양자암호 네트워크 라우팅에서 효율성과 공정성의 균형을 위한 가중 다목적 최적화 기법

정재원, 이주형

가천대학교

deviljoe996@gachon.ac.kr, j17.lee@gachon.ac.kr

A Weighted Multi-objective Optimization Approach for Balancing Efficiency and Fairness in Quantum Key Distribution Network Routing

Jaewon Jeong, Joohyung Lee

Department of Computing (AI Major) at Gachon University

요 약

본 논문은 양자암호 네트워크의 제한된 암호 키 자원을 효율적으로 활용하기 위한 다목적 최적화 라우팅 알고리즘을 제안한다. 제안 된 알고리즘은 암호화 요청 처리량을 최대화하고 링크 간 자원 편중을 완화하여 네트워크 성능을 향상시킨다. 시뮬레이션 결과, 기존 방식 대비 낮은 요청 차단율과 높은 자원 활용 공정성을 동시에 달성함을 확인하였다.

I. 서 론

최근 양자컴퓨터의 기술이 빠르게 발전함에 따라 기존의 공개키 기반 암호화 체계는 심각한 보안 위협에 직면하고 있다. 이에 차세대 보안 통신 인프라에 대한 필요성이 급증하고 있으며, 이에 대한 유력한 대안으로 양자암호 네트워크(Quantum Cryptography Network, QCN)가 주목받고 있다[1]. 하지만 양자암호 네트워크에서는 각 링크에서 사용할 수 있는 암호 키 수량이 제한적이므로, 네트워크 전반의 자원 소모를 효율적으로 조절하는 라우팅이 필요하다. 이에 따라, 키의 낭비를 최소화하면서도 사용자 요청을 만족시킬 수 있는 효율적인 라우팅 알고리즘의 필요성이 제기된다.

본 논문에서는 QCN 상에서 암호화 요청을 효율적으로 처리하기 위한 다목적 최적화 기반 라우팅 알고리즘을 제안한다. 제안하는 알고리즘은 링크별 키 자원의 가용성과 네트워크 병목 현상을 수학적 제약 조건으로 모델링하며, 전체 네트워크의 암호화 요청 처리량을 극대화하고 링크 병목을 완화하는 라우팅 경로를 탐색한다. 이를 통해 제한된 자원 환경에서 실용적이고 효율적인 암호화 요청 라우팅 전략을 구현할 수 있음을 보인다.

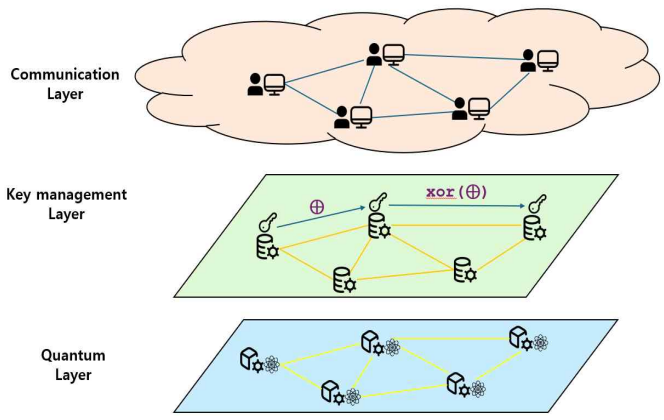

그림 1 양자암호 네트워크 (QCN) 구조도와 암호화 요청 라우팅

II. 본 론

II-I. 양자암호 네트워크

그림 1은 양자암호 네트워크에서 사용자의 암호화 요청을 처리하는 아키텍처를 보여준다. 상용화된 비대칭 공개 키 기반 데이터 암호화 방식(Rivest-Shamir-Adleman, RSA) 등과 마찬가지로, 양자암호 네트워크에서도 사용자 간의 안전한 통신을 위해 암호화 요청이 발생하며, 이때 양자암호 키가 사용된다. 이 키는 Quantum Key Distribution (QKD) 모듈을 통해 생성되며, 전자적 알고리즘이 아닌 양자역학 원리에 기반한 물리적 장비에 의해 생성된다는 점에서 기존 방식과 차별된다.

그러나 QKD 모듈은 고가이며 생성 속도에 기술적 한계가 있어, 양자 암호 키는 생산량이 매우 제한적이고 재사용이 불가능한 소모성 자원으로 간주된다[2]. 따라서 특정 링크에서 키가 소진되면 해당 링크는 더 이상 암호화 요청을 처리할 수 없으며, 이 경우 요청은 차단(blocked)된다.

