情報保護學會論文誌
第 21 卷 第 2 號, 2011. 4

Mobile IPTV 서비스 환경을 위한 non-CAS 기반의 서비스 보호 기법*

노 효 선† , 정 수 환‡
숭실대학교 정보통신전자공학부

A Service Protection Scheme based on non-CAS for Mobile IPTV Service*

Hyosun Roh† and Souhwan Jung‡
School of Electronic Engineering, Soongsil University

요 약

최근 IPTV 서비스 환경이 Mobile IPTV 서비스로 발전함에 따라 이동 단말에서 안전하게 IPTV 서비스를 제공 받을 수 있도록 지원하는 보안 기술이 요구되고 있다. CAS는 IPTV 서비스 환경에서 콘텐츠 보호와 서비스 보호를 위해 사용되고 있다. 그러나 CAS의 경우 사용되는 보안 키를 갱신 하는 과정에서 사용하는 EMM으로 인한 채널 대역폭이 증가하고, 키 관리 서버에서 각 가입자들에게 서비스 키를 갱신하기 위해 계산해야하는 연산량이 증가하는 문제점이 있다. 본 논문에서는 이러한 문제점을 해결하기 위해 서비스에 가입할 때 스마트카드 또는 USIM에 초기 마스터 키를 보관하여 분배하고, 마스터 키로부터 계층적 키를 유도함으로써 EMM을 사용하지 않고도 서비스 키를 갱신 할 수 있도록 제안하였다.

ABSTRACT

Due to the advancement of IPTV technologies, Mobile IPTV service is needed to be supported for service and content protection. CAS is generally used in the IPTV service to protect service and content. However, the CAS is not efficient in the Mobile IPTV. The CAS needs too much bandwidth for Service Key update to the each subscriber. Moreover, the CAS is increasing computation burden for the service key refreshment in the key management server when the subscriber frequently changes of the IPTV service group. To solve the problems, we used hierarchical key structure based on pre-shared key that is securely stored into smart card or USIM and do not use the EMM for Service Key update. As a result, the proposed scheme decreases computation burden at the key management server and wireless bandwidth burden in the Mobile IPTV service.

Keywords: Mobile IPTV, Authentication, Key Management, CAS

I. 서 론

최근 방송 시스템은 급속하게 발전하고 있는 초고속 통신망의 영향으로 빠르게 아날로그 방송 시스템에서 디지털 방송 시스템으로 전환되고 있다. 이러한 디지털 방송 서비스 중 IPTV (Internet Protocol Television)는 IP (Internet Protocol) 망을 통해 사용자가 원하는 멀티미디어 서비스를 양방향으로 제공하는 통신방송 융합 서비스들 중 대표적인 기술로 많은 관심을 받고 있다[1]. IPTV 서비스는 기존 TV (Television)와 PC (Personal Computer)가 가지고 있는 고유한 서비스 특성을 그대로 가지고 있으

접수일(2010년 12월 31일), 게재확정일(2011년 2월 13일)
* 이 논문은 2010년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No.2010-0000100).
† 주저자, peterhyo@ssu.ac.kr
‡ 교신저자, souhwanj@ssu.ac.kr

며, 최근 유무선 통합망 및 모바일 통신망의 확산으로 유선을 통한 IPTV 서비스에서 무선을 이용한 IPTV 서비스를 제공하기 위한 연구가 활발하게 진행되고 있다[2].

세계 여러 나라에서 IPTV에 대한 연구와 실용화를 위한 표준화가 가속화되면서 ITU-T (International Telecommunication Union-Telecommunication Standardization Sector)에서 국제 표준화에 대한 필요성이 제기되었고, 이에 따라 ITU-T SG13 (Study Group 13)의 FG IPTV (Force Group IPTV) 를 통해 표준화가 시작되었다[3]. 이후 IPTV 표준화는 GSI IPTV (Global Standards Initiative IPTV)를 통해 본격적으로 진행되고 있으며, 2010년에는 Mobile IPTV를 위한 기술적인 요구사항 및 보안 요구사항들이 정리 되고 표준화를 위한 논의가 계속되고 있다. 현재 ITU-T에서 표준화가 진행되고 있는 IPTV 표준화 기술 중 보안에 관련된 표준은 서비스 보호 (Service Protection)와 콘텐츠 보호 (Content Protection)을 지원하기 위한 보안 취약점, 보안 요구사항, 보안 구조 및 세부 메커니즘 등을 위한 표준화가 진행되고 있다[4].

표준화 중인 IPTV를 위한 서비스 보호 및 콘텐츠 보호를 위해서 기존 케이블 방송 시스템에서 적용되었던 CAS (Conditional Access System) 기술[5]이 대표적인 보안 기술로 논의 되고 있다. 그러나 CAS의 경우 기술적인 한계로 IPTV 서비스 환경에서 충분한 서비스 보호 및 콘텐츠 보호를 제공하지 못한다. 뿐만 아니라 Mobile IPTV 서비스 환경의 경우 무선 네트워크 환경 특성과 이동 단말의 성능 등 다양한 이유로 CAS를 적용하는 것이 사실상 어렵다. 이러한 이유로 최근 Mobile IPTV 서비스 환경에서 이동 단말 또는 콘텐츠 제공업자의 빈번한 변경 등으로 인해 바뀌는 CAS 기술을 이동 단말 또는 가입자에게 손쉽게 제공하기 위한 발전된 CAS 기술이 제안되고 있다. 대표적으로 미국의 OpenCable 표준화 그룹을 통해 개발되고 있는 DCAS (Downloadable CAS)[6]와 국내 TTA (Telecommunications Technology Association)를 중심으로 표준화 개발 중인 XCAS (Exchangeable CAS)[7]를 들 수 있다. 그러나 이러한 기술들의 경우 CAS를 기반으로 하고 있기 때문에 Mobile ITPV 서비스 환경에서 CAS 사용으로 인한 문제점이 그대로 존재한다.

