DOI: 10.3745/KIPSTC.2010.17C.1.37

IPTV 환경에서 스마트카드 복제에 강건한 다중 셋톱박스 인증기법

임 지 환[†] · 오 희 국[††] · 김 상 진[†††]

요 약

IPTV 시스템에서 콘텐츠 및 서비스 제공자의 권익보호는 수신제한시스템(CAS, Conditional Access System) 및 디지털저작권관리(DRM, Digital Right Management)를 통해서 이루어진다. 특히 CAS의 경우, 계층화된 인증키를 사용하여 권한이 있는 사용자에게만 암호화된 콘텐츠를 복호화할 수 있도록 한다. 하지만 CAS가 콘텐츠 제공자와 스마트카드(SC, Smart Card) 사이 구간만의 보안을 제공하기 때문에 셋톱박스(STB, Set-Top Box)와 SC 간 보호 받지 못하는 채널을 도청하는 McCormac Hack 공격이나 SC 복제 공격으로부터 시스템을 보호할 수 없다. 본 논문에서는 McCormac Hack 공격뿐 만 아니라 SC 복제 공격에도 강건하면서 다중 STB를 지원할 수 있는 SC / STB 인증 기법을 제안한다. SC 복제 공격을 막기위해 SC등록 단계에서 STB와 SC를 바인딩하였던 기존 기법은 다중 STB환경을 지원하지 못한다. 제안하는 시스템은 가입자관리시스템에서 STB 정보를 IPTV의 양방향 채널 특성을 이용하여 동적으로 갱신함으로서 사용자의 다중 STB를 효과적으로 지원한다.

키워드 : IPTV, 스마트카드 복제, 다중 셋톱박스, 수신제한시스템

A Robust Multiple Set-Top Box Authentication Scheme for IPTV Against Smart Card Cloning Attack

Jihwan Lim[†] · Heekuck Oh[††] · Sangjin Kim[†††]

ABSTRACT

In an IPTV system, the rights of the content and service provider can be protected by using Conditional Access System (CAS) and Digital Right Management (DRM). In case of the CAS, only the authorized user who has structured authentication keys can decrypt the encrypted content. However, since the CAS establishes a secure channel only between content provider and Smart Card (SC), it cannot protect the system against McCormac Hack attack which eavesdrops on unsecure channel between SC and Set-Top Box (STB) and SC cloning attack. In this paper, we propose a robust multi-STB assisted SC / STB authentication protocol which can protect the IPTV system against not only McCormac Hack attack, but also SC cloning attack. The previous works which bind a STB and a SC during the SC registration phase against the SC cloning attack does not support multi-STB environments. The proposed system which dynamically updates the STB information in subscriber management system using the bi-directional channel characteristic of IPTV system can support the user's multi-STB device effectively.

Keywords : IPTV, Smart Card Cloning, Multiple Set-Top Box, Conditional Access System

1. 서 론

아날로그 TV에서 디지털 TV로의 변화, 광대역 통신 인프라의 보급 등은 방송과 인터넷의 융합을 이끌었고 IPTV 서비스를 실현 가능하게 만들었다. 인터넷과 방송의 융합이라는 점에서 디지털 컨버젼스의 한 유형인 IPTV는 인터넷 초고속 통신망을 이용하여 방송 콘텐츠를 제공하는 서비스이다. IPTV의 개념은 VOD(Video On Demand)의 개념에서부터 시작되었으나, 실시간 방송 서비스뿐만 아니라 다양한 양방향 서비스로의 확장이 빠르게 진행되고 있으며, PC에 비해 접근도가 높은 가전기기 및 정보 단말기를 포함하는 매체의 다형성 또한 주도하며 그 상업적 가치를 높이고 있다.

IPTV에서 사업자는 수신제한시스템(CAS, Conditional Access System) 및 디지털저작권관리(DRM, Digital Right Management)를 통해 제공하는 콘텐츠 및 서비스에 대한

※ 본 연구는 지식경제부 및 정보통신산업진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음(NIPA-2009-C1090-0902 -0035).
이 논문은 2009년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. 2009-0080351).
† 준 회 원 : 한양대학교 컴퓨터공학과 박사과정(주저자)
†† 종신회원 : 한양대학교 컴퓨터공학과 교수
††† 종신회원 : 한국기술교육대학교 인터넷미디어공학부 부교수(교신저자)
논문접수 : 2009년 11월 25일
수 정 일 : 1차 2009년 12월 28일
심사완료 : 2009년 12월 28일

권익을 보호받는다. 넓은 의미로서의 DRM은 CAS 및 콘텐츠의 복제 방지(copy protection)를 포함한 전사적인 저작권 보호 및 관리를 의미하지만 IPTV에서는 일반적으로 DRM을 사업자에서 사용자에게 넘어온 콘텐츠의 불법적 복제를 방지하는 기술(content protection)로, CAS를 사업자와 사용자 사이의 종단 간 서비스 보호 기술(service protection)로 간주한다[7, 8].

사업자는 CAS를 이용하여 권한 있는 사용자에게만 콘텐츠를 전달할 수 있다. 사업자의 가입자관리시스템(SMS, Subscriber Management System)은 가입자가 납부한 요금에 따라 스마트카드(SC, Smart Card)를 발급하고 가입자는 스마트카드 내에 저장된 키를 이용하여 암호화된 콘텐츠를 복호화 할 수 있으며 셋톱박스(STB, Set-Top Box)를 통해 디코딩/디스크램블링(decoding/descrambling) 후 콘텐츠를 재생하게 된다. 하지만 이와 같은 시스템은 Kanjanarin 등[1]이 소개한 McCormac Hack 공격과 스마트카드 복제 공격에 취약성을 가진다. 공격자는 셋톱박스와 스마트카드 사이의 보안되지 않은 채널에서 전송되는 제어어(CW, Control Word)를 손쉽게 획득할 수 있고 이를 다른 셋톱박스에 넘겨줌으로서 불법적으로 유료 콘텐츠를 배포할 수 있으며 스마트카드를 복제하여 한 번의 과금으로 다수의 불법적 가입자를 생성해 낼 수 있다.

본 논문에서는 IPTV의 양방향 서비스 특성을 활용하여 스마트카드와 셋톱박스의 바인딩 정보를 SMS에 등록하고 등록된 셋톱박스에 대한 세션키를 티켓 형식으로 발급하는 방법으로 스마트카드 복제 문제와 McCormac Hack 문제를 동시에 해결한다. 제안하는 기법은 단일 사용자가 사용하는 다수의 셋톱박스 및 사용자 디바이스를 지원하도록 설계 되었으며 복제된 스마트카드를 사용할 경우 이전에 등록된 스마트카드와 셋톱박스의 바인딩 정보를 갱신함으로서 콘텐츠의 디스크램블이 불가능하도록 하여 불법적 가입자의 생성을 막는다.

