IPTV 를 위한 프로그램 가치를 고려하는 적응적인 그룹 키 갱신 방법[1]

이상호*, 김유나*, 김종*, 이진호**
*포항공과대학교 컴퓨터공학과
**주식회사 알티캐스트
e-mail : sangho2@postech.ac.kr

Program-Value Aware Adaptive Group-Key Rekeying for IPTV

Sangho Lee*, Yuna Kim*, Jong Kim*, Zino Lee**
*Dept. of Computer Science and Engineering, POSTECH
**Alticast Corporation

요 약

인터넷 프로토콜 텔레비전(IPTV) 시스템에서 특정 프로그램을 허가된 가입자에게만 전달하기 위해 그룹 키 관리 방법을 이용할 수 있다. 그러나 기존의 그룹 키 관리 방법은 가입자의 수가 많아지거나 가입자가 서비스에 자주 가입하고 탈퇴할수록 서버의 부하가 커진다는 문제점이 있다. 이를 해결하기 위한 많은 연구들이 진행되어왔지만 해당 연구들은 IPTV 시스템의 특성을 고려치 못했다는 단점이 있다. 우리는 IPTV 시스템의 특성을 고려한 새로운 그룹 키 갱신 방법을 제안한다. 제안 방법은 현재 IPTV 채널 상에서 전송되는 프로그램의 가치를 고려해서 그룹 키 갱신 주기를 조절하는 방법이다. 이를 통해서 서버의 부하를 줄일 수 있을 뿐만 아니라 프로그램의 가치에 따라서 차등적인 보안 수준을 제공할 수 있다.

1. 서론

인터넷 프로토콜 텔레비전(IPTV)은 TV 프로그램을 인터넷을 통해서 가입자들에게 전달하는 기술이다. IPTV 시스템은 보통 IP 멀티캐스트 기술을 사용해서 한 번의 전송으로 다수의 가입자들에게 프로그램을 전달한다. 그러나 IP 멀티캐스트 기술은 전송 데이터에 대한 수신자의 접근 권한 소유 여부를 판단하지 않기 때문에 권한이 없는 수신자가 데이터에 접근할 수 있다는 문제점이 있다. 따라서 암호화와 같은 접근 제어 기술을 통해서 권한이 없는 수신자가 데이터에 접근하는 것을 차단해야만 한다.

그룹 키 관리 방법은 비밀 키를 그룹에 할당하고 또한 그 비밀 키를 갱신하기 위해 사용되는 기술이다[1]. 이 방법은 IP 멀티캐스트 기술을 사용하는 IPTV 시스템에도 사용될 수 있다. 예를 들어, 특정한 IPTV 채널을 시청할 수 있는 권한을 가진 가입자들을 그룹 키 관리 방법을 통해서 하나의 그룹으로 묶고, 해당 그룹에 소속된 가입자에게만 비밀 키를 전달한다면, IPTV 서버는 해당 채널의 데이터를 해당 비밀 키로 암호화하는 것을 통해서 접근 제어를 할 수 있다. 그러나 그룹 키 관리 방법은 그룹에 소속된 참여자의 수와 그룹에 대한 가입 및 탈퇴 요청에 의한 그룹 키 갱신 주기의 변화에 큰 영향을 받는다는 문제점이 있다. 특히 기존의 그룹 키 관리 방법이 많이 사용하는 개별적 키 갱신 방법은 그룹에 변화가 생길 때마다 키 갱신을 수행하기 때문에 보안성은 높지만 시스템의 부하가 크다는 단점이 있다.

그룹 키 갱신에 의한 시스템 부하를 줄이기 위해서 주기적 키 갱신, 배치 키 갱신, 그리고 가치 손실을 고려한 키 갱신 방법 등이 제안되었다. 주기적 키 갱신은 일정 주기 동안의 가입 및 탈퇴 요청을 모아서 처리하는 방법이고[2], 배치 키 갱신 방법은 일정 개수의 가입 및 탈퇴 요청을 모아서 한 번에 처리하는 방법이다[3][4]. 두 방법 모두 키 갱신에 필요한 시스템의 부하를 줄일 수 있지만 전송되는 데이터의 가치를 고려치 않기 때문에 데이터 제공자의 실제 손실을 고려하지 못한다는 단점이 있다. 이를 해결하기 위해 데이터가 노출되었을 때 입게 될 손실을 추산해서 그 손실이 일정 값을 넘어섰을 때 키 갱신을 하는 방법이 제안되었다[5][6]. 이 방법들은 특정 그룹을 위한 데이터의 가치가 동일하다고 가정한다. 그러나 IPTV 의 경우 한 채널에서도 전송되는 프로그램에 따라서 그 가치가 모두 다를 수 있기 때문에 기존 방법들을 IPTV 환경에 그대로 적용하긴 어렵다.

