韓國컴퓨터情報學會 論文誌
第15卷 第7號, 2010. 7.

2010-15-7-3-4

Open IPTV 환경에서 재암호화 과정 없는 댁내 컨텐츠 분배를 위한 키관리 기법

정 서 현*, 노 효 선*, 이 현 우**, 이 정 현***, 정 수 환****

A Key Management Scheme without Re-encryption for Home-domain Contents Distribution in Open IPTV Environments

Seohyun Jung*, Hyosun Roh*, Hyunwoo Lee **, Jeonghyun Yi***, Souhwan Jung****

요 약

최근 IPTV 환경이 점차 개방형 IPTV로 발전함에 따라, 댁내에서 사용되는 IPTV 단말의 경우도 다양한 형태로 발전하고 있다. 이러한 환경에서 사용자는 노트북, 휴대폰, PDA와 같은 댁내에 존재하는 다양한 IPTV 서비스 가용 단말을 통해 IPTV를 시청할 수 있게 된다. 하지만, 방송 콘텐츠보호를 위해 셋탑박스 (STB)에 탑재된 CAS 기술로 인해 같은 댁내에서도 각 단말의 개수만큼의 STB를 필요로 하거나, STB에 연결가능한 모든 단말에는 CAS가 해제된 상태로 무제한 제공하여야 하는 것이 현재의 기술 수준이다. 본 논문에서는 추가적인 STB 설치 없이 댁내 사용자가 선택한 IPTV 가용 단말들로 컨텐츠를 재분배함과 동시에 서비스 사업자가 복수의 사용자 단말에 대하여 수신제어가 가능한 기술을 제안한다. 제안 기법은 RSA 서명의 개인키 분할 방식을 사용하여 STB에서 댁내 IPTV 단말로 전달되는 컨텐츠를 기존 CAS 시스템을 통해 스크램블링된 내용 그대로 재암호화과정 없이 전달할 수 있다. 따라서, 제안기법은 STB에서 사용자 단말 구간에 재암호화 기법을 활용하여 콘텐츠를 분배하는 기존 기법에 대비하여, 기존의 보안 수준을 유지하면서도 계산량 및 전송량 측면에서 기존 기술과 비교하여 많은 성능개선과 함께, 댁내에 재분배되는 컨텐츠에 대한 불법적인 유출을 방지하는 효과도 부수적으로 제공한다.

Abstract

Due to the advancement of IPTV technologies, open IPTV services are a step closer to becoming reality. In such service environment, users are able to enjoy IPTV services using a variety of devices available at their home domain. However, it is impossible to get such flexible services at their convenience unless each of devices is individually connected to Set-Top-Box (STB) because of Conditional Access System (CAS) or service providers otherwise allow STB to freely distribute decoded contents to every user devices attached to STB. In this paper, we propose a key

• 제1저자 : 정서현 교신저자 : 이정현
• 투고일 : 2009. 11. 24, 심사일 : 2010. 03. 01, 게재확정일 : 2010. 05. 18.
* 숭실대학교 정보통신전자공학부 **ETRI 융합미디어인프라연구팀 ***숭실대학교 컴퓨터학부 교수
**** 숭실대학교 정보통신 전자공학부 교수
※ 이 논문은 2009년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No. 20090089245)

management scheme for securely distributing contents from STB to multiple user devices at home domain. The proposed scheme also makes the service providers be able to control the access rights to each of user devices without installing individual STBs. It is achieved by computationally dividing a private key of RSA signature scheme into three parts and thus makes possible to distribute the contents scrambled through a underlying CAS mechanism without re-encrypting them that the existing scheme should employ. It improves significantly computation and communication complexities, maintaining it as secure as the existing schemes. Additionally, it prevents misbehaving users from illegally distributing the contents from STB to their devices available at home domain.

▸ Keyword : IPTV, 콘텐츠분배(contents distribution), RSA, CAS(Conditional Access System)

Ⅰ. 서 론

최근 빠르게 발전하고 있는 초고속 인터넷 기술의 영향으로 IP (Internet Protocol) 기반의 융·복합 서비스가 빠르게 현실화되고 있으며, IPTV를 이용한 서비스 활성화를 위하여 다양한 비즈니스 모델들이 제안되고 있다. 이러한 다양한 서비스로는 원하는 시간에 원하는 멀티미디어 서비스를 제공하기 위한 VOD(Video on Demand) 서비스[1], 사용자 편의를 고려하여 다양한 멀티미디어 컨텐츠의 유연한 조작을 제공하는 EPG(Electronic Program Guide) 서비스[2], 기존 TV에서 제공하였던 광고효과에서 발전하여, 광고된 상품에 대하여 시청자의 구매를 돕는 T-Commerce 서비스[3] 등이 있다.

IPTV는 초고속 인터넷망을 통하여 사용자의 요청에 따라 양방향으로 다양한 멀티미디어 컨텐츠를 제공하는 방송통신 융합서비스로 정의 된다 [4]. IPTV 서비스의 등장으로 기존 인터넷을 통해 전달되는 잘 분류되지 않은 방대한 양의 컨텐츠를 체계적이면서 보다 좋은 품질로 제공이 가능해지고 있으며, 유료 서비스과 함께 서비스가 활성화 단계에 있다 [5]. IPTV 보안 서비스를 위해서는, 국제 표준화 기구인 ITU-T의 FG-IPTV (Focus Group-IPTV)에서 IPTV 서비스를 위한 방송 수신 제한 기술에 대한 표준화를 진행하고 있다 [6~8]. ITU-T에서는 X.iptvsec-1을 통해 IPTV 서비스의 기본 보안 요구사항과 보안 구조, 세부 적인 보안 기술 등을 정의한다. X.iptvsec-1에서는 크게 컨텐츠 보안과 서비스 보안이라는 두 가지 개념으로 나누어 IPTV 서비스에 대한 보안 기술을 설명한다. 컨텐츠 보안이라 함은 제공되는 컨텐츠에 대한 복사 방지, 재분배 관리 및 불법적인 컨텐츠에 대한 추적 등이 가능하도록 보장하는 기술이고, 서비스 보안이란 서비스에 접근제어를 위한 보안 기술로서 인가된 사용자가 허가된 서비스에 접근하여 서비스에 포함된 컨텐츠를 사용할 수 있도록 지원하는 기술이다 [9].

