한국항행학회 논문지 제13권 제5호 2009년 10월

방송 채널 효율 향상을 위한 그룹 계층 구성 기반 접근 제어 시스템

Conditional Access System with A Group Hierarchy to Improve Broadcasting Channel Efficiency

양장훈*, 김동구*

Jang-Hoon Yang*, Dong-Ku Kim*

요 약

본 논문에서는 방송 시스템에서 채널의 대역폭이 제한되는 상황에서 유효 가입자 제어를 위한 메시지 전송 오버헤드를 감소시키는 접근 제어 시스템을 제안하였다. 이를 위해서 IP 기반 멀티캐스트에 제안되었던 트리 계층 구조의 키 개정 시스템을 도입하여 가입자를 트리 구조에 직접 매핑하는 경우와 가입자를 채널 그룹별로 나누어 채널 그룹을 트리 구조에 적용하는 시스템을 고려하였다. 제안 시스템의 효율성을 평가하기 위해 기존의 시스템과 제안 시스템에 대해서 보안을 위한 주기적인 키 개정을 위한 오버헤드 전송율과 동적이면서 비주기적으로 가입자의 변동이 발생을 할 때의 오버헤드 전송율을 분석하였다. 다양한 시스템 환경에서 제안 시스템은 기존 시스템에 비해서 가입자의 변동이 발생할 경우에 수 배에서 수십 만배의 키 개정을 위한 메시지 오버헤드 전송율을 크게 감소시키는 것을 분석 평가를 통해서 확인하였다.

Abstract

In this paper, we proposed a novel conditional access system to reduce the overhead transmission rate for messages which verify the entitlement of subscribers in bandwidth-limited system. We adapted a key update system with the tree structure which had been used for IP multicast to a group hierarchy for the subscriber groups or channel groups. We also analyzed the overhead transmission rate for periodic key update and aperiodic one for change in a subscriber. The numerical evaluations show that the proposed system can significantly reduce the overhead transmission rate for dynamic subscriber change up to several hundred thousands times for various system configuration.

Key words : Conditional Access System, CAS, IPTV

I. 서 론

방송 시스템은 지역 기반 공공 방송 시스템에서 케이블이나 위성을 통한 방송 시스템으로 진화가 이루어졌고 새로운 매체를 통한 방송 시스템 즉, 디지털 휴대 방송이나 IPTV와 같은 방송 시스템도 급속도로 보급되고 있는 상태이다. 또한 방송과 통신이 융합되면서 단말기를 통해서 IPTV를 전송하는

* 연세대학교 전기전자공학부(School of Electrical & Electronic Engineering, Yonsei University)
· 제1저자 (First Author) : 양장훈
· 투고일자 : 2009년 9월 24일
· 심사(수정)일자 : 2009년 9월 25일 (수정일자 : 2009년 10월 28일)
· 게재일자 : 2009년 10월 30일

mobile IPTV 기술도 현재 차세대 셀룰라 통신 시스템에 도입될 것으로 예상되어 진다. 방송은 공영 방송이나 소수의 방송 사업자에서 다수의 케이블이나 위성 방송 사업자로 그 영역이 확장되었으며 인터넷의 발달과 함께 인터넷 개인 방송이나 UCC와 같은 매체를 이용한 특화된 방송까지 방송 매체의 수가 작은 단위로 분할되어 가고 있는 상황이다. 케이블이나 위성 방송, 그리고 차세대 방송에서 가장 중요한 기술들 중의 하나는 자격을 가진 사용자에게만 방송을 볼 수 있는 권리를 효율적으로 부여하는 방법이다. 다양한 방송 매체들이 등장함에 따라서 보다 효율적인 사용자 관리 방법들에 대한 연구가 필요하게 되었다.

현재 많은 위성이나 케이블에서 사용되고 있는 사용자 권한 제어 방법인 CAS (Conditional Access System) 라고 불리우는 접근 제어 시스템은 1995년도에 유럽 방송 연합에서 제안한 기본 모델을 바탕으로 하고 있다 [1]. 이후에 CAS 를 다양한 매체 환경과 시스템 운용 목적에 따라서 변형된 알고리듬 들이 개발되었다. [2] 에서는 두 개 이상의 매체를 통해서 방송 신호를 전송할 때에 다중화, 제어, 암호화 등의 효율적인 치환 방식등이 소개되었다. [3] 에서는 홈 서버에서 가입자 인증과 저장되는 콘텐츠의 디지털 권리 관리 방식을 결합해서 하는 방법이 제시되었고, [4] 에서는 인증 시스템이 모바일 단말기에 위치할 때에 언제 어디서나 방송 시스템에 접근할 수 있는 사용자 인증 시스템 구조가 되었다. [5] 에서는 보안성을 증가 시키기 위해서 IP를 통해서 양방향 방송이 가능할 때에 IP 멀티 캐스트를 채용한 사용자 인증 시스템이 제안되었다. 이런 다양한 진화된 방식에 대한 연구에서의 기본 가정은 접근 제어를 위한 시그널링을 위한 메시지 교환이 제한을 받지 않는다는 것이다. 하지만, 메시지가 특히 무선을 통해서 전송될 때에는 시스템의 사용 대역에 의해서 메시지 전송량이 제한을 받게 된다.