[1] 본 연구는 주식회사 콘트론의 지원과 지식경제부 및 정보통신연구진흥원의 대학 IT 연구센터 지원사업의 연구결과로 수행되었음 (IITA-2008-C1090-0801-0045)

그룹 키 갱신에 관한 기존의 연구들은 IPTV 에 적합하지 않다. 왜냐하면 기존의 방법들은 IPTV 에선 한 채널을 통해서 전송되는 프로그램이라도 다른 가치를 가질 수 있다는 점을 고려치 못하였기 때문이다. 이런 특성은 데이터의 가치를 고려치 않는 주기적 키 갱신 방법과 배치 키 방법뿐만 아니라 기존의 가치 손실을 고려한 키 갱신 방법들도 동일하다. 그러므로 우리는 IPTV 의 특성을 고려한 가치 손실 기반의 그룹 키 갱신 방법을 제안한다. 제안 방법은 현재 전송되는 프로그램의 가치, 해당 프로그램이 노출된 시간, 그리고 프로그램에 불법 접근할 수 있는 가입자의 수를 이용해서 최적의 키 갱신 시점을 계산하는 방법이다. 키 갱신 시점이 결정되면 기존의 배치 키 갱신 방법 등을 이용해서 키 갱신을 수행할 수 있다. 또한 제안 방법은 프로그램 가치에 따라 차등적인 보안 수준을 제공할 수 있다.

본 논문의 구성은 다음과 같다. 제 2 장에선 시스템 모델과 가정에 대해서 설명한다. 제 3 장에선 제안 방법에 대해서 소개한다. 제 4 장에선 제안 방법을 분석한다. 마지막으로 제 5 장을 통해서 본 논문을 마무리 지을 것이다.

2. 시스템 모델 및 가정

제안하는 시스템은 시청 시간 기반의 과금 정책을 지원한다고 가정한다. 이런 과금 정책하에선 가입자가 어떤 채널을 시청하고 있는지, 해당 채널에서 어떤 프로그램이 방영되고 있는지, 그리고 가입자가 해당 프로그램을 언제부터 얼마나 보았는지를 파악해야 한다. 그리고 가입자의 특정 채널에 대한 불법 접근을 막기 위해서 가입자가 해당 채널에 대한 시청을 시작할 때 채널 키의 갱신을 통해서 해당 채널의 과거 데이터에의 접근을 차단해야 하며, 가입자가 해당 채널을 더 이상 시청하지 않는다면 키 갱신을 통해서 해당 가입자가 추후에 그 채널에 접근하는 것을 차단해야 한다. 특정 채널에 대한 시청 시작과 종료를 해당 채널의 시청 그룹에 대한 가입과 탈퇴로 본다면 기존의 그룹 키 관리 방법을 이용해서 위의 요구사항을 만족시킬 수 있다. 제안하는 시스템 모델에서 동일 채널을 통해서 전송되는 프로그램들의 가치는 모두 다 다를 수 있다고 가정한다. 각 프로그램의 가치는 프로그램 제공자와 IPTV 서비스 제공자의 합의에 의해서 미리 결정되어 있다고 가정한다.

