IPTV 환경에서 가입자의 인증 상태정보를 이용한 인증 보안 모델 설계

정회원 정 윤 수*, 정 윤 성**, 김 용 태***°, 박 길 철***, 종신회원 이 상 호****

A Security Model Analysis Adopt to Authentication State Information in IPTV Environment

Yoon-Su Jeong*, Yoon-Sung Jung**, Yong-Tae Kim***°,
Gil-Cheol Park***, *Regular Members,* Sang-Ho Lee**** *Lifelong Member*

요 약

최근 통신망이 광대역화 됨에 따라 다양한 양방향 TV 서비스를 제공하는 IPTV(Internet Protocol Television) 서비스가 증가하고 있다. 그러나 IPTV의 셋톱박스와 스마트 카드 간에 전달되는 데이터가 셋톱박스 내에서 대부분 전달되기 때문에 맥코맥 핵 공격을 이용하여 불법적으로 콘텐츠 내용에 접근하여 합법적인 권한을 획득하는 불법 사용자를 완벽하게 예방할 수 없다. 이 논문에서는 스마트카드로부터 셋톱박스까지 연결된 데이터 라인을 불법 사용자가 동일 기종의 다른 셋톱박스를 이용하여 불법적으로 IPTV 서비스의 접근 허가를 받으려는 맥코맥 핵 공격(McComac Hack Attack)을 예방하기 위한 셋톱박스 접근 보안 모델을 제안한다. 제안 모델은 사전에 셋톱박스에 사용가능한 스마트 카드의 상태정보를 등록하여 불법적으로 접근허가를 승인받으려는 사용자를 인증서버에서 점검하여 점검 결과를 셋톱박스에 통보하여 불법 사용자를 사전에 예방한다. 특히, 제안 모델은 Pseudo 랜덤 함수를 통해 생성된 임의의 난수와 비밀값을 통해 이웃 링크 설립과 상호 인증 과정에 사용되는 공개키에 적용하여 셋탑박스에 대한 보안을 강화하고 있다.

Key Words : IPTV 서비스(IPTV Service), 사용자 인증(User Authentication), 보안(Security)

ABSTRACT

Now a days, as a communications network is being broadband, IPTV(Internet Protocol Television) service which provides various two-way TV service is increasing. But as the data which is transmitted between IPTV set-top box and smart card is almost transmitted to set-top box, the illegal user who gets legal authority by approaching to the context of contents illegally using McComac Hack Attack is not prevented perfectly. In this paper, set-top box access security model is proposed which is for the protection from McComac Hack Attack that tries to get permission for access of IPTV service illegally making data line which is connected from smart card to set-top box by using same kind of other set-top box which illegal user uses. The proposed model reports

※ 이 논문은 2009년 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(2009-0074117)
* 충북대학교 전자계산학과 네트워크보안 연구실(bukmunro@gmail.com)
** Department of Advanced Technologies, Alcorn State University(yjung@alcorn.edu)
*** 한남대학교 멀티미디어공학부 강의전담 교수(ky7762@hannam.ac.kr, gcpark@hnu.kr), (°:교신저자)
**** 충북대학교 전기전자컴퓨터공학부 교수(shlee@chungbuk.ac.kr)
논문번호 : KICS2009-10-478, 접수일자 : 2009년 10월 23일, 최종논문접수일자 : 2010년 3월 15일

the result of test which tests the user who wants to get permission illegally by registration the information of a condition of smart card which is usable in set-top box in certification server so that it prevents illegal user. Specially, the proposed model strengthen the security about set-top box by adapting public key which is used for establishing neighbor link and inter-certification process though secret value and random number which is created by Pseudo random function.

Ⅰ. 서 론

최근 방송 콘텐츠가 디지털화되면서 통신망이 광대역화 됨에 따라 다양한 양방향 TV 서비스를 제공하는 IPTV(Internet Protocol Television) 서비스가 증가하고 있다. IPTV 서비스는 초고속 인터넷을 이용하여 정보 서비스, 동영상 콘텐츠 및 방송 등을 제공한다[1].

IPTV를 가정에서 이용하기 위해서는 텔레비전 수상기와 셋톱박스, 인터넷 회선이 연결되어 있으면 되기 때문에 텔레비전을 켜듯이 전원만 넣으면 이용할 수 있다. 컴퓨터에 익숙하지 않은 사람이라도 리모콘을 이용하여 간단하게 인터넷 검색은 물론 영화 감상, 홈쇼핑, 홈뱅킹, 온라인 게임, MP3 등 인터넷이 제공하는 다양한 콘텐츠 및 부가 서비스를 제공받을 수 있다.

