위성 보안 통신을 위한 양자 키 분배 기술 및 머신러닝 최적화 기법 동향

박민용, 윤훈석, 이병주
인천대학교 정보통신공학과
{pmy1143 ,hunseok2002 ,bjlee}@inu.ac.kr

Recent Trends in Quantum Key Distribution Technologies and Machine Learning Optimization for Secure Satellite Communications

Minyong Park, Hunseok Yun ,Byungju Lee
Department of Information and Telecommunication Engineering
Incheon National University

요 약

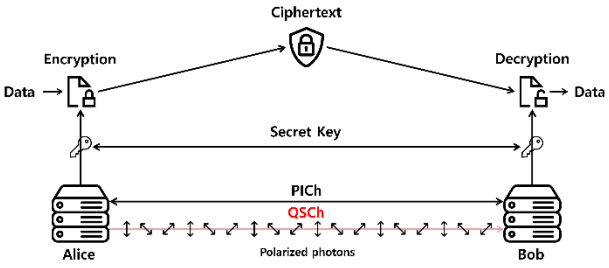
최근 양자 컴퓨팅 기술의 급속한 발전으로 기존 고전 암호 체계의 보안 취약성이 심화됨에 따라, 정보 이론적 보안을 제공하는 양자 키 분배(QKD) 기술이 차세대 보안 통신의 핵심 기술로 부상하고 있다. 특히, 지상 광섬유 기반 QKD 의 전송 거리 한계를 극복하기 위해 레이저 빔을 활용한 위성 기반 QKD 시스템이 필수적으로 요구된다. 본 논문에서는 이산 변수 기반 QKD(DV-QKD)와 연속 변수 기반 QKD(CV-QKD)의 작동 원리를 비교 및 분석하고, 위성 통신 환경의 동적 특성으로 인해 발생하는 주요 한계점을 고찰한다. 또한 이러한 한계를 보완하기 위한 머신러닝(ML) 기반 최적화 기법의 연구 동향을 분석하고, 향후 통합 보안 네트워크 구축을 위한 발전 방향을 제시한다.

Ⅰ. 서 론

최근 양자 컴퓨팅 기술의 급속한 발전은 기존의 수학적 복잡성에 기반한 공개 키 암호화 체계에 심각한 보안 위협을 초래하고 있다. 이에 대한 대안으로, 양자역학의 원리를 활용하여 정보 이론적 보안을 제공하는 양자 키 분배(Quantum Key Distribution, QKD) 기술이 주목받고 있다 [1]. 특히 지상 광섬유 기반 QKD 는 전송 손실로 인해 통신 거리가 약 100 km 내외로 제한되는 반면, 위성 기반 QKD 는 레이저 빔을 이용해 수만 킬로미터에 걸쳐 광자를 전송할 수 있어 글로벌 양자 암호 네트워크 구축의 핵심 기술로 평가된다.

II. QKD 기술 개요 및 위성 적용 한계

QKD 는 송신자 (Alice) 와 수신자 (Bob) 사이에 보안이 보장된 비밀 키를 생성 및 분배하는 기술이다 [1].



[그림 1] QKD 의 작동원리 [1]

QKD 시스템은 양자 상태를 전송하는 QSCh(Quantum Signal Channel)과 키 생성 및 사후 처리를 수행하는 PICh(Public Interaction Channel)로 구성된다 [1]. 송신자는 QSCh 를 통해 단일 광자 소스를 이용하여 양자 상태가 인코딩된 광자를 전송하며, 이 과정은 하이젠베르크의 불확정성 원리와 양자 복제 불가능성 정리에 기반한다. 만약 도청자(Eve)가 전송 중인 광자를 측정하거나 복제할 경우 양자 상태가 변화하므로, 송신자와 수신자는 이를 즉시 감지할 수 있다 [1].

