMS에 보내고 SMS는 R을 다음과 같이 계산한다.

$$R = h(ID_C \oplus x_S) \oplus PW$$

SMS는 $\{R, g, ID_S, h(\cdot), E(\cdot), MPK\}$ 를 스마트카드에 입력하여 U에게 보낸다.

2.2 로그인 단계

사용자는 자신이 원하는 프로그램을 받아 보기를 원할 때, 자신의 스마트카드를 셋톱박스에 넣고, 자신의 아이디와 암호를 입력한다. 아이디 ID_C와 암호 PW를 입력받은 스마트카드는 다음의 순서로 로그인 단계를 수행한다.

(1) 임의의 난수 $a \in Z_q^*$를 선택한 후 $A = g^a \bmod p$를 계산한다.

(2) 다음과 같이 X와 Y를 구한다.

$$X = R \oplus PW$$

$$Y = h(X \| A \| ID_C \| ID_S)$$

(3) 스마트카드는 로그인 요청 메시지 $\{ID_C, Y, A\}$를 셋톱박스로 보낸다.

2.3 상호인증 단계

로그인 요청을 받은 셋톱박스는 다음과 같이 상호 인증 단계를 수행한다.

(1) 셋톱박스는 우선 사용자의 아이디 ID_C가 옳은지 검사한다. 만약에 옳은 아이디가 아니면 로그인 요청을 거절한다.

(2) 셋톱박스는 다음의 등식이 성립하는지 확인한다.

$$Y = h(h(ID_C \oplus x_S) \| A \| ID_C \| ID_S)$$

위의 등식이 성립하면 다음 단계를 수행한다.

(3) 다음으로 셋톱박스는 임의의 난수 $b \in Z_q^*$를 선택한 후 다음과 같이 B, K, M을 계산하여 $\{B, M\}$ 을 스마트카드로 보낸다.

$$B = g^b \bmod p$$

$$K = A^b = g^{ab}$$

$$M = h(K \| A \| ID_C \| ID_S).$$

User		SMS
[Registration phase]		
Select ID_C and PW	$\xrightarrow{\{ID_C, PW\}}$ $\xleftarrow{smart\ card: \{R, g, ID_S, h(\cdot), E(\cdot), MPK\}}$	$R \leftarrow h(ID_C \oplus x_S) \oplus PW$

User		STB
[Login phase]		
Input ID_C, PW Select $a \in Z_q^*$ $A \leftarrow g^a \bmod p$ $X \leftarrow R \oplus PW$ $Y \leftarrow h(X \| A \| ID_C \| ID_S)$	$\xrightarrow{\{ID_C, Y, A\}}$	
[Mutual authentication phase]		
		Check the validity of ID_C $Y \stackrel{?}{=} h(h(ID_C \oplus x_S) \| T \| ID_C \| ID_S)$ Select $b \in Z_q^*$ $B \leftarrow g^b \bmod p$ $K \leftarrow A^b$ $M \leftarrow h(K \| A \| ID_C \| ID_S)$
	$\xleftarrow{\{B, M\}}$	
$K \leftarrow B^a \bmod p$ $M \stackrel{?}{=} h(K \| A \| ID_C \| ID_S)$ $D \leftarrow h(K \| B \| ID_C \| ID_S)$	$\xrightarrow{\{D\}}$	
		$D \stackrel{?}{=} h(K \| B \| ID_C \| ID_S)$
[Session key agreement phase]		
$SK \leftarrow h(K \| ID_C \| ID_S)$		$SK \leftarrow h(K \| ID_C \| ID_S)$

그림 3. Yoon-Yoo 기법

(4) 스마트카드는 $K = B^a \bmod p$를 계산하여 다음의 등식이 성립하는지 확인한다.

$$M = h(K \| A \| ID_C \| ID_S)$$

(5) 위의 등식이 성립하면 스마트카드는 셋톱박스를 인증하고 다음과 같이 D를 계산하여 셋톱박스로 보낸다.

$$D = h(K \| B \| ID_C \| ID_S)$$

(6) 셋톱박스는 $h(K \| B \| ID_C \| ID_S)$를 계산하여 스마트카드로부터 받은 D 값과 같은지 확인한다. 만일 두 값이 같다면 셋톱박스는 스마트카드를 인증하고, 결국 상호 인증이 성립된다.

