hv photonics

IMPACT FACTOR 1.9

CITESCORE 3.5

Article

Multi-Dimensional Resource Allocation in QKD-Enabled Cross-Domain Data Center Interconnection Networks

Hao Jiang, Xiaoyu Wang, Jianwei Li, Zhonghua Liang, Yijia Zheng and Yuan Cao

Special Issue

Optimizing Communication and Routing in Optical Data Center Networks

Edited by

Dr. Jialong Li and Dr. Ao Yu

MDPI

https://doi.org/10.3390/photonics12121175

photonics

MDPI

Article

Multi-Dimensional Resource Allocation in QKD-Enabled Cross-Domain Data Center Interconnection Networks †

Hao Jiang [1], Xiaoyu Wang [1,*], Jianwei Li [1], Zhonghua Liang [1], Yijia Zheng [2] and Yuan Cao [2]

[1] China Academy of Information and Communications Technology, Beijing 100191, China
[2] School of Communications and Information Engineering, Nanjing University of Posts and Telecommunications, Nanjing 210003, China
* Correspondence: wangxiaoyu@caict.ac.cn
† This paper is an extended version of our paper, Zheng, Y.; Cao, Y.; Wang, X. Globally balanced multidimensional resource allocation for data center optical networks secured by quantum key distribution. In Proceedings of the Asia Communications and Photonics Conference, Suzhou, China, 5–8 November 2025.

Abstract

In recent years, cloud computing and edge computing have flourished, establishing data centers as pivotal hubs for information exchange. However, the security for the interconnection of these data centers faces increasingly severe challenges. Traditional cryptographic techniques face potential risks of being compromised under the threat of quantum computing, whereas quantum key distribution (QKD), which possesses information-theoretic security, provides an effective foundation for secure data center interconnection. This paper focuses on the QKD-enabled cross-domain data center interconnection network, delving into the multi-dimensional resource (i.e., computing, wavelength, and key resources) allocation problem. By constructing a QKD-enabled cross-domain data center interconnection network model, it integrates key resources with traditional computing and wavelength resources, forming a multi-dimensional resource allocation framework. Furthermore, we design two heuristic algorithms, i.e., the local balancing factor-based multi-dimensional resource allocation (LBF-MDRA) and the global balancing factor-based multi-dimensional resource allocation (GBF-MDRA) algorithms, which rationally perform virtual network function (VNF) node selection and efficiently allocate multi-dimensional resources. Simulation results indicate that the LBF-MDRA and GBF-MDRA algorithms can increase the success probability of cross-domain service requests by 24.53% and 30.91% compared to the benchmark algorithm, respectively.

Keywords: data center networks; resource allocation; virtual network function; security

Received: 14 October 2025
Revised: 27 November 2025
Accepted: 28 November 2025
Published: 29 November 2025

Citation: Jiang, H.; Wang, X.; Li, J.; Liang, Z.; Zheng, Y.; Cao, Y. Multi-Dimensional Resource Allocation in QKD-Enabled Cross-Domain Data Center Interconnection Networks. *Photonics* **2025**, *12*, 1175. https://doi.org/10.3390/photonics12121175

1. Introduction

The evolution of network technology has driven a paradigm shift in data center infrastructure, marking the onset of the big data era. This transformation has spurred a series of technological innovations, notably the emergence of data center interconnection (DCI). The deployment of DCI networks enables data centers to achieve flexible capacity scalability and agile service provisioning. Such capabilities are of critical importance, as DCI networks constitute the foundational network infrastructure that supports the communication, computing, and caching needs of modern service operations. Driven by the growing demands for cloud storage and computing, intelligent computing power, as well as mobile edge computing [1], data centers have seen widespread adoption and have evolved into the core infrastructure underpinning computing power networks.

Given their critical role as core infrastructure, data center networks have attracted significant research attention. To achieve optimal congestion avoidance and enhance overall network performance, Zhang et al. [2] proposed predictive and proactive congestion avoidance for rapid determination of optimal strategies. In addition, the RateMP algorithm [3] addressed low bandwidth utilization efficiency in data center networks through a multipath approach, featuring high burst tolerance. Yang et al. [4] developed an ILP-based traffic-aware configuration scheme for the all-optical Hyper-FleX-LION architecture to minimize port utilization and reduce operational costs in all-optical data center networks. Additionally, the unified routing for optical networks was devised in [5], which serves as a universal routing framework designed to support fast switched optical data center networks across various hardware architectures. Collectively, these studies illustrate the continuous advancement and importance of data center networks.

As hubs for information exchange, data centers store vast amounts of users' private data, rendering secure interconnection within data center networks indispensable. A critical approach to addressing this lies in adopting high-security encryption methods to ensure secure DCI. However, existing cryptographic methods fall short of delivering sufficient security in the face of quantum computers [6,7]. Specifically, the key distribution methods based on classical cryptographic systems face severe security threats at multiple levels, which significantly challenge their long-term security and usability. DCI networks can meet the communication, computing, and caching demands of future services, such as cloud-based Internet of Things (IoT) services. However, data transmitted across these networks remains susceptible to attacks such as eavesdropping.

Quantum key distribution (QKD) [8] serves as a practical approach to providing keys to users. This technology, which derives unconditional security [9,10] from quantum physical laws such as Heisenberg's uncertainty principle and the no-cloning theorem, delivers key resources that can resist quantum computing attacks. A number of studies have explored the potential application of QKD technology in data center networks. Zhu et al. [11] proposed a key-dependent heuristic resource allocation algorithm to minimize the consumption rate of key resources in QKD-enabled data center networks. Ma et al. [12] devised three efficient load balancing methods for routing, wavelength, and time slot allocation, which demonstrate effective improvements in quantum key resource efficiency and network security performance. In addition, two joint optimization algorithms have been proposed in [13], which considers the load balancing of computing and spectral resources, achieving lower blocking probability and enhanced network performance. Guo et al. [14] investigated a second-moment vliant load balancing scheme that leverages idle capacity on optical links temporarily free of burst traffic for load balancing, based on which they proposed an architectural framework for optical data center networks.

In practice, as the scale of data center racks continues to expand, the demand for secure cross-domain DCI services is on the rise. Given that each of the existing QKD protocols exhibits distinct advantages, future scenarios will see more services supporting secure DCI operating across multiple protocols in cross-domain environments. In this work, we focus on QKD-enabled cross-domain DCI networks. To address cross-domain scenarios, we investigate the allocation of multi-dimensional resources (including computing, wavelength, and key resources) to enhance the success probability of cross-domain DCI services while achieving balanced network load. The main contributions of this paper are summarized as follows.

1. A QKD-enabled cross-domain DCI network model is established. This model introduces QKD technology to ensure the security of cross-domain DCI, expanding the computing and wavelength resource allocation problem into a multi-dimensional resource allocation problem that involves computing, wavelength, and key resources.

2. We propose two types of balancing factors, namely, the local balancing factor and the global balancing factor, to constrain path selection and resource allocation for cross-domain DCI services. To achieve network load balancing, these balancing factors guide the optimal selection of service paths and virtual network function (VNF) nodes.
3. We design two heuristic algorithms, i.e., the local balancing factor-based multi-dimensional resource allocation (LBF-MDRA) algorithm and the global balancing factor-based multi-dimensional resource allocation (GBF-MDRA) algorithm. Numerical simulations demonstrate the superiority of the designed algorithms in terms of the success probability of cross-domain service requests, multi-dimensional resource utilization, and the average number of trusted relays.

The remainder of this paper is organized as follows. Section 2 introduces the network architecture. Section 3 presents a multi-dimensional resource allocation strategy based on balancing factors. Section 4 designs the LBF-MDRA and GBF-MDRA algorithms. Section 5 demonstrates the simulation results and analyzes the performance of the designed algorithms. Section 6 provides the associated discussions, and Section 7 concludes this paper.

2. Network Architecture

An architecture of QKD-enabled cross-domain DCI networks is illustrated in Figure 1. This architecture comprises the cloud layer and the edge layer, which achieve coordinated management of computing, wavelength, and key resources. Cloud nodes in the cloud layer host cloud data centers with powerful computing resources, which are interconnected via a core network. Some edge nodes in the edge layer connect to edge data centers deployed near users. These edge data centers provide limited computing resources to supplement the multi-dimensional resource allocation capabilities of cloud nodes, enabling localized content processing and caching. Content requested by users can be offloaded to nearby edge nodes for encryption processing, which avoids the communication overheads and key resource consumption caused by long-distance transmission in traditional architectures.

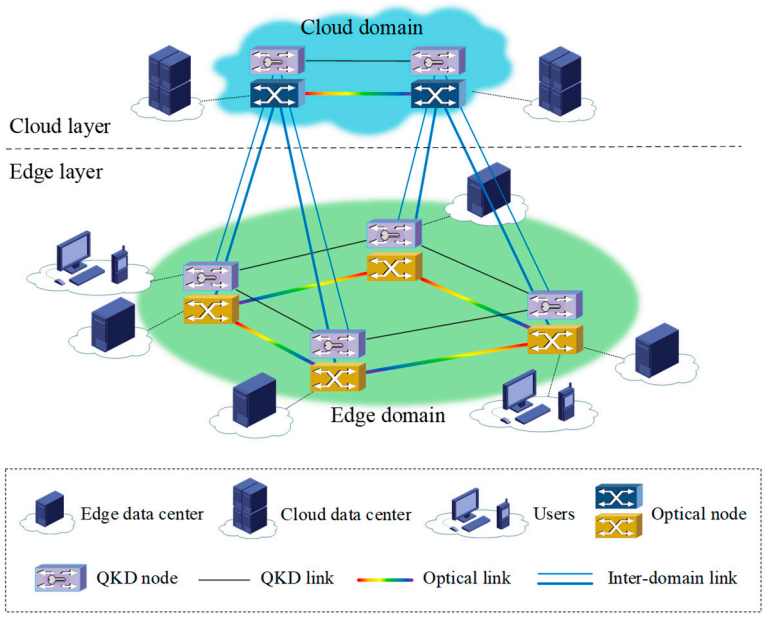

Figure 1. QKD-enabled cross-domain DCI network architecture.

In the QKD-enabled cross-domain DCI network, optical nodes and QKD nodes can be uniformly abstracted as logical network nodes, while optical links and QKD links can be

abstracted as logical network links. The optical network serves as the underlying infrastructure, responsible for providing communication resources and supporting data transmission. QKD links work in concert with classical channels to achieve key generation and secure distribution based on QKD technology, providing theoretically unconditionally secure key resources across the network. All nodes are equipped with QKD transceivers, forming converged nodes that integrate communication and encryption functions. Consequently, the QKD-enabled cross-domain DCI network not only reduces service delivery latency but also strengthens the overall security of cloud-edge data center networks through QKD-provided key resources. This approach satisfies cross-domain key distribution requirements and enables efficient allocation of multi-dimensional resources.

