멀티로봇 시스템에서 로봇 그룹 간 협력 임무 수행을 위한 인증 모델 연구

이고은[1], 홍다희[1], 서승현[2]
[1]한양대학교 ERICA 지능정보양자공학전공 학부생
[3]한양대학교 ERICA 전자공학부 교수

dbsal0320@hanyang.ac.kr, dahi3553@hanyang.ac.kr, seosh77@hanyang.ac.kr

Study of an Authentication Model for Inter-Group Cooperative Missions in Multi-Robot Systems

Go-Eun Lee[1], Da-Hee Hong[1], Seung-Hyun Seo[2]
[1]Dept. of intelligent information quantum engineering, Hanyang University ERICA
[2]Dept. of Electronic Engineering, Hanyang University ERICA

요 약

본 논문에서는 멀티로봇 시스템의 신뢰 기반 통신과 인증 문제를 해결하기 위해, 신뢰할 수 없는 멀티로봇 그룹이 협업을 수행하는 시나리오를 가정하고, 각 로봇의 신원 인증 및 작업 이력을 블록체인에 안전하게 저장하는 ROS 2 환경의 블록체인 기반 로봇 인증 시스템을 제안한다. 그룹 내 및 그룹 간 인증을 통해 각 로봇은 신뢰성 있게 상호작용하며, 작업 이력은 변경 불가능한 방식으로 블록체인에 기록된다. 실험 결과 시스템의 신뢰성과 투명성이 입증되었으며, 향후 양자 내성 암호 기반 보안 통신 체계가 무인 자동화 공정에 적용될 수 있을 것으로 기대된다.

1. 서론

최근 건설, 물류, 재난 대응 등 다양한 산업 분야에서 멀티로봇 간 협력을 통한 작업 수행 시스템이 확산되고 있다. 특히, 재난 현장에서 골든타임 내 효율적인 구조 활동을 위해 서로 다른 기관 간 협력이 활발히 이뤄지고 있다[1]. 이처럼 복잡한 산업 환경에서는 기관 간 로봇 협력이 필수적이다.

하지만 여러 기관 간 협업 구조에서는 로봇 그룹 간 신뢰가 보장되지 않기 때문에, 로봇 간 신원 인증 및 작업 이력 검증 체계가 필요하다. 특히 일부 기관이 정보를 고의로 은폐하거나 조작할 경우 전체 임무의 신뢰성이 훼손되며, 이는 임무 지연, 인명 피해, 책임 분쟁으로 이어질 수 있다. 따라서 분산된 협력 환경에서도 이러한 위협에 효과적으로 대응할 수 있는 인증 체계의 구축이 요구된다.

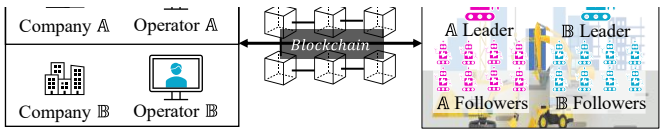
비잔틴 로봇 대응을 위한 인증 메커니즘을 제안한 연구들[2,3]이 존재하지만, 단일 기관 내 협력을 전제로 하며, 기관 간 협력 시 인증 문제가 고려되지 않았다. 또한 ROS 2(Robot Operating System 2)는 기본적인 접근 제어 기능만 제공하며, 단일 조직 내 사용을 가정하기에 다기관 협업 환경에 적합하지 않다.

본 논문은 서로 다른 기관의 멀티로봇이 독립된 운영자(operator)에 의해 관리되는 시나리오를 가정하고, ROS 2 기반 멀티로봇 환경에 블록체인을 결합한 인증 프로토콜을 제안한다. 블록체인의 분산성, 데이터 불변성, 기록 추적 기능은 신원 인증을 지원하며, ROS 2의 분산형 통신 구조와 상호보완적으로 결합되어 시스템의 보안성과 신뢰성을 강화한다.