IPTV 서비스에서 활발하게 논의 및 적용되고 있는 컨텐츠 보호 기술에는 기존 케이블 TV 환경에서 방송 수신 제한을 위해 사용되고 있는 CAS (Conditional Access System) 기술과 [10] 컨텐츠를 보호하기 위한 DRM (Digital Rights Management) 기술이 [11] 많은 관심을 받고 있다. CAS 기술은 전달되는 컨텐츠를 암호화 키로 암호화하여 전달함으로써 적법한 사용자만이 서비스에 접속하여 서비스에 포함된 컨텐츠를 사용할 수 있는 IPTV 수신 제한 기술이다. 이를 위해 CAS 시스템에는 켄텐츠를 암호화하고 복호화 하는데 필요한 키 관리 기술이 포함되어 있다. 현재 IPTV 서비스 환경에서 CAS 시스템을 이용하여 서비스 제공업자와 STB 간에 전달되는 컨텐츠를 보호하는 방법이 활발하게 논의 및 적용되고 있다.

최근 IPTV 환경이 점차 개방형 IPTV로 발전함에 따라, 댁내에서 사용되는 IPTV 단말의 경우도 다양한 형태로 발전하고 있다. 이러한 환경에서 사용자는 노트북, 휴대폰, PDA와 같은 댁내에 존재하는 다양한 IPTV 서비스 가용 단말을 통해 IPTV를 시청할 수 있다. 따라서 STB에서 댁내 사용자가 선택한 IPTV 가용 단말들로 컨텐츠를 재분배하는 것이 필요하다 [12]. 그러나 CAS 시스템은 서비스 제공업자와 STB 구간의 컨텐츠는 보호할 수 있지만, 댁내 STB에서 휴대 단말로 컨텐츠를 재분배하기 위해서는 재암호화 과정이 필요하다. 이때 STB에서는 사용자의 IPTV서비스 가용 단말별로 컨텐츠를 재암호화하여 분배해야 하기 때문에 오버헤드가 발생한다. 또한, 수익성 창출에 민감한 IPTV 사업자 측면에서는 STB에서 등록된 IPTV 서비스 가용 단말에게만 컨텐츠가 분배되도록 관리할 수 있어야 한다. 따라서 개방형 IPTV 환경에서 효율적이고 안전한 댁내 컨텐츠 분배기법이 필요하다.

본 논문에서는 기존 CAS 시스템의 수정을 최소화하면서 효율적이고 안전하게 댁내에서 IPTV 컨텐츠를 재분배하는 기법을 제안한다. 제안 기법은 분할된 RSA 개인키를 IPTV 사업자가 댁내의 IPTV 가용 단말에게 각각 분배하여, 암호화된 IPTV 컨텐츠를 복호화할 수 있는 서비스 키를 복원할 수 있도록 한다. 이는 STB에서 IPTV 가용 단말에게 컨텐츠를 재분배할 때, 기존기법에서 처럼 개별 단말별로 스크램블된 컨텐츠를 재암호화하는 과정을 요구하지 않고, IPTV 사업자 측에서 등록된 단말에게만 IPTV 컨텐츠 자체를 재분배할 수 있도록 관리할 수 있다. 또한 제안기법은 기존 시스템에 대한 수정이 적으면서 기존과 동일한 보안 수준을 유지한다.

논문의 구성은 다음과 같다. 2장에서는 관련 기술인 CAS 시스템과 기존 RSA 분할 기법을 살펴보고, 3장에서 제안하는 댁내 컨텐츠 재분배 기법을 살펴본다. 4장에서 제안 기법에 대한 안전성 및 성능을 평가하고, 5장에서 본 논문의 결론을 맺는다.

II. 관련 연구

2.1 Open IPTV 환경에서 CAS 시스템

CAS는 방송 수신제한시스템으로 현재 스카이라이프 및 위성 DMB (Digital Multimedia Broadcasting)에서 사용되고 있으며, IPTV 서비스에서도 유료 컨텐츠를 적법한 사용자에게 안전하게 전달하기 위한 핵심 기술로 논의되고 있다. 또한 이 시스템은 STB를 이용하여 컨텐츠 전달에 필요한 액세스 인증을 수행하며, 이를 위한 여러 단계의 키 관리 시스템을 사용한다. 사용자가 컨텐츠를 사용하기 위해서는 적법한 절차에 따라 허가한 키를 인수 받아야 하고, 허가된 올바른 키를 전수 받은 사용자만 컨텐츠를 시청할 수 있다.

CAS의 키 관리 시스템은 다단계의 키 구조를 갖으며, 그림 1과 같이 상위 단계의 키가 하위 단계의 키를 암호화 하고, 최고 단계의 키는 스마트 카드를 이용하여 물리적 방법을 통하여 전송된다. 이러한 키 관리 시스템은 스트리밍 서비스 암호화로 인해 발생할 수 있는 잦은 키 사용에 대한 부담을 분산시킨다. 또한, 키를 분배 받은 사용자로 하여금 직접 서비스에 필요한 키를 연산하도록 하여 관리자가 모든 가입자에 대하여 동일하게 암호화된 컨텐츠를 제공할 수 있게 한다. 이와 같이 CAS 기술은 콘텐츠 운영 정책에 관한 키 관리 기술과 CAS의 보안을 위한 하드웨어적인 기술을 접목시켜 안전성을 유지하면서 간단한 구조를 갖추고 있다.