2.4 세션키 생성 단계

상호인증 단계가 성공적으로 이루어졌으면, 셋톱박스와 스마트카드는 세션키 $SK = h(K \| ID_C \| ID_S)$를 공유한다.

2.5 CW 전송 단계

CW전송 단계는 Jiang *et al.*의 기법과 같다.

Lee *et al.*은 Yoon-Yoo 기법이 중간자 공격에 취약하다고 하였는데, 해쉬 함수 $h(\cdot)$를 오직 셋톱박스와 스마트카드만이 안다고 한다면, 이 역시 불가능한 공격이다. 하지만, 스마트카드의 내용이 노출된다면 $h(\cdot)$를 알 수 있기 때문에 Lee *et al.*이 지적한대로 중간자 공격이 가능해진다.

IV. 제안하는 기법

Yoon-Yoo가 제안한 인증 기법은 해쉬함수가 노출되지 않는다면, 지금까지 제안된 디지털 방송의 인증 기법 중에 보안 요구 사항을 모두 만족하는 기법이다. 하지만, 스마트카드에 부담이 되는 모듈라 멱승 계산이 필요하다. 우리는 본 장에서 모듈라 멱승을 사용하지 않고 빠른 해쉬함수와 exclusive-or 연산만을 이용해서 상호인증과 키교환을 하는 기법을 제안한다.

1. 등록 단계

사용자는 등록을 위해서 자신의 스마트카드 아이디 ID_C와 암호 PW를 선택하고 SMS로 보낸다. SMS는 다음과 같이 R을 계산한다.

$$R = h(ID_C \| x_S) \oplus PW_i$$

SMS는 $\{R, ID_S, h(\cdot), E(\cdot), MPK\}$ 를 스마트카드에 입력하여 사용자에게 보낸다. 여기에서 셋톱박스의 아이디 ID_S와 해쉬함수 $h(\cdot)$는 오직 셋톱박스와 스마트카드만이 아는 값이다.

2. 로그인 단계

사용자는 자신이 원하는 프로그램을 받아 보기를 원할 때, 자신의 스마트카드를 셋톱박스에 넣고, 자신의 아이디와 암호를 입력한다. 아이디 ID_C와 암호 PW를 입력받은 스마트카드는 다음의 순서로 로그인 단계를 수행한다.

(1) 입력받은 ID_C와 PW와 임의의 난수 a 값을 선택하여 다음과 같이 K와 W 를 계산한다.

$$K = R \oplus PW$$

$$W = K \oplus a$$

(3) 스마트카드는 로그인 요청 메시지 $\{ID_C, W\}$ 를 셋톱박스로 보낸다.

3. 상호인증 단계

로그인 요청 메시지 $\{ID_C, W\}$ 를 받은 셋톱박스는 다음과 같이 상호 인증 단계를 수행한다.

(1) 셋톱박스는 $K = h(ID_C \| x_S)$를 구한 후 $a = K \oplus W$ 를 계산한다.

(2) 셋톱박스는 임의의 난수 b을 선택하여 다음과 같이 X와 Y를 계산하여 $\{X, Y\}$ 를 스마트카드로 보낸다.

$$X = K \oplus b$$

$$Y = h(W \| a \| ID_S).$$

(3) $\{X, Y\}$를 받은 스마트 카드는 $b = K \oplus X$를 계산하여 다음의 등식이 성립하는 확인한다.

$$Y = h(W \| a \| ID_S)$$

(4) 위의 등식이 성립하면 스마트카드는 셋톱박스를 받아들이고 다음과 같이 Z를 계산하여 셋톱박스로 보낸다.

$$Z = h(X \| b \| ID_S)$$

(5) 셋톱박스는 자신이 선택했던 b와 자신의 아이디를 이용하여 스마트카드로부터 받은 Z 값이 $h(X \| b \| ID_S)$의 계산값과 일치하는지 확인한다. 만약에 두 값이 같다면, 셋톱박스는 스마트카드를 인증하고, 상호 인증이 성립하게 된다.

