아이디 기반의 일 라운드 삼자 간 키 합의 프로토콜을 이용한 효율적인 결함 허용 회의 키 합의 방법

(Efficient Fault-Tolerant Conference-Key Agreement using ID-based One Round Tripartite Key Agreement Protocol)

이 상 호 † 김 종 ††
(Sangho Lee) (Jong Kim)

홍 성 제 ††
(Sung Je Hong)

요 약 컴퓨터 네트워크를 이용한 회의에 있어서 공유 키 합의 프로토콜은 보안이 필요한 회의에 필수적이다. 그 중에서도 결함 허용 회의 키 합의 프로토콜은 가짜 참여자가 키 생성을 방해한다고 하더라도 정당한 참여자만이 회의 키를 공유할 수 있게 만들어주는 방법이다. 그러나 기존의 방법은 가짜 참여자의 수가 많을 경우 효율적으로 동작하지 못한다는 문제점이 있다. 본 논문은 결함 허용 회의 키 합의 방법에 아이디 기반의 삼자 간 키 합의 프로토콜을 적용하여 기존의 방법들에 비하여 낮은 키 합의 비용으로 동작하는 결함 허용 회의 키 합의 방법을 제안한다. 실험결과는 효율적이라고 알려진 Yi의 방법보다 제안 방법이 효율적이며, 특히 공격자가 많은 경우엔 더욱 효율적으로 동작하는 것을 보여준다.

키워드 : 회의 키 합의 프로토콜, 결함 허용, 일 라운드 삼자 간 키 합의 프로토콜, 아이디 기반 암호학

Abstract A conference-key agreement protocol is essential for computer network conferences that need secure communications. Especially, the fault-tolerant conference-key agreement can make a shared conference-key even if some fake conferees disturb the key agreement processes. However, the performance of the previous fault-tolerant conference-key agreement protocols is decreasing significantly when the number of fake conferees is increasing. In this paper, we propose an efficient fault-tolerant conference key agreement protocol. Our scheme is based on the ID-based one round tripartite conference key agreement protocol. Simulation results show our scheme's efficiency against Yi's method especially when the number of fake conferees is large.

Key words : Conference-key agreement protocol, fault tolerance, One round tripartite key agreement protocol, ID-based cryptography

1. 서 론

컴퓨터 네트워크 회의는 컴퓨터 네트워크를 통해서 다수의 참여자가 회의나 협업을 하기 위한 기술이다. 이러한 컴퓨터 네트워크 회의를 지원하기 위한 일반적인 방법은 모든 참여자가 회의 교량(conference bridge) 서버에 접속하는 것이다. 회의 교량은 여러 참여자로부터 메시지를 전달받아 모든 참여자에게 다시 브로드캐스트하는 것을 통해서 전체 네트워크 트래픽을 줄인다[1].

회의나 협업의 결과물들이 기밀 사항이나 사생활 정보 등과 같은 중요한 내용을 담고 있다면 이를 보호하기 위한 방법이 필요하다. 이러한 기밀성을 보장하기 위한 가장 일반적인 방법은 암호화를 이용하는 것이다. 그런데 암호화를 위해선 모든 참여자가 동일한 키를 공유하기 위한 과정이 필수적이다. 회의 키를 공유하는 방법은 크게 분배와 합의로 나눌 수 있다. 회의 키 분배는 특정한 키 분배자가 공유 키를 생성해서 모든 회의 참여자에게 나눠주는 방식으로 프로토콜이 단순하고 통신 비용도 적다는 장점이 있지만 키 분배자가 TTP(Trusted Third Party)여야만 한다는 요구사항이 있다. 회의 키 합의 방법은 위와 다르게 공유 키를 만드는 과정에 모든 회의 참여자가 참여하는 방식으로 TTP가 없이 참여자 사이의 통신만으로 키를 만들 수 있다는 장점이 있지만 프로토콜이 상대적으로 복잡하고, 통신 비용도 크다는 단점이 있다. 하지만 회의에 참여하는 참여자들만이 키를 공유하기 때문에 분배에 기반한 방법보다 보