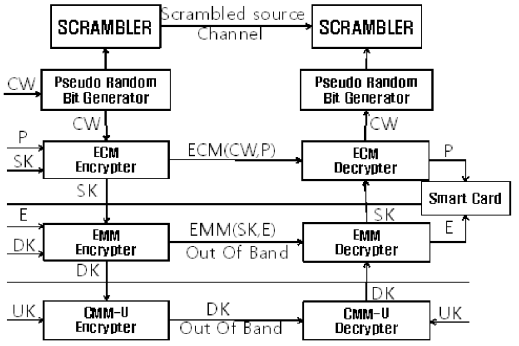

그림 1. CAS시스템의 키 관리 구조
Fig. 1. Key management System on CAS

CAS 시스템의 동작 과정을 구체적으로 살펴보면, 그림 1과 같이 방송 사업자는 스크램블 되어 전달된 컨텐츠를 필요한 복호화 키와 수신 조건을 포함한 ECM (Entitled Control Message)을 방송과 함께 송출한다. ECM을 복호화하기 위한 키는 서비스에 대한 수신자격 정보와 함께 EMM (Entitled Management Message)에 실어 사용자에게 방송망이 아닌 별도의 채널을 통해 전송한다. ECM에는 각 프로그램 또는 채널 별로 생성된 CW (Control Word)가 SK에 의해 암호화되어 포함되고, 이 정보는 미디어 스트림을 통해 오디오 및 비디오 컨텐츠들과 함께 전달된다. 이때 함께 전달된 제어 단어는 방송 스트림을 복호화 하는데 사용되고 변경 주기가 빠르다. EMM에는 가입자의 수신자격 정보와 CW를 복호화하기 위한 SK가 포함되어 있으며, 일반적으로 스마트 카드에 저장된다. 저장된 정보는 적법한 사용자의 정보가 변경되었을 때, 또는 서비스 사업자에 의해 주기적으로 EMM을 통해 업데이트 된다. EMM을 통해 수신자격 정보와 SK를 수신하면 사용자는 CW로 암호화되어 전달되는 컨텐츠를 복호화하여 시청할 수 있다.

현재 IPTV 환경은 사용자가 댁내에서 다양한 IPTV 가용 단말을 통해 언제, 어디서든 IPTV를 사용할 수 있는 개방형 IPTV 환경으로 발전하고 있다. 그러나 기존 CAS 시스템은 STB에서 컨텐츠가 재분배되는 개방형 IPTV 환경에 적합하지 않다. 왜냐하면 개방형 IPTV 환경에서 CAS는 STB를 통해 수신된 컨텐츠를 댁내에서 사용자가 원하는 IPTV 단말로 컨텐츠를 재전송 할 때, 방대한 컨텐츠의 재암호화 과정을 수행해야 하는 것과 수익 창출의 근원이 되는 컨텐츠의 자유로운 이동을 IPTV 사업자가 관리하는 것이 어렵기 때문이다. 따라서 개방형 IPTV환경에서 이러한 문제점을 보완하기 위

한 방안이 필요하다.

표 1은 본 논문에서 사용된 약어를 정리한 내용이다.

표 1. 약어표
Table 1. Abbreviation and Notation

CAS	Conditional Access System
CP	Contents Provider
cRSA	Combined RSA
CW	Control Word
d_c	Private key for CP
d_m	Private key for smart card
d_s	Private key for STB
d_u	Private key for UD
DK	Distribution Key
E	Empowered Message
ECM	Entitled Control Message
EMM	Entitled Management Message
mRSA	Mediated RSA
P	Policy of Contents
RSA	Rivest Shamir Adleman
SK	Service Key
STB	Set-Top Box
TA	Trust Authorities
UD	User Device
UK	Unique Key
VSS	Video Streaming Server

2.2 댁내 컨텐츠 분배를 위한 요구 사항

본 논문에서는 개방형 IPTV환경에서 댁내 컨텐츠를 안전하게 재분배하기 위한 고려사항을 다음과 같이 정의 한다.

- 재분배 되는 방송 컨텐츠의 안전성 및 효율성
- 기존 시스템과의 연동

재분배 되는 방송 컨텐츠의 안전성을 보장하기 위해서 개방된 IPTV 망에 접속을 요구하는 가용 단말을 올바르게 판별해야 한다. 또한 각 단말과 STB 간의 통신내용은 다른 인가 장비로부터 안전해야한다. 따라서 이를 만족하기 위한 STB와 가용단말간에 보안채널을 형성할 필요가 있다. 그러나 실시간 방송되는 컨텐츠를 채널별로 재암호화 한다는 것은 연산량에서 많은 오버헤드를 증가시킬 뿐 아니라, 각 가용단말에 대한 전송 대역폭이 요구되므로 효율성이 떨어진다. 그러므로 안전성과 효율성을 모두 고려한다면, 기존의 시스템으로 암호화된 방송 컨텐츠를 변형 없이 이용하는 것이 유리하다.

기존 시스템을 유지한다고 했을 때, 키 관리 시스템의 일부를 수정하여 가용 단말에게 전송해야 하며, 다음과 같이 키 분배 정책에 대해 다음과 같은 고려가 필요하다. 첫째, 키 전송 주기를 고려해야 한다. 전달되는 키의 갱신 기간이 너무 길면 빈번한 가입과 탈퇴에 적절하지 못하고, 너무 짧으면 키 전송에 관한 오버헤드가 크다. 다시 말해, CW를 재가공하여 전송할 경우 CW의 주기가 짧기 때문에 재가공 작업에 대한 오버헤드가 크다. 반면 UK (Unique key)와 DK (Distribution Key)의 경우 전송주기가 길기 때문에 오버헤드는 적으나 한 번의 가입으로 구매하는 사용기간이 다소 길어지므로 갱신 주기가 적당하지 않다. 둘째, 가용 단말에 합당한 권한의 키가 전송 되어야 한다. 구매한 컨텐츠에 관한 권한정보 (E)가 컨텐츠의 권한 정보 (P)와 비교하는 과정이 STB에 구현되어 있으며, STB에는 권한에 대한 정보를 임의로 수정할 수 없도록 스마트카드 등을 이용하여 하드웨어로 보호되어있다. 기존 시스템의 안전성을 유지하기 위해서는 위와 같은 권한 정보 비교 과정이 STB에서만 수행되어야 하며, 따라서 가용단말에게 DK 미만의 정보가 전송되는 것이 바람직하다.

