QKD 네트워크 거리확장을 위한 국가별 연구동향 분석

석우진

한국과학기술정보연구원

wjseok@kisti.re.kr

Analysis of Research Trends in Distance Extension for QKD

Woojin Seok

Korea Institute of Science and Technology Information

요 약

본 논문에서는, 양자키분배(QKD) 네트워크 구성에서 기술적 한계로 인식되고 있는 전송거리 문제를 소개하고 이를 해결하기 위한 국가별 기술 접근 방안을 분석하고자 한다. 싱가포르와 중국의 경우 위성통신기술을 사용하여 거리한계를 극복하고자 하였으며, 일본과 유럽의 경우, 높은 보안수준의 중간 경유지 노드를 사용하여 거리한계를 극복하고자 하였다.

Ⅰ. 서 론

양자컴퓨터의 출현으로 정보통신의 기반이 되는 암호통신 자체가 위협을 받게 되었다. 이를 양자위협이라고 하며, 이에 대한 대응기술로써, 양자물리현상을 정보통신에 적용한 양자암호통신 기술이 발전하게 되었고, 양자키분배(QKD)기술은 양자키를 안전하게 전송하는 양자암호통신 기술 중 하나이다.

2020년에 보고된 미국 에너지부의 양자인터넷 청사진 전략에서는 양자물리현상을 기반한 양자네트워킹 기술을 크게 2가지로 구분하였으며, “Upscaling Quantum Computing” 그리고 “Secure Quantum Communication”으로 구분하였다.

“Upscaling Quantum Computing” 연구의 사례로는, 양자 얽힘교환(entanglement swapping)을 통하여 큐비트 정보를 교환하는 기술로써, 미국 LBNL 연구소를 중심으로 QUANT-NET 이름으로 진행된 사례가 있다 [1]. QKD 기술은 양자적 특성을 활용하여 안전하게 암호키를 전달하는 방식으로써 “Secure Quantum Communication”에 해당한다.

본 논문에서는 “Secure Quantum Communication” 기술영역에서 QKD 기술이 가지는 거리한계에 대한 문제점을 소개하고, 이를 해결하기 위하여 각국에서 추구하는 연구 동향을 소개하고 분석하고자 한다.

Ⅱ. QKD 네트워크에서의 거리적 한계 문제점

QKD 네트워크를 구성하기 위해서는 기존 광통신 선로(dark fiber optical cable)를 기반으로 구축된다. 광통신 선로를 바탕으로 송신자와 수신자 개념으로 QKD 전송장비가 필요하다.

대전과 오창에 설치된 사례로써, 양자키분배를 위하여 두 개의 원거리 사이트에 각각 QKD 전송장비가 설치되며 이를 광통신 선로로 연결된다. 하지만 문제는 70-80키로미터를 벗어나서 더 먼거리를 전송하기 위해서는 중간 노드 역할의 장비가 필요하다. 하지만 현재 기존 네트워크 인프라처럼, 양자 특성상 양자 정보는 저장이 되기 어려워서 네트워크 스위치나 라우터 같은 장비가 개발되어 있지 않다.

Fig.1. QKD network between Daejon and Ochang

이러한 기술적 제약으로 인하여, 우리나라 국가연구망에서는 단일홉 기반의 QKD 네트워크 수준의 인프라를 제공하고 있다. 싱가포르도 QKD 장비를 통하여 단일홉 기반의 QKD 네트워크 인프라를 제공하고 있다. 미국의 경우, 다양한 연구기관에서 각각 다른 수준의 양자네트워크 연구를 보여주고 있으나, 오크리지 연구소(ORNL)에서는 단일홉 기반의 QKD 네트워크를 구축하고 테스트베드로 활용하고 있다.

Ⅲ. 국가별 거리문제 해결 연구 동향 및 분석

양자특성상 단일홉 이상을 전달하기 위한 중간노드 개발이 양자물리 특성상 실현이 어려운 상태에서, 안전한 네트워크를 위한 QKD 네트워크 연장의 요구는 필요한 상황이다.

QKD 네트워크 거리 연장을 위하여, 중국의 경우, 인공위성을 사용하여 거리의 한계를 늘리고 있다. 광통신선로 기반 양자키전달은 단일홉 최대 약 70-80키로미터 이상의 거리가 어려운 한계가 있다. 그래서 무선통신 혹은 프리스페이스통신(Free Space Network) 방식으로 양자키 전달의 거리를 늘리고자 한 것이다. 중국은 현재까지 두 개의 위성을 사용하여 양자네트워크를 구성하고 있으며, 중국내 다수의 도시간의 피어-투-피어 양자네트워크를 구성하였다. 두 개위성과 기존 광선로기반 통신을 혼용하여 전국망 수준의 QKD 네트워크를 구축하고 있다고 보고되고 있다.

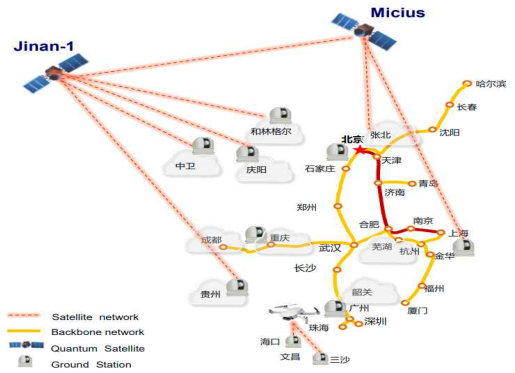

Fig.2. Satellite QKD for China

싱가폴의 경우도, 위성을 사용하여 거리의 한계 문제를 해결하고자 한다. 싱가폴의 경우, 국가의 특성상 스타-토폴로지 방식의 단일홉으로 싱가폴 국가를 양자 네트워크로 연결이 가능하나, 국제간 양자네트워킹을 위해서 위성을 사용하여 거리의 한계 문제를 해결하려고 한다. 특히 싱가폴의 경우, 자국기업에서 제작한 위성QKD 기술을 사용하고자 하며, 산학연 연계한 기술협력 체제가 우수하게 구축되어 있다.