4. 세션키 생성 단계

상호인증 단계가 성공적으로 이루어졌으면, 셋톱박스와 스마트카드는 다음과 같은 세션키 SK를 공유한다.

$$SK = h(K \| a \| b \| ID_C \| ID_S).$$

5. CW 전송 단계

CW전송 단계는 Jiang *et al.*의 기법과 같다.

V. 제안하는 기법 분석

Ⅲ장에서 살펴본 Jiang *et al.*의 기법과 Yoon-Yoo 기법에서는 스마트카드 내용이 노출되어 해쉬 함수를 알

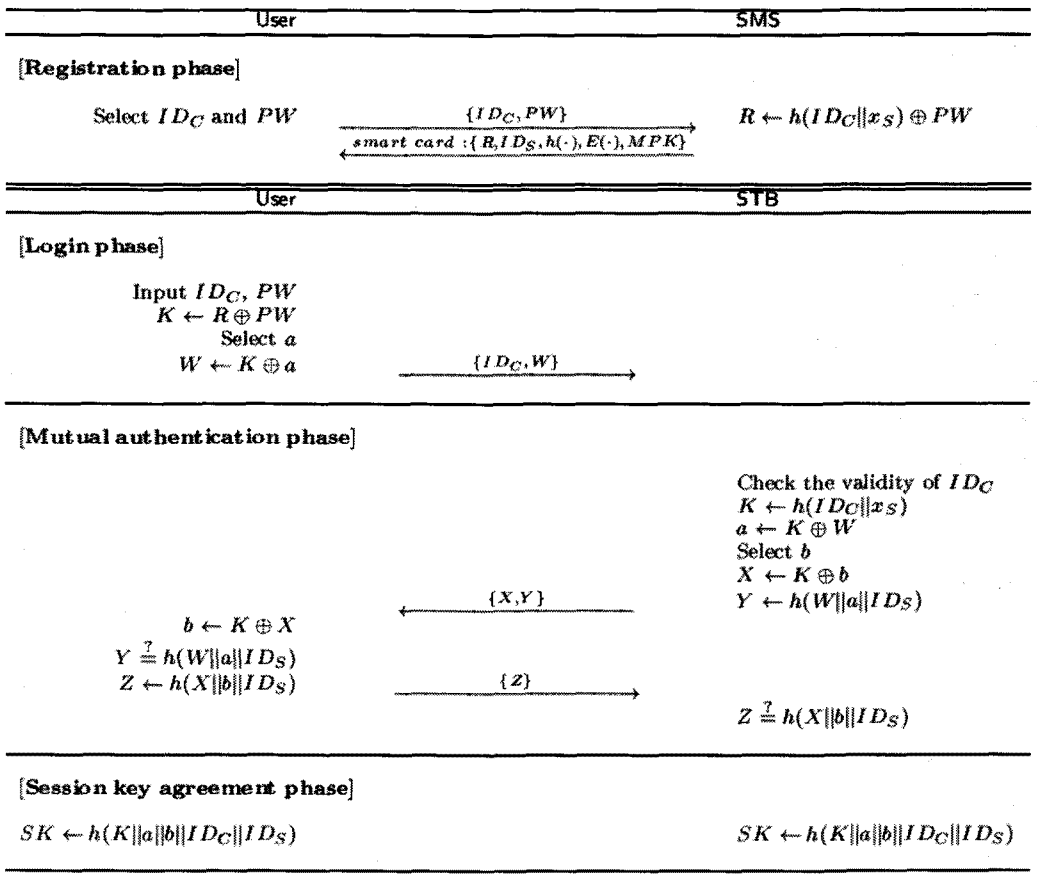


그림 4. 제안하는 기법

게 된다면, Jiang et al.의 기법에서는 제 3자가 세션키를 계산해낼 수 있음을 기술했고, Yoon-Yoo의 기법에서는 중간자 공격이 가능함을 보였다. 이번 장에서는 우리가 제안하는 기법이 I장에서 기술한 보안 요구 사항에 만족함을 보이겠다.

1. 안전도 분석

이번 절에서는 제안하는 기법이 I장에서 기술했던 공격들에 안전함을 보인다.

1.1 맥코맥핵 공격에 대한 안전성

맥코맥 핵 공격 (McCormac Hack Attack)은 스마트카드로부터 셋톱박스로 연결되는 데이터 라인을 같은 종류의 다른 셋톱박스로 전송하여 접근 허가를 받으려는 공격인데, 우리가 제안하는 기법은 이 공격에 안전하다. 즉, 제안하는 기법에서 스마트카드가 가지고 있는 ID_S 는 각 셋톱박스가 갖는 유일한 식별자이기 때문에 다른 식별자를 갖는 셋톱박스와는 인증이 불가능하다.

1.2 스마트카드 복제 공격에 대한 안전성

스마트카드 복제 공격은 정당한 스마트카드를 복제하여 자신이 이용할 수 없는 셋톱박스에 넣어서 접근 허가를 얻어내려는 공격이다. 제안하는 기법은 이러한 공격에 안전한데, 이유는 맥코맥핵 공격에서와 같이 각 셋톱박스가 자신의 고유한 식별자 ID_S와 비밀키 x_S를 가지고 있기 때문이다.

