情報保護學會論文誌
第20卷 第2號, 2010. 4

Clone 공격에 강한 IPTV-RFID 융합 기술*

정 윤 수,[1†] 김 용 태,[2‡] 박 길 철,[2] 이 상 호[1]
[1]충북대학교, [2]한남대학교

A Convergence Technology of IPTV-RFID against Clone Attack*

Yoon-Su Jeong,[1†] Yong-Tae Kim,[2‡] Gil-Cheol Park,[2] Sang-Ho Lee[1]
[1]Chungbuk National University, [2]Hannam University

요 약

최근에 TV와 인터넷 등의 통신 기술의 발달로 인하여 인터넷망에 멀티미디어 콘텐츠를 융합한 IPTV 서비스가 증가하고 있다. 그러나 사용자가 임의의 장소에서 서비스를 제공받을 때 기존 IPTV 서비스는 이동 사용자의 가입 유·무 및 인증 과정이 복잡하여 불법적인 사용자의 증가와 서비스 지연 등의 통신 장애가 발생하는 문제점이 있다. 이 논문에서는 IPTV 서비스를 불법적으로 도용하는 사용자를 효율적으로 추출하여 무선 구간에서 많이 발생하는 복제 공격을 예방하기 위한 통신 보안 메커니즘을 제안한다. 제안 메커니즘은 사용자들이 사용하는 RFID 태그에 스마트 카드를 융합하여 플러그 앤 플레이 기능을 수행할 수 있도록 RFID-USB 장비에 보안 에이전트를 두어 키 초기화 과정, 상호 인증과정, 키 분배과정 등을 수행한다. 또한, 제안 메커니즘은 사용자가 RFID-USB 범위안에 접근할 때마다 RFID-USB에서 생성한 랜덤수와 이동 사용자의 ID를 해쉬 함수에 적용하여 해쉬된 토근값을 업데이트함으로써 무선 구간에서 자주 발생하는 재사용 공격과 man-in-the-middle 공격을 예방하고 있다.

ABSTRACT

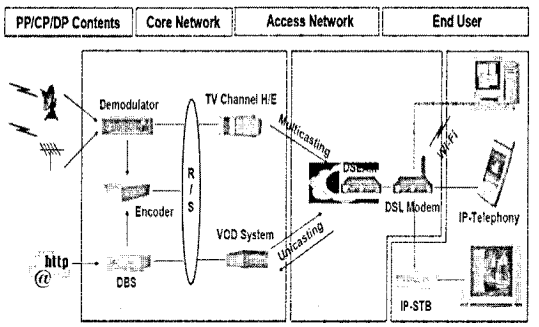
Now a days, the development of TV and internet like communicational technique makes IPTV service which combines internet with multimedia contents increase. But when a user gets service in specific place, the certification process and user's ID check in IPTV service is complicate so that there occurs communicational difficulty like increasing illegal users and service delay etc. This paper proposes communication security mechanism to prevent Clone attack which happens in wireless section by efficiently extracting illegal user. The proposed mechanism performs key distribution procedure, inter certification procedure, and key initiation procedure by putting security agent in RFID-USB for RFID tags users use to perform plug-and-plug function. Also, the proposed mechanism updates the hased token value by its ID and the random number which RFID-USB creates whenever a user accesses in the area of RFID-USB so that it protects reply attack and man-in-the-middle attack which happen often in the area of wireless section.

Keywords: IPTV USB, Clone attack, RFID

I. 서 론

최근 TV 방송이 디지털화 되면서 새롭고 다양한 디지털 TV 산업이 통신 분야와 접목되고 있다. 최근 방송 프로그램은 멀티캐스팅 기술을 이용하여 이용자에게 인터넷망을 통하여 멀티미디어 콘텐츠를 제공하는 통신방송 융합 서비스 IPTV가 증가하고 있다[1]. IPTV는 QoS가 보장된 매니지드 IP 네트워크를 통해서 스트림화된 비쥬얼 콘텐츠를 가입자의 TV 또는 유사장비에 안정적으로 제공하는 방송서비스이다. IPTV 시스템의 기본 구성은 플랫폼, IP 네트워크, 단말장치이며 케이블 TV 가입자망을 통해 방송과 초

접수일(2009년 8월 14일), 수정일(2009년 10월 23일), 게재확정일(2009년 11월 9일)
* 본 연구는 지식경제부 지역혁신센터사업인 민군겸용보안공학연구센터 지원으로 수행되었음.
† 주저자, bukmunro@gmail.com
‡ 교신저자, ky7762@hannam.ac.kr



〔그림 1〕. IPTV 시스템의 기본 구성

고속 인터넷, 전화를 함께 제공하는 TPS(Triple Play Servic)를 제공할 수 있는 장비로 그림 1과 같이 IPTV 시스템이 구성된다.

IPTV는 여러 유사 장비에 안정적으로 서비스를 제공하기 위해서 서비스를 제공받는 사용자가 합법적인 사용자인지를 판별할 수 있도록 IPTV 셋톱박스(STB, Set Top Box)에서 확인하고 있지만 이동 사용자인 경우 사용자의 이동성으로 인하여 발생되는 사용자 정보 유출의 보안 문제를 보장받지 못하고 있다〔4〕. 최근 연구에서는 이동 사용자의 가입 유·무를 효과적으로 지원할 수 있도록 스마트카드에 RFID 기술을 접목하는 연구가 활발하게 진행중이다〔2,3,5〕. 대부분의 IPTV 브로드캐스팅 방법은 온라인상에서 헤드 엔드(Head-End)와 가입자 사이의 인증이 단방향으로 이루어진다. 서비스 제공자는 이러한 문제를 해결하기 위해서 셋톱박스와 스마트카드 사이에 양방향 인증을 수행한다.

McCormac Hack과 스마트카드 복제 공격(clone attack)은 스마트카드와 셋톱박스 사이에서 인증을 처리할 때 발생한다. 스마트카드의 복제 공격은 스마트카드의 하드웨어 특성을 파악한 후 동일한 하드웨어를 사용하여 물리적으로 동일한 스마트카드를 복제하거나 또는 스마트카드의 메모리 정보를 모두 해킹한 후에 동일한 정보를 가진 복제 스마트카드를 만들어서 셋톱박스 시스템을 교란시킨다. 반면, McCormac Hack 문제는 스마트카드와 셋톱박스의 데이터 라인에서 발생되고 데이터는 동일한 스마트카드를 사용하여 다른 셋톱박스 방향으로 보낼 수 있다〔6〕.

IPTV 관리자는 이동 사용자의 IPTV 가입 유·무를 한 장소에서 인식하지 않고 사용자가 원하는 위치에서 IPTV 서비스를 제공할 수 있어야 한다. 그러나 RFID 태그를 가진 이동 사용자가 특정 장소에서 서비스를 제공받을 때 이동 사용자의 가입 유·무 및 인증 과정이 복잡하면 통신 오버헤드 및 서비스 지연과 같은 통신 장애가 발생할 수 있고 불법적인 RFID 사용자가 서비스를 지속적으로 이용하려고 하는 경우가 발생할 수 있다.

이 논문에서는 IPTV 서비스를 제공받는 이동 사용자가 RFID 태그를 사용하여 무선 구간에서 많이 발생하는 복제 공격을 예방하기 위한 통신 보안 메커니즘을 제안한다. 제안 메커니즘에서는 RFID 태그들이 플러그 앤 플레이(Plug-and-Play) 기능을 수행할 수 있도록 RFID 태그와 RFID-USB에 보안 에이전트를 두어 키 초기화 과정, 상호 인증과정, 키 분배과정 등이 수행된다. 제안 메커니즘에서는 RFID 태그와 RFID-USB의 에이전트가 논리적으로 동작하면서 다수의 RFID 태그가 RFID-USB와 연동할 수 있도록 상호운영 역할을 수행한다.