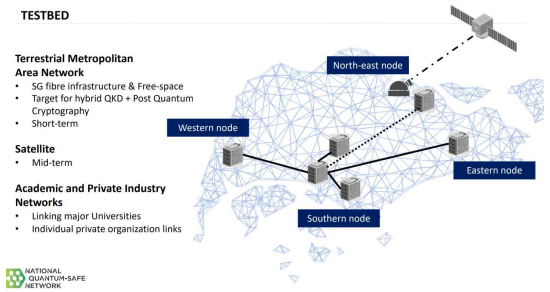

Fig.3. Satellite QKD for Singapore

유럽의 독일, 폴란드, 스페인의 경우, 각국별 QKD 네트워크가 존재하고 이를 상호 연결하기 위한 연구를 하고 있다. 이를 통하여, 각각의 단일홉 기반 QKD 네트워크 거리 한계를 극복하고자 한다. 중간 노드인 독일 사이트에서는 PQC 암호를 사용하여 보안/암호 관점에서 충분히 높은 수준의 암호로 인캡슐레이션 하는 방식을 사용하며 QKD 양자키를 전달하는 하이브리드 방식으로 구현하였다. 이는 양자위협의 대응이라는 차원에서 충분히 높은 수준의 PQC 암호를 사용하여 양자네트워크를 구성하는 것이라 할 수 있겠다. PQC 암호방식으로는 Kyber/Falcon 및 NTRU/Dilithium 알고리즘을 사용하였다. 이는 미국 NIST에서 제공하는 PQC 암호표준안을 수용하는 것이다.

비록 PQC 암호체계를 혼용하여 QKD 네트워크 연장에 사용하는 것이 완벽하게 종단간 양자적 특성을 기반한 보안망이라고 할 수는 없으나, 기술적으로 충분히 우수한 수준의 보안망 구축이라는 의미 부여는 가능한 것으로 판단된다.

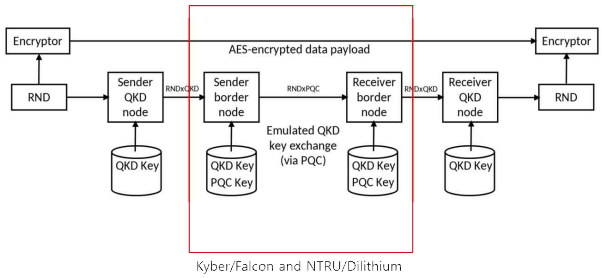

Fig.4. Using PQC to Interconnect QKD Networks

일본도 유럽과 유사한 방식을 사용하지만, 다소 차이가 있다. 하나의 중간노드에서 양자키를 전환하는 방식으로 거리를 연장하는 방식을 취하고 있다. 유럽 방식처럼 완전한 QKD 네트워크 라고 할 수는 없지만, 암호 네트워크 관점에서 단일노드 안에서 기밀성을 유지한 채로 키를 전달한다는 점에서 충분히 높은 수준의 보안망 구성의 의미는 있다고 하겠다.

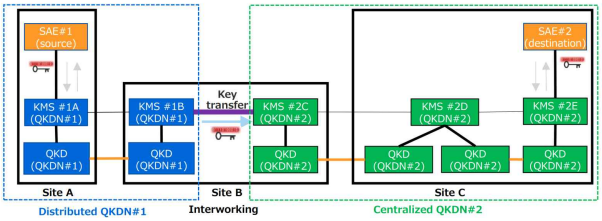

Fig.5. Interoperable Key Relay for heterogeneous QKD

IV. 결론

QKD 네트워크는 강력한 안전성을 보장하는 네트워크이지만, 양자특성상 기술적 한계로 인하여 거리의 제약을 받고 있다. 이를 극복하기 위한 방안으로 중국, 싱가폴, 유럽, 일본 등 각나라에서는 위성을 사용하거나, PQC 혹은 중간 노드내에서 암호키를 전달하는 방법을 사용하고 있다. 위성을 사용하는 방안은 추가적인 위성 운용을 요구하는 점에서 충분한 예산을 수반해야 하는 방안이다. 충분한 수준의 기밀성 및 보안을 구성한 중간노드를 사용하여 양자정보를 디지털 정보로 변환하여 거리를 연장하는 방안은 위성운용 방안보다는 현실성이 있다고 할 수 있겠다.

ACKNOWLEDGMENT

이 논문은 2025년도 한국과학기술정보연구원(KISTI)의 기본사업으로 수행된 연구입니다. (국가연구 인프라 기반 양자암호통신망 기술개발, K-25-L05-M02-C02-S01)

참 고 문 헌

[1] “QUANT-NET: A testbed for quantum networking research over deployed fiber”, Inder Monga et al., QuNet '23, NY USA, September 10 - 14, 2023

[2] “Interoperable key relay between heterogeneous QKDNs”, Mayuko Koezuka et al., Qcrypt 2023