본 논문의 구성은 다음과 같다. 먼저 2장에서는 일반적인 IPTV 시스템의 구조와 수신제한시스템의 동작을 소개하고 IPTV 환경에서 효과적인 수신자 제어 프로토콜 설계를 위한 설계이슈를 서술한다. 3장에서는 기 제안된 스마트카드와 셋톱박스 간 키동의 프로토콜들에 대해서 살펴보고, 4장에서는 제안하는 스마트카드 인증 시스템을 소개한다. 5장에서는 제안한 시스템의 안전성을 분석하고 6장에서 결론을 짓는다.

2. 연구 배경 및 프로토콜 설계

2.1 표기법

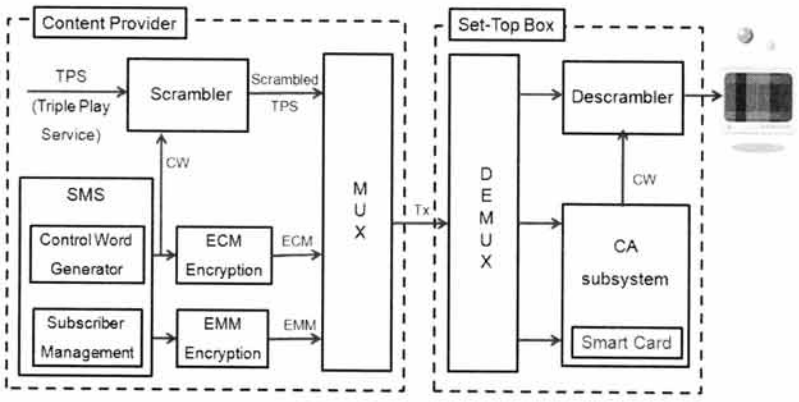
본 논문에서는 관련 연구 및 제안하는 프로토콜의 서술에 <표 1>의 표기법을 사용한다.

2.2 수신제한시스템(CAS, Conditional Access System)

IPTV에서 CAS는 사업자의 유료화 정책에 맞게 요금을 지불한 가입자에게만 원하는 콘텐츠 및 서비스를 제공하는 시스템으로서, 방송 사업자에게는 무자격자의 불법적 콘텐츠 획득 및 서비스 이용을 사전 방지할 수 있게 하고 가입자에게는 개인의 선호도가 반영된 다양한 서비스를 제공받을 수 있는 기회를 제공한다. CAS는 SMS와 함께 운용되어 가입자에게 원하는 프로그램의 제공하며 PPV(Pay-Per-View) 및 VoD(Video on Demand)등과 같은 다양한 부가서비스가 안전하게 지원될 수 있게 한다. (그림 1)은 CAS의 기본 구조를 보여준다. 사업자(Content Provider)는 TPS(Triple Play Service)로 불리는 비디오(video), 오디오(audio), 데이터(data) 콘텐츠를 제어어를 이용하여 스크램블링하여 전송하고 이를 수신한 가입자는 스마트카드를 이용하여 역으로 제어어를 획득해 디스크램블링한다. 스크램블링에 사용되는 이 제어어는 인증키(AK, Authentication Key) 또는 서비스 키로 불리는 키로 암호화 되어 자격제어메시지(ECM, Entitlement Control Message)에 포함되어 전송되고, 인증키는 다시 사용자의 마스터키(MPK, Master Private Key)로 암호화되어 자격관리 메시지(EMM, Entitlement Management Message)를 통해 가입자에게 전달된다. 고객 정보를 관리하는 가입자관리시스템(SMS, Subscriber Management System)에서는 접근제어 관련 정보만을 가지고 가입자의 가입 및 탈퇴에 따라 자격관리메시지와 자격제어메시지를 생성하여 신규 가입자가 가입한 방송 채널을 수신하거나 탈퇴한 가입자가 더 이상 방송을 수신하지 못하도록 하는 기능을 가입자 인증시스템(SAS, Subscriber Authentication System)을 통해 사업자에게 제공한다. 사업자는 가입자의 마스터키를 스

〈표 1〉 표기법

SMS	가입자관리시스템 (Subscriber Management System)	SC	스마트카드 (Smart Card)
STB	셋톱박스 (Set-Top Box)	$E_K(M)$	키 K로 메시지 M을 대칭키 암호화함
$D_K(M)$	키 K로 메시지 M을 대칭키 복호화함	H	암호학적 일방향 해쉬함수
ID_{SC}	스마트카드의 아이디	ID_{STB}	셋톱박스의 아이디
PW	사용자 비밀번호	K_{STB}	셋톱박스의 비밀키
p, q	서로 다른 큰 소수이며$(p-1 \mid q)$	g	$GF(p)$의 원시 원소
a, b	Z_q^*의 임의 원소		



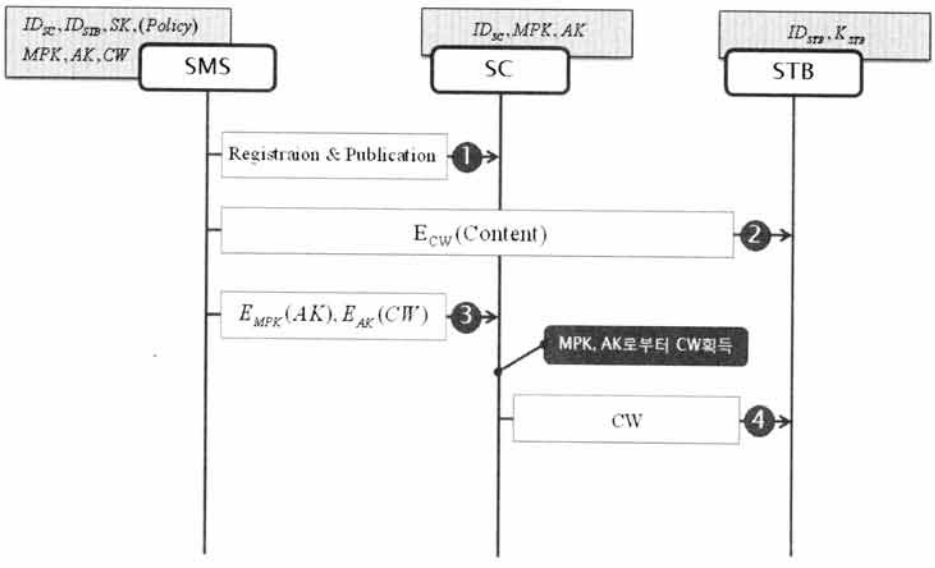
(그림 1) 수신제한 시스템 기본 구조

마트카드에 등록하여 발급하기 때문에, 가입자는 스마트카드를 이용해 콘텐츠의 디스크램블링에 필요한 제어어를 획득할 수 있다. 제어어는 비교적 작은 크기로 생성되기 때문에 보안을 위해 짧은 주기마다 갱신해주어야 하며, 갱신 될 때마다 인증키로 암호화되어 ECM에 실린다. ECM에는 암호화된 제어어 외에 제어변수가 포함되며, 수신기는 전송된 ECM을 수신할 수는 있지만 제어변수와 수신기의 인증변수를 비교하여 정당한 사용자로 판단될 경우에만 제어어를 해독하고, 이를 이용하여 수신된 프로그램을 디스크램블링한다. 반면 EMM은 가입자의 마스터키로 암호화된 인증키를 포함하며, 수신기에 자격을 부여하고 갱신, 관리하는 역할을 담당한다.