· 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 지원 사업의 연구결과로 수행되었음(IITA-2007-C1090-0701-0045)
· 이 논문은 제34회 추계학술대회에서 '아이디 기반 삼자 간 키 합의 프로토콜에 기반한 효율적인 결함 포용 회의 키 합의 방법'의 제목으로 발표된 논문을 확장한 것임

† 학생회원 : 포항공과대학교 컴퓨터공학과
sangho2@postech.ac.kr
†† 종신회원 : 포항공과대학교 컴퓨터공학과 교수
jkim@postech.ac.kr
sjhong@postech.ac.kr

논문접수 : 2007년 12월 6일
심사완료 : 2008년 4월 24일

정보과학회논문지: 컴퓨팅의 실제 및 레터 제14권 제5호(2008.7)

안성은 더 높다고 볼 수 있다.

기존의 회의 키 합의 방법은 악의적인 참여자가 단 한 명이라도 있다면 회의 키 생성을 보장할 수 없다. 이 문제를 해결하기 위해서 악의적인 참여자의 수에 상관없이 정당한 참여자만이 회의 키를 얻을 수 있는 결함 허용 회의 키 합의 프로토콜이 제안되었다[1-4]. 그러나 지금까지 제시된 방법들은 결함이 발생할 때마다 회의 키 합의 과정을 처음부터 다시 실행한다는 문제점이 있다. 공격자가 이 점을 이용해서 t명의 거짓 참여자를 이용, 한 순간에 하나의 참여자만이 결함을 발생시키게 한다면 최소한 t+1번의 회의 키 합의 과정이 필요하게 되게 되기 때문에 회의 키 합의를 지연시키고, 네트워크 트래픽을 증대시키는 공격을 할 수 있다.

본 논문은 공격자의 수가 많더라도 효율적으로 작동할 수 있는 새로운 회의 키 합의 프로토콜을 제안한다. 제안 방법은 하나의 회의를 세 개의 부 회의 (sub-conference)로 나누어, 각각의 부 회의에서 회의 키를 생성한 뒤, 일 라운드 삼자 간 키 합의 프로토콜[5]을 이용해서 전체 회의의 공유 키를 만드는 방법을 사용한다. 모든 참여자를 세 개의 부 회의에 임의로 할당한다면 공격자가 t명의 거짓 참여자를 이용한다고 하더라도 회의 키 합의 과정은 평균적으로 $t/3$+1번 정도만 실행된다. 또한 이 방법은 각 참여자가 원래 회의의 1/3 크기인 부 회의에 대한 키 합의 과정에만 직접 참여하기 때문에, 제안하는 방법은 공격이 없는 상황에서도 각 참여자의 비용을 1/3 수준으로 줄일 수 있다. 그러므로 제안하는 방법은 공격이 발생하는 경우 약 1/9 수준의 비용만 요구하게 된다. 추가적으로, 제안 방법을 재귀적으로 적용하는 것을 통해서 $\log_3 t$에 비례하는 비용 감소를 달성할 수 있다. 회의 키 합의 과정의 효율성을 높이기 위해 이 논문에선 효율적이라고 알려진 Yi의 방법[1]으로 부 회의의 공유 키를 생성한다.

이 논문의 구성은 다음과 같다. 2장에서는 아이디 기반의 암호학과 일 라운드 키 합의 프로토콜 대해서 설명하고, 3장에서는 부 회의의 공유 키 합의 과정에 사용할 Yi의 방법에 대해서 소개할 것이다. 4장에서는 제안하는 방법에 대해서 보다 자세히 설명할 것이고, 5장과 6장을 통해서 제안 방법의 비용을 분석하고 Yi의 방법과의 비교를 통해서 제안 방법의 효율성을 보일 것이다. 마지막으로, 7장에서 결론을 맺는다.