따라서, 이런 문제를 해결하기 위한 많은 다양한 방법들이 제시되었다. 기존의 CAS 가 세단계의 키 계층구조 (Key hierachy) 를 갖는 반면에 네단계 키 계층구조를 가지면서 시스템내의 사용자의 변동이 있는 환경에 적합한 방식이 제안되었다 [6]. 또한 멀티미디어 데이터와 CAS관련 메시지를 효율적으로 다중화 채널에서의 전송 데이터 량을 줄이는 방법도 개발되었다 [7]. [8] 에서는 자격 제거 제어 메시지를 도입하여 [6]에서 동적으로 사용자들의 변화가 있을 때의 메시지 증가량을 줄이는 방법을 제안하였으나 제안 방법의 보안성이 취약하여 실제 시스템에 적용할 수 없는 구조를 가지고 있다.

본 논문에서는 [6]에서 제안된 방식을 동적인 환경에서 보다 진화된 방식으로 제어함으로써 메시지 증가량을 억제하는 방식을 제안한다. [6]을 개선하는 방식으로 [9]에서 멀티캐스트의 키 개정에 사용되는 트리 구조를 도입함으로써 그룹 트리를 생성하여 동적인 환경에서의 전반적인 메시지량을 줄이는 방법을 제안한다. 이는 특히 무선 채널에서 주파수 사용량이 제한된 시스템에서 다수의 사용자를 가입자로 가지고 있는 상당히 큰 시스템에서 유용하게 사용될 수 있을 것으로 예상된다.

논문은 다음과 같이 구성된다. 먼저 2장에서는 CAS 시스템과 기준 성능이 되는 [6]에서 제시된 시스템에 대한 설명을 제공하고, 3장에서는 제안 방식인 그룹 트리 방식의 키 관리 시스템을 제안한다. 4장에서는 제안 방식의 성능을 요구되어지는 다양한 메시지 전송율을 기반으로 비교 분석하고 5장에서는 다양한 시스템 환경에서 전송 효율을 비교한다. 6장에서 전반적인 제안 알고리듬에 대한 성능에 대한 결론과 향후 필요한 연구를 제시한다.

Ⅱ. CAS와 SFLH의 개요

본 장에서는 일반적으로 많이 사용되는 CAS 시스템의 동작 구성과 관련된 메시지에 대해서 정리하고 이를 좀 더 효율적으로 만들기 위해서 제안된 SFLH (Simple Four Level Hierachy) [6] 에 대한 동작에 대해서 설명한다.

2-1. CAS

CAS는 자격이 주어진 가입자에 대해서만 시스템이나 콘텐츠에 접근을 허용하는 보안 솔루션으로서 주로 위성 방송이나 케이블 방송에서 유료 방송에

사용되고 있다 [1]. CAS는 3단계의 계층 구조를 갖는데 송신단에서 동작 구조는 그림 1을 따르고 수신단에서는 그림 1의 역과정을 실시한다. 먼저 SMS (Subscriber Mangement System)은 가입자에게 고유한 MPK (Master Private Key)를 부여한다. 이 키는 시스템에 따라서 방송 수신기 내에 위치하거나 스마트 카드에 위치한다. 송신기에서는 가입자별 MPK로 채널별 암호화 키에 해당하는 AK (Authorization Key)를 암호화하고 AK는 다시 데이터의 스크램블링에 사용되는 CW (Control Word) 키를 암호하 하는 3단계 계층 구조를 갖는다. 수신단에서는 역과정을 실시하는데 먼저 MPK를 가지고 AK를 암호화 해제 과정을 통해 획득하고 AK를 가지고 CW를 암호화 해제 과정을 획득함으로써 스크램블링되어 들어오는 데이터 신호의 원래 신호를 복구하는 절차를 따르게 된다.

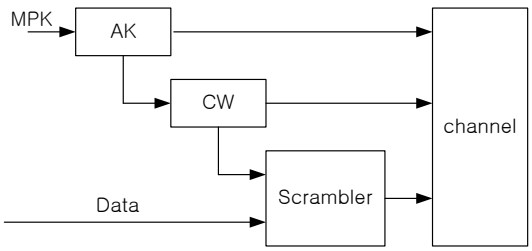

그림 1. CAS 를 구현하는 송신기 구조
Fig. 1. Transmission block for implementing CAS.

이런 암호화 키는 서로 다른 메시지를 통해서 보내지는데 암호화된 AK는 EMM (Entitlement Management Message) 라는 자격 관리 메시지를 통해서 보내지고 암호화된 CW는 ECM (Entitlement Control Message) 라는 자격 제어 메시지를 통해서 전송된다. 보안을 강화하기 위해서 암호화에 사용되는 키들은 주기적으로 개정되거나 사용자의 변동이 생길 때에 갱신된다. 보통 시스템에서는 CW는 수초내의 주기로 개정하고 AK의 경우는 수일에서 한달 정도의 주기로 개정한다. CW를 갱신하기 위해서는 ECM을 채널 단위로 보내야 하는 반면에 AK를 갱신하기 위해서는 사용자 단위로 갱신해야 하기 때문에 가입자가 많은 시스템에서는 이 메시지 전송으로 인한 채널의 사용량이 상대적으로 커지는 문제가 발생하게 된다. 또한, 사용자의 변동이 생길 때에는 이 모두를 갱신해야 하기 때문에 동적으로 사용자의 변경이 허용되는 시스템에서도 동일한 문제가 발생할 수 있다.

