情報保護學會論文誌
第19卷 第2號, 2009. 4

RFID를 이용한 IPTV 사용자의 경량화 인증 프로토콜*

정 윤 수,[1†] 김 용 태,[2‡] 박 길 철,[3] 이 상 호[4]
[1]충북대학교, [2]한남대학교, [3]한남대학교, [4]충북대학교

A Low-weight Authentication Protocol using RFID for IPTV Users*

Yoon-Su Jeong,[1†] Yong-Tae Kim,[2‡] Gil-Cheol Park,[3] Sang-Ho Lee[4]
[1]Chungbuk National University, [2]Hannam University,
[3]Hannam University, [4]Chungbuk National University

요 약

최근에는 초고속인터넷망을 통하여 이용자의 요청에 따라 양방향으로 다양한 멀티미디어 콘텐츠를 제공하는 통신방송 융합서비스인 IPTV 서비스가 증가하고 있다. 그러나 이동성이 잦은 사용자가 IPTV 서비스를 제공받기 위해서는 사용자의 IPTV 서비스 가입 유무가 필수적이지만 현재 이동 사용자에게 제공되는 IPTV 서비스는 이동 사용자의 인증을 안전하게 제공하지 못하고 있다. 이 논문에서는 IPTV 서비스를 제공받는 이동 사용자를 안전하게 인식하기 위해 IPTV STB에 RFID를 부착하여 이동 사용자를 인증할 수 있는 경량화된 사용자 인증 프로토콜을 제안한다. 제안된 프로토콜은 이동 사용자의 인증과정에서 임의로 생성된 랜덤수를 태그가 IPTV STB로 전달하면 IPTV STB는 전달받은 랜덤수와 자신의 ID로 해쉬 함수에 의해 해쉬된 결과값을 태그에게 전달하도록 하여 무선 구간에서 자주 발생하는 reply 공격과 man-in-the-middle 공격을 예방하고 있다.

ABSTRACT

.At the most recent, IPTV service is increasing, which isa communicativebroadcasting fusion service that provides various multimedia contents interactively followed by user's request through super high-speed internet. For IPTV user service with high mobility, IPTV user's enrollment is essential. However, IPTV service provided to mobile userscan't provide the certification of mobile user securely. This paper proposes light user certification protocol which can certificate mobile users by attaching RFID to IPTV STB for secure awareness of mobile users who get IPTV service. The proposed protocol prevent reply attack and man-in-the-middle attack from happening oftenin a wireless section by transmitting the result value hashed by hash function with both its' ID and random number received from tag after tag transmits random number which generated randomly in the process of certification of mobile user to IPTV STB.

Keywords: IPTV, RFID, 인증 프로토콜(Authentication Protocol)

I. 서 론

최근에는 초고속 인터넷망을 통하여 이용자의 요청에 따라 양방향으로 다양한 멀티미디어 콘텐츠를 제공하는 통신방송 융합서비스인 IPTV 서비스가 증가하고 있다[1]. IPTV는 비디오, 오디오 그리고 제어신호를 전송하기 위한 IP 프로토콜을 적용하여 엔터테인먼트 비디오와 관련 서비스를 가입자에게 안정적으로 제공하고 QoS가 보장된 메니지드 IP 네트워크를 통해서 스트림화된 비쥬얼 콘텐츠를 가입자의 TV 또는 유사장비에 안정적으로 제공하도록 하고 있다. IPTV가 여러 유사 장비에 안정적으로 서비스를 제공받도록 하기 위해서는 서비스를 제공받는 사용자가 합

접수일(2008년 12월 1일), 수정일(2009년 2월 18일), 게재확정일(2009년 3월 13일)
* 본 연구는 지식경제부 지역혁신센터사업인 민군겸용보안공학연구센터 지원으로 수행되었음.
† 주저자, bukmunro@gmail.com
‡ 교신저자, ky7762@hannam.ac.kr

법적인 사용자인지를 IPTV STB가 확인할 수 있도록 하여야 한다. 특히 이동장비를 지원하는 IPTV 2.0은 IPTV 시스템이 사용자의 이동성으로 인해 발생되는 사용자 정보 유출에 의해 야기되는 보안 문제를 보장하고 있지않다[2].

현재까지 사용자에게 서비스되고 있는 IPTV 서비스는 유선 IPTV 서비스를 중심으로 서비스가 이루어지고 있다. 그러나 이동성이 잦은 사용자가 IPTV 서비스를 제공받기 위해서는 사용자의 IPTV 서비스 가입 유·무가 필수적이다. IPTV 시스템에 이동 사용자의 가입 유·무를 효과적으로 지원할 수 있는 RFID 기술이 있다. RFID 기술은 현재 유통분야를 시작으로 국방, 환경, 의료, 항공 등 다양한 분야에 적용되고 있으며 그 구성이 간단하여 IPTV STB에 부착하여 사용할 수 있다[3-5].

RFID 태그를 IPTV STB에 부착하면 IPTV 서비스를 요구하는 사용자의 이동성을 보장할 수 있으며, IPTV 관리자는 이동 사용자의 IPTV 가입 유·무를 한 장소에서 인식하지 않고 사용자가 원하는 위치에서 IPTV 서비스를 제공할 수 있는 특징이 있다. 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 있다.

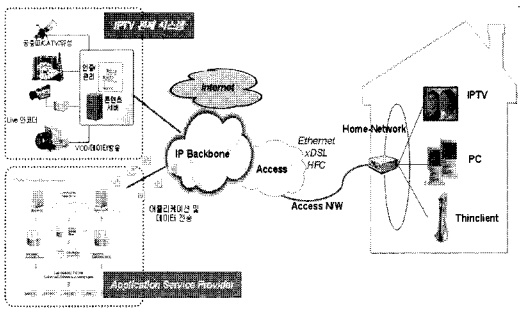
이 논문에서는 IPTV 서비스를 제공받는 이동 사용자를 인식하기 위해 IPTV STB에 RFID를 부착하여 이동 사용자를 인증할 수 있는 경량화된 사용자 인증 프로토콜을 제안한다. 제안된 프로토콜은 이동 사용자의 인증과정에서 임의로 생성된 랜덤수를 태그가 IPTV STB로 전달하면 IPTV STB는 전달받은 랜덤수와 자신의 ID로 해쉬 함수에 의해 해쉬된 결과값을 태그에게 전달하도록 한다. 이 과정은 이동 사용자가 매번 접속할 때마다 매번 변경되므로 공격자가 결과값을 도청되더라도 공격자는 출력값을 통해 인증을 수행할 수 없다. 또한, 제안 프로토콜은 기존 IPTV에서 지원하지 못한 이동성을 보장하고 있어 사용자가 특정 장소에서 서비스를 요청할 때 인증 서버의 낮은 통신 오버헤드와 서비스 지연을 제공한다.

