양자암호통신망 양자키 확장 구조 및 장애 대응 방안

유기성, 김용환
한국과학기술정보연구원
{ksyu, yh.kim086}@kisti.re.kr

An quantum key expansion structure and fault recovery scheme in quantum cryptography communication network

Gi-Seong Yu, Yong-hwan Kim
Korea Institute of Science and Technology Information

요 약

최근 양자컴퓨팅 기술의 발전에 따른 기존 보안체계의 위협에 따라 양자암호통신 기술은 새로운 안전한 통신 방안으로써 논의되고 있다. 하지만 현재 QKD 기술은 양자암호통신망 서비스를 안정적으로 제공하기에는 아직까지 충분한 수준으로 성숙되지 않았으며 이와 관련된 양자키 관리 정책 또한 미진한 상황이다. 이에 따라, 본 논문에서는 한정적인 양자키 자원을 기반으로 상이한 보안 수준을 지닌 다수의 양자암호통신 서비스들을 안정적이고 원활하게 제공하기 위한 2-tier 양자키 관리 방안을 제안한다. 또한 안정적인 양자암호통신망 환경을 구축하기 위하여 제안한 양자키 관리 구조에서의 장애 및 양자키 부족 현상에 대한 대응 방안을 제시하고자 한다.

Ⅰ. 서 론

최근 새로운 보안체계에 대한 이슈로 부각된 양자암호통신 기술은 임의의 두 노드 사이에 양자역학적 원리를 활용하여 기밀성을 보장하는 대칭키를 생성 분배하는 양자키 분배(QKD, Quantum Key Distribution) 기술, 분배된 비밀키에 기반한 데이터 암·복호화 기술, 암호화된 데이터를 안전하게 전송하기 위한 데이터 전송 기술을 통칭하여 일컫는다.

기본적으로 QKD 기술은 물리적인 거리상의 제약을 지닌 단대단(Point to Point) 키 분배에 국한된 기술이다. 따라서, 중장거리 구간의 양자키 분배 및 네트워크상의 다수의 노드들 사이의 양자키 분배를 위해서는 신뢰노드(Trusted node)를 통한 네트워크 단위의 양자키 전달 메커니즘이 필요하다. 이를 위해서는 QKD 네트워크에 대응하는 양자키 관리 계층 망 구성을 통한 양자키 전달이 필요하다. 이에 따라, 양자암호통신 기술 기반 네트워크 보안 서비스 제공을 위하여 양자암호통신망은 QKD 계층, 양자키 관리 계층, 양자키 서비스 계층으로 구성한다[1].

현재 QKD 기술은 아직까지 양자암호통신망 서비스를 안정적으로 제공하기에 충분한 수준으로 성숙되지 않았으며 이와 관련된 양자키 관리 정책 또한 미진한 상황이다. 또한, 향후 많은 수의 다양한 양자암호통신망 서비스들을 끊김없이 안정적으로 제공하기 위해서는 서비스 보안 요구사항 수준에 따른 양자키 제공 정책 및 양자키 부족 등의 여러 장애 요인에 따른 대응 방안이 요구된다.

이에 따라, 본 논문에서는 서비스 요구사항(보안 수준, 요구 양자키 수 등)에 따른 2-tier 양자키 관리 방법을 통하여 양자키 부족 현상을 해결하고 이와 관련된 장애 대응 방안을 제시한다. 이를 통하여 안정적인 양자암호통신망 서비스 환경을 마련하고자 한다.

Ⅱ. 본론

본 논문에서 양자암호통신망 서비스 제공을 위한 양자키 저장 및 관리 구조는 그림 1과 같다. 양자키 관리 네트워크상에서 각 도메인을 담당하는 QKMS#s는 서로 다른 임의의 모든 QKMS#t마다 별도의 양자키 저장소(Quantum Key Pool, $Q_{key}(s,t)$)를 사전(Proactive Method)에 생성하여 관리한다. 그리고 이 때, 각각의 QKMS 쌍마다 주 양자키 저장소(Primary Quantum Key Pool, $Q^{p}_{key}(s,t)$)와 부 양자키 저장소(Secondary Quantum Key Pool, $Q^{s}_{key}(s,t)$)를 지니며 해당 저장소내의 양자키를 각각 $q^{p}_{key}(s,t)$. $q^{s}_{key}(s,t)$라 정의한다. 또한, 임의의 양자키 저장소를 $Q^{p}_{key}(s,t)$, $Q^{s}_{key}(s,t)$의 총 양자키 수를 $N^{p}_{key}(s,t)$, $N^{s}_{key}(s,t)$으로 정의하며 각각의 주 양자키 저장소 $Q^{p}_{key}(s,t)$와 부 양자키 저장소 $Q^{s}_{key}(s,t)$마다 요구하는 최소 양자키의 수에 대한 임계값은 각각 $th^{p}_{key}(s,t)$, $th^{s}_{key}(s,t)$로 정의한다.