2. 배경 지식

2.1 아이디 기반 암호학

기존의 인증서 기반의 PKI(Public Key Infrastructure)는 인증서의 검증을 위해서 모든 인증서의 정보를 관리하고, 인증서 상의 CA (Certificate Authority)의 전자 서명을 확인해야 하는 과정이 필수적이었다. 이러한 저장 공간과 계산량을 감소시키기 위해서 등장한 것이 바로 ID 기반의 암호학으로 이메일 주소 같은 특정 사람의 공개 정보를 공개 키로 사용하는 방법이다. 이 방법은 인증서를 관리할 필요가 없이 사용자의 공개 키를 바로 알아낼 수 있다는 장점을 가진다. 이 장에선 Yi의 논문[1]에서 사용된 Weil 페어링을 이용한 아이디 기반 암호학을 소개한다[6].

ID 기반의 암호학은 페어링이라는 특성에 기반한다. 페어링의 정의와 그 특성은 다음과 같다.

- 정의
  - $p = 6q - 1$, p와 q는 소수
  - E: F_p 상에서 Weierstrass 방정식($y^2 = x^3 + 1$)으로 정의된 초특이 타원곡선(supersingular elliptic curve)
  - $E(F_p)$: 차수(order)가 $p+1$인 순환군(cyclic group)
  - G_1: $E(F_p)$에 속하는 차수 q인 순환 부분군(cyclic subgroup)
  - ϑ: G_1의 생성자(generator)
  - G_2: 차수 q의 모든 원소를 포함하는 F_{p^2}의 부분군
  - $\hat{e}: G_1 \times G_1 \rightarrow G_2$ (Pairing)
- 특성
  - $\hat{e}(aP, bQ) = \hat{e}(P,Q)^{ab}, P, Q \in G_1, a, b \in Z$
  - $\hat{e}(\vartheta, \vartheta)$: G_2의 생성자
  - $\hat{e}(P_1 + P_2, Q) = \hat{e}(P_1, Q)\hat{e}(P_2, Q)$
  - $\hat{e}(P,Q) \neq \hat{e}(Q,P)$

ID 기반의 암호학이 성립하기 위해선 기존 PKI의 CA에 준한 KGC(Key Generation Center)가 필수적이다. KGC는 도메인 파라미터인 기준점 P를 선택하고 자신의 비밀 키 s를 임의로 선택한 뒤, 자신의 공개 키 $P_{KGC} = sP$를 계산한다. ID 기반의 암호학에선 사용자의 ID 정보가 공개 키로 사용되며 ($G_i = H(ID_i), H: \{0,1\}^* \rightarrow G^*$), 그 사용자의 개인 키는 KGC의 개인 키 s와 사용자의 공개 키의 곱인 sG_i이다. KGGC는 이 사용자 개인 키를 계산하여 해당 사용자에게만 안전하게 전달해준다고 가정한다.

2.2 인증 가능한 일 라운드 삼자 간 키 합의

Zhang 등은 ID 기반 암호학을 이용한 인증 가능한 일 라운드 삼자 간 키 합의 프로토콜을 제안했다[5].

A, B, & C have public/private key pairs:

$$G_i = H(ID_i), S_i = sG_i$$

$$A \rightarrow B,C: \; P_A = aP, T_A = h(P_A)S_A + aP_A$$

$B \rightarrow A,C$: $P_B = bP, T_B = h(P_B)S_B + bP_B$

$C \rightarrow A,B$: $P_C = cP, T_C = h(P_C)S_C + cP_C$

A verifies: $\hat{e}(T_B + T_C, P) \stackrel{?}{=}$

$\hat{e}(h(P_B)G_B + h(P_C)G_C, P_{KGC})\hat{e}(P_B, P_B)\hat{e}(P_C, P_C)$

A computes: $K = \hat{e}(P_B, P_C)^a = \hat{e}(P, P)^{abc}$

본 논문에선 위의 방법을 부 회의 키를 이용하여 전체 회의 키를 만드는 과정에 사용할 것이다.