이 논문의 구성은 다음과 같다. 2장에서는 IPTV 개념, IPTV 콘텐츠 보안 및 IPTV 보안기술에 대해서 분석한다. 3장에서는 RFID 기술을 이용하여 이동 사용자의 낮은 통신 오버헤드와 서비스 지연을 제공하기 위한 IPTV 사용자의 경량화된 인증 프로토콜을 제시하고, 4장에서는 제안 프로토콜에 대한 성능평가와 보안평가를 분석한다. 마지막으로 5장에서는 이 논문의 결과를 요약하고 향후 연구에 대한 방향을 제시한다.

II. 관련연구

2.1 IPTV 개념

IPTV(Internet Protocol TV)는 초고속인터넷 망을 통하여 이용자의 요청에 따라 양방향으로 다양한 멀티미디어 콘텐츠를 제공하는 통신방송 융합서비스이다[1]. IPTV는 방송 전파가 아닌 인터넷 프로토콜을 이용하여 인터넷 방송처럼 스트리밍 방식의 방송 프로그램을 이용자가 시청할 수 있도록 서비스한다. IPTV는 기존 아날로그 시대의 단방향적 방송이 갖는 시·공간적 제약을 붕괴시킴으로써 보다 적극적이고 능동적으로 여러 부가 서비스를 이용할 수 있는 장점을 가진다.



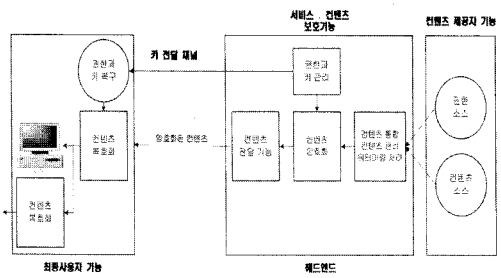
[그림 1] IPTV 서비스 구성도

[그림 1]은 플랫폼(HeadEnd), IP 네트워크, 단말장비 등과 함께 Triple Play의 서비스를 제공할 수 있는 장비로 구성된 IPTV 서비스의 구성도를 보여주고 있다. [그림 1]의 IPTV 서비스 구성도는 주문형 콘텐츠(VOD 등), 인터넷 검색, T-Commerce 서비스 및 이용자 요청에 따라 실시간으로 방송 프로그램을 전송하는 서비스 등에 사용된다.

2.2 IPTV 콘텐츠 보안

IPTV 컨텐츠 보안은 서비스 기술에 따라 컨텐츠 소유자에 의해 허용된 권한으로 획득한 컨텐츠를 사용하도록 보장하는 기술과 적법한 사용자가 해당 서비스와 서비스 내에 포함되어 있는 컨텐츠를 이용하도록

지원하는 기술로 구분된다[1]. IPTV 콘텐츠의 기본 보안 구조는 [그림 2]와 같다. [그림 2]의 주요 구성 요소로는 최종 사용자 기능, 서비스·컨텐츠 보호 기능, 네트워크 기능 그리고 컨텐츠 제공자 기능 등이 있다.



[그림 2] IPTV 일반 보안구조

[그림 2]에서 컨텐츠 제공자에 의해 제공된 컨텐츠는 서비스·컨텐츠 보호 기능에 의해 암호화되고, 암호화된 컨텐츠와 암호화된 세션키가 최종 사용자 기능에 별도로 전달된다. 최종 사용자는 암호화된 세션키를 복호화해 세션키를 복구하고, 복구된 세션키로 암호화된 컨텐츠로부터 해당 컨텐츠를 얻고 사용자가 콘텐츠를 디스플레이한다. [그림 2]의 구성요소 중 컨텐츠 제공자는 서비스 제공자에게 컨텐츠를 제공하는 개체를 의미하며 경우에 따라서 컨텐츠 제공자는 서비스 제공자 역할도 함께 수행한다. 서비스·컨텐츠 보호는 헤드엔드의 핵심 기능이며, 서비스와 서비스 내 컨텐츠에 대한 접근을 제어함은 물론 서비스 인프라를 보호하는 역할을 수행한다. 네트워크 기능은 컨텐츠를 전달하는 네트워크를 인증하고 접근을 제어하며, 네트워크 요소의 무결성을 보장한다. 또한 최종 사용자 기능은 IPTV 단말에 대한 무결성을 보장하고, 컨텐츠가 다른 IPTV 단말로 재분배될 때 컨텐츠의 무결성과 기밀성을 제공한다.

IPTV 서비스 보안을 위해 최근까지 연구된 브로드캐스트 암호화[6-8]와 멀티캐스트 키 관리[9-12]와 같은 기술들은 pay-TV 시스템의 액세스 제어를 위해 응용되고 있다. 이 기술들은 일반적으로 하나의 그룹만을 위한 권한을 고려하고 있다. 이 방법들은 시스템의 많은 채널들은 통신과 계산 부하가 존재하게 된다. 브로드캐스트 암호 기법을 위해서는 고정 계층에 위치하기위해 모든 사용자에게 키 설정 값을 주는 것을 고려해볼 수 있다. 브로드캐스트 암호 기법[7,8]을 위해서는 불법적인 사용자를 무효화시키는 기능에도 불구하고 통신과 계산 로드가 크게 나타난다. 반면 멀티캐스트 키 관리 기법[9-12]은 동적 사용자 계층을 포함하고 있어 제공자와 모든 사용자 사이의 계층 관리와 동기화가 가능하다. [5]는 워터마크 기술을 기반으로 Pay-TV에 적용시킨 기법을 제안하고 있다. 이 기법은 저작권 관리 문제를 처리하기 위해 동일 시간동안에 제어 액세스을 위한 마스크 프레임을 사용하였다.