한편, 임의의 QKMS s와 QKMS t 사이의 n번째 서비스 세션에 대한 요청이 발생(Reactive Method)하면 상응하는 QKD 서비스키 저장소(QKD Service Key Pool, $P_{service\_key}(s,t,n)$)를 생성하고 상응하는 양자키 저장소 $Q_{key}(s,t)$의 양자키 $q_{key}(s,t)$를 활용하여 서비스키를 생성 및 관리한다. 그리고 이 때, 정상적인 경우 네트워크 관리자가 지정한 양자암호통신 서비스 요구 보안 수준에 따라 주 양자키 $q^{p}_{key}(s,t)$와 부 양자키 $q^{s}_{key}(s,t)$ 중 선택하여 서비스키 $p_{service_key}(s,t,n)$를 제공한다.

주 양자키 저장소 $Q^{p}_{key}(s,t)$는 QKMS#s와 QKMS#t의 상응하는 QKD 도메인 간 인접 여부에 따라 직접 방식 양자키 저장소와 간접 방식 양자키 저장소로 구분된다. 직접 방식 양자키 저장소는 임의의 두 QKD 노드 간 물리적인 QKD 장비 연결을 통하여 생성하여 QKD 계층에서 각 도메인에 상응하는 양자키 관리 계층으로 전달되는 직접 방식 양자키(Direct Quantum Key)를 저장 및 관리한다. 간접 방식 양자키 저장소는 물리적인 QKD 장비 연결 없이 양자키 관리 계층에서 양자키 전달을 통하여 생성한 간접 방식 양자키(Indirect Quantum Key)를 저장 및 관리한다. 본 논문에서는 양자키 전달 방식으로 ITU-T 표준의 OTP(One Time

