안정적인 양자암호통신망 서비스 제공을 위한 양자키 확장 방안

김용환, 심규석, 이은주, 이원혁
한국과학기술정보연구원
{yh.kim086, kusuk007, saranha, livezone}@kisti.re.kr

An quantum key expansion scheme for providing reliable QKDN (quantum key distribution network) service

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

요 약

최근 양자키 분배(QKD, Quantum Key Distribution) 기술은 양자 불확정성의 원리를 기반으로 암호화 프로토콜을 구현하는 안전한 통신 방법을 제공할 수 있는 방안으로써 두각을 나타태고 있다. 하지만 현재 QKD 기술을 바탕으로 안정적인 양자암호통신망 서비스를 제공하기는 충분한 양의 양자키 생성이 가능하지 않고 이와 관련된 양자키 관리 정책이 미진한 상황이다. 이에 따라, 본 논문에서는 양자키 생성 속도 대비 양자키 소비량 증대 및 QKD 계층 장애로 인한 양자키 생성 중단 등으로 인한 양자키 부족 현상을 해결하기 위하여 파생키 기반의 양자키 확장 방안에 대하여 제안한다. 또한 양자키 확장 방안과 관련된 양자키 관리 정책에 대하여 제안한다. 이를 통하여 QKD 기술 기반의 안정적인 양자암호통신망 서비스 환경을 마련하는데 기여하기를 기대한다.

Ⅰ. 서 론

최근 양자컴퓨팅의 발전과 개발에 따라 기존 보안체계는 새로운 위협에 직면하고 있으며, 이에 따라 새로운 보안체계에 대한 연구가 활발하게 이루어지고 있다. 이는 기존 보안체계인 RSA 공개키 암호화 방식이 양자컴퓨팅을 통하여 빠르게 풀어낼 수 있다는 것이 증명되었기 때문이다[1]. 이중 양자키 분배(QKD, Quantum Key Distribution) 기술은 양자 불확정성의 원리를 기반으로 암호화 프로토콜을 구현하는 안전한 통신 방법을 제공하는 방안으로써 두각을 나타태고 있다.

현재 단대단 양자키 분배를 위한 QKD 기술 및 장비는 상용화 수준으로 발전중이지만 아직까지 충분한 수준의 사용자 서비스를 제공하기에는 양자키 생성률 및 안정성 측면에서 부족함이 있다. 물론, 점진적으로 위의 이슈들이 해결되겠지만 향후 동시에 많은 수의 양자암호통신망 서비스를 안정적으로 제공하기 위해서는 장애 대응 및 양자키 확장 활용 등의 보안 책이 요구된다.

이에 따라, 본 논문에서는 먼저 표준화 문서를 기반으로 양자암호통신 계층 구조 및 양자키 관리 방안에 대하여 소개하고, 양자키 생성 속도 대비 양자키 소비량 증대 및 QKD 계층 장애로 발생되는 양자키 생성 중단 등으로 인한 양자키 부족 현상을 해결하기 위한 파생키 기반의 양자키 확장 방안 및 이와 관련된 양자키 관리 정책에 대하여 다루도록 한다.

Ⅱ. 본론

본 논문에서는 QKD 네트워크 계층, 양자키 관리 계층, 서비스 계층으로 구성되는 국내외 양자암호통신망 표준화 문서의 양자암호통신망 참조 모델을 따른다[2-3]. QKD 네트워크 계층은 QKD 장비를 통해 양자키를 생성 및 분배하고, 양자키 관리 계층은 도메인마다 양자키 관리 시스템(QKMS, Quantum Key Management System)를 두어 양자키를 서비스 계층에 제공하기 위한 양자키 생성, 삭제 등을 생애주기 관리를 포함하는 양자키 관리 역할을 수행한다. 또한 모든 QKMS는 중앙 집중 형태의 통합제어기(Q-SDN Controller)에 의하여 관리한다. 그림 1에서는 이러한 양자암호통신망 참조 모델을 보인다.

양자암호통신망 서비스 제공을 위하여 각각의 도메인내의 QKMS는 네트워크상의 모든 QKMS에 대하여 각각마다 별도의 양자키 저장소(Quantum key pool)를 관리하고 있으며, 임의의 종단간 서비스 제공을 위하여 해당 종단의 서비스키 저장소(Service key pool)를 관리한다. 한편, 양자키 저장소 크게 물리적인 QKD 장비 연결을 통하여 획득한 직접방식의 양자키와, 물리적인 QKD 장비 연결 없이 신뢰노드 기반 양자키 전달을 통하여 생성한 간적방식의 양자키로 구분할 수 있다. 본 논문에서는 양자키 전달 방식으로 ITU-T 표준[4]에서 OTP(One Time Password) 기반 방식을 준용하였다. 상세한 양자키 전달 방식에 대한 설명은 분량상의 제약으로 생략한다.