1.3 재전송 공격에 대한 안전성

제안하는 기법은 재전송 공격(replay attack)에 안전하다. 왜냐하면, 재전송 공격에 이용될 수 있는 W, X, Y, Z 값이 매 세션마다 다른 임의의 난수 a 또는 b를 포함하기 때문이다.

1.4 중간자 공격에 대한 안전성

제안하는 기법에서 스마트카드가 셋톱박스를 인증하도록 하기 위해서는 중간자가 스마트카드가 받아들일 수 있도록 Y 값을 계산해야 한다. 하지만, 임의의 난수 a 없이는 스마트카드가 받아들일 수 있는 Y 값을 계산하는 것은 불가능하다.

1.5 오프라인 패스워드 추측 공격에 대한 안전성

제안하는 기법에서 패스워드 추측 공격을 하려면 $W = R \oplus PW \oplus a$ 에서 패스워드 추측 공격을 해야 하는데, 이 공식에서는 두 개의 값 R과 a를 모르기 때문에 패스워드 추측 공격이 불가능하다.

1.6 스마트카드 내용이 노출되는 경우에 대한 안전성

만약에 스마트카드의 내용이 노출이 된다면 공격자는 스마트카드의 내용을 가지고 스마트카드 가장 공격을 시도하거나, 패스워드 추측 공격을 시도할 것이다. 하지만, 이 둘은 모두 불가능하다.

(1) 가장 공격 : 스마트카드 내용만을 가지고 정당한 가입자로 가장하려면 셋톱박스가 받아들일 수 있는 W 값을 계산해야 하는데, 이는 패스워드 없이 불가능하다.

(2) 패스워드 추측 공격 : 스마트카드의 내용과 도청한 메시지들을 가지고 패스워드를 추측하려면 앞에서 언급한 오프라인 패스워드 추측 공격에서처럼 $W = R \oplus PW \oplus a$ 식에서 시도해야 하는데, 여기에서 W와 R를 안다고 하여도 임의의 난수 a를 모르기 때문에 패스워드 추측 공격은 불가능하다.