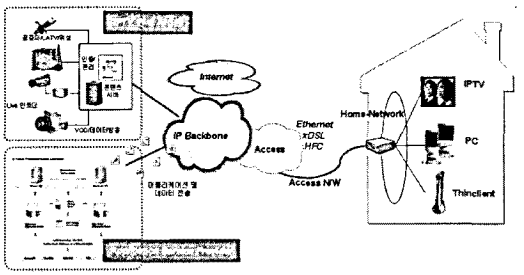
이 논문의 구성은 다음과 같다. 2장에서는 IPTV 개념, IPTV 콘텐츠 보안 및 IPTV 보안기술에 대해서 분석한다. 3장에서는 RFID-USB 기술을 이용하여 가입자의 Clone 문제를 해결하기 위한 보안 프로토콜을 제시하고, 4장에서는 제안 프로토콜의 보안평가를 분석한다. 마지막으로 5장에서는 이 논문의 결과를 요약하고 향후 연구에 대한 방향을 제시한다.

II. 관련연구

2.1 CAS

CAS(Conditional Access System)는 방송에 가입자 개념을 도입하여 정당한 시청권한을 가진 가입자만이 특정 프로그램을 수신할 수 있도록 지원해주는 서비스 방식이다. CAS의 동작은 크게 송신측과 수신측으로 구분되며 송신측에서는 암호화된 프로그램 신호와 수신자 인식자 또는 특정 그룹에게 부여된 수신자격(entitlement)을 전송하고 수신측에서는 수신인가를 받은 가입자만이 수신기에 붙어있는 스마트카드를 이용해 암호를 해독해 프로그램을 수신할 수 있도록 한다〔7〕.

그림 2에서 CAS의 주요 구성 요소는 플랫폼(HeadEnd), IP 네트워크, 단말장비 등과 함께 트리플 플레인(Triple Play)의 서비스를 제공할 수 있는 장비로 구성되어 있다. 그림 1의 IPTV 서비스 구성도는 주문형 콘텐츠(VOD 등), 인터넷 검색, T-Commerce 서비스 및 이용자 요청에 따라 실시간으로 방송 프로그램을 전송하는 서비스 등에 사용된다.



〔그림 2〕 IPTV 서비스 구성도

2.2 RFID-USB 기술

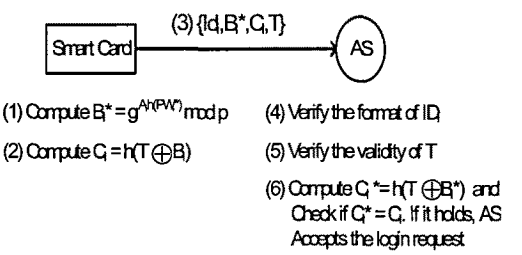
RFID는 1980년대 이후로 꾸준하게 발전해온 자동인식 기술의 한 종류로써 RFID 시스템은 수집된 데이터의 처리를 위해 기본적으로 태그, 리더 그리고 응용 시스템으로 구성된다. 리더는 객체에 붙어있는 태그들로부터 데이터를 획득하고 떫떫 미들웨어를 통해 응용 시스템에 데이터를 전달한다. 리더는 태그로부터 전달되는 신호들의 상태를 제어하는 역할을 수행하며 만약 신호들에 에러가 있다면 발생된 에러를 체크하고 수정한다. 현재까지 개발된 프로토콜 중 일부는 태그들로부터 수신된 신호들을 제어하기 위해 리더 중심의 시스템을 설계하였다. Yuli[8]는 USB 키를 이용하여 RFID의 인증 정보를 안전하게 서버에 등록하기 위해 USB 디바이스로 서버에 접속하여 인증을 수행하는 RFID-USB 기술을 제안하였다. Yuli의 RFID-USB 기술은 PKI 시스템을 기반으로 서버에 등록할 RFID 사용자의 인증 요소인 USB 키를 생성하는 역할을 수행하며 USB 키 시스템의 비대칭 암호는 시스템의 보안을 기존 기법보다 향상시키고 있다. RFID-USB에서 디지털 서명, 개인 키 그리고 다른 비밀 데이터를 안전하게 저장되기 위해서 USB 키 내의 메모리(key-storage)에 저장한다. USB 키는 RFID-USB를 통해 안전하게 PKI 시스템을 수행할 수 있는 부정 조작을 못하게 만든 하드웨어로써 USB 키 내의 메모리는 사용자에 의해 직접적으로 읽기/쓰기할 수 없기 때문에 정보 보안이 보장된다. USB 키 내에 존재하는 운영 장치는 데이터 요약 정리, 암/복호화 그리고 디지털 서명 알고리즘 등을 수행한다. USB 키는 그 자체에서 암호화되기 때문에 개인 키는 개인 컴퓨터의 메모리나 하드디스크에 나타나지 않는다.

2.3 기존 보안연구

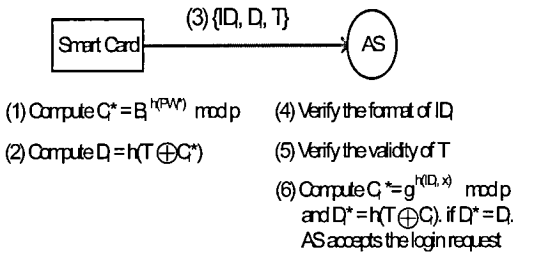
Wong 과 A. H. Cahn[11]은 재사용 공격과 man-in-middle 공격을 예방하기 위해 낮은 전력의 무선 통신을 위한 상호 인증과 키 교환 기법을 제안하였지만 K. shim[10]이 알려지지 않는 키 공유 공격에 안전하지 않다는 것을 증명하였다. C. P. Schnorr[13]은 스마트카드를 위한 효율적이고 안전한 효율적인 디지털 시그너처 프로토콜을 제안했다. 특히, 2004년에는 Jiang et al.[14]이 스마트카드와 셋톱박스를 위한 상호 인증을 실현하기 위해서 C. P. Schnorr의 프로토콜을 적용한 기법을 제안하였다. 2004년 IPTV 기술이 소개된 이후 Jiang et. al.은 Schnorr의 디지털 시그너처 프로토콜과 one-way 해쉬 함수를 기반으로 셋톱박스와 스마트카드 사이의 상호인증 프로토콜을 최초로 제안했다[12]. Jiang. et. al의 프로토콜은 보안, 동적 세션키, 상호 인증 등에 장점을 가지면서 패스워드 교환을 수행하여 스마트카드 복제와 McCormac Hack 문제를 예방하였지만 지수 연산에 의한 계산량이 많이 발생되는 단점이 있다. Hou et al.[9]은 스마트카드와 셋톱박스 사이의 안전한 통신을 위한 보안 기법을 제안했다. 그러나 Hou et. al.이 제안한 기법은 상호 인증을 보장하기 위해 RSA 암호화/ 복호화 알고리즘을 사용하면서 스마트카드에 시간 소비가 매우 큰 지수 연산이 필요한 문제점이 나타났다.

