One-Round 무인증서 기반 인증 및 그룹키 합의 프로토콜+

임혜민*, 이임영**
*순천향대학교 소프트웨어융합학과
**순천향대학교 컴퓨터소프트웨어공학과
renchn1127@sch.ac.kr, imylee@sch.ac.kr

One-Round Certificateless Authentication and Group Key Agreement Protocol

Huimin Ren*, Im-Yeong Lee**
*Dept. of Software Convergence, Soonchunhyang University
**Dept. of Computer Software Engineering, Soonchunhyang University

요 약

인증 및 그룹키 합의 프로토콜은 통신하고자 하는 여러 구성원들의 그룹키를 합의하여 안전한 그룹 통신을 제공할 수 있다. 현재 안전하고 효율적인 인증 및 그룹키 합의 프로토콜을 위한 연구가 활발히 진행 중이다. 기존의 공개키 인프라 기반 인증 및 그룹키 합의 방식에는 인증서와 키의 관리 문제가 나타나며 신원 기반 인증 및 그룹키 합의 방식에는 키 에스크로 문제가 나타난다. 본 논문은 이러한 문제를 해결 할 수 있는 무인증서 기반 인증 및 그룹키 합의 방식을 제안한다. 또한, 본 논문에서는 기존에 무인증서 암호시스템에 발생할 수 있는 공개키 대체로 인한 위장 공격을 방지할 수 있는 방법을 설계한다. 제안하는 방식은 효율성을 제공하기 위해서 구성원 수가 증가하더라도 통신 Round 수가 증가하지 않는 특징을 갖는다.

1. 서론

그룹키 합의 프로토콜은 안전한 그룹 통신을 위한 방법이다. 이러한 프로토콜은 한 그룹의 구성원들이 신뢰할 수 없는 통신채널을 통해 공유할 수 있는 일회용 그룹키를 공유하며, 이 키를 통해서 개방된 네트워크 환경에서 그룹 통신 데이터의 안전을 보장할 수 있다. 최근 인터넷의 발달로 파일 공유 시스템, 화상회의 등의 서비스 사용이 증가하고 있다. 이러한 환경을 지원하기 위해 안전한 그룹 통신을 위한 인증 및 그룹키 합의(Authentication and Group Key Agreement, AGAK)프로토콜이 요구되고 있다.

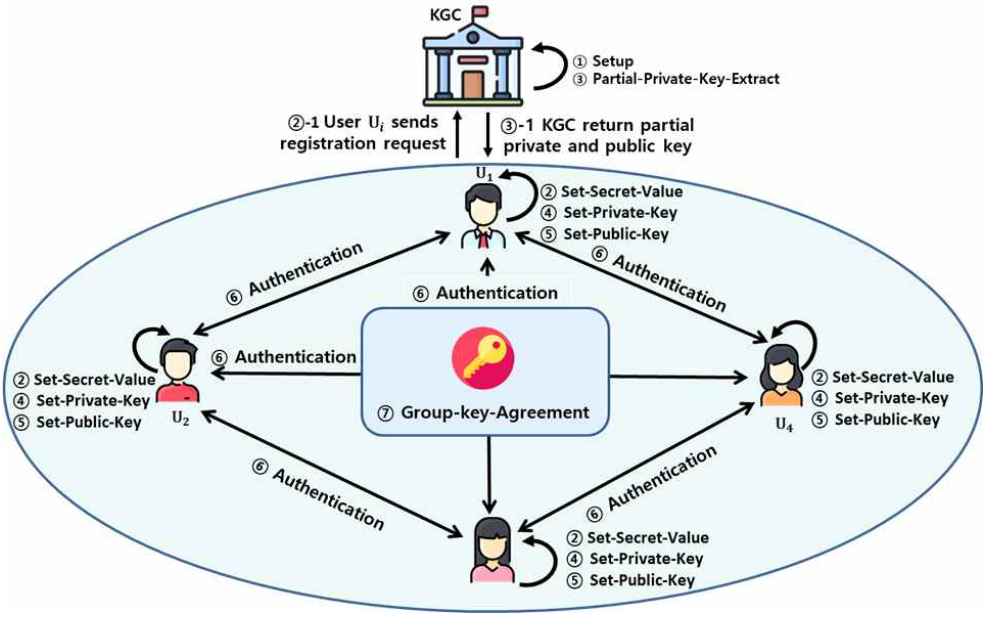
공개키 암호시스템에 따라 AGKA는 기존의 공개키 인프라 기반 인증 및 그룹키 합의 방식(Public Key Infrastructure Authentication and Group Key Agreement, PKI-AGKA), 신원기반 인증 및 그룹키 합의 방식(Identity-based Authentication and Group Key Agreement, ID-AGKA), 또는 무인증서 기반 인증 및 그룹키 합의 방식(Certificateless Authentication and Group Key Agreement, CL-AGKA)으로 나눌 수 있다[1, 2].

