情報保護學會論文誌
第 21 卷 第 1 號, 2011. 2

IPTV Flexible-PPC 환경에서의 안전한 콘텐츠 접근 제어 시스템*

강 용 구,† 임 지 환, 오 희 국‡
한양대학교

Secure Contents Access Control System in IPTV Flexible-PPC Model*

Yonggoo Kang,† Jihwan Lim, Heekuck Oh‡
Hanyang University

요 약

제한수신시스템은 IPTV 서비스의 가입자에게 비용을 청구하고 인가된 사용자에게만 서비스를 제공하기 위한 필수적인 요소이다. 현재 IPTV는 PPC(pay-per-channel)와 PPV(pay-per-view) 두 가지 환경으로 서비스되고 있는데, 사용자의 취향에 따라 임의의 채널을 조합할 수 있고 구독기간에 관계없이 개별적인 채널 추가 및 해지가 가능한 F-PPC(Flexible-PPC) 환경이 요구된다. 기존에 제안된 제한수신시스템 기법들을 F-PPC 환경에 적용하기에는 문제점이 존재한다. 본 논문에서는 F-PPC 환경에 적용할 수 있는 4계층 키 구조의 제한수신시스템을 제안한다. 제안하는 시스템은 이진트리를 이용하여 효율적인 키 관리가 가능하고 키 갱신에 요구되는 메시지 통신량이 $O(1)$ 수준이기 때문에 대역폭의 부담이 적다. 따라서 기존의 제한수신시스템에 비해 효율적이고 안전하다.

ABSTRACT

A conditional access system is an essential element in IPTV services enabling service providers to allow authorized access to their services only to paid subscribers. Currently, there are two types of IPTV service models, namely PPC (pay-per-channel) and PPV (pay-per-view). However, a more desirable model would be the flexible PPC model, in which subscribers are free to choose any combination of preferred channels and add/remove channels independently. In this paper, we first point out that a previously proposed key management scheme for F-PPC is not secure. We then propose a new conditional access system using 4-level key hierarchy to realize secure F-PPC services. Compared to existing schemes, the proposed system is very efficient, just requiring $O(1)$ communication for key update.

Keywords: IPTV, conditional access system, CAS, group key

I. 서 론

최근 다양한 기술의 발달과 함께, 전 세계에 걸쳐 멀티미디어 방송 시스템이 서비스 되고 있다. IP망을 이용하여 방송이나 동영상 등 여러 가지 미디어 콘텐츠를 TV 혹은 이동 단말에 제공하는 통신/방송 융합 서비스가 IPTV이다. 이때, 공개 채널을 통해 서비스가 제공되기 때문에 인가된 사용자만 전송되는 프로그

접수일(2010년 5월 31일), 수정일(2010년 9월 24일)
게재확정일(2010년 11월 25일)
* 이 논문은 2010년도 정부(교육과학기술부)의 재원으로 한국과학재단의 지원을 받아 수행된 연구임(No. 2010-0000438).
† 주저자, suhostar@hanyang.ac.kr
‡ 교신저자, hkoh@hanyang.ac.kr

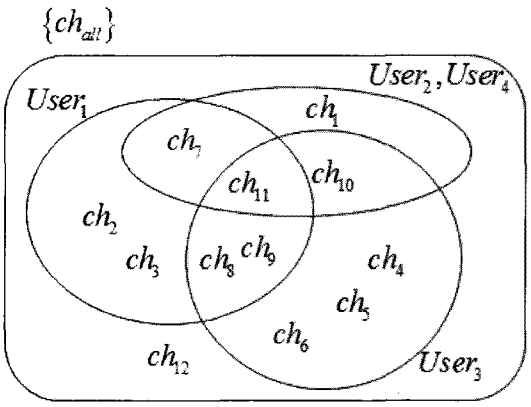
램 데이터에 접근할 수 있도록 하기 위해서는 제한수신시스템이 필수적이다. 그러므로 효율적인 제한수신시스템에 대한 연구가 많이 진행되었다[1-6].

1.1 제한수신시스템

서비스 제공자는 제한수신시스템(CAS, Conditional Access System)을 통해 인가된 사용자에게만 프로그램 데이터에 접근할 수 있도록 한다. 이때 사용되는 기본 함수가 스크램블 함수이다. 암호학적 함수의 일종인 스크램블 함수는 프로그램의 디지털 신호를 섞기 위해 키와 같은 기능을 하는 하나의 CW(Control Word)를 필요로 한다. 제한수신시스템은 의사난수생성기에 CW를 넣고, 그 결과를 통해 원본의 신호를 스크램블링하여 해독하기 어려운 형태의 스트림을 만들어낸 후 그것을 방송한다. 이를 통해 공개채널 상에 전송되는 데이터를 안전하게 보호할 수 있기 때문에 빈번한 CW의 갱신과 그것의 안전한 전송은 중요한 문제이다. 전송되는 신호를 수집하여 분석하여 공격자가 CW를 획득하기 전에, 약 5-20초마다 CW를 갱신한다. 따라서 갱신된 CW를 안전하게 전송하는 메커니즘이 매우 중요하다. 제한수신시스템은 사용자들이 등록할 때 각각에 대한 비밀 정보를 제공한다. 이 비밀 정보는 CW를 암호화할 때 사용하는 키와 같은 역할을 수행하며, 공격자가 이 키를 획득한다는 것은 제한수신시스템을 무력화시키는 것을 의미한다. 공격자가 비밀 정보를 획득하지 못하도록 하는 키 관리 기술이 제한수신시스템에서의 중요한 이슈이다.

1.2 IPTV 서비스 환경

일반적으로 현재 IPTV의 서비스 환경은 PPC(pay-per-channel)와 PPV(pay-per-view) 두 가지 환경으로 나눌 수 있다[2-6]. PPC는 한 사용자가 하나 이상의 채널 그룹을 한 주 또는 한 달 등 일정 기간동안 구독하는 환경을 말한다. 사용자는 구독을 원하는 채널이 속한 그룹을 신청한다. 그러나 일정 기간의 구독료를 지불하기 때문에 원하는 시점에서의 즉각적인 채널 해지가 불가능하고, 서비스 제공자에 의해 채널그룹이 형성되었기 때문에 어떤 하나의 채널을 구독하기 위해 관심 없는 다른 채널까지 구독하게 되는 경우가 생긴다. 반면에 PPV는 프로그램 단위별로 비용을 지불하여 구독하는 환경을 말한다. 사용자는 프로그램 리스트 중에서 보고 싶은 것을 골라 개별적으로 신청한다. 이 환경은 개별적인 요금을 부과하기 때문에 채널그룹보다 비싸고, 새로운 프로그램을 구독할 때마다 구독신청 절차를 거쳐야 하는 번거로움이 있다.