2.3 IPTV 보안 요구사항

IP 망을 이용하고 있는 IPTV의 방송 전송 기술은 손실 없는 영상을 전송할 수 있는 특징과 IP 망을 이용한 새로운 서비스의 적용이 쉬운 특징이 있지만 공개된 네트워크 IP를 이용하기 때문에 사용자의 불법적인 방송 시청, 사업자에 종속적인 접근 제어 기술의 보급, 시청자 맞춤형 서비스의 어려움 그리고 방송 단말 사이의 상호호환성 부재 등의 문제점이 발생한다.

사용자의 불법적인 방송 시청은 IPTV 시스템이 제3자로부터 공격을 받을 경우 모든 단말기(STB)의 관련 기능을 갱신해야하는 문제점이 있다. 특히, IPTV 서비스에서 사용자의 서비스가 전송 중간에 네트워크 가로채기(TCP-hijacking) 기술로 인하여 연결되어 있는 세션에 대해서 연결을 가로채는 공격이 가능하다. 이 문제를 해결하기 위해서는 가입자 정보를 기반으로 채널인증을 하는 동일 네트워크의 다른 사용자가 사용자의 불법적인 방송시청에 접근할 수 있도록 해야 한다.

IPTV의 콘텐츠 불법 유출은 영화, 비디오, 방송 등을 이용하여 사용자에게 전송되는 과정중에 발생되며 이러한 컨텐츠 불법 유출을 예방하기 위해서는 일정 수준 이상의 수신 제한 기술이 요구된다. 콘텐츠 제공자의 요구에 맞는 수신 제한 기술을 적용하기 위해서 콘텐츠 제공자는 서버 제품과 방송 수신 제어 모듈에 탑재된 단말 및 케이블 카드를 일괄 구입하여 수신 제한 기술을 적용해야 한다.

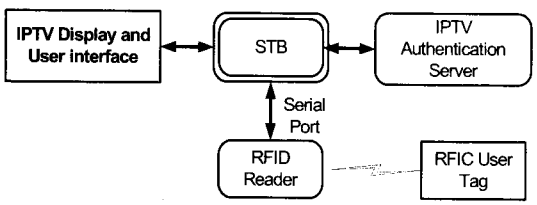
IPTV 환경에서 시청자의 맞춤형 시청을 제공하기 위해서는 SI(System Information) 정보를 처리하는 기술도 중요하지만 사용자의 요구에 적합한 다양한 형태의 유료 방송 서비스가 필요하다. IPTV의 맞춤형 방송이 활성화 된다면 일방적인 방송 가입(기본 채널 가입)보다는 사용자가 선호하는 채널 혹은 프로그램에 대해서만 지불하는 다양한 형태의 방송 시청이 가능하다. VOD나 PPV와 같은 유료 콘텐츠에 대해서 해당 서비스를 받는 방송 수신 기술과 콘텐츠 제공 사업자는 동적 재구성이 가능한 수신 제한 기술을 사

용해야 한다.

IPTV 서비스가 다양한 형태의 수신 제한이 가능하고 콘텐츠 제공자마다 서로 다른 수신 제한 기술이 동작하도록 하기 위해서는 IPTV 서비스가 특정 수신 제한 기술에 종속되지 않고 동적으로 재구성이 가능한 시스템 구조가 필요하다. 방송 수신 제어 기술은 그 기술의 안정성이 가장 중요한 요소이기 때문에 새로운 방식의 방송 수신 제한 기술을 적용하기 쉽고 해킹이나 오류가 발생하는 경우 이를 쉽게 대치할 수 있어야만 한다.

III. RFID 기술을 사용하는 IPTV 사용자의 경량화된 인증 프로토콜

이 절에서는 RFID 기술을 이용하여 이동 사용자의 낮은 통신 오버헤드와 서비스 지연을 제공하기 위한 IPTV 사용자의 경량화된 인증 프로토콜을 제안한다. 제안 프로토콜에서 사용한 XOR 알고리즘의 목적은 태그의 비용을 낮추면서 계산 속도를 향상시키기 위해서다.



〔그림 3〕 제안된 인증 프로토콜을 위한 IPTV 시스템의 인터페이스

〔그림 3〕은 IPTV 시스템에 RFID 태그를 부착한 경량화된 사용자 인증 프로토콜의 IPTV 시스템 인터페이스를 나타내고 있다. 〔그림 3〕의 RFID 리더는 STB와 직접적으로 시리얼 포트를 사용하여 연결되며 STB와 RFID 리더 사이에 시리얼 포트를 이용할 수 없다면 USB 포트를 사용한다. STB는 플로그 앤 플레이 기능을 가지고 리더를 인식하도록 프로그램되어야 하고 드라이버를 로드하도록 한다. IPTV 인증 서버에는 사용자의 태그 정보를 데이터베이스에 저장되어 있으며 데이터베이스에 저장되어 있는 태그 정보는 태그 인식자와 인정정보 쌍으로 구성된다. 성공적으로 로드된 후 초기 명세는 EPG(Electronic Program Guide)에 의해 서버로부터 다운로드 되도록 한다. 이것은 사용자가 RFID 태그로부터 특정 입력 부분에 대해서 안내하고 사용자의 모든 행동의 경로를 유지한다. 서버는 암호, 인증, 프로그램 설치, 사용자 플파일, 사용자 콘텐츠 등을 업무를 수행한다.

