국방 통신망 보안을 위한 Trusted-MDI 하이브리드 양자 키 분배(QKD) 네트워크 구조 제안

차민선, 허준*
고려대학교, *고려대학교

alstjs9748@korea.ac.kr, *junheo@korea.ac.kr

A Trusted- MDI Hybrid Quantum Key Distribution Network Architecture for Secure Military Communications

Cha Min Seon, Heo Jun*
Korea Univ., *Korea Univ.

요 약

본 논문은 국방 통신망 보안 강화를 위해 TN QKD 와 MDI QKD 를 결합한 하이브리드 QKDN 아키텍처를 제안한다. QKD 는 도청 탐지가 가능한 보안성을 제공하지만 거리 및 확장성 한계가 있으며, TN QKD 와 MDI QKD 는 각각 효율성과 보안성 측면에서 상반된 특성을 가진다. 본 논문은 이러한 특성을 상호 보완적으로 활용하여, 고정형 노드를 중심으로 유선·무선·위성 구간에서 적합한 키 분배 방식을 선택적으로 적용하는 하이브리드 구조를 제시한다. 이를 통해 국방 환경의 이질적 네트워크 조건을 충족하면서 보안성과 효율성을 동시에 달성할 수 있음을 보인다.

Ⅰ. 서 론

최근 양자기술은 국가 경쟁력과 안보 측면에서 핵심 전략 기술로 부상하고 있으며, 국방 분야에서도 적용 가능성이 주목받고 있다. 기존 연구는 정책적·전략적 접근을 중심으로 진행되었으나[1], 실제 국방 통신망에 적용 가능한 구체적 구조 모델은 부족하다.

본 논문은 국방 통신 환경을 대상으로 QKD 및 QKDN 적용 방안을 검토하고, 특히 TN QKD 와 MDI QKD 의 장점을 결합한 하이브리드 아키텍처를 제안한다. 제안 구조는 지상·도서·위성 등 다양한 작전 환경에서 고정형 노드를 기반으로 키를 효율적이고 안전하게 분배할 수 있도록 설계되었다. 이를 통해 국방 통신망의 보안성과 효율성을 동시에 강화할 수 있는 실질적 대안을 제시한다.

Ⅱ. 본론

1) 양자 키 분배(QKD)

양자 키 분배(QKD, Quantum Key Distribution)은 양자역학의 원리를 활용하여 양자 채널을 통해 비밀키를 교환하는 방식으로, 도청이 불가능한 안전하고 강력한 보안을 가진 키 분배 방식이다[2]. 그러나 구현 방식에 따라 전송 거리와 확장성의 한계가 존재하며, 이를 극복하기 위한 장거리 전송 기술 연구가 활발히 진행되고 있다.

2) TN QKD(Trusted Node, 신뢰 노드 QKD)

TN QKD 는 장거리 전송을 위해 점대점(Point-to-Point) 구간 사이에 신뢰 릴레이 노드를 배치한다. 각 릴레이에 로컬 비밀키를 저장한 후 홉-별(hop-by-hop) 방식으로 전달한다[3]. 키 분배율이 높아 효율적이지만 모든 중계 노드를 신뢰한다는 것을 전제로 한다.

3) MDI QKD(Measurement Device Independent)

MDI QKD 는 통신 당사자(Alice, Bob)가 각각의 양자 상태를 비신뢰 측정 노드(UM)로 전송하고, UM 에서는 벨 상태 측정(BSM)만 수행하여 키를 간접적으로 생성한다[4]. UM 은 키 생성에 필요한 정보를 획득할 수 없으므로, 측정 및 검출 과정이 비신뢰 환경에서 이루어져도 보안성이 보장된다.

표 1 은 TN QKD 와 MDI QKD 의 주요 특성을 비교한 것으로 두 방식이 상호 보완적임을 보여준다.

표 1. TN QKD 와 MDI QKD 의 특성 비교

구 분	TN QKD	MDI QKD
보안모델	중간 노드 신뢰	중간 노드 비신뢰
키분배율	높음	낮음
시스템 복잡도	단순 (hop-by-hop 전달)	높음 (간섭 정렬 필요)
적용환경	물리적 보안 확보 (내부, 유선 등)	물리적 보안 취약 (무선, 위성 등)
주요 취약점	내부자/중계 노드 공격 시 보안 위협	구현 난이도 높음

4) QKDN

QKDN 은 QKD 기술을 활용하여 다자간통신 및 장거리 키 분배를 지원하는 통합 네트워크 인프라이다. QKDN 은 키 관리 계층과 제어 계층을 포함하는 다중 계층 구조로 구성되며, 키 관리 계층은 키를 수집/저장/분배 역할을 하고, 제어 계층은 네트워크 토폴로지 관리, QKD 링크 모니터링, 장애 발생 시 동적 키 라우팅을 수행한다[5].

