양자암호통신망에서 양자키 자원 효율적 활용을 위한 라우팅 방법 연구

임현교[1], 이찬균[1], 이원혁[1], 한연희[2,*]

[1]한국과학기술정보연구원

[2]한국기술교육대학교, 미래융합공학전공

[1]{hk.lim, chankyunlee, livezon}@kisti.re.kr

[2]yhhan@koreatech.ac.kr

A Study on Research on Routing Methods for Efficient Utilization of Quantum Key Resources in Quantum Cryptography Networks

Hyun-Kyo Lim[1], Chankyun Lee[1] and Wonhyuk Lee[1], Youn-Hee Han[2,*]

[1]Korea Institute of Science and Technology Information

[2]Korea University of Technology and Education

요 약

본 논문은 양자암호통신망에서 양자키 자원의 효율적 활용을 위해 양자 자원의 다양한 척도를 고려한 라우팅 방법에 대한 연구이다. 양자암호통신망은 양자의 물리적 특성을 활용하여 도청으로부터 완벽한 안전성을 제공하는 통신을 실현한다. 양자암호통신망에서는 서비스 계층의 데이터 전달 시 양자키 관리 계층의 양자키 자원을 고려해야 한다. 이를 위해 효율적인 라우팅 방법을 고려하여 단대단 양자키 생성을 통해 양자암호통신망의 양자키 자원을 효과적으로 활용해야 한다. 본 논문에서는 제한된 양자키 환경의 양자암호 서비스를 위한 단대단 양자키 생성 시 다양한 양자암호통신망의 척도를 고려하여 양자암호통신망의 성능을 향상시키는 라우팅 방법에 대해 제안한다. 또한 제안하는 라우팅 방법의 효율성 입증을 위해 간단한 시뮬레이션 양자암호통망 환경을 구성하고 제안하는 라우팅 방법을 적용하여, 서비스 성공과 blocking 수치를 기반으로 기존의 라우팅 방법과 비교 평가를 수행한다.

Ⅰ. 서 론

최근 양자키분배 기술을 이용하여 도청으로부터 안전한 양자암호통신망을 구축 서비스하기 위한 노력이 진행 중이다[1]. 양자암호통신망은 서비스 계층의 데이터를 양자키 관리 계층의 양자키 자원을 활용하여 암호화 후 전송한다. 이때, 제한된 양자키 환경의 양자암호통신망에서 양자암호 서비스를 위한 단대단 양자키 생성 시 다양한 양자 자원의 척도를 고려하는 방법이 연구되고 있다[2][3].

본 논문은 서비스 계층의 단대단 데이터 전송을 위해 양자키 관리 계층의 양자키 생성 시 출발지 노드와 목적지 노드 간의 다양한 척도를 고려하여 경로상의 양자키를 소모해 새로운 단대단 양자키를 생성하기 위한 라우팅 방법을 제안한다. 그림 1은 서비스 계층에서 데이터 전송을 위한 요청이 생겼을 시, 양자 관리 계층은 새로운 단대단 양자키 생성을 위해 단대단 경로상의 direct 양자키를 소모하여 새로운 단대단 indirect 양자키 생성의 예시를 보여준다. 양자암호통신망에서는 양자키 분배를 위해 모듈 간 거리가 멀지 않도록 구성되어야 하기 때문에 출발지와 목적지 간에 릴레이 노드를 거쳐 데이터를 전송해야 한다. 따라서, 단대단 통신을 위한 indirect 양자키를 효율적으로 생성하기 위해서는 다양한 양자 자원의 척도를 고려하는 라우팅 방법이 제안되고 있다.

