이기종 QKD 네트워크에서 자원 효율성 향상을 위한 QKD 모듈 배치 기법

임현교, 이찬균, 이원혁
한국과학기술정보연구원
{hk.lim, chankyunlee, livezone}@kisti.re.kr

Resource-Efficient QKD Module Deployment in Heterogeneous QKD Networks

Hyun-Kyo Lim, Chankyun Lee, Wonhyuk Lee
Korea Institute of Science and Technology Information

요 약

본 논문은 이기종 QKD 네트워크 환경에서 효율적인 양자키 자원의 활용을 위해 QKD 모듈의 성능에 따른 배치 기법을 제안한다. 제안하는 배치 기법은 네트워크 토폴로지의 구성에 따라 링크 매개 중심성을 기반으로 중요도가 높은 링크에 보다 고성능의 모듈을 배치하여 양자키 부족으로 인한 병목현상이 발생하지 않도록 함으로써 효율적인 양자키 활용률과 양자 보안 서비스 제공 횟수를 증가시킨다.

Ⅰ. 서 론

최근 양자 컴퓨팅 기술의 발전으로 인해 기존 공개키 기반 암호 체계의 안전성에 근본적인 위협[1]이 되고 있으며, 이에 대응하기 위한 기술로 양자키분배(Quantum key distribution, QKD) 기술을 활용한 네트워크 구성이 주목받고 있다. QKD는 양자역학 원리에 기반하여 정보 이론적으로 안전한 키 분배를 가능하게 하며, 차세대 보안 통신 인프라의 핵심 기술이 되어가고 있다.

국제 표준기구 ITU-T는 QKD 네트워크의 체계적인 구성을 위해 전반적인 네트워크 아키텍처에 대한 표준을 진행 중이며, 특히 ITU-T Y.3810 표준[2]에서는 이기종 QKD 모듈이 혼재된 네트워크 환경을 정의하고 있다. 실제 QKD 네트워크 구성에 있어서 단일 제조사의 QKD 모듈만을 활용한 구축 방식은 비용과 확장성, 상호운용성 측면에서 한계를 가지므로, 추후 구축될 QKD 네트워크에서는 서로 다른 성능 특성을 갖는 이기종 QKD 모듈의 혼합 배치가 불가피할 것으로 예상된다.

그러나 서로 다른 제조사에서 만든 QKD 모듈의 경우 서로 성능이 다르며, 이로 인해 각 QKD 링크에서 양자키 생성률이 상이하므로 네트워크 토폴로지의 특성을 고려하지 않은 QKD 모듈의 배치는 전체 양자키 자원의 효율성 및 양자 보안 서비스 제공을 저하시킬 수 있다. 따라서 네트워크 내에서 상대적으로 트래픽이 집중되는 링크를 고려하여 고성능의 QKD 모듈을 배치하고, 트래픽 집중도가 낮은 링크에는 저성능의 QKD 모듈을 배치하는 전략적 설계가 필요하다. 본 논문에서는 이기종 QKD 네트워크 환경에서 네트워크 토폴로지 특성을 고려한 QKD 모듈 배치 기법을 제안하고, 제안한 기법의 효율성 증명을 위해 COST266 토폴로지를 기반으로 성능 평가를 진행한다.

Ⅱ. 토폴로지 기반 QKD 모듈 배치 기법

본 논문에서는 ITU-T Y.3810 표준[2]에서 정의한 이기종 QKD 네트워크 구조를 기반으로 한다. QKD 네트워크의 각 QKD 링크 단위로 서로 다른 제조사 및 성능 특성을 가지는 QKD 모듈이 링크의 양 끝 단에 배치될 수 있다. 이기종 QKD 네트워크 환경에서는 QKD 모듈 간의 성능 차이에 따라 링크별 양자키 생성률이 서로 다르다. 본 논문에서는 QKD 모듈을 성능 수준에 따라 고성능, 중간 성능, 저성능의 세 가지 유형으로 분류하고, 네트워크 토폴로지 상의 각 링크 중요도에 따라 이들 모듈을 배치하는 기법을 고려한다.

