군함 운용환경에서의 양자통신 기반 QKD 기술 적용 가능성과 발전방향

서형식, 허준 교수님*

고려대학교, 고려대학교*

suhhsik@korea.ac.kr *junheo@korea.ac.kr

Applicability and Future Directions of Quantum Communication-Based QKD Technology in Naval Warship Environments

Seo Hyeong Sik, Heo Jun*

Korea Univ., Korea Univ.

요 약

본 논문은 군함 운용환경에서 양자 키 분배(QKD, Quantum Key Distribution) 기술의 적용 가능성과 실용적 발전방향을 검토하고, 전파간섭과 기동성이 큰 해상환경에 적합한 광학 무선 기반 QKD 시스템의 적용성을 중심으로, RF-to-Optical 연계 기술, QKD 실증, PQC 병행운용 등의 전략을 제시하며, 군 통신망의 보안성과 실시간성 강화를 위한 핵심 체계로서 QKD 기술의 군사적 활용 가능성을 제안한다.

Ⅰ. 서 론

현대戰에서 통신은 단순 정보전달을 넘어 지휘통제, 정보우위 확보, 다영역 통합작전의 핵심 기반이다. 사이버전·전자전 위협이 심화됨에 따라 기존체계의 보안 한계가 존재하며, 양자컴퓨터 등장으로 전통 암호기술의 붕괴 가능성까지 제기되고 있다. 이런 배경에서 양자의 불확정성과 중첩원리를 활용한 키 분배(QKD) 기술은 이론적으로 도청 불가능한 통신을 가능하게하여, 군의 통신보안 대안으로 부각되고 있다. 특히, 군함 및 해상 플랫폼은 고속기동, 전파간섭, 해양기상 등 특수성이 크고, 기존 통신체계의 한계가 뚜렷하게 드러나는 환경이다. 이로 인해 해상운용에 최적화된 양자 기반 통신에 대한 실증적 검토가 필요하다. 본 논문은 양자기술을 전술통신에 적용하는 전략적 타당성과 구현방안, 함정 적용 시나리오, 운용제약 요소 및 발전방향을 종합검토한다. 특히, RF-to-Optical 융합, QKD 적용, PQC 병행 운용, 실증 기반 적용 방안, 연합작전 고려 등 군 운용 현실에 밀착된 적용 전략을 중심으로 다룬다.

Ⅱ. 본 론

A. 기술개요 및 원리

양자통신은 양자역학 원리 기반으로 도청 시도를 물리적으로 탐지할 수 있도록 설계된 보안통신 기술이다. 대표적인 QKD 방식인 BB84 프로토콜은 송·수신자가 간 비밀키를 공유하며, 제3자의 개입은 양자상태의 붕괴로 즉시 탐지된다[1]. QKD는 광 또는 무선환경에서 구현 가능하며, 광자 검출기, 편광필터, 랜덤 수 생성기 등과 통합된 시스템으로 구성된다. 군 환경에서 이러한 QKD 시스템을 광학모듈, 실시간 필터링/보정 알고리즘과 연계하여 운용 해야하며, 기존 통신체계와의 인터페이스 호환성확보가 중요하다[2].

B. 군함 적용 요구사항

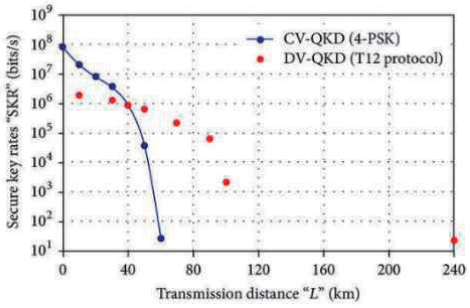
양자통신 기반 QKD 시스템은 실시간 도청 탐지와 보안 키 분배 기능을 통해, 군 함정 간, 함정-기지 간, 무인기(UAV)와의 통신에서 군 통신망의 보안성과 데이터 무결성 확보를 위한 유력한 보완 기술로 활용될 수 있다. 그러나 기동 중인 플랫폼 간에는 광자 정렬 유지가 필수적이며, 해양기상 변화, 전파 간섭, 염분 등 복합적인 제약 요인으로 인해 기존 통신체계의 안정적인 운용에는 한계가 따른다. 이를 극복하기 위해서는 FSM(Fast Steering Mirror) 기반의 실시간 정렬 기술과 더불어, 환경 적응형 하드웨어 설계, 다중 경로 대응 기술, 예측 기반 정렬 알고리즘 등의 병행 개발이 요구된다[2].

C. 발전 방향

1. RF-to-Optical 변환 및 다중통신 모듈 융합 : 군 플랫폼은 현재 RF 기반 무전기, 위성통신기, 내부망 등 다양한 전술 통신수단을 운용하고 있으며, 광학 무선 기반 양자통신 시스템을 기존 체계와 통합운용하려면 RF 기반 장비와 상호연동 되어야 한다. RF ↔ 광 변환기 개발과 다중 통신모듈 간 인터페이스 설계가 선결과제로 요구된다. 양자통신은 광자 기반 신호전송을 사용하므로, 기존 RF 채널과는 물리적 특성 및 운용조건이 달라, 이기종 채널 간 정밀한 융합 설계가 필요하다. 이를 통해 기존 전술망 속에서 양자보안 통신의 실시간 적용 기반을 마련할 수 있다[1, 3].