3. 제안 방법

3.1 개요

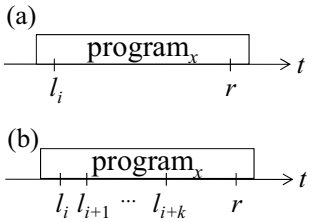
제안 방법은 특정 채널에 대한 가입이나 탈퇴로 인해 해당 채널의 그룹 키의 갱신이 필요할 때 바로 키 갱신을 하는 것이 아니라 키 갱신의 지연에 따른 프로그램 가치의 손실을 예측하여 그 값이 일정 수준을 넘어서는 시점에 키 갱신을 수행하는 방법이다. 가치 손실을 계산하기 위해 현재 채널 상에서 전송되는 프로그램의 시간 당 가치, 프로그램이 노출 된 시간, 그리고 해당 채널에 가입하거나 탈퇴한 가입자의 수를 이용한다. 프로그램 제공자나 IPTV 서비스 제공자가 감내할 만한 손실 값을 미리 결정해 놓으면 이 값을 이용해서 키 갱신을 해야 할 시점을 계산할 수 있다. 표 1 은 이 장에서 사용하는 기호들의 의미를 정리해 놓은 것이다.

<표 1> 표기법

기호	의미
l_i	i 번째 가입자의 탈퇴 시점
j_i	i 번째 가입자의 가입 시점
r	키 갱신이 일어나는 시점
e_x	프로그램 x 의 종료시점
L	시간 당 기대 손실 값
v_x	프로그램 x 의 단위 시간 당 가치
$r(L)$	주어진 L 값으로 키 갱신 시점 계산

3.2 탈퇴에 대한 키 갱신 방법

가입자가 특정 채널에서 탈퇴하는 경우 키 갱신을 해야만 그 가입자가 차후에 해당 채널에 접근하는 것을 차단할 수 있다. 이 절에선 우리가 제안하는 탈퇴에 대한 그룹 키 갱신 시점 계산 방법에 대해 소개한다. 첫 번째 탈퇴와 키 갱신과의 간격이 한 프로그램의 길이보다 작다고 가정하면 탈퇴에 대한 그룹 키 갱신은 크게 한 프로그램 내에서의 키 갱신과 두 프로그램을 걸친 키 갱신으로 나눌 수 있다.



(그림 1) 탈퇴에 대한 프로그램 내에서의 키 갱신. (a) 한 가입자만 탈퇴한 경우. (b) $k+1$ 명의 가입자가 탈퇴한 경우.

그림 1(a)는 한 가입자의 탈퇴에 대한 키 갱신이 한 프로그램 내에서 일어나는 경우를 나타낸다. 이 경우 L 은 $v_x(r-l_i)$ 로 계산할 수 있다. 이 식을 바탕으로 프로그램 제공자와 IPTV 서비스 제공자가 설정한 손실을 감내할 수 있는 값(L)을 통해 키 갱신 시점을 구하는 아래와 같은 공식을 유도할 수 있다.

$$r(L) = l_i + \frac{L}{v_x} \qquad (1)$$

그림 1(b)는 $k+1$ 명의 가입자의 탈퇴에 대한 키 갱신이 한 프로그램 내에서 일어나는 경우다. 이 경우 L 은 $\sum_{a=i}^{i+k} v_x(r-l_a)$ 로 계산할 수 있다. 이를 통해 키 갱신 시점을 구하는 공식을 유도할 수 있다.

$$r(L) = \frac{\sum_{a=i}^{i+k} l_a}{k+1} + \frac{L}{(k+1)v_x} \qquad (2)$$

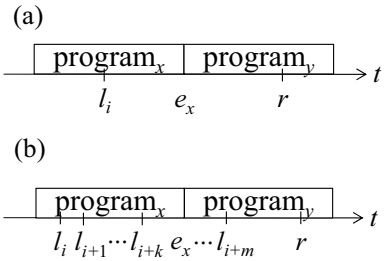
그러나 k 가 아무리 크더라도 식 (2)가 어떤 특정한 값에 수렴해야만 시스템의 보안성을 유지할 수 있다. 정리 1 을 통해서 우리는 식 (2)가 수렴함을 보인다.

정리 1. 한 프로그램 내에서의 키 갱신에서 탈퇴자의 수가 무한대이더라도 키 갱신이 일어난다.