2-2. SFLH

아주 많은 가입자나 채널 수가 많은 시스템에서 보다 효율적으로 키를 전달함으로써 메시지 전송 효율을 증가시키는 4 계층 구조 보안 시스템이 제안되었다 [6]. 이 시스템에서는 가입된 채널 셋이 동일한 사용자들을 묶어 수신 그룹을 정의하고 이 그룹이 가입한 채널들을 수신 채널 그룹이라 정의를 하였다. 이 그룹에 대해서 RGK (Receiving Group Key)라는 키를 정의하여 그림 2에서와 같은 4단계 계층 구조를 갖는 보인 시스템이 제안되었다. 기존의 CAS가 AK를 개정하기 위해서 U_A(가입자수)$\times N_C$ (채널수) 수만큼의 EMM 메시지를 송신해야 했던 반면에 제안 방식은 RGK와 AK를 개정하기 위해서 $U_A + N_{CG}$ (채널 그룹 수) 만큼의 EMM 메시지를 보내면 되기 때문에 보다 효율적으로 암호화 키를 전송할 수 있는 장점이 있다.

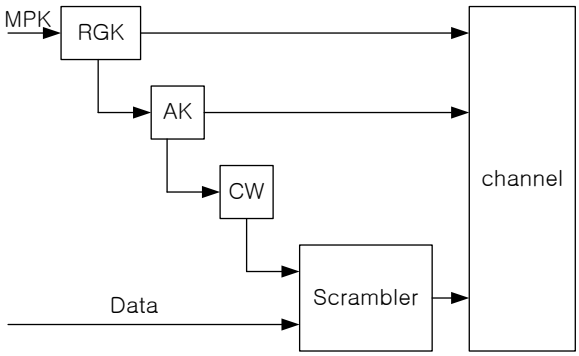

그림 2. SFLH 를 구현하는 송신기 구조
Fig. 2. Transmission block for implementing SFLH.

Ⅲ. 그룹 트리 접근 제어 시스템

SFLH 는 CAS에 비해서는 주기적으로 보내는 메시지 양을 상당히 줄일 수 있지만 가입자 정보가 동적으로 자주 변경되거나 채널 그룹의 수가 아주 많은 경우에는 보다 더 효율적인 키 메시지 전송을 필요로 한다. 따라서 이를 해결하기 위해서 본 논문에서는 멀티캐스트 시스템이나 IP 기반 양방향 방송 시스템

에서 암호화 키 관리를 위해서 사용된 LKD (Logic Key Distribution) 구조 [8],[9] 를 도입하여 다양한 시스템 환경에서 효율적으로 키 메시지를 전송할 수 있는 시스템을 제안한다.

LKD는 그림 3과 같은 트리 구조를 갖는다. 트리의 가장 밑부분에 위치하는 잎사귀 부분에는 알고리듬에 따라서 다르게 형성되는 그룹이나 사용자들이 위치하고 트리의 각 노드에 키를 할당한다. 잎사귀에 위치한 사용자들이나 그룹에 변동이 생길 때에는 관련된 부분의 노드들의 키만을 바꾸어서 전반적인 키 교환의 복잡도를 줄이는 효과를 갖는다. 각 노드들에 위치한 키는 바로 밑의 하위 키에 의해 암호화되어서 전송이 되는 구조를 가지며 이에 의해서 모든 사용자나 그룹은 가장 상단에 위치한 루트 키를 공통적으로 가지게 된다. 이런 기본적인 구조를 바탕으로 사용자에게 변동이 발생되었을 때에는 관련된 부분의 노드에 위치한 키를 변경 시켜준다. 예를 들어 예를 들어 G5에 변동이 발생하는 경우에는 K6를 K6'로, K3를 K3'로, K1을 K1'로 변경한다. 또한, 변경 후에는 하위에서 상위로 암호화 되는 구조를 이용하여 변경 정보를 송신한다. 먼저 K6'를 송신하고, K3'를 K6‘로 암호화 하여 전송하고, 또한 K3'의 자식 노드에 해당하는 K7으로 암호화하여 전송한다. 한단계 더 올라가서 K1'를 K3'로 암호화 하여 전송하고 마찬가지로 K1'의 자식 노드에 해당하는 K2'로 암호화하여 K1'를 전송한다. 따라서, 그림 3과 같은 구조에서는 총 5번의 키 갱신을 위한 메시지 전송이 필요하고 일반적으로 노드당 k개의 가지를 가지면서 깊이가 d단계의 노드를 갖는 트리에서는 kd-1 번의 메시지 전송이 필요하다. (예를 들어, 그림 3에서는 k가 2이고 d가 3이다.) 따라서, LKD구조를 적용하면 사용자나 그룹의 수가 많아질수록 효과적으로 메시지를 갱신할 수 있는 구조를 갖을 수 있다.

3-1. UGLKD (User Group Logic Key Distribution)

LKD를 적용하기 위해서는 가입자를 트리의 잎사귀의 어떤 규칙에 의해서 배치하느냐에 그 형태가 달라진다. 가장 직접적인 방법으로 사용자를 각각 하나의 잎사귀에 매핑하는 방법을 제안한다. 이 방법을 사용하면 가장 낮은 곳에 위치한 노드에 자연스럽게 사용자 그룹이 형성된다.

이 방식을 구현하기 위해서 키 전달 형태는 다음과 같은 순서에 의해서 실시된다. 먼저 트리의 노드에 각각 독립된 키를 할당한다. 이 때에 형성된 트리의 깊이를 d라 한다면, 송신단에서는 MPK를 사용하여 가입자의 바로 상위 부모에 해당하는 노드의 키 TK(d) (트리의 깊이 d에 위치한 노드에서의 트리 키)를 암호화 하여 전송한다. 이 후에는 그림 4에 도식된 바와 같이 LKD와 마찬가지로 바로 루트키에 도달할 때까지 바로 상위의 키를 암호화 하여 전달한다. 최종적으로 루트키에 도달하면 루트키 TK(0) 로 AK를 암호화하여 전송하고 AK로 CW를 암호화하여 전송한다. 이 방식에서 주기적인 키 개정을 위해서 송신되는 키는 가입자별로 자신이 속하는 가장 하위 노드의 키이기 때문에 U_A개의 가입자 별 메시지의 전송이 필요하다. 자세한 전송 메시지 양은 4장에서 제공하도록 한다.

