양자암호통신망 사용자 확장을 위한 스마트 양자키관리 시스템 설계

심규석, 이원혁
한국과학기술정보연구원
{kusuk007, livezone}@kisti.re.kr

Design of a Smart Quantum Key Management System for Expanding Users of QKD Networks

Kyu-Seok Shim, Wonhyuk Lee
Korea Institute of Science and Technology Information

요 약

양자키분배 기반 암호통신은 점차 확장되어 가고 있으며, 현재 상용화 단계로 접어들고 있다. 하지만 사용자가 사용할 수 있는 환경이 매우 많은 조건이 있기 때문에 양자키분배 기반 암호통신을 사용할 수 있는 사용자는 많지 않다. 즉, 일부 국방망, 금융망, 연구망등에서 백본 단위에서 활용할 수 있는 기술로 극한되고 있다. 따라서 사용자가 손쉽게 양자키분배 기반 암호통신에 접근하여 사용할 수 있도록 다양한 환경에서 암호통신 서비스를 제공할 수 있어야하며, 또한 도메인에 종속되지 않는 서비스를 제공할 수 있어야한다. 본 논문은 양자암호통신망 사용자 확장을 위한 스마트 양자키 관리 시스템 구조를 제안한다. 스마트 양자키 관리 시스템은 다양한 사용자가 양자암호통신 서비스를 사용할 수 있도록 사용자에 대한 범위를 확장하고, 한종류의 장비로 종속되지 않는 인터도메인간 연동을 가능하게 한다.

Ⅰ. 서 론

최근 양자컴퓨팅 기술의 급속한 발전으로 기존 공개키 암호체계의 안전성에 대한 우려가 증가함에 따라 정보통신 환경 전반에서 양자내성 보안 기술에 대한 관심이 높아지고 있다. 특히 양자역학의 원리를 이용하여 이론적으로 무조건적 안전성을 보장하는 양자키분배(Quantum Key Distribution, QKD) 기술은 차세대 보안 통신의 핵심 기술로 주목받고 있으며, 연구단계를 넘어 점차 상용화 단계로 진입하고 있다.

그러나 현재의 양자키분배 기반 암호통신은 적용 가능한 환경이 매우 제한적이라는 한계를 지닌다. 고가의 장비 구성, 전송 거리 및 물리적 인프라 제약, 운용 복잡성 등의 이유로 인해 일반 사용자나 소규모 네트워크 환경에서의 활용은 현실적으로 어려운 상황이다. 이에 따라 양자암호통신 기술은 주로 국방망, 금융망, 연구망 등과 같은 특정 고보안 요구 환경에서 백본 네트워크 단위로 제한적으로 적용되고 있으며, 사용자 접근성과 확장성 측면에서는 한계가 존재한다. 이러한 제한적 적용은 네트워크 구성 상 보안홀을 만들게 하며, 이러한 다점은 활용성 측면에서 매우 감소되는 원인이다.

또한 기존 양자암호통신 시스템은 특정 제조사의 장비나 단일 도메인 환경에 종속되는 구조를 가진다. 즉, 이기종 양자암호통신 시스템간의 키 생성 및 키교환이 매우 어려운 구조이기 때문에 확장성의 한계를 가진다. 따라서 서로 다른 도메인 간 연동이나 이기종 장비 간 상호운용성이 충분히 고려되지 못하고 있다. 이러한 구조적 제약은 향후 양자암호통신 서비스의 대규모 확산과 상용 서비스로의 전환에 있어 중요한 장애 요소로 작용할 수 있다. 따라서 다양한 네트워크 환경과 서비스 도메인에서 사용자가 손쉽게 양자키분배 기반 암호통신을 활용할 수 있도록 보다 유연하고 확장가능한 관리 체계가 요구된다.[1-3]

본 논문에서는 이러한 문제를 해결하기 위해 양자암호통신망 사용자 확장을 위한 스마트 양자키관리 시스템 구조를 제안한다. 제안하는 스마트 양자키관리 시스템은 다양한 사용자와 서비스 환경을 고려하여 양자암호통신 서비스의 적용 범위를 확장한다. 사용자와 양자키관리 시스템간의 보안을 강화하기 위해 PQC 적용 유무에 따른 상이한 프로토콜 적용 방안을 적용한다. 또한 특정 장비나 도메인에 종속되지 않는 인터도메인 연동을 가능하게 하기 위해 사용자 레벨, 양자키보유현황, 네트워크 환경에 따라 상이한 양자키 전달 체계를 구축한다. 이를 통해 기존의 제한적인 양자암호통신 활용 환경을 개선하고, 향후 범용적인 양자암호통신 서비스 제공을 위한 기반을 마련하고자 한다.