CAS는 IPTV 서비스 및 콘텐츠 보호를 위해 MK (Master Key), SK (Service Key), CW (Control Word) 등과 같은 세 종류의 키를 사용하고, CW는 SK로 암호화되어 ECM (Entitlement Control Message)을 통해 수 초 간격으로 갱신 되고, SK는 MK로 암호화되어 EMM (Entitlement Management Message)을 통해 수 시간 간격으로 갱신 된다. 때문에 이동 통신망 환경에서 IPTV 서비스 그룹에 속한 각각의 가입자들에게 CW와 SK를 갱신하는 과정에서 발생하는 EMM으로 인한 채널 대역폭이 증가하는 문제가 있다. 또한 가입자들의 빈번한 이동으로 인해 키 관리 서버에서 SK를 갱신하기 위해 키를 계산하고 분배하는 과정에서의 연산량이 증가하는 문제가 있다[8]. 이러한 문제를 해결하기 위해 본 논문에서는 사전 분배된 대칭키를 기반으로 계층적인 키를 생성 및 분배함으로써 키 관리 서버의 연산 부담과 EMM을 사용하지 않고도 SK를 갱신 할 수 있는 Mobile IPTV 서비스를 위한 보안 기법을 제안하였다.

본 논문의 구성은 다음과 같다. 2장에서 관련 기술에 대해서 설명하고, 3장에서 본 논문에서 제안하고 있는 보안 기법을 설명한다. 4장에서는 제안 기법의 보안 분석과 기존 기법과의 성능 비교 분석을 통해 제안 기법의 효율성을 확인하고, 5장에서 결론을 맺는다.

II. 관련 기술

이번 장에서는 Mobile ITPV 서비스를 위한 서비스 및 콘텐츠 보안에 대한 요구사항[9]과 IPTV 서비스 환경에서 적용되고 있는 CAS에 대해서 정리하였다.

2.1 Mobile IPTV 서비스를 위한 보안 요구사항

이번 장에서는 Mobile ITPV 서비스를 위한 서비스 및 콘텐츠 보안에 대한 요구사항과 IPTV 서비스 환경에서 적용되고 있는 CAS에 대해서 정리하였다.

- 서비스 보호를 위한 보안 요구사항: Mobile IPTV 서비스 환경에서는 사용자들에 대한 서비스 접근 제어가 제공되어야 한다. 이때 제공되는 서비스 접근 제어는 이동 통신망 환경에서 자유롭게 이동하는 가입자들을 고려하여 제공되어야 한다. 뿐만 아니라 가입자가 사용하는 이동 단말에서 안전하게 서비스 접근 제어 모듈을 변경 또는 관리가 가능해야 하고, 제공 받는 서비스에 대한 보안 등급을 변경하는 것이 가능해야 한다. 특

히, 이동 통신망을 통해 전달되는 IPTV 콘텐츠에 대해서 서비스에 가입하지 않은 사용자가 불법적으로 시청하지 못하도록 해야 한다.

- 콘텐츠 보호를 위한 보안 요구사항: Mobile IPTV 서비스 환경에서 서비스 가입자에게 전달되는 IPTV 콘텐츠에 대한 보안이 제공되어야 한다. 이동 통신망을 통해 전달되는 콘텐츠에 대한 암호화가 제공되어야 하고, 트랜스코딩이 발생하는 중간경로에서 콘텐츠에 대한 불법 사용 및 전달, 삽입을 막을 수 있어야 한다. 또한 전달되는 콘텐츠를 불법적인 사용자가 가로채어 변조, 삭제 및 비정상적인 콘텐츠로 변경하여 정상적인 콘텐츠로 가장하는 공격을 막을 수 있어야 한다.

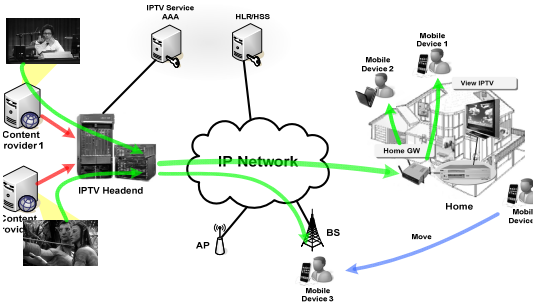
2.2 Conditional Access System (CAS)