수신자는 수신된 광자를 검출기를 통해 측정한 후, PICh 를 통해 송신자와 측정 기저 정보를 교환한다. 이후 기저가 일치하는 비트만을 선별하는 시프팅(sifting), 오류 정정(error correction), 프라이버시 증폭(privacy amplification) 과정을 거쳐 최종적인 비밀 키를 공유한다 [1]. 생성된 비밀 키는 [그림 1]에 나타난 데이터 암호화 및 복호화에 사용되며, 일회성 패드(one-time pad)와 결합될 경우 기존의 수학적 난제 기반 암호 체계와 달리 이론적으로 완전한 보안을 제공할 수 있다 [1][2].

QKD 는 전송 및 검출 방식에 따라 이산 변수 기반 QKD(DV-QKD)와 연속 변수 기반 QKD(CV-QKD)로 구분된다. DV-QKD 는 단일 광자의 편광(State of Polarization, SOP) 또는 위상과 같은 불연속적인 양자 상태에 정보를 인코딩한다. 대표적인 예로 BB84 프로토콜이 있으며, 송신자는 단일 광자 소스 또는 감쇄된 레이저를 이용해 $|0\rangle$, $|1\rangle$, $|+\rangle$, $|-\rangle$와 같은 큐비트 상태를 전송한다 [1][2]. 수신단에서는 광자 계수 (Photon Counting) 방식의 단일 광자 검출기(Single Photon Detector, SPD)가 필수적이며, 위성 탑재 환경에서는 소형화와 기술적 성숙도가 높은 Si-SPAD(Silicon Single Photon Avalanche Diode)가 주로 사용되고, 지상국에서는 높은 검출 효율을 갖는 SNSPD(Super-conducting Nanowire Single Photon Detector)가 선호된다 [2].

DV-QKD 는 장거리 전송에서도 낮은 양자 비트 오류율(Quantum Bit Error Rate, QBER)을 유지할 수 있는 보안 증명을 제공하지만, 다중 광자 발생 시 완벽한 단일 광자가 아닐 경우 광자 수 분할 (Photon Number Splitting, PNS) 공격에 취약하다. 이를 보완하기 위해 신호 세기를 무작위로 변화시키는 Decoy state 프로토콜이 함께 사용된다 [2].

CV-QKD 는 Coherent state 레이저의 전기장 진폭과 위상 같은 연속적인 물리량에 정보를 인코딩한다 [1]. 고가의 단일 광자 검출기 대신 Homodyne 또는 Heterodyne 검출 방식을 사용하므로 기존 광통신 인프라와의 호환성이 높고 구현 비용이 상대적으로 낮다. 또한 수신단의 국부 발진기(Local Oscillator, LO)가 강력한 정합 필터 역할을 수행하여 주간의 강한 태양광 잡음 환경에서도 동작 가능하다는 장점이 있다 [2]. 반면, CV-QKD 는 위상 잡음에 민감하며 거리 증가에 따른 신호 감쇄로 인해 낮은 SNR(Signal-to-Noise Ratios)이 발생한다. 이로 인해 DV-QKD 에 비해 통신 거리 확장에 한계가 있으며, 사후 처리 과정의 계산 복잡도 또한 높은 편이다 [2].

위성 통신 환경은 다양한 물리적 변수로 인해 지상 환경에서 검증된 QKD 기법을 그대로 적용하기 어렵다. DV-QKD 의 경우, 위성-지상국 링크에서 태양광 및 달빛과 같은 강한 배경 잡음은 단일 광자 검출기의 신호 식별을 방해하여 주간 운용을 제한한다. 또한, 우주 방사선은 위성 탑재 검출기 소자의 열화를

유발하여 내부 잡음인 dark count 를 증가시키며, 이는 시스템 SNR 저하와 통신 가용 시간 감소로 이어진다 [2].

CV-QKD 는 대기권을 통과 시 발생하는 대기 난류 및 섬광 효과로 인해 광자의 위상이 불규칙하게 변형되어 수신단의 Coherence 유지가 어렵다. 특히, 저궤도 위성의 고속 이동으로 인해 발생하는 수 GHz 수준의 Doppler shift 는 주파수 동기화를 복잡하게 만들어 안정적인 통신을 저해하는 주요 요인으로 작용한다 [2].

III. 머신러닝 기반 QKD 최적화 기법 동향

위성 통신 환경에서 QKD 기법은 다양한 물리적 제약에 직면하므로, 이를 보완하기 위한 머신러닝(Machine Learning, ML) 기반 최적화 기법에 대한 연구가 활발히 진행되고 있다.