이기종 QKD 네트워크에서 효율적인 양자키 자원 활용을 위해서 네트워크 내 각 링크가 전체 통신 흐름에서 차지하는 상대적 중요도를 평가해 중요도를 기반으로 링크의 양 끝단에 QKD 모듈의 성능에 따라 배치한다. 이기종 QKD 네트워크에서 QKD 링크의 중요도 지표로 링크 매개 중심성(Link betweenness centrality)을 활용한다. 링크 매개 중심성은 네트워크 내 모든 노드 쌍 간 최단 경로 중 특정 링크가 포함되는 빈도를 나타내는 지표로, 해당 링크를 경유하는 트래픽의 집중도를 반영할 수 있다. 이를 통해 이기종 QKD 네트워크 내에서 해당 QKD 링크의 중요도를 식별할 수 있다. 따라서, 매개 중심성이 높을수록 해당 링크는 높은 트래픽 수요를 담당하는 것으로 볼 수 있다.

QKD 링크 e의 중심성을 계산하기 위해 본 논문에서는 링크 매개 중심도를 활용하여 네트워크 내 모든 노드 쌍 간 최단 경로 중 특정 링크가 포함되는 비율을 나타내며, 중요도 $w(e)$는 다음과 같이 정의된다.

$$w(e) = \sum_{s \in V} \sum_{t \in V, t \neq s} \frac{\sigma_{st}(e)}{\sigma_{st}} \quad (1)$$

해당 수식에서 V는 네트워크 내 모든 노드 집합이며, e는 QKD 네트워크 내 임의의 QKD 링크를 의미한다. s, t는 서로 다른 임의의 출발지 노드와 목적지 노드($s \neq t$)를 나타내며, σ_{st}는 노드 s에서 노드 t까지 전체 최단 경로의 수를 나타내며, $\sigma_{st}(e)$는 전체 최단 경로 중 QKD 링크 e를 포함하는 경로의 수를 나타낸다.

수식 (1)을 통해 계산된 링크 중요도 $w(e)$를 기반으로 제안하는 QKD 모듈 배치 절차는 다음 Algorithm 1과 같다. 네트워크 토폴로지 정보를 기반으로 모든 QKD 링크에 대해 링크 매개 중심성을 계산한다. 계산된 링크 중요도 $w(e)$를 기준으로 QKD 링크를 내림차순 정렬한 후, 가용한 QKD 모듈을 고성능부터 중요도 순서에 따라 차례로 배치한다.

Algorithm 1 QKD deployment process

Input:
$G(V, E)$ QKD network topology
M_{high}High performance QKD module set
M_{mid}Middle performance QKD module set
M_{low}Low performance QKD module set
Output:
$Deploy(e)$ Module deployment results for each QKD link

for all $e \in E$ **do**
  $w(e) \leftarrow$ ComputeLinkBetweenness(e, G) (Equation (1))
end for

Sort QKD links E in descending order based on $w(e)$

for all $e \in E$ **do**
  if $M_{high} \neq \emptyset$ **then**
    $m_{high} \leftarrow$ Select one module from M_{high}
    $Deploy(e) \leftarrow m_{high}$
    Remove assigned module from M_{high}
  else if $M_{mid} \neq \emptyset$ **then**
    $m_{mid} \leftarrow$ Select one module from M_{mid}
    $Deploy(e) \leftarrow m_{mid}$
    Remove assigned module from M_{mid}
  else
    $m_{low} \leftarrow$ Select one module from M_{low}
    $Deploy(e) \leftarrow m_{low}$
    Remove assigned module from M_{low}
  end if
end for

return $Deploy(e)$

Ⅲ. 성능 평가

제안하는 QKD 모듈 배치 기법의 효과를 검증하기 위해 COST266 토폴로지를 기반으로 한 시뮬레이션 환경을 구성하였으며, QKD 네트워크는 총 28개의 노드와 41개의 링크로 구성된다. 이기종 QKD 모듈이 혼재하는 환경을 고려하기 위해 COST266 네트워크 토폴로지의 각 QKD 링크의 양 끝 단에 배치를 위한 고성능 QKD 모듈 14쌍, 중간 성능 QKD 모듈 14쌍, 저성능 QKD 모듈 13쌍이 있다. 제안하는 QKD 모듈 배치 기법의 성능을 검증하기 위해, 무작위 QKD 모듈 배치 전략과 비교한다.

이기종 QKD 모듈 배치 기법의 성능을 평가를 위해 키 릴레이 라우팅 알고리즘으로 DARPA QKD 네트워크에서 제안하는 OSPFv2 기반의 양자 키 릴레이 알고리즘[3]을 적용한다. 각 타임 스텝에서 사용자 네트워크의 모든 노드 쌍에 대해 하나의 양자 보안 서비스 요청이 생성되며, 매 20 타임 스텝마다 키가 생성되며, 키 생성률은 QKD 모듈의 성능에 따라 달라진다.