2. 블록체인 기반 로봇 그룹 간 상호 인증 모델

2.1 협력 임무를 수행하는 로봇 집단 시나리오

본 논문은 각각 다른 기관이 멀티로봇을 운영하는 건설 현장 협업 시나리오를 가정한다. 각 기관의 멀티로봇은 서로 신뢰하지 않으며, 각 멀티로봇 그룹 A와 B는 서로 다른 작업을 수행한다. 각 그룹은 리더 로봇 1대와 여러 대의 팔로워 로봇, 운영자로 구성된다. 제안 시나리오의 아키텍처는 그림 1과 같다.



(그림 1) overall model diagram for multi-robot system

- **리더 로봇**: 트랜잭션 생성 및 스마트 컨트랙트에서 작업 명령을 수신하여 팔로워 로봇들에게 이를 분배한다. 또한, 블록체인에 직접 접근 가능하여 블록체인에 등록된 로봇의 신원과 작업 이력을 추적하고, 팔로워 로봇의 작업 결과를 블록체인에 기록한다.
- **팔로워 로봇**: 리더 로봇을 통해 작업 명령을 수신하고, 작업 결과를 리더 로봇에게 보고한다. 팔로워 로봇은 블록체인에 직접 접근할 수 없고, 리더를 통해서만 자신의 정보를 등록할 수 있다.
- **운영자 (Operator)**: 스마트 컨트랙트를 설계하고,

로봇 간 작업 요청과 인증, 작업 이력 관리를 담당한다. 인증 정보를 블록체인에 등록하고, 로봇 그룹 간 협업을 스마트 컨트랙트에 반영한다. 또한 인증과 작업 로그를 주기적으로 모니터링한다.

2.2 인증 과정 및 절차

본 장에서는 서로 신뢰하지 않는 A 기관과 B 기관이 협업 업무 수행을 위한 로봇 상호 인증 프로토콜을 제안한다. 이때, 로봇 간 통신 메시지와 세션키는 블록체인에 모두 기록된다.

① 협업 요청

- **작업 제안 요청**: B 운영자가 요청 트랜잭션 생성
- **작업 제안 응답**: A 운영자는 응답 트랜잭션을 생성하고 작업 지시를 위한 로그 기록
- **작업 지시**: 로그를 확인한 A 리더 로봇은 A 팔로워 로봇에게 작업 지시

② 인증 요청

- **인증 요청 메시지 전송**: A 팔로워 로봇은 B 리더 로봇의 공개키를 수신하고 인증 요청 메시지를 생성해 B 리더 로봇에게 전송

$$Sig_A = Sign_{sk_{A\ follower}}(serial_{A\ follower} \parallel Num1 \parallel TS1)$$

$$Req = Enc_{pk_{B\ leader}}(serial_{A\ follower} \parallel Num1 \parallel TS1 \parallel Sig_A)$$

③ 인증 응답

- ***Req* 메시지 복호화 및 타임스탬프 검증**
- **서명 검증**: 블록체인에 미리 등록된 A 팔로워 로봇의 공개키로 서명 검증
- **검증 결과 반환**: 성공 시 자신의 인증 정보로 *Req*와 동일한 메시지를 생성해 암호화된 메시지 *Ans*를 A 팔로워 로봇에게 전송

④ 세션키 생성

- ***Ans* 메시지 복호화 및 타임스탬프 검증**
- **검증**: 검증에 성공할 경우 서로의 세션키 생성

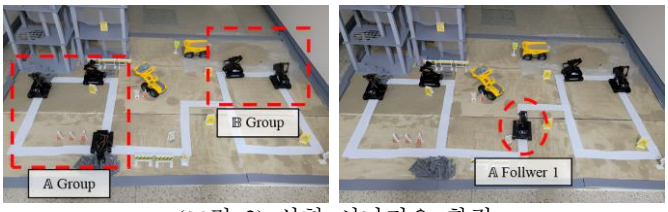
$$key_{ss} = ((pk * sk) \parallel Num1 \parallel Num2)$$