CAS는 과거 케이블 TV에서 사용자들에 대한 서비스 접근 관리를 제공하기 위해 개발된 보안 시스템이다. CAS는 오직 유료 서비스에 가입한 사용자들만이 특정 유료 콘텐츠를 시청할 수 있도록 전달되는 미디어 콘텐츠를 스크램블링하여 전달한다. 스크램블링된 미디어 콘텐츠는 유료 사용자들만이 디스크램블링할 수 있는 보안 키를 통해 정상적인 미디어 콘텐츠를 시청할 수 있도록 지원한다. 이를 위해 CAS는 MK, SK, CW 등의 3 가지 종류의 키를 사용한다. MK는 사용자가 유료 서비스에 가입할 때 인증 서버가 가입자에게 분배하는 초기 비밀 키이고, SK는 동일한 유료 서비스 가입자들에게 미디어 콘텐츠를 스크램블 할 때 사용하는 CW를 복호화할 수 있도록 MK로 암호화하여 전송하는 서비스 그룹 키 이다. CW는 미디어 콘텐츠를 스크램블 하기 위해 사용되는 키로 AES-128 bit 알고리즘으로 생성된 키를 사용한다[10]. CW는 수초 간격으로 제공되는 유료 채널별로 갱신되고, SK로 암호화한 후 ECM에 포함하여 전송되는 미디어 콘텐츠와 함께 가입자에게 전송한다. SK는 수시간 간격으로 갱신 되고, 각 가입자와 인증 서버간에 공유하는 각각의 MK로 SK를 암호화한 다음 EMM을 통해 각 사용자들에게 전송된다. 스크램블링 되어 전송되는 미디어 콘텐츠를 STB에서 수신하면 SK를 이용하여 CW를 복호화한 다음 미디어 콘텐츠에 대한 디스크램블링을 하여 IPTV로 전달한다. 이처럼 CAS는 3 종류의 키를 이용하여 서비스 보호 및 콘텐츠 보호를 제공하지만, 무선 환경에서 사용할 경우 몇 가지 문제점이 발생한다. SK 갱신을 위한 EMM은 가입자의 수가 증가할수록 무선 채널 대역폭이 증가하는 문제점이 있고, 이동 통신망 환경에서 가입자의 빈번한 이동에 따라 키 관리 서버에서 SK를 갱신하기 위해 필요한 연산량이 증가하는 문제가 있다.

III. 제안 기법

본 장에서는 본 논문에서 제안하고 있는 Mobile IPTV 서비스 환경에서 CAS의 EMM을 사용하지 않고도 SK를 갱신 하고, 가입자들의 빈번한 이동에도 키 관리 서버의 연산 부담을 줄일 수 있는 보안 기법에 대해서 설명한다.

3.1 기본 아이디어



〔그림 1〕 Mobile IPTV 서비스 환경

본 논문에서 제안하고 있는 보안 기법은 사전에 분배된 대칭키로부터 계층적인 키를 유도하여 IPTV 서비스 AAA (ISA)와 서비스 가입자의 댁내에 존재하는 셋톱박스 (Set-Top-Box, STB) 간에 공유한다. 이후 이동 통신망 환경에서 가입자가 원하는 이동 단말을 통해 IPTV 서비스를 제공 받을 수 있도록 지원하기 위해 STB는 이동 단말에게 IPTV 서비스 접속을 위한 보안 키를 계층적 키로부터 유도하여 분배한다. 위의 〔그림 1〕은 본 논문에서 제안하는 보안 기법이 적용되는 Mobile IPTV 서비스 환경을 보여준다. IPTV 서비스를 위한 미디어 콘텐츠는 콘텐츠 제공업자로부터 IPTV 서비스 제공업자가 공급 받은 후 IP 망을 통해 가입자의 댁내에 설치되는 STB로 전달된다. 가입자의 댁내에는 STB에 유선으로 연결된 IPTV와 IPTV 서비스 이용 가능한 이동 단말들이 존재한다. 이동 단말들은 기본적으로 WiFi 인터페이스를 가지고 있고, 추가적으로 WiBro 또는 3G 망을 위

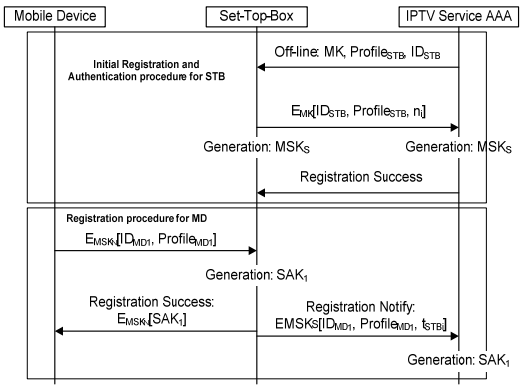
〔표 1〕 주요 용어 정리

용 어	내 용
PK_X^+, PK_X^-	RSA 기반의 노드 X의 공개키 및 개인키 쌍〔14〕
$h(\ )$	일방향 해쉬함수
t_x	X의 시간에 생성되는 타임 스탬프
MSK_S	IPTV 서비스를 접속을 위해 ISA와 STB 간에 사전에 공유하는 MK로부터 유도되는 Master Session Key
MSK_N	네트워크 채널 보안을 위한 Master Session Key로 이동 단말이 최초 네트워크 접속시 인증서버와 이동 단말 간에 EAP-AKA를 통해 공유하는 IK와 CK의 해쉬를 통해 유도되는 암호화키〔15〕
n_i	STB의 초기 인증 및 등록 과정에서 STB가 MSK_S를 MK로부터 유도하기 위해 선택하는 임의의 수
r_i	이동 단말이 Mobile IPTV 서비스 접속 인증을 수행하는 과정에서 SAK로부터 TSAK를 유도하기 위해 선택하는 임의의 수
k_i, k_{i+j}	콘텐츠 서버에서 서비스 인증을 성공한 이동 단말에게 SK를 업데이트하기 위해 생성하는 임의의 수 k_i와 이후 j 번째에 선택하는 임의의수 k_{i+j}
CW	CAS에서 콘텐츠 스트램블링을 위해 사용되는 제어단어
SK	그룹키를 암호화하는데 사용되는 이동 단말 및 셋톱박스를 위한 Service Key
SAK_i	셋톱박스에서 등록한 이동 단말 i가 Mobile IPTV 서비스에 접속할 때 인증을 위해 사용하기 위해 발급하는 Service Access Key
$TSAK$	CS와 이동 단말 간 무선 채널을 보호하기 위해 SAK로부터 유도하는 Temporary SAK

