IPTV 서비스에서 사용자의 수신자격을 효율적으로 판별할 수 있는 해쉬 함수 기반의 상호 인증 프로토콜

(A Mutual Authentication Protocol based on Hash Function for Efficient Verification of User Entitlement in IPTV Service)

정 윤 수 † 김 용 태 †† 정 윤 성 ††† 박 길 철 †††† 이 상 호 †††††
(Yoon-Su Jeong) (Yong-Tae Kim) (Yoon-Sung Jung) (Gil-Cheol Park) (Sang-Ho Lee)

요 약 최근 방송과 통신의 융합 흐름은 방송 영역에서 제공되던 멀티미디어 콘텐츠를 초고속 인터넷, 케이블 TV망 그리고 위성 망 등을 통해 실시간으로 전송하는 IPTV 서비스로 변화되고 있다. 그러나 디지털 방송 서비스가 다양한 매체로 확산되면서 서비스 제공자가 사용자들에게 제공하는 IPTV 서비스의 콘텐츠 보안은 기존 방송 시스템에서 제공하는 CAS(Conditional Access System)만을 이용해서는 완벽하게 지원할 수 없다. 이 논문에서는 IPTV 서비스의 콘텐츠 보안 문제를 해결하기 위해 IPTV 시스템을 구성하는 구성 요소 중 수신기(Set-Top BoX, STB)와 스마트카드 사이의 사용자 수신자격을 효율적으로 판별할 수 있는 상호인증 프로토콜을 제안한다. 제안된 프로토콜은 기존 프로토콜에 비해 사용자가 지불하는 채널에 대한 수신자격을 수신기가 올바르게 전송할 수 있도록 서명기반의 해쉬함수를 사용한다. 또한, 제안 프로토콜은 상호인증 과정을 통해 수신기와 스마트카드 사이에서 생성된 세션키를 이용하여 EMM를 암호화한 후 제3자가 서비스를 불법적으로 이용할 수 없도록 한다.

키워드 : IPTV 서비스, CAS, 상호 인증, 해쉬 함수, 프로토콜

Abstract The fusion stream of recent broadcasting and communication make multimedia content served in the area of broadcasting into IPTV service which transmits it through high-speed internet, cable TV net and satellite net in realtime. However, as the digital broadcasting service is extended to various media, the security of IPTV service content provided to users by service provider is not fully supported by CAS(Conditional Access System) provided by existing broadcasting system. This paper proposes interactive certification protocol which can efficiently distinguish the receiving-qualification of user between Set-Top Box and Smart Card which are parts of configurations for IPTV system. The proposed protocol uses hash function to make Set-Top Box transmit receiving-qualification about the channel fee which user pays more properly than existing protocol. Also, the proposed protocol uses session key generated between receiver and smart card through inter certification process and encrypts EMM not the service to be used by anyone illegally.

Key words : IPTV Service, CAS, Mutual Authentication, Hash Function, Protocol

· 이 논문은 2010년도 한남대학교 학술연구조성비 지원에 의하여 연구되었음

† 정 회 원 : 한남대학교 산업기술연구소 전임연구원
bukmunro@gmail.com
†† 정 회 원 : 한남대학교 멀티미디어학부 강의전담
ky7762@hannam.ac.kr
††† 정 회 원 : Alcorn State University Department of Advanced Technologies Assistant Professor/Statistician
ysjung72@gmail.com
†††† 정 회 원 : 한남대학교 멀티미디어학부 교수
gcpark@hannam.ac.kr
(Corresponding author임)
††††† 정 회 원 : 충북대학교 전기전자컴퓨터공학부 컴퓨터전공 교수
shlee@chungbuk.ac.kr

논문접수 : 2008년 11월 19일
심사완료 : 2010년 2월 23일

Copyright©2010 한국정보과학회 : 개인 목적이나 교육 목적인 경우, 이 저작물의 전체 또는 일부에 대한 복사본 혹은 디지털 사본의 제작을 허가합니다. 이 때, 사본은 상업적 수단으로 사용할 수 없으며 첫 페이지에 본 문구와 출처를 반드시 명시해야 합니다. 이 외의 목적으로 복제, 배포, 출판, 전송 등 모든 유형의 사용행위를 하는 경우에 대하여는 사전에 허가를 얻고 비용을 지불해야 합니다.

정보과학회논문지: 정보통신 제37권 제3호(2010.6)

1. 서 론

IPTV는 트리플 플레이 서비스(Triple Play Service)의 대표적인 서비스 중 하나이며, 방송, 통신, 그리고 데이터 서비스를 하나의 서비스로 구성하여 제공하는 융합서비스이다[1]. IPTV 서비스는 주문형 서비스(Video on Demand, VoD) 뿐만 아니라 위성 DMB, 지상파 DMB 등의 방송 서비스를 인터넷 환경에서 제공할 수 있는 서비스로 각광받고 있다. 그러나 IPTV 시스템은 표준 모델이 존재하지 않아 기존 방송 시스템에서 제공하는 수신제한시스템(CAS : Conditional Access System)만을 이용하여 방송 서비스를 접근하는 사용자의 접근 여부를 제어함으로써 콘텐츠 보호 문제를 해결하고 있다[2].

방송 컨텐츠 보호를 위해 최근 IPTV에 대한 보안 연구는 Lee[3], Tu et al[4], Huang et al.[5]을 중심으로 활발히 연구되고 있다. 그 중에서 Lee 기법은 수신제한 시스템을 위해 제어문자(Control Word, CW), 직접 수신자격 키(Direct Entitlement Key, DEK), 분배 키(Distribution Key, DK), 마스터 개인키(Master Private Key, MPK) 등 4레벨 키 계층 기반의 키 분배기법을 제안했다[3]. Lee 기법은 n 레벨의 키에 의해 n-1 레벨의 키를 암호화하는 방식(Lee 기법에서 사용되는 키들은 직접 수신자격 키로 제어문자를 암호화, 분배키로 직접 수신자격 키를 암호화, 마스터 개인키로 분배키를 암호화하는 방식 등)을 사용한다. Lee 기법은 안전한 모듈을 통해 개인키와 공개키를 서비스 제공자가 업로드 할 경우에 적합한 장점을 가지지만 통신과정 중에 통신 부하가 많이 발생되는 단점을 가지고 있다.

Tu et al. 기법은 Lee 기법에서 사용되는 분배 키 대신에 RGK 키로 대체한 4 계층 기법을 제안했다[4]. Tu et al. 기법에서 가입자들은 서로 다른 수신 그룹을 구성하고 특정 기간동안 가입자의 채널과 요금지불에 따라서 그룹을 변경하도록 하고 있다. 그러나 Tu et al. 기법은 분배 키를 업데이트하는 것이 패키지 브로드캐스팅의 많은 양을 요구하여 IPTV 서비스의 성능을 최상으로 유지하지 못하는 단점을 가지고 있다. Huang et al. 기법은 IPTV 서비스를 가입자 중심의 서비스로 제안한 기법이다[5]. Huang et al. 기법은 제어문자, 권한 키, 분배키 그리고 가입자를 위한 비밀키로 구성된 4레벨 기법이다. Huang et al. 기법은 권한 키와 분배 키의 전달과 갱신을 제어함으로써 한 달에 한 번 청구서를 청구하는 기본 방송서비스와는 다르게 1일 사용하는 서비스에 대한 기본 청구서를 청구할 수 있는 서비스 제공자를 제공하는 장점을 가진다. 그러나 Huang et al. 기법은 다른 기법들에 비해 안전성이 떨어지는 문제점이 있다.

