국가 과학기술연구망 기반 양자암호통신 구축을 위한 양자키 관리 시스템 Southbound에서의 역할 및 구조 설계

심규석, 김용환, 손일권, 이은주, 이원혁
한국과학기술정보연구원
{kusuk007, yh.kim086, d2estiny, saranha, livezone}@kisti.re.kr

Design of Sounthbound Quantum Key Management System for Role and Establish of KREONET based Quantum Cryptography and Communications

Kyu-Seok Shim, YoungHwan Kim, Ilkwon Sohn, Eunjoo Lee and Wonhyuk Lee
Korea Institute of Science and Technology Information

요 약

국가연구망 기반 양자암호통신 구축을 위해 최근 QKD(Quantum Key Distribution) 기술 및 양자 암호 키 관리 기술에 대한 연구를 활발히 진행하고 있다. 특히 국가연구망 적용을 위해 키 활용률을 높이고, 다수의 유저들이 양자암호통신을 사용하기 위해서는 양자키 관리 시스템의 역할이 중요하다. 양자키 분배 시스템으로부터 생성된 양자암호 대칭키를 양자키 관리 시스템에서 저장/할당/파생키 생성 등을 통해 생성된 대칭키를 그대로 사용하는 것보다 키 활용률을 높이고, 기존 P2P(Peer to peer)통신만 가능한 양자키 분배 시스템의 한계를 양자키 관리 시스템을 활용하여 N:N 통신이 가능하게 한다. 양자키 관리 시스템은 키를 각 노드의 암호화모듈로 보안 요구 조건에 맞게 할당하고, 관리하는 Northbound, 다른 도메인의 키 관리 시스템과 키 전달 및 키 관리 망 구축하는 East-Westbound, 그리고 양자키 분배 시스템에서 생성된 키를 받을 수 있는 Southbound로 인터페이스를 구별한다. 본 논문은 양자키 분배 시스템으로부터 대칭키를 수신하여 키를 저장하고, 파생키를 생성할 뿐만 아니라 QKD 시스템을 관리할 수 있는 Southbound의 역할 정의와 구조를 설계한 내용이다. 양자키 관리 시스템에서 Southbound 인터페이스의 영향을 미치는 KMA(Key Management Agent)와 QKDE(Quantum Key Distribution Entity) Manager 모듈의 구조 및 인터페이스에 대해 설명한다.

Ⅰ. 서 론

최근 양자컴퓨팅 관련 기술 개발에 따른 기존 암호 체계에 대한 새로운 보안 알고리즘에 관련된 연구가 진행되고 있다. 국가 과학기술연구망은 다양한 연구데이터 및 민감데이터가 전송되기 때문에 양자컴퓨터 개발에 발 맞춰 보안 알고리즘 및 보안 체계를 연구하고 있다[1]. 양자컴퓨터 환경에서 네트워크 보안을 유지하기 위해 대표적으로 PQC(Post Quantum Cryptography)와 QKD(Quantum Key Distribution)이 연구되고 있다[2]. 그 중 국가 과학기술연구망은 QKD를 기반으로 양자암호통신망을 구축하기 위해 관련된 기술을 연구하고 있다. 그러나, QKD는 상대적으로 단거리(현재 80km 내외) 통신만 가능하고, QKD의 성격 상 P2P(Peer to peer) 통신만 가능하기 때문에 다양한 유저를 확보하고, 전국적인 망 서비스를 제공하기 위해 국가 과학기술연구망에서는 이러한 단점을 해결할 수 있는 양자키 관리 시스템을 동행하여 연구하고 있다[3].

본 논문에서는 QKD 장비와 QKMS를 연동하는 Southbound에서의 역할과 구조에 대한 내용을 정의한다. 또한, QKMS를 제어, 관리, 모니터링할 수 있는 QKMS Manager 모듈과 연동되는 QKDE 장비들을 관리하고 모니터링할 수 있는 QKDE Manager에 대한 역할 및 구조도 정의한다. QKD에서 생성되는 양자 대칭키를 저장하고, 관리하는 역할을 함으로써 QKD와의 연동 인터페이스가 중요할 뿐만 아니라 키를 전달받는 메커니즘에서 보안에 대한 부분도 중요하다. QKMS의 Northbound, East-Westbound와 달리 Southbound는 표준에 대해서도 큰 범위로만 정의되어있고, 세부적인 내용이 정의되어 있지 않다. 따라서 QKMS의 Southbound 쪽에 대한 표준 내용을 참고하여 인터페이스 및 구조, 그리고 역할에 대해 정의한다.