3.1 용어정의

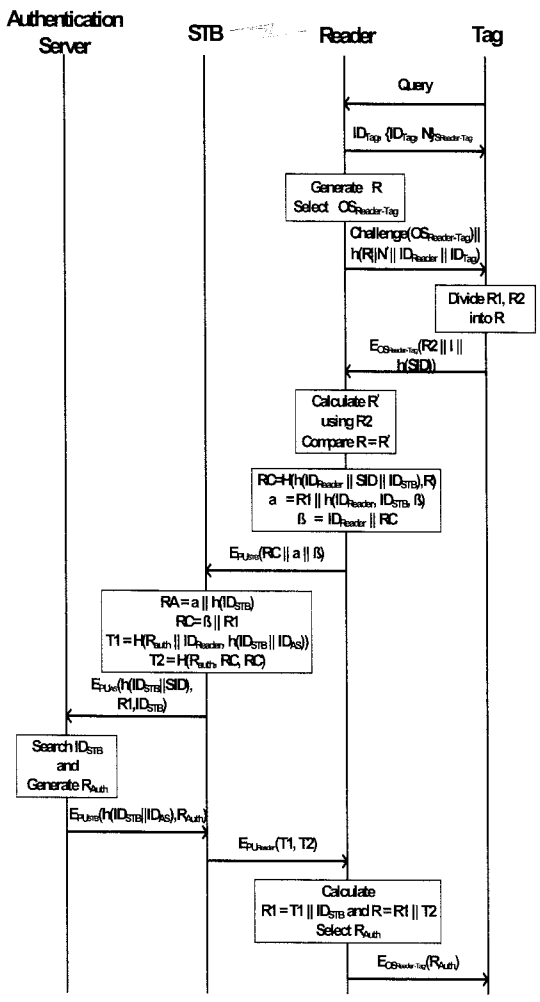
제안 프로토콜에서 사용하는 주요 용어를 정의하면 〔표 1〕과 같다. 〔표 1〕의 SID_i는 태그의 보안 인식자로써 IPTV 서비스를 가입한 모든 사용자에게 태그와 함께 제공되며 인증을 위해 사용되는 키는 마스터 키 K_M, 태그의 비밀 키 $K_S^{'}$, 리더와 태그 사이에 사전에 공유된 공유키 K_{pub} 등이 있다. 정보의 최신성을 위해 제안 프로토콜에서는 태그의 랜덤수 N, 리더의 랜덤 수 R과 R'을 사용하며 일방향성의 해쉬 함수 $h()$로 연접되어 공격자의 메시지 정보 노출 시도를 예방한다.

〔표 1〕 제안 프로토콜의 용어 정의

용 어	정 의
AS	인증 서버
ID_i	i의 인식자
SID_i	태그 i의 보안 ID
STB	SET-Top Box
N	리더가 생성한 난수값
$S_{Reader-Tag}$	리더와 태그가 사전에 공유한 비밀키
PU_A	A의 공개키
PR_A	A의 개인키
$E_{PU_A}(X)$	A의 공개키를 가고 X를 암호화
$D_{PR_A}(X)$	A의 개인키를 통해 X를 복호화
I	제어 인식자
N	태그의 랜덤 수
R, R'	리더의 랜덤 수
$R1$, $R2$	리더가 생성한 R을 태그가 임의의 2개 크기로 분할한 랜덤 수
$h(\cdot)$	128비트 크기의 일방향 collision-resistant 해쉬 함수
$H(\cdot)$	RFID 리더와 STB 만이 알고 있는 일방향 collision-resistant 해쉬 함수
$Token_{A-B}$	A와 B사이의 토근 정보
R_{Auth}	리더의 인증정보
RC, RA, RS, α, β	인증과정 중에 생성된 값을 저장하기 위한 파라미터

3.2 경량 인증 프로토콜

이 절에서는 태그를 소유한 이동 사용자가 STB에 부착된 리더를 통해 인증서버로부터 서비스를 안전하게 요청받기 위한 동작과정을 수행한다. [그림 4]에서는 태그와 리더, 리더와 인증 서버 사이에 임의의 랜덤수와 해쉬함수를 적용하여 경량화된 인증 과정을 보여주고 있다. 또한 STB와 리더는 시리얼포트로 연결되어 동작되며 리더와 인증서버간 동작과정은 사용자의 서비스 지불여부를 확인하는 과정으로써 사용자의 인증 여부는 인증서버에 전달된 사용자의 정보를 검색한 후 검색 결과가 올바르면 검색 결과를 STB/리더에게 전달하여 사용자를 인식하도록 한다.



[그림 4] IPTV 시스템에서 RFID 기술을 이용한 인증 프로토콜 과정

[그림 4]의 경량 인증 프로토콜은 전체 15단계로 구성되며 1~3 단계는 리더 자신이 생성한 랜덤수를 태그에게 전달하고 4 단계는 챌린지한 비밀키를 리더 자신이 생성한 랜덤 수 R, 랜덤 수 N', 인식자 ID_{Reader}, ID_{Tag} 등과 함께 해쉬하여 태그에게 전달한다. 5~6 단계는 전달받은 R를 $R1$과 $R2$로 분리한 후 데이터 정보 I와 보안 인식자 SID를 비밀키로 암호화하여 리더에게 전달한다. 7 단계는 태그에게 전달받은 정보를 복호화한 후 복호화한 $R2$를 이용하여 랜덤수 R'를 생성한다. 8 단계는 시리얼 포트를 통해 STB에게 리더가 생성한 α, β, RC 값을 전달한다. 9 단계는 인증서버에게 태그의 정보를 인증받기 위해 RA와 RS를 생성한다. 10~11 단계는 태그의 인증서를 인증서버에게 부여받기 위해 태그 정보를 해쉬하여 공개키 PU_{AS}로 암호화하여 인증서버에게 전달하면 인증서버는 데이터베이스로부터 태그의 정보를 검증받고 인증정보 R_{Auth}를 생성한다. 단계 12~13 단계는 인증정보와 태그 정보를 암호화하여 시리얼 포트를 통해 리더에게 전달한다. 마지막으로 14~15 단계는 리더로부터 전달받은 인증정보 R_{Auth}를 저장하기 전에 랜덤수 R을 비교검증한다. 각 단계의 세부적인 동작과정은 다음과 같다.

• 단계 1: 리더는 태그의 랜덤 수 N을 요청하기 위해 리더의 ID를 포함한 쿼리 정보를 태그에게 전송한다. 태그가 쿼리를 수신한 후에 태그는 이전에 저장된 리더의 ID와 함께 XOR 과정을 통해 랜덤 수 N을 생성한다.

• 단계 2~3: 리더는 자신이 생성한 난수 값 N과 태그 인식자 ID_{TAG}을 리더와 태그가 사전에 공유한 비밀키 $S_{Reader-Tag}$로 암호화하여 전달한 후 태그와 임시적으로 사용할 랜덤수 R을 생성하여 비밀키 $S_{Reader-Tag}$를 AES 암호 알고리즘에 적용하여 일회성 비밀키 $OS_{Reader-Tag}$를 생성한다.