[그림 1] 사용자 스스로 채널 조합이 가능한 F-PPC 환경

이에 따라 PPC와 PPV의 장점을 결합한 F-PPC(Flexible-PPC) 환경이 요구되며, 2008년 Sun 등에 의해 처음 제시되었다[6]. F-PPC 환경은 서비스 제공자가 채널 그룹을 사전에 정하는 것이 아니라, 같이 사용자의 기호에 맞는 채널 조합을 자유롭게 구독할 수 있는 환경을 말한다. [그림 1]은 12개의 채널에 대해 3명의 사용자가 각자 취향대로 채널을 선택한 모습을 나타내었다. 각각의 채널은 서비스 제공자에 의해 제공되는 콘텐츠이며 사용자들은 자신이 원하는 채널들만 선택하여 구독한다. 이렇게 생성된 채널 조합들을 하나의 그룹으로 관리하며, 사용자 2, 4는 같은 채널들을 선택하여 같은 그룹에 속하게 된다. 이는 구독 기간에 관계없이 즉각적이고 개별적인 채널 해지 및 추가가 가능하며, 구독 기간에 따라 적절한 요금을 지불한다. 사용자의 입장에서 자신이 구독하는 채널에 대해서만 요금을 지불하는 F-PPC 환경을 선호한다. 제공되는 채널의 수가 CH개라고 할 때, 생성될 수 있는 채널 조합의 수는 최대 2^{CH}개이다. 그렇지만 사용자가 채널의 조합을 선택하기 때문에 가입된 사용자의 수가 M이라고 할 때 동시에 발생할 수 있는 채널 그룹의 수는 최대 M개다.

1.3 연구 동기 및 논문 구성

F-PPC 환경에서는 기존에 제안되었던 제한수신시스템의 적용이 어렵다. Sun 등이 이 환경에 적합한 제한수신시스템을 제안하였으나, 분석 결과 이 기법에

치명적인 문제점이 존재함을 발견하였다. 본 논문에서는 효율적인 그룹 키 관리 기법을 설계하고, 이를 이용하여 F-PPC 환경에 적합한 안전한 제한수신시스템을 제안한다.

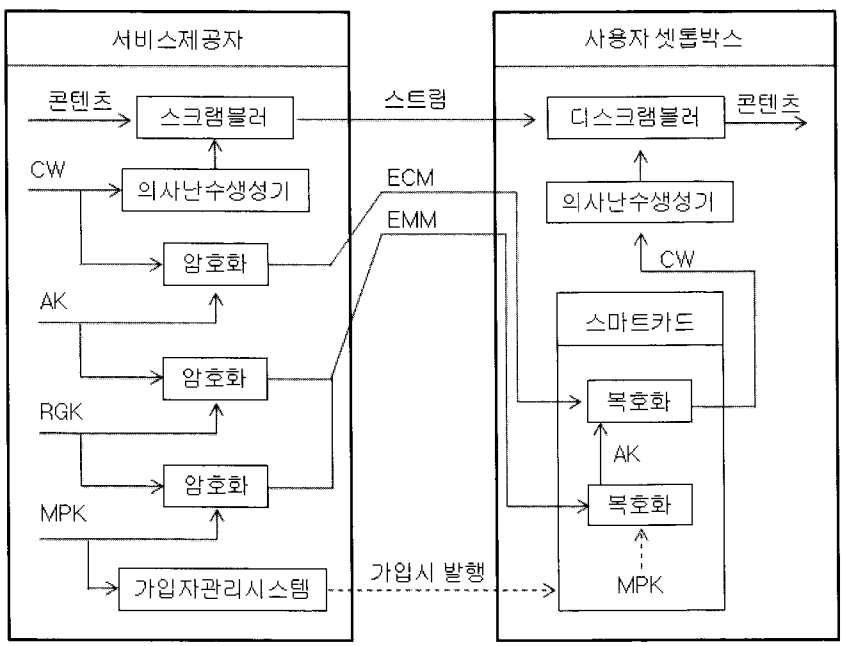
본 논문의 구성은 다음과 같다. 2장에서 제한수신시스템에 관련한 연구들을 기술하고, 3장에서 F-PCC 환경에 적합한 그룹 키 관리 메커니즘과 이를 적용한 제한수신시스템을 제안한다. 4장에서 제안하는 기법에 대한 안전성 및 성능 분석을 보이며, 5장에서 결론을 맺는다.

II. 관련 연구

2.1 PPC, PPV 환경의 제한수신시스템

제한수신시스템은 *CW*와 *MPK*(Master Private Key)으로 이루어진 2단계 키 계층 구조를 기본으로 한다. 사용자는 서비스를 이용하기 전에 서비스 제공자에게 등록 절차를 거치고 개인 고유의 *MPK*를 제공받아 스마트카드에 저장한다. *CW*의 안전한 배분을 위해 제한수신시스템은 키를 계층적으로 설계하였고, *CW*를 하위계층, *MPK*를 상위계층으로 구분한다. 실시간으로 전송해야 할 데이터의 양이 많기 때문에 제한수신시스템의 데이터 보호를 위해 스크램블 함수를 이용한다. 스크램블 함수는 각 채널마다 할당되어 있는 *CW*를 통해 생성한 의사난수를 이용하여 비디오 신호를 뒤섞는다. 차후 사용자가 스크램블 된 데이터를 복원하기 위해서는 해당 채널의 *CW*가 필요하기 때문에 인가된 사용자만이 *CW*를 획득할 수 있도록 해야 한다. 현재 시스템에 S 명의 사용자와 C 개의 채널이 있다고 가정하자. 서비스 제공자는 모든 채널에 대해 각 사용자의 *MPK*를 이용하여 *CW*를 암호화하여 전송한다. 스크램블 함수의 보안성을 위해 통상적으로 *CW*는 5-20초마다 갱신되기 때문에 그때마다 $S \times C$ 개의 메시지 생성이 필요하며 각 사용자에게 전송해야 하기 때문에 서비스 제공자와 통신 비용측면에서 큰 부담이 된다.

위와 같은 통신 부담을 줄이고, *CW*를 효율적으로 분배하기 위해, *AK*(Authorization Key)를 이용하는 3단계 키 계층 구조가 제안되었다[1-4]. *CW*와 마찬가지로 각 채널마다 특정한 시간에 하나의 *AK*가 할당되어 같은 채널을 보는 사용자들끼리는 같은 *AK*를 획득하게 된다. *AK*는 *CW*를 암복호화 하는데 사용되고, 일주일에서 한 달에 한 번 갱신된다. 이로써 *CW*를 갱신하는 비용은 줄어들었으나 이 방법 역시 *AK*를 각 사용자의 *MPK*로 암호화하여 분배하기 때문에 *AK*의 갱신이 필요한 경우 $S \times C$ 개의 메시지를 생성하여 전송해야 하므로 여전히 통신 부담이 존재한다. [3]에



[그림 2] 4계층 키 구조의 제한수신시스템 동작 원리

서 언급되었듯이, 3단계 키 계층 구조를 가진 제한수신시스템은 적은 수의 채널을 갖고 채널 그룹이 독립적인 PPC 혹은 PPV 환경에 적합하다.