2015년 Toshiba에서는 Quantum Bit Error Rate (QBER)을 척도로 활용한 방법을 제안했다[2]. QBER은 양자 암호키 분배 시스템의 비트 오류율

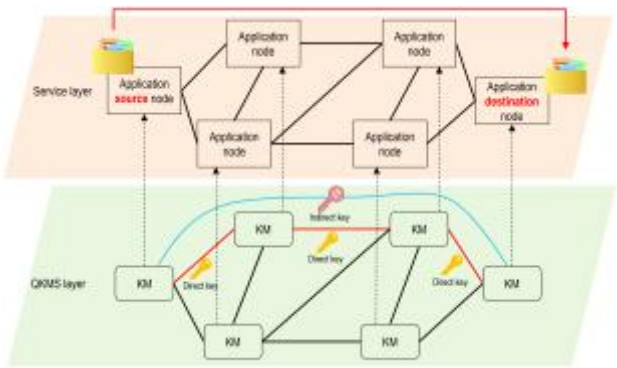

그림 1. 양자암호통신망에서 데이터 전송을 위한 단대단 양자키 생성 방법

을 계산하여 나타낸 것으로 생성되는 양자키 자원의 오류율을 나타낸다. 따라서, QBER이 낮은 경로의 direct 양자키를 소모해 indirect 양자키를 생성하는 방법과 이전의 선택된 경로의 가중치를 누적하는 라우팅 방법을 사용함으로써 단대단 경로를 한번에 고려한다. 2020년에는 DARPA에서 양자키 개수를 척도로써 고려한 라우팅 방법을 제안했다[2]. 이는 Open Shortest Path First (OSPF) 라우팅 방법을 변형한 것으로 링크의 가중치를 양자키 개수로 계산하는 방법을 제안한다. 본 논문에서는 Toshiba에서와 DARPA에서 제안하는 방법을 조합하여 QBER과 양자키 개수를 모두

고려할 수 있는 라우팅 방법을 제안한다.

본 논문은 서론에 이어 2장 본론에서는 제안하는 indirect 양자키 생성을 위한 라우팅 방법을 설명하고, 간단한 양자암호통신망 시뮬레이션을 통해 기존의 방법과 비교 분석을 하며, 3장 결론으로 논문을 마친다.

Ⅱ. 본론

단대단 양자키 생성을 위해 라우팅 경로 설정을 hop-by-hop으로 할 수 있지만, hop-by-hop에서는 경로를 구성하는 각 링크를 독립적으로 가정하므로, 최적 경로 대비 성능이 떨어지게 된다. 따라서, 본 논문에서는 양자키 라우팅 경로 결정에 있어, 출발지 노드에서 목적지 노드를 연결하는 양자키 라우팅 단대단 경로를 한번에 계산하며, 이를 통해 경로를 구성하는 링크간의 상관관계를 고려하도록 한다.

제안하는 라우팅 방법은 QBER과 현재 사용 가능한 양자키 개수를 모두 고려한 척도를 기반으로 각 링크의 가중치를 계산한다. 특히, 가중치 계산 시 hop-by-hop이 아닌 단대단 경로를 한번에 계산하기 위하여 경로 출발지부터 목적지 까지 경로 선택시 계산된 가중치를 누적하는 방법을 사용한다. 수식 (1)은 QBER과 현재 양자키 개수를 모두 고려한 라우팅 방법의 가중치 계산식이다.

$$l_i = \alpha_i \cdot w_i + (1-\alpha_i) \cdot \overline{m}_i \quad (1)$$

수식 (1)에서 l은 QBER과 양자키 개수를 모두 고려한 가중치를 나타내며, α는 QBER과 양자키 개수 각각의 가중치 파라미터이며, w_i와 $\overline{m}_i$는 각각 QBER의 누적 가중치와 normalization 한 양자키 개수의 누적 가중치를 나타낸다. QBER의 누적 가중치 w_i 계산식은 다음과 같다:

$$w_i = \frac{\sum_{n=1}^{N}(r_n \times c_n) + (r_k \times c_k)}{\sum_{n=1}^{N}(c_n + c_k)}, k \in N_i \quad (2)$$

수식 (2)에서 r은 QBER을 나타낸 것이고, c는 QBER의 측정 카운트 값을 의미한다. n은 선택된 경로상의 노드 인덱스를 의미한다. N_i는 현재 노드의 이웃들의 집합을 의미하며, k는 현재 노드(즉, 마지막 선택된 노드)의 이웃 노드들의 인덱스를 의미한다. 만약 이웃 노드의 가중치 값이 모두 동일한 경우, 각 이웃 노드의 다음 이웃 노드들까지 추가 계산하여 가장 낮은 가중치를 갖는 경로를 선택하도록 한다.