Telecom operators typically rely on virtualization technologies [15,16] to deliver network services within DCI networks, particularly network function virtualization (NFV). Specifically, operators can deploy VNFs [17] on servers and route services through VNFs in a sequential manner to deliver network services. To elaborate further, VNFs encompass diverse types such as firewalls, network address translation, intrusion detection systems, and load balancers [18]. VNF types are defined exclusively by their functional logic, allowing VNFs of the same type to be deployed repeatedly across different nodes [19]. For instance, a firewall can be instantiated both on the cloud nodes and the edge nodes. However, certain VNFs must be deployed in either the edge domain or the cloud domain due to their QoS requirements or resource demands. As an example, latency-sensitive VNFs are commonly deployed at the edge to meet strict delay constraints, whereas compute- or storage-intensive VNFs are usually instantiated in the cloud domain where abundant IT resources are available [20,21].

In the QKD-enabled cross-domain DCI network, the integration of VNFs with edge nodes enables rapid local data processing and response, which reduces reliance on central clouds. Furthermore, the modular design and plug-and-play characteristics of VNFs enable rapid adaptation to diverse service scenarios, which further enhances network flexibility and scalability. By comprehensively optimizing VNF selection and multi-dimensional resource allocation, QKD-enabled cross-domain DCI networks can realize efficient, flexible, and secure network operations, thereby providing robust technical support for the future development of data center networks.

3. Multi-Dimensional Resource Allocation Strategy

3.1. Problem Statement

In the QKD-enabled cross-domain DCI network, cloud and edge data centers are deployed at different locations within metropolitan area networks, interconnected via optical networks. Edge data centers are located close to users but possess limited computing resources, while cloud data centers provide substantial computing power. There are also key resources provided by QKD to ensure secure interconnection among data centers, and the massive data transmission demands wavelength resources from the optical network. Figure 2 illustrates the multi-dimensional resource allocation in a QKD-enabled cross-domain DCI network, where different types of VNFs are deployed at critical nodes. These VNFs are required and utilized by multiple cross-domain service requests, such as those illustrated between nodes E3 and C2 in Figure 2. The same type of VNF may be deployed at different network nodes. Depending on the specific VNF requirements of the cross-domain service, different node combinations emerge, thereby influencing the path selection for cross-domain services and the multi-dimensional resource allocation.

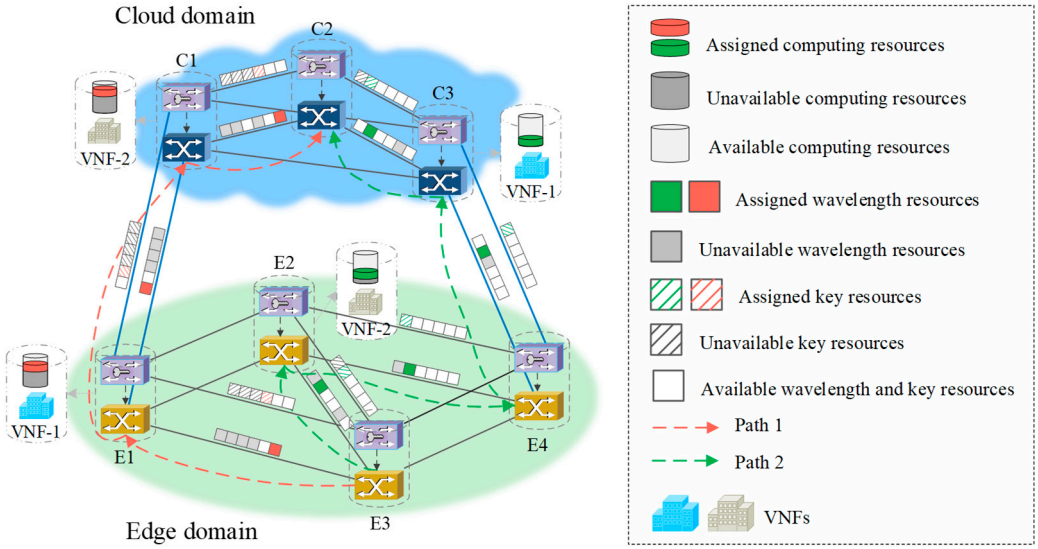

Figure 2. Illustration of multi-dimensional resource allocation in a QKD-enabled cross-domain DCI network.

Figure 2 illustrates an example of the selection of two different paths and the allocation of multi-dimensional resources resulting from distinct VNF choices. Assuming each link contains 6 wavelength resources and 6 key resources, each VNF node has 100 computing units, with source and destination nodes being E3 and C2, respectively, and the network supporting two virtual network functions, i.e., VNF-1 and VNF-2. Suppose the cross-domain service requires 1 wavelength resource (e.g., 1 wavelength channel), 1 key resource (e.g., 1 kbps key rates), 10 computing units, as well as VNF-1 and VNF-2. On Path 1, the cross-domain service selects E1 and C1 as the VNF node combination, with the path from source to destination being E3 $\rightarrow$ E1 $\rightarrow$ C1 $\rightarrow$ C2. Selecting Path 1 leaves 1 or 2 wavelength channels as well as 1 or 2 kbps key rates remaining per link, with 20 computing units remaining per VNF node. In contrast, Path 2 selects E2 and C3 to provide the required VNFs, with the path from source to destination being E3 $\rightarrow$ E2 $\rightarrow$ E4 $\rightarrow$ C3 $\rightarrow$ C2. Each hop along this path consumes 1 wavelength channel and 1 kbps key rates. Then, each link retains 3 or 4 wavelength channels as well as 4 or 5 kbps key rates, with VNF nodes retaining 70 and 80 computing units at E2 and C3, respectively. Although this option involves one additional hop due to the inclusion of a trusted relay node, it achieves a more balanced distribution of network load across computing, wavelength, and key resources. Therefore, the rational selection of VNF nodes and the optimal allocation of multi-dimensional resources are critical in realizing an efficient, flexible, and secure cross-domain DCI network.

3.2. Network Model

The modeling of a QKD-enabled cross-domain DCI network is presented in Table 1. The cloud domain and edge domain collaboratively provide multi-dimensional resources for transmission, computing, and encryption of content required by service operations. The multi-dimensional resources will be detailed hereinafter.

Table 1. Notations and definitions.

Notation	Definition
$G(N, L)$	Cross-domain DCI network topology
N	Set of nodes on the cross-domain DCI network topology
L	Set of links on the cross-domain DCI network topology
A	Set of VNFs on the cross-domain DCI network topology

Table 1. *Cont.*

Notation	Definition
n	Index of the VNF node on the cross-domain DCI network topology, $n \in N$
$C_n(t)$	Available computing resources of VNF node n on the cross-domain DCI network topology at time slot t
$C_n^{\mathrm{C}}(t)$	Available computing resources of VNF node n in the cloud domain at time slot t
$C_n^{\mathrm{E}}(t)$	Available computing resources of VNF node n in the edge domain at time slot t
$W_l(t)$	Available wavelength resources of link $l \in L$ at time slot t
$Q_l(t)$	Available key resources of link $l \in L$ at time slot t
R	Set of cross-domain service requests
$r(s_r, d_r, A_r, c_r, w_r, q_r, t_r)$	A cross-domain service request, $r \in R$
s_r	Source node of r
d_r	Destination node of r
A_r	Set of VNFs required for r
c_r	Computing resources required for r
w_r	Wavelength resources required for r
q_r	Key resources required for r
t_r	Duration of r

The QKD-enabled cross-domain DCI network proposed in this paper employs the BB84 [22] protocol in the cloud domain and the GG02 [23] protocol in the edge domain. We describe the secret key rate models for the BB84 and GG02 protocols, and then obtain the secret key rate for each link in the cross-domain DCI network using these models. The secret key rate for the BB84 protocol can be calculated as [24,25]:

$$G_{\mathrm{BB84}} = q \cdot \left\{ -Q_\mu \cdot f_e(E_\mu) \cdot H_2(E_\mu) + Q_1 \cdot [1 - H_2(e_1)] \right\} \tag{1}$$

where q represents the basis reconciliation factor, $f_e(\cdot)$ denotes the error correction efficiency, Q_μ is the overall gain of signal states, and E_μ is the quantum bit error rate. Additionally, Q_1 and e_1 are the gain and error rate of single-photon pulses, respectively, as well as $H_2(x)$ denotes the binary Shannon entropy function.

Furthermore, the secret key rate of the GG02 protocol can be calculated by [26]:

$$G_{\mathrm{GG02}} = \frac{m}{M} [\delta I_{\mathrm{AB}} - \chi_{\mathrm{bE}} - \Delta(m)] \tag{2}$$

where M and m denote the total sampling length and the block length for final key estimation, respectively. In addition, δ is the reconciliation efficiency, I_{AB} represents the Shannon mutual information between Alice and Bob, χ_{bE} indicates the Holevo bound, as well as $\Delta(m)$ is associated with the security of the privacy amplification.

Combining the secret key rate calculation formulas for the BB84 and GG02 protocols, as well as considering the relationship between secret key rate and transmission distance for different QKD protocols, the secret key rate corresponding to each QKD link can be determined. This yields the set of secret key rates for all links in the network. Accordingly, the key resource utilization in a QKD-enabled cross-domain DCI network can be defined as:

$$U_{\mathrm{Q}} = \frac{\sum\limits_{l \in L} q_l}{\sum\limits_{l \in L} Q_l(0)} \tag{3}$$

where q_l and $Q_l(0)$ represent the occupied secret key rates and the initial secret key rates on link l, respectively.

Each VNF node has a computational capacity, and the computing resources are characterized by the computing units, where each unit has a fixed computational capacity. Let $C_n^{\mathrm{C}}(0)$ and $C_n^{\mathrm{E}}(0)$ represent the initial computing resources (i.e., the number of computing units) of a cloud-domain VNF node and an edge-domain VNF node, respectively. If a computing unit is allocated to a service, it is considered unavailable. The unit becomes available again only after the service releases it. In a QKD-enabled cross-domain DCI network, the computing resource utilization can be defined as:

$$U_{\mathrm{C}} = \frac{\sum\limits_{n \in N} c_n}{\sum\limits_{n \in N^{\mathrm{C}}} C_n^{\mathrm{C}}(0) + \sum\limits_{n \in N^{\mathrm{E}}} C_n^{\mathrm{E}}(0)} \tag{4}$$

where c_n represents the occupied computing units on the VNF node n in the cloud domain or edge domain.