인터넷을 통한 기존 서버-클라이언트 인증 기법에서는 둘 사이에 주고받는 데이터가 인터넷을 통하여 전달되기 때문에 인터넷 상의 데이터를 가로채서 변형하는 공격에 취약하다[2],[3]. 반면, IPTV의 셋톱박스와 스마트 카드 간의 인증에서는 둘 사이에 전달되는 데이터가 셋톱박스 내에서 전달되기 때문에 맥코맥 핵 공격과 스마트카드 복제 공격에 취약하다. 특히, IPTV에서는 멀티캐스트 방식을 이용하여 방송 콘텐츠를 여러 사용자들이 안전하게 받아 볼 수 있도록 하기 위해서 셋톱박스내에 가입자 인증 판별 기능이 필요하다.

이 논문에서는 스마트카드로부터 셋톱박스까지 연결된 데이터 라인을 불법 사용자가 동일 기종의 다른 셋톱박스를 이용하여 불법적으로 IPTV 접근 허가를 받으려는 맥코맥 핵 공격(McComac Hack Attack)과 같은 공격을 예방하기 위한 셋톱박스 접근 보안 모델을 제안한다. 제안 모델은 사전에 셋톱박스에 사용가능한 스마트 카드의 상태정보를 등록하여 불법적으로 접근허가를 승인받으려는 사용자를 인증서버에서 점검하여 점검 결과를 셋톱박스에 통보하여 불법 사용자를 사전에 예방한다. 특히, 제안 모델은 Pseudo 랜덤 함수를 통해 생성된 임의의 난수와 비밀값을 통해 트래픽 발생을 최소화 하면서 셋톱박스에 대한 보안을 강화하고 있다.

이 논문의 구성은 다음과 같다. 2장에서는 IPTV의 개념 및 보안에 대해서 분석한다. 3장에서는 불법적으로 IPTV 서비스에 대한 접근 허가를 시도하는 맥코맥 핵 공격을 예방하기 위한 셋톱박스 접근 보안 모델을 제시하고, 4장에서는 제안 모델을 네트워크 효율성, 통신 오버헤드, 서비스 지연등에 대해서 성능 평가한다. 마지막으로 5장에서는 이 논문의 결과를 요약하고 향후 연구에 대한 방향을 제시한다.

Ⅱ. 관련연구

2.1 IPTV 서비스

IPTV(Internet Protocol TV)는 초고속인터넷망을 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. IPTV 서비스를 제공하기 위해서는 플랫폼(HeadEnd), IP 네트워크, 단말장비 등과 함께 Triple Play의 서비스를 제공할 수 있는 장비가 필요하다. IPTV 서비스는 주문형 콘텐츠(VOD 등), 인터넷 검색, T-Commerce 서비스 및 이용자 요청에 따라 실시간으로 방송 프로그램을 전송하는 서비스 등에 사용된다.

2.2 IPTV 보안 요구사항

IPTV 환경에서는 셋톱박스와 스마트카드 간의 인증에서 둘 사이에 전달되는 데이터가 셋톱박스 내에서 전달되기 때문에 맥코맥 핵 공격과 스마트카드 보안 공격에 안전함을 보이는 것이 가장 중요한 보안 요구사항으로 인식되고 있다. 맥코맥 핵 공격은 스마트카드로부터 셋톱박스로 연결되는 데이터

라인을 같은 종류의 다른 셋톱박스로 전송하여 접근허가를 받으려는 공격을 의미하고 스마트 카드 복제 공격은 정당한 스마트카드를 복제하여 복제된 카드를 다른 셋톱박스에 넣어서 접근허가를 받으려는 공격을 의미한다. IPTV 보안과 관련하여 많은 연구자들은 무결성(Integrity), 보안(Security), 감사(Auditing), 프라이버시(Privacy), 부인방지(Non-reputation), 인증(Authentication), 기밀성(Confidentiality), 권한(Authorization), 면역(immunity), 이용성(Availability), 신원확인(Identification) 등의 보안 요소들에 대해 연구해왔다[1]-[3]. IPTV 보안과 관련하여 공격 유형에 따른 보안 범위는 표 1과 같다.

IPTV의 콘텐츠 불법 유출은 영화, 비디오, 방송 등을 이용하여 사용자에게 전송되는 과정 중에 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 사용해야 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.

