이기종 양자암호통신망 연동에서의 저지연 키 전송을 위한 적응형 양자키전달 기능 개발

심규석, 이원혁

한국과학기술정보연구원

{kusuk007, livezone}@kisti.re.kr

Development of Adaptive Quantum Key Relay for Low-Latency Key Relay in Inter-Domain QKD Network

Kyu-Seok Shim, Wonhyuk Lee

Korea Institute of Science and Technology Information

요 약

양자암호통신 시장은 점차 확대되고 있고, 장비의 다양성 및 기능의 다양성을 갖추고 있다. 이에 양자암호통신 장비는 점차 확장성 및 호환성에 대한 연구를 진행하고 있다. 현재 양자암호통신 장비는 동일한 벤더사에서 개발한 제품으로 구성되면 문제없지만, 다른 벤더사 및 다른 통신 사업자간의 연결이 요구될 시 장비 간의 기능 개선이 필요하다. 그럼에도 불구하고 ITU-T 및 ETSI 등 국제 표준 기관에서 인터도메인간 양자키 전달을 위한 표준을 진행하고 있다. 따라서 본 논문에서는 이기종 양자암호통신망 연동에서 다수의 키 전달 요청이 한 구간으로 집중되며 발생할 수 있는 병목현상을 해결하기 위한 적응형 양자키전달 기능을 제안한다. 사용자 보안 레벨 및 양자키관리 시스템의 키 보유량에 따라 키를 전달할 시 서로 다른 암호체계(OTP, AES256, RAW)를 적용한다. 제안하는 시스템을 통해 양자암호통신 확장 구간에 대한 보안 및 저지연 키 전달할 수 있는 기능을 증명한다.

Ⅰ. 서 론

양자컴퓨터의 발전과 더불어 사이버 보안 위협은 점차 정교해지고 있으며, 이에 따라 차세대 보안 기술로 양자암호통신(Quantum Key Distribution Network, QKDN)이 주목받고 있다. QKDN은 양자역학적 원리에 기반하여 절대적인 보안성을 제공할 수 있는 기술로 금융, 국방, 공공 인프라 등 다양한 분야에서 활용 가능성이 제시되고 있다[2].

그러나 양자암호통신망은 확장성에 한계를 가진다. 현재 양자암호통신망은 동일한 벤더의 장비로 구성될 경우 안정적으로 동작하지만 이기종 장비 및 서로 다른 통신사업자간의 연동이 요구되는 상황에서는 상호운용성 문제가 발생한다. 대표적으로 각 도메인을 연결시키는 구간에서 다수의 키 전달 요청이 집중될 경우 네트워크 병목 현상이 발생하여 키 부족 및 키 생성에 지연이 발생될 수 있고 이것은 서비스 품질을 저하시킬 수 있다.

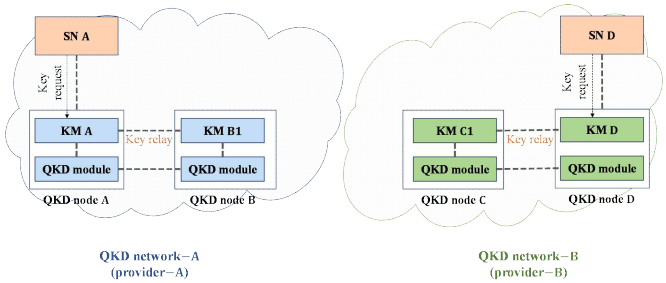
각 도메인을 연결시키기 위한 국제 표준 ITU-T 및 ETSI를 중심으로 표준화작업이 활발히 진행되고 있다.[4][5] 주로 구조 및 인터페이스 정의에 집중하고 있으며 이기종 네트워크 환경의 호환성 확보를 목표로 한다. 그러나 이러한 표준은 보안성 및 대규모 키 요청이 몰릴 경우 발생하는 지연 문제와 키 스케줄링 전략에 대한 고려가 충분하지 않다.

따라서 양자암호통신망이 국가적 규모로 확장되고 있고, 더 나아가 글로벌 규모로 확장됨에 따라 저지연, 고효율 키 전달은 필수 요건이다. 특히 사용자의 보안 요구 수준과 네트워크 상황에 따라 유연하게 대응할 수 있는 키 전달 기능이 요구된다. 이를 통해 한정된 양자키 자원을 효율적으로 활용하고, 보안성과 서비스 품질을 동시에 만족시킬 수 있다.