그림 3에서 Wu[15]는 사용자 자신의 메모리에 패스워드를 저장할 때 서버가 정한 일정 길이의 패스워드를 사용해야하는 SUN[20]의 문제점을 해결하고 있지만 공격자는 사용자가 선택한 속성들에 대해서 정당한 인증 메시지를 생성하여 서버의 비밀키 값을 알아내는 사용자 가장 공격과 인증메시지에 대한 정당한 답신 메시지를 생성하는 서버 가장 공격에 취약한 문제점이 있다.

그림 4에서 Wu[16]은 Wu[15]의 가장 공격에 취약한 문제점을 해결하기 위해서 패스워드 테이블을 유지하지 않고 사용자 원격 인증을 수행하는 기법을 제안하였다. 그러나 Wu[15]보다 2번의 해쉬 함수를 추



〔그림 3〕 〔15〕 기법의 로그인과 인증 구문



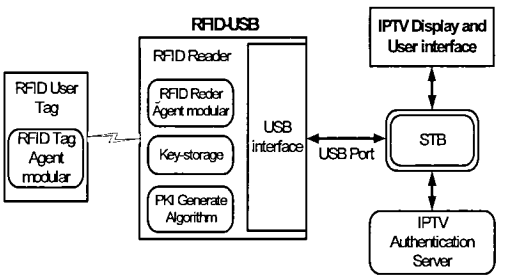
〔그림 4〕 〔16〕 기법의 로그인과 인증 구문

가 사용하여 인증 계산량이 높은 단점이 있다.

〔18〕은 스마트카드를 이용하여 사용자와 서버간의 상호 인증을 만족하며 사용자 프라이버시를 위해 제 3자뿐만 아니라 원격 서버에서도 안전한 익명성을 제공하는 사용자 인증 프로토콜을 제안하였다. 그러나 〔18〕은 제 3자뿐만 아니라 원격 서버에게도 안전한 익명성을 제공하기 위해서 로그인 단계와 인증 단계에서 해쉬 함수를 추가하기 때문에 계산 비용이 높다. 〔17〕은 사용자를 인증하는 기술중에서 스마트카드를 이용한 속성 기반 인증 기법을 제안하였다. 이 기법은 스마트카드를 이용하여 계산량 측면에서 효율성을 높였고, 사용자는 한 번의 등록으로 속성에 따라 다양한 서비스를 안전하게 제공받을 수 있는 특징이 있다. 그러나 원격 서버에서 익명성을 제공받기 위해서는 추가 등록 및 인증 비용이 발생한다. 〔19〕는 제3자뿐만 아니라 원격 서버에 대해서도 사용자의 신원에 대한 익명성을 보장하고 악의적인 사용자의 행동에 따른 문제 발생 시에 이를 추적 가능하다는 장점이 있지만 로그인 과정과 인증 과정에서 많은 해쉬함수를 사용하여 높은 연산비용이 발생하는 단점이 있다.

III. RFID-USB 메커니즘을 이용한 프로토콜 구현

이 절에서는 RFID-USB 기술을 이용하여 이동 IPTV 환경에서 발생하기 쉬운 복제 공격을 예방할 수 있는 통신 보안 메커니즘을 제안한다. 제안 메커니즘은 RFID 태그와 RFID-USB에 논리적으로 동작하는 에이전트를 두어 디바이스 드라이버의 인스톨 파일을 사전에 저장하여 도청 행위 공격을 사전에 예방한다. 특히, 제안 메커니즘은 RFID 태그를 USB 기술과 연동하여 사용하기 때문에 복제 공격과 같은 보안 위협을 예방하기 위해서 RFID-USB가 플러그 앤 플레이 기능을 수행할 때 RFID 태그와 RFID-USB



〔그림 5〕 제안된 인증 프로토콜을 위한 IPTV 시스템의 인터페이스

에서 생성한 랜덤 수를 이용하여 보안 토큰을 생성한다. RFID-USB 기술은 2.45GHz 대역으로 15~20m내의 자동 무선 태그를 인식 할 수 있는 개인 위치 측정, 물류관리, 창고 관리, 폐회로 자산 추적, 고가치 자산 추적 등의 분야에 적용된다.

3.1 개요

IPTV 환경의 셋톱박스와 RFID 사용자 사이의 무선구간은 보안 공격(복제 공격과 도청 행위 공격 등)에 취약하며 이러한 보안 취약점을 보장받기 위해서는 셋톱박스에 설정된 값이 변경되지 않아야 하고 소프트웨어 설치없이 플러그 앤 플레이 기능이 동작되는 RFID 태그가 요구된다. 그림 5는 제안 메커니즘의 전체 인터페이스를 보여주고 있으며 그림 5에서 RFID 리더는 셋톱박스와 직접적으로 USB 포트를 사용하여 연결되며 셋톱박스와 RFID리더 사이에 USB 포트를 이용할 수 없다면 시리얼 포트를 사용한다.

RFID-USB는 인증, 서버의 키 저장, PIN 인증을 위한 개인키 검색 그리고 공개키 검색 등이 실시간 관점에서 동시에 실행한다. 기존 USB 키와 비교해서 그림 5의 인터페이스는 다중 사용자들이 RFID를 통해 무접촉으로 인증이 수행될 수 있으며 RFID 태그들이 RFID-USB의 인식 필드를 벗어날 경우 인증은 수행되지 않는 특징이 있다. 특히 RFID 태그가 태그 인식 필드를 벗어날 경우 셋톱박스를 사용하는 모든 사용자의 프로그램들은 일정 시간이 경과한 후에 인터럽트가 발생한다.

제안 메커니즘은 다수의 RFID 사용자들을 위해 RFID-USB내에 PKI 시스템을 사용하는 RFID 사용자의 개인키 K_{pri}가 저장되는데 이 때 저장된 개인키 K_{pri}는 테이블 검색 방법을 통해 검색되며 RFID

사용자들의 테이블 정보를 노출하지 않아도 된다. RFID 사용자의 개인키와 서버의 랜덤키에 의해서 동작되는 해쉬 과정은 RFID-USB 운영 장치를 통해 수행되며 USB 인터페이스를 통해 키와 다른 데이터 정보들을 셋톱박스에 사전에 저장된 정보들과 서로 교환하는데 이 부분이 제안 케머니즘이 기존 USB나 RFID 리더와 다른점이다. RFID-USB는 RFID 리더에게 전원을 공급하여 RFID 태그가 셋톱박스에 무접촉으로 인식되어 RFID 태그와 셋톱박스 사이의 인터페이스 역할을 수행한다. RFID-USB는 RFID 태그와 셋톱박스의 통신 브리지 역할로써 PIN 디코드 정보, USB에 의해 생성된 랜덤코드, 해쉬 결과 등을 전달한다. 셋톱박스는 다중 사용자의 공개키를 저장하고 있어 마이크로 제어 장치(MCU, Micro Control Unit)로부터 개인 식별 번호(PIN, Personal Identification Number)을 체크하고 해쉬 결과로부터 랜덤 코드를 검색한 후 검색된 코드를 셋톱박스가 보유하고 있는 정보와 비교하여 두 결과가 일치한다면 인증이 성공적으로 이루어지고 그렇지 않으면 에러 정보가 반환된다.