3. 부 회의 키 합의 방법: Yi의 아이디 기반 결함 허용 회의 키 합의 방법[1]

3.1 부 회의 키 합의 프로토콜

1. 모든 참여자가 회의 교량 서버에 접속
2. 회의 교량은 모든 참여자에게 모든 참여자의 ID목록과 회의 번호 N을 전송
3. 각 참여자 i는 서브 키 k_i를 임의로 선택하고, 그 서브 키를 다른 참여자의 공개 키 $G_j = H(ID_j)$로 암호화한 값 e_{ij}와 인증을 위한 값 A_i, $Sign_i$를 회의 교량에 전송

$A_i = k_i P, e_{ij} = k_i + h(\hat{e}(k_i P_{KGC}, G_j), N) \bmod q, i \neq j$

$R = rP, Sign_i = rP_{KGC} + h(A_i, \Sigma e_{ij}, R)S_i$

회의 교량은 서명을 확인한 후 서브 키 목록 γ_i를 각각의 참여자에 전달

$\gamma_i = \Sigma e_{ij}, i \neq j$

4. 각 참여자는 전달받은 서브 키들의 암호를 풀어서 부 회의 키 K를 생성

$K = k_i + \gamma_i - \Sigma h(\hat{e}(A_j, S_i), N) \bmod q$

$= \Sigma k_i \bmod q$

$\Sigma A_i \stackrel{?}{=} KP$ (Verification)

3.2 결함 허용 기법

1. 참여자는 회의 키를 만드는데 실패한 경우(서브 키를 다 받지 못했거나, $\Sigma A_i \neq KP$인 경우) 회의 교량에 결함이 발생했다고 통보
2. 회의 교량은 아래와 같은 참여자를 참여자 목록에서 제외
   - 결함 통보를 너무 자주 발생시킨 참여자(네트워크 결함)
   - 가짜 결함 통보를 발생시킨 참여자(공격자)
   - 가짜 서브 키를 보낸 참여자(공격자)
3. 새로운 참여자 목록을 기반으로 회의 키 합의를 재시작
4. 위의 과정을 결함이 발생하지 않을 때까지 반복

4. 제안하는 회의 키 합의 방법

4.1 회의 키 합의 프로토콜

1. 회의 교량은 모든 참여자를 세 개의 부 회의에 임의로 나누어 배정한다.
2. 각 부 회의는 독립적으로 키 합의 과정(3.1 절)을 수행한다. 다시 말하면, 각 부 회의는 다른 부 회의에 결함이 발생여부에 상관없이 자신에게 결함이 발생하지 않았다면 키 합의 과정을 종료
3. 회의 교량은 부 회의1의 모든 참여자에 P_1과 T_1을 요청
4. 참여자 j는 회의 교량에 $P_1 = K_1 P, T_1 = h(P_1)S_J + K_1 P_J$를 전송
5. 회의 교량은 모든 참여자가 전송한 P_1이 같은지 확인하고, $\hat{e}(T_1, P) \stackrel{?}{=} \hat{e}(h(P_1)G_j, P_{KGC})\hat{e}(P_1, P_1)$을 통해서 인증 과정을 수행
6. P_1와 T_1를 다른 부 회의에 속한 참여자에게 전송
7. 부 회의$_2$, 부 회의$_3$에 대해서도 동시에 3-6번 과정을 수행
8. 부 회의$_1$의 참여자 j는 P_2와 P_3를 확인한 뒤, 회의 키를 계산

$\hat{e}(T_2 + T_3, P) \stackrel{?}{=}$

$\hat{e}(h(P_2)G_k + h(P_3)G_l, P_{KGC})\hat{e}(P_2, P_2)\hat{e}(P_3, P_3)$

$conference - key = h(\hat{e}(P_2, P_3)^{K_1})$

9. 부 회의$_2$, 부 회의$_3$의 참여자도 8번 과정을 수행해서 회의 키를 계산

4.2 제안 방법의 이점

Yi의 방법은 결함이 발생하면 모든 참여자가 다시 키 합의과정을 수행하는 방식이기 때문에 결함을 처리하는데 상당한 비용이 필요하다. 제안 방법은 이에 필요한 비용을 줄이기 위해서 하나의 회의를 세 개의 부 회의로 나누었다. 이렇게 하면 세 개의 부 회의 중에 하나라도 키 합의 과정을 성공적으로 수행한 경우엔 그 부 회의에 속한 참여자들은 더 이상 키 합의 과정을 수행할 필요가 없기 때문에 결함 허용을 위한 비용을 줄일 수 있다.