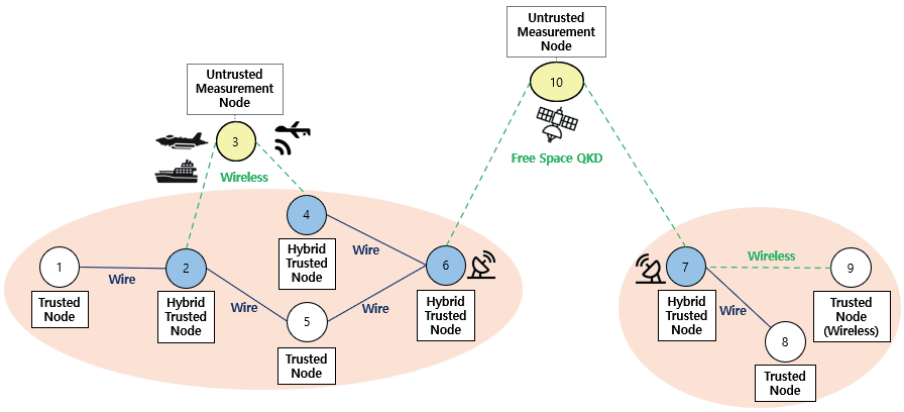

그림 1. 국방 적용을 위한 TN/MDI 하이브리드 QKDN 제안 아키텍처

QKDN 의 목표는 모든 통신 당사자 간에 종단 간 보안을 제공하는 것이며, 다양한 QKD 프로토콜의 상호 운용성을 확보하는 것이 중요한 연구 과제로 대두되고 있다.

5) 제안 하이브리드 QKDN 구조

본 연구는 그림 1 과 같이 고정형 노드를 중심으로 하는 국방 유선망(예: 국방광대역통합망)을 기반으로, TN QKD 와 MDI QKD 를 결합한 하이브리드 QKDN 을 제안한다. 적용 범위는 기지·거점·도서 지역 등 물리적 보안이 확보된 고정 노드에 한정하며, 항공기·선박·무인기 등 이동체 단말에 대한 키 분배는 후속 연구로 남긴다. 제안 구조는 표 2 와 같이 세 가지 노드 유형으로 구성된다.

표 2. 하이브리드 QKDN 의 노드 유형 및 역할

Trusted Node (TN)	보안 구역 내에서 유선 QKD 를 통한 빠르고 효율적인 키 분배 (고속·저지연)
Untrusted Measurement Node (UM)	비신뢰 환경(무인 항공기, 위성)에 배치하여 벨 상태 측정만 수행하며 MDI QKD 링크 형성(높은 보안)
Hybrid Trusted Node (HTN)	TN 과 MDI 의 송신 기능을 모두 갖추고, 제어 계층의 지시에 따라 상황에 맞게 동적으로 역할을 전환

운용 방식은 표 3 과 같이 구분한다.

표 3. 하이브리드 QKDN 운용 방식(그림 1. 예시)

구 분	적용기술	경로(노드)
유선 구간	TN QKD	1-2-5-6-4, 7-8
유선 불가, 고정 무선	FWF 기반 무선 QKD	7-9
경로 단축, 노드 우회	MDI QKD (무선 UM)	1-2-3(UM)-4
도서/해상	MDI QKD (위성 UM)	6-10(UM)-7

내부 유선 구간은 TN QKD 를 통해 고속 키 분배를 확보하며, 유선 인입이 곤란한 구간은 FWF(Fixed Wireless Fiber) 기반 무선 QKD 로 대체한다. 장거리 경로 단축이나 노드 우회가 필요할 경우 UM 기반 MDI QKD 를 적용하고 도서/해상과 같은 특수 지역은 위성 UM 을 통해 안전한 키 동기화를 유지할 수 있다.

이 구조는 고보안 구간에서 MDI QKD 를 적용하고 내부망에서는 TN QKD 를 적용하여 보안성과 효율성의 균형을 맞출 수 있다. 또한 HTN 의 동적 전환 기능을 활용해 네트워크 상황에 맞는 최적 경로 선택이 가능하며, 침해나 장애 발생 시 우회 경로를 즉시 구성할 수 있어 시스템 복원력도 강화된다.

Ⅲ. 결론

본 논문은 국방 환경의 특성을 반영한 TN/MDI 하이브리드 QKDN 아키텍처를 제안하였다. 보안이 취약한 외부 링크에서는 MDI QKD 를 적용하고, 내부망에서는 TN 방식을 적용하여 보안성과 네트워크 운용 효율성을 동시에 확보할 수 있음을 보였다. 다만, 항공기·선박·무인기 등 이동형 단말에 대한 적용은 후속 연구 과제로 남아 있으며, 향후 연구에서는 HTN 노드 기반 동적 키 라우팅 및 프로토콜 전환 시 오버헤드 분석에 중점을 둘 예정이다.

ACKNOWLEDGMENT

이 논문은 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원-대학 ICT 연구센터(ITRC)의 지원(RS-2021-II211810, 50%)과 정부(과학기술정보통신부)의 재원으로 한국연구재단 양자정보과학 인적기반 조성사업의 지원을 받아 수행된 연구임 (Grant No.2022M3H3A1063074, 50%).

참 고 문 헌

[1] Sangkyu Han, et al., "Exploring Military Use of Quantum Technologies and Strategic Tasks in the Era of Defense Innovation 4.0" Journal of Defense and Security 7, no.1 (2025) : 541-562.

[2] H.-K. Lo, M. Curty, and K. Tamaki, “Secure quantum key distribution,” Nature Photon., vol. 8, no. 8, pp. 595- 604, Jul. 2014.

[3] Zhang, et al., “Large scale quantum key distribution : Challenges and solutions [Invited],” Opt. Exp., vol. 26, no. 18, pp. 24260- 24273, Sep. 2018

[4] H.-K. Lo, et al., “Measurement device independent quantum key distribution,” Phys. Rev. Lett., vol. 108, no. 13, Mar. 2012, Art. no. 130503.

[5] Cao, Yuan, et al. “Hybrid trusted/untrusted relay-based quantum key distribution over optical backbone networks.” IEEE Journal on Selected Areas in Communications 39.9 (2021): 2701-2718.