기존의 PKI-AGKA 방식은 인증서와 키의 관리 문제가 존재하며, ID-AGKA 방식에 키 에스크로 문제가 존재한다. CL-AGKA 방식은 이러한 문제들을 해결할 수 있기 때문에 현재 CL-AGKA 프로토콜에 대해서 활발히 연구가 진행 중이다.

하지만 CL-AGKA에서는 구성원의 공개키 인증서를 사용하지 않기 때문에 구성원의 신분 및 공개키에 대한 인증할 수 없다. 따라서 현재 CL-AGKA에서 공격자가 구성원의 공개키를 대체한 위장공격을 방지할 수 있는 연구가 많이 진행 중이다[3].

그룹키 합의의 안전성과 함께 효율성이 중요하게 요구된다. 그룹키 합의 과정에서 모든 구성원은 동시에 온라인 상태를 유지해야 하며 모든 구성원은 키 합의 알고리즘을 완료하기 위해 서로 통신이 끝날 때까지 기다려야 한다. 합의 과정에서 구성원 간의 통신 Round 회수가 효율성에 직접 영향을 미치

+ 이 논문은 과학기술정보통신부 및 정보통신기획평가원의 글로벌핵심인재양성지원사업(2021-0-01516)과 2019년도 정부(교육부)의 한국연구재단 기초연구사업(No. NRF-2019R1A2C1085718)의 연구결과로 수행되었음



[그림 1] 전체 시나리오

기 때문에 구성원 간 통신 횟수는 구성원의 온라인 시간을 계량화할 수 있는 중요한 지표이다[4].

고정된 횟수의 Round 그룹키 합의는 하나의 통신 Round수가 고정되어 그룹 구성원의 수와 무관한 횟수의 통신을 수행하며, 가변 횟수의 Round 그룹키 합의는 통신 횟수가 선형적으로 또는 대수로 늘어날 수 있다. 즉, 구성원 수가 많을수록 통신 Round수가 많아진다.

그룹키 합의는 보안성을 확보함과 동시에 구성원의 온라인 통신대기 시간을 현저히 낮출 수 있기 때문에 높은 활용도를 가지며, 정보보안 분야의 연구 이슈가 되고 있다. 통신 Round의 수는 구성원의 온라인 시간을 계량화하는 중요한 지표, 즉 구성원이 그룹키 합의 알고리즘을 수행할 때 한 합의 과정에서 다른 구성원과 메시지 교환 횟수를 의미한다.

따라서 One-Round를 가지는 CL-AGKA 프로토콜은 그룹키를 합의하기 전에 통신횟수 및 구성원 대기 시간을 대폭 줄여 통신 효율을 높일 수 있다.

본 논문에서 KGC의 공개키를 이용하여 구성원의 공개키 검증 기능을 제공하여 공개키 대체 공격을 방지할 수 있다. 또한, 그룹키를 합의하기 전에 서명을 통해 구성원의 신분을 인증하여 메시지의 변조 및 악의적인 공격자의 위장공격을 방지하는 기능을 설계한다. 통신횟수 및 구성원 대기 시간을 대폭 줄여 통신 효율을 높이기 위해 One-Round 통신 횟수를 가지는 CL-AGKA 프로토콜을 제안한다.

2. 제안방식

본 장에서는 기존에 있는 CL-AGKA 프로토콜에서 발생 가능한 위장공격을 방지할 수 있는 안전하고 효율적인 One-Round 통신 횟수를 가지는 CL-AGKA 프로토콜을 제안한다.

2.1 전체 시나리오

본 제안방식은 [그림 1]과 같이 Setup, Set-Secret-Value, Partial-Private-Key-Extract, Set-Private-Key, Set-Public-Key, Authentication, Group-Key-Agreement 총 7단계로 구성된다.

2.2 세부 시나리오

본 제안방식의 세부 시나리오는 다음과 같다.

① Setup: KGC는 보안 매개변수 입력으로 공개 파라미터와 마스터 비밀키를 생성한다.

② Set-Secret-Value: 구성원은 공개 파라미터와 구성원 식별 정보를 입력하여 자신의 부분 비밀키를 생성하고 부분 비밀키를 이용하여 부분 공개키를 생성한다.

③ Partial-Private-Key-Extract: KGC는 공개 파라미터, 마스터 비밀키 그리고 구성원의 개인 식별 정보를 이용하여 구성원의 부분 비밀키와 부분 공개키를 생성하여 구성원에게 전달한다.