본 논문에서는 이기종 양자암호통신망 연동 환경에서 다수의 키 요청이 집중될 때 발생하는 병목현상을 해결하기 위해 적응형 양자키 전달 기능을 제안한다. 제안하는 시스템은 사용자 보안 레벨과 양자키관리 시스템의 키 보유량, 그리고 구축 환경에 따라 다양한 암호체계(OTP, AES256, RAW)를 선택적으로 적용한다. 이를 통해 확장된 네트워크 구간에서도 저지연, 고신뢰 키 전송을 가능하게 하고, 이기종 네트워크간 연동의 실질적 보안성을 증명한다.

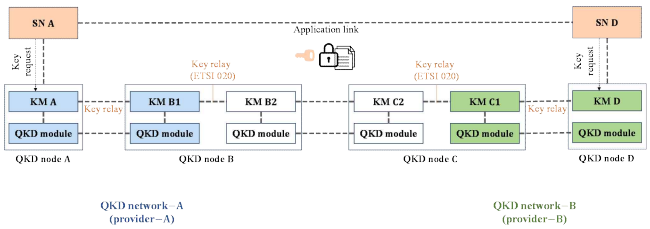
Ⅱ. 본론

본 논문에서는 이기종 양자암호통신망 환경에서 양자암호통신 확장을 위한 적응형 키 전달방안을 제안한다. 이기종 양자암호통신망 환경은 아래 그림과 같이 서로 다른 장비 및 서로 다른 통신사간의 양자암호통신망을 의미한다. 이기종 양자암호통신망 환경에서는 양자키분배장치(QKD)로 대칭키를 분배하는 것이 불가능하며, 같은 장비 사용으로 대칭키 분배가 가능하더라도 서로 다른 통신사간의 민감 정보를 전달해야하기 때문에 현실적인 어려움이 있다[3].

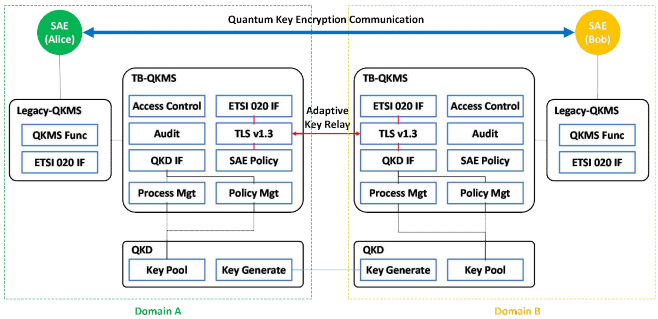


따라서 그림과 같이 이기종 양자암호통신망 연동을 위한 구조를 Trusted-Bridge 양자키관리 시스템을 통해 제안하였으며, 해당 구조를 통해 서로 다른 양자암호통신망에 속한 Service Node(SN)간에 양자암호

통신이 가능하게 되었다.[1] 그러나, Trusted-Bridge 형태의 구조로 네트워크를 구축하였을 때 QKD Network A에 있는 모든 SN와 QKD Network B에 있는 모든 SN간 양자암호통신을 위해 오직 Trusted-Bridge 양자키관리 시스템이 구축된 경로로만 키를 전달할 수 있는 한계가 있다.



본 논문에서는 해당 구간에 키 전달 요청이 과도하게 발생할 것으로 예상하기 때문에 적응형 양자키 전달 기능을 개발하였다. 적응형 양자키 전달 기능은 사용자의 보안레벨, 양자키관리 시스템의 키 보유량 그리고 환경 구축에 따라 키 전달 시 암호체계를 변경하여 희소성 있는 양자키를 효율적으로 운영하며 보안성까지 확보하는 기능이다. 그림은 적응형 양자키 전달 시스템의 구조이다. 기존 양자키관리 시스템과의 연동은 ETSI QKD 020표준을 사용하며 상호운용성을 확보하였으며, 키 전달 시 암호체계는 TLS v1.3을 사용한다.



