

브로드캐스트 암호화를 이용한 효율적인 콘텐츠 제공

이 덕 규*, 이 임 영*

* 순천향대학교 정보기술공학부

요 약

브로드캐스트 암호화 기법은 공개된 네트워크 상에서 멀티미디어, 소프트웨어, 유료 TV 등의 디지털 정보들을 전송하는데 적용되고 있다. 브로드캐스트 암호화 기법에서 중요한 것은 오직 사전에 허가된 사용자만이 디지털 정보를 얻을 수 있어야 한다는 것이다. 브로드캐스트 메시지가 전송되면 권한이 있는 사용자들은 자신이 사전에 부여받은 개인키를 이용하여 먼저 세션키를 복호화하고 이 세션키를 통하여 디지털 정보를 얻게 된다. 본 논문에서는 브로드캐스트 방법을 이용하여 콘텐츠에 대한 요구사항을 살펴본 뒤 이를 통해 브로드캐스트 암호화의 개념을 적용하여 DRM 모델을 제시하고자 한다. 사용자로 하여금 원하는 복사의 수만큼 복사할 수 있는 권한을 제공함으로써 사용하기에 편리하도록 하였다.

Efficient Offered Contents Using Broadcast Encryption

Deok-Gyu Lee*, Im-Yeong Lee*

ABSTRACT

The method of broadcast encryption has been applied to the transmission of digital information such as multimedia, software, and paid TV on the open network. In this broadcast encryption method, only previously authorized users can gain access to digital information. When broadcast message is transmitted, authorized users can first decode the session key using the previously given private key and get digital information using this session key. This way, users retrieve a message or a session key using the key transmitted by broadcasters. For their part, broadcasters need to generate and distribute keys. Broadcasters should also carry out efficient key renewal when users subscribe or un-subscriber. In this paper use a broadcast, and present the DRM model, using that look into the requirement about the contents and apply also the concept of a broadcast encryption. We offer the authority to copy as the number of reproduction to want to the user, and the low so that we were convenient because we used.

1. 서 론

최근 브로드캐스트 암호화 기법은 공개된 네트워크상에서 멀티미디어, 소프트웨어, 유료 TV 등의 디지털 정보들을 전송하는데 적용되고 있다.

키를 제공하는 방식 중에 하나인 공개키 방식은 세션키를 암호화하기 위한 그룹의 암호화키는 하나이고 이를 복호화하기 위한 키는 여러 개의 무수히 많은 키를 이용함으로써 서버는 세션키를 암호화하고 각 사용자에게는 서로 다른 키를 이용하여 복호화 할 수 있도록 되어 있다. 브로드캐스트 암호화 기법에서 중용한 것은 오직 사전에 허가받은 사용자만이 디지털 정보를 얻을 수 있어야 한다는 것이다. 브로드캐스트 메시지가 전달되면 권한이 있는 사용자들은 자신이 사전에 부여받은 개인키를 이용하여 먼저 세션키를 복호화하고 이 세션키를 통하여 디지털 정보를 얻게 된다. 브로드 캐스트 암호화에 있어 가장 중요한 것은 키 생성, 분배, 갱신이다.

제안 방식에서는 콘텐츠의 특성에 의해 제공하는데 있어 일방향성을 지니게 된다. 이러한 상황에 맞도록 사용자에 키를 생성, 분배 시에 사용자가 상거래에 이용할 수 있도록 키를 생성하여 보낼 수 있는 방식을 제안하도록 한다. 기존의 키 생성 방식을 이용하여 개인의 키를 생성하며 이에 추가적으로 각각의 사용자가 상거래를 위한 키를 생성하는 방식이다.

본 논문은 콘텐츠에 대한 개요와 Broadcast Encryption의 개요에서 적용방식에 대해 간략히 설명하고 제안방식의 각 단계에 관하여 살펴본 후 마지막으로 결론으로써 끝을 맺도록 한다.

2. Broadcast Encryption 개요

브로드캐스트 암호화는 2가지 모델을 기반으로 할 수 있다. 적용모델간의 차이점이 있지만

각각에 대하여 살펴보면 다음과 같다.