⑤ 임무 수행

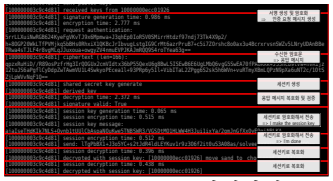
- **세션키 생성 성공 메시지**: A 팔로워 로봇이 B 리더 로봇에 세션키 생성 성공 메시지를 암호화해 전송
- **작업 할당 메시지 전송:** B 리더 로봇은 작업 할당 메시지를 암호화해 전송
- **로봇 간 협업 수행:** A 팔로워 로봇은 B 리더 로봇이 할당한 협업 임무 수행

3. 시나리오 구현 및 평가

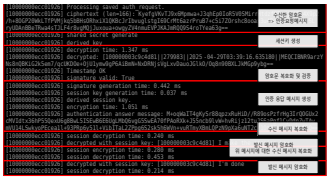
본 논문에서는 ROS 2 기반 환경에서 Ethereum 네트워크를 통해 제안한 인증 프로토콜을 구현하였다. 제안 인증 프로토콜의 성능 평가를 위해 ROS 2 기반의 분산 노드 환경에서 실험을 수행하였으며, 실험은 ECDSA 기반 인증 메시지 서명 생성 및 검증, ECDH 기반 세션키 생성, AES-GCM 방식에 의한 메시지 암호화 및 복호화 단계를 포함하였다.



(그림 2) 실험 시나리오 환경



(a) 𝔸 Follower 1 실행화면



(b) 𝔹 Leader 실행화면

인증요청메시지 서명 생성	0.0986
인증요청메시지 암호화 시간	2.777
인증응답메시지 복호화	2.372
인증응답메시지 서명 검증	0.663
세션키 생성 시간	0.065
세션키로 암호화	0.515, 0.512
세션키로 복호화	0.396, 0.438

(c) 𝔸 Follower 1 실행시간

인증요청메시지 복호화	1.347
인증응답메시지 서명 생성	0.442
인증응답메시지 암호화	1.051
세션키 생성 시간	0.037
세션키로 복호화	0.240, 0.453
세션키로 암호화	0.280, 0.214

(d) 𝔹 Leader 실행시간

(그림 3) 협력 임무 실행화면 및 실행시간

그림 2 와 3 은 각각 시나리오 구현을 위해 구축한 실험 환경 및 로봇 간 실시간 인증 과정의 주요 단계를 보여준다. 그림 3(a)에서는 A 팔로워 로봇이 인증 요청 메시지를 생성하여 전송하는 과정을, (b)에서는 B 리더 로봇이 해당 메시지를 검증한 후 응답 메시지를 회신하는 과정을 보인다. 실험 결과, 각 연산에 소요되는 시간 측정 시, 서명 생성, 세션키 생성, 세션키 기반 암·복호화 등 모든 주요 연산이 밀리초(ms) 이하의 짧은 시간 내에 완료됨을 확인하였다. 이는 일반적으로 실시간 처리가 요구되는 협업 로봇 시스템의 지연 한계(수 밀리초 이내)를 만족하는 수준으로, 제안한 프로토콜이 실시간성이 요구되는 환경에서도 충분히 적용 가능함을 입증한다. 또한, 경량화된 암호 연산을 기반으로 통신 효율성과 시스템 안정성을 동시에 확보할 수 있음을 확인하였다.

[Acknowledge]

이 논문은 2024 년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구 결과임 (RS-2024-00341722, 지능형 서비스 로봇의 사이버 레질리언스 확보를 위한 보안기술 개발)

참고문헌

[1] 장길수, “드론 기반 다중관제시스템 구축 협업사업 본격 착수,”로봇신문, 2020.

[2] Barrion, Marck Herzon, et al. "Advancing Robotic Swarms with Blockchain Technology: A Dynamic Two-Factor Authentication Consensus Framework." (2024).

[3] Alsamhi et al. "Blockchain-empowered multi-robot collaboration to fight COVID-19 and future pandemics." Ieee Access 9 (2020): 44173-44197.