한 무선 인터페이스를 복수로 설치되어 있다. 이러한 이동 단말을 통해 가입자는 댁외에서 Mobile IPTV 서비스를 제공받게 된다. 본 논문을 위해 이동 단말들은 EAP-AKA 기반〔11〕의 네트워크 초기 인증을 수행하는 3GPP 통합망 환경〔12〕을 가정하였고 이를 위해 기본적으로 USIM이 장착되어 있음을 가정하였다. 이동 단말은 초기 부팅 후 네트워크 접속을 위한 EAP-AKA를 수행한 후 인증 서버와 Integrity Key (IK) 및 Cipher Key (CK)를 공유한다. 또한, IPTV 서비스 AAA와 콘텐츠 서버 간에는 IPSec〔13〕을 이용한 보안된 채널로 연결되어 있음을 가정한다. 다음의 〔표 1〕은 본 논문에서 사용하는 주요 용어를 정리하였다.

3.2 등록 및 인증 과정

앞서 설명한 것과 같은 Mobile IPTV 서비스 환경에서 가입자가 IPTV 서비스에 가입하면 IPTV 서비스 사업자는 가입자에게 스마트카드 또는 USIM에 초기 마스터 키인 MK (Master Key)와 서비스 가입 정보가 포함된 ProfileSTB, 댁내에 설치되는 STB의 IDSTB를 안전하게 저장하여 발급한다. 이후 IPTV 서비스 가입자의 댁내에 STB가 설치되면 IPTV 서비스 가입자로부터 발급받은 스마트카드 또는 USIM을 장착 후 STB를 부팅하면 IP 망을 통해 IPTV 서비스 AAA에 초기 등록 및 인증 과정을 수행한다. 다음 〔그림 2〕는 셋톱박스 초기 인증 및 이동 단말 등록 과정을 보여준다. 다음은 초기 등록 및 인증 과정과 이동 단말에게 Mobile IPTV 서비스 접근을 위한 키 분배 과정을 과정 별로 자세하게 설명한다.



〔그림 2〕 셋톱박스 초기 인증 및 이동 단말 등록 과정

Step 1: 댁내에 STB가 설치된 후 부팅하면 ISA에게 IPTV 서비스 초기 등록 및 인증 과정을 수행한다. 먼저 스마트카드 또는 USIM에 저장된 MK로 가입자의 서비스 등록 정보가 포함된 $Profile_{STB}$와 ID_{STB} 그리고 MK로부터 유도되는 계층적 키인 MSK_S를 유도할 때 사용하는 임의의 수 n_i를 암호화하여 ISA로 전송한다. 그리고 STB는 다음 수식 (1)처럼 MSK_S를 생성한다.

$$MSK_S = h(MK, Profile_{STB}, ID_{STB}, n_i) \quad (1)$$

Step 2: ISA는 STB가 전송한 메시지를 수신하면 MK로 암호화된 메시지를 복호화하고, $Profile_{STB}$에 포함된 가입자 등록 정보를 확인한다. 이후

STB에서 생성한 것과 같은 동일한 방법으로 MSK_S를 생성한 다음 STB에게 초기 인증 및 등록 성공 메시지를 STB에게 전송한다. STB에서 등록 및 인증 성공 메시지를 수신하면 STB에 연결된 IPTV를 통해 IPTV 서비스를 사용할 수 있게 된다.

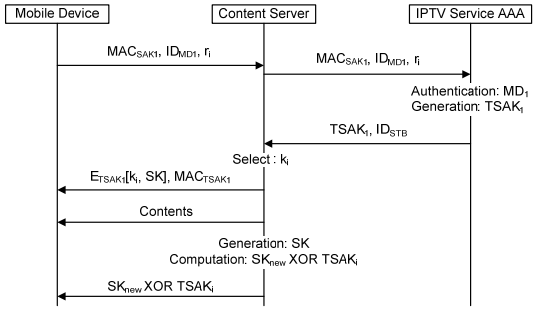
Step 3: 댁내에서 가입자가 사용하기를 원하는 이동 단말을 MD_1이라고 가정하고, 가입자가 MD1을 선택한 후 이동 단말 MD_1을 STB에 등록시킨다. 이때 이동 단말 MD_1은 초기 네트워크 접속 인증과정에서 3GPP 인증 서버와 공유하는 MSK_N으로 자신의 ID_{MD1}와 가입자가 선택한 $Profile_{MD1}$을 암호화하여 STB에게 전달한다.