In addition, the dense wavelength division multiplexing (DWDM) [27] technique provides communication resources for data transmission. It enables simultaneous transmission of signals over a single optical fiber by utilizing a fine-spaced grid (e.g., 50 GHz) of different wavelengths, significantly increasing the total communication bandwidth. Hence, the wavelengths are considered communication resources. It is important to note that the wavelength continuity constraint must be followed when allocating wavelengths to services. The wavelength resource utilization in a QKD-enabled cross-domain DCI network can be defined as:

$$U_{\mathrm{W}} = \frac{\sum\limits_{l \in L} w_l}{\sum\limits_{l \in L} W_l(0)} \tag{5}$$

where w_l and $W_l(0)$ represent the occupied wavelength channels and the initial wavelength channels on link l, respectively.

The number of trusted relays can reflect both operational costs and actual security levels. A higher number of trusted relays increases costs while reducing actual security levels. For each successful cross-domain service request $r \in R_{\mathrm{S}}$ (where R_{S} denotes the set of requests successfully provisioned), with a key relay path hop count of h_r, the number of trusted relays can be defined as:

$$\gamma_r = h_r - 1 \tag{6}$$

Therefore, the average number of trusted relays for cross-domain services can be defined as:

$$\overline{\Gamma} = \frac{\sum\limits_{r \in R_{\mathrm{S}}} \gamma_r}{|R_{\mathrm{S}}|} \tag{7}$$

Moreover, the success probability (SP) of the cross-domain service requests can be determined as:

$$SP = \frac{|R_{\mathrm{S}}|}{|R|} \tag{8}$$

3.3. Balancing Factor-Based Multi-Dimensional Resource Allocation Strategy

In order to efficiently deliver cross-domain services within QKD-enabled cross-domain DCI networks, we propose the concept of the balancing factor to evaluate the impact of different VNF node selection methods on network load. On this basis, we propose a multi-dimensional resource allocation strategy, which effectively addresses two issues: how to

select appropriate data center nodes to provide the required VNFs and how to allocate multi-dimensional resources for the path from source to destination nodes.

In practice, each type of VNF can be deployed across several data centers. Let $\varphi(n)$ denote the balancing factor. Considering computing resources within data centers alongside link-based wavelength and key resources, we define two types of $\varphi(n)$, i.e., local balancing factor $\varphi_{\mathrm{LB}}(n)$ and global balancing factor $\varphi_{\mathrm{GB}}(n)$. For each candidate node that contains VNFs, $\varphi(n)$ reflects the impact of different VNF selections on the load status of a QKD-enabled cross-domain DCI network. Specifically, a smaller balancing factor indicates that selecting this VNF node would result in a relatively minor impact on the load conditions of multi-dimensional resources for new services. The calculation process for the balancing factor can be defined as follows.

$$\varphi(n) = \varphi_{\mathrm{c}}(n) + \varphi_{\mathrm{w}}(p_n) + \varphi_{\mathrm{q}}(p_n) \tag{9}$$

where $\varphi_{\mathrm{c}}(n)$, $\varphi_{\mathrm{w}}(p_n)$, and $\varphi_{\mathrm{q}}(p_n)$ represent the computing resource balancing factor, wavelength resource balancing factor, and key resource balancing factor, respectively. The calculation methods for the global balancing factor $\varphi_{\mathrm{GB}}(n)$ and the local balancing factor $\varphi_{\mathrm{LB}}(n)$ are not entirely identical. For the computing resource balancing factor, the local and global balancing factors share the same calculation method for $\varphi_{\mathrm{c}}(n)$, as formulated below.

$$\varphi_{\mathrm{c}}(n) = \frac{c_r}{C_n(t)} \tag{10}$$

However, the local balancing factor and the global balancing factor use different methods in the calculation for $\varphi_{\mathrm{w}}(p_n)$ and $\varphi_{\mathrm{q}}(p_n)$. For the local balancing factor $\varphi_{\mathrm{LB}}(n)$, the calculation methods for $\varphi_{\mathrm{w}}^{\mathrm{LB}}(p_n)$ and $\varphi_{q}^{\mathrm{LB}}(p_n)$ are defined as follows:

$$\varphi_{\mathrm{w}}^{\mathrm{LB}}(p_n) = \frac{\beta \cdot w_r}{\sum\limits_{l \in L_n} W_l(t)} \tag{11}$$

$$\varphi_{\mathrm{q}}^{\mathrm{LB}}(p_n) = \frac{\beta \cdot q_r}{\sum\limits_{l \in L_n} Q_l(t)} \tag{12}$$

where β depends on the position of the selected VNF node. If the selected VNF node is the source node or destination node of the path, then β = 1; otherwise, β = 2. L_n denotes the set of all links connected to this VNF node n.

For the global balancing factor $\varphi_{\mathrm{GB}}(n)$, the calculation methods for $\varphi_{\mathrm{w}}^{\mathrm{GB}}(p_n)$ and $\varphi_{\mathrm{q}}^{\mathrm{GB}}(p_n)$ are defined as follows:

$$\varphi_{\mathrm{w}}^{\mathrm{GB}}(p_n) = \frac{w_r}{W_{p_n}} \tag{13}$$

$$\varphi_{\mathrm{q}}^{\mathrm{GB}}(p_n) = \frac{q_r}{Q_{p_n}^{\min}} \tag{14}$$

where W_{p_n} denotes the number of common available wavelengths across all links on path p_n, and $Q_{p_n}^{\min}$ indicates the minimum available key rate across all links on path p_n.

Figure 3 provides the calculation examples for local balancing factor and global balancing factor. Available wavelength and key resources for relevant links are marked on the seven-node topology. For the cross-domain service request, s_r and d_r are nodes E1 and C2, respectively, while c_r, w_r, and q_r are 5 units, 1, and 1 kbps, respectively. Nodes E2 and C3 currently have 25 and 15 available computing units, respectively. First, compute the local balancing factor and global balancing factor at VNF node E2. For both factors, the value of $\varphi_{\mathrm{c}}(n)$ is the same. Since E2 is an intermediate node, β is set to 2. According to the

computation shown in Figure 3, the value of $\varphi_{\mathrm{LB}}(\mathrm{E2})$ is 0.74. Path 2 traverses VNF node E2. The common available wavelength on Path 2 is only one wavelength, while the minimum available key rate on this path is 2 kbps, hence the value of $\varphi_{\mathrm{GB}}(\mathrm{E2})$ is 1.70. Similarly, $\varphi_{\mathrm{LB}}(\mathrm{C3})$ and $\varphi_{\mathrm{GB}}(\mathrm{C3})$ for VNF node C3 are 0.81 and 0.92, respectively.

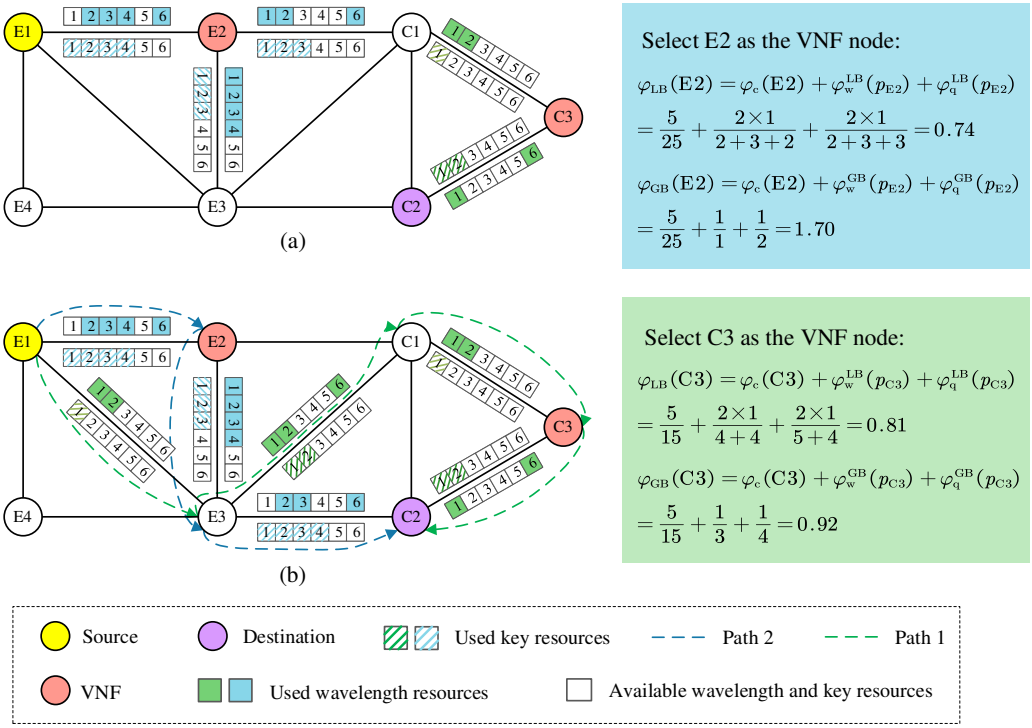

Figure 3. Examples of VNF and path selection based on the (**a**) local balancing factor and (**b**) global balancing factor.

As demonstrated in Figure 3, the VNF node selected based on the local balancing factor should be E2, because E2 has a smaller local balancing factor. This choice minimizes the impact on the load of the links connecting the associated nodes. Conversely, the VNF node selected based on the global balancing factor is C3. Although this choice increases the number of hops of the selected path by one, it minimizes the impact on the load of all links included along the path. Thus, different balancing factors directly influence VNF node selection, leading to varying network performance. In addition, for scenarios requiring two VNFs, we calculate the balancing factors for each node independently and sum them directly to obtain the combined balancing factors for the VNF node combination.

4. Heuristic Algorithm Design

Based on the QKD-enabled cross-domain DCI network model and the balancing factor-based multi-dimensional resource allocation strategy, this section designs the LBF-MDRA and GBF-MDRA algorithms to achieve the optimal selection of VNF nodes and realize network load balancing.