④ Set-Private-Key: 구성원은 자신의 부분 비밀키 및 KGC가 생성한 부분 비밀키를 입력으로 비밀키를 설정한다.

⑤ Set-Public-Key: 구성원은 자신의 부분 공개키, 검증용 공개키, KGC가 생성한 부분 공개키를 입력으로 공개키를 설정한다.

⑥ Authentication: 구성원들은 자신의 식별자, 공개키 그리고 임시키를 이용하여 메시지 및 서명을 생성하고 다른 구성원한테 보내준다. 다른 구성원한테 받은 서명을 통해서 신분을 인증할 수 있다. 또한, 구성원은 KGC의 공개키를 이용하여 다른 구성원의 검증용 공개키를 검증할 수 있다.

⑦ Group-Key-Agreement: 구성원들은 자신의 식별자, 공개키, 임시키를 교환한 후에 서로의 신분인증을 성공하면 구성원은 자신의 비밀 정보 및 다른 구성원한테 받은 값을 이용하여 그룹키를 생성한다. 프로토콜이 성공적으로 수행되면 구성원이 생성한 그룹키는 동일한 값을 가지게 된다.

3. 제안방식 분석

본 장에서는 One-Round CL-AGKA의 보안 안전성을 분석한다.

- 상호 인증(Mutual Authentication, MA): 본 제안방식은 그룹에 통신의 쌍방이 서명을 통해서 다른 모든 구성원의 신원을 확인할 수 있으며 상호인증을 제공한다.
- 전방향 안전성(Forward Secrecy, FS): 제안하는 CL-AGKA 프로토콜에서 하나 또는 둘 이상의 구성원들의 장기적인 비밀키가 노출되더라도 그룹키를 생성할 때마다 구성원들은 새로운 임시키를 선택하여 그룹키를 생성한다. 공격자는 임시키를 알 수 없기 때문에 구성원의 장기적인 비밀키 노출에도 이전에 합의한 그룹키들에 대한 안전성이 보장된다.
- 무 키 제어(No Key Control, NKC): 구성원은 키를 합의할 때 모든 구성원의 정보와 임시키 등이 모두 모여야 결정되며 구성원은 다른 구성원 의 임시키 및 비밀키를 알 수 없기 때문에 그룹에 누구도 그룹키를 정확히 예측할 수 없다.
- 효율성(Efficiency): 효율성을 보장하기 위해 본 제안방식은 페이링 연산을 대체하여 타원곡선을 통해 One-Round CL_AGKA 방식을 구현한다.

4. 결론

본 제안방식은 위장공격을 방지할 수 있는 효율적이고 안전한 One-Round의 통신횟수를 가지는 CL-AGKA 프로토콜을 제안한다.

본 제안방식은 PKI-AGKA 방식에 발생하는 인증서 관리 문제, 또는 ID-AGKA 방식에 발생할 수 있는 키 에스크로 문제를 해결할 수 있다.

그리고 ECC 암호기반에 KGC의 공개키를 이용해 다른 구성원들 사이에 공개키 검증하여 공격자가 구성원의 공개키 대체할 수 없다. 따라서 공격자가 공개키 대체를 이용해 위장공격을 할 수 없다. 또한, 서명을 이용하여 상호인증 제공한다. 구성원의 비밀키, 임시키 등을 바인딩 하여 서명이 위조 불가능하며 위장공격을 방지할 수 있다.

효율성 보장하기 위해 본 제안방식은 페이링 연산 대체하여 타원곡선 연산을 이용하여 프로토콜을 구현한다. 또한, 통신 Round 수는 1번이기 때문에 그룹키를 합의하기전에 통신횟수 및 구성원 대기 시간을 대폭 줄여 통신 효율을 높일 수 있다.

따라서 본 제안방식은 기존 CL-AGKA 방식보다 더욱 안정적이고 효율적이다[5].

참고문헌

[1] Bresson E, “Provably authenticated group Diffie-Hellman key exchange,” in Proc. CCS, Philadelphia, Pennsylvania, USA, Nov. 2001.

[2] Shamir A. "Identity-based cryptosystems and signature schemes." Workshop on the theory and application of cryptographic techniques. Springer, Berlin, Heidelberg, 1984.

[3] Al-Riyami S. “Certificateless public key cryptography,” in Proc. ASIACRYPT 2003, Taibei Taiwan, Nov. 2003.

[4] Teng, J "A provable authenticated certificateless group key agreement with constant rounds." Journal of Communications and Networks 14.1, 2001.

[5] Kumar A, "A pairing free certificateless group key agreement protocol with constant round." Advanced Computing, Networking and Informatics-Volume 2. Springer, Cham, 2014.