3.2 용어정의

〔표 1〕 용어 정의

용 어	정 의
STB	Set-Top Box
SID_i	태그 i의 보안 ID
S_{serial}	셋톱박스의 유일한 시리얼 번호
$Token_{AB}$	A와 B사이의 토근 정보
∞o_x`	x의 정보
α, β, γ, δ	메시지 정보
$SIDIdx$	보안 인식자 인덱스
K_m	암호 키
K_{pri}	개인 키
K_{pub}	공개 키
K_{share}	리더와 태그 사이에 사전에 공유된 공유키
WID	RFID-USB가 생성한 RFID 태그 사용자의 임시 ID
TID	RFID 태그가 임의로 생성한 ID
TSN	태그 세션 넘버
RSI	RFID 태그의 보안 정보
$h()$	해쉬 알고리즘
R	랜덤수
||	XOR 연산

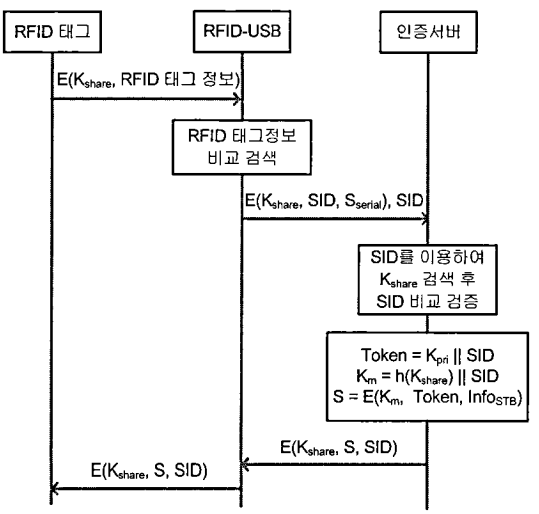
제안 메커니즘에서 사용하는 주요 용어를 정의하면 표 1와 같다. 표 1의 SID_i는 태그의 보안 인식자로써 IPTV 서비스를 가입한 모든 사용자에게 태그와 함께 제공되며 인증을 위해 사용되는 키는 크게 암호키 K_m, 공개키 K_{pub}, 개인키 K_{pri}, 공유키 K_{share} 등이 있다. 정보의 최신성을 위해 제안 메커니즘에서는 랜덤수 R을 사용하며 일방향성의 해쉬 함수 $h()$로 연접되어 공격자의 메시지 정보 노출 시도를 예방한다.

Clone 공격을 예방하기 위한 통신 보안 프로토콜

이 절에서는 셋톱박스와 다수의 RFID 태그 사이의 무선 구간에서 많이 발생하는 복제 공격을 예방하기 위해서 RFID 태그들이 플러그 앤 플레이 기능을 수행할 수 있도록 RFID 태그와 RFID-USB에 보안 에이전트를 두어 키 초기화 과정, 보안 ID 검증과정, 상호 인증과정, 키 분배과정 등의 과정을 통해 RFID 태그 사용자들이 안전한 통신을 보장받기 위한 통신 보안 프로토콜을 제안한다. RFID 태그와 RFID-USB의 에이전트는 논리적으로 동작되며, RFID-USB의 에이전트는 다수의 RFID 태그가 셋톱박스와 연동할 수 있도록 상호운영 역할을 수행하고 RFID 태그의 에이전트는 RFID 태그내에 자리잡고 있으면서 사용자의 민감한 데이터를 메모리에 유지할 수 있도록 하여 액세스되는 데이터의 암호 동작을 수행한다.

3.3.1 초기화 과정

키 초기화 과정은 사용자가 셋톱박스를 통해 지불



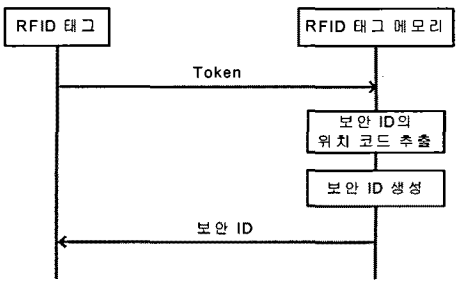
〔그림 6〕 초기화 과정

된 데이터를 수신하는데 필요한 기본 정보를 생성하는 과정으로써 인증서버는 사용자가 사전에 등록한 RFID-USB내의 개인키 K_{pri}와 RFID 태그의 보안 인식자 *SID*를 이용하여 보안 토큰 *Token*($=K_{pri}$ || *SID*)을 생성한다. 인증서버는 생성된 토큰 *Token*과 셋톱박스의 유일한 시리얼 번호 S_{serial}의 정보를 암호화하기 위해서 사전에 공유된 공유키 K_{share}을 해쉬체인에 적용한 후 보안 인식자 *SID*와 결합하여 암호키 K_m을 초기화한다.

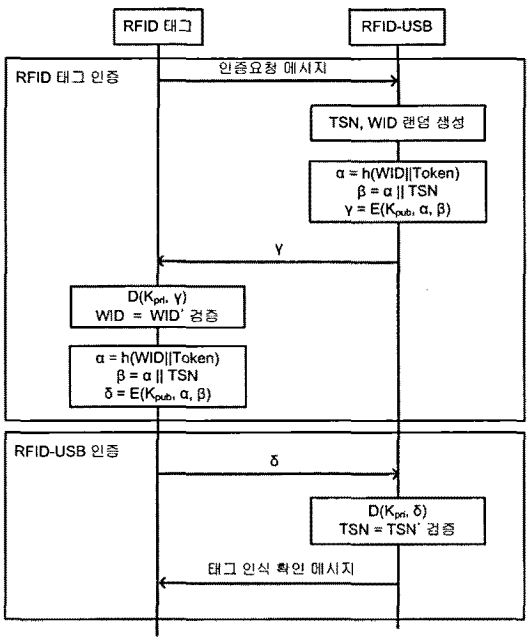
공유키 K_{share}는 인증서버의 데이터베이스에 *SID*와 쌍으로 저장되어 있으며 RFID_USB로부터 전달받은 *SID*를 이용하여 인증서버는 공유키 K_{share}을 검색한다. 검색된 공유키 K_{share}는 사전에 장비를 등록할 때 설정되어 있는 공유키 K_{share}와 비교 검증을 수행한다. 비교 검증이 완료되면 암호키 K_m을 초기화하기 위해 공유키 K_{share}를 해쉬체인에 적용한다. 암호키 K_m는 사용자가 셋톱박스에 접속할 때마다 서버에서 생성되는 키로써 제 3자가 불법적으로 접근하여 데이터를 수신하는 것을 예방한다. 암호키 K_m는 RFID 태그를 RFID-USB에 접근할 때마다 인증 서버의 보안 토큰 *Token*에 의해 동적으로 랜덤하게 생성된다. RFID리더는 RFID 태그 정보를 RFID-USB에 전달하여 RFID-USB의 데이터 베이스에 저장되어 있는 사용자 정보를 검색하여 검색과정이 일치되면 검색 결과를 인증 서버에 전달하여 사전에 등록된 공유키 K_{share}를 인증 서버의 데이터베이스에서 추출한다. 인증 서버는 생성된 사용자의 가입정보(*Token*, ID_U 등)와 셋톱박스의 정보(unique 셋톱박스 시리얼 번호, ID_{STB} 등)를 암호키 K_m을 이용하여 암호화하여 RFID 태그에게 전달한다.

