Ad-hoc 환경에서 브로드캐스트 암호화 기법을 이용한 키 분배에 관한 연구

이덕규*, 이임영*
*순천향대학교 정보기술공학부
e-mail:{hbrhcdbr, imylee}@sch.ac.kr

A Study on Key Distribution Using Broadcast Encryption for Ad-hoc Environment

Deok-Gyu Lee*, Im-Yeong Lee*
*Division of Information Technology Engineering,
Soonchunhyang University

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. 이와 같이 사용자는 브로드캐스터가 전송하는 키를 이용하여 메시지나 세션키를 획득하게 되는데, 이러한 과정에서 브로드캐스터가 키를 생성하고 분배하는 과정이 필요하다. Ad-hoc 통신망은 기반구조 없이 각 무선 호스트들 사이에 대하여 전송이 가능하고, 잦은 위치 변화에 따라 망구조가 유동적으로 변하는 특성으로 인해 PKI와 같은 기반구조를 적용하기 힘들다.
이에 본 논문에서는 Ad-hoc 네트워크에 적용하여 회의장 등과 같은 특정한 공간에서 Ad-hoc 통신망을 구성할 수 있는 무선 호스트를 사용하여 소규모 그룹의 회의하고자 할 경우를 고려하여 쉬운 키 생성과 키 갱신을 하도록 제안하였다.

1. 서론

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

키를 제공하는 방식 중에 하나인 공개키 방식은 세션키를 암호화하기 위한 그룹의 암호화키는 하나이고 이를 복호하기위한 키는 여러 개의 무수히 많은 키를 이용함으로써 서버는 세션키를 암호화하고 각 사용자에게는 서로 다른 키를 이용하여 복호화할 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 Ad-hoc 네트워크의 특성에 의해 회의장 등과 같은 어느 특정한 공간에서 Ad-hoc 통신망을 구성할 수 있는 무선 호스트를 사용하여 소규모 그룹이 회의하는 경우 등과 같은 환경을 기반으로 제안한다. 기존의 키 생성 방식을 이용하여 개인의 키를 생성하는 것이 아니라 중앙 역할을 하는 디바이스가 전체적으로 키를 생성하여 분배하고 이를 이용하여 통신하는 방식을 제안하도록 한다.

본 논문은 Ad-hoc 네트워크에 대한 개요와 Broadcast Encryption의 개요 중에서 적용방식에 대해 간략히 설명하고 제안방식의 각 단계에 관하여 살펴본 후 마지막으로 결론으로써 끝을 맺도록 한다.

2. Ad-hoc 개요와 Broadcast Encryption 개요

2.1 Ad-hoc 네트워크 개요

Ad-hoc 통신망은 다음과 같은 특성으로 인해 PKI와 같은 기반구조를 적용하기가 힘들다.

- AP(Access Point)와 같은 기반구조 없이 각 무선 호스트를 사이에 데이터 전송이 가능한 망
- 각 무선 호스트들은 각 호스트의 무선 통달거리 내에 존재하는 호스트들과 직접 데이터 전송이

가능
- 라우터 기능을 가지는 무선 호스트들이 존재할 경우 원격 호스트(Multi-hop host)와도 통신이 가능
- 무선 호스트들의 잦은 위치 변화로 망구조가 유동적

이와 같은 Ad-hoc 통신망의 특징으로 인해 ad-hoc 통신망에서는 중앙 디바이스가 자신의 영역에 들어오는 디바이스에 키를 생성하여 분배하는 기법을 사용할 수 있다.

2.2 Broadcast Encryption 적용 모델

브로드캐스트 암호화는 다음과 같이 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.

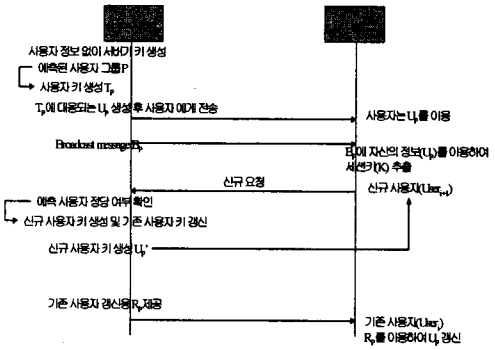

그림 1. 적용 모델 2

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

3. 제안 방식

Ad-hoc의 특수한 환경에서 중앙 디바이스가 단독으로 사용자의 키를 생성하고 분배하는 방식을 이용하여 여러 디바이스가 모여 ad-hoc 네트워크를 형성하였을 경우 각 디바이스마다 키를 공유하는 방식이 아닌 중앙 디바이스에서 기존 생성된 키를 분배하는 방식을 제안한다.