Step 4: MD_1이 전송한 메시지를 수신한 STB는 MD_1의 네트워크 초기 인증 과정에서 인증서버로부터 전달받은 MSK_N으로 메시지를 복호화하고, MD_1이 Mobile IPTV 서비스에 접근할 때 사용하게 되는 SAK_1을 다음 수식 (2)와 같이 생성한다. 이렇게 키를 생성한 다음 MSK_N으로 생성된 SAK_1을 암호화하여 MD_1으로 전송한다. 이후 MD_1은 수신한 메시지를 복호화하여 SAK_1을 USIM에 안전하게 보관하고 가입자가 이동 통신망 환경에서 Mobile IPTV 서비스를 사용하고자 원할 경우 SAK_1을 이용하여 서비스 접속 인증을 수행한다. 또한 STB는 MD_1에 대한 등록 및 키 분배가 성공적으로 끝나면 이동 단말의 $IDMD_1$과 $ProfileMD_1$, t_{STBi}를 MSK_S로 암호화하여 ISA에게 알린다. ISA는 이 정보를 관련 DB에 보관한 다음 가입자가 이동 단말을 통해 Mobile IPTV 서비스에 접근 할 경우 과금 및 인증을 위해 사용한다.

$$SAK_1 = h(MSK_S, ID_{MN1}, t_{STBi}, \text{'}MobileDevice1\text{'}) \quad (2)$$

3.3 Mobile IPTV 서비스 접속 인증 및 키 갱신 과정

앞서 설명한 것처럼 STB를 통해 가입자는 IPTV 서비스 초기 등록 및 인증 과정을 수행한다. 이후 가입자가 선택한 이동 단말을 통해 이동 통신망 환경에서 Mobile IPTV 서비스에 접속하여 서비스를 제공받을 수 있도록 하기 위해 STB에 등록 후 SAK_1을 분배받는다. 사용자가 STB에 등록한 이동 단말을 가지고 댁외에서 Mobile IPTV 서비스에 접속할 경우 다음과 같은 과정을 통해 서비스를 사용하고, 관련된 보안 키를 갱신 하게 된다. 다음 〔그림 3〕은 이동 단말에 대한 Mobile IPTV 서비스 인증 과정과 키 분배 과정을 보여준다.



〔그림 3〕 이동 단말에 대한 서비스 인증 및 키 분배 과정

Step 1: 가입자는 댁외에서 이동 단말 MD_1을 통해 Mobile IPTV 서비스를 사용할 경우 MD_1은 우선 가용한 무선 인터페이스와 이동 통신 환경을 검색한다. 그리고 STB로부터 분배 받은 SAK_1을 이용하여 다음 식 (3)과 같은 MAC_{SAK1}을 생성하고 자신의 ID_{MD1}과 IPTV 서비스 키인 SK를 갱신하는데 사용하게 되는 임의의 수 ri를 Mobile IPTV 서비스 콘텐츠를 제공하는 콘텐츠 서버 (Content Server, CS)에게 전송한다.

$$MAC_{SAK1} = h(SAK_1, ID_{MN1}, r_i, ID_{STB}) \quad (3)$$

Step 2: CS는 MD1이 전송한 메시지를 ISA에게 포워딩하여 이동 단말에 대한 인증을 요청한다. ISA는 CA로부터 전달 받은 메시지에 포함된 ID_{MD1}을 관련 DB에서 검색한 다음 ID_{MD1}에게 SAK_1을 발급한 STB를 확인하고, MD_1이 생성한 것과 동일한 MAC_{SAK1}'을 생성 및 비교하여 MD_1에 대한 인증을 수행한다. MD_1에 대한 인증이 성공하면 ISA는 $TSAK_1$을 다음 식 (4)와 같이 생성하여 CS에게 전송한다.

$$TSAK_1 = h(SAK_1, r_i, ID_{STB}, ID_{MN1}) \quad (4)$$

Step 3: ISA로부터 $TSAK_1$과 ID_{STB}를 전달받은 CS는 $TSAK_1$를 이용하여 CW를 암호화하여 전달하는데 사용하는 SK와 이후 SK를 갱신하기 위해 사용하는 임의의 수 k_i를 선택하여 SK와 함께 암호화하고 수식 (5)와 같이 $MACT_{SK1}$을 계산하여 함께 MD_1에게 전송한다.

$$MAC_{TSAK1} = h(TSAK_1, k_i, r_i) \quad (5)$$

Step 4: CS로부터 $TSAK_1$으로 암호화되어 전송된 SK와 k_i를 MD_1은 $TSAK_1$으로 복호화하고 SK와 ki를 USIM에 안전하게 보관한다. 이후 CS는 전송할 콘텐츠를 CW로 스크램블링하고 이때 사용한 CW는 SK로 암호화하여 전송하는 콘텐츠의 헤더에 포함하여 가입자들에게 전송한다. 스크램블링된 콘텐츠를 수신하면 사전에 받아둔 SK로 CW를 복호화하고, 이를 통해 습득한 CW를 이용하여 콘텐츠를 디스크램블링 한다. 그리고 CS는 주기적으로 수식 (6)과 같이 SK_i를 생성하여 갱신 한다. 이때 CS는 각 가입자들에게 SK를 갱신 할 때 사용한 k_{i+j}를 ECM에 추가하여 보낸다. 이렇게 함으로써 EMM을 사용하지 않고도 SK를 갱신 할 수 있다.