첫 번째 방식을 살펴보면, 사용자와 서버간의 정보를 이용하여 키를 생성/분배하는 방식이다. 다음은 기존의 멀티캐스트 방식과 유사하다. 이는 전송되는 방식에서 차이가 존재할 뿐 제공되는 메시지가 이전의 사용 그룹에 의해 결정되는 점에서 유사하다. (그림 1. 참조)

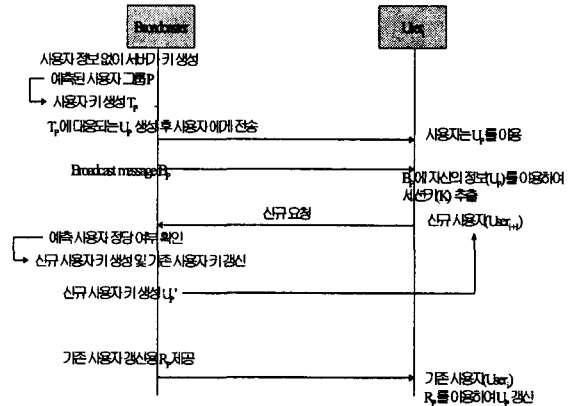


그림 1. 적용 모델-II

키 생성과정에서 사용자가 참여하여야 하므로 생성시간에 사용자의 참여 시간이 포함될 수 있다. 키 갱신과정에서도 기존 사용자의 탈퇴/신규 사용자의 참여 시 키 갱신에 따른 소요시간이 많이 발생하게 된다.

위 방식과 다르게 서버가 키를 생성하는 방식으로 두 번째 적용 모델을 살펴볼 수 있다.

서버가 단독으로 참여할 사용자를 예측하여 키를 생성한다. 이러한 방법은 사용자의 동의 없이 서버가 모든 사용자의 키를 생성하게 됨으로써 빠른 생성과 빠른 갱신이 가능하다. 하지만 서버가 악의적인 목적 혹은 서버가 공격의 대상이 되었을 경우 많은 취약점을 내포하고 있다.

하지만 두 방식 모두 서버가 사용자의 키를 모두 단독으로 생성하여 서버의 부담이 크다는 문제점을 가지고 있으며 서버가 공격당하였을 경우 모든 키가 노출된다는 취약점을 가지고 있

다. 이에 본 논문에서는 이러한 구조를 벗어나 서버가 하부 서버에 키를 생성/분배하고 다시 하부 서버가 사용자의 키를 생성/분배하는 방식을 제안한다.

3. 제안 방식

컨텐츠를 제공함에 있어 브로드캐스터가 단독으로 사용자의 키를 생성하고 분배하는 방식을 이용하여 방송을 시청하는 여러 사용자에게 컨텐츠 접근에 대한 키를 제공하며, 구매에 대한 키로서 자신의 비밀키를 이용하는 방식을 제안한다.

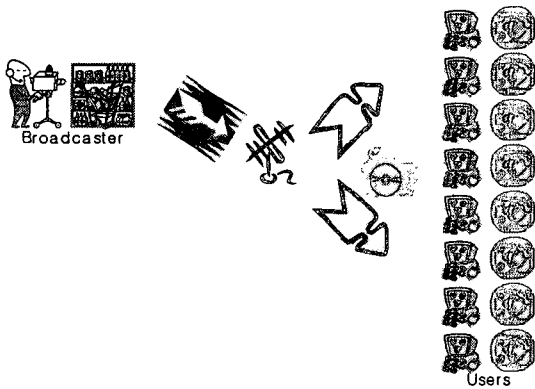


그림 2 전체 그림

3.1 제안방식 개요

다음은 제안방식의 전체적인 개요에 대하여 살펴본다.

다음 그림은 본 제안방식에서의 전체적인 도식을 표현 한 것이다. 다음의 그림을 살펴보면 브로드캐스터가 사용자들에게 제공할 키를 사전에 예측 생성하여 보관하고 있다가 사용자가 접근하면 키를 분배하는 방식이다. 또한 사용자는 제공받은 키를 이용하여 원하는 컨텐츠의 구매에 대한 키를 생성할 수 있다.

본 제안 방식은 컨텐츠 사용에서 발생될 수 있는 서비스에 이용될 수 있는데 이는 전체적인 컨텐츠가 사용자에게 발송되고 사용될 수 있다. 이때 사용자마다 각각의 키를 생성하여야 하는데 브로드캐스터에서 제공되는 키 이외에 다른 키를 생산하게 되면 브로드캐스터의 키의 증가로 각각의 컨텐츠에 대한 것과 동일하다. 따라서 키의 개수를 증가시키지 않고 기존의 키를 이용하여 상거래에 이용할 수 있는 키를 생성하여 사용하는 방법을 제안한다. 이것은 최초 메시지 전송에는 하나의 키로 전송이 되고 후에 키는 사용자의 키로 생성되기 때문에 브로드캐스터의 부담은 줄여줄 수가 있으며 새롭게 생성하는 것이 아니기 때문에 빠른 연산을 이룰 수 있다.