Ⅱ. 본론

양자키 관리 시스템은 기능별로 크게 KRA(Key Relay Agent), KSA(Key Supply Agent), KMA(Key Management Agent)로 구분되고 그 외 Database, Manager, Interface 등으로 나누어진다. KRA는 QKMS에서 저장된 키를 QKMS간 전달하여 장거리에 있는 노드와 양자암호통신이 가능하게 하는 키 전달 역할을 함으로써 East-Westbound로 정의한다. KSA는 보안이 필요한 서비스에 양자키를 제공하는 모듈로 Northbound로 정의한다. 본 논문에서 다루는 Southbound는 KMA 모듈이 QKD에서 생성된 키를 수신하여 Database로 저장하는 역할을 한다.

그림 1은 QKMS의 전체 구조를 나타낸다. 해당 그림에서 KMA, QKDE Manager, QKDE Adapter 그리고 QKMS manager에 대한 구조와 역할에 대해 정의한다. 먼저 QKMS는 다수의 QKD 장비와 연동되어야 하기 때문에 1:N 으로 매핑되어야 한다. 1:N의 통신은 다수의 QKD를 한번에 관리가 가능하고, 향후 장거리 통신이 필요할 때 키전달 기능에 있어 하나의 QKMS에서 다수의 QKD를 관리하고 해당 키들을 전달할 수 있는 구조를 가져야하기 때문이다.

KMA는 QKDE Adapter를 통해 연동된 다수의 QKD 장비로부터 지속적으로 생성된 양자 대칭키를 수신한다. 수신하면서 KMA는 각 장비에 대한 ID, 생성된 시간등 대칭키, 대칭 QKD쌍을 구분할 수 있는 고유의

ID를 각 키마다 입력시켜서 저장하게 한다. 향후 보안 요구사항에 만족할 수 있는 키 길이 및 연결된 노드에게 키 전달을 하기 위해 대칭키를 구별할 수 있는 ID를 부여해야하기 때문이다. 또한 Database에 저장되어 있는 키들의 생애주기를 관리하여 저장, 조회, 삭제, 할당, 서비스키 생성등의 역할을 수행한다.

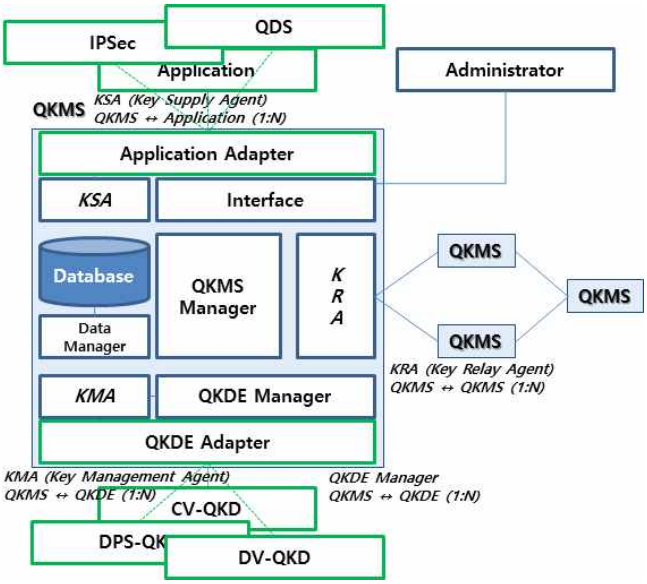

그림 1. QKMS 구조

QKMS에서 QKDE Manager의 역할은 해당 QKMS와 연결된 다수의 QKD 장비들의 상태 및 링크 상태에 대해 모니터링하고, 새로운 QKD 장비를 연결할 때 등록하는 절차 및 기존 QKD 장비를 해제할 때 삭제하는 절차를 진행한다. 또한 QKD 성능 (QBER(Quantum Bit Error Rate), Rraw)등을 조회할 수 있으며 QKD 설정, 정책 제어, 정보조회 기능을 수행한다.

QKDE Adapter는 종류가 다른 이기종의 QKD 장비를 연동하기 위한 모듈이다. 각 벤더 및 프로토콜 별로 다른 QKD 장비를 하나의 QKMS에서 관리하기 위해 다음과 같이 QKDE Adapter 모듈을 사용한다. QKDE Adapter 모듈은 ETSI QKD 014 표준을 따르며, KMA 및 QKDE Manager와 QKD 장비가 연동될 수 있도록 연동 인터페이스를 구축하는 역할을 한다.