4.1. Local Balancing Factor-Based Multi-Dimensional Resource Allocation Algorithm

The LBF-MDRA algorithm described in Algorithm 1 primarily consists of the following steps. When a cross-domain service request arrives, it is classified based on the number of VNFs required (Lines 1–2). Notably, we consider the number of required VNFs for a cross-domain service request is 1 or 2 in this work. If the number of required VNFs is 1, lines 3–7 obtain the node set containing the VNF types requested by the cross-domain service request. Also, nodes that do not meet the computing resource conditions are

removed, and the local balancing factor is calculated for each VNF node. Lines 8–18 employ the *K*-shortest path algorithm to generate a candidate path set for node combinations, as well as traverse the candidate paths to filter those satisfying the service requirements for key and wavelength resources, then sort them by local balancing factor in descending order. Lines 19–20 select the optimal path for resource allocation and update the resource occupancy status of nodes and links along the path. If the number of VNFs required is 2, lines 27–32 obtain the node pair set for the two VNF combinations, remove invalid node pairs, and compute the local balancing factor for each node combination. In lines 33–36, the *K*-shortest path algorithm generates candidate paths (three-segment sub-path combinations) for node pairs. Paths meeting the conditions are filtered and then sorted by local balancing factor from low to high, and the optimal path is selected for resource allocation (line 37). If there are no selectable VNF nodes (or node combinations) and no available paths according to lines 21–26 and 38–41, the service request is blocked. Finally, the results of multi-dimensional resource utilization rates, service request success probability, and average number of trusted relays can be returned.

In the worst case, the time complexity for processing each cross-domain service request is $O(|A|\cdot K^3\cdot|N|\cdot(|L|+|N|\log|N|)\cdot W_l(0))$. Hence, the overall time complexity of the LBF-MDRA algorithm is $O(|R|\cdot|A|\cdot K^3\cdot|N|\cdot(|L|+|N|\log|N|)\cdot W_l(0))$.

Algorithm 1: LBF-MDRA algorithm

Input: $G(N, L)$, R, A, $C_n^{\mathrm{C}}(0)$, $C_n^{\mathrm{E}}(0)$, $Q_l(0)$, $W_l(0)$
Output: VNF selection results, routing and multi-dimensional resource allocation results, U_{C}, U_{W}, U_{Q}, $\overline{\Gamma}$, SP

1: **for** each $r \in R$ **do**
2: **if** $|A_r| = 1$ **then**
3: initialize $N_{\mathrm{a}}(n_i \in N_{\mathrm{a}})$ based on A_r;
4: **if** $C_{n_i}(t) < c_r$ **then**
5: remove n_i from set N_{a} and update N_{a};
6: **end if**
7: calculate $\varphi_{\mathrm{LB}}(n_i)$ for each VNF node n_i within N_{a};
8: **if** $N_{\mathrm{a}} \neq \varnothing$ **then**
9: **for** each $n_i \in N_{\mathrm{a}}$ **do**
10: use K-shortest path algorithm to find $K = 2$ shortest paths from s_r to n_i and n_i to d_r respectively; combine the sub-paths to generate 2×2 kinds of paths and insert them into the candidate path set P;
11: **end for**
12: **for** each $p_j \in P$ **do**
13: **if** $Q_{p_j}^{\min} < q_r$ **then**
14: remove p_j from set P and update P;
15: **end if**
16: **if** $W_{p_j} < w_r$ **then**
17: remove p_j from set P and update P;
18: **end for**
19: **if** $P \neq \varnothing$ **then**
20: select the path that has the smallest φ_{LB} and the least hops to establish the cross-domain service; update the computing, wavelength, and key resource occupancies in the network; $R_{\mathrm{S}} \leftarrow R_{\mathrm{S}} + 1$;

Algorithm 1: *Cont.*

```
            else
               the cross-domain service request has failed;
            end if
          else
            the cross-domain service request has failed;
          end if
        else if |A_r| = 2 then
          initialize N_b((n_i^1, n_i^2) ∈ N_b) based on A_r;
          if C_{n_i^1}(t) < c_r and C_{n_i^2}(t) < c_r then
            remove (n_i^1, n_i^2) from set N_b and update N_b;
          end if
          calculate φ_LB(n_i^1), φ_LB(n_i^2), φ_LB(n_i^1, n_i^2) ← φ_LB(n_i^1) + φ_LB(n_i^2);
          if N_b ≠ ∅ then
            for each (n_i^1, n_i^2) ∈ N_b do
              use K-shortest path algorithm to find K = 1 shortest paths from s_r to n_i^1,
              n_i^1 to n_i^2 and n_i^2 to d_r respectively; combine the sub-paths to generate
              the final path and insert it into the candidate path set P;
            end for
            call lines 12 to 23 in Algorithm 1;
          else
            the cross-domain service request has failed;
          end if
        end if
      end for
      return U_C, U_W, U_Q, Γ̄, SP ← |R_S|/|R|, VNF selection results, as well as routing
      and multi-dimensional resource allocation results.
```

4.2. Global Balancing Factor-Based Multi-Dimensional Resource Allocation Algorithm

The procedure of the GBF-MDRA algorithm is shown in Algorithm 2. Unlike the LBF-MDRA algorithm, the GBF-MDRA algorithm uses a global balancing factor to rank candidate paths. In contrast to the local balancing factor, which focuses solely on the multi-dimensional resource usage of VNF nodes and all their connected links, the global balancing factor prioritizes the overall multi-dimensional resource utilization of the path. It calculates the multi-dimensional resource usage for each segment of the path, disregarding links unrelated to the path. When a cross-domain service request arrives, it is classified based on the number of VNFs required. If the VNF requirement is 1, retrieve the node set containing the requested VNF types for the cross-domain service request and remove nodes that fail to meet the conditions (line 3). Lines 5 employs the *K*-shortest path algorithm to generate a candidate path set for node combinations. By traversing the candidate paths, the algorithm filters out paths where both key and wavelength resources can satisfy the cross-domain service requirements. Lines 6–9 compute the global balancing factor for each path in the candidate path set, then sort the paths in ascending order of the factor value and hop count. The optimal path is selected for resource allocation, and the resource occupancy states of nodes and links along the path are updated. If the VNF requirement is 2, line 17 obtains the node combination set for the two VNFs and removes invalid combinations. Lines 18–22 employ the *K*-shortest path algorithm to generate candidate paths (three-segment sub-path combinations) for node pairs, filtering paths that meet the conditions. Lines 23–26 compute the global balancing factor for each path in the candidate

path set, then sort the paths in ascending order of their factor values and hop counts, and select the optimal path for resource allocation. If no selectable VNF nodes (or node combinations) and available paths exist according to lines 10–15 and 27–33, the service cannot be provisioned. Finally, the results of multi-dimensional resource utilization rates, service request success probability, and average number of trusted relays can be returned.

The worst-case time complexity for processing each cross-domain service request is $O(|A|\cdot K^3\cdot|N|\cdot|L|\cdot(|L|+|N|\log|N|)\cdot W_l(0))$. Hence, the overall time complexity of the GBF-MDRA algorithm is $O(|R|\cdot|A|\cdot K^3\cdot|N|\cdot|L|\cdot(|L|+|N|\log|N|)\cdot W_l(0))$.

Algorithm 2: GBF-MDRA algorithm

Input: $G(N, L)$, R, A, $C_n^{\mathrm{C}}(0)$, $C_n^{\mathrm{E}}(0)$, $Q_l(0)$, $W_l(0)$
Output: VNF selection results, routing and multi-dimensional resource allocation results, U_{C}, U_{W}, U_{Q}, $\overline{\Gamma}$, SP

1: **for** each $r \in R$ **do**
2: **if** $|A_r| = 1$ **then**
3: call lines 3 to 6 in **Algorithm 1**;
4: **if** $N_{\mathrm{a}} \neq \varnothing$ **then**
5: call lines 9 to 18 in **Algorithm 1**;
6: **if** $P \neq \varnothing$ **then**
7: calculate $\varphi_{\mathrm{GB}}(n_i)$ for each VNF node n_i within N_{a};
8: select the path with the VNF node that has the smallest φ_{GB} and the least hops to establish the cross-domain service;
9: update the computing, wavelength, and key resource occupancies in the network; $R_{\mathrm{S}} \leftarrow R_{\mathrm{S}} + 1$;
10: **else**
11: the cross-domain service request has failed;
12: **end if**
13: **else**
14: the cross-domain service request has failed;
15: **end if**
16: **else if** $|A_r| = 2$ **then**
17: call lines 28 to 31 in **Algorithm 1**;
18: **if** $N_{\mathrm{b}} \neq \varnothing$ **then**
19: **for** each $(n_i^1, n_i^2) \in N_{\mathrm{b}}$ **do**
20: use K-shortest path algorithm to find $K = 1$ shortest paths from s_r to n_i^1, n_i^1 to n_i^2 and n_i^2 to d_r respectively; combine the sub-paths to generate the final path and insert it into the candidate path set P;
21: **end for**
22: call lines 12 to 18 in **Algorithm 1**;
23: **if** $P \neq \varnothing$ **then**
24: calculate $\varphi_{\mathrm{GB}}(n_i^1)$, $\varphi_{\mathrm{GB}}(n_i^2)$, $\varphi_{\mathrm{GB}}(n_i^1, n_i^2) \leftarrow \varphi_{\mathrm{GB}}(n_i^1) + \varphi_{\mathrm{GB}}(n_i^2)$;
25: select the path with the VNF nodes that has the smallest φ_{GB} and the least hops to establish the cross-domain service;
26: update the computing, wavelength, and key resource occupancies in the network; $R_{\mathrm{S}} \leftarrow R_{\mathrm{S}} + 1$;
27: **else**
28: the cross-domain service request has failed;
29: **end if**

Algorithm 2: *Cont.*

else
  the cross-domain service request has failed;
end if
end if
end for
return U_C, U_W, U_Q, $\overline{\Gamma}$, $SP \leftarrow |R_S|/|R|$, VNF selection results, as well as routing and multi-dimensional resource allocation results.

5. Evaluation and Analysis

This section evaluates the applicability and effectiveness of the LBF-MDRA and GBF-MDRA algorithms in different scenarios through simulations. Three distinct VNF demand ratio scenarios are considered, i.e., the single-VNF/dual-VNF demand ratios of 20%/80%, 50%/50%, and 80%/20%. For comparison purposes, the multi-dimensional resource joint allocation (MRJA) algorithm proposed in [28] is adopted as the benchmark algorithm. As shown in Figure 4, the simulation employs a USNET topology, which divides 24 nodes and 43 links into cloud and edge domains [29]. To implement QKD, the BB84 protocol is used for cloud-domain links and inter-domain links, while the GG02 protocol is applied for edge-domain links. The QKD-related assumptions/parameters of the BB84 and GG02 protocols used to calculate key rates are derived from [30,31], respectively, which are listed in Table 2. Notably, the LBF-MDRA algorithm and GBF-MDRA algorithm mainly optimize the multi-dimensional resource allocation and routing selection for cross-domain services. They do not enhance or weaken the security of the QKD process itself. The information-theoretic security of the BB84 and GG02 protocols is guaranteed by the principles of quantum physics. In addition, each trusted relay is assumed to be protected against any intrusion or attack, and we also analyze the average number of trusted relays in Section 5.3 to discuss the practical security level of cross-domain services. The key-usage model (e.g., one-time-pad, symmetric key lifetimes, and session key refresh) can be flexibly determined by the cross-domain services, which may affect the required key resources characterized by the key rates. For different key-usage models, the encryption algorithms used are not the focus of this paper, but we consider a wide range of key rate requirements of [10, 100] kbps. Other simulation parameters are listed in Table 3.