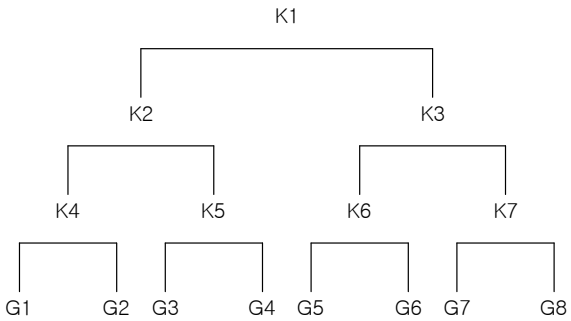

그림 3. LKD 구조
Fig. 3. LKD architecture.

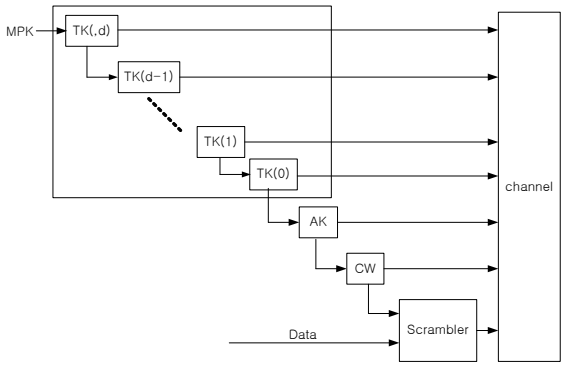

그림 4. UGLKD 송신단 암호화 구조
Fig. 4. Encryption Structure for UGLKD.

가입자의 변동이 생겼을 때에는 해당 가입자에게 직접할당된 노드의 키를 바꾸고 이 노드와 연결되어 있는 키를 LKD와 동일한 규칙에 의해서 변경을 시켜 준다. 따라서, 가입자 레벨에서 변경되는 키 관련 메시지는 (k,d) 트리의 경우에 k 개의 메시지 갱신과 (kd-1)개의 트리 키의 갱신과 N_C개의 AK 키 갱신이 필요하다.

3-2. CGLKD (User Group Logic Key Distribution)

가입자를 트리의 잎사귀에 배치하는 방법 중에 하나는 미리 가입자 그룹을 만든 후에 해당 그룹을 잎사귀에 매핑하는 방법이다. [6]에서 가입자를 가입된 채널에 따라서 그룹핑 하는 방법이 제시되었다. 따라서 이 방법을 적용하면 제안 방법은 [6]의 방법을 확장하여 그룹에 트리 구조를 적용하는 형태가 된다.

이 방법의 적용을 위해 N_{CG}개의 채널 그룹을 매핑할 수 있는 트리를 만들고, 각 노드 마다 키를 부여한 후에, 각 채널 그룹에는 CGK (Channel Group Key)를 할당한다. 각 가입자는 MPK로 CGK를 암호화하여 송신하고 각 채널 그룹은 CGK로 트리의 가장 하위에 위치한 자기 부모에 해당하는 노드의 키를 암호화하여 전송한다. 루트 키에 도달할 때까지 LKD와 동일한 암호화 과정을 실시한다. 루트 키에 도달 후에는 UGLKD와 동일하게 AK를 루트키로 암호화하고 AK로 CW를 암호화 한다.

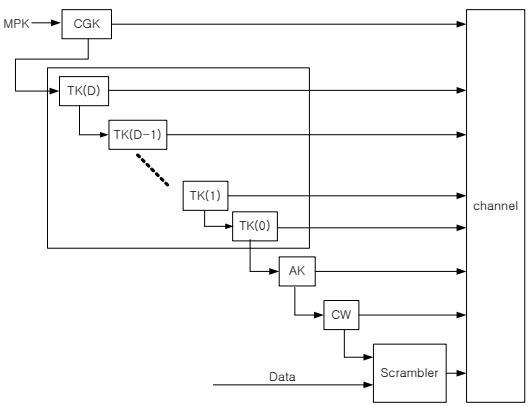

그림 5. CGLKD 송신단 암호화 구조
Fig. 5. Encryption Structure for CGLKD.

UGLKD와 마찬가지로 주기적인 키 개정에서 사용자 단위로 전송되는 키는 CGK만을 전송하면 된다. 가입자의 변동이 생겼을 때에는 변동된 가입자와 동일한 CGK를 사용하는 가입자에 대해서 CGK를 개정하고 (K,D) 트리를 사용하는 경우에 (KD-1)개의 트리 키의 갱신과 N_C개의 AK 키 갱신이 필요하다.

Ⅳ. 메시지 전송 오버헤드 분석

본 절에서는 세 가지 관점에서 기존 시스템과 제안 시스템의 메시지 전송 오버헤드를 분석한다. 모든 시스템에 있어서 CW는 짧은 주기로 개정해 주어야 한다. 따라서, SP (Short Period) 마다 개정을 위해서 필요로 하는 오버헤드 전송율, EMM과 같은 LP (Long Period) 마다 키를 개정하기 위해서 필요로 하는 오버헤드 전송율과 가입자의 변동에 의해서 비주기적으로 이벤트 발생에서 유발되는 오버헤드 전송율에 대한 분석을 실시한다.