표 1. 공격 유형과 보안 요소 분석

공격 유형	보안 요소	새로운 보안 요소
Interruption	액세스 제어	이용성
Inteception	액세스 제어, 통신 보안	권한
Modification	데이터 기밀성	무결성, 프라이버시
Fabrication	데이터 기밀성, 부인방지	프라이버시, 인증, 권한

Ⅲ. 인증 상태정보를 이용한 셋톱박스 접근 보안 모델

이 절에서는 사용자가 불법적으로 IPTV 서비스에 접근 허가를 부여받기 위해 스마트카드와 셋톱박스 사이를 연결하는 데이터 라인을 이용하여 같은 종류의 다른 셋톱박스로 사용자의 스마트 카드 정보를 전송하여 접근허가를 받으려는 맥코맥 핵 공격(McCormac Hack Attack)를 예방하기 위한 셋톱박스 접근 보안 모델을 제안한다. 제안 모델은 맥코맥 핵 공격을 예방하기 위해서 사용자가 셋톱박스로부터 인증을 요청할 경우 인증 상태정보를 생성하여 스마트카드와 셋톱박스의 메모리에 저장하여 불법적인 사용자가 접근허가를 사전에 차단한다. 특히, 제안 모델은 기존 IPTV 서비스에서 문제시되던 과도한 트래픽 발생을 막기 위해 인증과정에 해쉬 체인을 적용하여 인증 상태정보를 생성하고 인증 상태 정보를 암호화하기 위해 사용되는 키 정보는 사용자가 사전에 등록한 비밀키를 사용한다.

3.1 용어

제안 프로토콜에서 사용되는 용어는 표 2에서 정의하고 있다.

표 2. 파라미터

용 어	설 명
STB	Set-Top Box
CA	인증 권한 서버
Head-end	헤드 엔드
Cert	사용자가 IPTV 서비스를 제공받기 위해 사전에 등록을 통해 획득한 인증서
ASI	사용자의 인증 상태 정보(Authentication State Information)
PK_X / PR_X	X의 공개키/ 개인키
K_{Sh}	사용자와 셋톱박스 사이에 공유된 공유키
K_{S-A}	사용자가 사전에 인증서버에 등록한 비밀키
N_U	사용자가 임의로 생성한 랜덤 수
N_{STB}	STB가 임의로 생성한 랜덤 수

3.2 개요

그림 1은 스마트카드로부터 셋톱박스로 연결되는 데이터 라인을 같은 종류의 다른 셋톱박스로 전송하여 접근허가를 받으려는 사용자를 예방하기 위한 전체 구성도를 보여주고 있다. 그림 1은 기존 IPTV 네트워크 구조에서 사용자 중심의 서비스를 위해 자바카드를 부착한 사용자 장치를 사용한다. 자바카드를 부착한 사용자 장치는 자바카드를 내장하여 USIM과 IPTV 개별 사용자 정보를 저장하는 IDENTITY 애플릿을 포함하여 사용자가 직접 자신의 정보를 제어할 수 있다.

사용자는 IPTV 서비스를 지원받기 위해서 각 IPTV 장비에 설치된 IPTV 서비스 지원 프로그램을 통해 사용자 자신의 디바이스 인증과 사용자 인증을 수행한다. 이 때 STB의 인증 번호와 각 디바이스 인증번호를 통신측 디바이스 인증 서버의 데이터베이스에 저장, 갱신한 후에 IPTV 서비스를 사용할 경우 디바이스 인증 절차를 수행하지 않도록 한다. 컨텐츠 서비스는 통신 디바이스 인증 서버를 통해 STB의 인증번호를 이용하여 불법적인 사용자를 예방 한다. 통신 디바이스 인증 서버에서는 컨텐츠 서버에 서비스 요청을 한 후 컨텐츠 서버에서 사용자 인증을 거친 후 서비스를 지원한다.

IPTV 서비스를 요청하는 사용자는 사용자가 소유하고 있는 자바카드가 부착된 사용자 장치를 이용하여 사용자 인증 디바이스 인증 유무를 확인한 후 서비스를 제공받는다. 만약 디바이스 인증 및 사용자 인증이 정상적으로 수행되지 않는다면 사용자는 서비스를 제공받지 못한다.

3.3 셋톱박스 접근 제어

STB에 접근하는 사용자가 합법적인 사용자인지 불법적인 사용자인지를 판별하는 STB 접근 보안 모델은 그림 2와 같다. 그림 2에서 사용자는 스마트 카드로부터 STB로 연결되는 데이터 라인을 같은 종류의 다른 STB에 전송하여 접근허가를 받을 경우 다른 STB에 접근허가를 받았는지를 판별하여 합법적인 사용자가 아닐 경우 STB를 사용하지 못하도록 한다.

사용자가 동일 STB를 사용할 경우 사전 등록된 정보를 관리 서버에게 전달하여 CA에게 디바이스 인증 정보를 전달한다. 전달된 디바이스 인증 결과를 수신한 CA는 올바른 디바이스인지를 검토한 후 검토된 결과가 올바르면 컨텐츠 서버를 통해 CA에게 사용자 인증을 요청한다. 사용자가 동일 STB를 사용할 경우 사전에 등록된 정보를 이용하여 서비스를 빠르게 제공받는다.