4.3 재귀적 방법

제안한 방법을 개선시킬 수 있는 방법으로 결함이 발생한 부 회의를 다시 3개의 부 회의로 나누는 재귀적인 방법을 고려해볼 수가 있다. 이 방법을 이용하면 t명의 가짜 참여자가 있을 때 $t/3+1$번의 부 회의 키 합의 과정을 $\log_3 t+1$로 줄일 수 있다. 그러나 이 방법에선 부 회의 키를 합쳐서 회의 키를 만드는 과정의 횟수가 1번에서 $\log_3 t+1$ 번으로 늘어나는 역효과도 있다.

5. 비용 분석

키 합의 과정에서 가장 큰 비용을 차지하는 연산은 지수적 연산인 점 간의 곱셈 연산과 페어링 연산이다. 수식 표현의 편의를 위해 이 두 연산을 각각 m 과 w 로 표시할 것이다.

5.1 결함이 발생하지 않았을 때의 비용 비교

Yi의 방법은 n 명의 참여자가 있을 때 각 참여자마다 $(n+3)$번의 점 간의 곱셈 연산과 $2(n-1)$번의 페어링 연산을 수행해야 하므로 총 연산량은 $n((n+3)m+2(n-1)w)$ 이다. 제안하는 방법은 부 회의 키를 만드는 과정에서 각 참여자마다 $\left\lceil \frac{n}{3} \right\rceil + 3$번의 점 간의 곱셈 연산과 $2\left(\left\lceil \frac{n}{3} \right\rceil - 1\right)$번의 페어링 연산이 필요하고, 회의 키를 만드는 과정에서 각 참여자마다 5번의 점 간의 곱셈 연산과 5번의 페어링 연산이 필요하므로 총 연산량은 $n\left(\left(\left\lceil \frac{n}{3} \right\rceil + 8\right)m + \left(2\left\lceil \frac{n}{3} \right\rceil + 3\right)w\right)$. 그러므로 $n \geq 8$ 이면 제안하는 방법의 비용이 더 적다.

5.2 결함이 발생했을 때의 비용 비교

Yi의 방법은 n명의 참여자 중 t명이 공격자인 경우에 $(n-t)$ 참여자가 프로토콜을 $(t+1)$번 반복해야 하므로 연산의 총합은 $(n-t)\sum_{j=0}^{t-1}((n-j+3)m+2(n-j-1)w)$.

제안하는 방법의 경우는 공격자가 몇 개의 부 회의를 공격하느냐에 따라서 나눠서 분석해야 한다.

- 3개의 부 회의를 동시에 공격하는 경우: 공격자는 3개의 부 회의에 속한 가짜 참여자를 각각 선택해서 3개의 부 회의를 동시에 공격할 수 있다. 이 경우의 연산의 총합은 아래와 같다.

$$(n-t)\left(\sum_{j=0}^{\lceil t/3\rceil+1}\left(\left(\left\lceil \frac{n}{3} \right\rceil - j + 3\right)m + 2\left(\left\lceil \frac{n}{3} \right\rceil - j - 1\right)w\right) + 5m + 5w\right)$$