(3) 중간자 공격 : 우리가 제안하는 기법에서 상호 인증이 이루어지고 세션키를 제대로 계산하려면 사용자가 선택한 임의의 난수 a와 b를 알아야 한다. 따라서 중간자 공격은 불가능하다.

(4) 세션키 생성 불가능 : 세션키 SK 를 계산하기 위해서는 K를 알아야 한다. 하지만, 스마트카드 내용을 안다고 하더라고 사용자의 패스워드 또는 셋톱박스의 비밀키를 알아야 K를 계산할 수 있기 때문에 세션키를 스마트카드만을 가지고 계산할 수 없다.

표 1. 세 기법의 효율성 비교

	등록 단계	로그인 단계	상호인증 단계
Jiang et al.	$2T_h$ $2T_\oplus$ $1T_e$	$2T_h$ $1T_\oplus$ $2T_r$ $1T_e$	$4T_h$ $1T_r$ $2T_e$
Yoon-Yoo	$1T_h$ $2T_\oplus$	$1T_h$ $1T_\oplus$ $1T_r$ $1T_e$	$6T_h$ $1T_r$ $3T_e$
제안하는기법	$1T_\oplus$	$2T_\oplus$ $1T_r$	$5T_h$ $1T_r$ $3T_\oplus$

1.7 패스워드가 노출되는 경우에 대한 안전성

제안하는 기법에서 공격자가 사용자의 패스워드를 안다고 하여도, 스마트카드 내용을 모르면 K 값을 구할 수 없다. 따라서 제안하는 기법은 패스워드가 노출된다고 하더라도 안전함을 알 수 있다.

2. 효율성 분석

Yoon-Yoo는 자신들의 논문에서 Jiang *et al.* 프로토콜과 자신들의 프로토콜에 필요한 시간들을 비교하였다. 우리는 여기에 더하여 우리의 기법이 모듈라멱승 계산이 없다는 점에서 보다 효율적임을 보이고, 시간을 분석하겠다.

우선 시간 분석에 쓰이는 용어들은 같다.

- T_h : 일방향 해쉬 함수 계산에 필요한 시간
- $T_\oplus$: exclusive-or 계산에 필요한 시간
- T_r : 임의의 정수 선택에 필요한 시간
- T_e : 모듈라 멱승 연산에 필요한 시간
- T_s : 대칭키 암호에 필요한 시간

Jiang *et al.* 기법, Yoon-Yoo 기법, 그리고 우리가 제안하는 기법 모두 세션키 계산 단계, 그리고 CW 전달 단계에서는 다음과 같이 같은 시간이 필요하다.

- 세션 키 SK 계산 단계 : $2T_h$
- CW 전달 단계 : $2T_s$

따라서 여기에서는 등록단계, 로그인 단계, 상호 인증 단계에 필요한 계산량을 표로 정리한다. [표 1]에서 보듯이 가장 큰 차이는 상호인증단계에 있다. 즉, Yoon-Yoo의 기법에서는 3번의 모듈라 멱승 연산이 필요한 반면, 우리가 제안하는 기법에서는 모듈라 멱승 대신에 3번의 exclusive-or 연산이 필요하다.

VI. 결 론

최근에 Yoon-Yoo가 제안한 디지털 방송에서의 인증 기법은 스마트카드가 노출되지 않고 해쉬함수가 안전하다는 가정하에서 지금까지 제안된 기법 중에 보안 요구 사항을 모두 만족하는 기법이다. 하지만, 스마트 카드가 모듈라 멱승 계산을 해야 한다. 우리는 본 논문에서 모듈라 멱승을 사용하지 않고 빠른 해쉬함수와 exclusive-or 연산만을 이용한 셋톱박스와 스마트카드 간의 상호 인증과 세션 키 설계 기법을 제안하고, 제안한 기법이 가능한 여러 공격들에 안전함을 보였다. 또한 해쉬함수, 모듈라 연산, exclusive-or 연산의 계산량을 분석함으로써 제안하는 기법이 Jiang *et al.* 기법이나 Yoon-Yoo 기법보다 효율적임을 보였다. 또한 우리가 제안하는 기법은 스마트카드가 노출된다 하더라도 안전함을 보였다.