효율적인 IP 통신 기술인 멀티캐스트를 이용하여 그룹 키를 관리함으로써 통신 부담을 줄이고자 하는 연구가 진행되고 있다. 이에 따라 채널을 그룹화 하고, *AK*와 *MPK* 사이에 *AK*를 효율적으로 갱신할 수 있는 또 하나의 키를 추가 삽입한 4단계 키 계층 구조를 가진 제한수신시스템이 제안되었다[2]-[6]. 1999년 Tu 등은 *CW*, *AK*, *RGK*(Receiving Group Key), *MPK*를 사용하는 [그림 2]와 같은 4계층 키 구조의 제한수신시스템을 제안하였다[2]. *RGK*는 *AK*를 암복호화 하는데 사용되고, *MPK*는 *RGK*를 암복호화 하는데 사용된다. 콘텐츠를 스크램블링한 스트림과 *CW*를 암호화한 *ECM*(Entitlement Control Message), 그리고 *AK*와 *RGK*를 암호화한 *EMM*(Entitlement Management Message)를 사용자 셋톱박스에 전송하면, 스마트카드에서 *CW*를 복원하고 이를 이용하여 콘텐츠를 획득하게 된다. 이러한 방식으로 기존의 3계층 구조에 *RGK*를 추가함으로써 *AK* 갱신에 필요한 메시지 전송 수를 줄이고자 하였다. 이 기법에서는 사용자가 여러 그룹에 속할 수 있으며, 같은 채널들을 보는 사용자들은 같은 그룹으로 분류된다. Tu 등은 이 기법에 대해 두 가지 장점을 주장하였다. 첫 번째로, 사용자들은 자신의 선호에 따라 채널들의 그룹을 볼 수 있다. 그러나 그룹 수가 많을 경우 그에 따른 오버헤드가 많이 발생한다. 두 번째로, 사용자는 하나의 채널에 대해 요금을 지불한 기간 동안 볼 수 있다. 그러나 그 기간이 하루정도로 짧기 때문에 구독신청을 자주 해야 하는 번거로움이 있다. 2004년 Huang 등은 *CW*, *AK*, *DK*(Distribution Key), *SK*(Secret Key)를 사용하는 4계층 키 구조의 제한수신시스템을 제안하여 Tu 등의 기법에 대한 효율성을 향상시키고자 하였다[3]. 이 기법에서는 서비스 제공자가 어떤 그룹의 채널을 미리 지정한다. 따라서 사용자는 개인의 선호와는 관계없이 한 개 이상의 미리 정의된 그룹을 선택해서 볼 수밖에 없다. 그리고 한 채널의 *AK*를 갱신하기 위해서 그 등급 혹은 그룹 이하의 모든 *AK*를 갱신해야만 하는 비효율적인 면이 존재한다.

2.2 F-PPC 환경의 제한수신시스템

최근 Sun 등은 이진트리를 이용한 그룹 키 관리 메커니즘을 설계하였고, 이를 바탕으로 F-PPC 환경에 적합한 제한수신시스템을 제안하였다[6]. 이 시스템은 *CW*, *AK*, *RGK*, *MPK*를 사용하는 4단계 키 계층 구조를 기반으로 한다. 그룹 키 관리 메커니즘에 사용되는 트리에서 각 노드의 랜덤 값은 부모노드의 랜덤 값을 해시한 결과의 좌측 또는 우측의 반값이다. 그리고 각 사용자는 자신의 노드로부터 루트까지의 경로 위에 있는 노드들을 제외한 나머지 노드들의 랜덤 값을 유지한다. 이 트리를 이용하여 제한수신시스템의 *AK*와 *RGK*를 관리한다. *AK*에 대한 트리의 단말노드에는 채널이 속한 그룹이, *RGK*에 대한 트리의 단말노드에는 그룹에 속한 사용자가 할당된다. 사용자가 탈퇴 등의 이유로 키 갱신이 필요한 경우 서비스 제공자는 최소한의 정보만 전송하고, 각 사용자 특정 노드에 해당하는 랜덤 값을 이용하여 XOR 연산을 통해 키를 갱신한다. 특정 노드에 할당된 그룹 또는 사용자는 자신의 랜덤 값을 모르기 때문에 갱신된 키를 알 수 없다. 따라서 단 하나의 메시지 전송만으로 사용자의 가입과 탈퇴에 대한 *AK* 및 *RGK* 갱신이 가능하다.

하지만 이 방법은 임의의 사용자가 탈퇴하여 관련된 채널들에 대한 *AK*를 갱신하는 과정에서 보안상의 문제점을 내포한다. 사용자가 그룹 G_j에서 탈퇴할 경우, 구독했던 모든 채널들에 대해 서비스 제공자는 탈퇴 메시지를 전송한다. 먼저 G_j의 그룹 키를 갱신하는 절차가 진행된 후, *AK*를 갱신하게 된다. 이때, G_j에 속하지 않는 사용자들은 XOR연산을 통해 자체적으로 *AK*를 갱신하고, G_j에 속하는 사용자들에게는 서비스 제공자가 갱신된 그룹 키로 암호화하여 전송한다. 이때, G_j에 속하는 구독자들이 갱신된 *AK'*와 기존의 *AK*를 XOR연산하면 해당하는 채널의 랜덤 값을 계산해낼 수 있게 된다. 이는 Sun 등이 제안한 그룹 키 관리 메커니즘에서 자신의 노드의 랜덤 값을 몰라야 한다는 규칙을 위반하는 문제가 발생한다. 본 논문에서는 F-PPC 환경에 적용 가능하며 위 문제를 해결하는 그룹 키 관리 메커니즘과 이를 이용한 제한수신시스템을 제안한다.

III. 제안하는 방법

본 장에서는 F-PPC에서의 사용자 그룹 관리를 통해 인가된 사용자만이 *CW*를 획득할 수 있도록 하는 효율적이고 안전한 제한수신시스템을 제안한다. 제안하는 방법에서 사용되는 표기법은 [표 1]과 같다.

〔표 1〕 제안하는 방법 표기법

표기법	내 용
m_k	사용자 k
ch_i	채널 i
G_j	사용자 그룹 j
AK_i	ch_i에 대한 AK
RGK_j	G_j에 대한 RGK
MPK_k	서버가 m_k에게 발행한 MPK
T_{ch_i}	ch_i에 대한 키 관리 트리
T_{G_j}	G_j에 대한 키 관리 트리
CH_{G_j}	G_j에 속한 채널들의 집합
$R_{ch_i,n}$	T_{ch_i}에서 노드 n에 해당하는 랜덤 값
$R_{G_j,n}$	T_{G_j}에서 노드 n에 해당하는 랜덤 값
I_{m_k}	m_k 노드부터 루트까지 경로 위에 있는 노드들을 제외한 나머지 노드들의 랜덤 값들의 집합 (T에서 m_k가 유지하는 랜덤 값들의 집합)
I_{ch_i,G_j}	T_{ch_i}에서 G_j에 속하는 사용자들이 유지하는 랜덤 값들의 집합
I_{G_j,m_k}	T_{G_j}에서 m_k가 유지하는 랜덤 값들의 집합
$HL(x), HR(x)$	x를 해시한 결과의 좌/우측 반 값

3.1 보안 요구사항

안전한 제한수신시스템은 다음과 같은 보안 요구사항들을 만족하여야 한다.