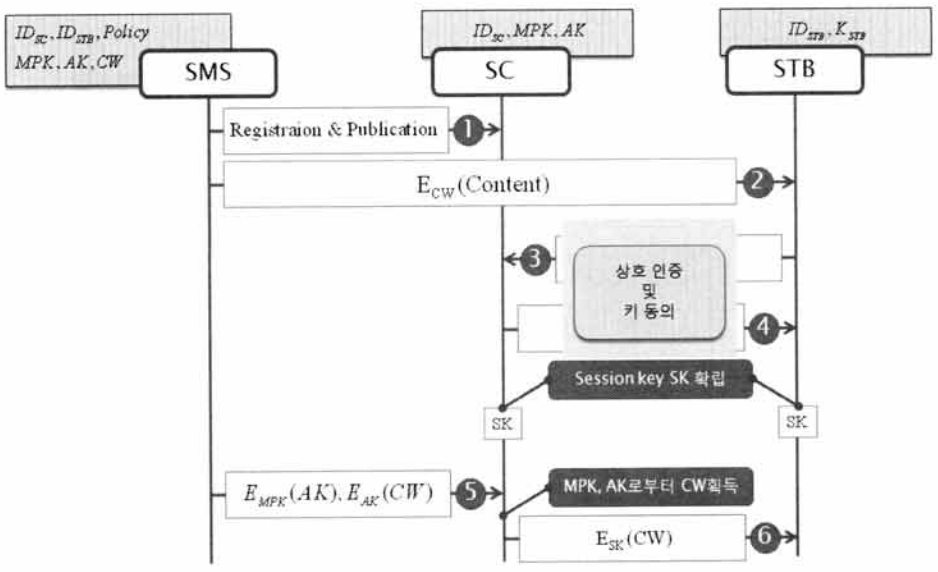
2.3 프로토콜 설계

앞서 언급한 것처럼 CAS는 개별 갱신 주기를 가지는 계층화된 키 구조를 통해 SMS와 스마트카드 사이의 구간에서 보안채널을 형성하게 된다. [1]은 CAS를 통해 정상적으로 제어어를 획득한 스마트카드가 셋톱박스에게 이를 전송하는 채널이 보안되지 않았음을 이용해 도청 등의 공격으로 제어어를 쉽게 확보할 수 있음을 소개 하였다. 즉 공격자는 스마트카드로부터 셋톱박스로 연결되는 데이터 라인을 도청하여 평문으로 전송되는 제어어를 같은 종류의 다른 셋톱박스로 전송함으로써 불법적으로 방송 콘텐츠를 획득할 수 있다. 이와 같은 공격을 McCormac Hack 공격이라고 한다. (그림 2)는 사업자의 SMS 시스템에서 전송한 스크램블된 콘텐츠와 제어어 CW가 어떻게 셋톱박스에 전달되지를 추상화하여 보여준다. SMS는 단계 1에서 가입자 정보 및 CAS에서 필요한 키 구조를 SC에 등록하고 이를 발급한다. 단계 2의 SMS가 전송한 스크램블링된 콘텐츠를 수신한 STB는 단계 4에서 SC로부터 CW를 획득하여 콘텐츠를 디스크램블링한다. (그림 2)의 단계 4에서처럼 평문으로 전송되는 CW에 대한 도청을 막기 위해서는 SC가 CW를 암호화하여 전달하면 된다. 즉 McCormac Hack 문제는 SC와 STB간 공유 비밀키 확립을 통한 보안채널 형성으로 간단하게 해결될 수 있다. (그림 3)은 세션키 확립을 통해 SC가 STB에게 안전하게 CW를 전달하는 과정을 보여준다.