• 단계 4: 리더 자신이 생성한 랜덤 수 R, 랜덤 수 N', 인식자 ID_{Reader}, ID_{Tag} 등을 해쉬한 후 일회성 비밀키 $OS_{Reader-Tag}$를 챌린지한 결과 값을 XOR하여 태그에게 전달한다. 이 때, 랜덤 수 N'는 단계 1에서 리더가 태그에게 전달한 랜덤 수 N을 검증하기 위한 랜덤 수를 의미한다. 또한 챌린지를 통해 태그에게 전달된 일회성 비밀키 $OS_{Reader-Tag}$는 태그와 리더사

이에 송수신되는 메시지를 암·복호하는데 사용된다.

• 단계 5~6 : 태그는 리더로부터 전달받은 정보 중 랜덤 수 N'을 보관중인 랜덤 수 N과 비교 검증을 통하여 검증결과가 올바르지 않으면 바로 인증동작을 그만둔다. 비교검증이 올바르면 태그는 전달받은 정보 중 랜덤 수 R를 $R1$과 $R2$로 분리한 후 $R2$, 추가적인 데이터 정보 I 그리고 태그의 보안 인식자 SID를 일회성 비밀키 $OS_{Reader-Tag}$를 이용하여 암호환 한 후 리더에게 함께 전달한다.

• 단계 7: 리더는 비밀키 $OS_{Reader-Tag}$를 이용하여 태그에게 전달받은 정보를 복호화한 후 복호화한 $R2$를 이용하여 랜덤수 R'를 생성한다. 리더는 태그에게 전달하기 전의 랜덤수 R과 새로 생성한 R'를 비교하여 랜덤수가 정확한지를 검증한다. 검증이 완료되면 리더는 랜덤수 R을 인식자 ID_{Reader}, ID_{STB}, SID과 함께 리더와 STB 만이 알고 있는 일방향 collision-resistant 해쉬 함수 $H()$에 적용하여 RC 값을 생성한다. 그리고 RC값과 인식자의 무결성을 보장하기 위해 제안 프로토콜에서는 α, β 값을 생성한다. α는 $R1$과 $h(ID_{Reader}, ID_{STB}, \beta)$을 XOR 하여 생성하고 β는 $Token_{R_Tag}$과 ID_{Reader}, RC를 XOR하여 생성한다. 마지막으로 SID는 해쉬 함수를 사용하여 태그의 정보를 찾기 위해 사용되는 동시에 태그가 데이터베이스로부터 전달받은 정보가 신뢰성이 있는지를 검사하기 위해 사용된다.

• 단계 8: 리더는 생성된 α, β, RC 값을 STB의 공개키 PU_{STB} 키를 이용하여 암호화한 후 시리얼 포트를 통해 STB에게 전달한다.

• 단계 9 : STB는 시리얼 포트를 통해 전달받은 정보를 STB의 개인키 PR_{STB}를 이용하여 복호화한 후 인증서버에게 태그의 정보를 인증받기 위해 RA와 RS를 생성한다. RA는 태그의 인식자를 판별하기 위한 정보이며 RS는 리더의 무결성을 보증하기 위한 정보이다.

• 단계 10 : STB는 인증서버에게 태그의 인증서를 부여받기 위해 태그가 생성한 SID와 ID_{STB}를 해쉬한 값 $h(ID_{STB}||SID)$에 $R1$와 ID_{STB}를 추가하여 인증서버의 공개키 PU_{AS}를 이용하여 암호화한 후 암호화된 정보를 인증서버에게 전달한다.

• 단계 11 : 인증서버는 STB에게 전달받은 정보를 이용하여 데이터베이스로부터 태그의 정보를 검증받고 검증이 끝난 후 태그의 정보를 이용한 인증정보 R_{Auth}를 생성한다.

• 단계 12~13 : 인증서버는 태그의 정보를 이용하여 생성한 인증정보 R_{Auth}를 SID, ID_{STB}, ID_{AS}와 함께 해쉬한 값을 STB의 공개키 PU_{STB}로 암호화한 후 STB에게 전달한다. STB는 전달된 정보를 STB의 개인키 PR_{STB}를 이용하여 복호화한 후 인증정보 R_{Auth}와 인식자 ID_{STB}, ID_{AS}, ID_{Reader}를 해쉬함수 $H()$를 이용하여 $T1$생성하고, 인증정보 R_{Auth}와 RA, RS를 해쉬함수 $H()$에 적용하여 $T2$를 각각 생성한다. 생성된 $T1$과 $T2$는 리더의 공유키 PU_{Reader}로 암호화한 후 시리얼 포트를 통해 리더에게 전달한다.

• 단계 14~15: 리더는 인증서버가 생성한 인증정보 R_{Auth}를 얻기위해 우선 먼저 리더가 STB에게 전달받은 정보중 랜덤수 R를 추출하여 리더가 보유하고 있던 랜덤수 R과 비교검증한다. 검증이 끝나면 리더는 인증 정보 R_{Auth}를 일회성 비밀키 $OS_{Reader-Tag}$로 암호화하여 태그에게 전달하고 태그는 전달받은 인증정보 R_{Auth}를 저장한다.

3.3 IPTV 인증 갱신

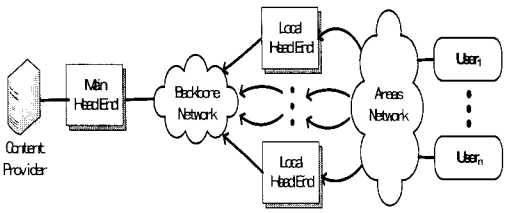
IPTV 사용자의 인증을 갱신하기 위해서 태그는 해쉬된 인식자 $h(SID_i)$를 리더에게 전달한다. 리더가 $h(SID_i)$의 해쉬 값을 수신할 때 인증서버는 데이터베이스와 통신하고 데이터베이스에 저장되어 있는 인식자 SID_i을 검색한다. 갱신 처리과정에서 인증된 리더는 이전 리더에서 목적지 리더로 변하게 된다. 리더는 태그의 해쉬값을 얻고 데이터베이스에게 해쉬값을 보낸다. 데이터베이스는 그 때 태그의 메모리에 저장된 SID_i을 갱신하고 알린다. 응답에서 데이터베이스는 새로운 SID_i을 찾고 그것을 리더에게 전달한다. 리더가 새로운 SID_i을 전달받았을 때 이전 값과 XOR하고 태그에게 XOR된 값을 전달한다. 태그는 이전 SID_i과 XOR 값으로부터 새로운 값을 얻는 후 정보를 갱신한다. 갱신처리 과정에서 새로운 SID_i와 이전 SID_i 사이에 XOR 값이 노출되더라도 공격자는 새로운 SID_i

를 얻지 못한다. 이것은 이전 SID_i의 정보를 알지 못하기 때문에 발생되는 현상이다.