3.2 시스템 계수

다음은 본 방식에서 사용되는 시스템 계수를 기술한 것이다.

- p : 소수 ≥ 512 bit
- q : 소수 ≥ 160 bit ($q \mid p-1$)
- l : 개인키 생성을 위한 수
- e : 공개 암호화 키
- d_1, \dots, d_k : 개별 복호화키 리스트
- M : 컨텐츠 · S : 세션 키 · k : 사용자
- r_i : 랜덤 수 집합($r_i \in Z_p$) (r_1, \dots, r_k)
- $h_i = g^{r_i}$ · $\langle y, h_1, \dots, h_k \rangle$: 공개키
- $y = \prod h_i^{a_i}$ · $z = \prod h_i^{a_i^0}$
- a_i : 랜덤수 ($a_i \in Z_q$) (a_1, \dots, a_k)
- $d_i = \theta_i \cdot v_{(i)}$ ($v_{(i)} \in \Gamma$) · $\Gamma = v_1, \dots, v_k$
- a : 랜덤 요소($a \in Z_q$)
- C : 방송 메시지(Broadcast message)
- $C = \langle M(\text{or } S)y^{aT}, h_1^a, \dots, h_k^a \rangle = \langle B, H_1, \dots, H_k \rangle$
- $B = M(\text{or } S)y^{aT}$ · $H_i = \prod h_i^a$
- T : 키 갱신을 위한 인자 ($t_1, \dots, t_k \in Z_q$), $T = t_1 \dots t_k$
- W : 사용자와 서버간의 키 $W = g(\text{ID} \parallel \theta_i)$
- A : 사용자의 구매 인자

3.3 프로토콜

다음은 전체적인 프로토콜에 대하여 개괄적으로 기술한 그림이다. 다음 그림에 따라 사용자의 키를 생성하고 이에 맞는 브로드캐스트 메시지를 생성하게 되며 사용자는 이에 대한 구매키를 생성하여 통신하게 된다.

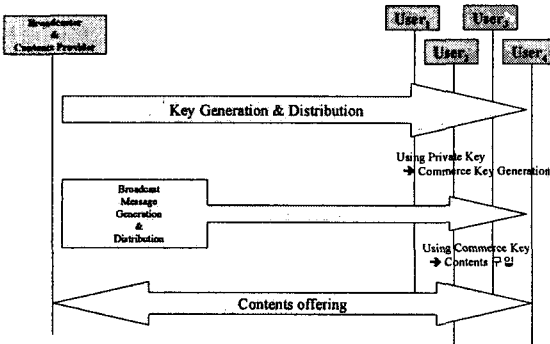


그림 3 전체 프로토콜

(1) 브로드캐스터에서의 키 생성 및 분배 단계

키 생성은 브로드캐스터의 담당이며, 개인키와 공개키를 생성하고 전달하기 위해 다음의 일련의 과정을 거친다.

Step 1. 브로드캐스터는 사용자들을 예측하여 이를 바탕으로 열을 랜덤하게 선택한다.

$$i = 1, \dots, k \text{ 예측} \Rightarrow r_i \text{ 열 선택}$$

Step 2. 이 선택된 랜덤열을 바탕으로 공개키 작성에 필요한 값을 생성한다.

$$h_i = g^{r_i} \text{ mod } q \text{ 계산}$$

$$\text{공개키 } \langle y, h_1, \dots, h_k \rangle$$

$$\text{갱신을 위해 T생성 : } T = t_1 \cdot \dots \cdot t_k$$

Step 3. 생성된 값 h를 이용하여 공개키를 작성한 후 이를 바탕으로 개인키를 계산한다.

$$\theta_i = (\sum r_j a_j t_j) / (\sum r_j v_j) \text{ mod } q$$

Step 4. 생성된 d_i 를 사용자에게 전송한다. 이때 사용자는 자신의 ID를 브로드캐스터에 등록한다.

$$d_i = \theta_i \cdot v_i$$

Step 5. 사용자는 전송받은 d_i 에서 개인키 θ_i 를 획득한다.

$$d_i = \theta_i \cdot v_i / v_i$$

(2) 콘텐츠 제공을 위한 브로드캐스트 메시지 생성단계

브로드캐스트 메시지를 전송하는데 있어 콘텐츠 자체를 암호화하여 전송한다. 다음은 브로드캐스터에서 사용자들에게로 제공하는 메시지에 대해 기술한다.

