마르코프 결정 과정 기반 양자키 분배 네트워크 자원 관리 문제 정의

김용환, 이원혁
한국과학기술정보연구원
{yh.kim086, livezone}@kisti.re.kr

Quantum key distribution network resource management problem definition based on Markov decision process

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

요 약

양자의 불확정성의 원리를 활용하여 임의의 두 노드 사이에 대칭키를 기밀성을 보장하도록 암호키를 생성 분배하는 양자키 분배(QKD, Quantum Key Distribution) 기술에 기반한 양자암호통신은 미래 정보산업 발전의 패러다임을 바꿀 차세대 보안 기술로 주목받고 있다. 현재 양자암호통신에 관한 표준화가 ETSI, ITU-T, TTA 등을 통하여 활발하게 진행 중에 있으며, 이에 기반 한 다양한 양자암호통신망에 대한 실증 사례 들이 생겨나고 있다. 본 논문에서는 최근 많은 표준화와 실증 작업 등이 수행된 양자암호통신망에서의 핵심 자원인 양자키의 효율적인 사용에 초점을 두고 있다. 이를 위하여 마르코프 결정 과정을 통하여 양자키 분배 네트워크 자원 관리 문제를 정의함에 있어 요구되는 시스템 구성요소와 주요 고려사항에 대하여 서술한다.

Ⅰ. 서 론

양자키 분배(QKD, Quantum Key Distribution) 기술은 데이터암호화에 활용되는 양자키를 사용자 간 분배하고 관리하는 기술로써, 도청이 불가하다는 양자의 물리적 특성 (no-cloning theorem, indistinguishability 등)을 통해, 일회성패드를 현실적으로 구현할 수 있는 기술이다[1]. 하지만 QKD는 단대단 암호키 분배 기술이기 때문에 네트워크 단위의 양자키분배를 위한 방안이 요구되며, 이러한 QKD 네트워크와 전달 네트워크(Transport Network)를 결합한 종단간 사용자에게 양자키 기반 암호통신 서비스를 제공하는 네트워크를 양자암호통신망이라 한다.

현재 양자암호통신망과 관련하여 네트워크 구조, 인터페이스, QoS, 보안요구사항 등을 포함하여 구성요소와 프로토콜의 상호 운용성을 보장하고 공통 인터페이스 정의를 통하여 QKD를 네트워크에 통합하고 상용화를 촉진하기 위한 표준화가 ETSI, ITU-T, TTA 등을 통하여 활발하게 진행 중에 있다. 또한 이러한 표준에 기반 한 다양한 양자암호통신망 실증 사례 들이 국내외에서 생겨나고 있다[3].

하지만 현재의 QKD 기반 양자암호통신망들은 표준 규격 기반의 기본적인 인터페이스 기능 구현에 초점을 두고 있어 양자암호통신망에서의 핵심 자원인 양자키의 효율적인 활용 측면에서는 연구가 미진한 상황이다. 본 논문에서는 QKD 계층, 양자키 관리 네트워크 계층, 양자키 서비스 계층으로 구성되는 다계층 형태의 양자암호통신망에서 발생하는 다양한 양자키 자원 관련 이벤트들을 고려하여 양자키 자원을 효율적으로 사용하기 위한 문제를 정의하기 위한 시스템 구성요소와 주요 고려사항에 대하여 다룬다.

Ⅱ. 본론

양자암호통신망 구조는 QKD 장비와 연결된 양자 채널과 일반 채널을 통해 양자키를 생성 및 분배하는 QKD 계층, 각 도메인마다 양자키 관리 시스템(QKMS, Quantum Key Management System)를 두고 QKD 링크로 직접 연결되지 않은 노드들 사이의 양자키를 전달하는 한편, 양자키를 서비스 계층에 제공하기 위한 양자키 생성, 삭제 등을 생애주기 관리를 포함하는 양자키 관리 계층, 양자키를 기반으로 양자암호통신 서비스를 제공하는 응용 계층으로 구성된다[3].