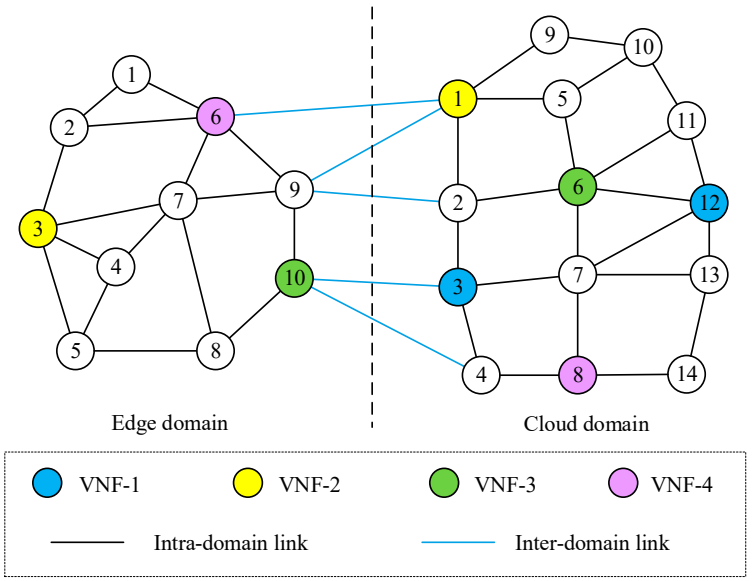

Figure 4. Network topology used in simulations.

Table 2. QKD-related assumptions/parameters of the BB84 and GG02 protocols.

	BB84 Protocol [30]	**GG02 Protocol [31]**
Misalignment error probability	0.7%	/
Overall dark count rate	3×10^{-7}	/
Detection efficiency	11%	56%
Error correction efficiency	1.5	/
Total pulse number	6.25×10^{8}	/
Fiber loss coefficient (dB/km)	0.2	0.2
Repetition frequency (MHz)	625	100
Total sampling length	/	10^{8}
Block length	/	5×10^{7}
Modulation variance	/	3.246
Excess noise	/	0.022
Electronic noise	/	0.042
Reconciliation efficiency	/	95%

Table 3. Simulation parameters.

Parameters	**Values**
Computing resources in the cloud domain	1500 units
Computing resources in the edge domain	1000 units
VNF types	{VNF-1, VNF-2, VNF-3, VNF-4}
Number of wavelengths on each link	40
Physical lengths of cloud-domain links and inter-domain links	[20, 80] km
Physical lengths of edge-domain links	[20, 50] km
$\lvert A_r \rvert$	[1, 2]
c_r	[10, 50] units
w_r	1
q_r	[10, 100] kbps

In the simulation, 500,000 cross-domain service requests dynamically arrive following a Poisson distribution. The source and destination nodes for each request are randomly generated across two distinct domains. Each VNF is deployed across two different data centers and attached to nodes with higher connectivity levels. This paper focuses on performance metrics including the success probability of cross-domain service requests, multi-dimensional resource utilization, and the average number of trusted relays. Since multi-dimensional resource utilization varies over time during the simulation, we record resource utilization every 5000 services and ultimately calculate the average of 100 utilization values.

5.1. Performance Evaluation on the Success Probability of Cross-Domain Service Requests

Figure 5 illustrates the success probability of cross-domain service requests versus traffic load under different single-VNF/dual-VNF demand scenarios. As shown in Figure 5, the success probability of cross-domain service requests gradually declines for each algorithm as traffic load increases. This occurs because higher load prolongs the average duration of cross-domain service requests, leading to longer periods of multi-dimensional resource occupancy within the DCI network. Consequently, service blocking due to resource shortages becomes more likely.

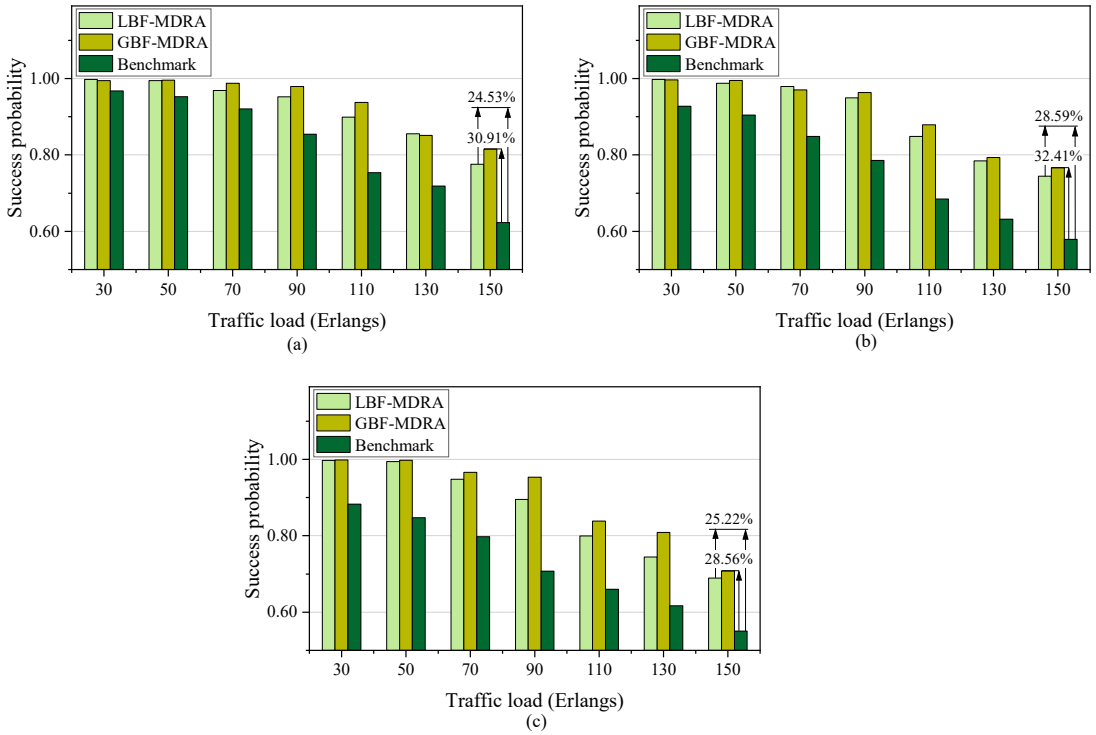

Figure 5. Success probability of cross-domain service requests versus traffic load under different single-VNF/dual-VNF demand ratios of (**a**) 80%/20%, (**b**) 50%/50%, and (**c**) 20%/80%.

Under varying proportions of single-VNF/dual-VNF demands, the success probabilities of cross-domain service requests for the proposed multi-dimensional resource allocation algorithms based on two balancing factors both exceed the benchmark algorithm. This gap becomes more pronounced as traffic load increases. As shown in Figure 5a, at high load levels, the LBF-MDRA algorithm increases the success probability by 24.53% (150 Erlang) compared to the benchmark algorithm, while the GBF-MDRA algorithm increases the success probability by 30.91% (150 Erlang). Figure 5b,c reflect similar trends. This is because both algorithms select VNF nodes and paths with more abundant resources when planning service routes and add more candidate paths for service routing, thereby significantly improving the success probability. Notably, the GBF-MDRA algorithm commonly achieves the higher success probability of cross-domain service requests than the LBF-MDRA algorithm. This is because the global balancing factor focuses on the network impact of resource demands across the entire path, whereas the local balancing factor only considers resource utilization related to VNF nodes. Although the LBF-MDRA algorithm still improves success probability compared to the benchmark algorithm, it lacks the advantages exhibited by the global balancing factor.

5.2. Performance Evaluation on the Multi-Dimensional Resource Utilization

Figure 6 demonstrates the results of the computing resource utilization versus traffic load under different scenarios, which reveals that the computing resource utilization of the LBF-MDRA, GBF-MDRA, and benchmark algorithms all exhibit an upward trend as the traffic load increases. This is attributed to the increased demand for computing resources driven by the growing load, consequently leading to higher utilization rates. At low load levels, the differences in computing resource utilization among the three algorithms are minor, but these differences significantly widen under high load conditions. Notably, the LBF-MDRA algorithm demonstrates markedly higher computing resource utilization compared to the benchmark under high load scenarios when the single-VNF/dual-VNF demand ratio is 20%/80%, which shows its robust capability in allocating and utilizing

computing resources during high load periods. The GBF-MDRA algorithm demonstrates a clear advantage in computing resource utilization when single-VNF demand services account for a larger proportion, outperforming both the benchmark algorithm and the LBF-MDRA algorithm. The pronounced advantage of the LBF-MDRA algorithm under the single-VNF/dual-VNF demand ratio of 20%/80% stems from its local balancing factor being computing resource-dominant. During computation, the local balancing factor considers the ratio of service demand resources to total resources in the selected VNF node and its connected links. The balancing factor for computing resources only relates to the computing unit of candidate VNF nodes, whereas the balancing factors for wavelength and key resources involve multiple links connected to the node. This feature results in limited influence of wavelength and key resources on the overall balancing factor, making paths containing VNF nodes with more computing resources more likely to be selected during routing.

