그룹 인증 기법을 이용한 이동 멀티미디어 방송 콘텐츠 사용자 관리 방안

*신기우 **박영훈 ***서승우

서울대학교

* shins0115@snu.ac.kr ** yhpark@cnslab.snu.ac.kr *** sseo@snu.ac.kr

Management of Digital Media Broadcasting Contents Users Based on Group Signature Scheme

* Shin, Ki-Woo ** Park, Young-Hoon *** Seo, Seung-Woo

Seoul National University

요약

급증하고 있는 이동 멀티미디어 방송 콘텐츠 서비스의 수요에 발맞추어 이 서비스를 이용하는 사용자들을 효율적으로 관리하는 방안에 대해 관심이 집중되고 있다. 1991년 Chaum과 van Heyst에 의해 소개된 그룹 인증 관리 기법은 익명성의 보장이나, 관리상의 편의로 인해 앞에서 언급된 문제를 해결하는 데 중요한 역할을 할 것으로 예상되었다. 하지만, 이후 소개된 몇 개의 그룹 인증 관리 기법들이 실제로는 익명성을 보장하지 못 하거나, 외부 그룹에 의해 악용될 수 있다는 점이 증명되어, 그룹 인증 관리 기법을 실제로 응용하기 이전에 안전성 보장을 위해 요구되는 적합한 기준들을 선정하고, 이 기준에 부합하는지를 살펴보는 일이 더욱 시급한 문제로 대두되었다.

이에 본 논문은 이동 멀티미디어 방송 콘텐츠 서비스를 이용하는 사용자들을 그룹 인증 기법으로 관리하는 데 있어, 요구되는 안전성 조건과 이에 적합한 그룹 인증 기법을 소개하고, 실제로 소개한 그룹 인증 기법이 본 논문에서 선정한 안전성 조건에 부합하는지를 증명하였다. 더불어, 그룹 인증 기법을 실제 효과적으로 응용할 수 있는 비즈니스 모델을 제안하여 그룹 인증 기법의 효용 및 앞으로의 개발 방향을 제시하였다.

1. 서론

무선 이동통신 기기를 이용한 이동 멀티미디어 방송의 수요가 급격히 증가함에 따라, 적어도 몇 년 내에 급증할 것으로 예상되는 이 분야의 방송 콘텐츠 사용 가입자 정보의 비밀성을 보장하고 관리의 효율성을 증가시키는 방안에 관하여 관심이 증가하고 있다. 현재 무료로 제공되고 있는 이동 멀티미디어 방송 또한 몇 년 지나지 않아 수익성 창출을 위해 유료로 전환하거나, 타 방송 콘텐츠와의 차별성을 시도할 것으로 예상되므로, 이와 같은 새로운 패러다임에 맞추어 효율적이고 안전한 관리 기법을 개발하는 것이 중요한 문제로 부각되고 있다.

그룹 인증 기법은 1991년, Chaum과 van Heyst에 의해 소개된 인증 방식으로서, 기존의 일반적인 인증 방식과는 달리 메시지 서명자가 같은 그룹 내에 속해 있다는 점만 알 수 있기 때문에, 사용자의 익명성을 보장할 수 있다는 장점을 가진다.[1] 또한, 그룹 내에 속한 사용자의 퇴출이나, 복귀 등에 관한 관리 방법이 용이하여 개별 미디어 서비스를 제공받는 사용자 그룹의 관리를 위한 방안으로 사용할 수 있다. 다만, 기존의 그룹 인증 방식으로 제안된 여러 가지 scheme들이 특정한 집단에 의해 악용될 소지가 있고, 익명성을 보장하지 못 하는 것으로 드러남에 따라[2], 이동 멀티미디어 방송에 적용하기 이전에 인증 방식의 안전성을 확립하도록 요구되고 있다.