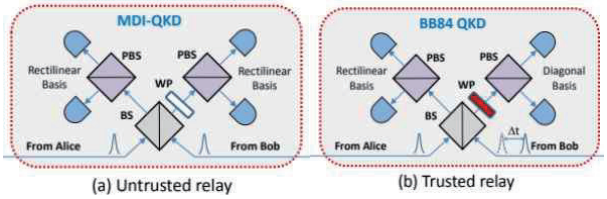
2. QKD 기반 전술환경 실험 : 해상 작전환경은 진동, 파도, 염분, 채널 불안정성 등 다양한 요인으로 인해 정밀한 광자제어가 필요한 DV-QKD(DV: Discrete Variable)에 불리한 조건이다. 반면, CV-QKD(CV: Continuous Variable)는 강한 레이저와 일반 광검출기

를 사용해 잡음내성이 높고, 기존 통신 장비와의 호환성이 우수하여 전술운용에 실용적일 수 있다. 해상 전술 환경에서 CV-QKD의 성능, 잡음 허용도, 실시간 처리력 등을 평가하는 실증실험이 필요하다. 다만, QKD 프로토콜은 작전반경과 임무성격에 따라 선택적 운용이 필요하며, 예를 들어 장거리 고보안 통신이 요구되는 해외파병/훈련(소말리아 해역, 태평양 등)에는 DV-QKD 기반 단일광자 방식이 적합해 보인다. 따라서, 향후 해상 QKD 시스템은 운용범위(한반도 및 원해)와 플랫폼 특성에 따라 프로토콜을 병렬적으로 설계하고, 환경별 실증 데이터를 기반으로 최적화하는 방향으로 발전되어야 한다[3].



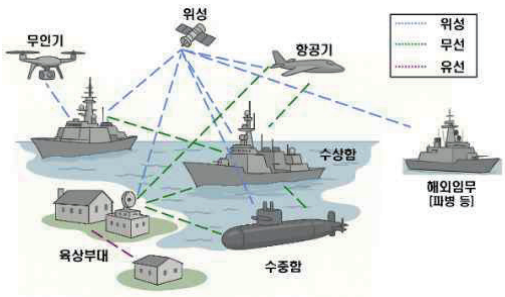
< Comparison of CV-QKD / DV-QKD[5] >

3. 연합작전 고려 표준화 및 네트워크 보안 : 우리 군 양자통신 기술은 연합/합동작전 환경까지 고려한 표준화가 필수적이다. 특히, 인터페이스 규격, 프로토콜 호환성, 키방식 등에 대해 국제표준 연계 및 상호운용성 확보방안이 필요하고, QKD 네트워크 보안 취약점은 양자채널 보다 단말장비(Endpoint)에 있으며, 이는 키를 수신한 이후에 사용하는 암호모듈, 인증서버 등이 여전히 기존 사이버 위협(내부자 위협, 물리적 침투 등)에 노출되어 있다. 이를 보완하기 위해 엔드포인트 보안 강화, 중계노드를 신뢰하지 않는 구조(MDI-QKD, Measurement Device Independent QKD)의 도입이 요구된다. 현재 노드 간 직접연결이 어려운 환경에서는 중계노드에 의존하는 방식이 보안상 약점이 될 수 있음으로, 군에서의 QKD 체계는 엔드포인트 보안, 무신뢰 구조, 국제표준 연계를 중심으로 발전이 필요해 보인다.



< MDI-QKD & BB84 QKD[6] >

4. 전장북상에 따른 양자통신 운용 전략 : 유사시(국지도발 등) 전장이 북상으로 확장될 수 있어, 이와 같은 환경에서는 통신의 기민한 전개와 도청방지 능력이 동시에 요구되므로, 양자통신 기반 QKD 시스템 탑재와 운용방식 또한, 전략적 유연성을 가져야 한다. 이동식 해상 플랫폼(UUV/USV), 고속함, 연안배치 장비 등에 QKD 모듈을 탑재하고, 통신노드를 분산배치함으로써, 적 탐지망을 회피한 보안 연결망을 구성할 수 있다. 특히, 전장 확장에 따라 해상 네트워크도 북상함에 따라, 위성 중계기 및 고고도 UAV를 이용한 QKD 링크와 병행하여 광역 커버리지 확보 전략이 필요하다.



< 군함 중심의 해 · 육상 통신망 개요 >

Ⅲ. 결 론

양자 기반 QKD 기술은 군 통신의 보안성과 실시간성을 근본적으로 향상시킬 수 있는 차세대 전략기술이다. 본 논문은 해상 운용 특수성에서 기술적용 가능성과 발전방향을 다각도로 제시하였으며, 향후 군사적 운용환경에서 양자기술은 작전 효율성과 정보우위 확보를 위한 핵심체계로 자리매김하고, 실질적 기여를 할 것으로 기대된다.

ACKNOWLEDGMENT

본 논문은 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. RS-2023-00242396)

참 고 문 헌

[1] Liorni, C., G. De Falco, and M. Dispenza. "Free-space quantum communication for security and defence applications. "Environmental Effects on Light Propagation and Adaptive Systems VII. Vol. 13194. SPIE, 2024.

[2] Kim, Dongkyu, et al. "Quantum-correlation-based free-space optical link with an active reflector. "Current Applied Physics41 (2022): 156-162.

[3] Liu, Hua-Ying, et al. "Optical-relayed entanglement distribution using drones as mobile nodes. "Physical Review Letters126.2 (2021): 020503.

[4] Hoi-Kwong, Marcos Curty, and Bing Qi. "Measurement -device-independent quantum key distribution. "Physical review letters108.13 (2012): 130503.

[5] Asif, Rameez, and William J. Buchanan. "Quantum-to -the-Home: Achieving Gbits/s Secure Key Rates via Commercial Off-the-Shelf Telecommunication Equipment. "Security and Communication Networks2017.1 (2017): 7616847.

[6] Qi, Bing, et al. "Free-space reconfigurable quantum key distribution network."2015 IEEE International Conference on Space Optical Systems and Applications (ICSOS). IEEE, 2015.