이 논문에서는 IPTV 서비스를 지원하는 장비 중 사용자의 스마트카드와 수신기(Set-Top BoX, STB)사이에 서명기반의 해쉬 함수를 이용하여 불법적으로 서비스를 제공받으려는 사용자의 서비스 수신자격을 효율적으로 판별할 수 있는 상호인증 프로토콜을 제안한다. 제안 프로토콜은 기존 프로토콜에 비해 해쉬 함수를 이용하여 사용자가 지불하는 채널에 대한 수신자격을 올바르게 판별할 수 있는 세션키를 생성하도록 하여 스마트카드에서 발생되기 쉬운 cloning 문제[6]와 McCormac 문제[7]를 해결하고 있다. 여기서 cloning 문제는 네트워크에 노드가 배포되는 시간동안 새로운 노드 또는 기존 노드로 위장하는 복제 노드를 주입하는 공격 방법이고, McCormac 문제는 스마트카드에서 STB까지의 데이터 라인에서 동일한 스마트 카드처럼 동작하는 다른 STB에 연결할 때 발생하는 공격방법이다. 제안 프로토콜에서 생성된 세션키 SK는 $R2_S$, $R_S^{'}$, ID_U, $h(ID_S)$를 연접하여 one-way 해쉬 함수에 적용시켜 갱신된 단말기 암호키와 사용자가 신청한 수신자격을 전송하기 위하여 수신자격 관리 메시지(EMM : Entitlement Management Message)을 암호화하도록 하였으며 이 과정을 통해 제3자가 인식자를 판별하지 못하도록 하여 제3자가 서비스를 불법적으로 이용할 수 없도록 하였다.

이 논문의 구성은 다음과 같다. 2에서는 IPTV 서비스와 IPTV 보안 기술에 대하여 분석한다. 3장에서는 스마트카드와 수신기 사이에서 안전한 사용자의 수신자격을 판별할 수 있도록 서명기반의 해쉬함수를 이용한 상호인증 프로토콜을 제시하고, 4에서는 제안 프로토콜에 대한 효율성 및 보안성에 대하여 분석·평가한다. 마지막으로 5장에서는 이 연구의 결과를 요약하고 향후 연구에 대한 방향을 제시한다.

2. 관련연구

2.1 IPTV 서비스

IPTV는 유/무선 IP망에 연결된 셋탑박스, 단말 등을 통해 TV 수상기로 제공하는 방송형 및 통신형 서비스이다[1]. 즉, IPTV는 방송용 전파가 아닌 인터넷 프로토콜을 이용하여 인터넷 방송처럼 스트리밍 방식의 방송프로그램을 시청한다. IPTV 서비스는 주문형 비디오(VOD), 디지털영상저장(DVR) 서비스뿐만 아니라 TV 스크린을 통한 인스턴트 메시지 전송서비스 등을 제공한다. IPTV는 버전에 따라 협의의 IPTV(IPTV 1.0)와 광의의 IPTV(IPTV 2.0)로 구분된다. 협의의 IPTV는 IP-STB을 기반으로 한 거실 TV형 유선방송 서비스를 의미하며, 광의의 IPTV는 ALL-IP 기반의 유선과 무선이 통합된 거실 TV형, 이동 TV형, 유무선 방송 서비스

를 의미한다. 그림 1은 협의의 IPTV의 전체 구성도를 나타내고 있다.

IPTV가 인터넷 방송과 다른 점은 컴퓨터 모니터가 TV 브라운관으로 바뀌고, 키보드 및 마우스가 리모콘으로 바꾸어 져서 컴퓨터를 다루기 쉽지 않은 이용자까지 서비스를 손쉽게 이용할 수 있다는 장점이 있다. 즉, 어린이나 노약자 등 PC에 익숙하지 않은 사람이라도 간단히 리모콘이나 무선 키보드를 이용하여 인터넷 검색은 물론 영화 감상, 홈쇼핑, 홈뱅킹, 홈트레이딩, 화상서비스, 온라인 게임, 노래방, MP3 등 TV 인터넷이 제공하는 다양한 콘텐츠 및 부가서비스를 제공받을 수 있다. IPTV는 데이터 통신기술의 강점인 우수한 양방향 특성에 기반하여 다음과 같은 서비스를 제공할 수 있다.

2.2 IPTV 보안 기술

2.2.1 수신제한시스템

수신제한시스템(CAS : Conditional Access System)은 유료 방송 서비스에 대한 사용자의 접근 여부를 제어하는 시스템으로써 접근 조건으로 시청료 납부, 수신지역, 수신등급 등을 검사하며 방송 사업자의 비즈니스와 수익을 보호하는 것을 목적으로 사용되어 왔다[8]. 그림 2는 수신자격 제어 메시지(ECM : Entitlement Control Message)와 수신자격 관리 메시지(EMM : Entitlement Management Message)가 어떻게 생성되고 전송되어 서비스되는지를 보여주는 수신제한시스템의 기본 동작 모델이다.