4-1. CAS

ECM과 같은 짧은 주기에 걸쳐서 보내는 메시지의 주기를 T_{SP}라고 한다면 CAS의 경우에는 각 채널마다 ECM의 메시지를 보내주기 때문에 ECM의 메시지의 크기를 D_{ECM}이라 한다면 SP에 필요한 메시지의 전송 오버헤드는 다음과 같이 계산된다.

$$r_{CAS-SP} = N_C \times D_{ECM} / T_{SP}. \quad (1)$$

LP 동안에는 EMM이 보내지는데 가입자별/채널별로 보내지기 때문에 전송 오버헤드는 전송주기를 T_{LP}, EMM 메시지의 크기를 D_{EMM}라고 한다면 관련 메시지의 오버헤드는 다음과 같다.

$$r_{CAS-LP} = U_A \times N_C \times D_{EMM} / T_{LP}. \quad (2)$$

가입자 변동이 발생할 경우 AK를 개정하기 위해서는 사용자별 채널 별로 EMM 메시지를 전송해야 하기 때문에 변동에 따른 개정 최대 시간을 T_U라고 했을 때에 비주기적 개정에 필요한 메시지 오버헤드

는 다음과 같다.

$$r_{CAS-AP} = N_C \times U_A \times D_{EMM} / T_U. \quad (3)$$

식(3)에서 가입자 변경에 대해서 빠른 시간에 키 개정을 필요로 하고 가입자가 많은 시스템에서는 메시지 오버헤드 전송이 매우 커지는 것을 관찰할 수 있다.

4-2. SFLH

SFLH의 CW를 전송하는 구조는 CAS와 동일하기 때문에 SP에 필요한 메시지의 전송 오버헤드는 CAS와 동일하게 계산된다.

$$r_{SFLH-SP} = N_C \times D_{ECM} / T_{SP}. \quad (4)$$

LP에 필요한 메시지 전송 오버헤드는 사용자 마다 RGK 정보를 보내고 채널 그룹에 대해서 AK를 전송하기 때문에 RGK와 가입자 프로그램 관련 메시지의 데이터량을 $\overline{D_{RGK}}$라고 하고 AK를 보내는 메시지의 데이터량을 D_{AK}라고 하면 다음과 같이 간단히 계산된다.

$$r_{SFLH-LP} = (U_A \times \overline{D_{RGK}} + N_{CG} \times D_{AK}) / T_{LP}. \quad (5)$$

가입자 변동이 발생할 경우 AK를 개정하기 위해서는 변동되는 가입자가 속한 채널 그룹의 키를 변동해야 하기 때문에 변동 가입자의 채널 그룹에 속한 가입자 수만큼에 대해서 RGK를 개정하고 개정된 AK를 각 RGK별로 전송해야 한다. 따라서, 이를 고려한 비주기적 개정에 필요한 메시지 오버헤드는 다음과 같다.

$$r_{SFLH-AP} = (|CG_i| \times D_{RGK} + N_{CG} \times D_{AK}) / T_U. \quad (6)$$

위식에서 D_{RGK}는 그룹키와 관련된 데이터 양, CG_i 는 변경된 가입자가 i번째 그룹에 속해 있다는 가정을 하고 $|CG_i|$ 는 i번째 그룹에 속한 가입자 수를 나타낸다.

CAS와 비교하여 크게 달라진 점은 가입자 변동이 발생시 시스템의 모든 사용자에 대해서 키 정보를 전송하는 것이 아니라 해당 그룹에 대해서 키를 전송함으로써 전송의 오버헤드가 감소된다는 점이다.

4-3. UGLKD

UGLKD의 CW를 전송하는 구조는 앞의 방법들과 동일하므로 SP에 필요한 메시지의 전송 오버헤드는 다음과 같다.

$$r_{UGLKD-SP} = N_C \times D_{ECM} / T_{SP}. \quad (7)$$

LP 동안에는 사용자 단위로는 트리의 가장 하위 부분에 해당하는 키만을 업데이트 하고 트리의 각 노드의 키를 업데이트하고 AK를 루트 키를 사용하여 업데이트 하기 때문에 실제 LP 동안에 키를 개정하기 위해 필요한 데이터율은 다음과 같다.

$$r_{UGLKD-LP} = (U_A \times \overline{D_{TK}} + \frac{(k^d - 1)}{k - 1} \times D_{TK} + N_C \times D_{ECM}) / T_{LP}. \quad (8)$$

위 식에서 D_{TK}는 실제 트리 키만 관련된 데이터 양이고 $\overline{D_{TK}}$는 트리 키 정보와 프로그램 정보까지 포함하는 데이터 양이다.

가입자의 변동이 생기는 경우에는 트리의 관련된 키만을 개정하면 된다. 따라서 먼저 가장 하단에 위치하는 변동이 생긴 가입자의 노드에 속하는 가입자들에 대해서 모두 해당 노드의 키를 개정하고 나머지 관련된 상위의 노드의 키를 개정한다. 따라서 이를 위해 필요한 오버헤드 전송율은 다음과 같다.

$$r_{UGLKD-AP} = (k \times D_{TK} + (dk - 1) \times D_{TK} + N_C \times D_{ECM}) / T_U. \quad (9)$$

UGLKD는 SFLH에 비해서 (6)과 (9)를 비교시 채

널 그룹의 수나 사용자 수에 따라서 제한적인 조건에서 가입자 변동에 따른 오버헤드를 크게 감소 시킬 수 있을 것으로 예상된다.