기존 시스템과의 연동은 사업자에게 새로운 기술을 도입하는데 들어가는 비용과 직접적인 연관이 있다. 또한 새로운 기술을 도입함에 있어서 투자비용과 함께, 기술 도입으로 인한 수익성이 고려되어야 한다. 댁내 컨텐츠 이용에 따른 추가적인 사용자를 등록하지 않는 경우 STB 이후에 댁내에서 컨텐츠가 어떻게 운영되는지는 알 수 없게 되어 추가 과금이 불가능하다. 반대로 서버에 사용자를 등록하는 경우는 서버에 대한 부하를 감수하는 반면, 추가 등록에 대한 추가 과금이 가능해 진다. 따라서 키 분배는 사업자, STB 및 UD가 모두 참여해야 한다.

2.3 mRSA

RSA기법은 공개키 기반의 서명기법이며 다음과 같은 서명 준비과정이 요구된다.

- 임의의 소수 p와 q를 선택
- $n = p \times q$로 정의
- $\phi(n) = (p-1)(q-1)$
- e를 Z_n에서 임의로 선택
- $e \times d \equiv 1 \pmod{\phi(n)}$를 만족하는 d를 계산

위에서 정의한 e는 공개키로 CA에 의해 신뢰적으로 공개되고, d는 개인키로 서명자만이 알도록 한다. 서명을 위하여 메시지 (M)에 관해 $h(M)^d \pmod{n}$으로 서명하면, 검증자는 $(h(M)^d)^e$를 계산하여 $h(M)$과 동일하면, 올바른 서명으로 인정한다. mRSA (mediated RSA) [13] 기술은 RSA 서

명기법의 변형된 형태로 비밀키가 덧셈으로 나누어진 기술이다. mRSA는 RSA와 동일하게 키를 설정하고, 추가적으로 SEM (Security Mediator)을 사용자가 신뢰할 수 있는 서버로 정의하여 비밀키의 일부를 관리한다. 동작방법을 구체적으로 설명하면 식 (1)과 같이 비밀키를 나눈 후 d_A는 사용자가 d_{SEM}은 SEM이 보관하고 있다가, 식 (2)와 같이 연산하여 서명을 생성한다. 검증하는 과정은 RSA와 동일하다.

$$d = d_A + d_{SEM} \quad (1)$$

$$h(M)^d = (h(M)^{d_A} \times h(M)^{d_{SEM}}) \bmod n \quad \cdots\cdots (2)$$

mRSA서명의 경우 빠른 서명을 목적으로 한다. 따라서 SEM은 연산능력이 뛰어난 프로세서로 가정하고, 연산량을 고려하여 $d_A \ll d_{SEM}$로 설정한다. SEM은 우수한 연산능력으로 $h(M)^{d_{SEM}} \pmod n$을 빠르게 계산하고, A는 적은 연산으로 $h(M)^{d_A} \pmod n$을 빠르게 계산하므로 단시간에 서명결과를 얻어 낼 수 있다. mRSA의 경우 제안하는 기법과 유사하게 키 분할 방법에 대하여 다루고 있으며, 이러한 키 분할 기법을 이용하여 제안기법과 비슷하게 댁내 컨텐츠 분배가 가능하도록 설계 할 수 있다.

III. 제안기법

3.1 기본 아이디어

본 논문에서는 RSA의 서명기법에서 키를 분리하여 사용하는 cRSA (combined RSA) 서명을 제안한다. 기존 mRSA는 RSA 키를 덧셈으로 나누는 반면, 제안하는 cRSA 서명은 응용환경에 따라 RSA키를 곱셈으로 양분한다. 각각의 서명기법은 서로 다른 장단점을 가지고 있다. 특수한 상황에서 사용될 수 있다. cRSA에서는 각각 n명의 서명자가 존재할 수 있고, m명의 검증자가 존재할 수 있다. d 는 비밀키, e는 공개키, d_1, d_2, e_1, e_2는 각각 비밀키 1, 비밀키 2, 공개키 1, 공개키 2로 정의한다. 구체적인 알고리즘을 설명하면, 우선 RSA와 동일하게 두 임의의 소수 p, q를 선택하고 $pq = n$ 으로 정의한다. 또한 $\phi(n) = (p-1)(q-1)$로 정의한다. 랜덤한 수 e를 선택하면 $\phi(n)$에 대한 e의 역수 d를 구한다. 이 때, d는 서명을 위하여 비밀키로 사용되고, e는 검증을 위하여 복호키로 사용된다. 서명을 2단계로 나누기 위해서 d를 2개로 나눌 수 있는데, $d = d_1 + d_2$로 정의하면, 서명시 $M^{d_1}M^{d_2} = M^d$로 서명이 가능하다. 반면 $d = d_1 \times d_2$로 정의하면, 서명시 $(M^{d_1})^{d_2}$가 되어 e로 복호화 할 수 있게 된다. 즉 덧셈으로 비밀키를 나눈 경우, 같은 메시지에 관하여 각각 서명한 정보를 곱셈으로 결합하여야 하고, 곱셈의 경우 이미 서명한 정보에 관하여 다시 한 번 서명해야 올바른 서명 값을 얻어 낼 수 있다. 곱셈으로 서명과정을 나누었을 때, $d_1 \times d_2 \equiv d(\bmod \phi(n))$이 성립한다. 즉, cRSA에서 n개의 사용자가 참여시, 식 (3)에 맞게 d_i를 구한다.

$$d_1 \times d_2 \times d_3 \times \ldots \times d_{n-1} \times d_n \equiv d(\bmod \phi(n)) \quad \cdots\cdots (3)$$

3.2 제안하는 댁내 컨텐츠 분배 기법

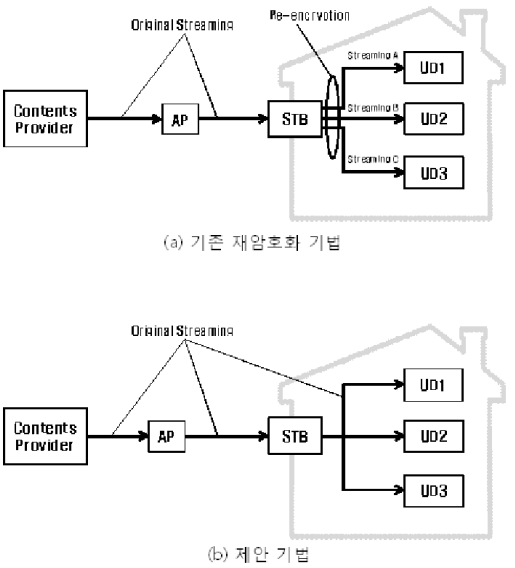

그림 2 . IPTV의 컨텐츠 분배 전송 구조 비교
Fig. 2 . Contents distributions system of IPTV

그림 2는 단순한 재암호화 기법을 이용할 경우(a)와 본 논문에서 제안하는 댁내 컨텐츠 분배 기법을 이용할 경우(b)의 컨텐츠 분배구조를 나타낸다. 개방형 IPTV환경에서 IPTV 사업자는 SK (Service Key)가 포함된 여러 개의 EMM (Entitled Management Message)과 컨텐츠를 서로 다른 채널을 통해 STB에게 전송하고, STB는 보호된 컨텐츠에 대해서 아무런 작업을 수행하지 않고 UD (User Device)에게