기존의 라우팅 알고리즘들은 대체로 전체 네트워크 효율성 또는 각 링크의 키 잔여량을 기반으로 한 공정성 중 하나에만 치우치는 경향이 있다. 이는 제한된 암호 키 자원을 고려한 실질적 분배 전략을 수립하는 데 한계를 드러낸다. 특히, 암호화 요청이 실시간으로 동적으로 발생하는 환경에서는, 네트워크 전체 성능과 자원 병목을 종합적으로 고려한 지능적인 라우팅 전략이 필수적이다[3].

II-II. 다목적 최적화 라우팅 알고리즘 설계

본 논문에서는 네트워크 전역의 정보를 바탕으로, 일정 시간 구간 내 발생한 다수의 암호화 요청을 일괄적으로 고려하여 최적의 경로를 산출하는 다목적(weighted multi-objective) 선형계획법 (Integer Linear Programming, ILP) 기반 라우팅 알고리즘을 제안한다. 제안된 알고리즘은 (1) 암호화 요청 처리량의 최대화와 (2) 링크 간 암호 키 잔여량의 편중 완화라는 두 가지 목적을 동시에 고려하며, 이를 위해 두 목적을 하나의 통합 목적함수로 구성하고, 각 항에 가중치를 부여하여 최적화를 수행한다. 제안된 최적화 문제의 목적함수는 다음과 같이 정의된다:

$$\max\left[\sum_{d_t \in D} x_{d_t} + \beta \times \min B_C(i,j)\right] \quad \forall\,(i,j) \in L$$

여기서 $x_{d_t} \in \{0,1\}$는 암호화 요청 d_t의 처리 여부를 나타내는 이진 변수이며, 1이면 요청이 수락되고, 0이면 차단됨을 의미한다. $B_C(i,j)$는 수락된 모든 암호화 요청을 처리한 이후 링크 (i,j)에서의 암호 키 잔여량 비율을 나타내며, 전체 네트워크의 암호 키 자원 분포 상태를 반영한다. β는 암호화 요청 처리량과 링크 간 암호 키 보유 공정성이라는 두 목적 간의 중요도 균형을 조절하는 가중치로, 본 연구에서는 각 항의 범위를 고려하여 실험적으로 5,000으로 설정한다.

제안된 라우팅 알고리즘은 위 목적함수를 기반으로, 각 링크의 현재 보유 중인 암호 키 양이 충분한 경우에만 해당 경로의 암호화 요청을 처리할 수 있다는 제약 조건 하에서 경로를 결정한다. 이러한 구조는 암호화 요청 수용률을 극대화하는 동시에 일부 링크에 암호 키 사용이 과도하게 집중되는 현상을 방지함으로써 전체 네트워크 자원의 효율성과 공정성을 동시에 향상시키는 효과를 갖는다.

II-III. 제안된 암호화 요청 라우팅 알고리즘 성능 평가

제안 된 알고리즘의 성능을 검증하기 위해 QKD 모듈 단위로 경로를 선택하는 기존의 one-hop 기반 라우팅 알고리즘과 비교 평가를 수행한다. 주요 평가 지표는 두 가지로 구성된다: (1) 지속적으로 발생하는 암호화 요청 처리 과정에서, 암호 키 자원 소진으로 인해 차단된 요청 비율을 측정한다. 이는 양자암호 네트워크의 처리 성능과 사용자 서비스 품질을 평가하는 핵심 지표이다. (2) 특정 링크의 암호 키 소진 여부를 비교하여 각 알고리즘의 경로 선택과 자원 분배의 공정성을 정량적으로 분석한다.

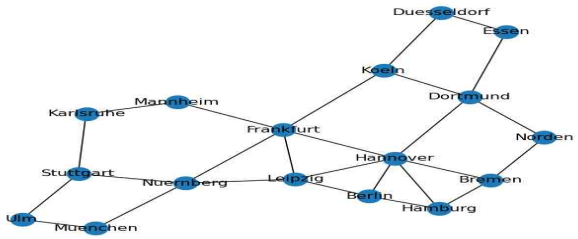

그림 2 Noble-Germany 네트워크 구조

시뮬레이션은 SNDlib[4]의 “Noble-Germany” 네트워크를 기반으로 진행하였으며, 시뮬레이션 네트워크 구조는 그림 2에 나타내었다. 구현된 네트워크는 총 17개의 QKD 모듈과 각 링크당 10,000 키 용량의 암호 키 저장소를 갖추고 있으며, 초기 상태에서는 모든 링크가 완전히 충전된 상태로 시작한다. 시뮬레이션은 총 100개의 에피소드로 구성되며, 각 에피소드에서는 모든 QKD 모듈로부터 암호 키를 생성하고 암호화 요청이 발생할 수 있다. 발생한 요청은 60초 단위로 네트워크 컨트롤러에게 전달되며, 컨트롤러는 탑재된 라우팅 알고리즘을 통해 각 요청의 경로를 결정한다. 라이브러리에서 제공하는 암호화 요청 데이터셋은 개별 요청의 크기가 매우 작아 라우팅 알고리즘의 성능 차이를 평가하기에 한계가 있다. 이에 본 평가에서는 네트워크에 극심한 자원 부족 상황을 유도하기 위해 각 암호화 요청의 크기를 20,000배 확대하여 라우팅 알고리즘의 성능을 비교한다.