수신자격 제어 메시지는 단말기 암호키(Device Key,

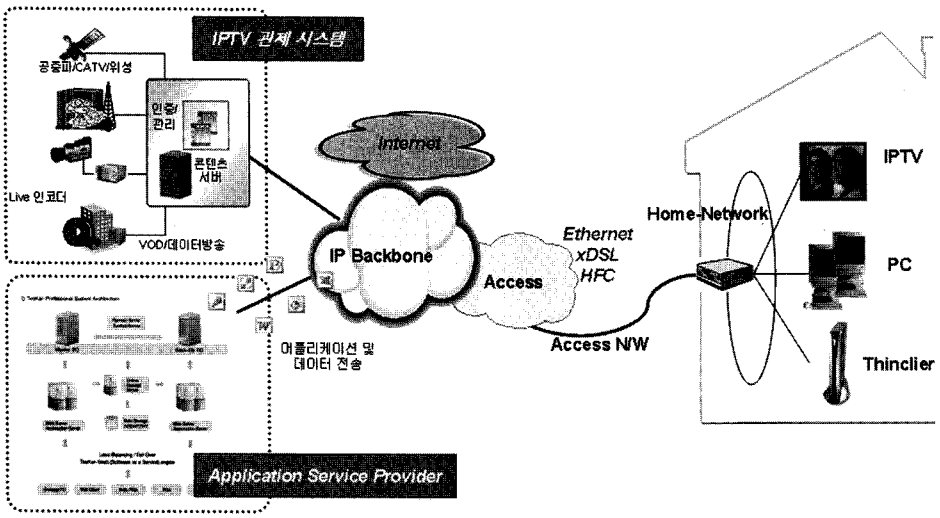
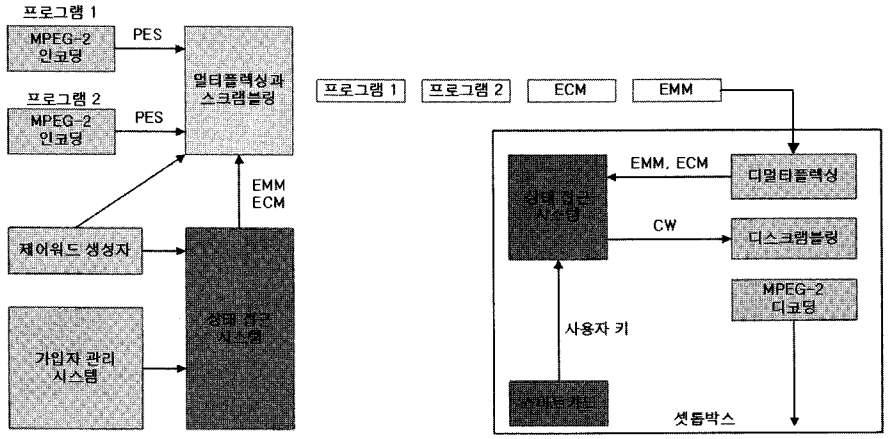


그림 1 IPTV 개요 및 서비스 구성도



<참조 : KBS 방송기술연구 - DTV 콘텐츠 저작권 보호기술 및 동향 -, 2007>

그림 2 수신제한시스템 동작 모델

DK)로 암호화된 제어단어(Control Word, CW)를 가입자에게 전달하기 위하여 사용된다. 수신자격 제어 메시지는 프로그램 정보와 접근조건 등과 함께 사용자에게 전달되며 사용자는 전달된 정보를 스마트카드로 입력하여 처리한다. 사용자가 보유하고 있는 스마트카드는 수신자격 제어 메시지의 접근조건과 스마트카드에 저장되어 있는 수신자격을 비교한 후, 해당 프로그램에 대한 권한을 갖고 있다고 판단되면 제어 문자를 복호화하여 수신기로 전달한다. 수신자격 관리 메시지는 갱신된 단말기 암호키와 사용자가 신청한 수신자격을 전송하기 위하여 사용된다. 수신자격 관리 메시지의 구성 및 수신자의 특성에 따라 수신자격 관리 메시지는 다양한 종류를 통해 사용되어진다.

2.2.2 DRM

DRM(Digital Rights Management)은 디지털 콘텐츠의 지적 재산권을 관리하고 제어하는 제반 기술이다[9]. DRM은 불법 복제를 방지하기 위하여 디지털 콘텐츠의 데이터를 암호화하고, 인증된 사용자나 단말기에 한해서만 라이센스를 발급하도록 콘텐츠의 이용을 제어한다. DRM을 사용하는 시스템은 디지털 콘텐츠의 데이터를 암호화하여 무단복제를 방지, 인증된 사용자 및 단말기에 대해서만 라이센스를 발급 그리고 라이센스에 포함된 Rights 및 키를 이용하여 복호화를 수행하는 기능을 수행한다. 그림 3은 DRM의 동작모델을 보여주고 있다.

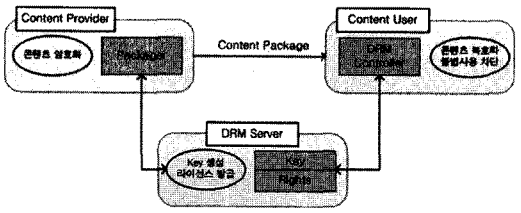


그림 3 DRM 동작 모델

그림 3의 동작과정에서 콘텐츠 정보가 DRM 서버에 등록되고, 콘텐츠 데이터에 대한 암호화가 이루어진다. 콘텐츠 제작자는 콘텐츠 패키지를 사용자가 접근할 수 있도록 하기 위해 DRM 서버에 Right와 키를 발급받아야 한다. 사용자는 DRM 서버로부터 발급받은 라이센스를 이용하여 콘텐츠 패키지를 복호화하여 이용한다.

2.3 기존연구

Lee 기법은 수신제한시스템을 위해 제어문자(Control Word, CW), 직접 수신자격 키(Direct Entitlement Key, DEK), 분배 키(Distribution Key, DK), 마스터 개인키(Master Private Key, MPK) 등 4레벨 키 계층 기반의 키 분배기법을 제안했다[3]. 제어문자와 직접 수신자격(Entitle) 키는 ITU-R 810에 정의된 제어 문자와 권한 키(Authorize Key, AK)와 동일한 기능을 갖는다. Lee 기법에서 사용되는 키들은 n 레벨의 키에 의해 n-1 레벨의 키를 암호화하는 방식(직접 수신자격 키로 제어문자를 암호화, 분배키로 직접 수신자격 키를 암호화, 마스터 개인키로 분배키를 암호화하는 방식 등)을 사용한다. Lee의 기법은 안전한 모듈을 통해 개인키와 공개키를 서비스 제공자가 업로드할 경우에 적합하지만 통신과정 중에 통신부하가 많이 발생되는 단점이 있다.

Tu et al. 기법은 Lee 기법에서 사용되는 분배 키 대신에 RGK 키로 대체한 4 계층 기법을 제안했다[4]. Tu et al. 기법에서 가입자들은 서로 다른 수신 그룹을 구성하고 특정 기간동안 가입자의 채널과 요금지불에 따라서 그룹을 변경하도록 하고 있다. 요금을 징수한 그룹과 함께 수신된 그룹들을 구분하기 위해 RGK를 할당하여 많은 소그룹의 크로스 참조(cross-referenced) 모델을 형성한다. 요금 지불이 특정한 날에 시작할 경우 Tu et al. 기법은 한 달의 모든 날로 키를 분산하여 공유하는 장점을 가진다. 그러나 대부분의 소비자는 한 달 중 특정 기간내에 가입하지 못한다. 이 때, 분배 키 업데이트가 패키지 브로드캐스팅의 많은 양을 요구할 경우 좋은 성능을 발휘하지 못하는 단점이 있다.

Huang et al. 기법은 가입자 서비스를 위해 제안된 기법으로 제어문자, 권한 키, 분배키 그리고 가입자를 위한 비밀키로 구성된 4레벨 기법이다[5]. 이 기법에서 사용되는 채널은 대응(corresponding) 키, 권한 키, 분배키를 가지는 서로 다른 그룹으로 구성된다. 권한 키는 분배키보다 상대적으로 작은 생명주기를 가진다. 이 때, 권한 키와 분배키의 전달과 갱신을 제어함으로써 Huang et al. 기법은 한 달에 한번 기본 청구서를 청구하는 기존 방송 서비스와는 달리 1일 기본 청구서를 청구할 수 있는 서비스 제공자를 제공될 수 있는 장점을 갖는다. 그러나 다른 기법에 비해 안전성이 떨어지는 단점이 있다. 이 같은 원인은 모든 권한 키가 IPTV 서비스동안 밀접하게 연관되어있어 특정 기간 동안에 다른 권한을 가진 사용자들이 현재 사용중인 서비스에 대해서 쉽게 계산할 수 있으며 이와 유사한 연구는 [10,11] 등이 있다.