사용자가 다른 STB를 사용할 경우 제안 모델은 기존 STB의 디바이스 정보와 사용자 정보가 저장되어 있는 CA에 현재 사용중인 디바이스 인증 정보와 사용자의 인증 정보를 CA에 전달하여 CA의 데이터베이스에 등록되어 있는 정보와 비교한다. 만일 데이터베이스에 등록된 정보와 일치하지 않는다면 사용자는 새로 접속한 STB의 정보를 관리 서버에게 전달하여 기존 사용자가 정보를 등록한 후 인증 서버에 등록된 새로운 정보에 대한 인증 정보를 생성한다. 기존 STB의 사용자 정보는 관리서버에게 전달하여 인증서버에 등록된 정보를 제거한다.

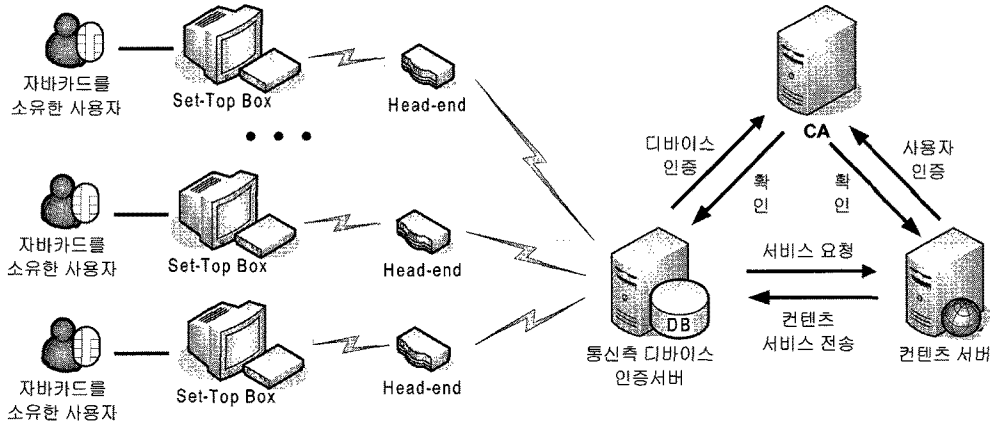


그림 1. 제안 모델의 전체 구성도

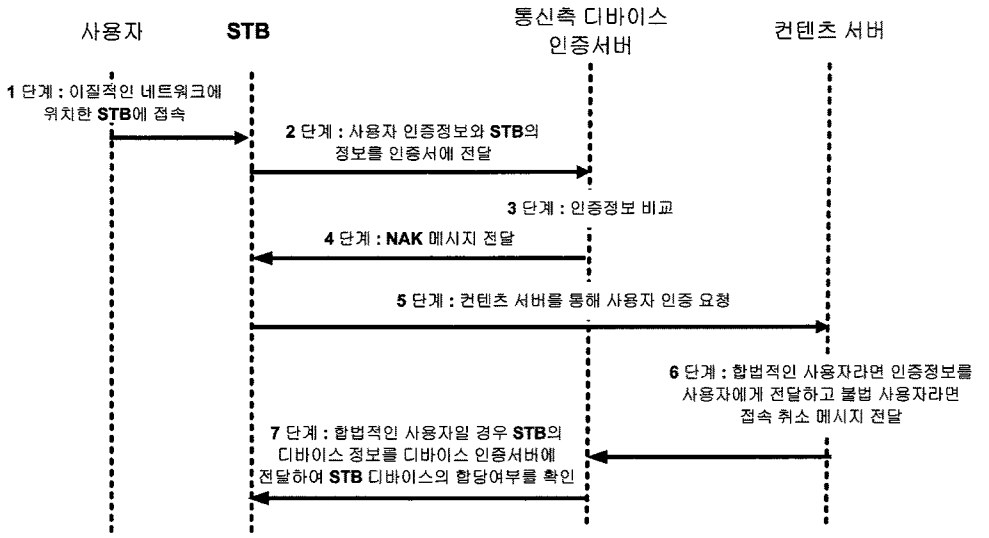


그림 2. 셋톱박스 접근 제어 과정

3.4 인증 상태정보

STB에서 사용될 스마트카드 정보를 관리서버(or 인증서버)로부터 정보를 확인한 STB는 스마트카드의 접속 승인을 수행한다. 사용자는 STB를 사용하기 위해서 사전에 STB를 관리서버에 등록한다. 사용자와 STB가 관리서버에 사전에 등록되었는지를 확인 한 후 정상 등록되었으면 서비스를 정상적으로 제공한다. 만약 STB가 변경된다면 변경된 STB의 인증이 수행되어야 하며 만약 STB의 인증이 수행되지 않는다면 서비스를 제공받을 수 없다.