그룹 인증 방식에서 일반적으로 요구되는 안전성 조건은 다음과 같은 여섯 가지 특성을 지닌다. 위조 불가능성(Unforgeability), 익명성(Anonymity), 연관 부정성(Unlinkability), 혐의 부정성(Exculpability), 추적 가능성(Traceability).[2] 그러나 VANET(Vehiclular Ad-Hoc Network)에서 요구되는 안전성을 연구한 Xiaoting Sun(2007)의 논문에서도 볼 수 있듯이, 그룹 인증 방식에서 요구되는 안전성 조건은 응용 방향에 따라 다양하게 달라질 수 있다.[3]

비교적 최근의 멀티미디어 방송 서비스의 동향을 살펴보면, Google이 시도하고 있는 위치 기반 광고 서비스를 포함하는 LBS(Location Based Service)와 Youtube나 twitter와 같은 SNS(Social Networking Service)에서의 자발적 동영상 배포 서비스 등의 발전이 두드러진다. 관련된 기존의 연구는 주로 거점 기지국을 통해서 서비스 사용자에게 콘텐츠를 일방적으로 전달하는 방안에 집중되었다. 하지만 변화하는 시장에서는 사용자간의 공유가 패러다임을 주도할 것으로 예상되므로, 미래 이동 멀티미디어 방송의 흐름을 선도하기 위해서는 기존의 서비스 제공자에게서 서비스 사용자에게 일방적으로 콘텐츠를 제공하는 방식에서 나아가, 서비스 사용자들끼리 자발적으로 멀티미디어 콘텐츠를 공유할 수 있는 플랫폼의 구축이 요구된다.

본 논문의 구성은 다음과 같다. 먼저, 서비스 사용자 간의 정보 제공에서 사용되는 그룹 인증 기법의 안전성 요구 조건을 제시할 것이다. 이동 멀티미디어 방송에 적합한 응용 모델을 제시하고, 타당성을 살펴

볼 것이다. 또한, 지금까지 제기된 그룹 인증 관리 기법들 중에서 가장 적합하다고 판단되는 방식을 택해 이에 대해 살펴보고, 인증 방식이 안전성 요구 조건에 부합하는지 수학적으로 살펴볼 것이다. 마지막으로 제기한 인증 기법이 가지고 있는 효율성이나 안전성 상의 난점을 제기하고, 추후 연구 방향을 제시할 것이다.

2. 서비스 상 안전성 요구 조건

일반적인 그룹 인증 기법에서 요구되는 안전성 조건[2]과 무선 이동 상황에서 요구되는 안전성 조건들[3]을 이동 멀티미디어 콘텐츠 서비스 상황에 맞추어 필요한 조건들을 조합하였다.

1) 무결성 및 입증성(Integrity and Source Authentication) : 전달되는 모든 정보는 변화되지 않은 상태로 전달되어야 하며, 정보 전송자는 입증될 수 있어야 한다.

2) 위치 정보 제공성(Location Information Exposure) : 정보 수신자는 자신의 위치 정보를 제공할 수 있어야 한다.

3) 익명성(Anonymity) : 그룹 내 멤버는 위치 정보 외에 다른 정보를 제공할 필요가 없다.

4) 혐의 부정성(Exculpability) : 정보 수신자는 별도의 장치를 통해, 수용 권한이 없는 자에게 서비스를 제공하지 못 해야 한다.

5) 추적 가능성(Traceability) : 부정한 정보를 제공한 사실이 드러날 시에, 이를 제공한 사용자를 추적할 수 있어야 한다.

6) 효율성(Efficiency) : 처리 부하 면에서 효율적이어야 하며, 적절한 처리 수준을 유지해야 한다.

7) 강인성(Robustness) : 외부의 공격에도 서비스 기능이 잘 작동해야 한다.

3. 이동 멀티미디어 방송에서의 그룹 인증 기법 제안

많은 그룹 인증 기법이 제안되었지만, 외부의 공격에 취약하거나, 안전성 요구 조건을 만족하지 못 하는 것으로 증명되었다. 또한, 효율성 면이나 사용자 관리 측면에서 적합한 기능을 하지 못 하는 단점들이 지적되었다.[4] 여러 그룹 인증 기법 중에 Boneh(2004)가 제기한 short group signature scheme이 이동 멀티미디어 방송에서 사용하기에 가장 적절하다고 판단하였다.[5] 이 방식은 다음과 같은 5가지 단계를 가진다.

