부분 집합 차를 이용한 안전한 그룹 통신*

김희열°, 이윤호, 정병천, 이재원, 윤현수, 조정완
한국과학기술원
{hykim°, yhlee, bcchung, jaewon, hyoon, jwcho}@camars.kaist.ac.kr

Secure Group Communications Using Subset Difference

Heeyoul Kim°, Yun-ho Lee, Byungchun Chung, Jaewon Lee, Hyunsoo Yoon, Jung-wan Cho
Korea Advanced Institute of Science and Technology

요 약

그룹 통신을 이용한 어플리케이션이 증가함에 따라 안전하면서도 효율적인 그룹 통신에 관한 요구가 높아지고 있다. 이를 위해서는 안전한 데이터 통신, 그룹 멤버 관리, 그리고 확장성이 요구되며, 특히 빈번한 멤버의 가입/탈퇴시에 효율적으로 키를 갱신하는 수단이 필요하다.

제안된 시스템에서는 대칭키 암호화 알고리즘을 통해 안전성을 확득하며, 부분집합 차를 이용해서 키 갱신을 수행하기 때문에 요구되는 메시지의 횟수를 감소시켰다. 기존 방법에서는 키 갱신을 위해 *O(log n)*번의 멀티캐스트가 요구되었지만, 제안된 시스템에서는 오직 한 번의 멀티캐스트만이 요구된다. 또한 제안된 시스템은 큰 정수의 인수분해 문제의 어려움에 기반하기 때문에, 안전성을 보장받을 수 있다.

1. 서론

그룹 통신은 클러스터 시스템, 원격 회의, 인터넷 방송 등 수많은 어플리케이션을 가능하게 해 주는 필수 요소로, 최근 그 중요성이 더욱 부각되고 있다. 이에 따라 그룹에 속한 멤버만이 통신에 참여할 수 있는 안전한 그룹 통신의 필요성이 높아졌다. 안전한 통신에 관한 기존 연구는 1대1 통신이 대상이었기 때문에 이를 그룹 통신에 적용하기에는 매우 비효율적이며, 그룹 통신에 적합한 새로운 방법을 찾기 위한 연구가 진행되고 있다.

안전한 그룹 통신이 만족해야 하는 특성은 다음과 같다.

- **안전한 데이터 통신** : 전송되는 데이터는 오직 그룹 멤버만이 알 수 있어야 한다. 이를 위해서는 그룹 멤버만이 공유하는 키가 있어야 한다.
- **그룹 멤버 관리** : 새로운 멤버의 가입과 기존 멤버의 탈퇴 등 그룹 멤버의 변화에 적절하게 대응할 수 있어야 한다. 특히 탈퇴한 멤버는 그 후에 전송되는 데이터를 알 수 없어야 하며, 이를 위해 공유된 키를 갱신한다.
- **확장성** : 한 멤버의 가입/탈퇴가 모든 그룹 멤버에게 영향을 주지 않아야 한다. 이 필요조건은 특히 규모가 큰 그룹에게 매우 중요한 요소이다.

본 논문에서는 부분집합 차를 이용해서 멤버의 가입/탈퇴시에 수행해야 하는 키 갱신 과정을 효율적으로 수행하는 새로운 방법을 제안한다. 특히 이 방법을 사용하면 규모가 큰 그룹에서의 확장성도 쉽게 얻을 수 있다.

2. 관련 연구

안전한 그룹 통신에 관한 연구는 오랫동안 진행되어 왔으며 [1, 2, 3, 4, 5], 그림 1과 같이 분류할 수 있다.

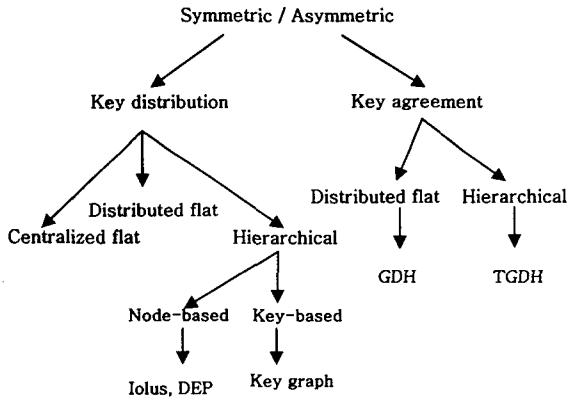

그림 1. 안전한 그룹 통신에 관한 분류

이 중에서 특히 [4]의 방법은 키 그래프를 사용하는 방법으로, 각 멤버가 트리의 리프 노드가 되어서 루트로부터 자신까지의 경로상에 있는 내부 노드의 키를 가지는 방식을 사용한다. 이 방식을 사용하면 멤버의 가입/탈퇴시 *log(n)*번의 멀티캐스트 메시지 전송으로 키를 갱신할 수 있다.