3.3.2 보안 ID 검증 과정

보안 ID 검증 과정은 RFID 태그의 사용자 인증과 무결성을 체크하기 위한 과정으로써 초기화 과정에서 생성된 보안 토큰 *Token*을 이용하여 RFID 태그의 메모리내에 존재하는 보안 ID의 위치 코드값을 추출한 후 RFID 태그의 보안 ID를 계산한다. 보안 ID는 메모리에 저장된 보안 ID의 시작 주소로부터 일정 크기만큼 떨어진 옵셋 크기만큼을 실시간으로 암호학적 해쉬(e.g. SHA-1)에 적용하여 생성한다. 해쉬과정에서 생성된 데이터와 각 보안 토큰 *Token*의 옵셋으로부터 분류된 리스트는 보안 토큰 과정에서 만들어진다. 보안 ID는 옵셋 리스트와 해쉬 값이 일치하는



〔그림 7〕 보안 ID 검증 과정



〔그림 8〕 키 상호 인증 과정

경우에만 내부 메모리에 안전하게 저장되면서 외부 프로그램에 노출되거나 읽히지 않는다. RFID-USB와 RFID 태그 사이의 인터페이스에서는 키 분배 과정동안 1개의 옵셋만으로 RFID-USB에 키를 요청한다.

3.3.3 키 상호인증 과정

키 상호 인증 과정은 그림 8와 같이 RFID 태그 인증 과정과 RFID-USB 인증 과정으로 구성된다.

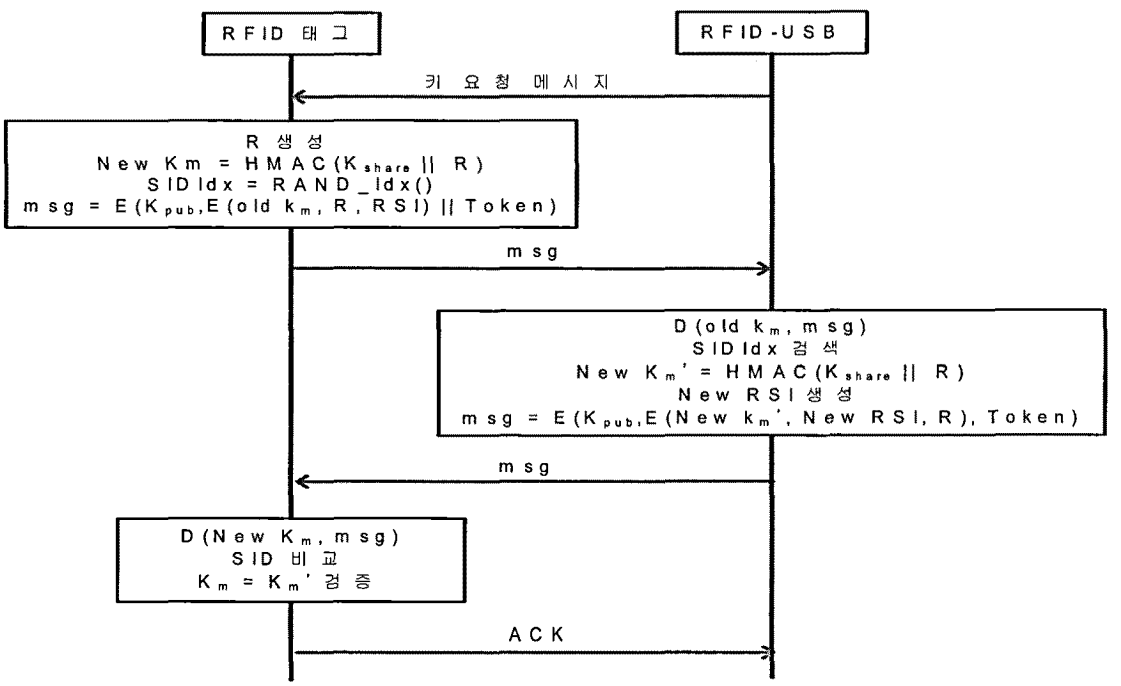
RFID 태그 인증 과정은 초기화 과정을 통해 생성된 정보값을 이용하여 RFID-USB에 인증하는 과정으로써 RFID 태그의 인증요청 메시지를 수신받은 RFID-USB는 TSN(Tag Session Number)과 WID를 랜덤하게 생성하여 RFID 태그에게 전달한

다. TSN 값은 세션에서 세션으로 통신을 수행하는데 사용되고 메시지의 도청 행위의 트래킹과 replaying을 예방하는데 사용된다. WID는 RFID-USB의 Key-storage에 저장된 RFID 사용자의 키 정보를 사전 정의된 랜덤함수에 적용하여 생성한 RFID 태그 사용자의 임시 ID를 의미한다. RFID-USB는 WID와 보안 토큰 *Token*을 XOR하여 해쉬함수에 적용한 α(=h(WID||*Token*))와 α를 TSN과 XOR한 β(=α||TSN)를 공개키 K_{pub}로 암호화하여 암호화된 결과를 γ으로 대체한 후 RFID 태그에게 전달한다. γ 메시지를 전달받은 RFID 태그는 자신의 개인키 K_{pri}를 이용하여 RFID-USB로부터 전달받은 메시지 γ을 복호화한다. 사전 정의된 랩덤 함수에 의해 복호화된 결과값 WID'는 전달받은 WID와 비교 과정을 통해 결과값이 동일하면 RFID 태그는 RFID-USB를 합법적으로 인증하고 그렇지 않으면 RFID 태그는 RFID-USB를 무시한다.

RFID-USB 인증과정은 RFID 태그가 인증을 요청할 때 RFID-USB에 저장되어 있는 RFID 태그의 정보 값을 검증하는 과정으로써 RFID-USB가 합법적인 리더로서 인증되면 RFID-USB는 RFID 태그를 인증하기 위해서 RFID 태그로부터 메시지 δ를 수신받는다. 메시지 δ는 RFID 태그가 임의로 생성한 TID와 보안 토큰 *Token*을 XOR하여 해쉬함수에 적용한 α(=h(TID||*Token*))와 α를 TSN과 XOR한 β(=α||TSN)를 공개키 K_{pub}로 암호화한다. RFID-USB는 TSN과 개인키 K_{pri}를 사용하여 δ를 복호화하고 복호화된 정보 중 TID를 셋톱박스내 데이터베이스에서 검색한 후 검색된 TSN은 RFID 태그에서 획득한 TSN과 구분하기 위해서 TSN'으로 대체한다. 대체된 TSN'는 RFID-USB에 보내지고 RFID 태그로부터 전달받은 TSN과 비교한다. 만일 TSN이 동일하게 검증되면 RFID 태그는 정상적인 태그로 인식되고 그렇지 않다면 RFID 태그는 비정상적인 태그로 인식되어 인증과정이 중지된다.

3.3.4 키 분배 과정

키 분배 과정은 다수의 RFID 태그 사용자가 RFID-USB에 접속하여 멀티미디어 서비스를 제공받으려고 할 때 다수의 RFID 태그 사용자에게 키를 연속적으로 분배하기 위한 과정으로써 키는 사전에 등록된 토큰 *Token*과 보안 태그 인식자 *SID*을 해쉬체인에 적용하여 다수의 하부키(subkey)를 생성한다. 키 분배 과정의 동작 과정은 그림 9와 같으며 세부적은 동작 과정은 다음과 같다.



[그림 9] 키 분배과정

• 단계 1 : RFID-USB는 통신 범위안에 들어온 RFID 태그들에게 새로운 암호 키를 부여하기 위해서 RFID 태그에게 키 갱신 요청 메시지를 보낸다.