하지만 세션키 확립을 통한 CW의 안전한 전송만으로는 스마트카드 복제 공격으로부터 사업자를 효과적으로 보호할



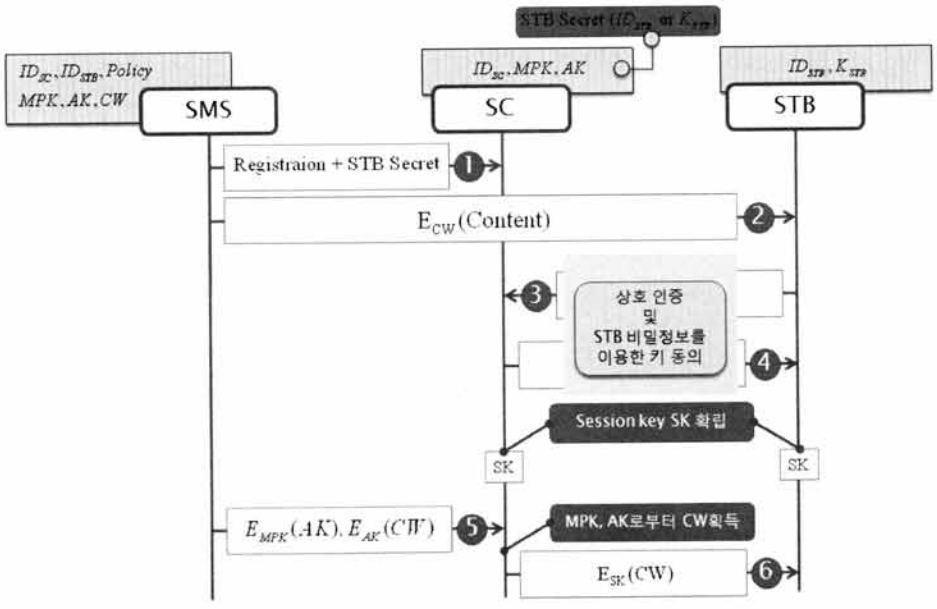
(그림 2) SC의 CW 획득 및 STB로의 전송



(그림 3) McCormac Hack 공격을 막기 위한 SC와 STB간 키 동의

수 없다. 공격자가 SC를 복제하여 다른 STB에서 사용하면 원본 SC와 마찬가지로 새로운 STB와 세션키를 확립할 수 있고, 또한 복제된 MPK, AK를 통해 CW를 획득한 후 STB에 CW를 전송함으로서 공격자의 불법적 콘텐츠 수신이 가능하게 된다. 이와 같은 스마트카드 복제 공격을 방지하기 위한 직관적이고 효과적인 방법은 단계 1의 등록과정에서 지정된 STB의 비밀정보를 함께 SC에 등록하여 등록된 STB만 해당 SC와 세션키를 확립할 수 있도록 두 개체를 바인딩하는 것이다. (그림 4)는 SC와 STB를 바인딩하여 공격자의 SC 복제로 인한 불법적 콘텐츠 수신을 막을 수 있음을 보여준다. 공격자가 SC를 복제하여 새로운 STB에 SC를 삽입하여 사용하려고 해도 SC에 등록된 STB의 비밀정보를 이용한 단계 3, 4의 상호인증 및 키 동의 과정을 정상적으로 수행할 수 없어 세션키 SK를 확립할 수 없다.

SC와 STB의 바인딩은 SC 복제를 방지하는 간단하면서도 효과적인 방법이긴 하지만, SC에 등록된 STB에서만 SC가 동작하는 이러한 기법은 IPTV 시스템의 확장성을 저해하는 제한적인 해결책이다. 즉 SC와 STB의 바인딩 기법은 다중 STB와 다수의 IPTV 지원 디바이스를 사용하는 환경에서 효율적인 보안을 제공하지 못한다. 한 번에 가입자가 사용할 수 있는 모든 디바이스를 등록해두고 SC를 발급하는 방법을 생각해 볼 수 있지만, 이 방법은 발급 후 새로운 사용자 장비를 추가하기 어려우며 초기에 임의로 등록해둔 가입자의 장비는 가입자의 의지에 따라 불법 시청자를 생성하는데 이용될 수도 있다. 이에 본 논문에서는 단일 가입자가 다수의 STB를 사용하는 IPTV 환경을 지원하면서도



(그림 4) SC복제를 위한 SC와 STB의 바인딩

McCormac hack 공격 및 SC 복제 공격에 강건한 SC/STB 인증 기법을 제안한다.

3. 관련 연구

지금까지 발표된 McCormac Hack 및 SC 복제에 관한 보안 연구는 [1-6]등이 있다. [1]에서 W. Kanjanarin과 T. Amornraksa는 이 두 공격이 사업자의 권익 보호에 매우 치명적인 위협이 될 수 있음을 소개하였고 두 위협에 대한 보안 필요성을 제시하였다. 이에 2004년 Jiang 등[2]은 Schnorr 디지털 서명과 일방향 함수를 사용하는 SC와 STB의 키동의 프로토콜을 제안하였다. Jiang 등은 그들의 프로토콜이 계산적으로 효율적이면서도 안전한 상호 인증을 제공하며 McCormac Hack 문제와 SC 복제에 안전하다고 주장하였지만 Yoon 등[3]은 그들의 프로토콜이 완전한 전방향 안전성을 보장하지 못하며 가장공격에 취약하다고 분석하였다. Yoon 등은 Jiang 등의 프로토콜을 개선하여 Diffe-Hellman 키동의 기법과 일방향 해쉬함수를 사용하는 새로운 키 동의 프로토콜을 제안하였다. 하지만 2009년 Lee 등[4]은 Yoon 등의 프로토콜이 여전히 가장 공격에 취약하고 상호 인증을 제공하지 못한다고 분석한 논문을 발표하였다.

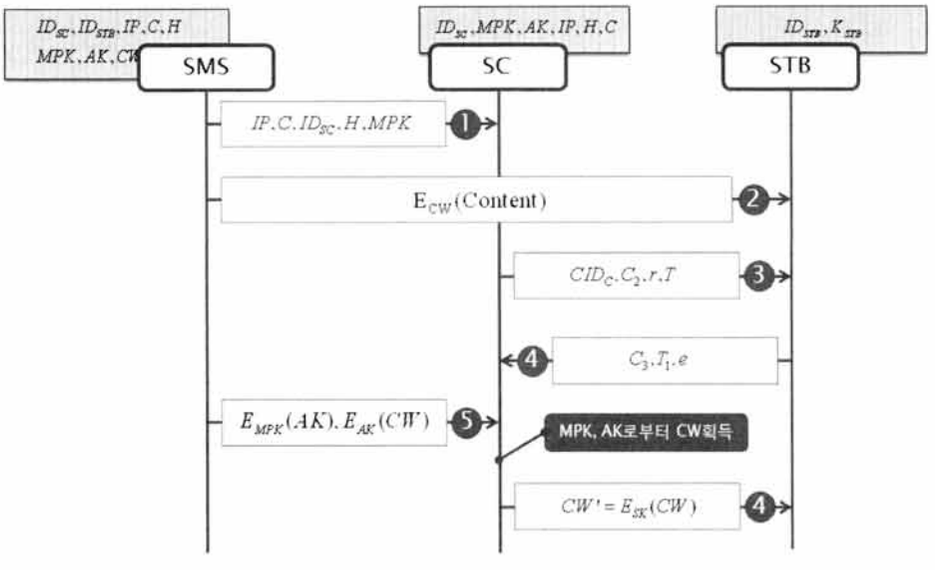
2007년 Hou 등[5]은 Jiang 등의 프로토콜이 연산량 측면에서 비효율적이다라고 분석하고 이를 개선한 프로토콜을 제안하였으나 2008년 Kim 등[6]은 Hou등의 프로토콜이 공격자의 위장 공격 및 메시지 변조 공격에 취약함을 지적하고 이를 개선한 새로운 프로토콜을 제안한다. Kim 등의 프로토콜은 지수연산을 사용하지 않으며 일방향 함수와 대칭키 암호 알고리즘을 사용한다.

따라서 본 논문에서는 Kim 등의 프로토콜과 Lee 등의 프로토콜을 관련 연구로 분석한다. 결론적으로 Kim 등의 프로토콜은 위장 공격 및 McCormac Hack 문제를 완전히 해결하지 못 하였고 Lee 등의 프로토콜은 지수 연산을 사용하는 등 연산량 측면에서 비효율적인 프로토콜이다.

3.1 Kim의 프로토콜

Kim의 프로토콜은 등록단계와 로그인 단계, 상호인증 및 키 동의 단계 그리고 마지막으로 CW 전송단계로 구분할 수 있다. (그림 5)는 Kim이 제안한 키 동의 프로토콜을 보여준다.