이와는 별도로, 하나의 전송자가 정해져 있고 그룹이 고정되어 있는 상황에서의 안전한 데이터 전송을 위한 브로드캐스트 암호화 방법이 제안되었다[6, 7, 8]. 그 중 [8]에서는 부분집합 차를 이용한 효율적인 방식이 제안되었지만, 자유롭게 멤버가 가입/탈퇴를 할 수 없다는 한계를 지닌다.

*본 연구는 첨단정보기술 연구센터를 통하여 과학재단의 지원을 받았고 대학 IT연구센터 육성·지원사업의 연구결과로 수행되었음

3. 제안된 시스템

3.1 부분집합 차를 이용한 키 분배

그림 2와 같이 n명의 멤버가 단말 노드가 되는 트리가 있다고 하고, S_i는 전체 노드에서 i 노드가 루트가 되는 트리를 제외한 노드의 집합이라 하자. 그리고, K_i는 S_i에 속한 노드만이 공유하는 키라고 하자. 각 멤버는 대응하는 단말노드로부터 루트까지의 경로상에 있는 각 노드의 형제 노드에 해당하는 키를 가지게 된다. 예를 들어, u_2는 K_3, K_5, K_8을 분배받는다. 이 키들과 3.2절의 함수 $f_1()$, $f_2()$를 사용하면, K_9를 제외한 모든 키를 얻을 수 있다. 멤버의 가입/탈퇴가 발생하면 이 키를 통해서 그 멤버를 제외한 나머지 멤버간의 안전한 통신이 가능하다.

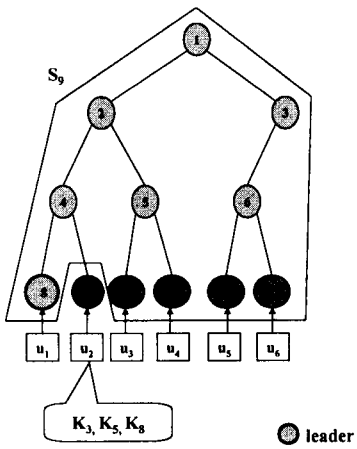

그림 2. 각 멤버가 가지는 키의 분배

3.2 키 계산 및 갱신을 위한 함수

각 멤버가 가지는 키의 계산 및 갱신을 위해서는 다음과 같은 특성을 가지는 함수 $f_1()$, $f_2()$가 요구된다.

- 각 키 K_i는 다음과 같은 관계를 만족하며, 이 관계를 통해서 K_i를 알고 있는 멤버는 i 노드의 모든 자손 노드 j의 키인 K_j를 알 수 있다.

$$K_{2i} = f_1(K_i),\ K_{2i+1} = f_2(K_i)$$

- 각 함수는 단방향성을 가지며, 이는 K_{2i}를 아는 멤버가 상위레벨의 키인 K_i를 알 수 없게 한다. 단방향성이란 주어진 x를 통해서 $f(x)$를 계산하는 것은 쉽지만, $f(x)$를 통해서 x를 구하는 것은 어려운 특성으로 해쉬와 암호 분야에서 많이 사용되고 있다.

- 각 함수는 곱의 특성을 가지며, 이는 키를 갱신하는 과정에서 사용된다. 곱의 특성을 가지는 함수란 다음의 식을 만족하는 함수를 말한다.

$$f(x \cdot y) = f(x) \cdot f(y)$$

이 특성을 만족하는 함수 중 널리 알려진 함수는 기존 RSA 암호 시스템에서 암호화에 사용되는 함수이다[11]. 큰 두 소수 p,q의 곱을 n이라 하고, $d \cdot e \equiv 1 \bmod (p-1)(q-1)$을 만족한다고 하자. 오직 n과 e만을 공개하고 $f(x) = x^e \bmod n$ 이라고 하면, d를 모르는 상태에서 $f(x)$를 통해서 x를 구하는 것은 매우 어려우며 이는 $f()$가 단방향성을 가짐을 말한다. 또한,

$$f(x) \cdot f(y) = (x^e \bmod n) \cdot (y^e \bmod n) = (x \cdot y)^e \bmod n = f(x \cdot y)$$

를 만족하므로 $f()$는 곱의 특성을 가진다.

3.3 시스템 초기화

m명이 모여서 그룹을 생성하고 시스템을 초기화하는 과정은 다음과 같다. 우선 한 멤버를 그룹 리더로 선출하게 되며, 선택된 리더는 그룹의 키와 멤버 변화를 관리하고 그룹간의 통신이 완료될 때까지 탈퇴할 수 없다.

초기화를 위해 리더는 다음을 수행한다.