3.1 제안방식 개요

다음은 제안방식의 전체적인 개요에 대하여 살펴본다.

다음 그림은 본 제안방식에서의 전체적인 도식을 표현 한 것이다. 다음의 그림을 살펴보면 공간에 중앙의 역할을 하는 디바이스가 존재하고 이 디바이스가 사전에 키를 예측 생성하여 보관하고 있다가 공간에 입장하게 되면 키를 분배하는 방식이다.

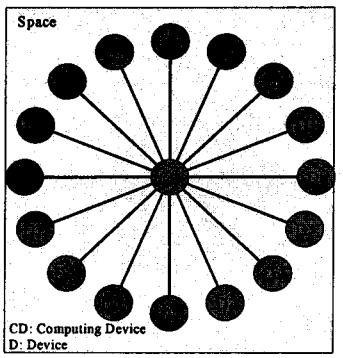

그림 2. 제안 방식 전체 그림

본 제안 방식은 회의장 등과 같은 특정한 공간에서 ad-hoc 통신망을 구성할 수 있는 무선 호스트를 사용하여 소규모 그룹이 회의하고자 할 경우에서 올바른 그룹 구성원들은 회의장에 들어오기 전에 안전한 방법으로 그룹간에 키를 교환하여야 한다. 이때 ad-hoc 통신망을 이용하기 때문에 다른 분배센터(DC:Distribution)와 같은 개체는 이용할 수 없다. 그룹 내의 회의나 공간에 무선 호스트가 중앙 디바이스로 존재하며, 이 디바이스는 강력한 계산능력을 가질 수 있다.

최초 공간이 형성되면 중앙 디바이스는 예상 키열을 생성하고, 디바이스가 특정한 공간에 들어오면 중앙 디바이스는 키를 발급한다. 한번 발급된 키는 종료시까지 변경없이 유지될 수 있으며, 서버뿐만 아니라 사용자들도 공개된 키를 이용하여 다른 디바

이스에 Broadcast Message를 전송할 수 있도록 제안한다.

3.2 시스템 계수

다음은 본 방식에서 사용되는 시스템 계수를 기술한 것이다.

- p : 소수 ≥512 bit
- q : 소수 ≥160 bit (q | p-1)
- l : 개인키 생성을 위한 수
- e : 공개 암호화 키
- $d_1,...,d_k$: 개별 복호화키 리스트
- M : 메시지 · S : 세션 키 · k : 사용자
- r_i : 랜덤 수 집합($r_i \in Z_p$) ($r_1, ..., r_k$)
- $h_i = g^{r_i}$ · <y, h_1, ... ,h_k> : 공개키
- $y = \Pi\ h_i^{a_i}$ · $z = \Pi\ h_i^{a_i\theta}$
- a_i : 랜덤수 ($a_i \in Z_q$) {a_1, ... ,a_k}
- $d_i = \theta_i \cdot \gamma^{(i)}$ ($\gamma^{(i)} \in \Gamma$) · $\Gamma=\gamma_1, ...,\gamma_k$
- a: 랜덤 요소($a \in Z_q$)
- C: 방송 메시지(Broadcast message)
- $C = <M(or\ S)y^{aT},h_1^a,... ,h_k^a> = <B, H_1, ... , H_k>$
- $B = M(or\ S)\ y^{aT}$ · $Hi = \Pi h_i a$
- T : 키 갱신을 위한 인자 ($t_1,...,t_k \in Z_q$), $T=t_1 \cdot ... \cdot t_k$

3.3 프로토콜

(1) 중앙 디바이스에서의 키 생성 및 분배 단계

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

Step 1. 중앙 디바이스는 하부 디바이스들을 예측하여 이를 바탕으로 열을 랜덤하게 선택한다.