- 등록 단계: SMS는 $IP=H(ID_{SC},PW)$, ID_{SC}, 일방향 해쉬 함수 H, $C=IP\oplus H(ID_{SC},K_{STB})$, MPK를 SC에 저장하여 발급한다.
- 로그인 단계: SC는 STB에게 $CID_{SC}=ID_{SC}\oplus H(ID_{STB})$, $C_2=H(T\oplus C\oplus IP)$와 임의변수 r, 타임스탬프 T를 전송하여 로그인을 시도한다.
- 상호인증 및 키 동의 단계: STB는 $C_2'=H(T\oplus H(ID_{SC},K_{STB}))$를 계산 C_2'과 C_2가 같은 값인지 비교. 같인 값이면 세션키 $SK=H(r,e,ID_{SC},ID_{STB})$로 계산함. 이후 랜덤 값 e와 타임스탬프 T_1, 그리고 로그인 단계에서 수신한 정보를 이용해 $e'=H(ID_{SC})\oplus e\oplus T$, $C_3=H(C_2'\oplus ID_{SC}\oplus T_1\oplus e')$를 계산하고 ($C_3$, T_1, e)를 SC에게 전송한다. 이 값을 수신한 SC는 $C_3'=H(C_2\oplus ID_{SC}\oplus T_1\oplus e')$를 계산하고 C_3와 같은지 확인함. C_3와 C_3'이 같다면 SC 역시 세션키 $SK=H(r,e,ID_{SC},ID_{STB})$를 계산한다.
- CW 전송단계: SC는 CW를 세션키 SK를 이용하여 암호화된 제어어 $CW'=E_{SK}(CW)$와 같이 계산, STB에 전송하고 STB는 이를 $CW=D_{SK}(CW')$로 복호화하여 CW를 획득한다.



(그림 5) KiM의 프로토콜

하지만 Kim의 프로토콜은 그가 개선하였다고 주장한 Hou등의 프로토콜과 마찬가지로 위장공격이 가능하며 결과적으로 McCormac Hack 공격이 가능하다. Kim의 프로토콜은 키 동의를 위한 비밀 값으로 STB의 아이디 값인 ID_{STB} 값을 사용한다. 하지만 STB의 아이디는 STB만의 비밀 값이 아니며 경우에 따라서 공개된 값으로 간주될 수 있다. 공격자는 stolen-verifier 공격이나 서버 데이터 도청 등의 일반적인 공격 방법을 사용해 STB의 ID 값을 획득할 수 있으며 이를 이용 키 동의 과정을 성공적으로 수행 할 수 있다. 키 동의를 마친 공격자는 세션키 SK로 암호화 되어 전송되는 CW를 복호화하여 콘텐츠를 획득할 수 있다. 또한 Kim 등의 프로토콜은 SC 복제 방지를 위해 바인딩 기법을 사용하고 있다. SMS가 발급하는 C에는 STB의 비밀키 K_{STB}가 등록되어 있어 복제된 SC는 해당 STB외에는 사용할 수 없게 된다. 이는 2.2절에서 언급한 것처럼 SC의 복제를 방지하는 효과가 있지만 다수의 IPTV 디바이스를 이용하고자하는 가입자에게 유연성 및 확장성을 지원하지 못하는 제한적인 해결책이다.

3.2 Lee 등의 프로토콜

Lee 등의 프로토콜은 Kim의 프로토콜과 마찬가지로 등록단계와 로그인 단계, 상호인증 및 키 동의 단계 그리고 마지막으로 CW 전송단계로 구분할 수 있다.

- 등록 단계: SMS는 $R=H(ID_{SC}\oplus K_{STB})\oplus H(PW)$과 생성자 g, 일방향 해쉬함수 H, 그리고 MPK를 SC에 등록하고 가입자에게 발급한다.
- 로그인 단계: SC는 다음의 A,X,Y를 생성하고 STB에게 Y와 ID_{SC}를 전송한다.

$$A=g^a \bmod p\ (a\in Z_q^*),$$
$$X=R\oplus H(PW)=H(ID_{SC}\oplus K_{STB}),$$
$$Y=H(X,ID_{SC},ID_{STB})\cdot A$$

- 상호인증 및 키 동의 단계: SC의 로그인 메시지를 수신한 STB는 다음의 B, K, M을 계산하고 B와 M을 SC에게 전송한다.

$$B=g^b \bmod p\ (b\in Z_q^*),$$
$$K=\left(\frac{Y}{H(H(ID_{SC}\oplus K_{STB}),ID_{SC},ID_{STB})}\right)^b,$$
$$M=H(K,X,B,ID_{SC},ID_{STB})$$

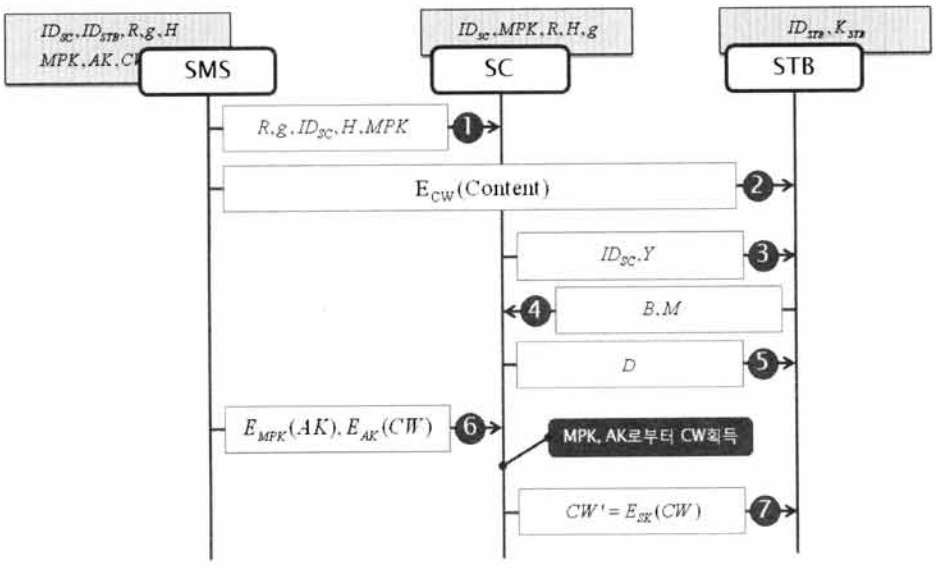
이를 수신한 SC는 $K=B^a=g^{ab} \bmod p$와 $M'=H(K,X,B,ID_{SC},ID_{STB})$를 계산하고 M과 M'이 같은지 확인함으로써 STB를 인증한다. 이후 SC는 $D=H(K,A,B,ID_{SC},ID_{STB})$를 계산해 STB에게 전송, STB는 $D'=H(K,A,B,ID_{SC},ID_{STB})$를 계산 두 값을 비교하고 D를 세션키로 사용한다.