1) 키 생성(Key gen) : generator로 g_1과 g_2를 가지는 2개의 bilinear groups G_1, G_2가 있다고 하자. g_2를 G_2에서 랜덤하게 선택하고, $g_1 \leftarrow \psi(g_2)$가 되도록 한다. $h \xleftarrow{R} G_1 \setminus 1_{G1}$, $\xi_1, \xi_2 \xleftarrow{R} Z_P^*$로 선택하고, $u^{\xi_1} = v^{\xi_2} = h$ 가 되도록, $u, v \in G_1$에서 선택한다. 또한, $\gamma \xleftarrow{R} Z_P^*$, $w = g_2^{\gamma}$ 가 되도록 한다.

γ를 이용해, 각 사용자를 위한 tuple (A_i, x_i), $x_i \xleftarrow{R} Z_P^*$와 $A_i \leftarrow g_1^{1/(\gamma + x_i)} \in G_1$를 생성한다.

이 때, 이동 멀티미디어 사용자 개별을 위한 그룹 공용키는 $gpk = (g_1, g_2, u, v, h, w)$ 가 된다. 그룹 관리자를 위한 비밀키는 $gmsk = (\xi_1, \xi_2)$ 가 된다. 개별 사용자의 비밀키는 $gsk[i] = (A_i, x_i)$ 가 된다.

2) 서명(Sign) : 서명은 기본적으로 Hash function을 이용하게 되는데, $c \leftarrow H(M, T_1, T_2, T_3, R_1, R_2, R_3, R_4, R_5) \in Z_P$ 과정을 거치며, Hash function에 사용되는 값들은 다음과 같은 계산 과정을 거치게 된다.

$$\alpha, \beta \xleftarrow{R} Z_P$$

$$T_1 \leftarrow u^{\alpha},\ T_2 \leftarrow v^{\beta},\ T_3 \leftarrow A h^{\alpha+\beta}$$

$$\delta_1 \leftarrow x\alpha,\ \delta_2 \leftarrow x\beta$$

$$r_{\alpha}, r_{\beta}, r_x, r_{\delta_1}, r_{\delta_2} \xleftarrow{R} Z_P$$

$$R_1 \leftarrow u^{r_{\alpha}},\ R_2 \leftarrow v^{r_{\beta}}$$

$$R_3 \leftarrow e(T_3, g_2)^{r_x} \cdot e(h, w)^{-r_{\alpha}-r_{\beta}} \cdot e(h, g_2)^{-r_{\delta_1}-r_{\delta_2}}$$

$$R_4 \leftarrow T_1^{r_x} \cdot u^{-r_{\delta_1}},\ R_5 \leftarrow T_2^{r_x} \cdot v^{-r_{\delta_2}}$$

위의 값들을 hash function에 대입함으로서 얻은 challenge c를 이용해 나머지 계산을 수행하게 된다.

$$s_{\alpha} = r_{\alpha} + c\alpha,\ s_{\beta} = r_{\beta} + c\beta,\ s_x = r_x + cx,$$

$$s_{\delta_1} = r_{\delta_1} + c\delta_1,\ s_{\delta_2} = r_{\delta_2} + c\delta_2$$

지금까지 구한 값들을 통해 다음과 같은 서명을 생성하게 된다.

$$\sigma \leftarrow (T_1, T_2, T_3, c, s_{\alpha}, s_{\beta}, s_x, s_{\delta_1}, s_{\delta_2})$$

3) 입증(Verify) : 그룹 공용키 $gpk = (g_1, g_2, h, u, v, w)$와 메시지 M, 서명 σ이 주어졌을 때, 입증 과정은 다음과 같다.

