

차량 간 양자 키 분배(V2V-QKD) 기술 동향 및 자율주행 보안 통신 적용 가능성 분석

황재성, 김성민, 신경철, 이윤아, 전현채
인천대학교

jambory1736@inu.ac.kr

Recent trends and potential of V2V-QKD for secure autonomous vehicles

Jae Seong Hwang, Sung Min Kim, Gyeong-cheol Shin, Lee Yuna, and Hyunchae Chun
Incheon National University

요약

본 연구는 자율주행 차량 간 통신 보안을 위한 양자 키 분배(QKD)의 적용 가능성과 주요 방식별 특성을 분석하였다. DV, CV, MDI-QKD의 비교와 함께 국내외 연구 동향을 정리하였으며, 차량 환경에서의 구현 과제를 제시하였다.

I. 서론

자율주행 차량 간 (Vehicle to Vehicles; V2V) 통신은 실시간 주행 제어와 충돌방지 등을 위해 높은 수준의 보안을 요구한다. 그러나 기존 암호화 기술은 양자컴퓨터의 발전으로 장기적인 보안성에 한계가 있다. 이에 따라 양자 키 분배 (Quantum Key Distribution; QKD)는 도청 탐지 및 무조건적 보안을 제공하는 미래 보안 기술로 주목받고 있다 [1]. 특히 차량 간 통신에 QKD를 적용하면, 이동 중에도 안전하게 키를 분배하고 인증할 수 있어 자율주행 보안성을 근본적으로 강화할 수 있다. 본 논문에서는 V2V-QKD 기술의 적용 가능성과 주요 QKD 방식들의 차량 환경 적합성을 비교하고, 국내외 연구 동향과 향후 과제를 고찰한다. 이를 통해 V2V 통신에 필요한 암호 키를 안전하게 분배하고, 도청 발생 여부를 실시간으로 감지함으로써 자율주행차 네트워크의 보안을 근본적으로 강화할 수 있다. 본 연구에서는 QKD의 V2V 통신 적용 가능성과 관련 기술 동향을 살펴보고, 차량 환경에 적합한 QKD 방식에 대한 기술적 평가와 국내외 연구·개발 사례, 자율주행 기술과의 통합을 위한 과제 및 향후 방향을 요약한다.

II. 본론

V2V 통신은 위치, 속도 등 민감한 정보를 교환하므로 도청, 위변조 등에 취약하다. QKD는 단일 광자 기반의 키 분배로 도청을 원천적으로 탐지할 수 있어 차량 간 안전한 통신 기반기술로 유망하다. DV-QKD (Discrete

Variable-QKD)는 단일 광자 검출 기반으로 보안성은 높으나 광학 정렬과 장비가 복잡하다. CV-QKD (Continuous Variable-QKD)는 기존 광통신 부품과 호환되어 소형화가 용이하고 차량용 모듈화에 유리하나, 채널 잡음에 민감하다. MDI-QKD (Measurement Device Independent-QKD)는 중계기의 신뢰가 불필요하여 네트워크 확장성에 강점을 가지지만, 시스템 동기화 요구가 높다. 미국에서는 실제 주행 중 차량 간 QKD 실험이 수행되었으며, 영국은 도로변 인프라-차량 간 QKD 실증에 성공하였다 [2]. 국내에서는 제주 자율주행 시범지구에 QKD 기반 C-ITS (Cooperative-Intelligent Transport Systems) 인프라가 구축되었고, 민간에서는 KT가 차량용 무선 QKD 기술을 시범 적용 중이다.

III. 결론

V2V-QKD는 자율주행 보안을 위한 핵심 기술로서 가능성을 보이고 있으나, 장비 소형화, 이동 환경 채널 안정화, 키 관리 등 과제가 남아 있다. 향후에는 포스트 양자 암호화 (Post-Quantum Cryptography; PQC)와의 하이브리드 통합, 위성·드론 기반 광역 QKD, 차량용 양자보안 모듈의 표준화가 필요하다. QKD는 자율주행 생태계 전반의 신뢰성 확보에 중추적 역할을 할 것으로 기대된다.

또한, V2V-QKD 기술은 위성통신 기술과의 융합을 통해 광역 커버리지를 제공하는 방향으로 확장될 수 있다. 특히 저궤도 위성(LEO) 간의 양자 중계는 고속 이동체 간 LOS 환경을 유사하게 공유하므로, 차량 네트워크의 키 분배를 위한 백홀 인프라로 활용될 수 있다. 위성

기반 QKD는 자율주행차의 전국적 네트워크 확장을 위한 고신뢰 키 분배 인프라를 제공할 수 있으며, 향후 차량-지상국-RSU(Road side unit)-위성 간 다자 연동 구조를 기반으로 한 다계층 QKD 네트워크 설계와, 위성 링크 특성에 최적화된 광트랜시버 모듈 및 고정밀 PAT(Pointing, acquisition and tracking) 시스템 개발이 병행되어야 하며, 이를 통해 자율주행 인프라의 양자보안 신뢰성을 확장할 수 있을 것이다.

ACKNOWLEDGMENT

This research was supported by the MSIT, Korea, under the ITRC support program (IITP-2025-RS-2023-00259061) supervised by the IITP. Also, this work was supported by the National Research Foundation of Korea (NRF) grant funded by MSIT (No.RS-2023-00253346).

참 고 문 헌

- [1] A. Conrad et al., "Vehicle-to-Vehicle QKD," CLEO 2024.
- [2] D. Fowler et al., "A Practical Implementation of Quantum-Derived Keys for Secure Vehicle-to-Infrastructure Communications," Vehicles, 2023.