증명. 식 (2)에서 k 가 무한대로 갈 때 r 값은

$$\begin{aligned}\lim_{k\to\infty} r(L) &= \lim_{k\to\infty} \frac{\sum_{a=i}^{i+k} l_a}{k+1} + \frac{L}{(k+1)v_x} \\ &\le \lim_{k\to\infty} \frac{(k+1)l_{i+k}}{k+1} + \frac{L}{(k+1)v_x} \\ &= \lim_{k\to\infty} l_{i+k} + \frac{L}{(k+1)v_x} \\ &= \lim_{k\to\infty} l_{i+k}\end{aligned}$$

위의 식은 한 프로그램 내에서의 키 갱신에서 무한대의 탈퇴자가 있는 경우 키 갱신 시간이 마지막 탈퇴가 일어난 시점보다 빠르거나 같다는 것을 보인다. 이는 아무리 많은 탈퇴자가 있다고 하더라도 키 갱신이 결국에는 일어난다는 것을 뜻한다. 그러므로 한 프로그램 내에서의 키 갱신에서 탈퇴자의 수가 무한대에 접근해도 키 갱신이 일어난다. □



(그림 2) 탈퇴에 대한 두 프로그램에 걸친 키 갱신. (a) 한 가입자만 탈퇴한 경우. (b) $m+1$ 명의 가입자가 탈퇴한 경우 ($k+1$ 명은 프로그램 x 시청 중에 탈퇴).

그림 2(a)는 한 가입자의 탈퇴에 대한 키 갱신이 두 프로그램을 걸쳐서 일어나는 경우를 나타낸다. 이 경우 L 은 $v_x(e_x - l_i) + v_y(r - e_x)$ 로 계산할 수 있다. 이 값을 바탕으로 키 갱신 시점을 구하는 아래와 같은 공식을 유도할 수 있다.

$$r(L) = l_i + \frac{L}{v_y} - \frac{(e_x - l_i)(v_x - v_y)}{v_y} \quad (3)$$

그림 2(b)는 $m+1$명의 가입자의 탈퇴에 대한 키 갱신이 두 프로그램을 걸쳐 일어나는 경우를 나타낸다. 이 경우 L 은 $\sum_{a=i}^{i+k} v_x(e_x - l_a) + \sum_{a=i}^{i+k} v_y(r - e_x) + \sum_{a=i+k+1}^{i+m} v_y(r - l_a)$ 로 계산할 수 있고 이를 통해 키 갱신 시점을 구하는 다음 공식을 유도할 수 있다.

$$r(L) = \frac{L - (k+1)v_x e_x + v_x \sum_{a=i}^{i+k} l_a + (k+1)v_y e_x + v_y \sum_{a=i+k+1}^{i+m} l_a}{(m+1)v_y} \quad (4)$$

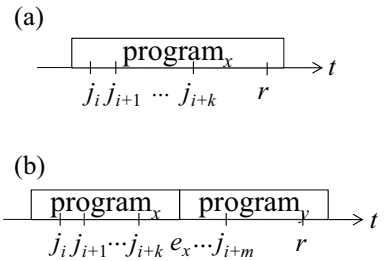
정리 2. 두 프로그램을 걸친 키 갱신에서 탈퇴자의 수가 무한대이더라도 키 갱신이 일어난다.

증명. 식 (4)에서 m 이 무한대로 갈 때 r 값은

$$\begin{aligned}\lim_{m\to\infty} r(L) &= \lim_{m\to\infty} \frac{L - (k+1)v_x e_x + v_x \sum_{a=i}^{i+k} l_a + (k+1)v_y e_x + v_y \sum_{a=i+k+1}^{i+m} l_a}{(m+1)v_y} \\ &= \frac{L - (k+1)v_x e_x + v_x \sum_{a=i}^{i+k} l_a + (k+1)v_y e_x + \lim_{m\to\infty} v_y \sum_{a=i+k+1}^{i+m} l_a}{\lim_{m\to\infty} (m+1)v_y} \\ &\le \frac{L - (k+1)v_x e_x + v_x \sum_{a=i}^{i+k} l_a + (k+1)v_y e_x + \lim_{m\to\infty} (m+1)v_y l_m}{\lim_{m\to\infty} (m+1)v_y} \\ &= \lim_{m\to\infty} l_m\end{aligned}$$