Ⅱ. 본론

본 논문에서는 양자암호통신망 사용자 확장을 위한 스마트 양자키관리 시스템을 제안한다. 양자키관리 시스템은 양자암호통신망 구조에서 양자키분배장치로부터 키를 수신받고, 서비스노드로 양자키를 공급하는 중심 역할을 수행한다. 본 논문에서 제안하는 스마트 양자키관리 시스템은 서비스 환경을 확대하고, 보안을 강화하면서 사용자 확장을 할 수 있으며, 도메인간 종속적인 양자암호통신망의 한계를 극복함으로써 사용자간 양자암호통신 서비스를 확장할 수 있다는 장점이있다. 스마트 양자키관리 시스템의 구조는 아래 그림과 같다.

그림과 같이 양자키분배장치는 동일한 장치로 Alice와 Bob으로 구성되며, 양자역학적원리를 이용하여 동일한 대칭키를 생성하여 분배한다. 생성된 대칭키는 양자키분배장치와 연결된 양자키관리 시스템으로 저장된다. 양자키관리 시스템은 양자키를 저장하고 있다가 서비스노드에서 보안요구사항과 함께 키를 요청하게 되면 사용자 식별 및 인증 후 양자키를 공급하게 된다. 기존 양자키관리 시스템은 보안정책 상 서비스노드가 물리적보안경계구역안에 있는 것을 가정한다. 만약 양자키관리 시스템과 서비스노드간의 보안 정책이 없다면 해당 구간은 보안취약점이 될 것 이다. 따라서 스마트 양자키관리 시스템은 그림1과 같이 PQC 보안과 TLS 보안

을 적용한다. 사용자는 데이터 보안을 위해 양자키 공급 구간이 키가 직접적으로 전송되는 구간이기 때문에 PQC 알고리즘을 적용해야한다. 하지만 현재 PQC 적용이 진행중이고, 표준화 진행 중이기에 일반 TLS 프로토콜을 사용하여 암호화할 수 있도록 적용한다.[4-5]

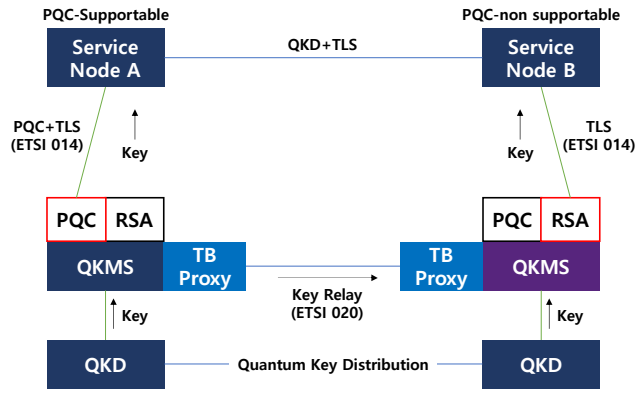

그림 1 스마트 양자키관리 시스템 구조

또한 양자키관리 시스템은 양자키분배장치가 키분배를 할 수 없을정도의 긴 구간에 대해서는 Trusted Node를 활용하여 키 전달 기능을 통해 키를 분배한다. 이는 양자키분배장치가 광원을 활용하여 키를 생성해냄으로써 거리의 한계가 있기 때문이다. 그러나 이기종 양자키관리 시스템간 양자키전달에 관련된 표준이 있으나, 많은 제품들이 적용하기 전이다. 또한 해당 표준은 인터페이스의 메시지 구조에 관련된 표준이기 때문에 보안에 대한 명시가 없다.