한편, 양자암호통신망에서의 양자키 자원은 QKD 계층에서의 인접 구간 양자키 생성, 양자키 관리 계층에서의 양자키 전달, QKMS 양자키 생애주기관리, 서비스 계층에서의 양자키 요청 등 다양한 양자암호통신망에서의 양자키 자원 증감 요인에 의하여 관리 및 제어된다. 그림 1은 이러한 양자암호통신에서의 자원 증가 및 감소 요인을 보여주며, 해당 항목은 다음과 같다.

- (증가) QKD 계층에서의 인접 구간 양자키 생성(QKD 페어 구간)
- (증가) 양자키 관리 계층에서의 양자키 전달(E2E 지점)
- (감소) 양자키 관리 계층에서의 양자키 전달(양자키 전달 구간)
- (감소) QKMS Pool에서의 Lifecycle Timeout
- (감소) 서비스 계층에서의 양자키 요청(E2E 지점)

이와 관련하여 양자키 분배 네트워크 자원 관리 문제 정의를 위한 시스템에서의 양자키 자원 모델은 다음과 같다. 임의의 QKMS 노드 i, j의 Per-link key는 QKD 계층에서 생성되며 각 key pool에 저장되며, 이 때, Per-link key는 일정한 비율로 생성된다. 또한 임의의 QKMS 노드 s, d의 E2E key는 양자키 관리 계층에서 종단 경로 상의 Per-link key를 소모하여 생성되며 각 key pool에 저장된다. 임의의 양자키 서비스 발생 시, 해당하는 종단 QKMS 노드 s, d 사이의 key pool에서 서비스 요구사항에 따라 n개의 key를 꺼내어 활용하면 해당 key는 key pool에서 삭제된다. 또한 모든 key마다 생애주기를 관리하며, 만료 시 key pool에서 삭제한다.

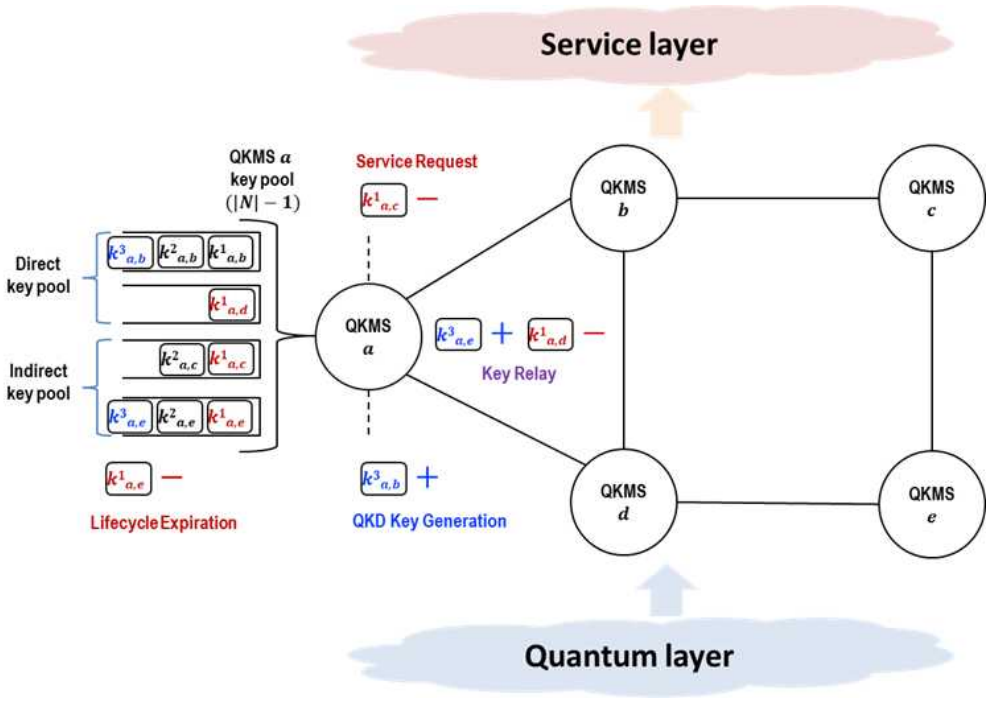

그림 1. 양자키 자원 증가/감소 요인

본 논문에서의 양자키 서비스 응답시간을 최소화하기 위하여 각 양자키마다 key pool 개념을 채택한다. Direct key pool은 QKD 계층에서의 QKD 쌍이 존재하여 QKD로부터 획득한 물리적인 방법으로 생성된 양자키 저장소이며, Indirect key pool은 QKD 계층에서 QKD 쌍이 존재하지 않아 양자키관리계층에서 양자키 기반 XOR 형태의 양자키 전달 방안을 통하여 생성된 양자키 저장소이다. 한편, 양자키 분배 네트워크 자원 관리 문제를 정의함에 있어 요구되는 시스템 구성요소는 다음과 같다.