$i = 1, ... , k$ 예측 ⇒ r_i열 선택

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

$h_i = g^{r_i} \bmod q$ 계산

공개키 <y, h_1, ... , h_k>

갱신을 위해 T생성 : $T = t_1 \cdot ... \cdot t_k$

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

$$\theta_i=(\sum r_j a_j t_j)/(\sum r_j \gamma_j) \bmod q$$

Step 4. 생성된 d_i를 디바이스에게 전송한다.

$$d_i = \theta_i \cdot \gamma_i$$

Step 5. 디바이스는 전송받은 di에서 개인키 θi를 획득한다.

$$di = \theta i \cdot \gamma i \ /\ \gamma i$$

(2) 중앙 디바이스 브로드캐스트 메시지 생성단계

브로트캐스트 메시지를 전송하는데 있어 메시지 자체를 암호화하여 전송한다. 다음은 중앙 디바이스에서 디바이스들에게로 제공하는 메시지에 대해 기술한다.

Step 1. 메시지 M 혹은 세션키 S를 암호화하여 계산하다. 이 때 세션키 S를 사용하는 경우에는 그 세션키 사용으로써 전체적인 통신이 이뤄진다. 하지만 계산된 키를 이용하여 메시지만을 제공할 경우에는 다음과 같이 계산한다.

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

Step 3. 중앙 디바이스와 디바이스들 간의 메시지 교환을 위해 다음 값을 암호화하여 디바이스들에게 전달한다.

$$C = <Ay^{aT},h_1^a,,h_k^a>$$

$$A=B/U^{\theta i},\ U=\Pi H_j^{\gamma j}$$

$$U^{\theta i}=(\Pi H_j^{\gamma j})^{\theta i}=(\Pi g^{arj\gamma j})^{\theta i}=(g^{rj\gamma j})^{\theta ia}=(g^{rjaj})^a=(h_j^{ajT})^a=y^{aT}$$

$$A = A \bullet y^{aT}/y^{aT}$$

Step 4. 브로드캐스트 메시지를 작성하여 디바이스들에게 전송한다.

$$C = <M(or\ S)y^{aT},h_1^a,,h_k^a>$$

Step 5. 전송받은 디바이스들은 메시지는 개인키를 이용하여 메시지 M를 획득한다.

$$M(or\ S)=B/U^{\theta i},\ U=\Pi H_j^{\gamma j}$$

$$U^{\theta i}=(\Pi H_j^{\gamma j})^{\theta i}=(\Pi g^{arj\gamma j})^{\theta i}=(g^{rj\gamma j})^{\theta ia}=(g^{rjaj})^a=(h_j^{ajT})^a=y^{aT}$$

$$M(or\ S) = M(or\ S) \bullet y^{aT}/y^{aT}$$

(3) 디바이스들의 브로드캐스트 메시지 생성단계

디바이스들은 상위 중앙 디바이스의 메시지 교환전에 받은 인자를 이용하여 자신과 다른 디바이스들에게 제공할 메시지를 계산한다.

Step 1. 중앙 디바이스가 세션키 S를 분배한 경우에는 단지 세션키 S를 이용하여 브로드캐스트 메시지를 생성하고 전송한다. 하지만 브로드캐스트 암호화를 이용하는 경우에는 중앙 디바이스에서 받은 인자를 이용하여 브로드캐스트 메시지를 작성한다.

Step 2. 디바이스들은 자신이 받은 A에서 랜덤 변수 a를 선택하여 다른 디바이스들에게 제공할 브로드캐스트 메시지를 계산한다.

Step 3. 브로드캐스트 메시지를 작성하여 다른 디바이스들에게 전송한다.

$$C = <M(or\ S)y^{aT},h_1^a,,h_k^a>$$

Step 4. 전송받은 디바이스들은 메시지는 개인키를 이용하여 메시지 M를 획득한다.

$$M(or\ S)=B/U^{\theta i},\ U=\Pi H_j^{\gamma j}$$

$$U^{\theta i}=(\Pi H_j^{\gamma j})^{\theta i}=(\Pi g^{arj\gamma j})^{\theta i}=(g^{rj\gamma j})^{\theta ia}=(g^{rjaj})^a=(h_j^{ajT})^a=y^{aT}$$

$$M(or\ S) = M(or\ S) \bullet y^{aT}/y^{aT}$$

(4) 키 갱신 단계(중앙 디바이스에서의 갱신 과정)

디바이스들의 탈퇴 혹은 신규 가입자가 발생한 경우 다음과 같이 중앙 디바이스에서 키 갱신 과정을 거친다.