Step 1. 콘텐츠 M 혹은 세션키 S를 암호화하여 계산한다. 이때 세션키 S를 사용하는 경우에는 그 세션키 사용으로써 모든 사용자들에 대한 전체적인 통신이 이뤄진다. 하지만 계산된 키를 이용하여 콘텐츠만을 제공할 경우에는 다음과 같이 계산한다.

Step 2. 랜덤요소 a를 선택하고 키 갱신 요소 T를 연산하여 랜덤요소와 갱신요소를 같이 메시지 작성에 사용한다.

Step 3. 브로드캐스트 메시지를 작성하여 사용자들에게 전송한다.

$$C = \langle M(\text{or } S)y^{aT}, h_1^a, h_k^a \rangle$$

Step 4. 전송받은 사용자들은 메시지는 개인키를 이용하여 콘텐츠 M를 획득한다.

$$M(\text{or } S) = B/U^{b_i}, U = \prod H_j^{v_j}$$

$$U^{b_i} = (\prod H_j^{v_j})^{b_i} = (\prod g^{a r_j v_j})^{b_i} = (g^{r_j v_j})^{b_i a} = (g^{r_j a j})^a = (h^{j a})^{i T} = y^{a T}$$

$$M(\text{or } S) = M(\text{or } S) \cdot y^{a T} / y^{a T}$$

(3) 사용자들의 브로드캐스트 메시지에 대한 키 생성단계

사용자들은 브로드캐스터로부터 받은 개인 키를 이용하여 자신과 브로드캐스터 간에 사용될 키를 계산하여 원하는 콘텐츠를 암호화하여 브로드캐스터에 전송한다. 다음은 구매에 대한 사용자의 키를 생성하는 과정에 대하여 기술한다.

Step 1. 브로드캐스터가 콘텐츠 M을 분배하였을 경우 사용자는 콘텐츠에 대한 구매의사가 발생하면 자신의 키를 생성하여 구매에 대한 키를 생성하게 된다.

Step 2. 사용자는 자신이 최초로 전송받은 자신의 개인키를 이용하여 키 W를 생성한다.

$$W = g(ID || \theta;)$$

Step 3. 사용자는 자신이 생성한 키 W를 이용하여 콘텐츠 구매에 대하여 암호화한 후 브로드캐스터에 전송한다.

$$A = [ID || E_w(ID || M || r)]$$

Step 4. 브로드캐스터는 전송받은 A를 이용하여 사용자의 구매의사에 대한 사후 통신을 실시한다.

(4) 키 갱신 단계

사용자들의 탈퇴 혹은 신규 가입자가 발생한 경우 다음과 같이 브로드캐스터에서 키 갱신 과정을 거친다.

Step 1. 사용자 i의 탈퇴 요청

Step 2. 브로드캐스터는 기존 사용자의 개인 키를 갱신하기 위해 갱신요소인 T에서 사용자 i의 갱신요소를 제거한다.

Step 3. 제거한 후 개인키를 갱신하고 나머지 사용자들에게 전송한다.

$$\theta_i \cdot v_{(i)} \cdot t^{i-1} = d_i'$$

Step 4. 갱신된 키를 이용하여 디바이스들은 브로드캐스트 메시지를 전송받고 다음과 같이 암호화된 메시지를 복호화하여 메시지를 획득하게 된다.

$$(C = \langle M(\text{or}S) \cdot y^{aT_{ii-1}}, h_1^a, \dots, h_k^a \rangle)^{\theta_i}$$

$$M(\text{or} S) = B/U^{\theta_{ii-1}}, U = \prod H_j^{v_j}$$

$$U^{\theta_{ii-1}} = (\prod H_j^{v_j})^{\theta_{ii-1}} = (\prod g^{ar_j v_j})^{\theta_{ii-1}} = (g^{r_j v_j})^{\theta_{ii-1}} = (g^{r_j v_j})^{\theta_{ii-1}} = (g^{r_j v_j})^{\theta_{ii-1}}$$

$$\theta_{ii}^{a_{ii-1}} = (H_j^{a_{ii}})^a = y^{aT_{ii-1}}$$

$$M(\text{or} S) = M(\text{or} S) \cdot y^{aT_{ii-1}} / y^{aT_{ii-1}}$$

4. 제안 방식 고찰

본 방식은 다음과 같은 특징을 갖도록 제안하였다. 향후 발전 중심에 있는 양방향 TV에 적합하도록 설계하였다.