스마트 양자키관리 시스템은 이기종 양자키관리 시스템간의 키를 전달하기 위해 국제 표준 ETSI 020 표준을 적용하고, 또한 해당 구간 보안을 강화하기 위해 보안체계를 구축한다. 그러나 해당 구간은 인터도메인 환경에서 활용되기 때문에 양자키 활용 측면에서 효율성을 고려해야한다. 즉, 해당 구간으로 많은 양자자원을 사용하기 때문에 키 전달 요청이 증가되면 양자자원이 부족할 수 있고, 부족한 양자키 자원은 네트워크 지연으로 발생할 수 있기 때문이다.

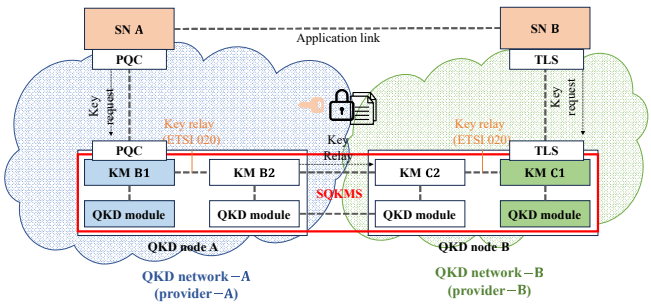

그림 2 스마트 양자키관리 시스템 동작 방식

따라서 스마트 양자키관리 시스템은 양자키 전달 시 사용자의 보안요구레벨, 양자키관리 시스템의 양자키 보유 현황, 네트워크 환경에 따라 다른 암호체계를 활용하여 양자키를 전달함으로써 양자키 자원 효율성을 증가시켰다. 스마트 양자키관리 시스템에서 적용할 수 있는 암호체계는 기존의 양자키 전달 기능에서 사용하는 보안강도가 가장 높은 OTP 암호체계와 보안강도가 OTP보다는 낮지만, 현재까지 양자컴퓨터로 해독하기 어렵다고 증명된 AES256 알고리즘, 그리고 네트워크 환경에서 이기종 양자키관리 시스템이 물리적 보안경계로 설정되어 있는 경우 암호체계가 필요없기 때문에 암호화 없이 보낼 수 있는 방안까지 설정한다.

OTP 암호방안을 사용하는 경우는 사용자의 보안요구레벨이 높을 경우 OTP 암호방안을 사용한다. 그러나 사용자의 보안요구레벨이 높지만, 양자키관리 시스템의 보유 양자키 자원이 부족할 경우 AES256 암호체계를 대체하여 사용한다. 양자키 전달 시 암호체계를 상황에 따라 다르게 선택할 수 있는 방안은 양자키 자원을 효율적으로 사용하며 이것은 네트워크 지연을 방지할 수 있는 효과가 있다.

Ⅲ. 결론

본 논문에서는 스마트 양자키관리 시스템을 제안한다. 스마트 양자키관리 시스템은 기존 양자키관리 시스템의 기능을 모두 수행하면서 서비스 노드로의 양자암호 서비스 확장 기능과 이기종 양자키 전달 기능을 수행한다. 양자암호 서비스 확장 기능은 양자암호 서비스 사용자가 PQC 암호화를 통한 양자키 공급을 요구할 시 PQC 암호체계를 이용하여 양자키를 공급하고, 만약 PQC 암호 적용이 안되는 사용자에게는 일반 TLS 프로토콜을 사용해서 양자키를 공급한다. 또한 이기종 양자키관리 시스템간의 연동을 통해 인터도메인간 양자키 전달을 가능하게 하여 서로 다른 도메인에 포함된 사용자간의 양자암호서비스를 가능하게 한다.

향후 스마트 양자키관리 시스템을 통해 국가 과학기술연구망 테스트망에 적용하여 실증할 계획이며, 실증을 통해 양자암호 서비스를 확장하고, 양자암호통신망의 효율적인 운영을 위한 스마트 양자키관리 시스템 기능 구현을 진행할 계획이다.

ACKNOWLEDGMENT

이 논문은 2026년도 한국과학기술정보연구원(KISTI)의 기본사업의 지원(과제번호: (KISTI)K26L1M3C5)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).