- CW 전송단계: SC는 CW를 세션키 SK를 이용하여 암호화된 제어어 $CW'=E_{SK}(CW)$와 같이 계산, STB에 전송하고 STB는 이를 $CW=D_{SK}(CW')$로 복호화하여 CW를 획득한다.

Lee 등의 프로토콜은 K값을 통해 SC와 STB를 바인딩하고 있기 때문에 Kim 등의 프로토콜과 마찬가지로 다수의 STB를 지원하지 못한다. 또한 상호인증 및 키 동의를 위해 Diffie-Hellman 키 동의 기법을 사용하여 군에서의 나눗셈 연산을 수행하여야하는 비용 부담이 있다.

4. 제안하는 시스템

제안하는 시스템의 설계 목표는 스마트카드 복제 공격에 강건하면서 McCormac Hack 문제, 가장 공격 등으로부터



(그림 6) Lee 등의 프로토콜

안전하게 사업자의 콘텐츠를 보호함과 동시에 가입자 측면에서 사용할 수 있는 IPTV 디바이스의 유연성과 확장성을 보장하는 것이다. 이를 위해 다음과 같은 IPTV 환경의 특징을 고려한다.

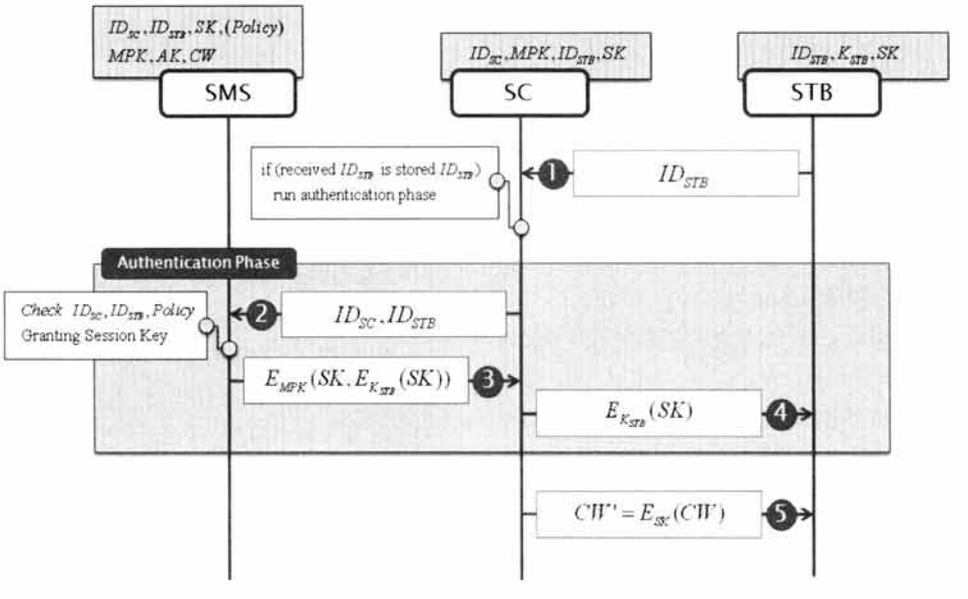
- IPTV의 양방향 채널: 기 제안된 관련 연구들은 DTV를 응용 모델로 하고 있거나 IPTV를 모델로 하면서도 SMS와 SC-STB 사이의 채널을 단방향 채널로 가정하고 있다. 이에 오프라인으로 발급하는 SC에 모든 비밀정보를 등록하고 SC와 STB 사이에서 키 동의를 진행하게 된다. 하지만 IPTV 환경에서 SMS와 SC 사이의 통신 구간은 양방향 채널이기 때문에 이를 이용하면 확장성 있는 프로토콜의 설계가 가능하다.
- 대칭키 기반의 암호 프리미티브 사용: 기 제안된 관련 연구들이 SC와 STB 사이에 확립되는 세션키의 완전한 전방향안전성(PFS, Perfect Forward Secrecy)를 보장하기 위해 공개키 암호 프리미티브를 사용하고 있으나, 확립한 세션키 SK로 암호화되는 제어어 CW의 생명주기를 고려할 때 PFS의 보장은 IPTV 시스템의 큰 보안 이슈가 아니다. 즉 수십 초마다 한 번씩 갱신되어 새롭게 전달되는 CW에 대한 PFS를 보장하는 것은 IPTV의 실시간 방송 응용에서는 중요한 부분이 아니다.
- 다중 STB 지원: 단말의 이동성이 강조되는 IPTV 2.0 환경에서 사용자는 지능화된 개인 휴대단말 및 홈 네트워크 내의 스마트 가전 기기 등을 이용하여 IPTV 서비스를 제공받을 수 있어야 한다. 이를 지원하는 간단한 프로토콜을 (그림 7)과 같이 설계해 볼 수 있다. (그림 7)에서 시스템은 양방향 채널을 이용하여 시도-응답(challenge-response)을 수행하고 이를 통해 다수의 STB를 인증한다. 하지만 이러한 방법은 새로운 STB에 대한 인증을 획득해 다중 STB를 지원할 수 있지만 이 때문에 SC 복제 공격에는 더욱 취약하게 된다.

(그림 7)의 기본 프로토콜은 다수의 STB를 지원할 수는 있지만 SC가 복제되면 복제된 SC로 인증 과정을 아무런 제약 없이 통과할 수 있기 때문에 공격자는 불법적으로 사업자의 콘텐츠를 획득할 수 있게 된다.