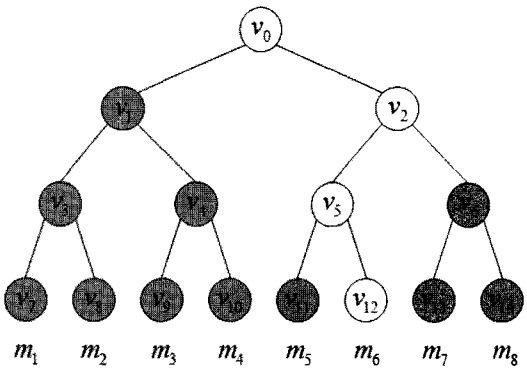
- 그룹 접근 통제: 인가된 그룹 사용자만 그룹에 해당하는 서비스를 제공받아야 한다. 따라서 그룹 키 RGK를 인가된 사용자만 보유하도록 하고, 어떤 사용자가 그룹을 탈퇴한 경우 를 갱신하여 더 이상의 서비스를 받지 못하도록 해야 한다.
- 채널 접근 통제: 각 채널에 가입된 사용자만 그 채널을 볼 수 있도록 해야 한다. 따라서 채널에 해당하는 AK를 인가된 사RGK용자만 보유하도록 하고, 어떤 사용자가 채널을 해지한 경우 해당 채널의 AK를 갱신하여 더 이상 그 채널을 볼 수 없도록 해야 한다.
- 키 독립성: RGK와 AK를 관리함에 있어 해지한 사용자가 현재 키로 갱신된 키를 계산해낼 수 있어서는 안 된다.

3.2 그룹 키 관리 기법

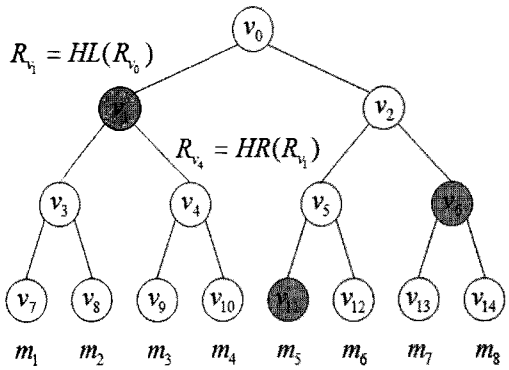
그룹 키의 효과적인 관리를 위해 Sun 등이 제안한 방법을 토대로 〔그림 3〕과 같은 이진트리를 구성한다. 트리의 모든 노드 v_i는 랜덤 값 R_{v_i}를 가진다. 그룹에 속하는 사용자 m_k는 단말 노드에 할당되고, 자신의 노드로부터 루트까지의 경로에 있는 노드를 제외한 나머지 모든 노드의 랜덤 값들의 집합 I_{m_k}를 부여받는다. 예를 들어, m_6은 $I_{m_6}=\{R_{v_1},R_{v_3},R_{v_1},R_{v_6},R_{v_7},R_{v_8},R_{v_9},R_{v_{10}},R_{v_{11}},R_{v_{13}},R_{v_{14}}\}$와 같은 값을 가지게 된다.

각 사용자가 유지해야 할 랜덤 값을 줄이기 위해 자식 노드의 랜덤 값은 부모 노드의 랜덤 값을 해시한 값의 좌측 또는 우측의 반값으로 정의한다. 즉, v_i의 좌측과 우측 노드의 랜덤 값은 $HL(R_{v_i})$, $HR(R_{v_i})$ 이다. 루트 노드의 좌우측 노드인 v_1, v_2의 랜덤 값은 각각 $R_{v_1}=HL(R_{v_0})$, $R_{v_2}=HR(R_{v_0})$이다. 마찬가지로 v_1 노드의 좌우측 노드인 v_3, v_4의 랜덤 값은 각각 $R_{v_3}=HL(R_{v_1})$, $R_{v_4}=HR(R_{v_1})$이다. 이 트리를 이용하면 특정 노드의 랜덤 값을 알 경우 이것을 루트로 하는 서브트리 상의 모든 노드에 대한 랜덤 값을 계산할 수 있다. 따라서 〔그림 4〕와 같이 m_6이 유지하게 되는 랜덤 값 집합 I_{m_6}는 $\{R_{v_1},R_{v_6},R_{v_{11}}\}$이다.

〔사용자 탈퇴〕 그룹 내 사용자 m_k의 탈퇴에 의해 그룹 키 갱신이 필요한 경우, 서버는 메시지 $\{LEAVE, m_k\}$ 를 방송하고 모든 사용자는 새로운 그룹 키 $RGK'=H(RGK,R_{v_i})$를 스스로 갱신한다. R_{v_i}는 m_k가 속단 단말 노드의 랜덤 값이다. 〔그림 3〕과 같이 m_5이 탈퇴하면, 서버는 메시지 $\{LEAVE, m_5\}$ 를 방송한다. 그리고 m_5을 제외한 모든 사용자는 새로운 그



〔그림 3〕 이진트리 구성과 m_6이 유지하는 랜덤 값



〔그림 4〕 해시를 통해 m_6이 유지하는 랜덤 값 감소

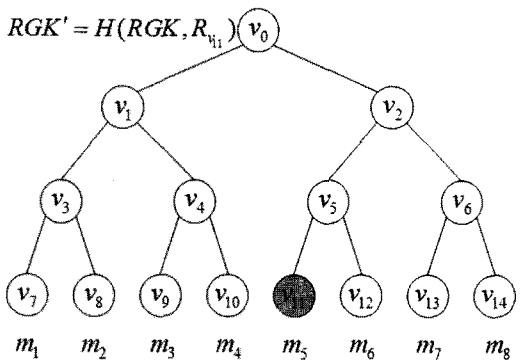
룹 키 $RGK' = H(RGK, R_{v_{11}})$를 스스로 갱신한다.

〔사용자 가입〕 현재 그룹에 M명의 사용자가 있고, $2^{n-1} < M \leq 2^n$ 인 n이 있다고 가정하자. 서버는 위와 같은 방식의 트리를 n 계층으로 구성한다. 새 사용자가 가입하면 서버는 메시지 $\{JOIN, m_k\}$ 를 방송하고, M에 따라 두 가지 경우로 나누어 가입절차를 수행한다. $M<2^n$인 경우, 가입한 사용자를 빈 단말노드에 바로 할당한다. 반면에 $M=2^n$인 경우, 서버는 노드 확장 절차를 수행해야 한다. 먼저 모든 단말 노드에 두 개의 자식 노드를 확장하고, 트리는 $n+1$ 계층이 된다. 모든 사용자 m_i는 왼쪽 자식 노드로 할당이 되고 새로운 $I_{m_i}' = I_{m_i} \cup R_{sibling-of-m_i}$ 값을 유지하게 된다. 〔그림 6〕은 현재 사용자가 8명이고 4계층 트리를 구성하고 있을 때 새로운 사용자가 가입하는 경우의 예를 나타낸다. m_1은 v_{15}에 할당되고, $I_{m_1}' = I_{m_1} \cup R_{v_{16}}$ 값을 유지한다. 가입자 m_9는 필요한 정보 I_{m_9} 등을 서버로부터 받는다.