IV. 평 가

4.1 실험환경

제안 프로토콜은 실험의 객관성을 유지하기 위하여 IPTV 모델에서 사용하는 [그림 5]의 실험 환경을 구축하여 표 1의 성능 평가 변수를 적용하여 시뮬레이션을 수행하였다. IPTV 인증 서버의 가입자 인식 시간은 0.1~1.5초로 설정하고 권한 레코드 크기를 20비트 크기로 전송하도록 실험한다.



[그림 5] 전체 실험 환경

[표 2] 실험 환경

용어	정의
가입자 수	5,000, 25,000, 50,000, 100,000
인증 리스트 갱신주기	60 분
가입자 인식 시간	0.1~15 초
권한키 재전송 시간	15 초
지불 시간 기간이 남은 가입자 비율	1%, 5%, 10%, 15%, 20%
권한 레코드 크기	20 비트

제안 프로토콜에서 STB와 IPTV 인증서버의 실험 명세는 [표 3]과 같다. [표 3]에서 기술한 IPTV 인증 서버와 STB의 세부명세 항목은 프로세서, 램, 운영체제, 포트, 메모리 등이 있다. IPTV 인증서버는 Intel Core 2 프로세스와 Linux 운영체제를 통해 TCP/IP 포트로 인증서버를 운영하며 STB는 MPEG 디코더를 이더넷, USB, RS-232등의 인터페이스를 통해 임베디드 Linux 운영체제를 사용하여 RFID 태그를 인식한다.

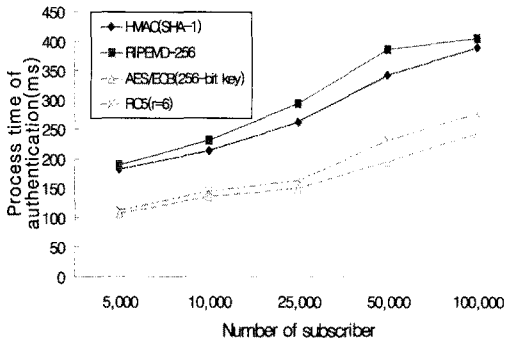
[표 3] STB와 IPTV인증 서버의 세부 명세서

IPTV Authentication Server	
Processor	Intel Core 2 Duo
RAM	2GB
Operating System	Linux
Port	TCP/IP
Memory	526 MB
Set-Top-Box	
CPU	MIPS 300MHz(SMP8634)
MPEG Decoder	MPEG-1, MPEG-2 MP@HL, MPEG-4.2 ASP@L5, MPEG-4.10(H.264), MP@L4.1, HP@L4.1, WMV9/VC-1 MP@HL
Interface	Ethernet, USB, RS-232
OS	Embedded Linux
Memory	256MB SDRAM, 32MB Flash Memory

4.2 성능평가

4.2.1 가입자 수와 암호 알고리즘에 따른 인증서버의 인증 처리시간

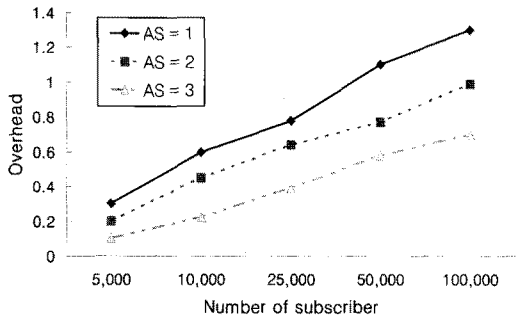
[그림 6]은 IPTV 인증서버와 가입자 사이에 송·수신 되는 인증 정보에 암호 알고리즘 HMAC (SHA-1),RIPEMD-256, AES/ECB(256-bit key) 그리고 RC5을 EAP-AKA 인증 유형에 적용한 가입자의 인증 처리시간을 평가하고 있다. 실험 결과의 객관성을 위해 가입자 수는 5,000명, 25,000명, 50,000명, 100,000명으로 설정하여 실험하였으며, 암호 알고리즘에 사용되는 서명과 검증 수치는 [14]의 벤치마크된 실험수치를 참조하여 평가하였다. [그림 6]의 X축 항목은 가입자수를 나타내며 Y축 항목은 인증 처리시간을 의미한다. 실험결과 가입자 수에 따른 인증 처리시간은 비례적으로 증가하였으며, 가입자 수가 50,000명 이하일 경우에는 인증 처리시간의 증가율이 일정하게 증가하였지만 가입자 수가 50,000명 이상일 경우에는 인증서버의 오버헤드로 인해 인증 처리시간의 증가율이 급격하게 증가하였다.



〔그림 6〕 가입자 수와 암호알고리즘에 따른 인증 서버의 인증 처리시간

4.2.2 가입자 수에 따른 인증서버의 오버헤드

〔그림 7〕은 가입자 수에 따른 IPTV 인증 서버의 오버헤드를 비교 평가하고 있다. 〔그림 7〕에서 인증서버(Authentication Server, AS)의 수는 콘텐츠 관리자가 1에서 3까지 그룹관리되는 것으로 실험하였으며 가입자 수가 5,000명에서 100,000명으로 증가할 경우 인증 서버의 오버헤드 또는 점차적으로 증가하였다.



〔그림 7〕 가입자 수에 따른 인증서버의 오버헤드

특히 오버헤드가 급격하게 증가하는 경우는 인증서버 1개를 운영할 경우에는 25,000명 이상부터 나타났으며 인증서버 2개를 운영할 경우에는 50,000명 이상부터 나타났다. 반면 인증서버를 3개 운영할 경우에는 가입자 수가 증가할 수록 오버헤드가 급격하게 증가하지 않고 비례적으로 증가하였다. 〔그림 7〕의 결과를 기반으로 인증서버 당 가입자수를 그룹 관리할 경우 그룹 관리하지 않을 경우보다 인증서버의 오버헤드를 최대 25%까지 줄일 수 있었다.