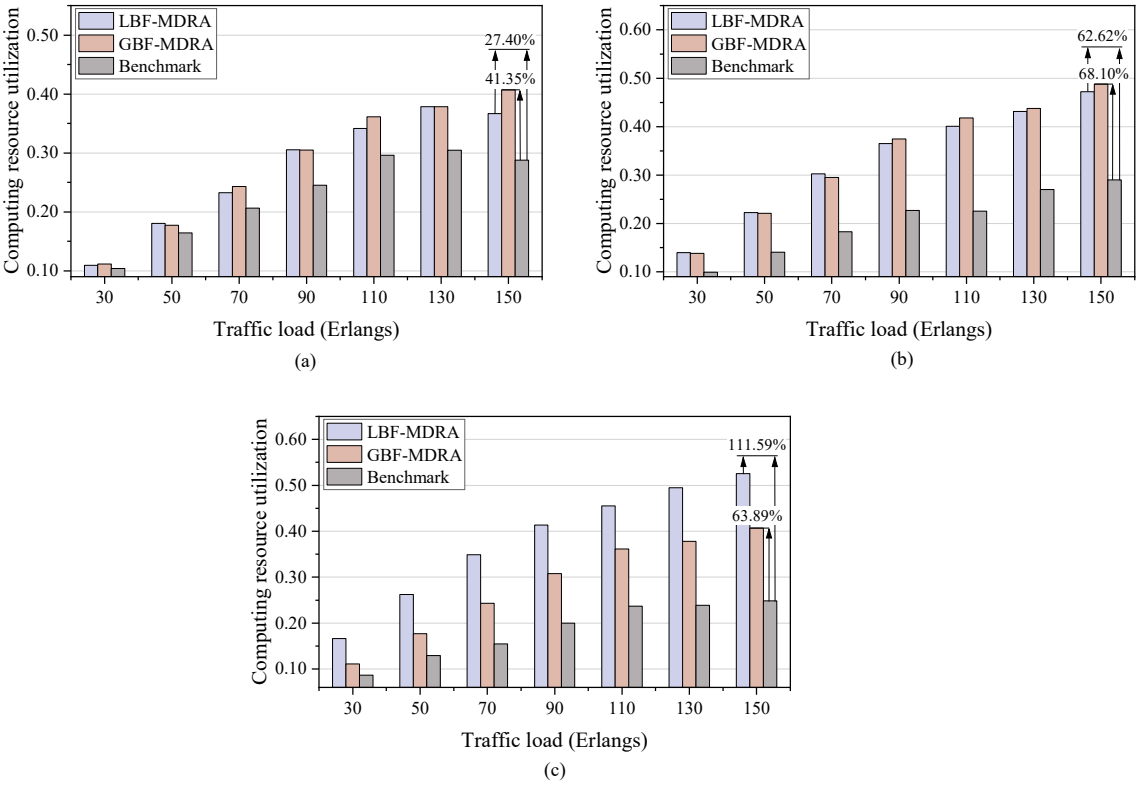

Figure 6. Computing resource utilization versus traffic load under different single-VNF/dual-VNF demand ratios of (**a**) 80%/20%, (**b**) 50%/50%, and (**c**) 20%/80%.

Figures 7 and 8, respectively, illustrate the relationship between resource utilization rates for wavelength and key resources versus traffic load across different algorithms. When the single-VNF/dual-VNF demand ratio is 80%/20%, as the load gradually increases from 50 to approximately 150, the wavelength resource utilization of all three algorithms shows an upward trend. Among them, the wavelength resource utilization of the GBF-MDRA algorithm at 150 Erlang improves by 41.03% compared to the benchmark algorithm. The key resource utilization of the GBF-MDRA algorithm increases by 17.10%, demonstrating significant advantages. Under a 50%/50% single-VNF/dual-VNF demand ratio, the overall changes are relatively gradual. However, at a load of 150 Erlang, the GBF-MDRA algorithm improves by 30.62% compared to the benchmark algorithm for wavelength resource utilization, still outperforming the LBF-MDRA algorithm. The GBF-MDRA algorithm demonstrates particularly better performance under different VNF demands, especially

in high-load scenarios. This indicates its superior resource allocation and scheduling strategy in high-load conditions, enabling more efficient utilization of wavelength and key resources.

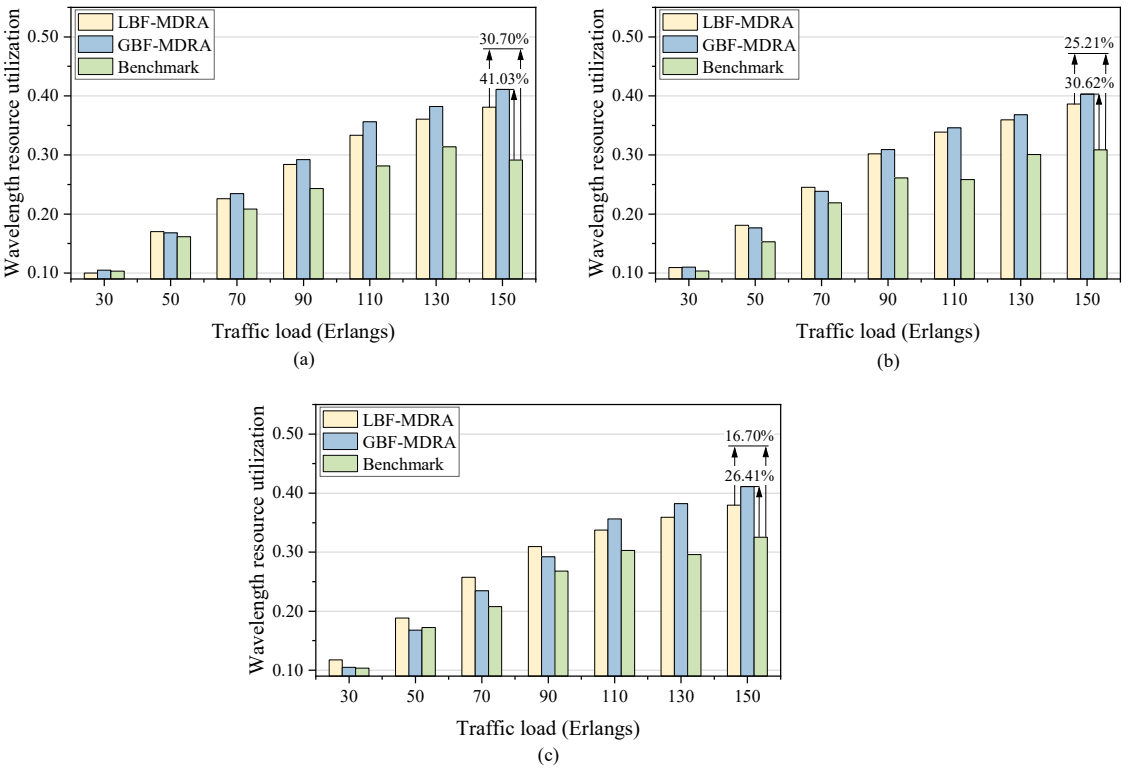

Figure 7. Wavelength resource utilization versus traffic load under different single-VNF/dual-VNF demand ratios of (**a**) 80%/20%, (**b**) 50%/50%, and (**c**) 20%/80%.

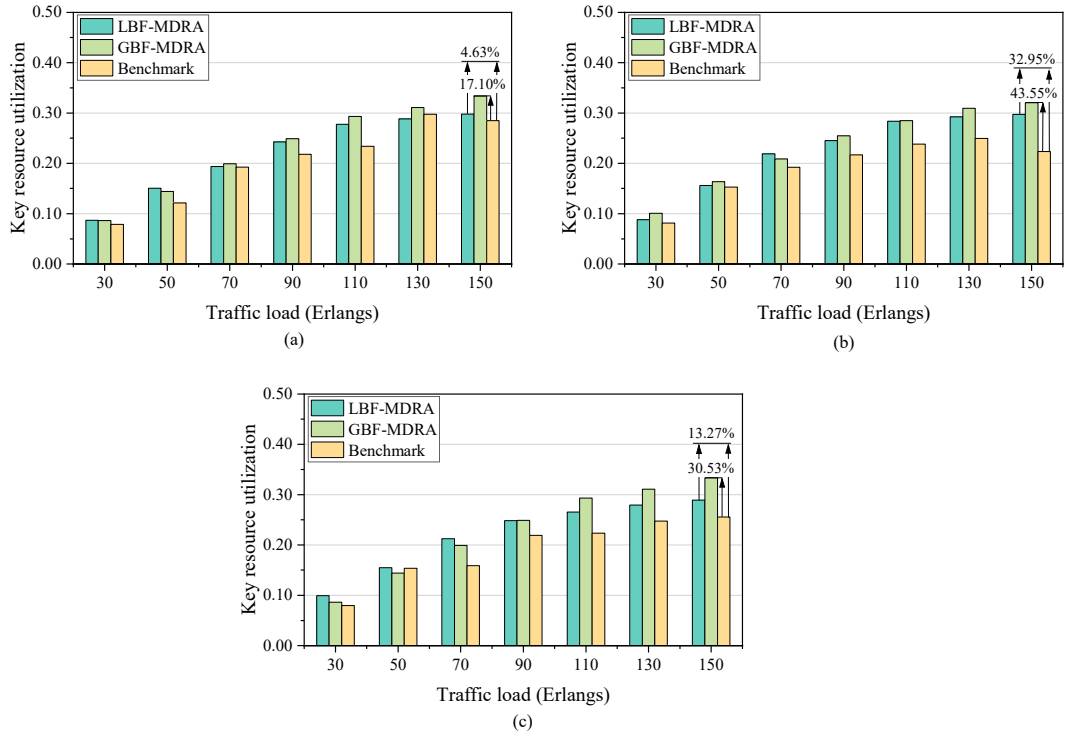

Figure 8. Key resource utilization versus traffic load under different single-VNF/dual-VNF demand ratios of (**a**) 80%/20%, (**b**) 50%/50%, and (**c**) 20%/80%.

5.3. Performance Evaluation on the Average Number of Trusted Relays

Figure 9 illustrates that the average number of trusted relays varies with traffic load under different single-VNF/dual-VNF demand ratios for various algorithms. For all three algorithms, the average number of trusted relays exhibits a fluctuating trend of increasing first and then decreasing as the load rises. This occurs because increased load leads to more hops in service paths, thereby requiring more trusted relays. However, when the load reaches a certain threshold, the service success probability declines, reducing the number of successful services in the network and thus decreasing the number of path hops, which in turn lowers the average number of trusted relays. Observing Figure 9 reveals that both LBF-MDRA and GBF-MDRA algorithms exhibit a lower average number of trusted relays than the benchmark algorithm. This stems from their approach to selecting VNF nodes and paths, i.e., both algorithms prioritize paths with balanced resource loads and fewer hops by sorting candidate paths based on a balancing factor. In contrast, the benchmark algorithm randomly selects VNF nodes with sufficient computing resources without additional filtering steps. This approach often results in longer paths, leading to a higher average number of trusted relays. When dual-VNF demand traffic constitutes a low proportion, the LBF-MDRA algorithm achieves the lowest average number of trusted relays. However, as this proportion increases, the GBF-MDRA algorithm begins to demonstrate a certain advantage in this regard. In summary, compared to the benchmark algorithm, both LBF-MDRA and GBF-MDRA algorithms can establish cross-domain services using fewer trusted relays. This contributes to reducing the cost of such services while enhancing their security levels.