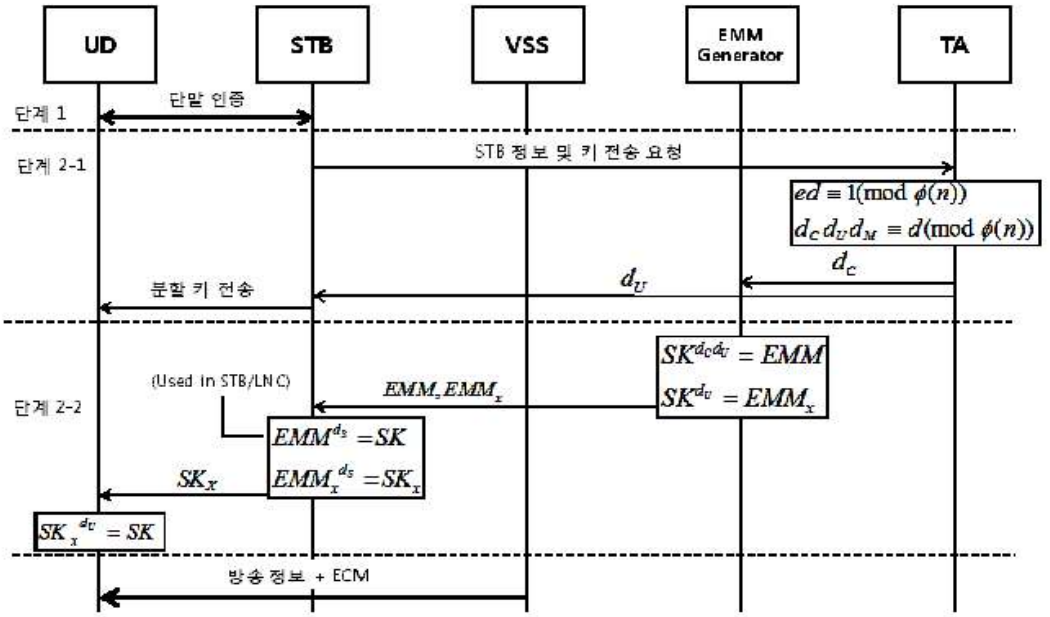

그림 3. 제안 프로토콜
Fig. 3. Proposed scheme

전송한다. 여기서, EMM은 STB의 EMM을 포함하여 등록한 UD의 개수만큼 보내지며, STB용 EMM은 EMM으로, UD1을 위한 EMM은 EMM_1 으로 UD2를 위한 EMM은 EMM_2로, 임의의 UDx는 EMM_X로 표기하도록 하였다. EMM_X의 경우, 사업자가 송신하면, STB 에서 임의로 재가공하여 UDx에게 전송하도록 하였다.

제안하는 댁내 컨텐츠 분배 기법에서 UD들은 단계 1을 통해 STB에 등록하고, 사용자가 댁내에서 IPTV 서비스를 이용할 때에는 단계 2를 수행한다.

- 단계 1 : 단말 (UD) 등록 단계
- 단계 2 : 댁내 이용 단계

단계 1은 UD를 올바르게 인식하기 위한 단계로, 사용자가 물리적인 방법을 통하여 STB와 UD간의 보안 채널을 형성하는 단계이다. 단계 2는 인식된 UD를 이용하여 댁내에서 서비스를 이용할 수 있도록 설정하는 단계이다. 이 단계에서는 인식된 UD들을 서비스 제공업자에게 등록하는 과정이 포함되며, 등록과정에서 과금을 위한 프로토콜이 추가 될 수 있다.

3.2.1 단말 등록 단계 (단계 1)

본 단계는 인가된 UD를 판별하기 위한 단계이다. 본 단계를 수행하기 위하여 STB는 기본적인 접속암호를 설정하고, 이후 사용자가 UD를 이용하여 STB에 접속하고자 할 때, STB가 UD에게 접속암호를 질문 한다. 접속암호를 이용하여 STB와 UD간의 암호화 세션을 설정할 수 있다. 본 논문에서는 접속암호의 성질에 대해서 정의하지 않으며, 최초 UD와 STB와의 상호인증이 성공하고 대칭키가 공유되면, 양자 간의 보안채널이 형성되었다고 가정한다. 하지만 양자 간의 보안채널이 형성되어 안전한 컨텐츠 분배가 가능하더라도, 재암호화에 필요한 연산량과 전송대역폭을 고려한다면 결코 효율적이지 못하다. 따라서, 단계 2를 거쳐 댁내에서 효율적으로 서비스를 받는다.

3.2.2 댁내 이용 단계 (단계 2)

단계 2에서는 수정된 RSA 키 분배 방법을 이용하여 DK를 암호화하고, 암호화된 DK를 이용하여 SK를 전송 받도록 설계한다. 우선 RSA 키를 생성하고 공개키 d를 d_c, d_u, d_m으로 분할한다. 상용화 된 RSA의 경우 e의 연산량을 고려하여 일반적으로 65537로 고정하여 사용하므로 [14] d_c, d_u, d_m은 각각 EMM Generator, UD, STB를 위하여 사용한다. 단, d_m는 스마트카드를 이용하여 사전에 전송하도록 하며 올바른

복호화를 위해 $d_s = d_m \times e$로 정의하고, STB에서 SK 복원 시 사용한다.