$$SK_i = h(SK, k_{i+j}) \quad (6)$$

위와 같은 과정을 통해 제안 기법에서는 가입자가 선택한 이동 단말을 이용하여 Mobile IPTV 서비스에 접속 및 서비스를 이용할 수 있다. 또한 EMM 메시지 사용을 하지 않고도 SK를 주기적으로 갱신할 수 있다. 뿐만 아니라 제안 기법은 동일한 Mobile IPTV 서비스 그룹에 속한 가입자 단말이 다른 그룹으로 이동하거나 새로운 단말이 그룹에 가입할 경우 CS에서 SK를 새롭게 생성하여 갱신할 수 있다. 이렇게 그룹 멤가 변경될 경우 CS는 새로운 서비스 키인 SK_{new}를 생성한 다음 그룹에 속한 각 가입자 단말들과 공유하고 있는 $TSAK_i$와 XOR 연산을 한다. 이후 $SK_{new} \oplus TSAK_i$는 각 가입자들에게 전송되고, 각 가입자들은 자신의 $TSAK_i$를 이용하여 안전하게 새로운 SK_{new}를 갱신하게 된다.

IV. 보안 분석 및 성능 평가

이번 장에서는 본 논문에서 제안하는 보안 기법에 대한 보안 분석과 기존 기법들과의 성능 평가를 통해 제안 기법의 효율성을 비교 분석한다.

4.1 보안 분석

본 논문에서 제안하는 기법은 IPTV 서비스를 위해 요구되는 서비스 보호와 콘텐츠 보호를 위한 보안 요구사항을 만족한다.

- Mobile IPTV를 위한 Service Protection: Mobile IPTV 서비스를 위한 서비스 보호는 정상적으로 서비스에 가입하지 않은 사용자가 비정상적인 방법을 통해 IPTV 서비스를 이용하는 것을 막을 수 있어야 하고, 정상적인 IPTV 서비스 가입자는 원하는 IPTV 서비스에 안전하게 접속하여 서비스를 제공받을 수 있도록 요구되는 보안 요구사항이다. 본 논문에서는 서비스 보호를 위해 IPTV 서비스 사업자는 서비스에 가입하는 가입자만이 알게 되는 마스터 세션키인 MK를 USIM 또는 스마트카드에 안전하게 저장한 후 오프라인을 통해 전달한다. 이후 STB이 초기 부팅을 시작하면 STB에 장착된 스마트카드 또는 USIM에 저장된 MK로 IPTV 서비스 인증을 위한 요청메시지를 IPTV 서비스 AAA인 ISA에게 전송한다. ISA는 MK를 확인함으로서 서비스에 가입한 가입자를 식별 및 인증하게 된다. 이후 MK로부터 유도하는 계층적 키인 MSK_S를 통해 IPTV 서비스 콘텐츠 서버에서 전송하는 콘텐츠를 시청하는데 필요한 SK를 암호화하여 전달한다. 때문에 IPTV 서비스에 정상적으로 가입하지 않는 사용자의 경우 IPTV 서비스에 접속할 수 없고, CW로 스크램블링되어 전송되는 IPTV 콘텐츠를 복호화 할 수 없다. 만약 서비스에 가입하지 않은 사용자가 비정상적인 방법으로 IPTV 서비스 콘텐츠를 시청하기 위해서는 STB에 장착된 USIM 또는 스마트카드의 MK를 알거나, MK로부터 유도된 MSK_S를 알아야 한다. 또는 CW를 암호화하여 전송하는 SK를 알아내거나 CW를 알아야 한다. CW는 수초 간격으로 변경되어 전송되기 때문에 이전의 CW를 알고 있어도 사용할 수 없고, SK의 경우 MSK_S로 암호화되어 전송되기 때문에 서비스에 가입하지 않은 사용자의 경우 알 수 없다.

- Mobile IPTV를 위한 Content Protection: Mobile IPTV 서비스를 위한 콘텐츠 보호를 위해서는 콘텐츠 서버에서 가입자들에게 전송되는 IPTV 콘텐츠를 비정상적인 가입자가 접근하여 시청하지 못하도록 콘텐츠에 대한 암호화가 제공되어야 한다. 본 논문에서 제안하는 기법의 경우 콘텐츠는 CW를 통해 스크램블링되어 전송된다. CW는 AES-128 bit 암호화 알고리즘을 통해 생성되는 키를 사용한다[10]. 또한 CW는 SK로

암호화되어 전송되고, SK는 수 시간 간격으로 IPTV 키 관리 서버를 통해 각 사용자들에게 갱신 된다. 따라서 서비스에 가입되지 않은 사용자의 경우 전달되는 콘텐츠를 네트워크 중간에서 가로채더라도 정상적인 콘텐츠를 시청할 수 없다. 악의적인 공격자가 임의로 유/무선 망을 통해 전송되는 IPTV 콘텐츠를 시청하려면 CW와 SK를 알고 있어야 한다. 그러나 이 키들은 서비스 가입시 가입자와 인증 서버만 알고 있는 MK로부터 유도되는 MSK_S로 암호화되어 전송되고, 이후 SK를 갱신 할 경우에는 MSK_S로부터 유도한 TSAK로 암호화되어 갱신되기 때문에 공격자는 관련된 키 정보를 확인할 수 없다.