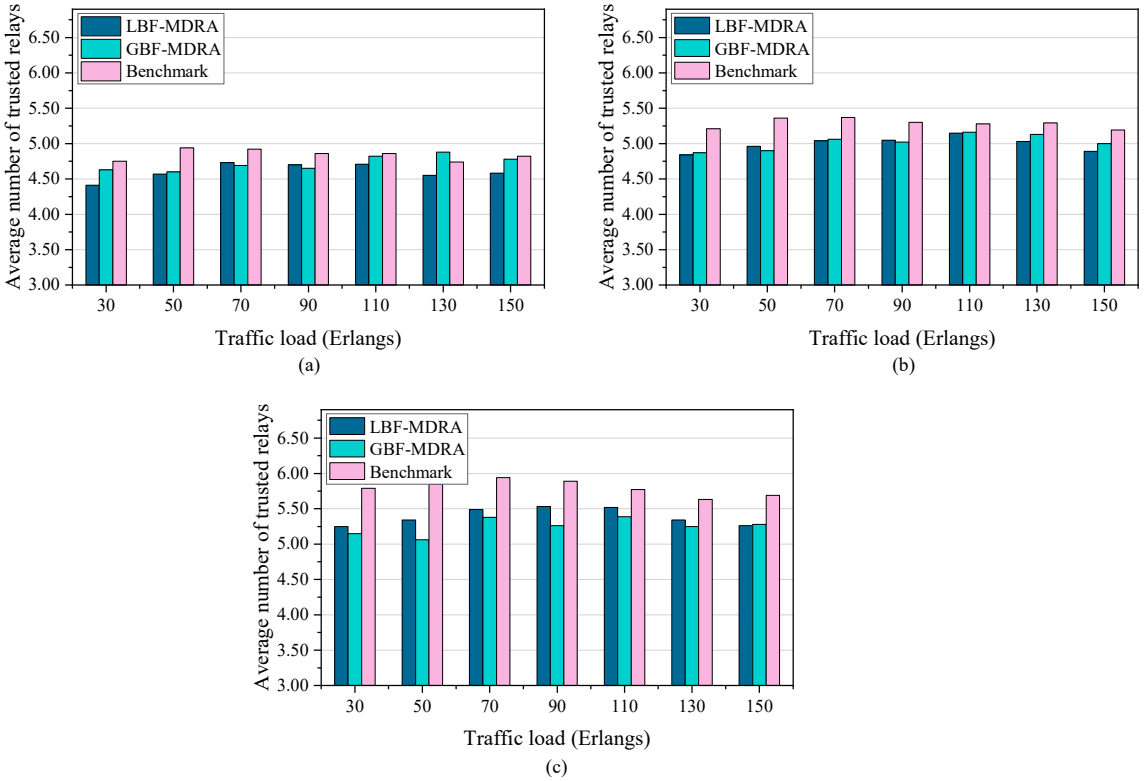

Figure 9. Average number of trusted relays versus traffic load under different single-VNF/dual-VNF demand ratios of (**a**) 80%/20%, (**b**) 50%/50%, and (**c**) 20%/80%.

6. Discussion

To verify algorithm performance more universally, we do not impose a single constraint on relevant parameters such as physical link distance, source node and destination

node locations, or service request attributes. Taking the physical link length as an example, in line with practical scenarios, we set the physical length of links within and between cloud domains as [20, 80] km, and links within edge domains as [20, 50] km. Additionally, we select appropriate protocols for each link, resulting in different key rates and consequently random outcomes. Therefore, the performance of the GBF-MDRA algorithm is not necessarily consistently superior to that of the LBF-MDRA algorithm. While the LBF-MDRA algorithm focuses solely on the multi-dimensional resources of VNF nodes and all links connected to them, the GBF-MDRA algorithm prioritizes the overall multi-dimensional resource utilization of the path itself, disregarding links unrelated to the path. This approach maximizes service establishment on paths with more abundant overall multi-dimensional resources, resulting in more balanced network-wide load distribution, higher cross-domain service request success probability, and improved multi-dimensional resource utilization. Meanwhile, both the LBF-MDRA and GBF-MDRA algorithms outperform the benchmark algorithm in all performance metrics, validating the superiority of the proposed GBF-MDRA and LBF-MDRA algorithms.

Figure 10 exemplifies key consumption and management in a QKD-enabled cross-domain DCI network. Cloud-domain node A and edge-domain node D serve as source node and the destination node, respectively. The QKD transmitter (QTx) and QKD receiver (QRx) are connected via a QKD link. Nodes A and B, as well as nodes B and C execute the BB84 protocol to share keys K_A and K_B, respectively. Nodes C and D share key K_C via the GG02 protocol. All secret keys are stored in their respective key managers. The key manager is a distributed entity that stores secret keys and provides an interface to upper-layer cryptographic applications; each QKD node hosts a single key manager that governs all local transceivers. Consequently, the key managers mediate end-to-end key delivery by relaying key material across trusted nodes and supervise the complete life-cycle from key generation to key consumption. To ensure continuous confidentiality along the path, the global key K_A is forwarded via hop-by-hop one-time-pad encryption:

1. Node B computes $K_A \oplus K_B$ and forwards it to node C.
2. Node C recovers K_A by XORing with K_B, then re-encrypts it as $K_A \oplus K_C$ and transmits the result to node D.
3. Node D retrieves K_A by decrypting (XORing) the received $K_A \oplus K_C$ with K_C.

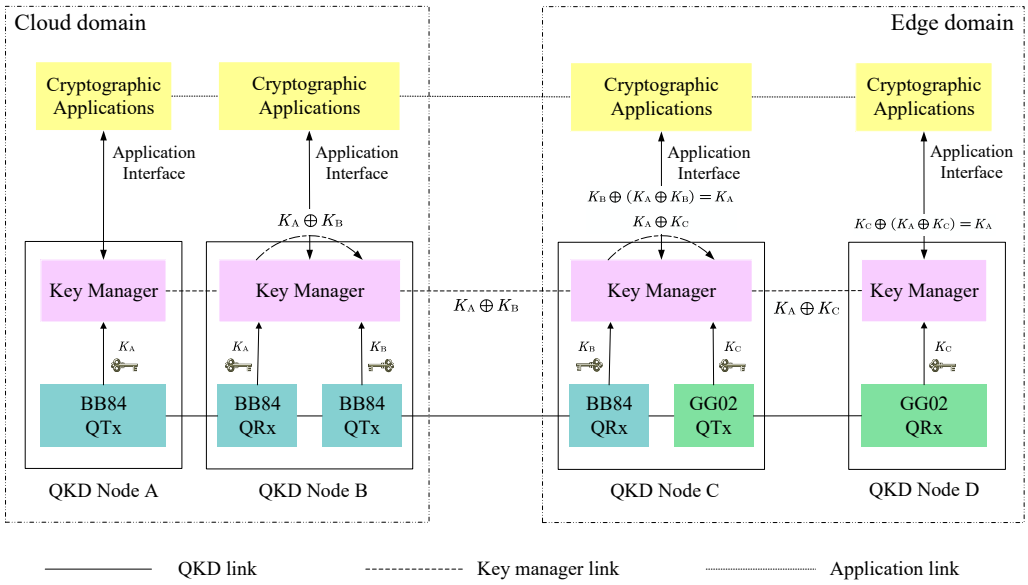

Figure 10. Illustration of key consumption and management in a QKD-enabled cross-domain DCI network.

Furthermore, QKD still faces several technical challenges. One such challenge is achieving high key rates over long distances. For fiber-optic implementations, this commonly leads to an exponential decline in key rate. Even considering optimistic system performance, key rates become unattractive beyond a few hundred kilometers. In the long term, advanced quantum repeaters hold promise for practical long-distance QKD; however, they remain in the fundamental research phase. Trusted relays offer a short-term solution, and this paper specifically employs trusted relays to extend QKD distances. Considering practical physical link lengths, we set cloud domain and inter-domain link lengths to 20–80 km, edge intra-domain links to 20–50 km, and matched them with appropriate QKD protocols.

In a trusted relay-based QKD network, long-distance QKD between two end nodes can be achieved through a series of QKD chains. Although trusted relay-based QKD network implementations are highly practical and scalable, they must assume that each trusted relay is protected from any intrusion or attack, which is an idealized simplification that cannot guarantee information-theoretic security. Therefore, the number of trusted relays can partially reflect the cost and practical security level provided by cross-domain services. Fewer trusted nodes generally lead to higher practical security and lower costs. The LBF-MDRA and GBF-MDRA algorithms proposed in this work require fewer average trusted relays compared to the benchmark algorithms, thereby enhancing the security level of QKD-enabled cross-domain DCI networks to some extent. Future research may design new algorithms to reduce the number of trusted relays, or establish untrusted relay-based QKD network. This approach relies on specific QKD protocols to reduce the dependence on trusted relays. Some important candidates include measurement-device-independent (MDI) [32], asynchronous MDI [33], twin-field (TF) [34], Bennett-Brassard-Mermin-1992 (BBM92) [35], and source-independent [36] protocols.

Currently, schemes for deploying QKD network infrastructure by sharing existing fiber-optic infrastructure are gaining significant attention. In this paper, we integrate QKD transmission with existing optical networks using DWDM technology, proposing a QKD-enabled cross-domain DCI network. However, during co-fiber transmission, nonlinear noise generated by phenomena such as Raman scattering and four-wave mixing can severely contaminate quantum signals, potentially causing significant degradation in the performance of quantum channels and QKD systems. Future advancements in multiplexing techniques or novel WDM layouts may enable co-fiber transmission while minimizing noise interference on quantum signals.

In addition to QKD, the quantum secure direct communication (QSDC) [37,38] technology may enhance the security of cross-domain data center interconnection networks. QSDC facilitates the direct transmission of secure information via quantum states. Future research can further advance in this direction.

7. Conclusions

This paper focuses on the QKD-enabled cross-domain DCI network and conducts the allocation of multi-dimensional resources (i.e., computing, wavelength, and key resources). Addressing the growing security demands of data centers in cloud-edge collaboration scenarios and the potential risks of traditional cryptographic technologies in the quantum era, this paper introduces QKD technology into DCI networks. We construct a multi-dimensional resource allocation framework and propose two multi-dimensional resource allocation algorithms, i.e., LBF-MDRA and GBF-MDRA, which aim to achieve network load balancing and enhance the success rate of cross-domain services. The simulation results demonstrate the superiority of LBF-MDRA and GBF-MDRA in different performance metrics, such as improving the success probability of cross-domain service requests,

optimizing multi-dimensional resource utilization, and reducing the average number of trusted relays.

In the future, as data center scales continue to expand and service demands grow increasingly complex, we will extend our research to address resource allocation challenges in multi-domain cloud-edge collaboration scenarios. This will enable the algorithms to better adapt to the complex and dynamic environments of DCI networks. Furthermore, more flexible VNF requirements, such as dynamic linking and adaptive resource sharing, will be incorporated into cloud-edge service requests, enabling the framework to adapt to diverse and evolving service scenarios.