참 고 문 헌

[1] 박종열, 문진영, 백의현, "IPTV 융합 서비스를 위한 보안 기술 동향," 전자통신동향분석, 제23권, 제5호, 2008(10).

[2] W.-S. Juang, "Efficient Password Authenticated Key Agreement Using Smart Cards," Computers & Security 23, pp.167-173, 2004.

[3] Y.-C. Chen and L.-Y. Yeh, "An Efficient Nonce-based Authentication Scheme with Key Agreement," Applied Mathematics and Computation 169, pp.982-994, 2005.

[4] W.-G. Shieh and J.-M. Wang, "Efficient Remote Mutual Authentication and Key Agreement," Computers &Security 25, pp.72-77, 2006.

[5] W.-G. Shieh and W.-B. Horng, "Efficient and Complete Remote Authentication Scheme with Smart Cards," IEEE International Conference on Intelligence and Security Informatics, pp.122-127, 2008.

[6] G. Yang, D. S. Wong, H. Wang, and X. Deng, "Two-factor Mutual Authentication Based on Smart Cards and Passwords," Journal of Computer and System Sciences 74, pp.1160-1172, 2008.

[7] T. Jiang, "Key Distribution Baesd on Hierarchical Access Control for Conditional Access System in DTV Broadcast," IEEE Trans. on Consumer Electronics, Vol.50, No.3, pp.882-886, 2004.

[8] T.-W. Hou, J.-T. Lai, and C.-L. Yeh, "Based on Cryptosystem Secure Communication between Set-top Box and Smart card in DTV Broadcasting," TENCON 2007, IEEE Region 10 Conference, pp.1-5, 2007.

[9] E.-J. Yoon and K. Yoo,, "Robust Key Exchange Protocol between Set-top Box and Smart Card in DTV Broadcasting," Informatica, Vol.20, No.1, pp.139-150, 2009.

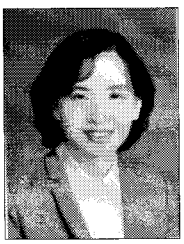
[10] S.-H. Lee, N.-S. Park, S.-K. Kim, and J.-Y. Choi, "Cryptanalysis of Secure Key Exchange Protocol Between STB and Smart Card in IPTV Broadcasting," ISA 2009, LNCS 5576, pp.797-803, 2009.

[11] W. Kanjanarin and T. Amomraksa, "Scambling and Key Distribution Scheme for Digital Television," IEEE International Conference on Networks, pp.140-145, 2001.

[12] F. Kamperman and B. V. Rijnsoever, "Conditional Access System Interoperability through Software Downloading," IEEE Trans. on Consumer Electronics, Vol.47, No.1, pp.47-53, 2001.

저 자 소 개

이 지 선(Ji-Seon Lee) 정회원



- 1991년 2월 : 서강대학교 전산학과(학사)
- 1998년 8월 : 서강대학교 컴퓨터공학과(석사)
- 2008년 2월 : 서강대학교 컴퓨터공학과(박사)
- 2008년 3월 ~ 현재 : 고려대학교 BK21 유비쿼터스 정보보호 사업단 연구교수

<관심분야> : 암호학, 네트워크 보안, 콘텐츠 보안

김 효 동(Hyo Kim) 정회원

- 1992년 2월 : 서강대학교 사학과(학사)
- 1997년 8월 : Univ. of Utah, Communications(석사)
- 2003년 1월 : Rutgers Univ. Communications(박사)
- 2004년 9월 ~ 현재 : 아주대학교 미디어학부 부교수

<관심분야> : 커뮤니케이션 테크놀로지, 디지털방송