다음과 같이 R_1, R_2, R_3, R_4, R_5를 계산한다.

$$\widetilde{R_1} \leftarrow u^{s_{\alpha}} \cdot T_1^{-c},\ \widetilde{R_2} \leftarrow v^{s_{\beta}} \cdot T_2^{-c}$$

$$\widetilde{R_3} \leftarrow e(T_3, g_2)^{s_x} \cdot e(h, w)^{-s_{\alpha}-s_{\beta}} \cdot e(h, g_2)^{-s_{\delta_1}-s_{\delta_2}} \cdot (e(T_3, w)/e(g_1, g_2))^{c}$$

$$\widetilde{R_4} \leftarrow T_1^{s_x} \cdot u^{-s_{\delta_1}},\ \widetilde{R_5} \leftarrow T_2^{s_x} \cdot v^{-s_{\delta_2}}$$

위의 값을 hash function에 대입하여, 함께 전달받은 challenge c와 일치하는 값을 가지는 지 확인한다. 만약 일치한다면, 메시지를 수용하고, 일치하지 않는다면 메시지를 수용하지 않게 된다.

$$c \stackrel{?}{=} H(M, T_1, T_2, T_3, \widetilde{R_1}, \widetilde{R_2}, \widetilde{R_3}, \widetilde{R_4}, \widetilde{R_5})$$

4) 개방(open) 혹은 복구(recover): 이는 특수한 상황에서 메시지를 서명한 사용자를 추적하는 경우에 사용되는 단계이다. 이는 그룹의 비밀키를 알고 있는 그룹 관리자의 경우에만 가능한 단계이다. 그룹 공용키 gpk, 그룹 비밀키 $gpmk$, 메시지 M, 서명 σ가 주어진 경우에 입증 단계를 거쳐, 메시지가 valid 한 것을 밝힌 이후에, 개별 사용자의 비밀키 중 $A \leftarrow T_3/(T_1^{\xi_1} \cdot T_2^{\xi_2})$ 를 계산할 수 있으므로, 그룹

관리자가 개별 사용자의 A_i를 모두 알고 있다면, 서명자를 찾을 수 있다.

5) 사용자 삭제(Revocation): 사용자 중의 일부가 부정한 정보를 제공하거나, 부적절한 목적으로 정보를 사용한 경우에 그룹 관리자는 이러한 사용자들을 서비스 대상에서 제외시킬 수 있다. 이러한 단계는 단순하게 이루어질 수 있는데, 사용자 그룹 내에서 삭제되어야 하는 사용자들의 명단을 그들의 개별 비밀키와 함께 공포함으로서 삭제 대상 외의 사람들이 이를 통해 각자 자신의 새로운 비밀키와 공용키를 계산하여 보유할 수 있다. 그룹 관리자 또한 삭제 대상인 사용자들의 비밀키를 이용해 새로운 그룹 비밀키를 생성해 보유함으로서 삭제 대상이 아닌 사용자들에 대한 관리 권한을 계속 유지할 수 있다.

4. 이동 멀티미디어 방송 그룹 인증 기법의 안전성 요구 조건 증명

본 논문에서 선정한 Boneh(2004)[5] 의 그룹 인증 기법이 이동 멀티미디어 방송 콘텐츠 사용자 관리에 적합한 지 판단하기 위해, 제시한 방식이 앞서 선정한 안전성 요구 조건에 부합하는지를 살펴보는 과정이 필요하다. 무결성 및 입증성(Integrity and Source Authentication), 위치 정보 제공성(Location Information Exposure), 익명성(Anonymity), 혐의 부정성(Exculpability), 추적 가능성(Traceability), 효율성(Efficiency), 강인성(Robustness)의 7가지 조건 중에서 인증 방식만을 통해 증명이 어려운 효율성과 강인성을 제외한 5가지 항목에 대해서 안전성 요구 조건 부합 여부를 살펴볼 예정이다.

1) 무결성 및 입증성 증명 : 서명과 입증 과정에서 단방향 hash function을 사용하기 때문에, 정보 전달 과정에서 오류가 발생하거나 외부의 공격으로 정보가 왜곡될 시에는 서명과 입증 과정에서 얻게 되는 challenge c의 값이 다르게 됨을 확인할 수 있다. 따라서, challenge c의 값을 비교함으로서 무결성을 입증할 수 있다. 입증성의 경우, 전달되는 정보가 왜곡되지 않았다고 가정하고 서명과 인증 과정에서 hash function에 대입되는 값들을 비교하면 서로 같은 것을 알 수 있으므로 쉽게 증명할 수 있다.