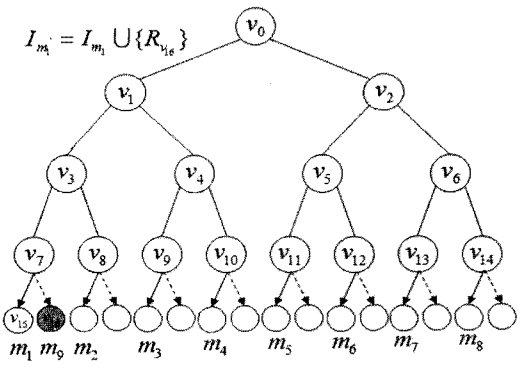
이때, 사용자가 탈퇴 후 재가입하여 기존의 위치와 다른 단말 노드에 할당된다면 알지 말아야 할 자신의 랜덤 값을 알게 되는 문제점이 존재한다. 〔그림 4〕의 상태에서 m_4가 탈퇴하고 $\{R_{v_1}, R_{v_6}, R_{v_{11}}\}$를 유지하는 m_6이 탈퇴 한 후 m_6이 재가입하여 v_{10}에 할당되면 $I_{v_{10}} = \{R_{v_2}, R_{v_3}, R_{v_0}\}$를 획득하게 된다. 그리고 기존에 알고 있던 R_{v_1}을 통해 m_6이 알아서는 안 될 $R_{v_{10}}$을 계산해 낼 수 있다. 이것은 재가입한 m_6을 기존 위치인 v_{12}에 재할당하는 방법으로 해결 가능하다. 이때, v_{12}가 다른 사용자 m_k에게 이미 할당된 경우, 서버는 노드 v_{12}에 대한 확장 절차를 수행하여 기존 사용자를 좌측 노드에, m_6을 우측 노드에 할당하고 적절한 I_{m_k}, I_{m_6}를 각각 전송함으로써 해결할 수 있다.

3.3 F-PPC 환경에서의 제한수신시스템

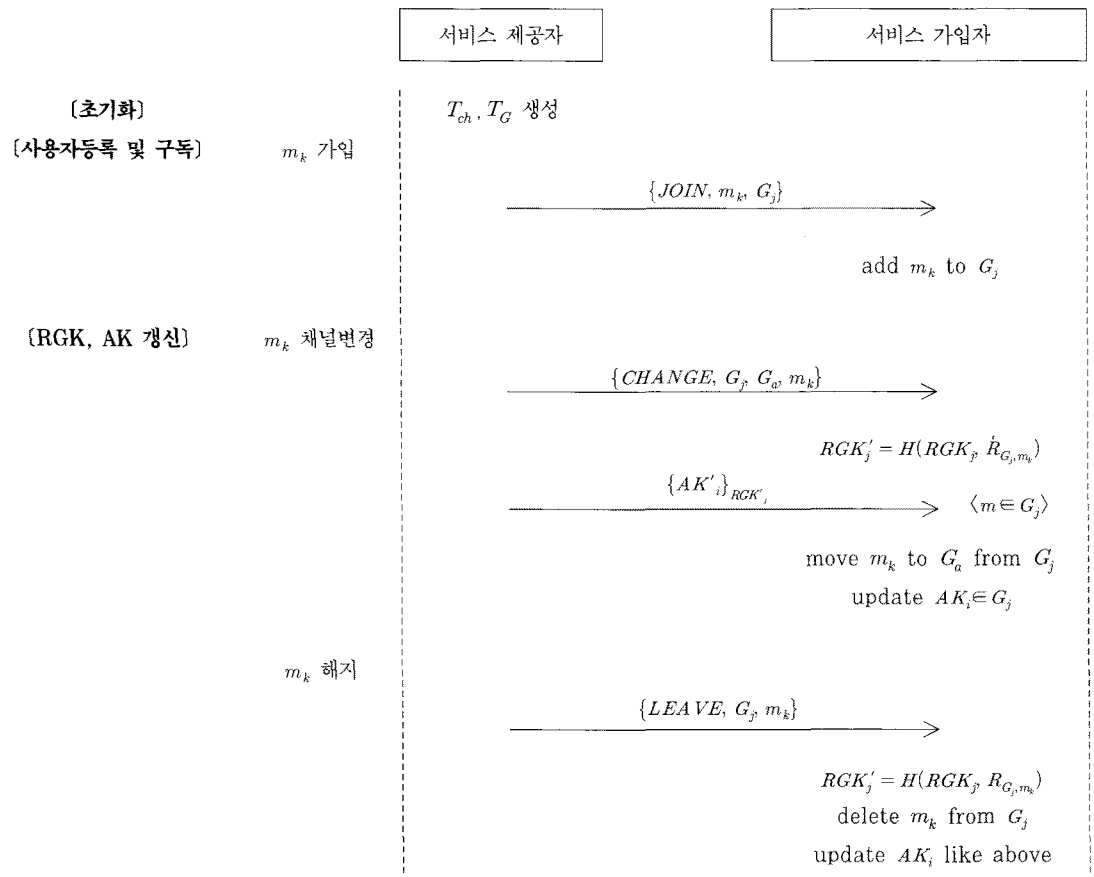
F-PPC 환경에서의 효과적인 사용자 그룹 관리를 위해 *CW*, *AK*, *RGK*, *MPK* 등의 4계층 키 구조 방식을 이용하며, 트리를 이용한 그룹 키 관리 메커니즘을



〔그림 5〕 m_5 탈퇴에 따른 그룹 키 갱신



〔그림 6〕 노드 확장의 예



〔그림 7〕 제안하는 제한수신시스템

적용하여 효율적으로 키를 관리한다. 〔그림 5〕와 같은 모델을 구성하여 채널에 해당하는 *AK* 관리를 위한 트리와 각 그룹에 해당하는 *RGK* 관리를 위한 트리를 유지 및 관리한다. 기존의 관련 연구들과 마찬가지로 *CW*는 *AK*를 통해 암호화되어 배포되고, *AK*는 *RGK*를 통해 암호화되어 배포된다. *MPK*는 서비스 제공자 측의 서버에 의해 발행되며, 최초 가입 시 *RGK*를 발행할 때 사용된다. 만일 채널 ch_i가 그룹 G_j에 더 이상 속하지 않는 경우, 해당 채널에 대한 AK_i가 갱신되고 ch_i가 속한 그룹 중 G_j를 제외한 나머지 그룹들에 속한 사용자들에게 각 그룹의 RGK_j를 이용하여 안전하게 전달된다. 즉, 사용자가 채널 조합을 변경하여 그룹 G_a에서 그룹 G_b로 이동한 경우, 기존 그룹의 그룹 키 RGK_a는 갱신되어 소속 사용자들에게 안전하게 전달되고, 채널 조합 변경에 따른 *AK* 갱신이 변경된 그룹 키 RGK_a'를 통해 이루어진다.

서비스 제공자가 그룹을 미리 정의하지 않는 F-PPC의 사용자 그룹 관리를 위해 *CW*, *AK*, *RGK*, *MPK* 등의 4계층 키 구조 방식을 이용한다. 서버는 채널에 대한 *AK* 관리를 위한 트리와 그룹 키 *RGK* 관리를 위한 트리 T_{ch_i}, T_{G_j}를 유지한다. 각 사용자는 원하는 채널의 조합을 구독할 수 있고, 그 조합은 곧 그룹이 된다. 따라서 같은 채널 조합을 사용하는 사용자끼리는 같은 그룹에 속하여 그룹 키를 공유한다. 임의의 사용자가 채널을 변경하거나 탈퇴하는 경우, 관련된 *AK*, *RGK*를 갱신해야 한다. 제안하는 사용자 그룹 관리 메커니즘은 〔그림 7〕과 같이 초기화, 사용자 등록, 구독, *RGK* 갱신, *AK* 갱신 등의 다섯 단계로 기술할 수 있다.