4-4. CGLKD

CGLKD의 CW를 전송하는 구조는 앞의 방법들과 동일하므로 SP에 필요한 메시지의 전송 오버헤드 $r_{CGLKD-SP}$는 다음과 같다.

$$r_{CGLKD-SP} = N_C \times D_{ECM} / T_{SP}. \quad (10)$$

CGLKD는 채널 그룹에 대해서 트리 계층 구조를 임베드시킨 구조이기 때문에 가입자당 보내는 정보량은 SFLH와 동일하고 트리 관련한 키 정보 전송과 AK를 루트키 단위로 보낸다는 것이 다르다. 따라서, 이를 고려한 LP 동안의 오버헤드 전송율 $r_{CGLKD-LP}$은 다음과 같이 계산된다.

$$r_{CGLKD-LP} = (U_A \times \overline{D_{CGK}} + K^D \times D_{TK} + N_C \times D_{AK}) / T_{LP}. \quad (11)$$

위 식에서 $\overline{D_{RGK}}$ 는 CGK와 가입자 프로그램 관련 메시지의 데이터량을 나타내고 (K, D)는 CGLKD에 사용된 트리의 노드당 가지의 개수와 깊이를 표시한다.

i번째 가입자 변동이 발생하는 경우에는 SFLH와 유사하게 변동이 생긴 그룹의 키를 개정하고 관련된 트리내에서의 키를 개정하기 때문에 이 때에 오버헤드 전송율$r_{CGLKD-AP}$은 다음과 같다.

$$r_{CGLKD-AP} = (|CG_i| \times D_{RGK} + (DK-1) \times D_{TK} + N_C \times D_{AK}) / T_U. \quad (12)$$

SFLH와 비교하여 가입자 변동시기나 LP동안의 개정에서 AK를 개정하기 위해서 기존의 SFLH는 그룹단위로 AK를 개정하였으나 제안 방법에서는 트리 구조를 사용하여 트리를 보내고 루트키를 사용하여 방송 채널 단위로 AK를 개정한다는 차이점을 가진다.

Ⅴ. 모의 실험

Ⅳ장에서 분석한 오버헤드 전송율을 비교하기 위해서 본 장에서는 다양한 가입자 수와 다양한 채널 수에 따라서 (1)에서 (12)번까지의 수식을 평가하였다. 이를 위한 가정은 다음과 같다. 첫째, 사용자별로 LP동안에 보내지는 사용자 단위 메시지의 크기는 같다고 가정하였다. 즉, $\overline{D_{TK}} = \overline{D_{RGK}} = \overline{D_{CGK}} = D_{EMM}$ 또한, D_{EMM}은 [8]에 따라서 488비트로 설정하였다. 둘째, 채널 그룹별로 동일한 사용자를 갖는다고 가정하였다. 실제 시스템에서는 채널 그룹에 따라서 사용자 수가 다르지만, 채널에 따라서 사용자 수가 같다고 가정하는 것이 각 사용자의 가입 정보가 변경될 확률이 각 사용자 별로 같다고 하였을 때에 SFLH와 CGLKD의 비주기적 오버헤드 전송에 대한 하한값을 제공하기 때문에 비교에 있어서 용이하다. 셋째로, 각 트리의 노드의 키 전송에 필요한 데이터 량과 AK를 전송에 필요한 데이터량은 D_{ECM}과 같다고 정의를 하고 이 값은 [8]에 따라서, 168비트로 고정하였다. 넷째, 채널 설정된 채널 그룹수가 총 가입자 수보다 많을 때에는 채널 그룹수는 총 가입자 수와 동일하게 설정하였다. 이는 여분의 채널 그룹은 사용되지 않을 것이기 때문이다.

각 오버헤드 전송율을 계산하기 위해서는 메시지 전송 시간을 고려해야 하는데 이 값은 다음과 같이 설정하였다. T_{SP}는 1초, T_{LP} 는 30일, T_U는 1일로 설정하여 실제 시스템에서 쓰는 시간 제한과 유사하게 설정하였다. 또한, 채널의 수는 실제 케이블 방송수와 비슷하게 100개로 고정하였다.

그림 6에서는 가입자 수가 고정된 상태에서 채널 그룹의 수에 따라서 가입자 변동에 따라 필요로 하는 오버헤드 전송율을 비교하였다. 10^8정도의 많은 가입자를 갖는 시스템에서는 SFLH는 채널그룹의 수가 증가하면서 채널 그룹당 사용자 수의 감소가 생기면서 전송율이 감소하다가 일정 임계값을 넘으면 AK 개정을 위한 오버헤드가 지배적이되면서 전체적으로 오버헤드 전송율이 증가하는 현상을 갖는다. 반면에 CGLKD는 가입자 수가 많을 때에는 채널 그룹당 가입자가 수에 의한 오버헤드가 지배적인 인자가 되기

때문에 채널 그룹수가 증가할 수록 오버헤드가 감소한다. 하지만, UGLKD는 채널 그룹 수에 무관하게 동작하게 때문에 채널그룹수에 관계없이 일정한 값을 갖으며 가입자 수가 많으나 적으나 오버헤드가 적은 것을 관찰할 수 있다. 예를 들어, $U_A = 10^8$이고 채널 그룹의 수가 적을 때에는 CAS에 비해서는 약 $1/10^7$수준이고 SFLH에 비해서는 약 $1/10^4 \sim 1/10^5$ 정도의 오버헤드 감소를 갖는다.