사용자는 그림 3과 같이 2바이트(16비트)의 인증 패킷 정보를 서비스 요청 메시지와 함께 디바이스 인증서버와 컨텐츠 서버에 전달하여 서비스 승인/거절 메시지를 전달받게 된다.

그림 3의 인증 패킷 정보는 2비트의 인증상태, 1비트의 STB 승인, 1비트의 서버 승인, 4비트의 사용자 인증번호, 8비트의 디바이스 Serial 번호 등으로 구성된다. 2비트의 인증상태 정보는 스마트카드로부터 STB로 데이터 라인의 접근허가 정보를 나타낸다. 예를 들어 인증 상태가 10과 01일 경우 인증서버에 등록된 사용자 정보를 키워드로 검색한 후 서버 승인 정보를 체크하여 체크 상태가 1인 경우 사전에 등록된 개인정보를 사용자에게 요청하여 올바른 사용자인지를 검토한다.

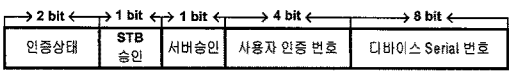


그림 3. 인증 패킷 정보

인증상태 정보(2 bit) :

비트	인증 상태 정보
11	인증 완료상태
10	다른 STB에서 인증 요청
01	동일 STB에서 인증 요청
00	인증 미완료 상태

STB 승인은 STB와 인증서버 사이에 스마트카드의 정보가 올바른지를 판단하는 정보로 1비트를 사용한다.

STB 승인(1 bit) :

비트	STB 승인 정보
0	미확인
1	STB와 인증서버 사이에 스마트카드의 정보가 올바른 경우

서버 승인은 서버가 사용자 정보를 수신받아 승인여부를 결정하는 정보로써 1비트를 사용한다.

서버 승인(1 bit) :

비트	서버 승인 정보
0	미승인
1	승인

사용자 인증번호와 디바이스 Serial 번호는 사전에 인증서버에 등록된 정보로써 사용자 인증번호는 사용자이외에는 알지 못하며 디바이스 Serial 번호는 유일한 번호를 가진다.

3.5 해쉬 체인을 이용한 사용자 인증

제안 모델은 셋톱박스에서 Pseudo 랜덤 함수와 임의로 생성한 난수를 이용하여 인증서버에 저장된 사용자 정보와 비교분석 과정을 수행한다. 이 때 전달되는 정보의 안전성을 셋톱박스가 보장하기 위해 공개키 알고리즘을 사용한다.

제안 모델에서는 사용자와 셋톱박스 사이에 서로 사전에 동의된 공유키 K_{Sh}을 공유한다고 가정한다. 공유키 K_{Sh}을 이용하여 사용자는 셋톱박스에게 사용자 정보(난수 N_U, 인증서 $Cert$)를 포함한 식 1를 셋톱박스에게 보낸다.

$$E_{PK_{STB}}(N_U),\ MAC_{K_{Sh}}(N_A,\ Cert) \qquad (1)$$

셋톱박스는 자신이 생성한 난수 N_{STB}와 인증 상태 정보 ASI(Authentication State Information)를 사용자 정보와 함께 인증서버에게 전달하여 인증서버의 승인정보를 수신받는다. 인증서버에게 전달되는 정보는 사용자가 IPTV 서비스를 제공받기 위해 사전에 인증 서버에 등록한 사용자의 비밀키 K_{S-A}와 랜덤수(N_U, N_{STB})를 one-way 해쉬 함수에 적용한다.

$$E_{PK_{CA}}(N_U,\ N_{STB}),\ h(MAC_{K_{S-A}}(N_U,\ N_{STB},\ ASI),\ Cert) \qquad (2)$$

인증서버는 데이터베이스에 저장된 사용자의 인증 상태정보를 확인 후 인증 상태 정보 ASI를 셋톱박스에게 전달함으로써 셋톱박스의 사용자 인증 상태 정보 ASI를 갱신한다. 셋톱박스는 갱신된 사용자 인증 상태 정보ASI 를 기반으로 사용자의 서비스 요청 상태를 체크하게 된다. 만약 사용자의 서비스 요구와 셋톱박스의 사용자 인증 상태 정보가 맞지 않을 경우 사용자의 서비스 요청을 무시한다.

Ⅳ. 평 가

이 절에서는 IPTV 환경에서 제공되고 있는 브로드캐스트 서비스 타입(Live Streaming과 Video-On-Demand)을 제안 모델에 적용하여 네트워크 효율성, 통신 오버헤드, 서비스 지연 등을 평가한다.