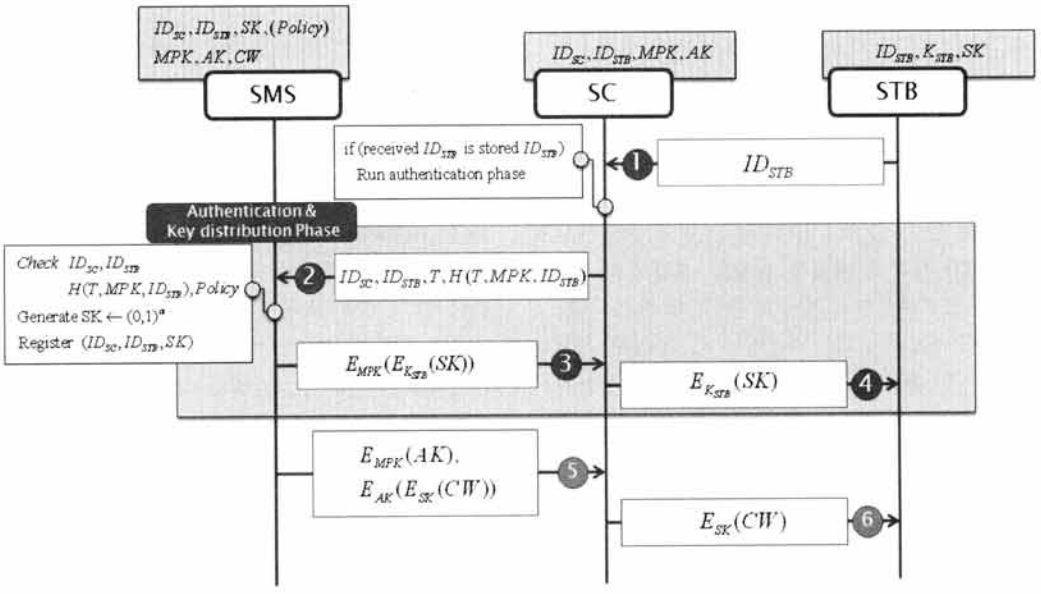
(그림 8)은 제안하는 시스템의 로그인 단계, 인증 및 키 분배 단계, CW 분배 단계를 보여 준다.

SC 등록 및 발급 단계에서 SMS는 SC의 아이디 ID_{SC}와 가입자의 마스터키 MPK를 SC에 등록하고 가입자에게 발급한다.

- 로그인 단계: 가입자의 SC가 STB에 삽입되면 STB는 자신의 아이디를 SC에게 전송한다. SC는 수신한 STB의 아이디 ID_{STB}와 자신이 저장하고 있는 값을 비교해 새로운 디바이스와 연결인지를 판단한다. 만약 수신한 ID_{STB}가 기존 아이디와 다르다면 새로운 STB와 연결되었다고 판단하고 인증 및 키 분배 단계를 수행한다.
- 인증 및 키 분배 단계: 이 단계에서 SC는 SMS에게 자신의 아이디 ID_{SC}와 새로운 STB의 아이디 ID_{STB}, 그리고 메시지 최신성을 보장하기 위한 타임스탬프 T, 정당한 SC의 요청인지를 확인하기 위한 인증값 $H(T, MPK, ID_{STB})$를 SMS에게 전송한다. SMS는 수신한 T와 ID_{SC}로부터 MPK를 사용자 데이터베이스에서 찾아내고 인증값 $H(T, MPK, ID_{STB})$를 생성하여 이를 수신한 인증값과 비교한다. 이상이 없다면 해당 SC의 유료화 정책에 따른 권한 등을 확인하고 랜덤한 값으로 세션키를 생성한 후 (ID_{SC}, ID_{STB}, SK) 쌍을 저장한다. 이 때 이미 등록된 ID_{SC}에 대한 STB와 SK정



(그림 7) 양방향 채널을 이용하는 기본 SMS-SC/STB 인증 프로토콜



(그림 8) 제안하는 SC-STB 인증 프로토콜

보가 있다면 이를 삭제하고 새로운 값으로 대체한다. 이후 STB에게 전달할 세션키를 SC의 마스터키 MPK를 이용하여 티켓 형식으로 발급한다.

- CW 전송단계: CW 전송단계에서 SMS는 SC-STB 쌍의 ID_{SC}, ID_{STB}를 확인하고 SK를 이용하여 CW를 $E_{SK}(CW)$로 암호화한다. 이 값은 SC의 인증키 AK를 이용해 $E_{AK}(E_{SK}(CW))$와 같이 STB에 전달된다.

5. 분 석

이 장에서는 제안하는 프로토콜이 다중 STB를 지원하면서도 SC 복제 공격에 안전하고 McCormac 공격 및 가장 공격과 같은 알려진 IPTV 보안 위협에 안전함을 분석한다. 분석을 위해 아래와 같은 표기법과 공격자 가정을 사용한다.

- $\{U_1, U_2, \ldots, U_n\}$: n명의 IPTV 방송 가입자 집합
- $\{SC_1, SC_2, \ldots, SC_m\}$: n명의 IPTV 가입자가 사용하는 m개의 스마트카드 $(m > n)$
- $\{ID_{SC_1}, ID_{SC_2}, \ldots, ID_{SC_m}\}$: 각 스마트카드의 아이디 값
- $\{STB_1, STB_2, \ldots, STB_p\}$: 방송 가입자가 사용할 수 있는 p개의 셋톱박스 집합$(p > m)$
- $\{ID_{STB_1}, ID_{STB_2}, \ldots, ID_{STB_p}\}$: 각 셋톱박스의 아이디 값

(시스템 가정 1) 공격자는 SC를 복제할 수 있으며 SMS와 SC 사이의 구간 및 SC와 STB 사이의 구간을 도청하여 전송되는 메시지를 획득 할 수 있다.

(시스템 가정 2) 제안하는 시스템에서 사용하는 대칭키 암호 알고리즘 E는 키를 모르는 공격자에 대해 계산적 안전성(computationally secure)을 보장한다.

[정리 1] 제안하는 SC-STB 인증 프로토콜은 McCormac Hack 공격에 안전하다.

[증명] McCormac Hack 공격은 공격자가 SC와 STB 사이의 비 보안 채널에서 평문으로 전송되는 CW를 공격자가 도청하거나 위장 공격을 통해 우회하여 CW를 획득하는 경우 성공했다고 말한다. 제안하는 프로토콜에서 콘텐츠 획득을 위한 제어어 CW는 SMS와 STB 사이에 확립된 세션키 SK를 이용하여 전달되고, 키 확립 과정에서 SK는 STB의 비밀키 K_{STB}를 이용하여 암호화되어 전송된다. 따라서 공격자가 전수 공격(brute force)을 통해 K_{STB}와 SK를 계산해 낼 확률을 무시한다면 가정 2에 의해 공격자는 CW를 획득할 수 없다. □

[정리 2] 제안하는 SC-STB 인증 프로토콜은 스마트카드 복제 공격에 안전하다.

[증명] 공격자의 SC 복제 공격의 목적은 SC를 복제하여 방송 사업자의 IPTV 콘텐츠를 불법적으로 수신하는 것이다. 이를 위해 공격자는 콘텐츠의 스크램블링에 사용되는 CW를 획득할 수 있어야한다.