2) 위치 정보 제공성 : 이동 멀티미디어 방송에서는 위치 정보가 중요하게 사용될 수 있으므로, 제공하는 정보에 사용자의 위치를 포함시킬 수 있어야 한다. 이는 메시지를 만드는 과정에서 위치 정보를 hash function에 대입하여 구성함으로서 간단히 해결할 수 있다.

3) 익명성 증명 : Boneh(2004)에서 가정하고 있는 random oracle model에서는 zero-knowledge인 상황이므로 서명 $\sigma \leftarrow (c, s_1, s_2, s_3, s_4, T_1, T_2, T_3)$은 사용자에 대한 아무런 정보도 제공하지 못 한다. 또한, decisional Diffie-Hellman인 것을 가정하고 있기 때문에, 주어진 정보만으로 사용자를 밝히고자 하는 것은 해결하기 어려운 discrete-logarithms 문제가 된다.

4) 혐의 부정성 증명: 서비스 사용자들은 다른 사용자가 같은 그룹에 속해 있는지에 대한 판단 외에는 아무런 정보도 알지 못하기 때문에, 다른 그룹 멤버를 위해 서명을 이용할 수는 없다. 그룹 관리자 또한 사용자들의 비밀키 (A_i, x_i) 중, A_i만 알고 있고, x_i는 알지 못한다. x_i의 경우, a^{x_i}만 알 수 있기 때문에, 이를 해결하기 위해서는 discrete-logarithm problem을 풀어야 한다. 하지만 이는 굉장히 시간이 오래 걸리기 때문에, x_i는 알 수 없다는 것을 보장할 수 있다. 따라서 그룹 내 사용자나 그룹 관리자 모두 다른 그룹 사용자를 위해 서명 정보를 제공하기 어렵다.

5) 추적 가능성 증명: 앞에서 살펴본 인증 과정 중 개방(open) 혹은 복구(recover)에서 볼 수 있듯이, 그룹 관리자는 자신이 알고 있는 개별 사용자들의 비밀키 A_i를 이용해 어떤 사용자가 정보에 대한 서명을 했는지 확인할 수 있다.

5. 이동 멀티미디어 방송 그룹 인증 기법 활용방안

개별 키 인증 기법 활용에 비해 그룹 인증 기법 활용의 장점은 개별 사용자의 익명성을 최대한 보장하면서도, 그룹 내에서의 원활한 정보 전달과 관리의 효율성을 지원한다는 점에 있다. 또한, 메시지에 포함된 내용을 바탕으로 개별 맞춤형 서비스를 수행할 수 있는 것은 사용자 익명성 보호라는 그룹 인증 기법 사용의 목적을 잃지 않으면서도, 다양한 비즈니스 모델을 개발할 가능성을 넓혀준다. 이동 멀티미디어 방송 서비스에서 그룹 인증 기법을 활용할 수 있는 예시 모델로 SNS(Social Networking Service)등과 유사한 서비스를 이용해 자발적 멀티미디어 생산 및 사용자 간의 공유가 이루어지는 상황을 예상해 볼 수 있다.

현재까지 멀티미디어의 생산 및 배포는 주로 방송사와 같은 전문 사업자가 수행했지만, 앞으로는 정보의 소비뿐만 아니라 생산에도 적극 참여하는 프로컨슈머(pro-consumer)의 등장에 힘입어 멀티미디어 시장에서도 이들의 역할이 중요하게 대두될 것으로 여겨진다. 특히 이동 멀티미디어 방송 서비스는 기존의 전통적인 멀티미디어 소비 집단에서 생산 집단으로의 변화를 용이하게 하여, 개별 사용자의 특성에 따른 다양한 미디어의 생산이 이루어질 것으로 예상된다. 서비스에 접근할 수 있는 권한을 가진 사용자간의 적극적인 멀티미디어 생산 및 공유가 새로운 패러다임으로 자리 잡게 된다면, 이들 사용자를 효율적으로 관리할 수 있는 방안을 찾는 것은 시급하게 해결되어야 하는 문제가 될 것이다. 그룹 인증 관리 기법은 이러한 문제를 해결하는데 핵심적인 역할을 할 수 있을 것으로 기대된다. Diffie-Hellman scheme에 따른 기존의 개별 키 인증 기법과는 달리, 그룹 인증 기법은 사용자들 간의 서명과 인증 과정에서 센터의 개입을 필요로 하지 않기 때문에, 개별 생산자의 자발적 서비스 제공에서의 편의를 향상시킬 수 있다. 또한, 서비스를 이용할 수 있는 권한을 가진 그룹 내 사용자가 서비스를 오용할 경우, 이와 같은 사용자에 대한 권한 삭제 및 차후 남아있는 사용자들에 대한 키 변경 과정이 개별 키 인증 기법에 비해 훨씬 간단하므로 관리의 효율성이 크게 증가되는 효과를 기대할 수 있다.