4.1 실험 환경

제안 시스템은 네트워크 효율성, 통신 오버헤드, 서비스 지연 등과 같은 평가 항목을 객관적으로 평가하기 위해서 [9],[10]에서 제시한 실험 환경을 OPNET 14을 통해 구축하였다. OPNET 14을 통해 구축된 실험 모델은 그림 4와 같고 실험 파라미터는 표 2와 같다.

4.2 성능평가

제안 기법과 기존 기법의 객관적인 성능 평가를 도출하기 위해 실험에서는 [10]의 평가항목을 이용하였으며 OPNet 14을 이용하여 네트워크 효율성, 오버헤드, 서비스 지연을 평가하고 있다. 표 3은 [10]처럼 제안 기법과 기존 기법[3]-[8]을 10가지 항목(보안, 사용자 편리성, 확장성, 실용 가능성, 비용 등)으로 비교분석 하고 있다. 표 3에서 패스워드 기

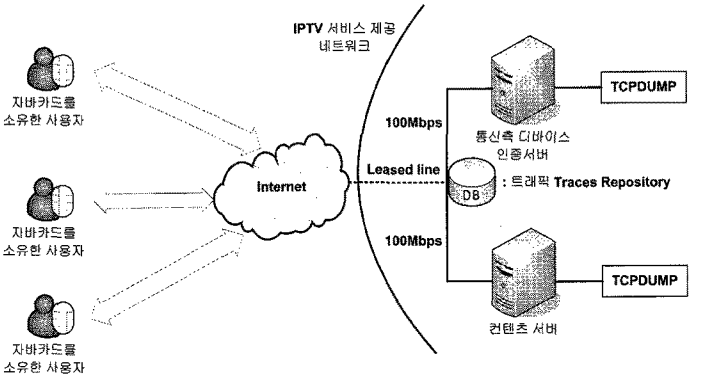


그림 4. 실험 환경

표 3. 실험 파라미터

용 어	설 명
사용자 수	20
시험시간	6시간
CPU	펜티엄 4
RAM	512 M
운영 환경	Windows XP SP3
시뮬레이터	OPNET 14

반 시스템[4]은 STB 프로그램에 개인 정보를 직접 입력하여 사용자 요구에 의해 제한된 개인 정보와 낮은 이용율을 가지지만 소프트웨어 수행에 의존하기 때문에 이점이 있다. STB에 의해 관리되는 사용자 정보를 보안 공격에 안전성을 강화하여야 한다. 생체인식 기반 시스템[5]-[7]은 사용자의 생체 정보를 이용하여 IPTV 서비스를 제공받는 사용자의 보안 서비스를 제공하지만 사용자의 행위 기반에 의한 서비스되기 때문에 상호 인증 기능은 제공하지 못하는 단점이 있다. RFID 기반 시스템[8]은 패스워드 기반 시스템과 유사하며 낮은 비용, 휴대 사용, STB에 사용자 활동 정보의 자동 기록 등과 같은 인증 사용작용이 적용된다. 그러나 RFID 태그가 유실되었을 경우 인위적으로 RFID 태그를 사용하는 사용자를 인증할 수 있는 단점이 있다. 기존 기법과 비교하여 제안 기법은 특정 개인화된 서비스에 대한 개인 정보를 넓게 수집하고, STB의 하드웨어와 소프트웨어의 수정없이 인증 메커니즘을 제공한다. 암호 동작과 같은 계산 수행을 증가하는 계산 능력을 제공하는 자바 카드 기술을 이용하고 있으며 사용자가 편리하게 사용할 수 있는 휴대성이 높다.

그림 5는 자바카드를 소유한 사용자들이 시간대별 IPTV 서비스를 제공받을 경우 Live Streaming과 Video-on-Demand 서비스의 네트워크 효율성을 보여주고 있다. 그림 5의 결과처럼 Live streaming 서비스는 Video-on-Demand 서비스에 비해 실시간 방송을 사용자들에게 서비스하기 때문에 시간대별 네트워크 효율성이 Video-on-Demand 서비스에 비해 평균 37.2% 낮게 나타났다.

그림 6은 시간대별 Live Streaming과 Video-on-Demand 서비스의 오버헤드 변화를 보여주고 있다. Live Streaming 서비스는 사용자가 시간대별로 서비스 요청이 집중 되었을 경우(2시~5시,9시~12시)에 Video-on-Demand 서비스보다 오버헤드가 상승되었지만 Video-on-Demand 서비스는 Live Streaming 서비스와 달리 6시~8시, 13시 ~15시에 높은 오버헤드를 나타났다. 전체적으로 통신 오버헤드의 변화량이 Live Streaming 서비스보다 Video-on-Demand 서비스가 시간에 변화에 따른 통신 오버헤드가 일정하게 나타났다.