현재 연구 중에 있는 브로드캐스트 암호화[12-14]와 멀티캐스트 키 관리[15-18] 같은 기술들은 pay-TV 시스템의 액세스 제어를 위해 응용되고 있다. 이 기술들은 일반적으로 하나의 그룹만을 위한 권한을 고려하고 있다. 만일 기술들이 pay-TV에 적용한다면 각 채널에 맞는 대응(corresponding) 그룹이 존재하여야 한다. 결과적으로 시스템의 많은 채널들은 통신과 계산 부하가 존재하게 된다. 브로드캐스트 암호 기법을 위해서는 고정 계층에 위치하기위해 모든 사용자에게 키 설정 값이 주어져야 한다. 브로드캐스트 암호 기법[13,14]은 불법적인

사용자를 무효화시키는 기능에도 불구하고 통신과 계산 로드가 크다. 반면 멀티캐스트 키 관리 기법[15-18]은 동적 사용자 계층을 포함하고 있어 제공자와 모든 사용자 사이의 계층 관리와 동기화가 가능하다. [19]는 워터마크 기술을 기반으로 Pay-TV에 적용시킨 기법을 제안하고 있다. 이 기법은 저작권 관리 문제를 처리하기 위해 동일 시간동안에 제어 액세스를 위한 마스크 프레임을 사용하였다.

3. 사용자 수신자격을 판별하기 위한 상호 인증 프로토콜

이 절에서는 서비스 가입 사용자가 IPTV 브로드캐스팅 과정중에 채널 사용 요금을 지불하지 않고 서비스를 제공받으려고 하는 불법 사용자를 예방하기 위해 해쉬 함수를 이용한 상호 인증 프로토콜을 제안하고 있다. 사용자들에게 IPTV 서비스를 제공하는 서비스 제공자(Service Provider, SP)는 제안 프로토콜에서 사용자간 프라이버시 문제를 처리할 수 있는 충분한 능력을 보유하고 있다고 가정한다.

3.1 용어

제안 프로토콜에서 사용하는 주요 용어를 정의하면 표 1과 같다.

3.2 서명기반 해쉬함수를 이용한 상호 인증 프로토콜

제안 프로토콜은 그림 4처럼 등록 과정, 상호인증 과정 그리고 유지보수 과정의 3 단계로 구성된다. 제안 프로토콜은 각 사용자가 수신기 디코더의 보안 모듈에 사용자만이 알고 있는 비밀키를 가지고 있다.

3.2.1 등록 과정

등록과정은 IPTV 서비스를 제공받기 원하는 사용자가 가입자 관리 시스템(Subscriber management system, SMS)에게 서비스를 요청하는 과정으로써 서비스를 제공받기 위해서는 사용자의 스마트카드 인식자 ID_U와 패스워드 PW_U가 필수적이다. 등록 과정의 세부적인 동작과정 절차는 그림 5와 같다.

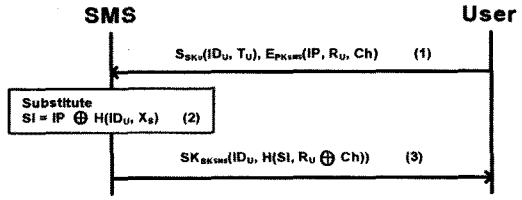


그림 5 등록과정 절차

표 1 제안 프로토콜의 용어 정의

용 어	정 의
U	가입자
SMS	가입자 관리 시스템(Subscriber Management System)
ID_U	스마트 카드의 가입자 ID 번호 인식자
ID_S	수신기의 ID 번호 인식자
PW_U	가입자의 패스워드
X_S	SMS의 비밀키
T_U	가입자의 서비스 등록 시간
R_U	가입자가 생성한 임의의 랜덤수
$R1_S$, $R2_S$	스마트카드가 생성한 임의의 랜덤수
Ch	가입자가 선택한 채널정보
$h(\cdot)$	128비트 크기를 one-way collision-resistant 해쉬 함수
$H(\cdot)$	스마트 카드와 수신기 만이 알고 있는 one-way collision-resistant 해쉬 함수
$E_{PK_x}(M)$	X의 공개키를 사용하여 암호화된 메시지 M
$S_{SK_x}(M)$	X의 개인키를 사용하여 서명된 메시지 M
$E_{SK}(M)$	스마트카드와 수신기가 서로 공유한 세션키로 암호화된 메시지 M
X ⊕ Y	X와 Y의 exclusive-or 동작

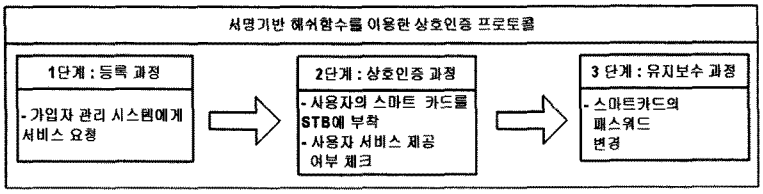


그림 4 제안된 상호 인증 프로토콜의 동작과정

• 단계 1 : 가입자 관리 시스템(SMS) ← 가입자

이 단계는 가입자가 IPTV 서비스를 제공받기 전에 가입자 관리 시스템에 가입정보를 전달하는 단계로써 가입자 U는 가입자 관리 시스템에게 서비스를 요청하기 위해서 사용자 U의 정보 중 스마트카드 인식자 ID_U와 패스워드 PW_U를 해쉬 함수 $H(\bullet)$에 적용하여 IP=H(ID_U, PW_U)를 생성한 후 가입자가 생성한 임의의 랜덤수 R_U, 채널 정보 Ch와 함께 가입자의 서비스 등록 시간 정보 T_U를 식 (1)처럼 가입자 관리 시스템에게 전달하여 등록한다.