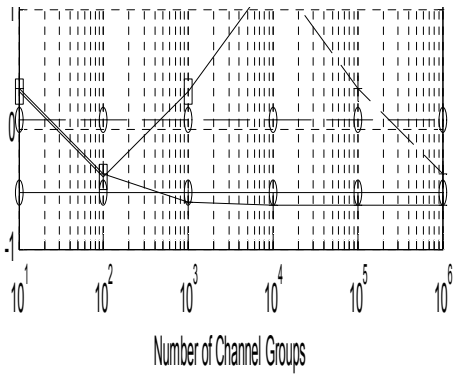

그림 6. 가입자 변동에 따라 요구되는 오버헤드 전송율 (실선 : $U_A = 10^4$, 점선 : $U_A = 10^8$)

Fig. 6. Overhead transmission rate for change in a subscriber (solid line : $U_A = 10^4$, dotted line : $U_A = 10^8$) .

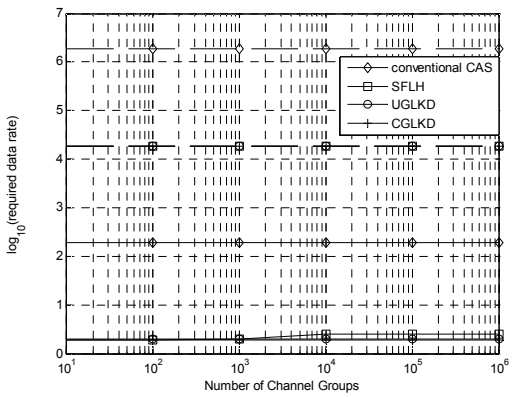

그림 7. LP 키 개정에 따라 요구되는 오버헤드 전송율 (실선 : $U_A = 10^4$, 점선 : $U_A = 10^8$)

Fig. 5. Overhead transmission rate for Key Update in Long Period (solid line : $U_A = 10^4$, dotted line : $U_A = 10^8$) .

그림 7에서는 그림 6과 동일환 환경에 LP 주기로 개정에 필요한 오버헤드 전송율을 비교하였다. 그림 6에서와 마찬가지로 CAS와 UGLKD는 채널 그룹수에 관계없이 일정한 값을 가지고 사용자 수가 클 때에는 사용자 수에 의한 인자가 지배적이기 때문에 SFLH와 CGLKD에서 마찬가지로 거의 일정한 값을 가지며 사용자 수가 적을 때에 SFLH에서 채널 그룹 증가에 대해서 약간 증가하는 현상을 보인다. 이는 수식 (5)에서 관찰되는 바와 같이 채널 그룹수가 가입자 수보다 많을 때에는 실제 운용 채널 그룹수는 사용자수와 같다는 가정 때문에 채널 그룹 수가 가입자 수와 같아지는 부분부터 증가된 값으로 일정한 값을 갖는 것이다. 이 결과로부터 가입자 수가 많을 때에는 CAS를 제외한 나머지 알고리듬이 거의 동일한 성능을 갖고 사용자가 적고 채널그룹 수가 많을 때에는 SFLH에 비해서 트리 구조에 의한 효과에 의해 UGLKD와 CGLKD가 효과적으로 오버헤드를 감소시키는 것을 확인할 수 있다.

그림 8에서는 고정된 채널 그룹 수에 대해서 가입자 수에 따른 가입자 변동시 메시지 오버헤드 전송율을 보여준다. SFLH는 $N_{CG} = 3$일 때에는 가입자 AK를 전송하는 오버헤드 보다 사용자 마다 RGK를 전송하는 오버헤드가 크기 때문에 가입자 수에 따라서 선형적으로 전반적인 오버헤드가 증가하나 $N_{CG} = 10^6$일 때에는 가입자 수가 적운 경우 실제 유효 AK전송 오버헤드는 가입자 수에 비례하기 때문에 가입자 수가 적을 때에는 선형적으로 증가하다가, 가입자 수가 채널 그룹수 보다 많은 경우에는 AK 전송 오버헤드가 지배적이기 때문에 거의 큰 증가가 보이지 않는다. UGLKD의 경우에는 채널 그룹 수에 관계없이 가입자 수의 증가에 따라서 전송 오버헤드가 로그 스캐일로 증가를 한다. 이는 트리 구조의 형태를 갖는데 기인한다. CGLKD는 채널 그룹의 수가 많아지면 키 개정을 해야하는 그룹내의 사용자 수가 줄어 들고 채널 그룹에 대해서 트리 구조를 적용하기 때문에 키 개정의 오버헤드가 줄어드는 효과가 상대적으로 크게 발생한다. 전반적으로는 채널 그룹수가 작을 때에는 가입자 수에 의한 오버헤드 증가가 지배적이기 때문에 SFLH와 UCLKD의 성능이 유사한 반면에 채널 그룹수가 클 때에는 채널당 사용자 수에 의존적이지 않은 UGLKD가 효율적이며 채널당 사용자 수의 감소와 채널 그룹핑 효과에 의해서 CGLKD

의 성능이 가장 효율적인 것으로 보인다.