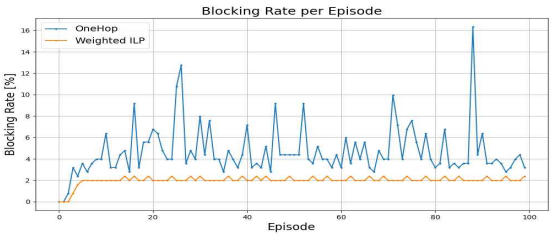

그림 3 두 라우팅 알고리즘의 암호화 요청 차단율 비교

그림 3은 제안된 알고리즘이 one-hop 기반 알고리즘보다 일관적으로 낮은 암호화 요청 차단율을 보임을 나타낸다. 특히 에피소드가 진행됨에 따라 one-hop 알고리즘은 요청 차단율이 크게 요동치는 반면, 제안된 알고리즘은 안정적인 처리 성능을 유지함을 확인할 수 있다.

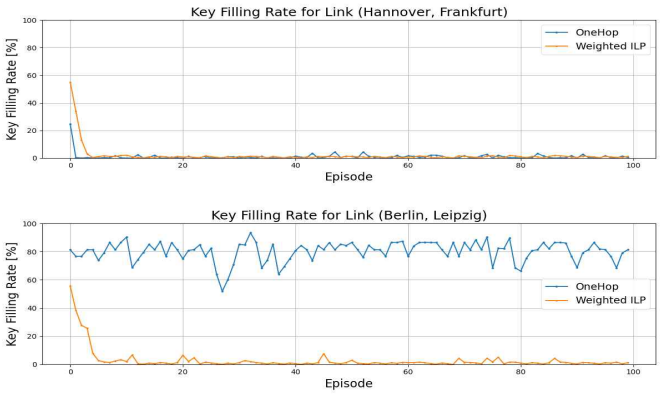

그림 4 에피소드 진행에 따른 특정 링크의 암호 키 잔여량 변화

그림 4는 특정 링크의 암호 키 사용량 변화를 비교한 결과이다. one-hop 알고리즘은 항상 거리만의 최단 경로만을 선택하여 특정 링크에 암호 키 사용이 집중되는 반면, 제안된 알고리즘은 네트워크 전반에 걸쳐 암호 키 사용을 균형 있게 분산시켜 특정 링크의 조기 소진을 효과적으로 방지하였다. 이를 통해 제안된 알고리즘이 요청 수용률과 자원 공정성을 동시에 향상시킬 수 있음을 실험적으로 입증하였다.

III. 결 론

본 논문에서는 양자암호 네트워크에서 제한된 암호 키 자원을 효율적으로 활용하기 위한 다목적 최적화 기반 라우팅 알고리즘을 제안한다. 제안된 알고리즘은 암호화 요청 처리량의 최대화와 링크 간 암호 키 사용 편중 완화라는 두 가지 상충 목표를 가중치를 부여한 단일 목적함수로 통합하여 최적화를 수행한다. 이를 통해, 네트워크 자원의 소모를 최소화하면서도 더 많은 암호화 요청을 수용할 수 있는 균형 잡힌 라우팅 전략을 설계한다. 시뮬레이션 실험을 통해 제안된 알고리즘은 기존의 one-hop 기반 라우팅 알고리즘에 비해 낮은 요청 차단율과 자원 사용의 공정성 향상을 동시에 달성함을 확인하였다.

ACKNOWLEDGMENT

본 연구는 한국과학기술정보연구원(KISTI)의 위탁연구개발과제로 수행한 것입니다. (과제번호 K25L5M2C2/P25030)

참 고 문 헌

[1] Seiler, Gavin. (2024). “Quantum Computing and the Future of Encryption”, Scholarly Review Journal. SR Online: Showcase.

[2] Emir Dervisevic, Amina Tankovic, Ehsan Fazel, Ramana Kompella, Peppino Fazio, Miroslav Voznak, and Miralem Mehic. “Quantum Key Distribution Networks -- Key Management: A Survey”, arXiv preprint arXiv:2408.04580, 2024.

[3] Johann T. et. al., “Comparison and optimization of different routing methods for meshed QKD networks using trusted nodes”, IEEE Journal of Optical Communications and Networking, Fedbruary 2024.

[4] S. Orlowski, R. Wessäly, M. Pióro, et al., “SNDlib 1.0—survivable network design library,” Networks 55, 276 - 286 (2010).