- 임의의 키 K_1을 생성한다.
- $n=p \cdot q$ (p,q는 소수)를 계산하고, $d1 \cdot e1 \equiv d2 \cdot e2 \equiv 1 \bmod (p-1)(q-1)$을 생성한다. 그리고, 함수 $f_1(x)=x^{e1} \bmod n$, $f_2(x)=x^{e2} \bmod n$을 정의한다.
- 키 K_1과 $f_1()$, $f_2()$를 통해 다른 모든 키 K_i를 계산한다.
- 데이터 전송시에 사용되는 임의의 세션키 S를 생성한다.

그리고, 리더를 제외한 나머지 멤버는 다음을 수행한다.

- 리더로부터 n, $e1$, $e2$, S를 얻는다.
- 3.1절에서 설명한 것처럼 자신이 가져야 할 키 K_i들을 리더로부터 얻는다.

3.4 데이터 전송

전송할 데이터에 대한 암호화는 DES등의 대칭키 암호 알고리즘을 사용한다[10]. 주어진 데이터 M에 대해서, 세션키 S를 키로 사용한 암호화/복호화를 $E_S()$/$D_S()$라 하자. 데이터를 전송하고자 하는 전송자는 $C=E_S(M)$를 계산해서 C를 멀티캐스트한다. 세션키 S는 그룹내의 모든 멤버가 공유하고 있기 때문에 오직 그룹 멤버만이 복호화를 통해 $M=D_S(C)$를 얻을 수 있다.

3.5 새로운 멤버의 가입

새로운 멤버가 추가되었을 때 수행되는 과정은 다음과 같다. 새 멤버 u_7이 가입했다면 이 멤버는 가입하기 전에 전송되었던 데이터를 알 수 없어야 하며, 이를 위해서는 세션키를 갱신해야 한다. 그룹 리더는 새로운 세션키 S'을 생성해서 $C=E_S(S')$을 멀티캐스트하며, 기존 멤버들은 S를 알기 때문에 C를 통해서 S'을 얻게 된다. 그리고 리더가 u_7에게 S'과 할당된 키 K_i들을 안전한 채널을 통해 전송하면, $u_1 \sim u_7$이 모두 S'이라는 공통된 세션키를 가지게 된다. 또한 u_7은 예전 세션키인 S를 알 수 없으므로 예전 데이터를 알 수 없다.

3.6 기존 멤버의 탈퇴

한 멤버가 그룹을 탈퇴한다면, 그 멤버가 알고 있던 키 K_i들과 세션키 S를 갱신해야 한다. 예를 들어, 그림 3에서 u_6이 알고 있던 키 K_2, K_6, K_{12}, S를 갱신해야 한다. 기존의 방법들은 키 갱신을 위해 최소한 $log(n)$번의 멀티캐스팅이 필요했으며, 본 논문에서는 다음의 과정을 통해 1번의 멀티캐스팅만으로 키 갱신을 수행한다.

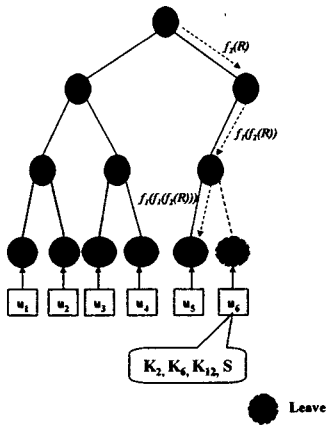

그림 3. u_6의 탈퇴

탈퇴하는 멤버 u_r에 대응하는 단말 노드를 r라고 하자. 그룹 리더는 새로운 세션키 S'과 임의의 수 R을 생성한 후에 $C=E_{Kl}(R \| S')$을 계산해서 멀티캐스팅한다. K_l는 r을 제외한 모든 다른 멤버가 알고 있으므로 남아있는 멤버들은 S'과 R을 알게 된다. 다음으로 리더는 $K_1'=K_1 \cdot R \bmod n$을 계산한다. K_i를 온 3.2절의 관계를 만족해야 하기 때문에, 새로 갱신되는 키 K_i'에 대해서 $K_{2i}'= f_1(K_i')$, $K_{2i+1}' = f_2(K_i')$을 만족해야 한다. 이 때,

$$K_2'=f_1(K_1')=f_1(K_1 \cdot R)=f_1(K_1) f_1(R)=K_2 f_1(R)$$

을 만족하므로 기존 키인 K_2와 R, 함수 $f_1()$을 알면 새로운 키 K_2'을 얻을 수 있으며, 마찬가지로 모든 i에 대해서 기존의 키 K_i'와 R, 함수 $f_1()$, $f_2()$를 알면 새로운 키 K_i'을 구할 수 있다. 멤버 r을 제외한 각 멤버는 이를 통해서 자신의 키를 갱신하게 된다.