SMS ← 가입자 : $S_{SK_U}(ID_U,\ T_U),\ E_{PK_{SMS}}(IP,\ R_U,\ Ch)$ (1)

• 단계 2 : 가입자 관리 시스템(SMS)

이 단계는 가입자 관리 시스템이 가입자로부터 전달받은 정보를 이용하여 가입자가 서비스를 제공받을 수 있도록 가입자의 정보를 가공하는 단계로써 가입자 관리 시스템은 가입자에게 전달받은 정보를 복호화한 후 전달받은 가입자의 스마트카드 인식자 ID_U와 가입자 관리 시스템(Subscriber Management System, SMS)이 생성한 비밀키 X_S를 식 (2)처럼 해쉬 함수에 적용한 후 가입자에게 전달받은 IP와 exclusive-OR 하여 SI로 대체한다.

$$\text{Substitute } SI = IP \oplus H(ID_U,\ X_S) \quad (2)$$

• 단계 3 : 가입자 관리 시스템(SMS) → 가입자

이 단계는 가입자 관리 시스템이 가공된 가입자의 정보를 가입자에게 전달하는 단계로써 가입자 관리자 시스템은 가입자가 생성한 임의의 랜덤수 R_U와 채널 정보 Ch를 exclusive-OR한 후 단계 2에서 생성된 SI와 함께 해쉬 함수 $H(\bullet)$에 적용한다. 가입자 관리자 시스템은 가입자 인식자 ID_U와 함께 $H(SI,\ R_U \oplus Ch)$를 식 (3)처럼 가입자 관리자 시스템의 개인키로 서명하여 가입자에게 전달한다.

SMS → 가입자 : $SK_{SK_{SMS}}(ID_U,\ H(SI,\ R_U \oplus Ch))$ (3)

3.2.2 상호인증 과정

상호인증 과정은 IPTV 서비스를 제공받기를 원하는 사용자가 스마트카드를 수신기에 부착한 후 사용자가 서비스를 제공받을 수 있는지를 체크하는 과정으로써 이 과정은 사용자가 보유하고 있는 스마트 카드와 수신기사이의 상호 인증과정을 통해 이루어진다. 스마트카드와 수신기 사이의 세부적인 상호인증 과정 절차는 그림 6과 같다.

• 단계 1 : 스마트카드 사용 유·무 체크

가입자가 서비스 제공자로부터 서비스를 제공받기 원한다면 가입자의 스마트카드를 수신기에 부착한 후 스마트카드 인식자 ID_U와 패스워드 PW_U를 입력하여 스마트카드 사용 유·무를 확인한다. 스마트카드 인식자 ID_U와 패스워드 PW_U를 입력한 스마트카드는 IP와 H(ID_U, PW_U)가 일치하는지를 체크한다. 만약 입력된 값이 일치하지 않으면 사용자 서비스 요청을 거절하고 입력된 값이 올바르면 스마트카드는 512 비트 크기를 가지는 두 개의 랜덤 수 $R1_S$와 $R2_S$를 생성한 후 $R1_S$을 이용하여 식 (4)~식 (8)를 계산한다.

$$\text{Compute } R_S' = H(h(ID_U \oplus ID_S),\ R_S) \quad (4)$$

$$\alpha = SI \oplus IP \quad (5)$$

$$\beta = \alpha \oplus R1_S \quad (6)$$

$$\gamma = R1_S \oplus h(ID_U,\ ID_S,\ \beta) \quad (7)$$

$$\delta = ID_U \oplus R_S' \quad (8)$$

• 단계 2 : 수신기(STB) ← 스마트카드

식 (4)~식 (8)의 과정을 통해 β, γ, δ를 계산한 스마트카드는 식 (9)처럼 STB의 개인키로 서명된 스마트카드의 인증 정보 요청 정보 $E_{PK_{STB}}(\beta,\ \gamma,\ \delta)$를 STB에게 전달한다.

수신기(STB) ← 스마트카드 : $E_{PK_{STB}}(\beta,\ \gamma,\ \delta)$ (9)

• 단계 3 : 수신기

스마트카드의 인증요청 정보 $E_{PK_{STB}}(\beta,\ \gamma,\ \delta)$를 수신한 수신기는 복호화를 과정을 통해 $R1_S$과 R_S'를 계산한다. $R1_S$는 사용자의 서비스 요청이 올바르게 검증된 것을 보장하기 위해 사용되며 R_S'는 사용자의 서비스 요청이 있을 경우 수신기의 ID를 생성하여 사용자가 수신기를 판별하기 위해 사용된다.

$$\text{Compute } R1_S = \gamma \oplus h(ID_S) \text{ and } R_S' = H(h(ID_S), R1_S) \quad (10)$$

수신기는 식 (11) 과정을 통해 스마트카드 인식자 ID_U를 획득한 후 전달된 ID_S를 비교 검증한다.

$$\text{Compute } ID_U = \delta \oplus R_S' \text{ and compare } ID_S \quad (11)$$

수신기는 식 (11)에서 추출된 ID_S의 비교 검증이 끝난 후 식 (12) 과정을 통해 α를 계산한다. 수신기는 가입자의 서비스 요청을 위해 가입자 관리자 시스템에 등록된 $H(ID_U,\ X_S)$와 식 (12)과정을 통해 추출된 $H(ID_U,\ X_S)$를 검증한다. 검증이 올바르게 종료되지 않으면 가입자의 서비스 요청은 거절된다.

$$\text{Compute } \alpha = \beta \oplus R1_S \quad (12)$$

• 단계 4 : 수신기(STB) → 스마트카드

서비스 요청이 승낙된 후 수신기는 $R2_S$를 이용하여 식 (13)을 계산한다. 수신기는 T_1와 T_2를 계산한 후 식 (14)처럼 스마트카드의 개인키로 서명된 SK_{SK_U}로 T_1와

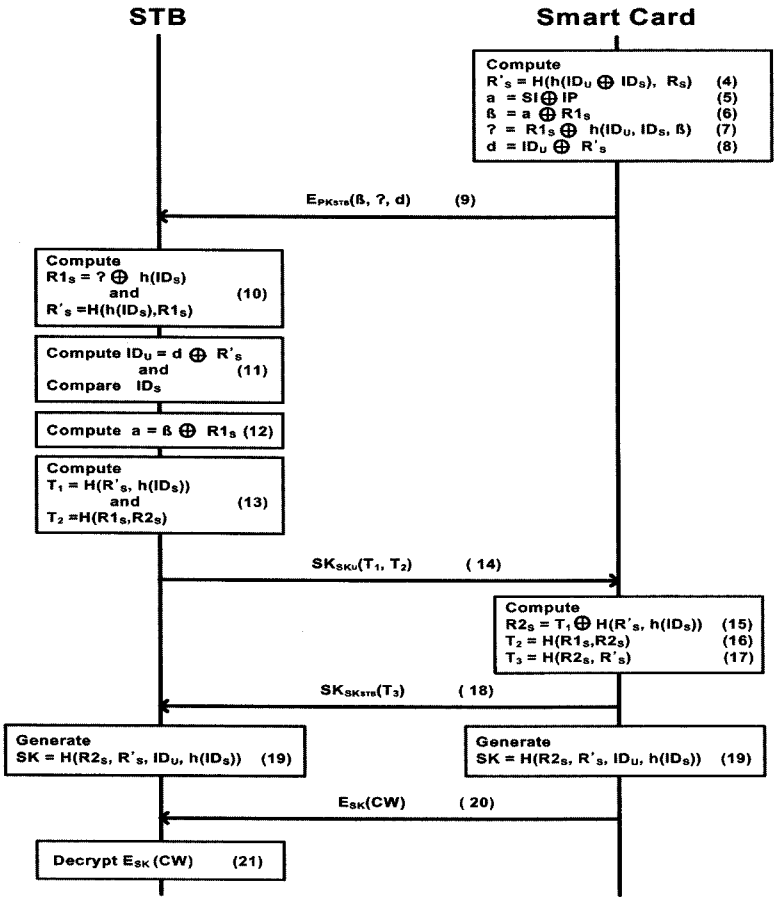


그림 6 상호인증 처리절차

T_2 를 암호화하여 스마트카드에게 전달한다.

