# 미래 모빌리티 환경에서의 양자 네트워크 기반 보안 통신 기술 동향

김진욱
한국자동차연구원
jwkim3@katech.re.kr

# Trends in Quantum Network - Based Secure Communication Technologies for Future Mobility Environments

Kim Jin Wook
Korea Automotive Technology Institute

요 약

미래 모빌리티(Future Mobility)는 자율주행차, 커넥티드카, 도심항공교통(UAM), 그리고 지능형 교통 인프라가 초연결되는 지능형 이동체 환경으로 진화하고 있다. 이러한 환경에서는 차량 간(V2V), 차량 - 인프라(V2I), 차량 - 클라우드(V2C) 통신을 통해 대용량 센서 데이터와 제어 메시지가 실시간으로 교환되며, 통신 지연이나 보안 침해는 물리적 사고로 직결될 수 있다. 기존 공개키 기반 암호(PKC)는 양자컴퓨터의 등장으로 인해 장기적인 보안 신뢰성을 보장하기 어렵다는 한계가 제기되고 있으며, 이에 따라 양자역학적 원리에 기반한 양자 키 분배(QKD) 및 양자 네트워크 기술이 차세대 보안 인프라로 주목받고 있다. 본 논문에서는 미래 모빌리티 환경에서 요구되는 보안·통신 특성을 분석하고, 양자 네트워크의 핵심 구성 기술(QKD, QKMS, 양자 라우팅)을 중심으로 기술 동향을 정리한다. 또한 V2X 통신, OTA 업데이트, 원격진단, 군집주행 등 주요 미래 모빌리티 서비스에 대한 양자 네트워크 기반 보안 적용 시나리오를 분석하고, 향후 연구 방향을 제시한다.

## Ⅰ. 서 론

미래 모빌리티 환경은 SAE Level 4~5 자율주행차를 중심으로 커넥티드 서비스, 도심형 C-ITS, 그리고 클라우드 기반 지능형 교통 시스템이 유기적으로 결합되는 형태로 발전하고 있다. 차량은 더 이상 독립적인 이동 수단이 아니라, 도로 인프라(RSU), 엣지 서버, 클라우드와 지속적으로 연결된 네트워크 노드로 동작한다. 이 과정에서 BSM, CAM, SPaT, MAP과 같은 핵심 교통 메시지와 대용량 센서 데이터가 실시간으로 교환된다.

이러한 통신 구조에서 메시지의 위·변조, 지연 공격, 인증 실패는 곧바로 주행 안전성 저하 및 대형 사고로 이어질 수 있다. 그러나 현재 널리 사용되고 있는 공개키 기반 암호(PKC)는 양자컴퓨터의 연산 능력으로 인해 장기적으로 무력화될 가능성이 제기되고 있으며, 차량 생애주기 전반에 걸친 보안 신뢰성을 보장하기 어렵다.

이에 따라 도청 자체가 탐지되는 특성을 갖는 양자 키 분배(QKD)와 이동체 환경에 최적화된 양자 네트워크 기술이 차세대 미래 모빌리티 보안 통신 기술로 주목받고 있다. 본 논문은 이러한 배경에서 미래 모빌리티 환경에 적용 가능한 양자 네트워크 기반 보안 통신 기술의 동향을 체계적으로 분석한다.


그림 1. 양자 네트워크의 3대 핵심 기술

## Ⅱ. Future Mobility와 양자 네트워크 적용 구조

미래 모빌리티 통신 구조는 차량, RSU, 엣지 서버, 클라우드가 계층적으로 연결된 복합 네트워크 형태를 가진다. 차량 제어 및 안전과 직결되는 메시지는 SAE J2735(BSM, MAP, SPaT 등)와 ETSI ITS(CAM, DENM 등) 표준을 기반으로 하며, 차량 - 클라우드 구간에서는 MQTT, AMQP와 같은 경량 메시지 프로토콜이 활용된다. 이러한 이종 메시지와 프로토콜이 혼재된 환경에서는 통합적이고 고신뢰의 보안 키 관리 체계가 필수적이다.

양자 네트워크는 기존 광통신 인프라와 병행하여 적용될 수 있으며, QKD를 통해 차량 - 인프라 - 클라우드 간 End-to-End 보안 키 분배를 제공한다. QKMS(Quantum Key Management System)는 다수의 이동 노드 환경에서 키 생성, 분배, 동기화, 폐기를 자동화하여 대규모 모빌리티 환경에서도 안정적인 보안 운영을 가능하게 한다.

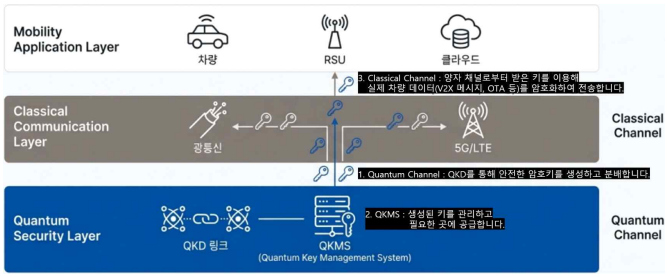


그림 2. 기존 통신망과 양자 네트워크의 통합 적용 구조

또한 지능형 양자 라우팅 기술은 이동성으로 인해 빈번히 변화하는 네트

워크 토폴로지를 고려하여 동적 경로 재구성과 고가용성을 지원한다. 이는 군집주행, 원격제어, 협력인지(Cooperative Perception)와 같이 초저지연·고신뢰 통신이 요구되는 서비스에서 핵심적인 역할을 수행할 수 있다.