4. 안전성 분석 및 성능 평가

제안된 시스템의 안전성은 큰 정수의 인수분해 문제의 어려움에 기반하고 있다. 특히, 키 갱신 과정에서 자신이 모르는 상위레벨의 키를 알기 위해서는 주어진 n을 인수분해 할 수 있어야 하며, 이는 매우 어려운 문제로 널리 사용되는 RSA방식도 이 문제에 안전성을 기반한다. 제안된 시스템은 그룹 내부에 속한 멤버가 공격자와 협동하지 않는다는 가정을 하고 있다. 그렇지 않을 경우 공격자가 알게 되는 키가 많아질 가능성이 높아지며, 이는 전체 시스템의 안전성을 위협하게 된다. 향후 과제로는 내부 협조자에도 안전한 시스템을 제안하고 이에 대한 증명이 수행되어야 한다.

안전한 그룹 통신의 성능 평가에서 고려해야 할 요소는 다음과 같다.

- 각 멤버가 가지는 키의 개수
- 가입/탈퇴시 전송되는 메시지의 횟수
- 가입/탈퇴시 각 멤버가 계산하는 연산량

표 1은 키 그래프를 사용하는 방법과 제안된 시스템을 비교하고 있다. 특히 가입/탈퇴시의 멀티캐스트 횟수를 줄임으로써 보다 효율적인 키 갱신이 가능해졌다.

	키 그래프	제안된 시스템
노드가 저장하는 키 개수	$O(\log n)$	$O(\log n)$
가입시 메시지 수 (멀티캐스트)	$O(\log n)$	$O(1)$
가입시 메시지 수 (유니캐스트)	$O(1)$	$O(1)$
탈퇴시 메시지 수 (멀티캐스트)	$O(\log n)$	$O(1)$
가입시 각 노드의 연산량	$O(\log n)$	$O(1)$
탈퇴시 각 노드의 연산량	$O(\log n)$	$O(\log n)^*$

*: 모듈라 지수 연산

표 1. 제안된 시스템의 성능 평가 및 비교

5. 결론

본 논문에서는 효율적이고 안전한 그룹 통신을 수행하는 시스템을 제안하였다. 그룹 통신을 수행하기 위해서는 전송되는 데이터의 비밀성 보장 뿐만 아니라 빈번하게 발생하는 멤버의 가입/탈퇴시에 효율적으로 키를 갱신할 수 있는 수단이 요구된다.

기존 방법 중 가장 효율적인 키 그래프를 사용한 방법에서도 키 갱신을 위해 $O(\log n)$의 멀티캐스트가 요구된 반면에, 제안된 시스템은 부분집합 차를 이용해서 키를 갱신하기 때문에 멤버의 가입/탈퇴시에 한번의 멀티캐스트만이 요구된다.

제안된 시스템의 안전성은 큰 정수의 인수분해 문제의 어려움에 기반하며, 이는 매우 어려운 문제로 알려져왔다. 그러므로 제안된 시스템도 단일 공격자에 대한 안전성을 가진다.

References

[1] Tony Ballardie. Scalable Multicast Key Distribution, RFC 1949, May 1996

[2] L. R. Dondeti, S. Mukherjee, and A. Samal. A dual encryption protocol for scalable secure group communication. Technical Report UNL-CSE-1999-001, University of Nebraska-Lincoln, February 1999

[3] S. Mittra. Iolus: A Framework for Scalable Secure Multicasting. In Proc. ACM SIGCOMM, pages 277-288, Cannes, France, September 1997

[4] C. K. Wong, M. Gouda, and S. S. Lam. Secure group communications using key graphs. In Proc. ACM SIGCOMM, August 1998

[5] Y. Kim, A. Perrig, and G. Tsudik. Simple and fault-tolerant key agreement for dynamic collaborative groups. In 7th ACM Conference on Computer and Communications Security, pages 235-244, Greece, Nov. 2000

[6] A. Fiat and M. Naor, Broadcast Encryption, Advances in Cryptology – CRYPTO '93, Lecture Notes in Computer Science 773, Springer, 1994, pages 480-491

[7] J. A. Garay, J. Staddon and A. Wool, Long-Lived Broadcast Encryption. Advances int Cryptology – CRYPTO '2000, Lecture Notes in Computer Science, vol 1880, pages 333-352, 2000

[8] D. Naor, M. Naor, and J. Lotspiech, Revocation and Tracing Schemes for Stateless Receivers, Lecture Notes in Computer Science 2139, Springer, 2001

[9] O. Goldreich, S. Goldwasser and S. Micali, How to Construct Random Functions. JACM 33(4), pages 792-807, 1986

[10] ANSI X3.92, American National Standard for Data Encryption Algorithm (DEA), American National Standards Institute, 1981

[11] ISO/IEC 9796, Information Technology-Security Techniques-Digital Signature Scheme Giving Message Recovery, International Organization for Standardization, Jul, 1991