위의 식은 두 프로그램을 걸친 키 갱신에서 무한대의 탈퇴자가 있는 경우 키 갱신 시간이 마지막 탈퇴가 일어난 시점보다 빠르거나 같다는 것을 보인다. 이는 아무리 많은 탈퇴자가 있다고 하더라도 키 갱신이 결국에는 일어난다는 것을 뜻한다. 그러므로 두 프로그램을 걸친 키 갱신에서 탈퇴자의 수가 무한대에 접근해도 키 갱신이 일어난다. □

식 (1), (2), (3), (4)를 통해서 IPTV 서비스 제공자는 프로그램 가치의 손실을 고려한 키 갱신 시점을 계산할 수 있다. 해당 갱신 시점에서 하나 또는 다수의 탈퇴에 대한 키 갱신은 배치 키 갱신 방법을 이용하여 처리할 수 있다[3][4].



(그림 3) 가입에 대한 키 갱신. (a) $k+1$ 명의 가입이 한 프로그램 내에서 일어난 경우. (b) $m+1$ 명의 가입이 두 프로그램에 걸쳐서 일어난 경우 ($k+1$ 명은 프로그램 x 방송 중에 가입).

3.3 가입에 대한 키 갱신 방법

새로운 가입자가 생길 경우 키 갱신을 해야만 그 가입자가 과거 데이터에 접근하는 것을 차단할 수 있다. 그러나 새로운 가입자가 생길 때 마다 키 갱신을 하는 것은 가입자가 탈퇴할 때마다 키 갱신을 하는 것과 마찬가지의 성능 저하를 가져온다. 우리는 이러한 성능 저하를 줄이기 위해서 첫 번째 가입자가 가입하는 시점에 새로운 그룹 키를 만들어서 기존 가입자와 새로운 가입자에게 전달하고, 연달아서 가입하는 다른 가입자들에게도 해당 키를 개별적으로 전달하다가 손실 값이 일정 값을 넘어서면 새로운 가입자

들을 가입자 그룹에 한꺼번에 포함시키는 방법을 제안한다. 이는 배치 키 갱신 방법의 머징 알고리즘을 이용하면 쉽게 달성할 수 있다[4]. 이 방법은 첫 번째 가입 시점에 새로운 키를 만들어서 기존 가입자들과 새로운 가입자에게 전달한다는 점을 제외하면 3.2 절의 탈퇴에 대한 키 갱신 방법과 동일하다.

그림 3 은 가입에 대한 키 갱신을 보여준다. 이를 통해 탈퇴의 경우와 유사한 공식들을 유도할 수 있다.

$$r(L) = \frac{\sum_{a=i}^{i+k} j_a}{k+1} + \frac{L}{(k+1)v_x} \quad (5)$$

$$r(L) = \frac{L-(k+1)v_x e_x + v_x \sum_{a=i}^{i+k} j_a + (k+1)v_y e_x + v_y \sum_{a=i+k+1}^{i+m} j_a}{(m+1)v_y} \quad (6)$$

3.4 탈퇴/가입에 대한 키 갱신 방법

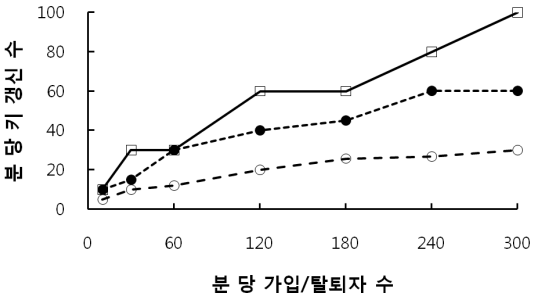
제안 방법에서 탈퇴와 가입에 대한 처리는 새로운 가입자에게 그룹 키 관리 방법이 아닌 개별 채널을 통해서 새로운 키를 전달한다는 차이점만 있고, 이는 그룹 키 갱신 시점을 계산하는 과정과 무관하다. 따라서 제안 방법은 특정 시점에 일어난 사건이 탈퇴냐 가입이냐에 상관없이 그대로 적용할 수 있다.