가입자 U_1이 SMS로부터 SC_1을 발급받아 STB_1을 이용해 IPTV 콘텐츠를 수신하는 환경을 가정해 보자. 이 때 SMS에 등록된 아이디-세션키 쌍을 $(ID_{SC_1}, ID_{STB_1}, SK_1)$으로 나타낸다. SMS는 가입자 U_1에게 CW를 SK_1을 이용, 암호화하여 전송한다. 즉 공격자가 CW를 획득하기 위해서는 SK_1을 알 수 있어야한다. 하지만 SC_1에는 SK_1과 관련된 아무런 정보가 포함되어 있지 않기 때문에 공격자의 SC_1의

〈표 2〉 관련 연구와의 비교

구분	SC 복제 방지	McCormac Hack 방지	다중 STB 지원	완전한 전방향 안전성	암호 프리미티브	비고
Jiang[2]	O	X	X	X	지수연산	가장공격으로 CW 획득
Yoon[3]	O	X	X	O	지수연산	가장공격으로 CW 획득
Lee[4]	O	O	X	O	지수연산	
Hou[5]	O	X	X	X	지수연산	가장공격으로 CW 획득
Kim[6]	O	X	X	X	대칭키 기반 연산	가장공격으로 CW 획득
제안하는 프로토콜	O	O	O	X	대칭키 기반 연산	

복제는 공격자에게 아무런 이득을 주지 않는다. 다중 STB를 지원하는 환경에서 가입자 U_1과 U_2가 공모해 U_1이 사용하고 있는 SC_1을 복제하는 공격을 생각해보자. U_1과 U_2는 U_1의 SC_1을 복제하여 과금 없이 IPTV 콘텐츠를 획득하고자 한다. 하지만 U_2가 복제된 SC_1을 새로운 STB_2에 삽입하고 (그림 8)의 인증 및 키 분배 과정을 거치게 되면 SMS에 등록된 U_1의 콘텐츠 수신 정보가 U_2가 등록하는 새로운 정보로 갱신되기 때문에 U_1은 더 이상 콘텐츠를 획득할 수 없다. 즉 SMS에 등록된 콘텐츠 수신 정보 $(ID_{SC_1}, ID_{STB_1}, SK_1)$는 $(ID_{SC_1}, ID_{STB_2}, SK_2)$로 갱신되어 이전에 생성된 SK_1만 가지고 있는 U_1의 STB는 SK_2로 암호화되어 전달되는 $E_{SK_2}(CW)$를 가정 2에 의해 복호화 할 수 없고 따라서 CW를 획득할 수 없다. □

<표 2>는 관련 연구와 제안하는 시스템의 알려진 보안 위협에 대한 안전성을 비교하여 보여준다. 기존 기법들 모두 SC에 사용가능한 단일 STB를 등록해 둠으로써 SC의 불법 복제를 방지하였지만 이들은 다중 STB 환경을 지원하지 못한다. 또한 기 제안된 프로토콜들이 CW를 상호인증을 통해 생성한 세션키 SK를 이용하여 암호화 전송하는 방법으로 단순 도청을 막을 수 있지만 중간자 공격과 같은 가장 공격으로 SK를 획득할 수 있고 이를 통해 CW를 확보할 수 있기 때문에 McCormac Hack 공격이 가능하다고 분석하였다. CW에 대한 완전한 전방향 안전성의 경우 Yoon 등과 Lee 등의 프로토콜을 제외하고는 모두 만족하지 못한다. 하지만 4장에서 언급한 것처럼 IPTV 시스템에서의 CW의 전방향 안전성은 중요한 보안 이슈가 아니기 때문에 제안하는 프로토콜은 지수연산이 필요한 공개기 프리미티브를 사용하는 대신 대칭키 프리미티브를 사용하여 프로토콜의 효율성을 높였다.

6. 결 론

본 논문에서는 IPTV 환경에서 사업자 권익 보호를 위한 CAS 시스템에서 발생할 수 있는 스마트카드 복제 문제와 McCormac Hack 문제를 해결한 안전한 스마트카드 인증 기법을 제안하였다. 기 제안된 기법들이 스마트카드와 셋톱박스를 바인딩하여 단일 셋톱박스 환경만 지원했던 반면 제안한 프로토콜은 다중 셋톱박스를 지원하여 가입자가 다수의 디바이스를 활용하여 IPTV 콘텐츠를 획득할 수 있도록 유연성과 확장성을 제공한다. 가입자는 SMS와 스마트카드 구간의 양방향 채널을 이용하여 다수의 셋톱박스를 등록하여 이용할 수 있으며 사업자는 지정된 셋톱박스에 티켓형식으로 발급되는 세션키를 이용하여 제어어를 암호화하여 전달함으로서 스마트카드 복제 공격에 안전하게 IPTV 콘텐츠를 전송할 수 있다. 제안하는 기법은 완전한 전방향 안전성을 제공하지 못하는 대신 대칭키 암호 알고리즘을 사용하여 효율적으로 동작한다.

참 고 문 헌

[1] W. Kanjanarin and T. Amornraksa, "Scrambling and Key Distribution Scheme for Digital Television," *Proc. of the 9th IEEE Int. Conf. on Net. (ICON)*, pp.140-145, 2001.

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

[3] 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 Informatics (ISI)*, Vol.3917 of LNCS, pp.139-150, 2009.

[4] 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 of LNCS, pp.797-803, 2009.

[5] 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.

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

[7] 신기은, 최형기, "해쉬 트리 기반의 효율적인 IPTV 소스 인증 프로토콜", 정보처리학회논문지C, 제16-C권, 제1호, pp.21-26, 2009.

[8] 김대엽, 주학수, "CAS기반 IPTV 보안 시스템", 정보처리학회 논문지C, 제15-C권, 제4호, pp.221-226, 2008.

임 지 환

e-mail : jihwan.lim@gmail.com
2005년 한양대학교 전자컴퓨터공학부(학사)
2007년 한양대학교 컴퓨터공학과(석사)
2007년~현 재 한양대학교 컴퓨터공학과 박사과정
관심분야 : 네트워크 보안, 암호프로토콜

오 희 국

e-mail : hkoh@hanyang.ac.kr
1983년 한양대학교 전자공학과(학사)
1989년 아이오와주립대학 전자계산학과(석사)
1992년 아이오와주립대학 전자계산학과(박사)
1993년~1994년 한국전자통신연구원 선임 연구원
1995년~현 재 한양대학교 컴퓨터공학과 교수
관심분야 : 암호프로토콜, 네트워크 보안

김 상 진

e-mail : sangjin@kut.ac.kr
1995년 2월 한양대학교 전자계산학과(학사)
1997년 2월 한양대학교 전자계산학과(석사)
2002년 8월 한양대학교 전자계산학과(박사)
2003년 3월~현 재 한국기술교육대학교 인터넷미디어공학부 부교수
관심분야 : 암호기술 응용