• 단계 2 : RFID-USB로부터 키 갱신 요청 메시지를 전달받은 RFID 태그는 랜덤 스트링 함수 RAND_String()을 이용하여 랜덤 스트링 R을 생성한다. 생성된 랜덤 스트링 R은 K_{share}와 XOR한 후 HMAC에 적용하여 새로운 암호키 $New\ K_m$를 생성한다. 새로운 암호키가 생성되는 동시에 RFID 태그는 랜덤 인덱스 함수 *RAND_Idx*()를 이용하여 RFID 태그의 보안 인식자 인덱스 *SIDIdx*를 새로 생성하며 생성된 보안 인식자 인덱스 *SIDIdx*는 RFID 태그의 메모리 시작주소 옵셋(offset)과 보안 인식자 *SID*의 쌍으로 구성된다. RFID 태그의 보안 정보 *RSI*(*RFID Security Information*)는 RFID 태그의 메모리에 저장되어 있는 보안 인식자 *SID*를 검색하는데 사용된다. RFID 태그는 랜덤 스트링 R과 보안 인식자 정보 *RSI*를 이전 암호키 $old K_m$을 사용하여 암호화한 후 *Token*과 XOR하여 RFID-USB의 공개키 K_{pub}로 암호화한다. 암호된 메시지 *msg*는 RFID-USB에게 전달한다.

• 단계 3 : RFID-USB는 이전 암호키 $Old\ K_m$로 암호화된 메시지 *msg*를 복호화하고 RFID-USB에 저장되어 있는 RFID 태그의 정보를 이용하여 RFID 태그로부터 전달받은 랜덤 스트링 R과 보안 인식자 인덱스 *SIDIdx*를 검색한다. 검색이 정상적으로 완료되면 RFID-USB는 K_{share}와 랜덤 스트링 R을 XOR하여 HMAC에 적용하여 새로운 키 $New\ K_m'$를 생성한다. 메모리에 저장되어 있는 보안 인식자 인덱스 *SIDIdx'*의 옵셋 정보를 SHA-1에 적용하여 RFID 보안 정보 *NewRSI*을 재계산한다. RFID-USB는 새로 생성된 암호키 $New\ K_m$을 사용하여 *NewRSI*와 랜덤 스트링 R을 암호화한 후 *Token*과 XOR하여 RFID 태그의 공개키로 암호화한다. 암호화된 메시지 *msg*는 RFID 태그에게 전달한다.

• 단계 4 : RFID 태그는 새로 생성한 암호키 $New\ K_m$을 획득하기 위하여 RFID 태그의 개인키 K_{pri}를 이용하여 RFID-USB로부터 전달받은 메시지를 복호화하고 RFID-USB의 보안 인식자 *SID*는 보안 인식자 *SIDIdx*를 통해 검색한다. RFID 태그는 *SID* 리스트내에 저장된 사전 계산 값을 이용하여 보안 인식 정보 *SID*를 비교한다. 만일 보안 ID가 리스트에 있는 보안 인식자 *SID*와 일치하지 않으면 RFID-USB는 RFID 태그의 인증 여부와 RFID 태그의 무결성을 검사한다. 그리고 RFID-USB와 RFID 태그 사이에 새로 생성된 암호키의 일관성 문제 등을 점검한다. 보안 인식자 *SID*가 일치한다면 보안 토근은 이전 암호키에서 새로운 암호키로 교체하고 RFID-USB에게 ACK를 전달한다. 만약 그렇지 않다면 RFID-USB에게 NAK를 전달한다.

• 단계 5 : 보안 ID가 일치한다면 보안 토근 Token은 이전 암호키에서 새로운 암호키로 교체되고 RFID-USB에게 ACK를 전달한다. 만약 RFID-USB가 NAK를 수신한다면 암호키는 새로 변경되지 않는다. RFID-USB의 보안 토큰은 키 갱신에 있어서 제한이 있어 일정 수준 이상의 키 갱신이 요청된다면 통신이 이루어지지 않는다.

IV. 평가

4.1 보안평가

이 절에서는 제안 메커니즘의 안전성을 분석하기 위해 [15-19]에서 분류된 안전성 평가 항목 중 은밀한 검증자 공격(stolen-verifier attack), 사용자 가장 공격(user-impersonation attack), 서버 가장 공격(server-impersonation attack), 오프라인 패스워드 공격(offline password attack), 사용자 익명성(user anonymity), 재사용 공격(replay attack) 등을 고려하여 보안평가를 수행하였고, 보안평가 중 제안 메커니즘이 기존 프로토콜보다 차별성을 갖는 이유는 기존 프로토콜에서 언급되지 않은 복제 공격(Clone attack)에 대해서도 안전성을 제공하기 때문이다.

제안 메커니즘을 구성하고 있는 장비 중에서 셋톱박스와 RFID-USB는 USB 포트로 연결되어 있고 RFID-USB와 RFID 태그는 시리얼 포트로 사용자의 접근을 제어한다. RFID-USB는 다수의 RFID 태그의 접근을 제어하기 위해서 RFID 에이전트 모듈과 키 저장 장치를 내장하고 있다. RFID-USB와 RFID 태그 사이의 무선구간에서 발생하기 쉬운 재사용 공격, 복제 공격, 도청 행위 공격 등의 보안문제를 해결하기 위해 제안 메커니즘의 RFID-USB에서는 다수의 RFID 태그들이 RFID-USB에 접근할 때마

다 보안 토큰 *Token*을 랜덤하게 생성하여 비밀 정보의 노출을 예방하고 있다. 제안 메커니즘에서는 RFID-USB와 RFID 태그사이의 무선구간에서 제 3자가 태그의 인식자 ID_{tag}을 인식하지 못하도록 태그의 인식자를 보안 인식자 *SID*를 사용하여 사용자의 익명성을 제공한다. 인증 서버는 다량의 RFID를 소유한 사용자를 구분 인식하기 위해서 사용자가 사전에 등록한 RFID-USB내의 개인키 K_{pri}와 RFID 태그의 보안 인식자 *SID*를 이용하여 보안 토큰 $Token(=K_{pri} \oplus SID)$을 생성한다.

RFID-USB는 공유키 K_{share}와 랜덤 스트링 R을 사용하여 데이터를 암호화하는 암호키 K_m을 생성하기 때문에 무선 구간에서 송·수신되는 데이터가 공격자에 의해 태그의 이전 정보를 이용한 공격을 받더라도 공격자는 인증서버로부터 인증정보를 수신받지 못한다. RFID-USB와 RFID 태그사이의 일부 세션에서 교환되는 메시지를 공격자가 도청하려고 하지만 제안 메커니즘에서는 메모리에 저장되어 있는 태그의 고유 보안 인식자 인덱스 *SIDIdx*의 옵셋 정보를 SHA-1에 적용하여 RFID 보안 정보 *RSI*을 계산하여 공격자의 정보 노출 시도를 예방하고 있다.

RFID 태그 사용자는 암호키를 갱신하기 위해 이전 암호키 $\alpha d\ K_m$로 메시지를 암호화하여 RFID-USB에게 전달하면 RFID-USB는 암호키 $\alpha d\ K_m$을 사용하여 전달받은 암호 메시지를 복호화하고 RFID-USB의 메모리내에 저장되어 있는 랜덤 스트링 R과 보안 인식자 인덱스 *SIDIdx*를 검색한다. RFID-USB는 새로운 키 $New\ K_m$을 생성하기 위해서 K_{share}와 랜덤 스트링 R을 사용한다. 보안 정보 *RSI*는 메모리에 저장되어 있는 보안 인식자 인덱스 *SIDIdx'*의 옵셋 정보를 SHA-1에 적용하여 얻는다. RFID-USB는 새로 생성된 암호키 $New\ K_m$을 사용하여 *RSI*와 랜덤 스트링 R을 암호화한 후 *Token*을 XOR한 결과값을 RFID 태그의 공개키로 암호화하여 RFID 태그에게 전달함으로써 메시지의 최신성을 보장한다.