4. 분석

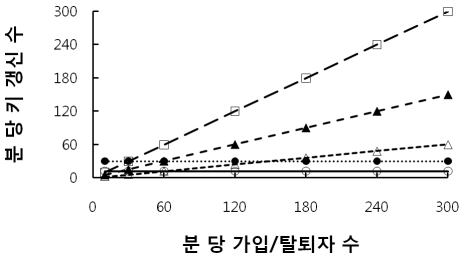
그림 4 는 제안 방법의 분 당 키 갱신 수가 분 당 가입/탈퇴자 수의 변화와 프로그램의 가치의 변화에 따라 어떻게 변하는 지를 보이는 그래프이다. 가입/탈퇴 시간은 균등 분포를 따른다고 가정하였다. 분석 결과 제안 방법은 프로그램의 가치가 높을수록 더 많은 키 갱신을 수행한다는 것을 확인할 수 있었다. 이는 제안 방법이 전송되는 프로그램의 가치에 따라서 차등적인 보안 수준을 제공할 수 있다는 것을 뜻한다. 또한 제안 방법은 개별적 키 갱신 방법, 주기적 키 갱신 방법, 배치 키 갱신 방법 등과는 다르게 가입/탈퇴 주기의 변화에 따라서 키 갱신 수도 능동적으로 변한다는 것을 그래프의 기울기 변화를 통해서 확인할 수 있다. 그림 5 는 동일한 상황에서 개별적 키 갱신, 배치 키 갱신 그리고 주기적 키 갱신의 키 갱신 수를 보여주는 그래프이다. 해당 방법들의 키 갱신 수는 프로그램 가치의 변화에 영향을 받지 않는다. 또한 그래프의 기울기가 일정한 점은 해당 방법들이 분 당 가입/탈퇴자 수의 변화에 대한 능동적인 대처를 하지 못한다는 점을 보여준다.

5. 결론

우리는 IPTV 에 적합한 그룹 키 갱신 주기 조절 방법을 제안했다. 제안 방법은 전송되는 프로그램의 가치에 따라 그룹 키 갱신 주기를 조절하는 방법이다. 이를 통해서 프로그램에 대한 접근 제어와 효율적인 키 갱신을 동시에 달성할 수 있었다. 분석 결과는 제안 방법이 프로그램의 가치에 따라 차등적인 보안 등급을 지정할 수 있다는 것과 가입/탈퇴자 수의 변화에 능동적으로 대응한다는 것을 보여줬다.



(그림 4) 분 당 가입/탈퇴자 수 및 프로그램 가치의 변화에 따른 제안 방법의 분 당 키 갱신 수 변화. 초 당 기대 손실 값은 100, 프로그램의 초 당 가치는 10(○), 50(●), 100(□).



(그림 5) 분 당 가입/탈퇴자 수 및 프로그램 가치의 변화에 따른 개별적 키 갱신 방법(□), 배치 키 갱신 방법(▲: 2 명, △: 5 명), 그리고 주기적 키 갱신 방법(●: 2 초, ○: 5 초)의 분 당 키 갱신 수 변화.

참고문헌

[1] D. Wallner, E. Harder, and R. Agee, “Key Management for Multicast: Issues and Architectures,” RFC 2627, 1999.

[2] S. Setia, S. Koussih, S. Jajodia, and E. Harder, “Kronos: A Scalable Group Re-Keying Approach for Secure Multicast,” Proceedings of 2000 IEEE Symposium on Security and Privacy, pp. 215—228, 2000.

[3] X. S. Li, Y. R. Yang, M. G. Gouda, and S. S. Lam, “Batch Rekeying for Secure Group Communications,” Proceedings of the 10th international conference on World Wide Web, pp. 525—534, 2001.

[4] W. H. D. Ng, M. Howarth, Z. Sun, and H. Cruickshank, “Dynamic Balanced Key Tree Management for Secure Multicast Communications,” IEEE Trans. Computers, vol. 56, no. 5, pp. 590—605, 2007.

[5] Q. Zhang and K. L. Calvert, “On Rekey Policies for Secure Group Applications,” Proceedings of the 12th International Conference on Computer Communications and Networks, pp. 559—564, 2003.

[6] G. Y. Lee, C. K. Jeong, Y. Lee, and H. J. Kim, “Re-key Interval Optimization for Secure Group Communications,” Journal of Information Science and Engineering, 23, pp. 893—905, 2007.