4.2 성능 평가

본 논문에서 제안하는 기법은 IPTV 서비스 환경에서 서비스 보호 및 콘텐츠 보호를 위해 적용되는 CAS에 비해 통신 오버헤드 및 키 관리 서버의 연산 부담을 줄일 수 있다. CAS의 경우 MK, SK 그리고 CW 등과 같은 3 종류의 암호화 키를 사용한다. CW는 수 초 간격으로 SK로 암호화되어 ECM을 통해 IPTV 콘텐츠와 함께 갱신 된다. SK는 MK로 암호화되어 EMM 메시지를 통해 수 시간 간격으로 각 가입자들에게 전송된다. 이런 환경에서 별도로 SK를 갱신하기 위해 전송하는 EMM의 경우 별도의 채널을 통해 Mobile IPTV 서비스에 가입된 각각의 사용자들에게 전송되기 때문에 가입자가 변동되거나 SK를 주기적으로 갱신하는 경우 무선 채널 대역폭 부담이 발생한다. 예를 들어 Mobile IPTV 서비스에 가입한 가입자 수가 50만 명이고, 가입자에게 제공되는 서비스 채널이 30 채널일 때 1 시간 동안 ECM과 EMM 갱신 따른 채널 대역폭과 패킷 량은 다음과 같이 계산할 수 있다. ECM은 168 bit, EMM은 488 bit로 가정 할 때 다음과 같이 전송되는 패킷 량과 필요한 채널 대역폭이 필요하다[10].

- ECM 갱신
  - 전송되는 패킷 량: *30 ch × 168 bit × 1,200 회 =* ***6.04 Mbit***
  - Bandwidth: *30 ch × 168 bit / 3 초 =* ***1,680 bps***
- EMM 갱신
  - 전송되는 패킷 량: *500,000 명 × 2 번 × 488 bit × 30 ch =* ***14,640 Mbit***
  - Bandwidth: *(500,000명 × 30 ch) × 488 bit/ 3,600 초 =* ***2.03 Mbps***

위에서 살펴본 것처럼 CAS는 SK를 갱신 할 때 채널 대역폭이 증가하지만 본 논문에서 제안하는 기법의 경우 SK를 갱신 할 때 채널 대역폭에 대한 부담이 상대적으로 적다. 제안 기법은 이동 단말에서 SK를 갱신 할 때 EMM을 사용하지 않는다. 제안 기법의 경우 MD_1이 처음 Mobile IPTV 서비스를 위한 CS에 인증을 요청하고 성공하면 CS와 MD_1 간에 공유하게 되는 $TSAK_1$으로 초기 SK_i를 암호화하여 전달한다. 이후 CS는 SK_i에 k_{i+j}를 해쉬하여 새로운 SK_{i+1}을 생성하고, 각 가입자들이 SK_i를 갱신 할 수 있도록 ECM에 k_{i+j}를 포함하여 전송함으로서 EMM을 사용하지 않고도 SK_i를 갱신 할 수 있다. 따라서 EMM 사용에 따른 채널 대역폭 부담을 줄일 수 있다.

또한, 제안 기법은 각 가입자에 대한 SK 갱신 따른 키 관리 서버의 연산 부담을 줄여 준다. CAS의 경우 동일한 서비스에 가입한 가입자들을 그룹으로 관리하고, 그룹의 멤버들이 변경될 경우 SK를 갱신하게 된다. 특히 Mobile IPTV 서비스 환경에서는 이동 단말을 가진 가입자들이 자유롭게 이동할 수 있기 때문에 IPTV 서비스 그룹의 멤버 변동이 지역적으로 빈번하게 발생한다. 이로 인해 키 관리 서버에서 각 가입자들에게 SK를 갱신하기 위해 필요한 연산 부담이 증가한다. 다음은 키 관리 서버에서 제안 기법과 CAS의 경우 멤버 변동에 따른 연산량을 비교하였다. CAS의 경우 새로운 멤버가 가입하거나 탈퇴할 때 SK를 갱신하기 위해 한 번의 SK 생성 시간과 그룹 멤버 수만큼의 암호화를 수행한다. 암호화 연산 시간은 T_{enc}, SK 생성 시간은 T_{gk}로 표시하고 멤버 수는 n으로 표시하였다.

〔표 2〕 암호화/복호화 및 사칙연산 수행시간

		표기	연산시간 (us)
대칭 키 기반 암/복호화	AES-128 bit 암호화	T_{enc}	24.117
	AES-128 bit 복호화	T_{dec}	22.798
사칙연산	1024 bit 곱셈	T_{mul}	1.018
	1024 bit 나눗셈	T_{div}	1.893
	1024 bit 덧셈	T_{add}	0.588

앞의 〔표 2〕는 Pentium Ⅳ 2.33 GHz의 데스크탑 PC에 OpenSSL〔16〕을 설치하여 키 관리 서버에서 SK를 갱신하는 과정에서 필요로 하는 암호화/복호화 및 사칙연산 수행 시간을 실제 측정한 값을 정리하였다. 제안 기법의 경우 Mobile IPTV 서비스 환경에서 SK를 새롭게 갱신 할 경우 CAS에서처럼 암호화를 수행하지 않는다. 각 가입자들과 공유하는 TSAK와 새롭게 생성한 SK를 XOR하여 전송하기 때문에 CAS에 비해 서버의 연산 부담을 줄일 수 있다. 다음의 〔표 3〕은 CAS와 제안 기법에 대해 동일한 Mobile IPTV 서비스 그룹에 속한 가입자가 5만명일 경우 키 관리 서버에서 SK를 갱신하기 위해 필요한 연산시간을 비교한 표이다. 표에서 확인할 수 있는 것처럼 CAS의 경우 서비스 그룹 멤버 변동에 따라 SK를 갱신하기 1.2 초의 연산 시간이 필요하지만 제안 기법의 경우 31.6 ms로 CAS에 비해 연산시간이 상대적으로 적게 필요함을 확인할 수 있다.