제안 메커니즘은 다수의 RFID 사용자들을 위해 RFID-USB내에 PKI 시스템을 사용하여 개인키가 저장되는데 이 때 저장된 개인키는 테이블 검색 방법을 통해 검색되어 RFID 사용자들의 테이블내 정보를 노출하지 않아도 되기 때문에 기존에 사용되고 있는 USB 키와는 구분이 된다. RFID 사용자의 개인키와 서버의 랜덤키에 의해서 동작되는 해쉬 과정은 RFID-USB 운영 장치를 통해 수행되며 USB 인터페이스를 통해 키와 다른 데이터 정보들을 셋톱박스에 사전에 저장된 정보들과 서로 교환하는 부분이 기존 USB나 RFID 리더의 동작과정과 다르다.

RFID-USB는 RFID 리더에게 전원을 공급하여 RFID 태그가 셋톱박스에 무접촉으로 인식될 수 있도록하여 RFID 태그와 셋톱박스 사이의 인터페이스 역할을 수행한다. RFID-USB는 RFID 태그와 셋톱박스의 통신 브리지 역할로써 PIN 디코드 정보, USB에 의해 생성된 랜덤코드, 해쉬 결과 등을 전달한다. 셋톱박스는 다중 사용자의 공개키를 저장하고 있어 MCU로부터 PIN 정보를 체크하고 해쉬 결과로부터 랜덤 코드를 검색한 후 검색된 코드를 셋톱박스가 보

〔표 2〕 효율성 비교평가

프로토콜 / 동 작	〔15〕	〔16〕	〔17〕	〔18〕	〔19〕	제안 메커니즘
등록 계산량	1 T_{Exp}, 2 T_H	1 T_{Exp}, 2 T_H	1 T_{Exp}, 2 T_H	5 T_H	1 T_{Exp}, 6 T_H	2 T_H
로그인 계산량	1 T_{Exp}, 2 T_H	1 T_{Exp}, 2 T_H	1 T_{Exp}, 2 T_H	5 T_H	1 T_{Exp}, 6 T_H	2 T_H
인증 계산량	1 T_H (상호인증 포함하지 않음)	1 T_{Exp}, 2 T_H(상호인증 포함하지 않음)	3 T_{Exp}, 2 T_H(상호인증 포함하지 않음)	4 T_H(상호 인증 포함)	2 T_{Exp}, 4 T_H(상호 인증 포함)	4 T_H (상호 인증 포함)
상호 인증	지원하지 않음	지원하지 않음	지원하지 않음	지원	지원	지원
패스워드 교환	지원	지원하지 않음	지원하지 않음	지원	지원	지원
잘못된 패스워드 탐지 속도	Slow	Slow	Slow	Fast	Slow	Fast
스마트카드 상의 공용 정보	$h(\cdot)$, p, g	$h(\cdot)$, p, g	$h(\cdot)$, p, g	$h(\cdot)$	$h(\cdot)$, p, g	$h(\cdot)$

p : a large prime number　　g : a public primitive element in $GF(p)$
T_{Exp} : 모듈러 연산에 대한 계산 시간　　T_H : one-way 해쉬 함수에 대한 계산시간

유하고 있는 정보와 비교하여 두 결과가 일치한다면 인증이 성공적으로 이루어지고 그렇지 않으면 에러 정보가 되돌아오게 된다.

서비스 거래 정보를 공격자가 기록하여 *SID*를 생성하거나 랜덤 스트링 *R*을 기록하여 태그를 추적할 경우 제안 메커니즘에서는 *Token*을 사용하여 공격자의 공격을 예방하고 있다. 제안된 메커니즘에서 해쉬 함수는 역으로 변환하기 어렵기 때문에 태그 인식자의 출력값이 공격자에 의해 캡처되더라도 태그의 인식자는 안전하며 태그가 새로운 리더 인식자 정보를 메모리에 갱신하려고 할 때도 새로운 리더 인식자는 이전 리더 인식자와 함께 암호화되어 리더와 태그사이의 통신이 도청될 때 안전성을 보장받는다. 제안된 메커니즘에서 생성되는 RFID-USB의 인식자는 수신기마다 서로 다른 인식자를 사용하기 때문에 제 3자가 복제된 자신의 태그를 다른 RFID-USB에 사용할 경우 RFID-USB가 태그를 인식하지 못하도록 한다. 이러한 방법은 태그에 등록된 RFID-USB의 인식자와 수신기가 해쉬함수에 의해 생성된 인식자 값과 서로 다르기 때문이다. 따라서, 복제된 태그를 사용하는 사용자는 제안 메커니즘의 해쉬함수에 의해 생성되는 인식자를 판별하기 어려워 제 3자가 자신의 스마트카드를 가지고 다른 수신기를 사용하는 것은 사실상 불가능하다.

4.2 효율성 평가

이 절에서는 제안 메커니즘의 안전성을 분석하기 위해 [15-19]에서 분류된 조건 중 제안 메커니즘에서 요구되는 7가지의 효율성 평가 요소(등록 계산량, 로그인 계산량, 인증 계산량, 상호 인증, 패스워드 교환, 잘못된 패스워드 탐지 속도, 스마트카드 상의 공용 정보)를 모두 고려하였다. 제안 메커니즘의 효율성을 평가하기 위해서 IPTV 환경의 대표적인 상호 인증 프로토콜[15-19]과 비교 평가한 결과는 표 2와 같다.

제안 메커니즘은 복제 공격을 보호하기 위해 다양한 기능들을 제공함과 동시에 기존의 사용자 인증 기법보다 기능대비 연산량면에서 효율적이다. 제안 메커니즘과 기존 프로토콜의 비교 평가는 모듈러 연산의 계산 시간(T_{Exp})과 one-way 해쉬 함수의 계산 시간(T_H)을 이용하여 등록 계산량(Computation in registration), 로그인 계산량(Computation in login), 인증 계산량(computation in authentication) 구문, 상호인증(Mutual authentication) 구문, 패스워드 교환(password change) 구문, 잘못된 패스워드 탐지 속도(Wrong password detection speed) 그리고 스마트카드의 공용 정보(public information on smard card) 등 7가지 항목을 사용한다. 제안 메커니즘은 등록 계산량과 로그인 계산량에서 모듈러 연산을 사용하는 기존 프로토콜과 달리 one-way 해쉬 함수을 2번 사용하여 사용자의 정보를 등록한다. 인증 계산량에서는 기존 프로토콜에 비해 one-way 해쉬 함수를 많이 사용하지만 상호인증을 지원하는 특징이 있다. 사용자와 셋톱박스 사이에 송·수신되는 정보 중 잘못된 패스워드를 탐지하기 위해서 제안 메커니즘에서는 다량의 RFID를 소유한 사용자를 구분 인식하는 Token을 사용한다. 또한 제안 메커니즘은 해쉬 함수만을 사용하기 때문에 기존 프로토콜에 비해 잘못된 패스워드 탐지 속도가 빠르다.