그림 7은 시간대별 IPTV 서비스의 지연 시간을 보여주고 있다. 실시간으로 IPTV 서비스를 사용자에게 제공하는 Live Streaming 서비스는 사용자의 서비스 요청 횟수가 Video-on-Demand 서비스보다 시간대별로 높아 서비스 지연이 심하게 발생한다. 반면 Video-on-Demand 서비스는 고정된 통신 대역폭을 사용하여 시간대별 서비스 지연의 차이가 거의 없이 일정하게 나타났다.

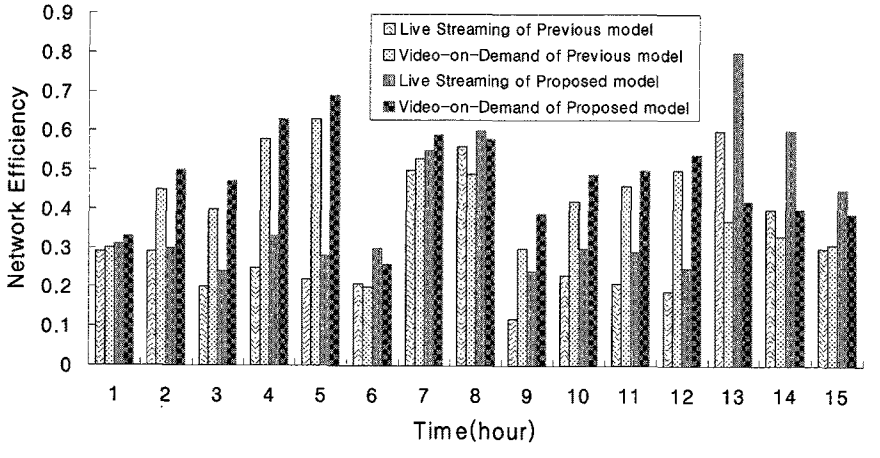


그림 5. 네트워크 효율성

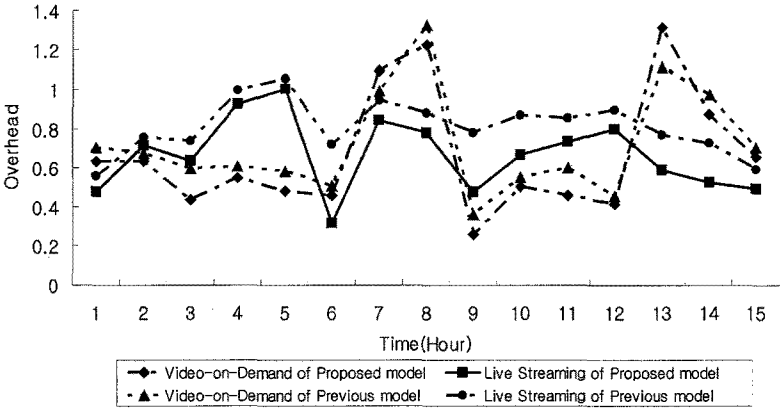


그림 6. 통신 오버헤드

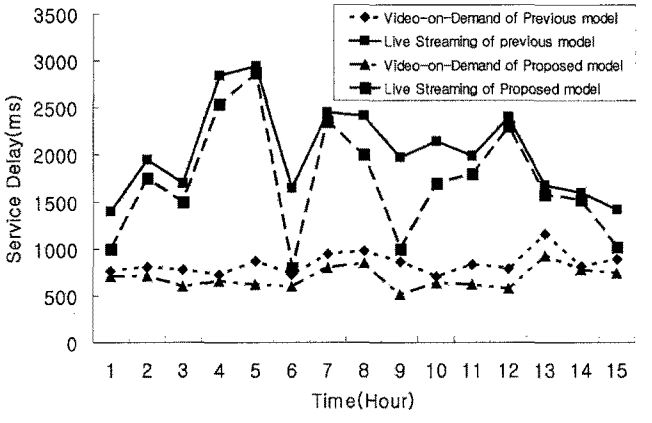


그림 7. 서비스 지연

V. 결 론

통신망과 인터넷이 발전함에 따라 IPTV 서비스가 점점 증가하고 있지만 불법적으로 IPTV 서비스를 제공받으려는 사용자 또한 증가하고 있다. 이 논문에서는 IPTV의 셋톱박스와 스마트 카드 간에 전달되는 데이터를 불법 사용자가 합법적으로 사용하는 맥코맥 핵 공격을 예방하기 위한 셋톱박스 접근 보안 모델을 제안하였다. 제안 모델은 제안 모델은 사전에 셋톱박스에 사용가능한 스마트 카드의 상태 정보를 등록하여 불법적으로 접근허가를 승인받으려는 사용자를 인증서버에서 점검하여 점검 결과를 셋톱박스에 통보하여 불법 사용자를 사전에 예방함으로써 셋탑박스의 보안 기능을 강화하였다. 브로드캐스트 서비스 타입(Live Streaming과 Video-On-Demand)을 제안 모델에 적용하여 네트워크 효율성, 통신 오버헤드, 서비스 지연 등을 실험 평가한 결과 제안 기법이 네트워크 효율성, 오버헤드, 서비스 지연 측면에서 기존 기법보다 9.3% 향상된 결과를 나타내었다. 향후 연구에서는 IPTV 서비스를 수신하는 수신자들의 트래픽 발생을 최소화하기 위한 멀티미디어 인증 기법을 연구할 계획이다.

참 고 문 헌

[1] T. Ojanpera and R. Mononen, "Security and Authentication in theMobile World," Wireless Personal Communications, 2002.

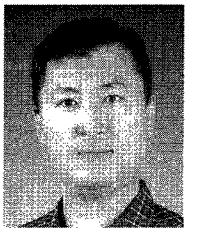
[2] T. Longstaff et al, "Security of the Internet," The Froechlish/Kent Encyclopedia of

Telecommunication, Vol.15, pp.21-255, 1997.
[3] International Organization for Standardization, "International Electro technical Commission Informational Technology-open distributed processing," ISO/iEC, 1996.
[4] J. M. Seok et al., "Development of Personalized broadcasting Service and Terminal based on TV-Anytime," Journal of the Institute of Eletronics Engineers of Korea, Vol.44-TC, No.1, 2007, pp.38-53.
[5] T. Mlakar, J. Zaletelj and JF. Tasic, "Viewer authenticaiton for personalized iTV services," Eighth International Workshop on Image Analysis for Multimedia Interactive Services, June, 2007, pp.63-63.