## Ⅲ. 미래 모빌리티 서비스에서의 활용 시나리오

양자 네트워크 기반 보안 통신은 다양한 미래 모빌리티 서비스에 적용 가능하다. 자율주행차와 도로 인프라 간 V2X 통신에서는 QKD 기반 세션 키를 활용하여 SPaT, MAP, BSM 메시지의 무결성과 신뢰성을 강화할 수 있다. 이를 통해 신호 위변조나 재생 공격으로 인한 사고 위험을 근본적으로 줄일 수 있다.

차량-클라우드 간 OTA 업데이트에서는 양자 키 기반 인증과 무결성 검증을 적용함으로써 악성 코드 삽입 및 업데이트 변조를 방지할 수 있다. 또한 실시간 원격진단 및 대용량 센서 데이터 전송 환경에서는 QKD 기반 세션 키 자동 갱신을 통해 지속적인 보안 수준을 유지할 수 있다.

군집주행 환경에서는 차량 간 제어 및 동기화 메시지가 실시간으로 교환되기 때문에 초저지연·고무결성 보안이 필수적이다. 양자 네트워크 기반 보안 채널은 이러한 요구사항을 충족하며, 차량 결제 및 신원 관리 서비스와 결합될 경우 모빌리티 생태계 전반의 보안 신뢰도를 크게 향상시킬 수 있다.

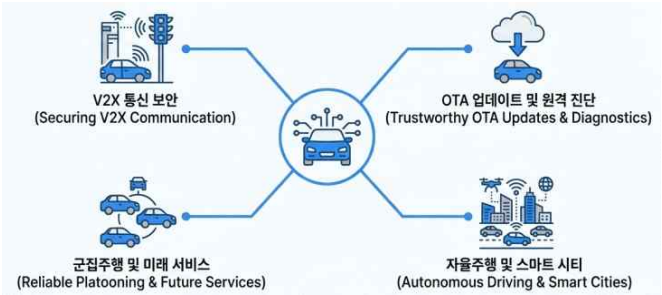


그림 3. 양자 네트워크 기반 보안 적용 시나리오

## Ⅳ. 결 론

본 논문에서는 미래 모빌리티 환경에서 요구되는 보안 통신 특성을 분석하고, 이를 충족하기 위한 양자 네트워크 기반 보안 통신 기술의 동향을 정리하였다. QKD, QKMS, 지능형 양자 라우팅 기술은 기존 공개키 기반 암호 체계의 한계를 보완하며, 자율주행 및 커넥티드 서비스의 장기적인 보안 신뢰성을 확보할 수 있는 핵심 기술로 평가된다.

향후 연구에서는 실제 모빌리티 네트워크 환경에서 양자 네트워크와 기존 통신 인프라의 하이브리드 적용 방안, 성능 지표(지연, 가용성, 키 갱신 주기) 기반 정량적 평가, 그리고 국제 표준 연계 방안에 대한 심층적인 분석이 필요할 것이다. 이를 통해 미래 자율주행 및 스마트시티 환경에 적합한 차세대 보안 통신 구조를 제시할 수 있을 것으로 기대된다.

## ACKNOWLEDGMENT

본 연구는 과학기술정보통신부의 지원을 받아 한국연구재단이 수행하는 「한미 전략기술 선행표준화 공동연구사업」의 일환으로 수행되었으며, “양자 네트워크 라우팅 및 제어/관리 핵심 기술과 표준 개발” 연구개발과제(연구개발과제번호: RS-2025-16067207)의 연구 결과를 포함하고 있습니다. 본 과제는 고려대학교 세종산학협력단이 주관하고, 한국자동차연구원이 공동으로 참여하여 수행되었습니다.

## 참 고 문 헌

[1] Bennett, C. H., & Brassard, G., “Quantum Cryptography: Public Key Distribution and Coin Tossing,” Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, pp. 175 - 179, 1984.

[2] Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H., “Quantum Cryptography,” Reviews of Modern Physics, vol. 74, no. 1, pp. 145 - 195, 2002.

[3] Pirandola, S., Andersen, U. L., Banchi, L., et al., “Advances in Quantum Cryptography,” Advances in Optics and Photonics, vol. 12, no. 4, pp. 1012 - 1236, 2020.

[4] Wehner, S., Elkouss, D., & Hanson, R., “Quantum Internet: A Vision for the Road Ahead,” Science, vol. 362, no. 6412, 2018.

[5] Amer, O., Krawec, W. O., & Wang, B., “Efficient Routing for Quantum Key Distribution Networks,” IEEE Transactions on Network Science and Engineering, vol. 8, no. 1, pp. 542 - 554, 2021.

[6] Cvitic, I., Perakovic, D., & Nolasco Pinto, A., “Overview of Routing Approaches in Quantum Key Distribution Networks,” IEEE Access, vol. 10, pp. 112345 - 112360, 2022.

[7] ITU-T, “Security framework for quantum key distribution networks,” ITU-T Recommendation Y.3800, 2019. (https://www.itu.int/rec/T-REC-Y.3800)