TB-QKMS는 Access Control을 통해 IP와 Common Name을 기반으로 양자키관리 시스템에 대한 접근 제어 기능을 한다. 또한 ETSI 020 인터페이스를 구축하여 ETSI 020 메시지를 파싱하여 키를 전달받거나, ETSI 020 형태로 메시지를 만들어서 키를 전달할 수 있다. TLS v.13. 연계 처리를 통해 키 전달 메시지를 암호화하는 전송 프로토콜을 사용하고, QKD 인터페이스를 통해 TB-QKMS에 연결되는 QKD로부터 키를 보급받을 수 있다. 마지막으로 SAE Policy 블록을 통해 사용자 ID에 따른 전송 양자키 적응형 암호화에 활용한다.

적응형 암호화 양자키 전달 기능은 TB-QKMS간 키를 전달할 때 보안레벨이 가장 높은 OTP를 사용하여 키를 전달하는 경우는 사용자의 보안레벨이 높을 경우 OTP를 사용한다. TB-QKMS간 키를 전달할 때 보안레벨이 OTP 보다는 낮지만, 양자컴퓨터의 알고리즘으로 해결하기 어려운 AES 256 알고리즘을 사용하여 키를 전달하는 경우는 두 가지 경우이다. 첫 번째는 사용자 보안 레벨이 낮을 경우 AES 256 알고리즘을 사용하고, 두 번째는 사용자 보안 레벨이 높지만 Quantum Key 보유량이 부족할 경우 AES 256 알고리즘을 사용하여 키를 전달한다. 마지막으로 RAW키를 전송하는 경우는 TB-QKMS가 모두 로컬(물리적 보안경계구역)에 있을 경우 암호화가 필요없기 때문에 암호화 없이 RAW키를 전송한다.

Ⅲ. 결론

본 논문에서는 이기종 양자암호통신망 환경에서 발생할 수 있는 병목현상으로 인한 지연발생을 예방하기 위한 적응형 양자키전달 기능을 제안하였다. 이기종 환경에서는 QKD 모듈 간 직접적인 대칭키 분배가 불가능하기 때문에 Trusted Bridge 양자키관리 시스템 구조를 선택해야하지만, 해당 구조는 키 전달을 위한 키 소모가 많이 발생할 수 있다는 한계가 존재한다. 따라서 제안하는 시스템은 사용자의 보안 레벨, 양자키관리 시스템의 키 보유량, 네트워크 환경을 종합적으로 고려하여 OTP, AES256, RAW키 전송 등 동적으로 선택한다. 이를 통해 양자키 자원을 효율적으로 활용하고, 보안 요구 수준을 충족시킬 수 있었다.
향후 연구로는 해당 시스템을 실제 양자암호통신망에 구축하여 확장성을 시험하고, 적응형 양자키관리 시스템의 성능을 테스트할 계획이다. 또한 QKD controller를 개발하여 각 도메인의 최적 양자키전달 경로를 선택할 수 있는 연구를 진행할 계획이다.

ACKNOWLEDGMENT

이 논문은 2025년도 한국과학기술정보연구원(KISTI)의 기본사업의 지원(과제번호: (KISTI)K25L5M2C2)과 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원(No.RS-2025-02263666)을 받아 수행된 연구임.

참 고 문 헌

[1] 심규석, 이원혁. “인터도메인 양자암호통신망 연동을 위한 Trusted Bridge 양자키관리 시스템 개발”, 2025년 한국통신학회 하계학술대회

[2] 심규석, 김용환, 이찬균, 이원혁. “KREONET 양자암호통신 환경에서 양자키 관리 시스템을 위한 양자키 저장 관리 모듈 설계 및 검증”, 2022년 한국통신학회 동계학술대회

[3] Shim, Kyu-Seok, Yong-Hwan Kim, and Wonhyuk Lee. "A design of secure communication architecture applying quantum cryptography." Journal of Information Science Theory and Practice 10.spc (2022): 123-134.

[4] ITU-T Y.3800-series . Quantum key distribution networks -Applications of machine learning, July 2021.

[5] ETSI GS QKD 020 2023. Protocol and data format of REST-based Interoperable Key Management System API. Group Specification Draft v0.2.1. European Telecommunications Standards Institute (ETSI), Industry Specification Groups (ISG).