본 논문에서 각 도메인 내 QKMS s의 서로 다른 임의의 QKMS t와의 양자키 저장소를 $p_{key}(s,t)$, 총 양자키 수를 $N_{key}(s,t)$으로 정의하며 이의 임계값($t_{key}(s,t)$)은 사전에 이미 정의되어 있음을 가정한다. 또한 임의의 QKMS s와 QKMS t 사이의 n번째 서비스 세션에 대한 서비스 저장소를 $p_{service_key}(s,t,n)$으로 정의한다. 그림 1에서는 양자암호통신망 키 관리를 위한 저정소 예를 보여준다. 이 때, 각각의 QKD 도메인간의 보유 양자키의 수는 동일하다. 가령, QKMS#1의 $p_{key}(1,3)$의 키의 수와 QKMS#3의 $p_{key}(3,1)$의 키의 수는 같다.

양자키 부족 현상은 주로 크게 1) QKD 계층 장애로 인한 양자키 생성 중단과 2) $p_{ket}(s,t)$를 활용하는 양자암호통신망 서비스에 의한 양자키 소비량이 양자키 생성률보다 높아질 때 발생한다.

한편, 파생키 기반의 양자키 확장 방안은 양자키 부족 현상 해결과 별개로 QKD 계층과 양자키 관리 및 서비스 계층의 관리자가 상이할 경우 보안 측면에서 더 유용하다. 만약 QKD 계층에서 획득한 양자키를 바탕으로 양자키 관리 계층 및 서비스 계층에서의 데이터의 복호화를 원칙적으로

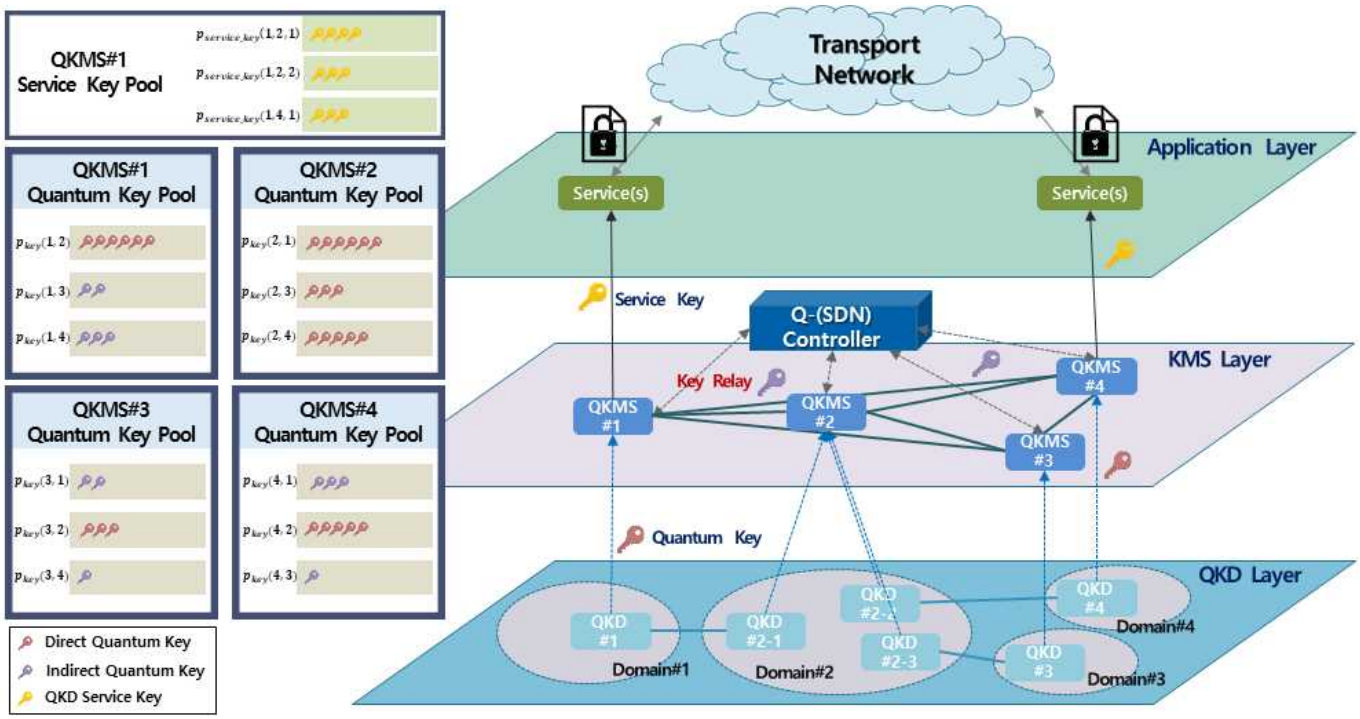

그림 1. 양자암호통신망 참조 모델 및 키 관리 예

방지할 수 있기 때문이다.