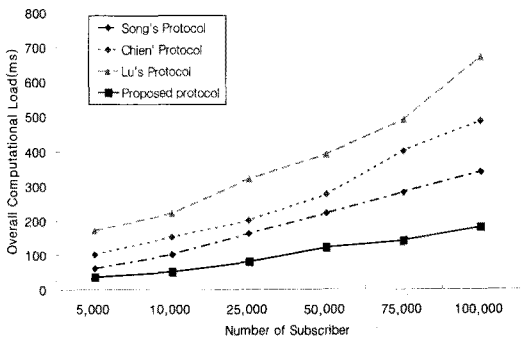
4.2.3 가입자 수에 따른 인증서버의 계산 지연시간

제안 프로토콜은 Chien〔15〕, Song〔16〕, Lu〔17〕와 함께 일방향 함수 사용에 따른 계산량 비교를 위해 〔표 4〕처럼 태그와 서버의 계산량을 평가한다.

〔표 4〕 태그와 서버의 계산량

	태그의 계산량	인증 서버의 계산량	총 계산량
제안 프로토콜	5H	6H	11H
Chien〔15〕	4H	$(K_2+3)H$	$(K_2+7)H$
Song〔16〕	3H	$(K_2+1)H$	$(K_2+4)H$
Lu〔17〕	$(2\log N+3)H$	$(\log N+K_1+3)H$	$(3\log N+K_1+6)H$

H : one-way 함수
N : 시스템에서 사용된 태그의 수
K_1 : $1\leq k \leq \log N$을 만족하는 정수
K_2 : $1\leq k\leq 2N$을 만족하는 정수



〔그림 8〕 가입자 수에 따른 서버의 계산 지연시간

〔그림 8〕에서 기존 프로토콜들은 사용자가 증가할수록 태그와 서버의 계산량이 제안 프로토콜에 비해 $\log N$(N은 가입자 수) 크기로 증가하게 되어 인증 서버의 전체 계산 지연시간이 비례적으로 증가하지만 제안 프로토콜은 태그와 인증서버에서 총 계산량이 일정크기로 증가하여 전체 계산 지연시간의 증가율이 다른 프로토콜에 비해 낮게 나타난다. 또한 제안 프로토콜은 다른 프로토콜에 비해 가입자의 수가 5,000에서 100,000으로 증가더라도 전체 계산 지연시간은 다른 프로토콜에 비해 일정하게 나타난다.

4.3 보안평가

4.3.1 사용자간 맞춤형 서비스 평가

STB에 부착되어 있는 리더와 태그사이에 올바른 상호 동작을 지원하기 위해서는 제 3자가 태그의 인식자를 인식하지 못하도록 하는 것이 중요하다. 제안 프로토콜에서는 태그의 인식자를 비밀 인식자 *SID*를 사용하여 제 3자가 태그의 인식자를 인식하지 못하도록 하였으며 정당한 세션 간에는 태그의 비밀 인식자 *SID*를 동일하게 사용하도록 하고 있다. 제안 프로토콜에서는 리더와 태그사이에 공유된 일회성 비밀키 $OS_{Reader-Tag}$에 의해 데이터를 암호화한 후 송·수신하기 때문에 공격자가 태그의 이전 정보를 이용하여 공격하더라도 공격자는 인증서버로부터 인증 정보를 수신받지 못한다.

4.3.2 사용자의 불법적인 방송 시청 평가

제안 프로토콜의 일부 세션에서 교환되는 메시지는 공격자가 리더와 태그 사이에서 도청하려고 하지만 제안 프로토콜의 메시지는 일방향성의 해쉬 함수 $h()$로 연접되어 공격자의 메시지 정보 노출 시도를 예방하고 있다. 특히 모든 세션에서 해쉬 함수 $h()$내에 랜덤 수 R을 포함시키고 있어 메시지의 최신성을 보장받게 된다. 리더와 태그 사이의 무선구간에서 태그는 단지 인증된 리더에게만 응답하며 태그 자신이 출력 정보를 생성하지 않기 때문에 공격자가 리더로 가장하여 태그의 정보를 유추하는 man-in-the-middle 공격을 수행하더라도 예방할 수 있다.

4.3.3 단말 사이의 상호 호환성 평가

제안 프로토콜에서 일반향 해쉬 함수를 사용한 이유는 공격자가 사전 이미지의 노출 정보를 이용할 수 없도록하기 위해서이다. 공격자는 사용자의 정당한 서비스 거래를 기록하여 *SID*를 복구하려고 시도하거나 *SID*를 생성하기 위해 랜덤 수 R을 기록하여 태그를 추적하려고 하지만 제안 프로토콜에서는 *SID*를 계산할 수 없도록 하고 있다. 제안 프로토콜에서 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.

4.3.4 서비스 제공자에 종속적인 접근 제어 평가

STB에서 생성되는 *RS* 정보는 제안 프로토콜에서 크게 2가지 역할을 수행한다. 첫째는 각 사용자가 서비스를 요청할 때마다 사용자가 소유하고 있는 태그와 STB/리더 사이에서 사용되는 세션키의 시드 정보를 나타내며 둘째는 제 3자가 시도하는 악의적인 공격 중 replay 공격과 impersonation 공격을 예방한다. 제안 프로토콜에서는 매 통신마다 서로 다른 일회성 비밀키 $OS_{Reader-Tag}$가 생성되며 생성된 일회성 비밀키 $OS_{Reader-Tag}$는 권한 관리 메시지 (Entitlement Management Message, EMM)의 제어 문자 (Control World, CW)를 암호화하여 전달하기 때문에 평문(plaintext) 공격의 암호 알고리즘 공격을 예방하고 있다. 여기서 CW는 채널 단위로 관리되며 주기적으로 갱신되고 암/복호화에는 서비스 제공자와 사용자가 공유하고 있는 단말기 암호키가 사용된다. 단말기 암호키는 효율적인 운영을 위해 계층화된 키 구성이 사용된다. 제안 프로토콜에서 생성되는 STB/리더의 인식자는 수신기마다 서로 다른 인식자 ID_{STB_i}/ID_{Reader_i}를 사용하기 때문에 제 3자가 복제된 자신의 태그를 다른 STB/리더에 부착하여 사용할 경우 STB/리더가 태그를 인식하지 못하도록 하고 있다. 이러한 방법은 태그에 등록된 STB/리더의 인식자와 수신기가 해쉬함수에 의해 생성된 인식자 값과 서로 다르기 때문이다. 따라서, 복제된 태그를 사용하는 사용자는 제안 프로토콜의 해쉬함수에 의해 생성되는 인식자를 판별하기 어려워 제 3자가 자신의 스마트카드를 가지고 다른 수신기를 사용하는 것은 사실상 불가능하다.