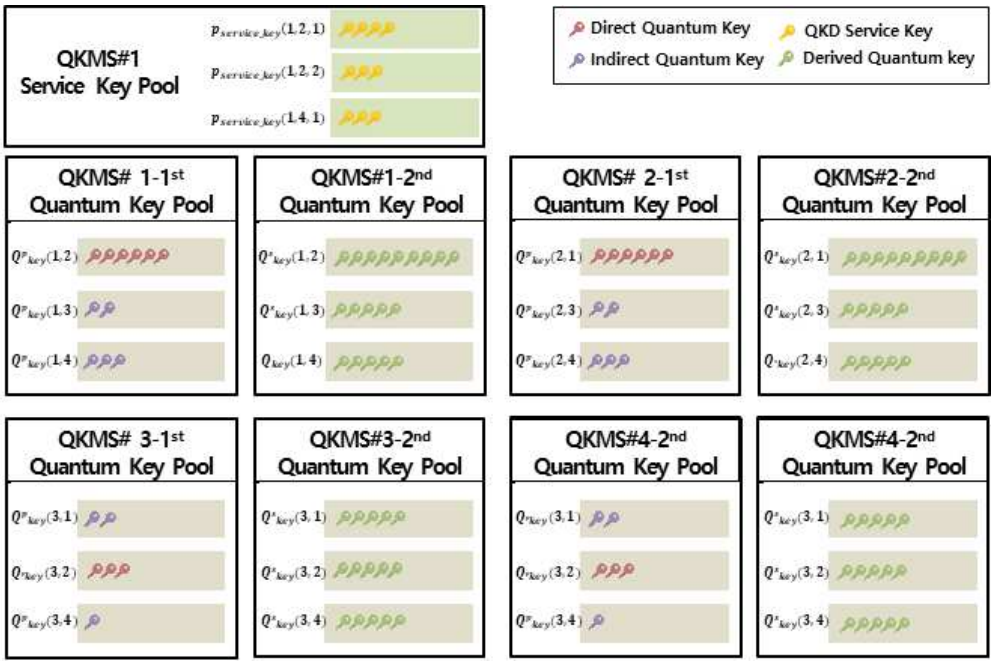

그림 1. 양자키 저장 및 관리 구조

Password) 기반 XOR(Exclusive OR) 연산 방식을 준용한다[2]. 해당 양자키 전달 방식에 따르면 $Q^p_{key}(1,4)$의 간접 방식 양자키를 생성하기 위하여 QKMS#1에서 QRNG(Quantum Random Number Generation)[3] 등의 무작위성을 보장하는 랜덤 비트 생성 방식을 통하여 양자키 $q^p_{key}(1,4)$를 생성하고, 이를 QKMS#11와 QKMS#4의 최적 경로 상의 양자키 $q^p_{key}(1,2)$, $q^p_{key}(2,4)$와 각각 XOR 연산 기반 암·복호화를 통하여 QKMS#4까지 전달한다. 즉, 간접 방식 양자키 생성을 위하여 해당 경로상의 양자키가 소모된다. 본 논문에서 최적 경로 계산에 대한 상세 방안에 대하여 다루지는 않으며 일반적으로 최소 홉 수, 보유 양자키 수량으로 가중치를 계상할 수 있음을 가정한다.

부 양자키 저장소 $Q^s_{key}(s,t)$의 $q^s_{key}(s,t)$는 양자키 부족 현상을 해결하고 이와 관련된 장애에 대응하기 위한 목적으로 생성된다. 양자키 부족 현상은 주로 QKD 계층 장애로 인한 양자키 생성 중단과 임의의 구간의 양자암호통신망 서비스에 의한 양자키 소비량이 해당 구간의 양자키 생성률보다 높아질 때 발생한다.

시스템 구동 초기 단계에서는 모든 부 양자키 저장소 $Q^s_{key}(s,t)$마다 주 양자키 $q^p_{key}(s,t)$를 활용하여 네트워크 운영자가 지정한 초기 임계값 $th^s_{key}(s,t)$까지 부 양자키 $q^s_{key}(s,t)$를 생성하며, 이후의 시스템 운영 단계에서는 기존의 양자키 $q^p_{key}(s,t)$. $q^s_{key}(s,t)$를 소모하여 각각의 부 양자키 $q^s_{key}(s,t)$를 파생키 기반 확장 형태로 생성 및 관리한다. 이 때, 주요 매개변수인 $th^s_{key}(s,t)$와 $N^s_{key}(s,t)$가 변경되면 각각의 부 양자키 저장소 $Q^s_{key}(s,t)$는 주어진 임계값 $th^s_{key}(s,t)$ 이상의 수를 상시 유지하도록 한다.

만약 임계값 $th^s_{key}(s,t)$ 미만으로 $N^s_{key}(s,t)$가 작아지면 QKMS#s와 QKMS#t 사이의 경로상의 모든 구간 <QKMS#a, QKMS#b>마다 $Q^p_{key}(a,b)$가 $N^p_{key}(s,t)$+1보다 큰 지 확인한다. 만약 조건이 만족하는 경로가 있다면, 해당 구간의 주 양자키 $q^p_{key}(a,b)$를 소모하고, 아니라면 최적 경로상의 부 양자키 $q^s_{key}(a,b)$를 소모하여 각 구간마다 동일 크기의 파생키를 생성한다. 이 때, 하나의 양자키를 활용하여 파생키 확장 방법을 통하여 수십에서 수백 배 이상의 파생키 확장 생성이 가능하다. QKMS#s는 확장된 파생키를 활용하여 OTP 기반 XOR 연산 형태로 전달 가능한 최대한의 신규 부 양자키 집합 $Q'^s_{key}(s,t)$을 무작위성을 보장하는 랜덤 비트 생성 방식을 통하여 생성한다. 신규 부 양자키 집합 $Q'^s_{key}(s,t)$은 해당 경로상의 구간에 따라 순차적으로 파생키의 OTP 기반 XOR 연산을 통하여 암·복호화되어 QKMS#t까지 전달된다. 이후 생성하고 소모된 양자키 정보를 각각의 양자키 저장소에 업데이트 한 후 다시 $N^s_{key}(s,t)$가 임계값 $th^s_{key}(s,t)$ 보다 큰 조건을 만족할 때까지 전체 과정이 반복된다.

Ⅲ. 결론

본 논문에서는 양자암호통신망 양자키 확장 구조와 장애 대응 방안을 제안하였다. 이을 통하여 QKD 기술의 물리적인 성능 제약에 따른 한정적인 양자키 자원을 기반으로 상이한 보안 수준을 지닌 다수의 양자암호통신 서비스들을 안정적이고 원활하게 제공하는 한편, 양자암호통신망에서 발생할 수 있는 서비스 장애에 대응 가능한 체계 구축 또한 달성할 수 있기를 기대한다.

ACKNOWLEDGMENT

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

참 고 문 헌

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

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

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