[6] Y. Gonno et al., "White Paper on Integrated Broadband Environment for Personalized TV Experience(IBEX) - Preliminary Edition," Proceedings of the 2000 ACM workshops on Multimedia, Nov., 2000, pp.63-66.
[7] D. D. Hwang and I. Verbauwhede, "Design of Portable Biometric Authenticators-Energy, Performance, and Security Tradeoffs," IEEE Transactions on Consumer Electronics, Vol.50, Issue 4, Nov., 2004, pp.1222-1231.
[8] H. Jabbar et al., "Viewer Identification and Authentication in IPTV using RFID Technique," IEEE Transactions on Consumer Electronics, Vol.54, Issue 1, Feb., 2008, pp.105-109.
[9] M. Alhisoni, A. Liotta and M. Ghanbari, "Resource Trade-off in P2P Streaming", 17th international packet video workshop 2009(PV 2009) , pp.1-8, May, 2009.
[10] Y. K. Park, S. H. Lim, O. Y. Yi, S. J. Lee and S. H. Kim, "User Authentication Mechanism using Java Card for Personalized IPTV Services," International Conference on Convergence and Hybrid Information Technology 2008 (ICHIT 08), pp.618-626, Aug., 2008.

정 윤 수 (Yoon-Su Jeong) 정회원

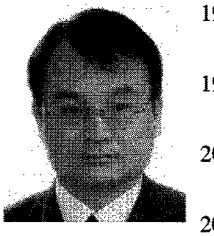
1998년 2월 청주대학교 전자계산학과 학사
2000년 2월 충북대학교 전자계산학과 석사
2008년 2월 충북대학교 전자계산학과 박사
2009년 9월~현재 한남대학교 산업기술연구소 전임연구원
<관심분야> 유·무선 보안, 암호이론, 정보보호, Network Security, 이동통신보안

정 윤 성 (Yoon-Sung Jung) 정회원



1995년 2월 Seowon Univeristy Applied Statistics, Bachelor of Sciences
1999년 2월 Korea University Statistics, Master of Sciences
2003년 5월 Texas A&M University Statistics, Master of Sciences
2009년 8월 Kansas State University Statistics, Ph.D.
2009년 9월~현재 Assistant Prfessor/Statistician Alcorn State University
<관심분야> Statistics, Statistical Computing, Data Mining, Network Security

김 용 태 (Yong-Tae Kim) 정회원



1984년 2월 한남대학교 계산통계학과 학사
1988년 2월 숭실대학교 전자계산학과 석사
2008년 2월 충북대학교 전자계산학과 박사
2002년 12월~2006년 2월 (주)가림정보기술 이사
2006년 3월~현재 한남대학교 멀티미디어 학부 강의전담교수
<관심분야> 모바일 웹서비스, 정보 보호, 센서 웹, 모바일 통신보안

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) 종신회원

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,