- 정보수집부 : 네트워크 토폴로지 정보 취득, QKD 계층, 양자키 관리계층, 서비스 계층에서의 양자키 생성량 및 소비량 취득, 양자키 생성률 분포 취득, 양자키 소비률 분포 취득
- 양자키전달부 : 사전에 미리 정의된 주기마다 네트워크제어부의 제어에 따라 요구하는 Indirect key pool의 양자키를 정의된 양자키 전달 알고리즘에 따라 경로를 선택하여 전달. 이 때, 경로상의 QKMS 간 Direct key pool의 양자키를 소모
- 양자키관리부 : Direct key pool, Indirect key pool 관리 주체로 각 key pool 내의 QKD key마다 별도의 생애주기관리 수행
- 계산부 : 네트워크 제어부의 요청에 따라 AI 연산(추론-Inference/훈련-Training) 등 계산복잡도가 높은 업무를 처리하여 그 결과를 네트워크제어부에 응답
- 네트워크제어부 : 양자암호통신망의 전반적인 제어를 담당하며, 정보수집부로부터 수신한 정보를 바탕으로 양자키전달, 양자키관리 등 각 구성요소에게 필요한 제어를 수행

QKMS 양자키 저장소 임계치 설정 및 양자키 관리를 위하여 마르코프 결정 과정(MDP, Markov Decision Process) 기반의 양자키 자원 관리 문제를 정의하기 위해서는 State, Action, Reward에 대한 정의가 요구된다. State 정의 시에는 양자암호통신망 총 양자키 보유량, QKMS 별 양자키 보유량, 각 양자키풀의 양자키 보유량, 양자암호통신망에서 발생하는 양자키 생성/소모 변화량에 대한 고려가 요구된다. Action은 강화학습 모델을 통하여 얻고자 하는 결과로써 각 양자키 풀에 대한 임계값을 의미하며, 해당 값이 정해지면 양자키 전달 알고리즘에 따라 해당하는 간접 양자키 풀을 채우게 된다. Reward는 Action을 통하여 산정한 양자키 풀에 대한 임계값이 얼마나 잘 산정된 것인지를 판단하는 지표로써 실제 양자키 요구량 및 네트워크 환경에 따른 판단이 요구된다. 또한 안정적인 서비스키 제공을 위하여 예측 실패에 따른 강한 페널티를 산정할 필요가 있다. 또한 어느 정도 여유분을 두어 서비스 가용성을 확보할 필요기 있으며, 이 때, 네트워크 환경의 동적인 정도에 따라 해당 여유분을 조정할 필요가 있다.

Ⅲ. 결론

다계층에서 발생하는 다양한 이벤트에 따라 QKMS 쌍간 요구하는 양자키의 수가 상이함으로 이를 고려한 종합적인 판단을 수행 지능형 양자키 관리를 위한 MDP 문제 모델링이 요구된다. 본 논문에서는 마르코프 결정 과정을 통하여 양자키 분배 네트워크 자원 관리 문제를 정의함에 있어 요구되는 시스템 구성요소와 주요 고려사항에 대하여 서술하였다. 이를 통하여 향후 문제 정의 및 강화학습 기반의 해결방안에 초석을 제시하고자 한다.

ACKNOWLEDGMENT

본 연구는 2023년도 한국과학기술정보연구원(KISTI) 주요 사업 과제로 수행한 것입니다

참 고 문 헌

[1] Scarani, Valerio, et al. "The security of practical quantum key distribution." Reviews of modern physics 81.3 (2009): 1301.

[2] Mehic, Miralem, et al. "Quantum key distribution: a networking perspective." ACM Computing Surveys (CSUR) 53.5 (2020): 1-41.

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