V. 결 론

인터넷망을 통하여 멀티미디어 콘텐츠를 제공하는 IPTV 서비스가 최근 급속하게 증가하고 있지만 이동 사용자와 셋톱박스 사이의 무선 구간은 많은 보안 위협에 노출되어 있다. 이 논문에서는 IPTV 서비스를 제공받는 이동 사용자의 정보를 불법적으로 도용하여 IPTV 서비스를 제공받으려는 불법 사용자를 예방하기 위한 통신 보안 메커니즘을 제안했다. 제안된 메커니즘은 RFID 태그와 RFID-USB의 에이전트가 논리적으로 동작하면서 다수의 RFID 태그가 RFID-USB와 연동할 수 있도록 상호 운영 역할을 수행하였다. 또한, RFID-USB 범위안에 접근하는 사용자가 발생할 때마다 RFID-USB에서 생성한 랜덤수와 자신의 ID로 해쉬함수에 의해 해쉬된 토근값을 업데이트하여 복제 문제를 해결하였다. 성능 평가 결과 제안 메커니즘은 one-way 해쉬 함수만을 사용하기 때문에 Wu et. al이 제안한 프로토콜보다 등록 계산량과 로그인 계산량에서 효율성을 높였으며, Token을 이용하여 사용자와 셋톱박스의 패스워드를 교환할 수 있도록 하는 동시에 상호 인증을 수행하도록 하여 잘못된 패스워드의 탐지 속도를 높였다. 향후 연구에서는 이동 사용자의 권한 접근 및 레벨을 부여하여 사용자 프라이버시를 보장하는 메커니즘을 연구 수행할 계획이다.

참 고 문 헌

[1] J. Lyu, S.J. Pyo, J.Y. Lim, M.C. Kim, S.W. Lim, and S.K. Kim, "Design of Open APIs for Personaled IPTV Service," Proceedings of 9th International Conference on Advanced Communication Technology, vol. 1, no. 4, pp. 305-310, Feb. 2007.

[2] S. Weis, S. Sarma, R. Rivest, and D. Engels, "Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems," in 1st Intern. Conference on Security in Pervasive computing(SPC), pp. 201-212, Mar. 2003.

[3] A. Juels, "Minimalist Cryptography for RFID Tags," In C. Blundo, ed., Security of Communication Networks(SCN), pp. 149-164, Sep. 2004.

[4] A.M. Eskicioglu, "Protecting Intellectual Property in Digital Multimedia Networks," IEEE Computer, vol. 36, no. 7, pp. 39-45, Mar. 2003.

[5] F.K. Tu, C.S. Laih, and S.H. Toung, "On key distribution management for conditional access system on pay-TV system," IEEE Trans. Consumer Electron., vol. 45, no. 1, pp. 151-158, Feb. 1999.

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

[7] 정윤수, 김용태, 박길철, 이상호, "RFID를 이용한 IPTV 사용자의 경량화 인증 프로토콜," 정보보호학회논문지, 19(2), pp. 105-116, Apr. 2009.

[8] F. Yuli and L. Wei, "A New RFID-USB Key," IEEE International Workshon on Anti-counterfeiting, Security, Identification 2007, pp. 440-443, Apr. 2007.

[9] 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, Oct. 2007.

[10] H. Sakakibara, K. Seki, K. Okada, and Y. Matsushita, "The ID-based noninteractive group communication key sharing scheme using smart cards," in Proc. Int. Conf. Network Protocols, pp. 91-98, Oct. 1994.

[11] D.S. Wong and A.H. Chan, "Mutually authentication and key exchange for low power wireless communications," proc. IEEE MILCOM 2001, vol. 1, pp. 39-43, Aug. 2001.

[12] T. Jiang, S. Zheng, and B. Liu, "Key Distribution Based on Hierarchical Access Control for Conditional Access System in DTV Broadcastion," IEEE Trans. On Consumer Electronics, vol. 50, no. 3, pp. 882-886, Aug. 2004.

[13] C.P. Schnorr, "Efficient identification and signatures for smart cards," In Crypto'89, LNCS 435, pp. 235-251, 1990.

[14] T. Jiang, Y. Hou, and S. Zheng, "Secure Communication between Set-top Box and Smart Card in DTV Broadcasting," IEEE Trans. on Consumer Electronics, vol. 50, no. 3, pp. 882-886, Aug. 2004.

[15] S.T. Wu and B.C. Chieu, "A User Friendly Remote Authentication Scheme with Smart cards," Computers & Security, vol. 22, no. 6, pp. 547-550, Sep. 2003.

[16] S.T. Wu and B.C. Chieu, "A Note on a User Freindly Remote User Authentication Scheme with Smart Cards," IEICE Transactions Fundamentals, vol. 87-A, no. 8, pp. 2180-2181, Aug. 2004.

[17] 유혜정, 이현숙, "스마트카드를 이용한 속성기반 사용자 인증 스킴," 정보보호학회논문지, 18(5), pp. 41-47, 2008년 10월.

[18] 김세일, 이현숙, 이동훈, "익명성을 제공하는 스마트카드 사용자 인증 프로토콜," 정보보호학회 논문지, 17(2), pp. 139-144, 2007년 4월.

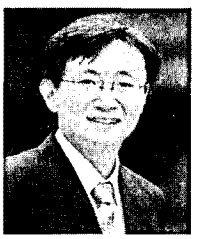
[19] 김세일, 천지영, 이동훈, "추적이 가능한 스마트카드 사용자 인증 기법," 정보보호학회논문지, 18(5), pp. 31-38, 2008년 10월.

[20] H.M. Sun, "An efficient remote user authentication scheme using smart cards," IEEE Transactions on Consumer Electronics, vol. 46, no. 4, pp. 958-961, Nov. 2000.

〈著者紹介〉

정 윤 수 (Yoon-Su Jeong) 정회원
1998년 2월: 청주대학교 전자계산학과 학사
2000년 2월: 충북대학교 대학원 전자계산학과 석사
2008년 2월: 충북대학교 대학원 전자계산학과 박사
2008년 3월~2009년 8월: 충북대 및 한남대 시간강사
2009년 9월~현재: 한남대학교 산업기술연구소 전임연구원
〈관심분야〉 정보보호, 멀티미디어, 네트워크 보안, 이동통신, 유·무선 통신, 암호이론

김 용 태 (Yong-Tae Kim) 정회원
1984년 2월: 한남대학교 계산통계학과 학사
1988년 2월: 숭실대학교 전자계산학과 석사
2008년 2월: 충북대학교 전산학과 박사
2002년 12월~2006년 2월: (주)가림정보기술 이사
2006년 3월~현재: 한남대학교 멀티미디어 학부 강의전담교수
〈관심분야〉 멀티미디어, 모바일 웹서비스, Real-time Multimedia Communicatio



박 길 철(Gil-Cheol Park) 정회원
1983년 2월: 한남대학교 전자계산학과 학사
1986년 2월: 숭실대학교 전자계산학과 석사
1998년 2월: 성균관대학교 전자계산학과 박사
2006년 3월~2007년 2월: UTAS, Australia 교환교수
1998년 8일~현재: 한남대학교 멀티미디어 학부 교수
2005년 2월~현재: 한국정보기술학회 이사 멀티미디어 분과 위원장
〈관심분야〉 Multimedia and Mobile Communication, Network Security

이 상 호 (Sang-Ho Lee) 정회원
1976년 2월: 숭실대학교 전자계산학과 학사
1981년 2월: 숭실대학교 전자계산학과 석사
1989년 2월: 숭실대학교 전자계산학과 박사
1981년 3월~현재: 충북대학교 전기전자 컴퓨터공학부 교수
〈관심분야〉 네트워크보안, Protocol Engineering Network Management