본 제안방식에서 살펴보면, 사용자가 메시지를 전송할 수 있다는 것이다. 이것은 공간의 특징을 이용하여 브로드캐스터만이 다른 디바이스에 브로드캐스트 메시지를 전송하는 것이 아니라 사용자가 자신의 개인키를 이용하여 콘텐츠에 대한 구매의사로써 브로드캐스터에게 메시지 전달이 가능하다. 이러한 경우에는 사용자와 브로드캐스터간의 키 갱신이 필요치 않다. 키 갱신은 사후에 사용자가 탈퇴할 경우 자동으로 이뤄지게 된다. 만약 사용자가 악의적인 사용자를 발견할 경우 사용자 식별자에 해당하는 값을 제거한 후 공간 사용자의 키를 갱신 뒤에 사용이 가능하다.

또한 본 방식에 랜덤 변수 a가 다른 사용자에 알려진다 하더라도 브로드캐스터에서 다른 디바이스 탈퇴 후 키 갱신에는 T를 이용하게 됨으로 a가 공개되었다하더라도 안전하게 통신을 할 수 있다.

5. 결 론

브로드캐스트 암호화는 공개된 네트워크 상에서 인가된 사용자에게만 콘텐츠를 제공하는데 사용한다. 인가된 사용자 이외에는 브로드캐스트 되는 메시지에 대해 아무런 정보를 얻어낼 수 없으며, 인가된 사용자는 사전에 전송된 개인키를 이용하여 세션키를 취득할 수 있게 된다.

본 논문은 콘텐츠 제공에서 모든 사용자가 각각의 키를 생성하는 것이 어려울 경우 Broadcast Encryption을 이용하여 최초 분배되는 개인키를 이용하여 해결하려 하였다. 이와 같은 경우는 키를 분배할 때 각각의 키 정보는 오직 사용자와 브로드캐스터만이 알고 있기 때문에 이를 이용한 비밀값을 생성하는 것은 유용하다고 할 수 있다.

향후 연구 분야로서는 콘텐츠를 제공할 때 콘텐츠에 대한 지불정보나 사용자가 구매의사를 수립하였을 경우 지불정보를 포함하는 연구가 진행되어야 하며, 콘텐츠의 구매이외에도 사용자의 편의성을 위해 키의 분배하고 관리하는 방법에 대해 더욱 깊은 연구가 필요하리라 본다.

참고문헌

- [1] Amos Fiat, and Moni Naor, "Broadcast Encryption", Crypto'93, LNCS 773, 480-491
- [2] C. Blundo, Luiz A. Frota Mattos, D.R. Stinson, "Generalized Beimel-Chor schemes for Broadcast Encryption and Interactive Key Distribution", Crypto'96, LNCS 1109
- [3] Carlo Blundo, Luiz A. Frota Mattos, and Douglas R. Stinson, " Trade-offs Between Communication and Storage in Unconditionally Secure Schemes for Broadcast Encryption and Interactive Key Distribution", Crypto 98
- [4] Juan A. Garay, Jessica Staddon, and Avishai Wool, "Long-Lived Broadcast Encryption", Crypto'00, LNCS 1880, 333-352
- [5] Ignacio Gracia, Sebastia Martin, and Carles Padro, "Improving the Trade-off Between Storage and Communication in Broadcast Encryption Schemes", 2001
- [6] Dani Halevy, and Adi Shamir, "The LSD Broadcast Encryption Scheme", Crypto'02, LNCS 2442, 47-60
- [7] Yevgeniy Dodis and Nelly Fazio, "Public Key Broadcast Encryption for Stateless Receivers", DRM2002, 2002. 11. 18
- [8] Donald Beaver, and Nicol So, "Global, Unpredictable Bit Generation Without Broadcast", 1993
- [9] Michel Abdalla, Yucal Shavitt, And Avishai Wool, "Towards Marking Broadcast Encryption Practical", FC'99, LNCS 1648
- [10] Dong Hun Lee, Hyun Jung Kim, and Jong In Lim, "Efficient Public-Key Traitor Tracing in Provably Secure Broadcast Encryption with Unlimited Revocation Capability", KoreaCrypto 02', 2003
- [11] 김효근, 문남미, "T-commerce 전략과 기술", SigmaInsight
- [12] 이임영, 이재광, 소우영, 최용락, "컴퓨터 통신 보안", 도서출판 그린