단계 2는 UD이 사업자에게 등록하기 위한 단계 (단계 2-1)와 사업자가 UD에게 SK를 전송하는 단계 (단계 2-2)로 분류한다. UD는 단계 2-1을 통해 d_u 정보를 전송 받는다. d_u는 STB의 DK가 사용기간이 만료되거나, 사업자가 더 이상 EMM_x를 전송하지 않을 때까지 유효하다.

3.2.2.1 분할키 요청 단계 (단계 2-1)

단계 2-1에서는 UD가 서비스 제공업자 (TA)에 등록하는 과정이다. 이 과정은 서비스가 지속되는 동안 최초 1회만 수행되며, 서비스가 끝나면 할당된 키가 만료되도록 설정한다. 또한 STB의 키가 만료되면, 동시에 모든 UD의 키를 사용할 수 없게 된다. 그림 3에서와 같이 단계 2-1에서 최초 STB는 해당 UD가 사용할 키를 분배받기 위해 사업자 서버인 TA에게 UD 키 (d_u)를 요청한다. TA가 사용자의 키 생성 요청을 받으면, 해당 STB의 아이디를 이용하여 d, d_m를 검출한다. 이후 3장 1절에서 설명한 방법으로 $d_c d_u d_m \equiv d \pmod{d}$를 만족하는, d_c, d_u를 계산한다. TA는 d_c를 EMM 생성기에게, d_u는 STB를 통해 UD에게 각각 전송한다.

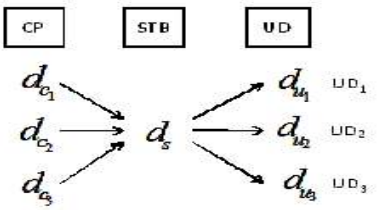

그림 4. 제안하는 키 관리구조
Fig. 4. Proposed key management

3.2.2.2 서비스키 전송에 필요한 단계 (단계 2-2)

이 단계는 서비스를 이용하기 위해 필요한 SK를 전송 받는 과정으로, 단계 2-1에서 유효한 키(d_u)를 다운받은 UD에 한해서 SK가 갱신되거나, 서비스에 접속시 1회 시행된다.

그림 4는 제안 프로토콜에서 관리되는 키 구조를 요약한 내용이다. 각 UD를 위한 d_u, d_c 키 쌍이 생성 및 관리되며, d_m의 경우 스마트카드에 보관하여 안전하게 전송하도록 한다. STB에서의 계산 편의를 위하여 $d_s = d_m e$로 정의한다. 키 전송이 시작되면, CP에 속한 EMM생성기는 EMM_x의 생성을 위하여 SK를 SK^{d_c}으로 암호화한다. EMM_x가 STB에 도달하면, STB는 이를 $(SK^{d_c})^{d_s}$로 1차 복호화를 시도하고, UD에 의해 최종 $((SK^{d_c})^{d_s})^{d_u} = SK$ 로 최종 복호화 된다. SK는 STB 내부에서 CW를 복호화 하는데 사용되며, 이후 VSS (Video Streaming Server)에서 전송하는 컨텐츠를 UD에서 이용할 수 있다.

IV. 제안 기법 분석

4.1 안전성 분석

4.1.1 에라토스테네스 소인수 분해의 방법을 이용한 $\phi(n)$ 추측 공격

에라토스테네스의 소인수 분해 방법이란 소인수 분해의 대상이 되는 수와 작은 소인수들로 이루어진 어떠한 수를 유클리드 알고리즘을 통하여 최대공약수를 구해내는 방법[15]으로 아래와 같은 공격 시나리오를 생각할 수 있다.

다음과 같은 상황을 가정한다. 2명의 서명자와 1명의 검증자가 있다. 서명자 1은 최종 서명권한을 갖는 자이고 서명자 2는 서명 메시지를 생성하는 자이다. 서명자 2가 임의의 수 d_2를 설정하여 서명자 1에게 전달하면 서명자 1은 자신이 소유한 d 를 이용하여 서명자 2가 설정한 임의의 수d_2로부터 d_1을 계산한다. 서명자 2가 메시지를 생성하여 m^{d_2}로 서명하면, 서명자 1은 이를 확인하고 $(m^{d_2})^{d_1}$으로 최종 서명하여, 본 서명이 효력을 발휘한다. 이 때 악의적인 서명자 2는 서명자 1이 소지한 d를 추측하기 위해, 작은 소수들의 집합으로 이루어진 d_2를 선택하여 서버에 전송한다. 만약 d_2가 $\phi(n)$이 서로소가 아닌 경우에 유클리드 호제법을 이용하여 d_1을 구할 수 없게 된다. 따라서 서명자 1은 서명자 2에게 다른 d_2를 선택하도록 요구할 것이고, 결국 악의의 서명자 2는 자신이 선택한 d_2가 $\phi(n)$이 공통 인자를 가지고 있다고 추측하게 된다. 본 논문에서는 키 선택의 권한을 CP가 갖고 있기 때문에 사용자가 임의로 많은 소인수로 구성된, 충돌이 의심되는 수를 키로 지정 할 수 없으며, 위 가정과 같이 여러 번의 키 선택 기회가 주어지지 않기 때문에 에라토스테네스의 소인수 분해 방법을 이용한 공격이 차단된다.

4.1.2 Common Modulus Attack

d_{u_1}과 d_{u_2}가 서로 소일 때 $rd_{u_1} + sd_{u_2} = 1$를 만족하는 r과 s를 확장 유클리드 알고리즘에 의해서 구해질 수 있다는

것이 Common Modulus Attack의 핵심이다. 본 논문에서 d_{u_1}과 d_{u_2}은 각 UD1과 UD2에게 나누어진 분할된 키이고, 따라서, r과 s는 d_{u_1}과 d_{u_2}가 서로 소일 때 두 사용자의 불법적인 공조로 인하여 쉽게 구해지고 이로 인해 $EMM_1^r \times EMM_2^s = SK$가 계산되어 SK가 노출된다. 이와 같은 공격을 예방하기 위해서 모든 d_u에 관하여 항상 서로 소이어야 하는 조건이 생긴다. 하지만, 본 논문에서와 같이 d_{u_1}과 d_{u_2}을 이미 알고 있는 UD의 공조가 의미가 없거나, 권한을 상실한 UDx가 공격에 가담할 경우 현재 가용한 서비스 가입자에 한해 EMM_x를 전송하도록 함으로 $EMM_1^r \times EMM_2^s = SK$가 성립하지 않아 SK를 추출하기 위한 공격이 불가능 하다.