Step 1. 디바이스 i가 탈퇴를 요청

Step 2. 중앙 디바이스는 기존 디바이스의 개인키를 갱신하기 위해 갱신요소인 T에서 디바이스 i의 갱신요소를 제거한다.

Step 3. 제거한 후 개인키를 갱신하고 디바이스들에게 전송한다.

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

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

$$(C=<M(orS) \cdot y^{aTti-1},h_1^a,\cdots,h_k^a>)^{\theta i} \text{ 계산}$$

$$M(or\ S)=B/U^{\theta iti-1},\ U=\Pi H_j^{\gamma j}$$

$$U^{\theta iti-1}=(\Pi H_j^{\gamma j})^{\theta iti-1}=(\Pi g^{arj\gamma j})^{\theta iti-1}=(g^{rj\gamma j})^{\theta iati-1}=(g^{rjajti})^{ati-1}=$$

$$(H_j^{ajti})^a=y^{aTti-1}$$

$$M(or\ S) = M(or\ S) \cdot y^{aTti-1}/y^{aTt-1}$$

4. 제안방식 고찰

본 방식은 다음과 같은 특징을 같도록 제안하였다. Ad-hoc 네트워크 이외에도 Ubiquitous 환경에서도 적용할 수 있도록 응용할 수 있다. 이것은 어느 일정한 공간에서 일정시간 동안만 키를 분배하는 경우 사용이 가능하며 향후 Ubiquitous 환경에서 사용자 주변의 기기간의 보안을 추구하고자 할 때 사용될 수 있을 것이다.

본 제안방식에서 살펴보면, 사용자가 메시지를 전송할 수 있다는 것이다. 이것은 공간의 특징을 이용하여 중앙 디바이스만이 다른 디바이스에 브로드캐스트 메시지를 전송하는 것이 아니라 사용자가 공개된 키를 이용하여 다른 사용자에게 메시지 전달이 가능하다. 또한 키의 갱신이 필요치 않다. 이것은 일정공간에서 일정시간만 사용한 후 폐기될 것이기 때문에 키 갱신이 필요치 않다는 것이다. 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 디바이스에 알려진다 하더라도 중앙 디바이스에서 다른 디바이스 탈퇴 후 키 갱신에는 T를 이용하게 됨으로 a가 공개되었다하더라도 안전하게 통신을 할 수 있다.

5. 결론

브로드캐스트 암호화는 공개된 네트워크 상에서 인가된 사용자에게만 컨텐츠를 제공하는데 사용한다. 인가된 사용자이외에는 브로드캐스트되는 메시지에 대해 아무런 정보를 얻어낼 수 없으며, 인가된 사용자는 사전에 전송된 개인키를 이용하여 세션키를 취득할 수 있게 된다.

본 논문은 ad-hoc 네트워크에서 모든 디바이스가 키 생성을 하는 것이 어려울 경우 Broadcast Enryption을 이용하여 해결 할 수 있다. 이와 같은 경우는 작은 공간에서 일시적인 네트워크에 키를 분배할 수 있다. 또한 모든 사용자가 브로드캐스트 메시지를 다른 사용자에게 전송할 수 있어 전체적인 보안 통신을 이룰 수 있다.

향후 연구 분야로서는 각각의 ad-hoc 네트워크에서 발급받은 키가 계속적으로 사용되도록 하는 연구가 필요하며, 향후 Ubiquitous로 발전하였을 경우 자신의 디바이스에 키를 분배하고 관리하는 방법에 관한 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 Enryption 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] 이원희, 구재형, 이동훈, "Ad-hoc 환경에서의 2-라운드 비대칭 키공유 기법", 한국정보보호학회하계학술대회 vol. 13. No. 1, 2003. 7