Author Contributions: Conceptualization, H.J., X.W. and Y.C.; Methodology, J.L., Z.L. and Y.Z.; Validation, H.J., J.L. and Y.Z.; Writing—Original Draft Preparation, H.J., Z.L. and Y.Z.; Writing—Review and Editing, X.W. and Y.C.; Funding Acquisition, H.J., X.W., J.L. and Z.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Key Research and Development Program of China (2023YFF0612900).

Institutional Review Board Statement: Not applicable.

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding author.

Acknowledgments: This article is a revised and expanded version of a paper entitled "Globally Balanced Multidimensional Resource Allocation for Data Center Optical Networks Secured by Quantum Key Distribution" [39], which was presented at the Asia Communications and Photonics Conference, Suzhou, China, November 2025.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Mach, P.; Becvar, Z. Mobile edge computing: A survey on architecture and computation offloading. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 1628–1656. [CrossRef]
2. Zhang, X.; Zhang, Y.; Quan, W.; Liu, M.; Zhuang, Y.; Luo, Y.; Luo, T.; Liang, J.; Liu, K.; Zhang, H. Predictive-proactive congestion avoidance for cross-domain data center interconnect. *IEEE Trans. Netw. Sci. Eng.* 2025; *in press*. [CrossRef]
3. Han, J.; Xue, K.; Wang, W.; Li, R.; Sun, Q.; Lu, J. RateMP: Optimizing bandwidth utilization with high burst tolerance in data center networks. In Proceedings of the IEEE Conference on Computer Communications (IEEE INFOCOM), Vancouver, BC, Canada, 20–23 May 2024.
4. Yang, H.; Zhu, Z. Traffic-aware configuration of all-optical data center networks based on Hyper-FleX-LION. *IEEE/ACM Trans. Netw.* **2024**, *32*, 2675–2688.
5. Li, J.; Marchi, F.D.; Lei, Y.; Joshi, R.; Chandrasekaran, B.; Xia, Y. Unlocking diversity of fast-switched optical data center networks with unified routing. *IEEE/ACM Trans. Netw.* 2025; *in press*. [CrossRef]
6. Gill, S.S.; Kumar, A.; Singh, H.; Singh, M.; Kaur, K.; Usman, M.; Buyya, R. Quantum computing: A taxonomy, systematic review and future directions. *Softw.-Pract. Exp.* **2022**, *52*, 66–114. [CrossRef]
7. Yang, Z.; Zolanvari, M.; Jain, R. A Survey of Important Issues in Quantum Computing and Communications. *IEEE Commun. Surv. Tutor.* **2023**, *25*, 1059–1094. [CrossRef]
8. Cao, Y.; Zhao, Y.; Wang, Q.; Zhang, J.; Ng, S.X.; Hanzo, L. The evolution of quantum key distribution networks: On the road to the Qinternet. *IEEE Commun. Surv. Tutor.* **2022**, *24*, 839–894.
9. Lo, H.-K.; Chau, H.F. Unconditional security of quantum key distribution over arbitrarily long distances. *Science* **1999**, *283*, 2050–2056. [CrossRef]
10. Scarani, V.; Bechmann-Pasquinucci, H.; Cerf, N.J.; Dušek, M.; Lütkenhaus, N.; Peev, M. The security of practical quantum key distribution. *Rev. Mod. Phys.* **2009**, *81*, 1301–1350. [CrossRef]
11. Zhu, Q.; Yu, X.; Zhao, Y.; Nag, A.; Zhang, J. Resource allocation in quantum-key-distribution-secured datacenter networks with cloud-edge collaboration. *IEEE Internet Things J.* **2023**, *10*, 10916–10932.

12. Ma, W.; Chen, B.; Liu, L.; Chen, H.; Shao, W.; Gao, M.; Wu, J.; Ho, P.-H. Equilibrium allocation approaches of quantum key resources with security levels in QKD-enabled optical data center networks. *IEEE Internet Things J.* **2022**, *9*, 25660–25672. [CrossRef]
13. Li, Y.; Zhao, Y.; Li, B.; Yu, X.; Yang, H.; Wang, X.; Zhang, J. Joint balancing of IT and spectrum resources for selecting virtualized network function in inter-datacenter elastic optical networks. *Opt. Express* **2019**, *27*, 15116–15128. [CrossRef] [PubMed]
14. Guo, Y.; Ye, T.; Ma, Y. Second-moment vliant load balancing (sVLB) in optical data center networks. *IEEE J. Sel. Areas Commun.* **2025**, *43*, 1793–1808.
15. Gong, L.; Zhu, Z. Virtual optical network embedding (VONE) over elastic optical networks. *J. Lightwave Technol.* **2014**, *32*, 450–460.
16. Liu, J.; Lu, W.; Zhou, F.; Lu, P.; Zhu, Z. On dynamic service function chain deployment and readjustment. *IEEE Trans. Netw. Serv. Manag.* **2017**, *14*, 543–553. [CrossRef]
17. Garay, J.; Matias, J.; Unzilla, J.; Jacob, E. Service description in the NFV revolution: Trends, challenges and a way forward. *IEEE Commun. Mag.* **2016**, *54*, 68–74. [CrossRef]
18. ETSI. *Network Functions Virtualisation (NFV); Architectural Framework. ETSI GS NFV 002 V1.2.1*; ETSI: Valbonne, France, 2014.
19. Mijumbi, R.; Serrat, J.; Gorricho, J.-L.; Bouten, N.; Turck, F.D.; Boutaba, R. Network function virtualization: State-of-the-art and research challenges. *IEEE Commun. Surv. Tut.* **2016**, *18*, 236–262.
20. Laghrissi, A.; Taleb, T. A survey on the placement of virtual resources and virtual network functions. *IEEE Commun. Surv. Tut.* **2019**, *21*, 1409–1434.
21. Yala, L.; Frangoudis, P.A.; Ksentini, A. Latency and availability driven VNF placement in a MEC-NFV environment. In Proceedings of the IEEE Global Communications Conference, Abu Dhabi, United Arab Emirates, 9–13 December 2018.
22. Bennett, C.H.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. In Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 9–12 December 1984; pp. 175–179.
23. Grosshans, F.; Grangier, P. Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.* **2002**, *88*, 057902. [CrossRef]
24. Gottesman, D.; Lo, H.-K.; Lütkenhaus, N.; Preskill, J. Security of quantum key distribution with imperfect devices. *Quantum Inf. Comput.* **2004**, *4*, 325–360. [CrossRef]
25. Ma, X.; Qi, B.; Zhao, Y.; Lo, H.-K. Practical decoy state for quantum key distribution. *Phys. Rev. A* **2005**, *72*, 012326. [CrossRef]
26. Leverrier, A.; Grosshans, F.; Grangier, P. Finite-size analysis of a continuous-variable quantum key distribution. *Phys. Rev. A* **2010**, *81*, 062343. [CrossRef]
27. International Telecommunication Union. *Spectral Grids for WDM Applications: DWDM Frequency Grid. ITU-T G.694.1*; International Telecommunication Union: Geneva, Switzerland, 2012.
28. Wang, X.; Jiang, H.; Li, J.; Liang, Z.; Zheng, Y.; Cao, Y. Resource allocation for key-enhanced cross-domain data center optical networks. In Proceedings of the International Conference on Optical Communications and Networks, Zhangjiajie, China, 28–31 July 2025.
29. Li, S.; Li, B.; Zhu, Z. On the game-theoretic analysis of dynamic VNF service chaining in edge-cloud EONs. *J. Lightwave Technol.* **2023**, *41*, 2940–2952. [CrossRef]
30. Mao, Y.; Wang, B.-X.; Zhao, C.; Wang, G.; Wang, R.; Wang, H.; Zhou, F.; Nie, J.; Chen, Q.; Zhao, Y.; et al. Integrating quantum key distribution with classical communications in backbone fiber network. *Opt. Express* **2018**, *26*, 6010–6020. [CrossRef]
31. Wang, H.; Pi, Y.; Huang, W.; Li, Y.; Shao, Y.; Yang, J.; Liu, J.; Zhang, C.; Zhang, Y.; Xu, B. High-speed Gaussian-modulated continuous-variable quantum key distribution with a local local oscillator based on pilot-tone-assisted phase compensation. *Opt. Express* **2020**, *28*, 32882–32893. [CrossRef] [PubMed]
32. Lo, H.-K.; Curty, M.; Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **2012**, *108*, 130503. [CrossRef] [PubMed]
33. Xie, Y.-M.; Lu, Y.-S.; Weng, C.-X.; Cao, X.-Y.; Jia, Z.-Y.; Bao, Y.; Wang, Y.; Fu, Y.; Yin, H.-L.; Chen, Z.-B. Breaking the rate-loss bound of quantum key distribution with asynchronous two-photon interference. *PRX Quantum* **2022**, *3*, 020315. [CrossRef]
34. Lucamarini, M.; Yuan, Z.L.; Dynes, J.F.; Shields, A.J. Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. *Nature* **2018**, *557*, 400–403. [CrossRef]
35. Bennett, C.H.; Brassard, G.; Mermin, N.D. Quantum cryptography without Bell's theorem. *Phys. Rev. Lett.* **1992**, *68*, 557–559. [CrossRef]
36. Xiao, Y.-R.; Yin, H.-L.; Hua, W.-J.; Cao, X.-Y.; Chen, Z.-B. Experimental efficient source-independent quantum secret sharing against coherent attacks. *Phys. Rev. Lett.* **2025**, *135*, 150801. [CrossRef]
37. Pan, D.; Long, G.-L.; Yin, L.; Sheng, Y.-B.; Ruan, D.; Ng, S.X.; Lu, J.; Hanzo, L. The evolution of quantum secure direct communication: On the road to the Qinternet. *IEEE Commun. Surv. Tutor.* **2024**, *26*, 1898–1949. [CrossRef]

38. Pan, D.; Liu, Y.-C.; Niu, P.; Zhang, H.; Zhang, F.; Wang, M.; Song, X.-T.; Chen, X.; Zheng, C.; Long, G.-L. Simultaneous transmission of information and key exchange using the same photonic quantum states. *Sci. Adv.* **2025**, *11*, eadt4627. [CrossRef] [PubMed]
39. Zheng, Y.; Cao, Y.; Wang, X. Globally balanced multidimensional resource allocation for data center optical networks secured by quantum key distribution. In Proceedings of the Asia Communications and Photonics Conference, Suzhou, China, 5–8 November 2025.