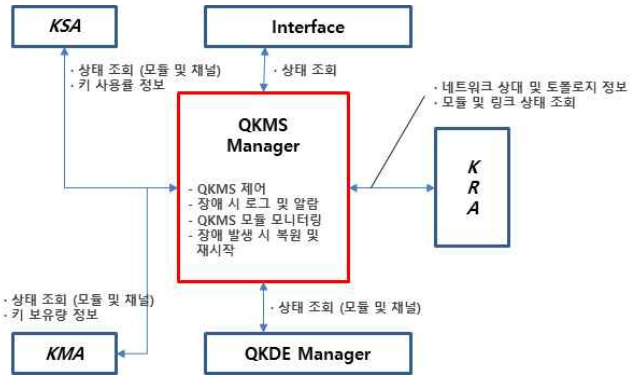

그림 2 QKMS Manager의 역할

마지막으로 QKMS 자체를 관리하고, 설정 및 제어할 수 있는 QKMS Manager는 QKMS의 구성요소를 관리한다. QKMS는 KMA, KRA, KSA, QKDE Manager등 모듈로 구성되기 때문에 각 모듈을 관리해주는 QKMS Manager가 필요하다. 각 모듈의 상태조회를 통해 장애를 감지하고, 모듈 뿐만 아니라 각 채널(링크) 상태 정보를 모니터링하여 장애를 감지한다. 이러한 각 정보를 제공하는 것은 관리자의 요청에 의해 정보를 전송하게 되며 장애가 감지될 시 재시작하는 등 자체적인 해결방안에 대한 내용을 포함한다. 그림2는 QKMS Manager의 각 모듈별 연결 및 역할에 대한 그림이다.

KMA, QKDE Manager, QKDE Adapter의 역할은 다수의 QKD로부터 생성된 양자 대칭키를 수신하여 Database에 저장하고, 각 QKD의 쌍과 시간을 입력하여 향후 KSA가 보안 요구사항에 적합하게 키를 사용할 때 적절히 제공해주는 역할을 한다. 이때 QKDE Manager는 각 QKD 장비들의 상태를 모니터링하여 장애를 판단하고, 상태에 따라 관리자에게 알림을 보낸다. 마지막으로 QKDE Adapter는 다양한 벤더와 다양한 프로토콜을 사용하는 QKD들을 하나의 QKMS에서 관리하기 위한 모듈로 표준에 따라 키를 제공받는다.

Ⅲ. 결론

본 논문에서는 국가 과학기술연구망에 양자암호통신 구축을 위한 QKMS 구조 중 QKD 장비와 연동되어 키를 수신받고, QKD 장비들과 연동 및 관리할 수 있는 Southbound의 역할 및 구조를 제안하였다. Southbound 구성 요소로는 KMA, QKDE Manager, 그리고 QKDE Adapter가 있으며, 추가로 QKMS 자체를 관리할 수 있는 QKMS Manager로 구성된다. KMA는 QKD로부터 키를 수신하여 Database로 저장하는 역할을 하고, QKDE Manager는 연동된 QKD 장비 및 채널의 상태를 모니터링하여 관리자가 상태를 확인할 수 있도록 한다. QKDE Adapter는 다양한 벤더 및 프로토콜을 사용하여 다수의 QKD를 하나의 QKMS에서 관리할 수 있게 한다. 마지막으로 QKMS Manager는 QKMS 구성요소들을 관리하며 장애 발생 시 복원 및 재시작하는 역할을 한다.

향후 연구로 해당 구성 모듈들을 설계된 내용대로 개발하여 실험을 진행한다. QKDE Adapter의 경우 지속적으로 발표되는 표준에 근거하여 개발할 예정이며, Southbound 뿐만 아니라 QKMS의 모든 구성요소를 개발하여 국가 과학기술연구망에 적용할 예정이다.

ACKNOWLEDGMENT

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

참 고 문 헌

[1] 이원혁, 석우진, 박찬진, 권우창, 손일권, 김승해, 박병연, “양자암호기반의 통신망 구축 및 성능시험 검증연구”. KNOM Review, 2019, vol.22, No.02, pp39-47

[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum Cryptography,” Rev. Mod. Phys., Vol.74, No.1, 2002, p.145

[3] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus,“Field test of quantum key distribution in the Tokyo QKD Network”, Optics Express, Vol 19, Issue 11, 2011