〔초기화〕 서비스 제공자는 각 채널 ch_i에 대해 AK_i를 부여하고, 그것을 관리하는 트리 T_{ch_i}를 구성한다. T_{ch_i}상의 단말 노드에 ch_i가 속한 그룹을 할당한다. 또한 각 그룹 G_j에 대해 RGK_j를 부여하고, 트리 T_{G_j}를 구성한다. T_{G_j}상의 단말 노드에 G_j에 속한 사용자들을

할당한다. 초기화 과정이 끝나면 [그림 5]와 같다.

[사용자 등록] 새로운 사용자 m_k가 가입하고자 하면, 서비스 제공자는 MPK_k를 발행하여 안전하게 제공하고, 이것은 사용자의 스마트카드에 저장된다.

[구독] 서비스 제공자는 m_k를 직접 선택한 채널들의 조합에 해당하는 그룹 G_j에 배정한다. 그리고 m_k에게 RGK_j와 T_{G_j}상에서 m_k가 유지해야할 랜덤 값들의 집합인 I_{G_j,m_k}를 MPK_k로 암호화하여 전송한다. 또한 선택한 모든 채널들에 대한 I_{ch_i,G_j} 집합들과 AK_i들을 RGK_j로 암호화하여 전송한다. 그 후 메시지 $\{JOIN, m_k, G_j\}$ 를 방송한다. 그러면 기존의 모든 사용자들은 T_{G_j}에 m_k를 할당한다. 만약 m_k가 선택한 채널 조합이 기존에 없는 새로운 것이라면, 서버는 새 그룹 G_{j+1}과 이에 대한 트리 $T_{G_{j+1}}$을 만들어 단말 노드에 m_k를 할당하고, G_{j+1}을 m_k가 선택한 모든 채널들에 대한 각 T_{ch_i}의 단말 노드에 할당한다.

예를 들어, [그림 5]에서 m_2가 ch_2, ch_4, ch_5를 신청하였다고 가정하자. $CH_{G_3} = \{ch_2, ch_4, ch_5\}$ 이므로 서버는 m_2를 G_3에 배정하고, 메시지 $\{JOIN, m_2, G_3\}$ 를 방송한다. 모든 사용자는 T_{G_3}에 m_2를 할당한다. 그리고 서버는 m_2에게 필요한 비밀 정보들을 제공한다. 즉, RGK_3, I_{G_3,m_2}를 MPK_2로 암호화한 메시지와, I_{ch_2,G_3}, I_{ch_4,G_3}, I_{ch_5,G_3}, AK_2, AK_4, AK_5를 RGK_3으로 암호화한 메시지를 전송한다.

[RGK 갱신] 사용자 m_k가 서비스를 해지하거나, 채널을 변경하는 등의 사유로 그룹 G_j를 탈퇴하면 그룹 키 RGK_j는 갱신되어야 한다. 서비스를 해지한 경우, 서버가 G_j에 속한 사용자들에게 메시지 $\{LEAVE, G_j, m_k\}$ 를 방송하면, G_j 내 모든 사용자들은 새로운 $RGK_j' = H(RGK_j, R_{G_j,m_k})$ 를 스스로 갱신한다. 탈퇴한 사용자 m_k는 R_{G_j,m_k}를 모르기 때문에 새로운 RGK_j'를 계산할 수 없고, 단방향 해시 함수이기 때문에 새로 가입한 사용자가 이전 세션의 그룹 키를 획득할 수 없다. 채널을 변경한 경우, 서비스 제공자가 메시지 $\{CHANGE, G_j, G_a, m_k\}$ 를 방송하면, 위와 같은 해지에 대한 RGK 갱신 과정이 종료된 후 G_a에 m_k를 추가하는 과정을 수행한다.

예를 들어, [그림 5]에서 m_2가 G_3에서 탈퇴했다고 가정하자. 서버는 메시지 $\{LEAVE, G_3, m_2\}$ 를 방송하고, 모든 남아있는 사용자는 $H(RGK_3, R_{G_3,m_2})$를 통해 RGK_3'를 스스로 갱신한다. m_2는 R_{G_3,m_2}를 모르기 때문에 갱신된 RGK_3'를 계산해낼 수 없다.

[AK 갱신] AK 갱신은 그룹 G_j에 속한 사용자 m_k가 서비스를 완전히 해지한 경우와 채널의 추가 및 삭제를 통해 구독중인 채널의 조합을 변경한 경우 두 가지 상황에 의해 발생한다.

(1) 서비스를 해지한 경우

m_k가 서비스를 해지하면 서비스 제공자가 메시지 $\{LEAVE, G_j, m_k\}$ 를 방송하고, RGK_j가 갱신됨과 동시에 해당 그룹에 속해있던 모든 채널 ch_i들에 대한 AK를 갱신해야 한다. 위 메시지를 받은 사용자들은 다음의 두 가지 입장에 따라 갱신을 수행한다.

① G_j에 속하지 않는 사용자들:
$AK_i' = H(AK, R_{ch_i,G_j})$ 으로 자체 갱신

② G_j에 속하는 사용자들:
RGK_j'를 키로 사용하여 암호화된 AK_i'를 서비스 제공자로부터 전송받아 갱신

(2) 채널 조합을 변경한 경우

서비스 제공자는 m_k가 채널을 추가로 등록하거나 어떤 채널을 해지하는 경우, 혹은 두 가지를 동시에 하는 경우에 그에 따른 적절한 그룹으로 재할당 해주어야 한다. m_k가 G_j에서 G_a로 이동한 경우, 서비스 제공자는 메시지 $\{CHANGE, G_j, G_a, m_k\}$ 를 방송한다. RGK_j가 갱신된 후, AK 갱신을 고려해야 하는 채널들은 다음과 같이 세 가지로 구분하여 이루어진다.

① $CH_{G_j} - CH_{G_a}$
이 집합에 속한 채널들은 m_k가 더 이상 구독하지 않는 해지된 채널들이다. 따라서 이 채널들에 대해 (1)과 같은 방법으로 AK 갱신을 실시한다.

② $CH_{G_a} - CH_{G_j}$
이 집합에 속한 채널들은 m_k가 새로 구독하는 추가된 채널들이다. 서비스 제공자가 이 채널들에 대한 필요한 정보를 m_k에게 전송한다.