위와 같이 그룹 인증 기법을 통한 사용자 관리는 중앙 관리 센터와 개별 사용자 간의 정보 전달보다는 사용자들 간의 정보 전달에 있어 강점을 보이고 있다. 또한 관리자의 개입을 통해, 정보 왜곡이나 권한의 오용을 적극적으로 방지하여 사용자 그룹 내의 건전성을 유지하고, 사용자 그룹 관리에 있어서 편의를 도모할 수 있다. 따라서, 사용자와 중앙 기지국 간의 정보 전달에서 사용되는 프로토콜의 단점을 보완하

고, 사용자들 간의 정보 전달에서 나타나는 효율성을 증가시키기 위해서는 그룹 인증 기법을 동반하여 사용할 수 있다.

6. 결론 및 추후 연구 과제

지금까지 이동 멀티미디어 방송에서 관리의 효율성을 증대시키기 위해 사용가능한 그룹 인증 방식을 살펴보고, 이 방식이 적절한 안전성 요구 조건에 부합하는 지에 대해서 증명해보았다.

그러나 일반적인 그룹 인증 방식이 응용되는 상황과는 달리 멀티미디어 방송 서비스에서는 연속적으로 정보가 계속 전달되어야 하기 때문에, 매번 정보 전송 시마다 서명 및 인증 과정을 거치는 것은 비효율적인 일이 될 것이라 생각된다. 이 문제에 대해서는 추후에 계속적인 연구가 필요하겠지만, 적어도 이 논문이 이동 멀티미디어 방송 서비스에서의 효율적인 사용자 관리에 대해 그룹 인증 방식을 제안하고 안전성 보장을 위해 필요한 조건들을 제시하고 증명했으며, 이의 활용방안을 모색했다는 점에서 소기의 목적을 달성했다고 할 수 있다.

후속적으로 전달 정보의 최적화를 통해 효율성 향상을 도모하고, 이를 통해 응용할 수 있는 서비스 분야를 개척하는 노력이 필요하겠다.

1) D. Chaum and E. van Heyst. "Group signatures," In D. W. Davies, editor, Proceedings of Eurocrypt 1991, volume 547 of LNCS, pages 257~265. Springer-Verlag, 1991.

2) G. wang, "Security analysis of several group signature schemes," In INDOCRYPT 2003, LNCS 2904, pp. 252-265. Springer-Verlag, 2003.

3) Xiaoting Sun, Xiaodong Lin and Pin-Han Ho. "Secure vehicular communications based on group signature and id-based signature scheme," Communications, 2007, ICC 07, IEEE International. pp1539~1545, 2007

4) Giuseppe Ateniese, Jan Camenisch, Marc Joys, and Gene Tsudik. "A practical and provably secure coalition-resistant group signature scheme", M. Bellare, editor., Advances in Cryptology - CRYPTO2000, vol.1880 of Lecture Notes in Computer Science, pp.255~270, Springer-Verlag, 2000.

5) Dan Boneh, Xavier Boyen and Hovav Shacham, "Short group signatures," M. Franklin, editor, Advances in Cryptology, CRYPTO2004, volume 3152 of Lecture Notes in Computer Science, pages 41~55, Berlin: Springer-Verlag, 2004