아이디 기반 삼자 간 키 합의 프로토콜에 기반한 효율적인 결함 포용 회의 키 합의 방법*

이상호° 김종 홍성제
포항공과대학교 컴퓨터공학과
{sangho2, jkim, sjhong}@postech.ac.kr

Efficient Fault-Tolerant Conference-Key Agreement based on ID-based Tripartite Key Agreement Protocol

Sangho Lee°, Jong Kim, and Sung Je Hong
Department of Computer Science and Engineering, POSTECH

1. 서 론

네트워크 회의의 기밀성을 보장하기 위한 회의 키 합의 방법에 대한 많은 연구가 진행되어왔다. 그러나 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 포용 회의 키 합의 프로토콜들이 제안되었다[1,2,3]. 그러나 지금까지 제시된 결함 포용 키 합의 방법은 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.

우리는 공격자의 수가 많아도 효율적인 새로운 회의 키 합의 프로토콜을 제안한다. 제안 방법은 하나의 회의를 세 개의 부 회의로 나누어, 각각의 부 회의에서 회의 키를 생성한 뒤, 한 라운드 삼자 간 키 합의 프로토콜[4]을 이용해서 전체 회의의 공유 키를 만드는 방법이다. 모든 참여자를 세 개의 부 회의에 임의로 할당한다면 공격자가 t명의 거짓 참여자를 이용한다고 하더라도 회의 키 합의 과정은 평균적으로 $\lceil t/3 \rceil + 1$번 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. 추가적으로, 제안 방법을 회귀적으로 적용하는 것을 통해서 $\log_3 t$에 비례하는 비용 감소를 달성할 수 있다. 회의 키 합의 과정의 효율성을 높이기 위해 이 논문에선 지금까지 제안된 방법 중에서 가장 효율적인 Yi의 방법[2]으로 부 회의의 공유 키를 생성한다.

2. 부 회의 키 합의 방법: Yi의 아이디 기반 결함 포용 회의 키 합의 방법[2]

2.1 부 회의 키 합의 프로토콜

1. 모든 참여자가 회의 교량 서버에 접속
2. 회의 교량은 모든 참여자에게 모든 참여자의 ID목록과 회의 번호를 전송
3. 각 참여자는 서브 키를 임의로 생성하고, 그 서브 키를 다른 참여자의 공개 키로 암호화한 값, 서명 값, 서브 키 검증을 위한 값을 회의 교량에 전송
4. 회의 교량은 서명을 확인한 후 서브 키 목록을 각각의 참여자에 전달
5. 각 참여자는 전달받은 서브 키들의 암호를 풀어서 부 회의 키를 생성하고 이를 검증

2.2 결함 포용 기법

1. 참여자는 회의 키를 만드는데 실패한 경우 (서브 키를 다 받지 못했거나, 검증에 실패한 경우) 회의 교량에 결함이 발생했다고 통보
2. 회의 교량은 결함 통보를 너무 자주 발생시키거나, 가짜 결함 통보를 발생시키거나, 가짜 서브 키를 보낸 참여자를 참여자 목록에서 제외
3. 새로운 참여자 목록을 기반으로 회의 키 합의를 재 시작

* 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음 (IITA-2007-C1090-0701-0045)

4. 위의 과정을 결함이 발생하지 않을 때까지 반복

3. 제안하는 회의 키 합의 방법

3.1 회의 키 합의 프로토콜

1. 회의 교량은 모든 참여자를 세 개의 부 회의에 임의로 나누어 배정
2. 각 부 회의는 독립적으로 키 합의 과정(2.1 절)을 수행
3. 회의 교량은 부 회의$_1$의 모든 참여자에 부 회의 키와 인증 값을 요청
4. 회의 교량은 모든 참여자가 전송한 부 회의 키가 같은지 확인하고, 인증 과정을 수행
5. 부 회의 키와 인증 값을 다른 부 회의에 속한 참여자에게 전달
6. 부 회의$_2$, 부 회의$_3$에 대해서도 동시에 3-6번 과정을 수행
7. 모든 참여자는 다른 부회의의 키를 확인한 뒤, 회의 키를 계산

3.2 제안 방법의 이점

Yi의 방법은 결함이 하나라도 발생하면 모든 참여자가 다시 키 합의과정을 수행하는 방식이기 때문에 결함을 처리하는 데 상당한 비용이 필요한 반면, 제안 방법은 이에 필요한 비용을 줄이기 위해서 하나의 회의를 세 개의 부 회의로 나누었다. 이로서 세 개의 부 회의 중에 하나라도 키 합의 과정을 성공적으로 수행했다면 그 부 회의에 속한 참여자들은 더 이상 키 합의 과정을 수행할 필요가 없기 때문에 키 합의를 위한 비용을 줄일 수 있다. 또한 제안 방법을 회귀적으로 적용하면 부 회의 키 합의 과정의 비용을 $\log_3 t + 1$로 줄일 수 있다.

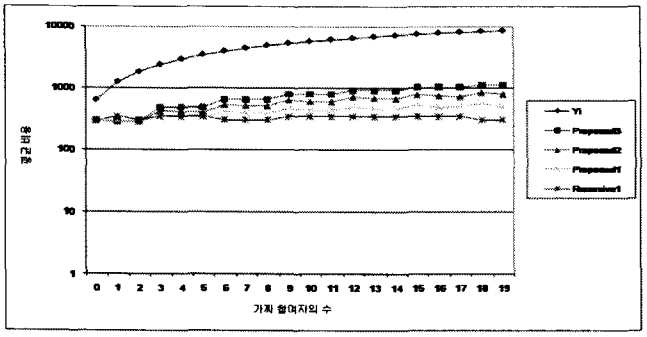

그림 1. Yi의 방법과 제안하는 방법의 평균 비용 비교

4. 결 론

우리는 결함 포용 회의 키 생성에 있어서 합의 비용을 줄이는 새로운 프로토콜을 제안하였다. 제안한 방법은 이전의 결합 포용 키 합의 방법들의 문제점인 다수의 가짜 참여자가 있을 경우 성능이 저하되는 현상을 개선한 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 과정은 Zhang et al.이 제안한 한 라운드 삼자 간 키 합의 프로토콜을 이용해서 비용을 최소화시켰다[4]. 또한 비용을 더 낮추기 위해서 제안한 방법을 회귀적으로 적용해보았다. 우리는 실험을 통해 제안하는 방법이 효율적이라고 알려진 Yi의 방법[2]에 비해 평균 비용이 더 적다는 것을 확인했다.

참고문헌

1. W.G. Tzeng, "A Secure Fault-Tolerant Conference Key Agreement Protocol", IEEE Trans. Computers, vol. 51, no. 4, pp. 373-399, Apr. 2002.
2. X. Yi, "Identity-Based Fault-Tolerant Conference Key Agreement", IEEE Trans. Dependable and Secure Computing, vol. 1, no. 3, July-Sept. 2004.
3. Y.M. Tseng, "An Improved Conference-Key Agreement Protocol with Forward Secrecy", Informatica, vol. 16, no. 2, pp. 275-284, 2005.
4. F. Zhang, S. Liu, and K. Kim, "ID-Based One Round Authenticated Tripartite Key Agreement Protocol with Pairings", Cryptology ePrint Archive, Report 2002/122.