$$\text{Compute } T_1 = H(R_S', h(ID_S)) \oplus R2_S \text{ and } T_2 = H(R1_S, R2_S) \quad (13)$$

$$\text{수신기(STB)} \rightarrow \text{스마트카드} : SK_{SK_U}(T_1, T_2) \quad (14)$$

• 단계 5 : 스마트카드

스마트 카드는 수신기에게 전달받은 T_1 과 T_2 를 복호화한 후 식 (15)를 통해 $R2_S$ 를 계산하고 수신된 T_2와 $H(R1_S, R2_S)$을 식 (16)처럼 비교 검증한다. 만일 식 (16) 과정에서 T_2와 $H(R_S, R2_S)$이 일치하지 않으면 서비스는 종료된다. 식 (16)의 과정이 정상적으로 동작되면 스마트카드는 식 (17) 과정을 통해 T_3를 계산한 후 계산된 결과값 T_3를 수신기의 개인키로 서명된 $SK_{SK_{STB}}$로 암호화하여 식 (18)처럼 수신기에게 전달한다.

$$\text{Compute } R2_S = T_1 \oplus H(R_S', h(ID_S)) \quad (15)$$

$$\text{Compare } T_2 = H(R_S, R2_S) \quad (16)$$

$$\text{Compute } T_3 = H(R2_S, R_S') \quad (17)$$

$$\text{수신기(STB)} \leftarrow \text{스마트카드} : SK_{SK_{STB}}(T_3) \quad (18)$$

• 단계 6 : 수신기

수신기는 스마트카드에게 전달받은 $SK_{SK_{STB}}(T_3)$를 복호화한 후 복호화된 T_3와 수신기에 저장되어 있는 $H(R2_S, R_S')$를 비교 검증한 후 두 값이 동일하면 수신기는 스마트카드에게 서비스를 승인하도록 한다.

• 단계 7 : 세션키 SK 생성

수신기와 스마트카드가 서로 상호인증을 모두 끝마치고 나면 수신기와 스마트카드는 식 (19)와 같은 과정을 통해 세션키 SK를 생성할 수 있다. 스마트카드는 생성된 세션키 SK를 이용하여 제어 문자(Control Word, CW)를 암호화하여 수신기에게 전달한 후 수신기는 전달된 $E_{SK}(CW)$를 식 (21)처럼 세션키 SK를 이용하여 복호화 한다.

$$\text{Generate } SK = H(R2_S, R_S', ID_U, h(ID_S)) \quad (19)$$

수신기(STB) ← 스마트카드 : $E_{SK}(CW)$ (20)

Decrypt $E_{SK}(CW)$ (21)

3.2.3 유지보수 과정

가입자는 서비스를 제공받는 과정 중에 등록과정에서 입력한 스마트카드의 패스워드 PW_U 를 변경할 수 있다. 유지보수 과정은 서비스를 제공받는 가입자가 임의 시간에 네트워크 그룹을 이탈할 경우 자신의 스마트카드의 패스워드를 변경하는 과정으로써 스마트카드의 패스워드를 변경하는 과정은 식 (22)와 같다. 식 (22)에서 스마트카드는 IP'와 SI'를 계산한 후 스마트카드에 저장되어 있는 IP와 SI를 IP'와 SI'로 변경한다.

Compute $IP' = H(ID_U, PW')$ and SI'

$= IP' \oplus SI \oplus IP$ (22)

4. 평 가

4.1 실험환경

제안 프로토콜은 실험의 객관성을 유지하기 위하여 IPTV 모델에서 사용하는 그림 7의 실험 환경을 구축하여 표 2의 성능 평가 변수를 적용하여 시뮬레이션을 수행하였다. 실험에서 설정된 권한 취소 가입자 수는 1,000,000명이며, 60분동안 권한 취소 리스트 갱신주기에 대한 실험을 수행한다. 그리고 각 가입자 관리 시스템의 가입자 인식 시간은 0.1~1.5초로 설정하고 권한 취소 리스트 레코드 크기를 20비트 크기로 전송하도록 실험한다.

표 2 용어 정의

용어	정의
권한 취소 가입자 수	1,000,000
권한 취소 리스트 갱신주기	60분
가입자 인식 시간	0.1~15초
권한 키 재전송 시간	15초
권한취소리스트 레코드 크기	20 bit
지불 시간 기간이 남은 가입자 비율	1%, 5%, 10%, 15%, 20%

4.2 성능평가

제안 프로토콜의 성능평가는 IPTV 보안 기법 중 가장 대표적인 기법인 Lee 기법, Tu etal. 기법, Huang et al. 기법 등을 IPTV 서비스에 적용하였을 경우에 권한 취소 가입자 수 증가에 따른 데이터 암호에서 발생하는 오버헤드와 가입자 관리 시스템과 가입자 사이의 통신 오버헤드 변화를 평가하기위해 암호 오버헤드와 통신 오버헤드에 대해서 평가한다.

4.2.1 암호 오버헤드

그림 8은 가입자 수에 따른 키 암호 오버헤드를 Lee 기법, Tu etal. 기법, Huang et al. 기법과 제안 프로토콜을 비교 평가하고 있다. 그림 8에서 제안 프로토콜은 가입자수가 증가하더라도 Lee 기법, Tu etal. 기법, Huang et al. 기법보다 암호 오버헤드가 낮게 평가되었다. 이 같은 결과는 제안 프로토콜에서 데이터를 암호화할 때 서명방식의 해쉬 함수를 사용하여 다른 기법에서 사용하는 공개키 기반의 암호 알고리즘에 비해 낮은 암호 오버헤드를 발생시켰기 때문이다. 제안 프로토콜은 가입자 수에 따른 키 암호 오버헤드를 평가한 결과 그림 8처럼 제안 프로토콜이 Lee 기법, Tu etal. 기법, Huang et al. 기법에 비해 평균 8.9%, 12.3%, 16%의 낮은 오버헤드를 갖는 결과를 얻었다.