4.2 성능 비교 분석

일반적인 보안 세션을 이용하여 컨텐츠를 분배하였을 경우에 STB는 VSS (Video Streaming Server)가 전달한 컨텐츠를 복호화 하고, UD에 관하여 각각 암호화를 진행한다. 이 방법은 정책적인 측면에서 컨텐츠 사용에 대한 감시가 이루어지지 않아 새로운 기술 도입이 수익성 창출에 아무런 도움이 되지 않을 뿐만 아니라, 무분별한 컨텐츠 유출이 우려된다. 성능적인 측면을 고려하면, TA가 각 가입자가 소지한 UD에 관하여 키 쌍을 생성 및 저장할 필요가 없고, EMM 생성기가 가입자당 각 1개의 EMM만을 전송하면 되지만, STB에서 실시간 전송되는 컨텐츠에 관하여 UD마다 재 암호화를 수행해야하므로 연산량이 폭증하고, 이에 따른 대역폭이 요구되므로 UD, STB간의 유무선 채널 환경에 따라 한정된 UD만이 시청 가능해 진다. 다른 컨텐츠 분배 방법으로 각 UD에게 모두 스마트카드를 발행하는 것을 고려해 볼 수 있으나, 이 방법은 사용자가 여러 장의 카드를 일일이 관리하기 번거로울 뿐 아니라, 카드 발행에 대한 막대한 비용이 추가되고, 카드가 장착되지 않던 기존 UD에 관한 하드웨어적 솔루션이 요구되어 사실상 불가능하다.

논문에서는 키 전송을 위하여 가능한 두 가지 방법과 비교분석을 하였다. 첫째는 2중 서명기법을 이용하였을 경우와 제안 기법을 사용하였을 때의 성능차이이고, 둘째는 기존에 제시되었던 mRSA기법을 도입되었을 때와 본 논문이 제시한 기법을 도입하였을 때의 성능차이다.첫째, 2중 서명기법을 사용하였을 경우, 모든 STB와 UD가 TA의 신뢰를 얻었다고 가정하고, 1차적으로 EMM생성기에서 SK를 STB의 비밀키로 암호화하고, STB에서 이를 복호화한 뒤, 각 UD의 비밀키로 재암호화해야 한다. 둘째, 본 논문에서는 기존 mRSA 기법과 성능 개선을 위해 수정된 mRSA가 각각 개방형 IPTV 환경에 적용되었을 때를 가정하여 제안 기법과 성능 측면에서 비교 분석한다. mRSA를 적용한 기법은 제안기법과 동일한 메시지 교환이 요구된다. 즉, 다음과 같이 기존 mRSA 기법이 댁내 컨텐츠 분배 기법에 적용되는 것으로 생각해 볼 수 있다. 먼저, 단계 1에서 UD와 STB간에 안전한 채널이 생성되면, UD 등록을 위하여 단계 2-1에서 STB는 자신의 정보를 TA에게 전송한다. TA는 UD로부터 키 요청을 받으면 제안한 논문과 같이 d_u와 d_c를 mRSA기법에 따라 생성하고 d_u를 UD에게 안전하게 전송한다. 단계 2-2에서는 서비스 시작을 위하여 EMM 생성기는 제안기법과 동일하게 $SK^e = EMMe$, $SK^{e(d_c + d_u)} = EMM$, $SK^{ed_c} = EMM_x$로 계산하고 이를 STB에게 전송하면, STB는 $EMMe^{d_s} \times EMM = SK$로 계산하여 자신의 SK를 복호하고, $EMMe$와 $(EMM_x \times SK^{d_s})^e = SK_x$를 UD에게 전송한다. 끝으로 UD가 $EMMe^{d_u} \times SK_x = SK$를 계산하면 SK가 복원된다.

표 1은 재암호화 기법과 mRSA 기법 및 제안 기법을 사용한 방법을 비교 분석한 내용으로 [16] k는 가입자가 소지한 UD의 개수이며 n은 RSA의 n을 의미한다. 표가 나타내듯이, 2중 서명기법은 TA - STB구간의 전송량과 TA연산량 측면에서 우수한 성능을 보인다. STB에서 재암호화 과정이 추가되기 때문에, 컨텐츠 분배에 관한 통제가 가능하다고 하더라도, STB내에 각 UD에 관한 인증서가 보관되어야 하므로, 메모리에 의해 UD의 개수가 제한되거나, STB를 교체해야 한다. 또한 CP가 모든 UD에 대해서 단 1개의 EMM을 송신하기 때문에 사용자가 컨텐츠에 대한 모니터링이 불가능해 진다. 제안 기법과 mRSA기법을 비교하면, 제안기법이 구간별 전송량에서 기존 mRSA 방법보다 우수한 성능을 보인다. 또한 각 도메인에서 연산량을 고려해 볼 때, 제안 방법이 모든 노드에서 mRSA 방법보다 연산량이 더 적다.