다음은 양자키 개수에 따른 누적 가중치 m_i 계산식은 다음과 같다:

$$m_i = \sum_{n=1}^{N} q_n + q_k, k \in N_i \quad (3)$$

수식 (3)에서 q는 현재 남은 양자키를 의미하며, q의 경우에는 일정 time step만큼의 양자키 개수의 가중 평균 혹은 양자키 개수의 변화량(미분) 등 양자키 개수의 변화 추이를 나타내는 척도로도 다양하게 사용할 수 있다. 그러나 본 논문에서는 단순 현재 사용 가능한 양자키의 개수를 나타낸다.

제안하는 QBER과 양자키 개수를 척도로써 모두 고려한 라우팅 방법의 효율성을 입증하기 위해 Toshiba에서 제안한 QBER만 고려한 누적 라우팅 방법[2], 그리고 DARPA에서 사용하는 변형된 OSPF 방법[3]을 비교한다. 비교를 위한 실험 환경으로 그림 1에서의 노드는 총 6개인 Butterfly 토폴로지를 기반으로 실험을 진행한다. 매 5 스텝마다 QBER을 반영하여 약 5개의 양자키가 생성되며, 초기 QBER은 1%~10%로 Uniform 분포에 따라 랜덤하게 생성된다. 양자키는 매 스텝마다 데이터 전송 서비스 요청을 위해 2개씩 소모된다. 다음 실험 결과는 10번의 시뮬레이션의 평균을 계산한 결과로 표 1과 같다.

표 1. 라우팅 척도에 따른 비교 결과

라우팅 척도	Success	Blocking
QBER	335.7	164.3
양자키 개수	348.1	151.9
QBER + 양자키 개수	**352.2**	**147.8**

Blocking은 서비스 요청이 양자키가 부족하여 서비스가 제공되지 못하는 횟수를 의미한다. 제안하는 QBER과 양자키 개수를 모두 고려한 라우팅 방법이 기존의 QBER만 고려하거나 양자키 개수만 고려하는 방법에 비해 더 좋은 성능을 보이고 있다. 이는 QBER과 양자키 개수를 모두 고려함으로써 QBER이 낮아 양자키의 개수가 적게 생산될 수 있는 경로를 되도록 피하고, 양자키의 개수가 많이 활용될 수 있는 상황을 모두 고려할 수 있어 높은 성능을 보여준다.

Ⅲ. 결론

본 논문에서는 제한된 양자키 환경의 양자암호 서비스를 위한 단대단 양자키 생성 시 QBER과 양자키 개수 척도를 모두 고려하여 양자암호통신망의 성능을 향상시키는 라우팅 방법에 대해 제안한다. 제안하는 라우팅 방법을 간단한 Butterfly 토폴로지 환경에 적용하여 제안하는 라우팅 방법이 기존의 방법에 비해 높은 성능을 보여주는 것을 증명했다. 추후 연구로 KREONET의 실제 네트워크와 동일한 환경에서 실험을 통해 효율성 증명을 진행할 것이며, 더 다양한 척도 및 다양한 제약사항을 고려한 라우팅 방법 및 강화학습 기반의 라우팅 방법 적용할 것이다.

ACKNOWLEDGMENT

본 연구는 2024년도 한국과학기술정보연구원(KISTI) 주요 사업 과제로 수행한 것입니다.

참 고 문 헌

[1] 김용환, 이원혁, “포스트 퀀텀 시대의 안전한 통신 - Quantum KREONET,” KISTI 이슈브리프 제 48호, 2022.

[2] Rika Takahashi, “Communication device, communication system and program,” Japanese Patent JP6426477, filed June 01, 2015, and issued November 21, 2018.

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