③ $CH_{G_j} \cap CH_{G_a}$
G_j와 G_a에 동시에 속한 채널 ch 각각에 대해 T_{ch}의 단말 노드에는 G_j와 G_a가 모두 속해있다. G_j에 속해 있던 m_k는 G_a의 노드로부터 루트까지의 노드를 제외한 모든 노드의 랜덤 값을 알고 있다. 즉, G_a 노드로부터 루트까지 노드들 중 G_j와의 공통 조상이 아닌 G_a만의 조상 노드들의 랜덤 값들은 갱신해주어야 한다. 이는 루트부터

〔표 2〕 분석 표기법

표기법	내 용
M, CH, G	시스템 내 총 사용자/채널/그룹 수
NM_{G_j}	그룹 G_j 에 속한 사용자 수
NG_{ch_i}	채널 ch_i가 속한 그룹 수
NM_{ch_i}	채널 ch_i를 구독하는 사용자 수
NCH_{m_k}	사용자 m_k가 구독하는 채널 수
$NCH_{m_k}^{-}, NCH_{m_k}^{+}$	사용자 m_k가 해지/추가한 채널 수

하향식 접근으로 이루어진다. 루트의 좌측 자식 노드가 v_n일 때, v_n이 G_α노드에서 루트가지 경로에 포함되지 않으면 랜덤 값은 그대로 유지된다. 반면에 그 경로에 포함되어 있으면 랜덤 값은 $R'_{ch_\alpha v_n} = HL(R_{ch_\alpha root}+1)$로 변경된다. v_n이 우측 자식노드일 경우 $HL()$ 대신 $HR()$을 사용한다. 이와 같은 방법으로 G_α 노드까지의 랜덤 값을 조건에 따라 변경한다. 결과적으로 이 집합에 속하는 채널들에 대한 AK 갱신은 하지 않고 m_k가 알지 말아야 할 랜덤 값들에 대한 변경만 이루어진다.

IV. 분 석

본 장에서는 제안하는 방법의 성능과 안전성을 분석한다. 2장에서 다루었던 Tu 등과, Huang 등의 방법은 서비스 제공자가 채널의 조합을 미리 선정하는 PPC 환경을 토대로 제안되었다. 반면에 본 논문에서는 사용자가 자신의 취향에 따라 채널의 조합을 마음대로 결정할 수 있는 F-PPC 환경에 적용 가능한 제한수신시스템을 제안하였다. 따라서 위 방법들과의 직접적인 비교 보다는 제안하는 방식의 성능과 안전성을 〔표 2〕와 같은 표기법을 토대로 〔표 3〕과 같이 분석하였다.

4.1 안전성 분석

사용자 m_k가 서비스에 가입하여 어떤 그룹에 속하는 경우, 그 그룹의 서비스를 받기 위해 필요한 정보 RGK와 I_{G,m_k} 값을 m_k의 개인 키 MPK_k로 암호화하여 전송한다. 따라서 인가되지 않은 사용자는 필요한 정보들을 획득할 수 없기 때문에 해당 그룹의 서비스에 접근할 수 없다.

채널에 대한 AK는 사용자가 속한 그룹의 그룹 키로 암호화하여 전송된다. 위에 기술했듯이 그룹 키는 인가된 사용자에게만 안전하게 전송된다. 따라서 분배되는 AK 역시 인가된 사용자만 획득할 수 있다. 해당 채널을 구독하지 않는 사용자는 다른 그룹에 속해 있기 때문에 다른 RGK를 보유하고 있고, 따라서 AK를 획득할 수 없다. 해당 채널을 구독하지만 다른 그룹에 속한 사용자에 대해서는 문제될 것이 없다.

키 갱신은 3.1과 3.2에서 기술한 방법을 이용한다. 사용자 m_k가 그룹 G_j에서 탈퇴하여 그룹 키 RGK_j가 $RGK_j' = H(RGK_j, R_{G_j,m_k})$갱신되는 경우, m_k는 R_{G_j,m_k} 값을 모르기 때문에 RGK_j'를 계산해낼 수 없다. 마찬가지로 AK 갱신 시 채널 ch_i를 해지한 m_k는 R_{ch_i,G_j}를 모르기 때문에 $AK_i' = H(AK_i, R_{ch_i,G_j})$ 값을 계산해낼 수 없다. 또한 단방향 해시함수의 특성상 G_j에 속하는 사용자들이 R_{ch_i,G_j}를 알아낼 수 없다. 따라서 AK'와 AK를 XOR연산하면 해당하는 채널의 랜덤 값 R_{ch_i,G_j}를 계산해낼 수 있었던 Sun 등이 제안한 기법의 보안 취약점을 해결한다.

4.2 성능 분석

사용자 m_k가 채널들 ch_i의 조합을 통해 그룹 G_j에 가입하는 경우, 서비스 제공자가 가입자 m_k에게 전송해야 하는 총 메시지의 양은 $2+\lg NM_{G_j}+NCH_{m_k}(1+\lg(NG_{ch_i}))$

〔표 3〕 메시지 전송 수 및 저장 공간 비교

구 분		Tu[2]	Huang[3]	제안하는 기법
메시지 전송 수	가입	2	4	2
	해지	$NM_{G_j}+NCH_{m_k}\times NG_{ch_i}$	$NM_{G_j}+NG_{ch_i}$	$2+NM_{G_j}$
	채널변경	$2+NM_{G_j}+NCH_{m_k}\times NG_{G_j}$	$4+NM_{G_j}+NG_{ch_i}$	$3+NM_{G_j}$
저장 공간	서버	$G\times NM_G+CH\times NG_{CH}$	$M+2(CH+G)$	$2M+CH(1+\lg(NG_{ch}))+G(1+\lg(NM_G))$
	사용자	$NM_{G_j}+NCH_{m_k}\times NG_{ch_i}$	$1+2(CH+G)$	$1+2M+\lg NM_{G_j}+NCH_{m_k}(1+\lg(NG_{ch_i}))$

이다. RGK_j, $I_{G_j m_k}$, 그리고 ch_i들에 대한 AK_i들과 $I_{ch_i G_j}$ 집합들을 전송해야 한다. 가입자 외의 기존 그룹 멤버에게 전송하는 메시지는 가입을 알리는 단 하나의 메시지뿐이다. 각 채널마다 속해있는 그룹의 수가 다를 수 있기 때문에 계산의 편의를 위해 평균값을 사용하였다. G_j에 속해 있던 m_k가 서비스를 해지하는 경우 단 두 개의 메시지가 필요하다. 하나는 m_k가 해지했음을 알리는 메시지이다. RGK_j'는 사용자가 직접 갱신이 가능하며, G_j에 속한 사용자들이 직접 갱신하지 못하는 AK'를 RGK_j'로 암호화하여 전송하는 메시지가 다른 하나이다.

사용자 m_k가 채널 조합을 변형하여 그룹이 G_j에서 G_a로 이동된 경우, 서비스 제공자는 하나의 채널변경 메시지를 방송한다. 그리고 가입 경우와 같이 m_k에게 RGK_a, $I_{G_a m_k}$와 함께 추가되는 채널 ch^+들에 대한 정보 AK와 I_{ch, G_a} 집합들을 전송한다. 또한 해지 경우와 같이, 구독을 취소하는 각각의 채널들에 대해 갱신된 AK'를 G_j에 속하는 사용자들에게 NCH_{m_k}개의 메시지를 전송한다. 채널변경을 하는 사용자 외의 모든 사용자들에게는 채널변경 메시지만을 전송하고, 각 사용자가 스스로 키를 갱신한다.

사용자 m_k의 가입과 해지, 그리고 채널조합변경 시 m_k에게 필요한 정보를 유니캐스트하는 것 외에 키 갱신에 필요한 메시지의 멀티캐스트 수의 복잡도는 $O(1)$이다. 따라서 네트워크 대역폭의 부담을 최소화하여 키 갱신이 가능하다.