표 1. 제안 기법 성능 비교
Table 1. performance comparison of proposed scheme

	재암호화 기법	mRSA 기법	제안기법
서명 참여 노드	STB, UD	TA, STB, UD	TA, STB, UD
TA - STB 전송량(bit)	$\log n$	$(2+k)\log n$	$(1+k)\log n$
STB - UD 전송량(bit)	$k\log n$	$2k\log n$	$k\log n$
TA 연산량	$O(\log^3 n)$	$O((2+k)\log^3 n)$	$O((1+k)\log^3 n)$
STB 연산량	$O((1+k)\log^3 n)$	$O((1+2k)\log^3 n)$	$O((1+k)\log^3 n)$
UD 연산량	$O(\log^3 n)$	$O(\log^3 n+\log^2 n)$	$O(\log^3 n)$

V. 결론

IPTV는 컨텐츠 보안을 위하여 일반적으로 CAS 시스템을 사용한다. CAS 시스템에서는 다단계 키 관리기법과 스마트 카드를 이용한 하드웨어 방어 시스템이라는 두 가지 주요한 보안 기술이 응용되고 있다. 하지만 이로 인하여 하드웨어적으로 방어가 용이하지 않은 개인 PC나 기타 서비스 가용한 UD까지의 서비스 확장에 어려움을 겪고 있다. 이는 사용자로 하여금 UD를 불문하고 권리 구매에 의한 접근이 용이하도록 구성되는 개방형 IPTV 환경에 적합하지 않다. 또한 단순히 UD와 STB 간의 보안 세션을 생성하여 컨텐츠를 재분배하는 방식은 연산량과 전송량 측면에서 많은 오버헤드를 발생시키며, IPTV 사업자가 참여하지 않는 컨텐츠 분배는 불법적인 컨텐츠 유출을 방조할 수 있다. 따라서 본 연구를 통해 개방형 IPTV 환경 구축을 위하여, 안전하고 효율적인 댁내 컨텐츠 분배 방법을 제시하였다. 또한 제안 기법은 제안 기술 도입에 필요한 비용을 최소화하기 위하여 기존 시스템을 상당부분 유지하도록 하였으며, 사업자 측면에서 추가적인 컨텐츠 이용에 관하여 수익창출이 가능하도록 하였다. 본 논문에서는 개방형 IPTV 서비스를 댁내 환경에서 안전하게 이용할 수 있는 방안을 제시하였으나, 인가받은 UD가 댁외 환경으로 이동할 경우의 안전한 컨텐츠 제공 방안에 대해서는 향후 추가 연구가 필요하다.

참고문헌

[1] VOD/IPTV, *http://www.tvover.net/2006/11/28/How+To+Build+Your+Own+IPTVVoD+System.aspx*

[2] ITU-T FG IPTV-ID-0089, "EPG system architecture and it's requirements," July 2006.

[3] T-Commerce, *http://www.iptvdictionary.com/iptv_dictionary_Television_Commerce_definition.html*

[4] R. Sharpe, J. Heiles, L. Hong, M. Deschanel, W. Yiyan, J. Maisonneuve, and L. Wei, "An Overview of IPTV Standards Development," IEEE Transactions on Broadcasting, Vol 55, Issue 2, pp. 315-328, Jun. 2009.

[5] H. Imsook, Y. Jaeheung, C. Junkyun, J. Sanggu, and K. Soohyung, and C. Youngmin, "Adoption of IPTV under the convergence of broadcasting and telecommunications," Advanced Communication Technology, ICACT 2009, pp 15-18, Feb. 2009.

[6] ITU-T X.iptvsec-1, "Draft Recommendation X.iptvsec-1: IPTV security aspects," Apr. 2008.

[7] ITU-T X.iptvsec-2, "The draft Recommendation for X.iptvsec-2: Functional requirements and mechanisms for secure transcodable scheme of IPTV," Feb. 2009.

[8] ITU-T X.iptvsec-3, "Proposed third draft text on Recommendation X.iptvsec-3 : Key management framework for secure IPTV services," Feb. 2009.

[9] S. O. Hwang, "Content and Service Protection for IPTV," IEEE Transactions on Broadcasting, Vol 55, Issue 2, pp 425-436, Jun 2009.

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

[11] DRM, *http://en.wikipedia.org/wiki/Digital_rights_ma nagement#cite_note-0.*

[12] E. Shihab, C. Lin, W. Fengdan, A. Gulliver, and N. Tin, "Wireless Mesh Networks for In-Home IPTV Distribution," IEEE Network, Vol 22, Issue 1, pp. 52-57, Jan. 2008.

[13] Dan Boneh, Xuhua Ding, GeneTsudik, and Chi Ming Wong, "A Method for Fast Revocation of Public Key Certificates and Security Capabilities," In proceedings of USENIX Security, May 2001.

[14] NIST Special Publication 800-78-1,

"Cryptographic Algorithms and Key Sizes for Personal Identity Verification," Aug. 2007.
[15] 이민섭, "*현대암호학*," 敎友社, 280p, 2007.
[16] Big O, *http://en.wikipedia.org/wiki/Big_O_notation*

저 자 소 개

정 서 현

2009 : 숭실대학교 정보통신전자공학부
2009~ 현재 : 숭실대학교 전자공학과 석사과정
관심분야 : 네트워크 보안, 차량 보안, IPTV 보안

노 효 선

2005: 숭실대학교 정보통신전자공학부
2007: 숭실대학교 정보통신전자공학부 석사
2007~ 현재: 숭실대학교 전자공학과 박사과정
관심분야 : 네트워크 보안, 이동 네트워크 보안, IPTV 보안

이 현 우

1993: 한국 항공대학교 정보통신공학
1999: 한국항공대학교 정보통신공학과 석사
2005: 한국항공대학교 정보통신공학과 박사
1995~현재: 한국전자통신연구원 IPTV 인프라연구팀 팀장
2002~현재: BcN포럼 통합망분과 간사
2007~현재: 한국항행학회 학술이사
2008~현재: 대한전자공학회 학회지 편집위원
관심분야 : 이동성제어, 트래픽제어, QoS/QoE

이 정 현

1992: 숭실대학교 전자 계산학과
1995: 숭실대학교 컴퓨터학과 석사
2005: University of California, Irvine 박사
1995~2001: 한국전자통신연구원 연구원
2000~2001: National Institute of Standards and Technology 객원연구원
2005~2008: 삼성종합기술원 수석연구원
2008~현재: 숭실대학교 컴퓨터학부 조교수
관심분야 : 모바일 보안, 네트워크 보안, 클라우드보안, 응용 보안

정 수 환

1985: 서울대학교 전자 공학과
1987: 서울대학교 전자 공학과 석사
1996: University of Washington 박사
1996~1997: Stellar One SW Engineer
1997~현재: 숭실대학교 정보통신전자공학부 부교수
2009~현재: 지식경제부 지식정보보안 PD
관심분야 : 이동 네트워크 보안, 차량 네트워크 보안, VoIP 보안, RFID/USN 보안