〔표 3〕 IPTV 서비스 키 관리 서버에서의 연산시간

	멤버 수	CAS 연산량	제안 기법의 연산량
초기	n (5 만명)	1.2 sec	31.6 ms
새로운 멤버 가입	n + 1	1.2 sec	31.6 ms
멤버 탈퇴	n - 1	1.2 sec	31.39 ms

V. 결 론

본 논문에서는 Mobile IPTV 서비스 환경에서 이동 단말을 위한 보안 기법을 제안하였다. 기존 IPTV 서비스 환경에서 적용되고 있는 CAS의 경우 사용되는 보안 키를 갱신하는 과정에서 채널 대역폭이 증가하고 가입자 수에 따라 키 관리 서버의 연산량이 증가하는 문제점이 있기 때문에 Mobile IPTV 서비스 환경에 그대로 적용하기가 어렵다. 본 논문에서는 이러한 문제점을 해결하기 위해 non-CAS 기반의 Mobile IPTV 서비스를 위한 보안 기법을 제안하였다. 제안된 기법은 서비스 가입과정을 통해 분배된 비밀키로부터 계층적 키를 유도하여 사용함으로써 CAS의 EMM을 사용하지 않고도 SK를 갱신 할 수 있도록 하였고, 키 관리 서버에서 SK를 갱신 할 때 XOR 연산만을 수행해서 SK를 갱신 할 수 있도록 제안하였다. 이로 인해 제안 기법의 경우 CAS에 비해 채널 대역폭에 대한 부담을 줄였고, 키 관리 서버에서 SK 갱신으로 인한 연산량을 감소 시켜 Mobile IPTV 서비스 환경에서 CAS를 적용하지 않고도 서비스 보호 및 콘텐츠 보호를 제공할 수 있도록 하였다.

참고문헌

〔1〕 O. Gerard, "Next Generation IPTV services and Technologies," *Wiley InterScience*, 2007.

〔2〕 S. Park, and S. Jeong, "Mobile IPTV: Approaches, Challenges, Standards, and QoS Support," *IEEE Internet Computing*, Vol. 13, Issue 3, pp.23-31, 2009.

〔3〕 T. Sharpe, J. Heiles, L. Hong, M. Deschanel, W.Yiyan, J. Maisonneuve, and L. Wei, "An Overview of IPTV Standards Development," *IEEE Transaction on Broadcasting*, Vol.55, Issue 2, pp.315-328, Jun. 2009.

〔4〕 ITU-T Y.miptv-req, "Functional Requirements of Mobile IPTV," Jul. 2010.

〔5〕 E. Cruselles, J.L. Melus, and M. Soriano, "An Overview of Security in Eurocrypt Conditional Access System," Global Telecommunications Conference, Nov. 1993.

〔6〕 Cable Television Laboratories, Inc., "OpenCable DCAS System Overview Technical Report," *OC-TR-DCAS-D01-060 206*, Sep. 2006.

〔7〕 TTAK.KO-07.0079, "Standard for eXchangeable CAS Transmitter/Receiver Interface," *TTA*, 2010.

〔8〕 Y. Zhang, C. Yang, J. Liu, and J. Tian, "Broadcast Encryption Scheme and Its Implementation on Conditional Access System," *Web Information System and Applications 2009*, May. 2009.

〔9〕 TTAK.KO-08.0021, "Requirements for Non-NGN Based Mobile IPTV," *TTA*, 2009.

〔10〕 TTAK.KO-08.0023, "IPTV Interchangeable CAS (iCAS)," Mar. 2010.

〔11〕 J. Arkko, H. Haverinen, and Nokia, "Extensible Authentication Protocol Method

for 3rd Generation Authentication and Key Agreement (EAP-AKA)," *IETF RFC 4187*, Jan. 2006.
〔12〕 3GPP, TR 23.828 V8.0.0, "3GPP System Architecture Evolution: Report on Technical Options and Conclusions," 2006.
〔13〕 Kent, S and R. Atkinson, "Security Architecture for the Internet Protocol," *IETF RFC 2401*, Nov. 1998.
〔14〕 R. Rivest, A. Shamir and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystem," *Communications of the ACM*, 1978.
〔15〕 J. Arkko, V. Lehtovirta, and P. Eronen, "Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA′)," *IETF RFC 5448*, May. 2009.
〔16〕 OpenSSL, http://www.openssl.org/

〈著者紹介〉

노 효 선 (Hyosun Roh) 학생회원
2005년 2월: 숭실대학교 정보통신전자공학부 졸업
2007년 2월: 숭실대학교 정보통신전자공학과 석사
2011년 2월: 숭실대학교 전자공학과 박사
〈관심분야〉 이동 네트워크 보안, 유비쿼터스 네트워크 보안, IPTV 보안

정 수 환 (Souhwan Jung) 종신회원
1985년 2월: 서울대학교 전자공학과 졸업
1987년 2월: 서울대학교 전자공학과 석사
1988년~1991년: 한국통신 전임 연구원
1996년 6월: University of Washington 박사
1996년~1997년: Stellar One SW Engineer
1997년~현재: 숭실대학교 정보통신전자공학부 교수
〈관심분야〉 이동 네트워크 보안, VoIP 보안, 네트워크 보안, RFID/USN 보안