- 2개의 부 회의만 공격하는 경우: 공격받지 않는 부 회의에 속한 $\frac{(n-t)}{3}$ 명은 $\left\lceil \frac{n}{3} \right\rceil + 8$ 번의 점 간의 곱셈 연산과 $2\left(\left\lceil \frac{n}{3} \right\rceil - 1\right) + 5$ 번의 페어링 연산만 수행하지만, 공격받은 나머지 두 부 회의에 속한 $\frac{2}{3}(n-t)$ 명의 경우는 3개의 부 회의를 동시에 공격하는 경우와 동일하므로,

$$\frac{(n-t)}{3}\left(\left(\left\lceil \frac{n}{3} \right\rceil + 8\right)m + \left(2\left(\left\lceil \frac{n}{3} \right\rceil - 1\right) + 5\right)w\right) +$$

$$\frac{2}{3}(n-t)\left(\sum_{j=0}^{\lceil t/3\rceil+1}\left(\left(\left\lceil \frac{n}{3} \right\rceil - j + 3\right)m + 2\left(\left\lceil \frac{n}{3} \right\rceil - j - 1\right)w\right) + 5m + 5w\right)$$

- 1개의 부 회의만 공격하는 경우: 2개의 부 회의만 공격하는 경우와는 반대로 $\frac{2}{3}(n-t)$ 명은 정상적으로 동작하고 $\frac{(n-t)}{3}$ 만 공격당하므로, 연산의 총합은 아래와 같다.

$$\frac{2}{3}(n-t)\left(\left(\left\lceil \frac{n}{3} \right\rceil + 8\right)m + \left(2\left(\left\lceil \frac{n}{3} \right\rceil - 1\right) + 5\right)w\right) +$$

$$\frac{(n-t)}{3}\left(\sum_{j=0}^{\lceil t/3\rceil+1}\left(\left(\left\lceil \frac{n}{3} \right\rceil - j + 3\right)m + 2\left(\left\lceil \frac{n}{3} \right\rceil - j - 1\right)w\right) + 5m + 5w\right)$$

3개의 부 회의가 모두 공격 당하는 경우가 비용이 가장 크지만 이 경우에도 Yi의 방법에 비해선 비용이 적다는 사실을 알 수 있다.

- 재귀적인 방법 분석: 재귀적인 방법에 대해선 1개의 부 회의만 공격하는 경우에 대해서만 분석했다. t명의 가짜 참여자의 영향력은 결함이 일어날 때마다 1/3로 감소하고, 부 회의 키를 합치는 횟수는 결함이 일어날 때마다 증가하므로 총 연산량은 아래와 같다.

$$\sum_{j=0}^{\lceil \log_3 t\rceil+1}\frac{n-t}{3^j}\left(\left(\left\lceil \frac{n}{3^{j+1}} \right\rceil + 3\right)m + 2\left(\left\lceil \frac{n}{3^{j+1}} \right\rceil - 1\right)w + 5m + 5w\right)$$

다른 방법들과 비교해보면 부 회의 키 합의과정이 로그 단위로 줄어들어서 연산량이 줄어든다는 점을 파악할 수 있다. 하지만 키를 합치는데 필요한 연산량이 $\log_3 t$ 에 비례하여 증가한다는 사실도 알 수 있다.

6. 실험 결과

5장에서 계산된 총 연산량과 네트워크 전송 비용을 함께 고려하여 평균 비용에 대한 실험을 수행하였다. 전체 참여자의 수는 30, 점 간의 곱셈 연산은 5, 페어링은 8, 네트워크 전송은 5로 비용을 임의로 설정했다. 구현을 통해 계산한 비용이 아니기 때문에 실제 값과는 차이가 있겠지만 경향성을 파악할 수는 있다. 그림 1은 Yi의 방법[2]과 제안하는 방법에서 가짜 참여자의 수에 따라 일반 참여자가 부담해야 하는 비용의 평균값을 보여주는 그래프다. Proposed1,2,3은 제안 방법을 공격 받는 부 회의의 수에 따라 나눈 것이며 Recursive1은 재귀적 방법을 뜻한다. 공격자가 없을 때도 제안하는 방법이 Yi의 방법에 비해서 평균 비용이 적으며 특히 공격자의 수가 많으면 그 비용 차가 더욱 크다.