그림 9는 수신자격을 가지는 가입자 수의 증가에 따른 권한 키의 키 암호 처리 시간을 Lee 기법, Tu etal. 기법, Huang et al. 기법과 함께 제안 프로토콜을 평가하고 있다. 그림 9의 제안 프로토콜은 다른 기법에서 사용하는 공개키 암호방식을 사용하지 않고 서명방식의 해쉬함수를 사용하면서 등록과정에서 등록된 스마트카

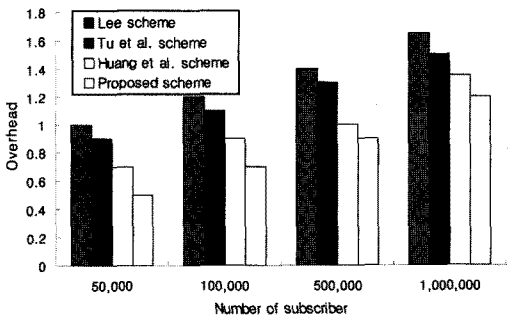


그림 8 가입자 수에 따른 키 암호 오버헤드

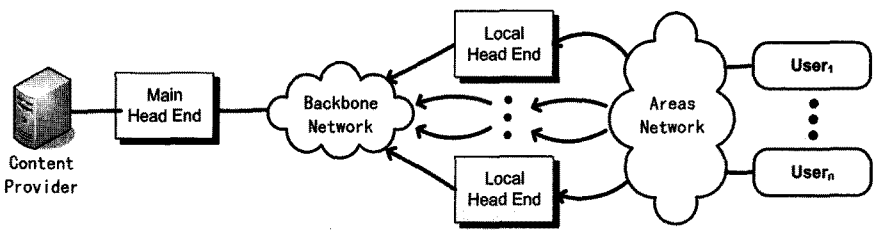


그림 7 실험 환경

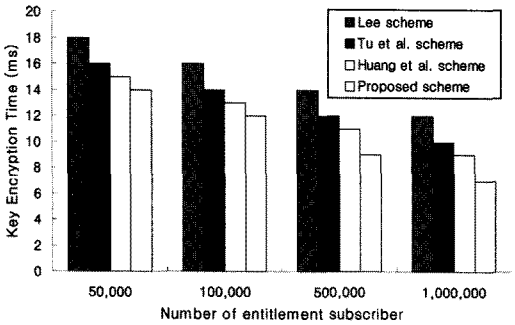


그림 9 수신자격 가입자의 키 암호 처리 시간

드의 인식자와 패스워드를 인증과정과 유지보수과정에 그대로 적용하였기 때문에 가입자 수가 급격히 증가하더라도 키 암호 처리 시간의 증가 비율이 Lee 기법, Tu etal. 기법, Huang et al. 기법에 비해 낮게 나타났다. 특히, 제안 프로토콜의 키 암호 처리 시간은 Lee 기법, Tu etal. 기법, Huang et al. 기법과 비교하여 평균 4%, 6.9% 8.5%의 시간을 단축시켰다.

4.2.2 통신 오버헤드

제안 프로토콜에서 가입자 관리 시스템은 가입자가 주기적으로 서비스를 수신받을 수 있는지를 판별하기 위해 가입자는 가입자 관리 시스템에게 서비스 채널에 대한 권한 취소 리스트를 주기적으로 보내어 권한 취소에 대한 정보를 업데이트한다. 이 때 서비스를 제공받는 사용자 수가 증가할수록 가입자 관리 시스템과 가입자 사이에는 통신 오버헤드가 증가하게 된다.

그림 10은 Lee 기법, Tu etal. 기법, Huang et al. 기법과 제안 프로토콜을 권한 취소 리스트의 마지막 갱신 주기(Authorization revocation list update period, AUP) 동안에 발생되는 평균 비트율을 비교하고 있다. 그림 10은 가입자의 다양한 권한 취소 리스트의 갱신 주기로 인해서 가입자 관리 시스템이 전체 가입자 중 마지막 10%의 가입자로부터 권한 취소 리스트의 갱신

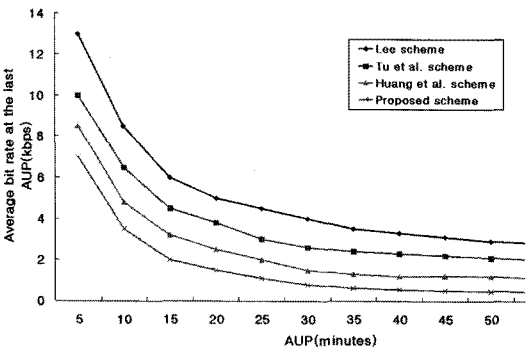


그림 10 AUP에 따른 평균 비율을 계산한 통신 오버헤드

주기에 따른 평균 비트율을 계산하였다. 그림 10처럼 평균 비트율에 따른 가입자 관리 시스템과 가입자 사이의 통신 오버헤드는 가입자의 권한 취소 리스트가 커질수록 서비스 요금 지불시간 동안에 전송되는 최대 전송 채널의 소비를 증가하는 결과가 발생된다. 이 같은 결과는 그림 10처럼 사용자의 수신자격(Entitlement)이 높아질수록 서비스 요금 지불시간 동안에 처리되는 권한 취소 처리율이 낮아지기 때문이다. 제안 프로토콜은 Lee 기법, Tu etal. 기법, Huang et al. 기법에 비해 권한 취소 리스트의 갱신 주기가 짧은 경우 5% 8% 11%의 낮은 처리율을 보였으며 권한 취소 리스트의 갱신 주기가 길어질수록 0.8%, 1% 1.2%의 처리율을 보였다.

4.3 보안평가

제안 프로토콜의 상호 인증과정을 통해 생성된 세션키 SK는 제안 프로토콜에서 사용되는 값들 중 $R2_S$, $R_S^{'}$, ID_U, $h(ID_S)$를 연접하여 one-way 해쉬 함수에 적용시켜 생성된 값이다. 해쉬함수에 적용한 $R2_S$, $R_S^{'}$, ID_U, $h(ID_S)$들은 스마트카드와 수신기만이 알고 있어 제3자는 알 수 없는 값들이다. 인증과정에서 생성한 $R_S^{'}$는 각 가입자가 서비스를 요청할 때 사용자가 소유하고 있는 스마트카드와 수신기 사이에 사용하는 세션키의 시드 정보를 나타내며 제3자가 시도하는 악의적인 공격 중 replay 공격과 impersonation 공격을 예방하는 역할을 수행한다. 제안 프로토콜에서는 매 통신마다 서로 다른 세션키 SK가 생성되며 생성된 세션키 SK는 EMM의 제어 문자 CW를 암호화하여 전달하기 때문에 제어 문자 CW를 얻으려는 평문(plaintext) 공격의 암호 알고리즘 공격을 예방하고 있다.

제안 프로토콜은 스마트카드에서 발생하기 쉬운 cloning 문제를 해결하기 위해 수신기의 인식자 ID_S를 해쉬함수 $h(\cdot)$를 통해 $h(ID_S)$를 생성한다. 제안 프로토콜에서 생성되는 수신기의 인식자는 수신기마다 서로 다른 인식자 ID_{S_i}를 사용하기 때문에 제3자가 복제된 자신의 스마트카드를 다른 수신기에 부착하여 사용할 경우 수신기가 스마트카드를 인식하지 못하도록 하고 있다. 이러한 방법은 스마트카드에 등록된 수신기의 인식자와 수신기가 해쉬함수에 의해 생성된 인식자 값이 서로 달라 cloning 문제를 예방하고 있다. 따라서, 복제된 스마트카드를 사용하는 사용자는 제안 프로토콜의 해쉬함수에 의해 생성되는 인식자를 판별하기 어려워 제3자가 자신의 스마트카드를 가지고 다른 수신기를 사용하는 것은 사실상 불가능하다.