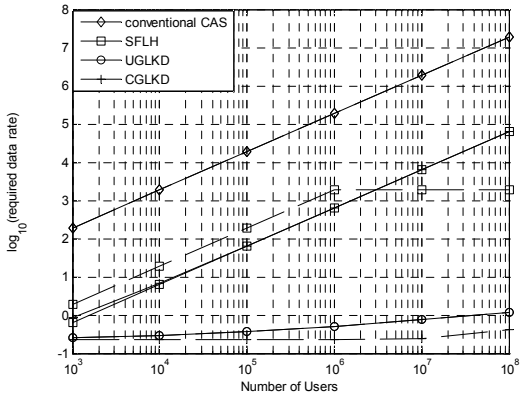

그림 8. 가입자 변동에 따라 요구되는 오버헤드 전송율 (실선 : $N_{CG}=3$, 점선 :$N_{CG}=10^6$)

Fig 8. Overhead transmission rate for change in a subscriber (solid line : $N_{CG}=3$, dotted line :$N_{CG}=10^6$) .

그림 9에서는 LP 동안에 주기적인 키 개정에시 고정된 채널 그룹 수에 대해서 가입자가 증가함에 따라 필요로 하는 오버헤드 전송율을 비교하였다. 모든 알고리듬이 사용자 단위의 키 개정이 필요하기 때문에 가입자 수에 따라서 선형적으로 증가하는 현상을 보인다. SFLH에서는 채널 그룹 수가 클 때에 AK를 채널 그룹 레벨에서 개정하기 때문에 UGLKD나 CGLKD에 비해서 상대적으로 조금 더 많은 오버헤드를 필요로 한다.

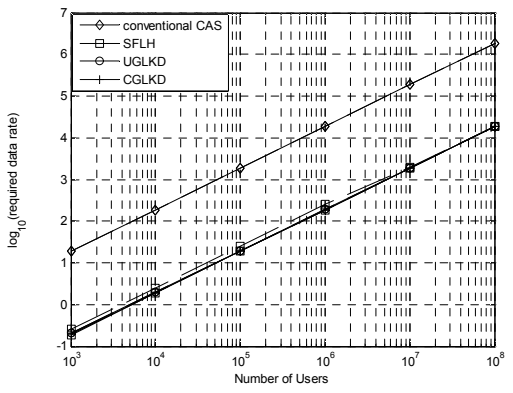

그림 9. LP 키 개정에 따라 요구되는 오버헤드 전송율 (실선 : $N_{CG}=3$, 점선 :$N_{CG}=10^6$)

Fig 9. Overhead transmission rate for Key Update in Long Period (solid line : $N_{CG}=3$, dotted line :$N_{CG}=10^6$) .

Ⅵ. 결 론

본 논문에서는 대역폭이 제한이 되는 방송 시스템에서 사용되는 자격 제어 시스템의 효과적인 키 개정을 위한 메시지 전송 알고리듬을 제안하고 메시지 오버헤드 전송율을 분석하였다. 제안된 알고리듬은 트리 계층 구조를 이용하여 가입자가 동적으로 변경되는 상황에서 기존의 CAS나 SFLH에 비해서 수 배에서 수 십만 배의 메시지 오버헤드 감소 효과를 갖는 것을 다양한 시스템 환경에서 확인하였다. 본 연구를 보다 복잡한 다양한 미디어를 통해 전송되는 헤테로 방송 시스템에서의 효율적인 접근 제어방법으로 확장은 미래의 가치 있는 연구로 예상된다.

참 고 문 헌

[1] EBU Project Group B/CA, Functional model of a conditional access system. EBU Technical Review, Winter, 1995.

[2] O. W. Bungum, "Transmultiplexing, transcontrol, and transscrambling of MPEG-2/DVB signal," International Broadcasting Convention, pp. 288-293, Sep. 12, 1996.

[3] Y. Nishimoto, A. Baba, T. Kurioka, and S. Namba, "A Digital Rights Management System for Digital Broadcasting Based on Home Servers," IEEE Trans. Broadcast. vol. 52, no. 2, pp. 167-172, Jun. 2006.

[4] H. Shirazi, "Security Architectures in Mobile Integrated Pay-TV Conditional Access System," Networks 2008, pp. 1-15, Oct. 2008.

[5] H. Cruickshank, M. P. Howarth, S .Iyengar, Z. Sun, "A Comparison between satellite DVB conditional access and secure IP multicast," IST'05, June 2005.

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

[7] Y. Lee, G. Lee, J. Lee, C. Ahn, S. Lee, and N.

Kim, "Effective Multiplexing Method for Conditional Access System in Terrestial DMB," ETRI Journal, vol.30, no.6, pp.859-681, Dec. 2008.

[8] H. Koo, O. Kwon, and J. Kim, "Key Refreshment Management for Conditional Access System in DTV Broadcasting," ICCE'05, Las Vegas, US, Jan. 2005.

[9] Y. Zhang, C. Yang, J. Liu, and J. Tian, "Broadcast Encryption Scheme and Its Implementation on Conditional Access System," WISA09, Nanchang, China, pp. 379-382, May. 2009.

양 장 훈 (梁長薰)

1996년 : 연세대학교 전파공학과(공학사)

1998년 : U.S.C Dept. of Electrical Engineering (공학석사)

2001년 : U.S.C Dept. of Electrical Engineering (공학박사)

2001년~2006년 : 삼성전자 책임연구원

2006년~현재 : 연세대학교 공과대학 전기전자공학부 연구 교수

관심분야 : CDMA, OFDMA, MIMO, Relay, Corss layer optimization, 간섭채널, 정보이론

김 동 구 (金東九)

1983년 : 한국항공대학교 통신공학과(공학사)

1985년 : U.S.C Dept. of Electrical Engineering (공학석사)

1992년 : U.S.C Dept. of Electrical Engineering (공학박사)

1999년~현재 : 연세대학교 공과대학 전기전자공학부 교수

관심분야 : UWB, CDMA, Scheduling scheme, MIMO, Relay