V. 결 론

이 논문에서는 IPTV 서비스를 제공받는 이동 사용자를 인식하기 위해 IPTV STB에 RFID를 부착하여 이동 사용자를 인증할 수 있는 경량화된 사용자 인증 프로토콜을 제안했다. 제안된 프로토콜은 이동 사용자의 인증과정에서 임의로 생성된 랜덤수를 태그가 IPTV STB로 전달하면 IPTV STB는 전달받은 랜덤수와 자신의 ID로 해쉬 함수에 의해 해쉬된 결과값

을 태그에게 전달하도록 한다. 이 과정은 이동 사용자가 매번 접속할 때마다 매번 변경되므로 공격자가 결과값을 도청되더라도 공격자는 출력값을 통해 인증을 수행할 수 없다. 성능 평가 결과, 가입자 수에 따른 인증 처리시간은 비례적으로 증가하였으며, 가입자 수가 50,000명 이하일 경우에는 인증 처리시간의 증가율이 일정하게 증가하였지만 가입자 수가 50,000명 이상일 경우에는 인증서버의 오버헤드로 인해 인증 처리시간의 증가율이 급격하게 증가하였다. 오버헤드가 급격하게 증가하는 경우는 인증서버 1개를 운영할 경우에는 25,000명 이상부터 나타났으며 인증서버 2개를 운영할 경우에는 50,000명 이상부터 나타났다. 반면 인증서버를 3개 운영할 경우에는 가입자 수가 증가할 수록 오버헤드가 급격하게 증가하지 않고 비례적으로 증가하였다. 인증서버 당 가입자수를 그룹 관리할 경우 그룹 관리하지 않을 경우보다 인증서버의 오버헤드를 최대 25%까지 줄일 수 있었다. 향후 연구에서는 이동 사용자의 권한 접근 및 레벨을 부여하여 사용자 프라이버시를 보장하는 메커니즘을 연구 수행할 계획이다.

참 고 문 헌

[1] WiMAX Forum NWG, "Stage-3: Detailed Protocol and Procedures," 2007.

[2] IEEE 802.16e-2005, "Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems," 2006.

[3] D. Sweeney, "WiMax Operator Manual: building 802.16 Wireless Networks," 2, illustrated, revised, 2th Ed., Apress, 2005.

[4] D. Johnston and J. Walker, "Overview of IEEE 802.16 security," IEEE Security & Privacy, vol. 2, no. 3, pp. 40-88, May-June 2004.

[5] S. Xu, M.M. Matthews, and C.T. Huang, "Security issues in privacy and key management protocols of IEEE 802.16," in ACM Southeast Regional Conference, R. Menezes, Ed. ACM, pp. 113-118, Mar. 2006.

[6] M. Barbeau, "Wimax/802.16 threat analysis," in Q2SWinet '05: Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks. New York, NY, USA: ACM Press, pp. 8-15, Oct. 2005.

[7] A. Ghosh, D.R.J. Wolter, G. Andrews, and R. Chen, "Broadband Wireless Access with WiMax/802.16: Current Performance Benchmarks and Future Potential," IEEE Communications Magazines, vol. 43, issue 2, pp. 129-136, Feb. 2005.

[8] IEEE 802.16e-2005, "Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems," 2006.

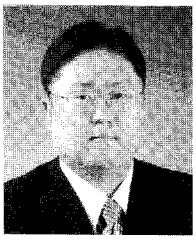
[9] IETF RFC 4285, "Authentication Protocol for Mobile IPv6," 2006.

[10] WiMAX Forum NWG, "Stage-3: Detailed Protocol and Procedures," 2007.

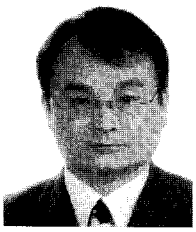
[11] S. Xu and C.T. Huang, "Attacks on PKM protocols of IEEE 802.16 and its later versions," Proceedings of the 3rd International Symposium on Wirelesss Comunication Systems (ISWCS 2006), pp. 185-189, Sep. 2006.

[12] D. Johnston and J. Walker, "Overview of IEEE 802.16 Security," IEEE Security & Privacy, pp. 40-48, May 2004.

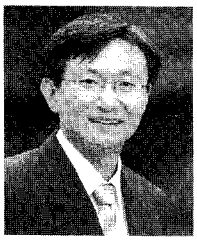
〈著者紹介〉



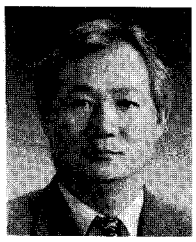
정 윤 수 (Yoon-Su Jeong) 정회원
1998년 2월: 청주대학교 전자계산학과 학사
2000년 2월: 충북대학교 대학원 전자계산학과 석사
2008년 2월: 충북대학교 대학원 전자계산학과 박사
2008년 3월~현재: 충북대 및 한남대 시간강사
〈관심분야〉 유·무선 보안, 암호이론, 정보보호, Network Security, 이동통신보안



김 용 태 (Yong-Tae Kim) 정회원
1984년 2월: 한남대학교 계산통계학과 학사.
1988년 2월: 숭실대학교 전자계산학과 석사.
1995년 2월: 충북대학교 전산학과 박사수료.
2002년 12월~2006년 2월: (주)가림정보기술 이사
2006년 3월~현재: 한남대학교 멀티미디어 학부 강의전담교수
〈관심분야〉 멀티미디어, 모바일 웹서비스,Real-time Multimedia Communication



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