7. 결 론

본 논문은 결함 허용 회의 키 생성에 있어서 합의 비용을 줄이는 새로운 프로토콜을 제안하였다. 제안한 방법은 이전의 결합 포용 키 합의 방법들의 문제점인 다

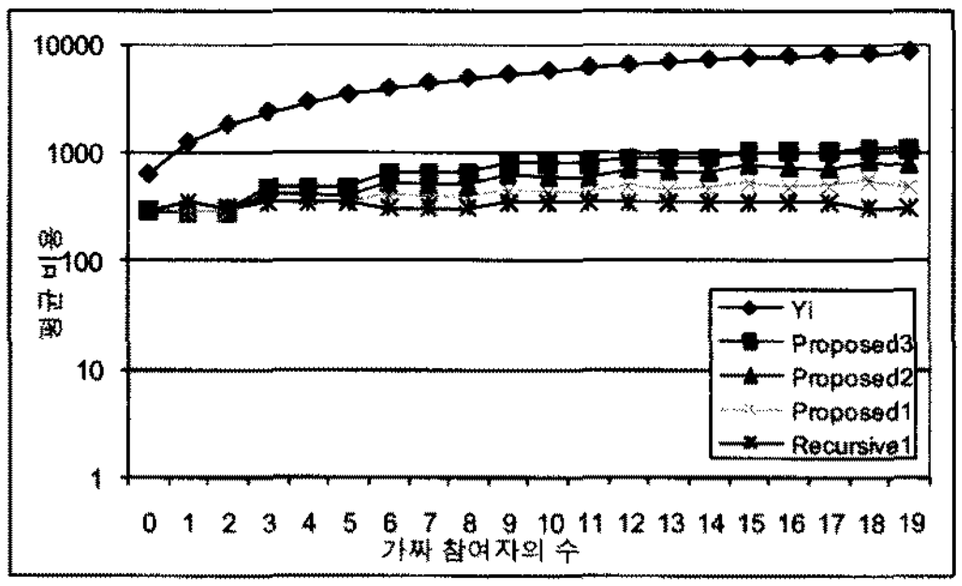

그림 1 Yi의 방법과 제안하는 방법의 평균 비용 비교

수의 가짜 참여자가 있을 경우 성능이 저하되는 현상을 개선시킨 방법이다. 회의를 세 개의 부 회의로 나누고 각각에 대해서 키 합의과정을 수행한 뒤 부 회의 키를 이용해서 다시 하나의 회의 키를 만드는 과정을 통하여 성능이 향상된다. 다시 합치는 과정에서 더 많은 비용이 요구되면 제안하는 방법에 의미가 없기 때문에 Zhang 등이 제안한 일 라운드 삼자 간 키 합의 프로토콜을 이용해서 세 부 회의 키를 합치는 과정을 일 라운드 통신만으로 가능하게 했다[5]. 또한 비용을 더 낮추기 위해서 제안한 방법을 재귀적으로 적용해보았다. 실험을 통한 성능 비교 결과는 제안하는 방법이 효율적이라고 알려진 Yi의 방법[1] 보다 저 비용으로 동작하는 것을 보여준다.

참 고 문 헌

[1] X. Yi, "Identity-Based Fault-Tolerant Conference Key Agreement," IEEE Trans. Dependable and Secure Computing, vol. 1, no. 3, July-Sept. 2004.

[2] W.G. Tzeng, "A Secure Fault-Tolerant Conference Key Agreement Protocol," IEEE Trans. Computers, vol. 51, no. 4, pp. 373-399, Apr. 2002.

[3] S. Tingjun, G. Yuanbo, and M. Jianfeng, "A Fault-Tolerant and Secure Multi-Conference-Key Agreement Protocol," International Conference on Communications, Circuits and Systems, 2004.

[4] Y.M. Tseng, "An Improved Conference-Key Agreement Protocol with Forward Secrecy," Informatica, vol. 16, no. 2, pp. 275-284, 2005.

[5] F. Zhang, S. Liu, and K. Kim, "ID-Based One Round Authenticated Tripartite Key Agreement Protocol with Pairings," Cryptology ePrint Archive, Report 2002/122.

[6] D. Boneh and M. Franklin, "Identity-Based Encryption From The Weil Pairing," Proc. Crypto '01 Conf., pp. 213-229, Aug. 2001.