DV-QKD 는 위성 통신 시 기계적 진동과 대기 환경 변화로 인해 신호의 SOP 가 불규칙하게 변동하며, 이는 QBER 을 증가시켜 키 교환 성능을 저하시킨다 [3]. 이를 완화하기 위해, 과거 데이터를 학습한 심층 신경망(Deep Neural Networks, DNN)을 이용하여 SOP 변화를 실시간 예측하고, 수신단의 EPC (Electronic Polarization Controllers)를 선제적으로 제어함으로써, SOP 변동이 심한 환경에서도 QBER 을 1% 미만으로 유지하고 비밀 키 교환률을 최대 89% 향상시켰다 [3]. 비록 공중 광섬유 환경을 대상으로 수행되었으나, 위성 통신 역시 유사한 편광 변동 메커니즘을 가지므로, 본 기법은 위성 QKD 의 SOP 왜곡 보정에 효과적으로 적용될 수 있을 것으로 기대된다.

CV-QKD 는 대기 잡음과 기존 신호 간 간섭에 민감하며, 동적인 위성 환경에서 최적 주파수를 실시간으로 계산하는 과정은 높은 계산 복잡도와 지연을 수반한다 [2]. 이를 해결하기 위해, XGBoost 모델을 활용하여 양자 채널과 고전 채널이 공존하는 환경에서 잡음을 최소화하는 주파수 최적화 기법이 제안되었다. 해당 모델은 Decoy-BB84 프로토콜 기반 SKR (Secret key Rate) 하한식을 목적 함수로 하여 최적 주파수를 예측하며, SKR 은 다음과 같이 정의된다.

$$SKR \geq \max\{0, \left(Q_1[1-H(e_1)] - \eta_{ec} Q_\mu H(E_\mu)\right)/T_s\} \quad (1)$$

여기서 Q_μ 와 E_μ 는 전체 이득과 QBER 을 나타내며, Q_1 과 e_1 은 단일 광자 상태에서의 이득과 QBER 을 의미한다. η_{ec} 는 오류 정정 효율, T_s 는 레이저 펄스 반복 주기이며, $H(x)$ 는 Shannon 이진 엔트로피 함수이다 [1] [4].

$$H(x) = -x\log_2(x) - (1-x)\log_2(1-x) \quad (2)$$

연구 결과, 제안된 모델은 기존의 수치 적분 기반 방식이 수백 초 소요되던 계산을 0.1 초 이내로 단축하면서도 높은 예측 정확도를 유지하였다 [4]. 비록 해당 연구는 Multi-band EONs (Elastic Optical Networks) 내 양자 채널과 기존 채널의 공존 환경을 다루었으나, 위성 채널 역시 배경 잡음과 도플러 효과로 인해 채널 상태가 빠르게 변화한다는 점에서 유사한 특성을 갖는다. 따라서 본 기법을 위성 QKD 환경에 적용할 경우, 계산 복잡도를 크게 줄이면서도 효과적인 잡음 최소화가 가능할 것으로 기대된다.

위성 통신 환경에서 발생하는 복합적인 물리적 왜곡을 동시에 고려하기 위해, SOP 예측을 위한 DNN 과 주파수 자원 최적화를 위한 XGBoost 를 SDN (Software Defined Networking) 기반 구조 내에서 통합 운용하는 방식이 제안되고 있다 [1] [3] [4].

SOP 와 주파수는 물리적으로 상호 독립적인 변수이므로, 본 논문에서는 다음과 같은 통합 성능 지표를 정의하여 두 요소를 동시에 최적화한다.

$$SKR_{total} \geq \frac{Q_1[1-H(e_1)]-\eta_{ec}Q_\mu H(E_{total})}{T_s} \quad (3)$$

전체 오류율 E_{total} 은 DNN 기반 SOP 보정에 따른 오류 E_{SOP} 와 XGBoost 가 선정한 잡음 최소화 주파수 기반 에러 E_{Noise} 의 합으로 정의된다[3] [4].

$$E_{total} = E_{SOP}(\Delta\theta, \Delta\varphi) + E_{Noise}(f_{opt}, LF) \quad (4)$$

여기서 $\Delta\theta$ 와 $\Delta\varphi$ 는 DNN 을 통해 예측된 편광각 과 타원율 오차이며, f_{opt} 와 LF 는 XGBoost 가 최적화하는 주파수와 부하율이다 [3] [4].