위의 이유로 인한 (1) 직접방식 양자키, (2) 간접방식 양자키를 위한 파생키 기반 양자키 확장 절차는 다음과 같다.

1) 임의의 양자키 저장소 $N_{key}(s,t) < t_{key}(s,t)$ 감지
2) QKMS s의 QRNG[5]로부터 신규 양자키 집합 생성.
   * 생성 가능한 양자키 수는 4) 절차를 통하여 전달 가능한 범위로 한정
3) $p_{ket}(s,t)$에 남아 있는 양자키 하나(key_{raw})를 선택하여 파생키 생성
   * HKDF[6]의 경우, 8000 바이트 크기로 파생키 생성 가능
4) 2)의 과정을 통하여 생성한 신규 양자키 집합을 3)의 파생키로 OTP 암호화하여 QKMS t로 전달하고 이를 수신한 QKMS t는 이를 복호화하여 신규 양자키 집합 획득
   * QKMS s와 QKMS t간의 동기화 절차 필요(key_{raw} ID, Hash 관련 정보 전달 등). 이에 대한 총괄 제어는 양자암호통신망 토폴로지 정보를 사전에 알고 있는 통합제어기를 통하여 이뤄짐
   * 직접방식의 경우, QKMS t가 인접하므로 절차 종료
   * 간접방식의 경우, QKMS t로의 양자키 전달 경로 상의 모든 QKMS 쌍에 대하여 3)-4) 과정을 수행하며 수신한 신규 양자키 집합을 최종 목적지인 QKMS t까지 전달

또한 양자암호통신망 서비스 요청이 발생하여 암호화 서비스키를 제공함에 있어서도 파생키 기반 양자키 확장을 수행할 수 있다. 해당 $p_{key}(s,t)$에서 양자키를 선택하여 HKDF 등의 방식으로 파생키를 생성하여 서비스에서 요구하는 암호화키를 제공한다. 더욱이 이 때, 서비스마다 요구하는 암호화키의 사이즈를 상이할 수 있기 때문에 $p_{key}(s,t)$에 저장되는 양자키의 사이즈는 동일하게 생성하지만 $p_{service_key}(s,t,n)$에는 서비스 요청에 부합하는 키 사이즈의 파생키를 생성하여 제공하도록 한다.

한편, 파생키 형태로 생성되는 양자키와 서비스키의 식별자는 각 QKMS에서 생성된 키의 데이터와 해당 QKMS 쌍의 식별자를 기반으로 동일한 규칙으로 UUID 형태로 생성함으로써 해당하는 QKMS 쌍이 동일한 식별자를 가지도록 한다.

Ⅲ. 결론

본 논문에서는 양자키 부족 현상을 해결하고 이와 관련된 장애에 대응하여 안정적인 양자암호통신망 서비스 환경을 마련하기 위한 양자키 확장 방안에 대하여 제안하였다. 또한 이를 위한 QKMS에서의 키 관리 정책에 대하여 제시하였다. 향후 이의 실질적인 구현을 위해서는 동시에 다수의 양자암호통신망 서비스가 제공될 때 적절한 임계값을 설정하는 것이 양자키 자원 최적화 및 서비스 QoS 지원 측면에서 중요한 이슈중 하나이기에 이에 대한 연구를 진행할 계획이다.

ACKNOWLEDGMENT

본 연구는 2021년도 한국과학기술정보연구원(KISTI) 주요 사업 과제로 수행한 것입니다

참 고 문 헌

[1] Shor, Peter W. "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer." SIAM review 41.2 (1999): 303-332.

[2] TTA TTAK.KO-01.0214, “양자암호 전달 네트워크 기능구조”, Approved in 2019-12-11

[3] ITU-T Y.3800, “Overview on networks supporting quantum key,” Approved in 2019-10-25

[4] ITU-T Y.3803, “Key management for Quantum Key Distribution network,” Proposed in 2020-12

[5] Ma, Xiongfeng, et al. "Quantum random number generation." npj Quantum Information 2.1 (2016): 1-9.

[6] Krawczyk, Hugo, and Pasi Eronen. Hmac-based extract-and-expand key derivation function (hkdf). RFC 5869, May, 2010.