그림 1은 서비스 계층에서 생성된 양자 보안 서비스에 양자키 자원이 할당되어 서비스가 제공된 건수를 통해 비교한 것으로, 제안된 배치 기법을 적용해 총 1,000개의 양자 보안 서비스 중 545개의 양자 보안 서비스를 제공하였으며, 비교를 위한 무작위 배치 기법은 433개의 서비스를 제공한다. 또한, 그림 2에서는 양자 보안 서비스 제공을 위해 제안하는 배치 기법의 경우 트래픽이 집중되는 QKD 링크에 고성능 모듈을 효율적으로 배치함으로써 효율적으로 양자키를 활용할 수 있기에 무작위 배치 기법보다 7.31% 더 많은 양자키 활용률을 확인할 수 있다.

Ⅳ. 결론

본 논문에서는 이기종 QKD 네트워크 환경에서 네트워크 토폴로지를 고려한 QKD 모듈 배치 기법을 제안한다. 링크 매개 중심성을 활용하여 각 QKD 링크의 중요도를 평가하고, 이를 기반으로 성능이 상이한 이기종 QKD 모듈을 차등적으로 배치함으로써 전체 자원 효율성을 향상시킬 수 있음을 확인하였다.

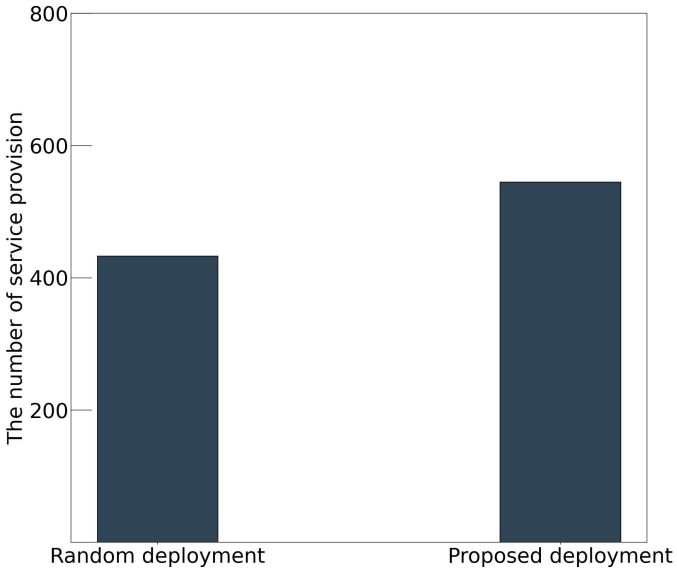

그림 1. 양자 보안 서비스 제공 횟수 비교

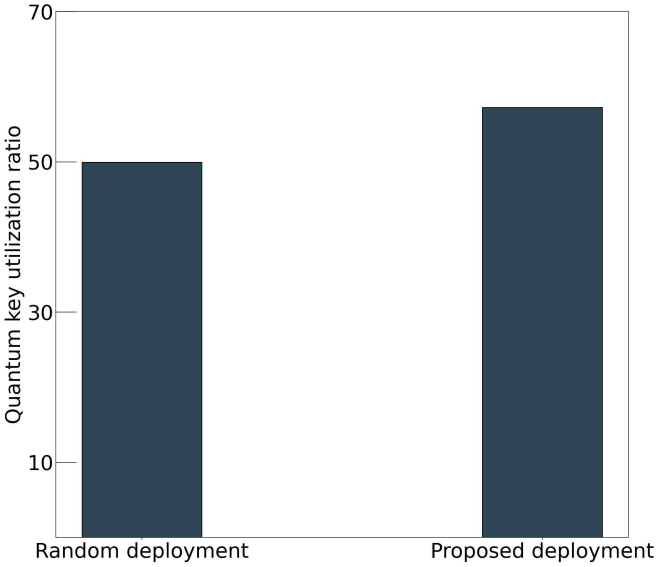

그림 2. 양자키 자원 활용률 비교

ACKNOWLEDGMENT

이 논문은 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원(No. RS-2025-02263666)과 한국과학기술정보연구원(KISTI)의 기본사업의 지원(과제번호: (KISTI)K26L1M3C5)을 받아 수행된 연구임

참 고 문 헌

[1] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," Proceedings 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, USA, 1994, pp. 124-134.

[2] ITU-T, Y.3810: Framework for Quantum Key Distribution Networks, International Telecommunication Union, Geneva, Switzerland, Dec. 2022.

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