SDN 컨트롤러를 통해 두 모델이 협력적으로 동작할 경우, 주파수 최적화를 통해 SNR 이 개선되고 이는 DNN 입력 데이터의 품질을 향상시켜 SOP 예측 정확도를 높이는 선순환 구조를 형성할 수 있다. 또한 저궤도 위성의 고속 이동으로 인한 수 GHz 수준의 도플러 편이에 대해서도, 통합 모델은 주파수 변화와 SOP 왜곡을 동시에 학습함으로써 보다 유연한 대응이 가능하다 [2].

결과적으로 이러한 통합 ML 기반 최적화 방식은 통신 단절을 최소화하고 연산 시간을 밀리초 수준으로 단축함으로써, 대규모 위성 기반 양자 암호 네트워크의 실시간 운영을 가능하게 하는 핵심 기술로 기대된다 [4] [5].

IV. 결론

본 논문에서는 차세대 보안 통신의 핵심 기술로 주목받는 위성 기반 QKD 의 기술 현황과 저궤도 위성 환경에서 직면하는 물리적 한계, 그리고 이를 극복하기 위한 머신러닝 기반 최적화 방법론을 분석하였다. 분석 결과, 위성 통신의 동적 특성으로 인해 발생하는 SOP 변동, 도플러 편이, 배경 잡음 및 Dark count 문제는 기존의 정적 제어 기법만으로는 효과적인 대응이 어려운 복합적 과제임을 확인하였다. 이러한 한계를 완화하기 위한 머신러닝 기반 최적화 기법은 유의미한 성능 향상 가능성을 보이고 있다. 향후 위성 기반 QKD 는 지상 광 네트워크와 연계된 통합 양자 보안 네트워크로의 발전이 기대되며, 이를 위해 이기종 QKD 기법을 통합 제어할 수 있는 하이브리드 머신러닝 모델에 대한 연구와 실제 우주 환경에서의 장기적 성능 검증이 병행되어야 한다. 결론적으로, 양자역학에 기반한 물리적 보안성과 머신러닝 기반 최적화 기술의 결합은 안정적인 양자 인터넷 구현을 위한 핵심 기반이 될 것으로 기대된다.

ACKNOWLEDGMENT

본 연구는 과학기술정보통신부 및 정보통신기획평가원의 대학 ICT 연구센터사업 (IITP-2026-RS-2023-00259061)의 연구결과로 수행되었음

참 고 문 헌

[1] P. Sharma, A. Agrawal, V. Bhatia, S. Prakash and A. K. Mishra, "Quantum Key Distribution Secured Optical Networks: A Survey," in IEEE Open Journal of the Communications Society, vol. 2, pp. 2049-2083, 2021.

[2] J. J. Shawe, J. Horgan and D. Kilbane, "Advances in Receiver and Detection Systems for Low Earth Orbit Nanosatellite Quantum Communications," in IEEE Access, vol. 13, pp. 147545-147568.

[3] M. Ahmadian, M. Ruiz, J. Comellas and L. Velasco, "Cost-Effective ML-Powered Polarization-Encoded Quantum Key Distribution," in Journal of Lightwave Technology, vol. 40, no. 13, pp. 4119-4128.

[4] P. Mehdizadeh, M. Dibaj, H. Beyranvand and F. Arpanaei, "ML-Optimized QKD Frequency Assignment for Efficient Quantum-Classical Coexistence in Multi-Band EONs," in IEEE Communications Letters, vol. 28, no. 12, pp. 2794-2798.

[5] A. Mamiya et al., "Satellite-based QKD for Global Quantum Cryptographic Network Construction," 2022 IEEE International Conference on Space Optical Systems and Applications (ICSOS), Kyoto City, Japan, 2022, pp. 47-50.