제안된 프로토콜은 cloning 문제이외에 McCormac Hack 문제 또한 예방하고 있다. McCormac 문제는 제3

자가 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 센션키 SK는 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.

5. 결 론

이 논문에서는 IPTV 서비스를 제공받기를 원하는 사용자의 스마트카드와 수신기 사이에 서명기반의 해쉬함수를 이용한 상호 인증 프로토콜을 제안하였다. 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 SK를 상호 인증 과정에서 생성하였다. 세션키 SK는 $R2_S$, $R_S^{'}$, ID_U, $h(ID_S)$를 연접하여 one-way 해쉬 함수에 적용시켜 EMM을 암호화하도록 하여 제3자가 인식자를 판별하지 못하도록 하여 서비스를 이용할 수 없도록 하였다. 성능 평가 중 암호 오버헤드의 평가에서는 제안 프로토콜이 Lee 기법, Tu etal. 기법, Huang et al. 기법보다 평균 8.9%, 12.3%, 16%의 낮은 오버헤드 결과를 얻었으며 통신 오버헤드의 평가에서는 권한 취소 리스트의 갱신 주기가 짧은 경우와 긴 경우로 나누어 평가한 결과 짧은 경우에는 Lee 기법, Tu etal. 기법, Huang et al. 기법보다 5% 8% 11% 낮은 처리율을 보였으며 긴 경우에는 0.8%, 1% 1.2%의 낮은 처리율을 얻을 수 있었다. 향후 연구에서는 수신제한시스템을 기반으로 DRM의 기능을 결합하여 가입자의 권한 접근 및 레벨을 부여한 인증 메커니즘을 연구 수행할 계획이다.

참 고 문 헌

[1] M. Pagani, "Multimedia and Interactive Digital TV - Managing the Opportunities Created by Digital Convergence," IRM Press, 2003.

[2] 우제학, 노창현, 이완복, "IPTV 콘텐츠 보호 기술의 비교 - CAS와 DRM 중심으로", *한국콘텐츠학회논문지*, vol.6, no.8, pp.157-164, 2006.

[3] J. W. Lee, "Key distribution and management for conditional access system on DBS," *in Proc. Int. Conf. Cryptology and Information Security*, pp. 82-86, 1996.

[4] 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.

[5] Y. L. Huang and S. Shi도, "Efficient key distribution scheme for secure media delivery in pay-TV systems," *IEEE Trans. Multimedia*, vol.6, no.5, pp.760-769, Oct. 2004.

[6] S. Zhu and S. Setia, "LEAP+ : Efficient security mechanisms for large-scale distributed sensor networks," *ACM Trans. on Sensor Networks*, 2(4), pp.500-528, 2006 (the journal version of CCS'03 paper)

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

[8] A. M. Eskicioglu, "Protecting Intellectual Property in Digital Multimedia Networks," *IEEE Computer*, vol.36, pp.39-45, 2003.

[9] B. Rosenblatt, B. Trippe, and S. Mooney, "Digital Rights Management-Business and Technology," M&T Books, 2002.

[10] B. Liu, W. Zhang, and T. Jiang, "A scalable key distribution scheme for conditional access system in digital pay-TV system," *IEEE Trans. Consumer Electron.*, vol.50, no.2, pp.632-637, May 2004.

[11] W. Kanjanarin and T. Amornraksa, "Scrambling and key distribution scheme for digital television," *in Proc. 9th IEEE Int. Conf. Networks*, pp. 140-145, 2001.

[12] A. Fiat and M. Naor, "Broadcast encryption," in *Advances in Cryptology - CRYPTO'93*, vol.773, pp.480-491, 1994.

[13] D. Naor, M. Naor and J. B. Lotspiech, "Revocation and tracing schemes for stateless receivers," *in Advances in Cryptology - CRYPTO'01*, vol.2139, LNCS, pp.41-62, 2001.

[14] D. Halevy and A. Shamir, "The LSD broadcast encryption scheme," *in Proc. CRYPTO 2002*, vol.2442, LNCS, pp.47-60, 2002.

[15] R. Canetti, J. Garey, G. Itkis, D. Micciancio, M. Naor, and B. Pinkas, "Multicast security: A taxonomy and some efficient constructions," *in Proc. IEEE Infocomm'99*, vol.2, pp.708-716, Mar. 1999.

[16] D. Wallner, E. Harder, and R. Agee, "Key Management for Multicast: Issues and Architectures IETF," *RFC 2627*, 1999.

[17] A. T. Sherman and D. A. McGrew, "Key establishment in large dynamic groups using one-way functions trees," *IEEE Trans. Softw. Eng.*, vol.29,

no.5, pp. 444-458, May 2003.
[18] H. Harney and E. Harder, "Logical Key Hierarchy Protocol," IETF 1999[Online]. Availaber: Internet Draft, draft-harney-sparta-lkhp-\sec-00.txt
[19] S. Emmanuel and M. S. Kankanhalli, "A Digital rights management scheme for broadcast video," *multimedia Syst. J.*, vol.8, no.6, pp.444-458, 2003.

정 윤 수

1998년 2월 청주대학교 전자계산학과 학사. 2000년 2월 충북대학교 대학원 전자계산학과 석사. 2008년 2월 충북대학교 대학원 전자계산학과 박사. 2009년 9월~현재 한남대학교 산업기술연구소 전임연구원. 관심분야는 정보보호, 멀티미디어, 네트워크 보안, 이동통신, 유·무선 통신, 암호이론

김 용 태

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. 관심분야는 멀티미디어, 모바일 웹서비스, Real-time Multimedia Communication

정 윤 성

1995년 2월 Seowon University, Department of Applied Statistics, BS, Applied Statsitics. 1999년 2월 Korea University, Department of Statistics, MS, Mathematical Statistics. 2003년 5월 Texas A&M University, Department of Statistics, MS, Statistics. 2009년 8월 Kansas State University, Department of Statistics, Ph.D., Statistics. 2009년 9월~현재 Research Assistant Professor/Statistician School of Agriculture, Research, Extension, and Applied Sciences 1000 ASU Drive #690 Alcorn State University, 관심분야는 Linear model, Design of Experiments, Bioinformatics, Computer network, Computer Programming

박 길 철

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. 관심분야는 multimedia and mobile communication, network security

이 상 호

1976년 2월 숭실대학교 전자계산학과 학사. 1981년 2월 숭실대학교 전자계산학과 석사. 1989년 2월 숭실대학교 전자계산학과 박사. 1981년 3월~현재 충북대학교 전기전자 컴퓨터공학부 교수. 관심분야는 네트워크보안, Protocol Engineering, Network Management