각 사용자가 IPTV 서비스를 제공받기 위해 유지하는 정보는 자신이 속한 그룹의 트리 정보와 구독하고 있는 채널들에 대한 트리 정보이다. 즉, 사용자 m_k는 본인이 속한 그룹 G_j의 그룹 키 RGK_j와 해당 트리의 랜덤 값 $I_{G_a m_k}$을 유지한다. 그리고 가입한 채널들 ch_i에 대한 AK_i와 각 AK_i에 대한 트리의 랜덤 값 $I_{ch_i G_j}$을 유지한다. 서버는 모든 사용자들의 MPK와 모든 채널의 AK, 모든 그룹의 RGK를 유지한다. 그리고 각 채널과 그룹별 트리를 유지한다.

[표 3]은 제안하는 방법의 메시지 전송량과 저장 공간을 기존 연구와 비교한 것이다. Tu 등의 방법과 Huang 등의 방법은 PPV 환경에 적용 가능하도록 제안되었다. 따라서 본 논문에서 제안하는 기법과의 비교를 위해 F-PPC 환경에 적용했을 때 요구되는 메시지 전송량과 저장 공간을 산출하여 비교하였다. 기존의 기법들은 가입 및 해지, 그리고 사용자의 채널 변경이 발생하는 경우 기존 연구에서는 갱신되는 키를 직접 서버가 사용자들에게 전송해야 한다. 따라서 제안하는 기법이 갱신에 요구되는 메시지 전송량 측면에서 기존 연구보다 효율적임을 확인할 수 있다. Tu 등의 기법은 트리 대신 행렬을 이용하며, Huang 등의 기법은 각 그룹과 채널에 대해 AK, DK(Distribution Key)를 유지한다. 제안하는 기법에서 사용자와 서버에게 요구되는 저장 공간은 Tu 등의 방법보다는 적고, Huang 등의 기법보다는 많다.

V. 결 론

사용자의 취향에 따라 구독하고자 하는 채널들을 임의로 조합할 수 있는 F-PPC 환경의 필요성에 따라 이 환경에 적합한 사용자 관리 시스템에 대한 연구를 진행하였다. F-PPC 환경에 적합한 기존의 방법에서는 단 하나의 메시지로 그룹 키 갱신이 가능하지만, 특정한 경우 사용자가 자신의 랜덤 값을 계산해낼 수 있는 치명적인 문제점을 내포하고 있다. 본 논문에서는 이를 보완하여 안전하고 효율적인 그룹 키 관리 메커니즘과 F-PPC에 적용할 수 있는 제한수신시스템을 제안하였다. 제안하는 방법은 가입자의 위치를 유지하고 있어야 한다는 점에서 Trade-off가 발생한다. 하지만 그룹 키를 갱신하는 경우에는 단 하나의 메시지가 요구되며, AK를 갱신하는 경우에는 해당 채널이 속한 그룹의 수만큼의 메시지가 요구되어 서비스 제공자 측의 연산 부담을 줄였다. 또한 기존의 방법에서 발견되었던 사용자가 자신의 랜덤 값을 알아내는 문제를 해결하였기에 제안하는 시스템은 F-PPC 환경에서 안전하고 효율적인 콘텐츠 접근 권한 제어가 가능하다. 앞으로 서버와 사용자가 유지해야 하는 저장 공간측면에서의 부하를 줄이면서 적은 양의 메시지 전송으로 키 갱신이 가능한 키 관리 기법에 대한 연구가 필요하다.

참고문헌

[1] "Conditional-Access Broadcasting Systems," ITU Rec., 810, 1992.

[2] F. Tu, C. Laih, and H. Tung, "On Key Distribution Management for Conditional Access System on Pay-TV System," IEEE Trans. Consumer Electronics, Vol. 45, pp.151-158, February 1999.

[3] Y.L. Huang, S. Shieh, F.S. Ho, and J.C. Wang, "Efficient key distribution schemes for secure media delivery in pay-TV systems," IEEE Trans. Multimedia, vol. 6, no. 5, pp. 760-769, October 2004.

[4] T. Jiang, S. Zheng, and B. Liu, "Key distribution based on hierarchical access control for conditional access system in DTV broadcast," IEEE Trans. Consumer Electronics, vol. 50, no. 1, pp. 225-230, February 2004.

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

[6] H.M. Sun, C.M. Chen, and C.Z. Shieh, "Flexible-Pay-Per-Channel: A new model for content access control in pay-TV broadcasting systems," IEEE Trans. Multimedia, vol. 10, no. 6, pp. 1109-1120, October 2008.

[7] C.K. Wong, M. Gouda, and S.S. Lam, "Secure group communications using Key graphs," IEEE/ACM Trans. Networking, vol. 8, pp. 16-30, February 2000.

[8] D.M. Wallner, E.J. Harder, and R.C. Agee, "Key management for multicast: Issues and architecutres," RFC 2627, June 1999.

[9] R. Canetti, J. Garay, G. Itkis, D. Micciancio, M. Naor, and B. Pinkas, "Multicast security: A taxonomy and som efficient constructions," IEEE INFOCOM, vol. 2, pp. 708-716, March 1999.

[10] A.T. Sherman and D.A. McGrew, "Key establishment in large dynamic groups using one-way function trees," IEEE Trans. Software Engineering, vol. 29, pp. 444-458, May 2003.

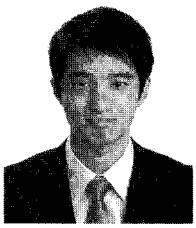
[11] M. Li, R. Poovendran, and C. Bernstein, "Design of secure multicast key management schemes with communication budget constraint," IEEE Communication Letters, vol. 6, pp. 108-110, March 2002.

[12] M.J. Mihaljevic, "Reconfigurable key management for broadcast encryption," IEEE Communication Letters, vol. 8, pp. 440-442, July 2004.

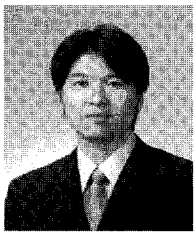
[13] W.T. Zhu, "Optimizing the tree structure in secure multicast key management," IEEE Communications Letters, vol. 9, no. 5, pp. 477-479, May 2005.

[14] Q. Kang, X. Meng, and J. Wang, "An optimized LKH scheme based on one-way hash function for secure group communications," IEEE ICCT, November 2006.

〈著者紹介〉



강 용 구 (Yonggoo Kang) 학생회원
2009년 2월: 한양대학교 컴퓨터공학과(학사)
2009년 3월~현재: 한양대학교 컴퓨터공학과 (석사과정)
〈관심분야〉 정보보호, IPTV 보안, 그룹키 관리



임 지 환 (Jihwan Lim) 학생회원
2005년 2월: 한양대학교 전자컴퓨터공학부(학사)
2007년 2월: 한양대학교 컴퓨터공학과(석사)
2007년 3월~현재: 한양대학교 컴퓨터공학과 (박사과정)
〈관심분야〉 네트워크 보안

오 희 국 (Heekuck Oh) 종신회원
1983년: 한양대학교 전자공학과(학사)
1989년: 아이오와주립대학 전자계산학과(석사)
1992년: 아이오와주립대학 전자계산학과(박사)
1993년~1994년: 한국전자통신연구원 선임연구원
1995년 3월~현재: 한양대학교 컴퓨터공학과 교수
〈관심분야〉 암호프로토콜, 네트워크 보안