Quantum Cloud with Communication, Computing, Caching, and Cipher (4C) Resource Coordination

Qingcheng Zhu
State Key Lab of Information Photonics and Optical Communications
Beijing Univ. of Posts and Telecommunications
Beijing, China
qingcheng@bupt.edu.cn

Yongli Zhao*
State Key Lab of Information Photonics and Optical Communications
Beijing Univ. of Posts and Telecommunications
Beijing, China
yonglizhao@bupt.edu.cn

Xiaosong Yu
State Key Lab of Information Photonics and Optical Communications
Beijing Univ. of Posts and Telecommunications
Beijing, China
xiaosongyu@bupt.edu.cn

Jie Zhang
State Key Lab of Information Photonics and Optical Communications
Beijing Univ. of Posts and Telecommunications
Beijing, China
lgr24@bupt.edu.cn

***Abstract*—The cloud services requiring communication, computing and caching (3C) resources are supported by datacenter networks (DCNs). The service security is threatened due to the development of quantum computers. Quantum key distribution (QKD) technology promises to share secret keys as cipher resources between remote users with information-theoretic security. The quantum cloud is illustrated which is realized by the QKD-secured cloud datacenter network. In the quantum cloud, the communication, computing, caching and cipher (4C) resources are provided for data transmission, processing, storing and encryption. To solve the newly emerged 4C resource coordination problem, a 4C-oriented control architecture is designed and the heuristic algorithms for securing service function chains are innovatively proposed. The simulation results show that the proposed algorithms can achieve the great service success ratio performance compared with the baseline.**

Keywords—quantum cloud, communication, computing, caching, cipher, quantum key distribution

I. Introduction

Many services are being migrated into the cloud with the development of the cloud computing and caching paradigm. The inter-Datacenter (inter-DC) network is an important infrastructure for the cloud, where optical network is employed for the DC interconnection (DCI). It can provide data transmission, processing and storage capabilities with communication, computing and caching (3C) resources. In the cloud, the network function virtualization (NFV) technologies are widely applied, which enable the virtual network functions (VNFs) using the computing and caching resources. The traditional connectivity services (e.g., virtual private networks) will move to service function chain (SFC) which includes a set of VNFs required by the specific traffic flow in an order [1]. A service function path (SFP) needs to be established, which is a certain route to steer traffic to form an SFC [2]. 3C resources over the SFP need to be allocated. The joint 3C resource allocation was studied for SFC in the cloud [3][4]. However, the confidential and sensitive data over the SFP will face critical security threats with the advent of quantum computing.

Quantum key distribution (QKD), as a quantum cryptography, enables symmetric keys sharing between remote users based on the principles of quantum physics with information-theoretic security. The quantum cloud is promising to be formed, where QKD systems are integrated in the cloud inter-DC networks [5]. There are the cases to realize the quantum cloud. NFV orchestration was combined with QKD using a time-shared approach for cost-effective VNF distribution across DCs [6]. QKD was applied for validating ordered proof-of-transit (OPoT) on top of the Madrid Quantum Network and can alleviate the security breach in SFC [7]. In the quantum cloud, apart from the 3C resources, the QKD systems equipped per node can supply cipher resources (i.e., secret keys) for enroute data encryption and decryption. The communication, computing, caching and cipher (4C) resource coordination (4CRC) problem has newly emerged. A 4CRC solution in the quantum cloud-edge collaboration was designed to minimize the cipher resource consumption [8]. But it cannot solve the 4CRC problem for securing SFC efficiently due to the additional traffic steering constraint in SFC.

In this paper, the quantum cloud is formed where the new 4CRC problem needs solutions. To solve the problem for SFC, a 4C-oriented control architecture is designed. The heuristic 4CRC algorithms considering different VNF selection strategies are proposed to satisfy the 4C requirements of SFC. The simulation results show that the proposed algorithms achieve the higher success ratio compared with the baseline.

II. Control Architecture and Problem Statement

Fig. 1 illustrates the designed 4C-oriented control architecture of the quantum cloud. The architecture has four layers including DCI layer, QKD layer, control layer and service layer. In the DCI layer, the computing and caching resources such as CPU cycles and storage are provided by DCs; the communication resources (i.e. bandwidth) are provided by the substrate optical networks; each type of VNF can be deployed in multiple DCs for survivability. The QKD layer is newly added, where QKD modules for key generation and key managers for key management can be deployed together with each node in the DCI layer, so as to provide cipher resources for each user and eliminate the additional limitations of quantum channels. In the control layer, the 4C-resource-aware control function is newly enabled, which can make routing and resource allocation decisions based on the 4C resource availability in the QKD layer and DCI layer. In the service

978-3-903176-54-6

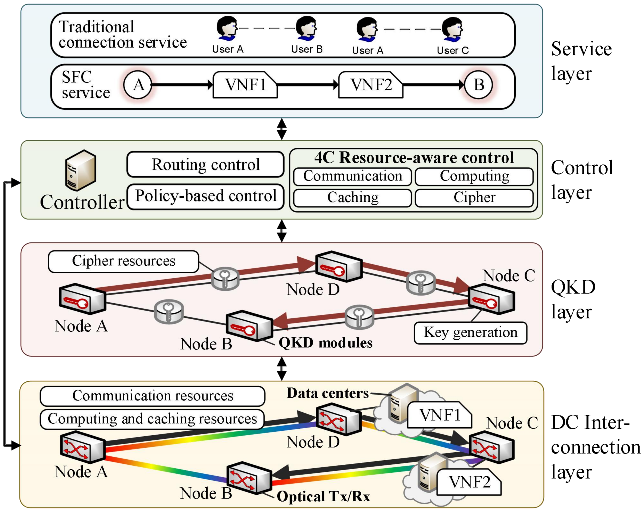

Fig. 1. The 4C-oriented control architecture of the quantum cloud.

layer, the services requiring 4Cresources are initiated, such as the traditional connection services and the SFC requests. The SFC request passes through different VNFs in an order. The data rate steered from a VNF will change based on the functions of the VNF. The 4C requirements of the specific traffic can be illustrated as follows: to transmit the data from a node to another node, the bandwidths require to be allocated and configured with a line rate; to process and store the data, the CPU cycles and storage need to be occupied; to secure the enroute data, the secret keys will be used whose consumption is calculated based on the data rate and encryption algorithms.

Faced with the 4C requirements of SFC requests, the 4CRC problem needs to be solved in the quantum cloud. Limited by the network topology and the 4C resource availabilities [8], the successfully carried requests are expected to be maximized. In 4CRA, VNFs are selected, SFPs are calculated and the 4C resources over the selected SFP are allocated coordinatively. For each SFC request, the SFP is constructed with the ordered chain of VNFs each of which is from specific DC. Apart from the traditional communication paths to allocate spectrum resources over the SFP, the QKD paths are newly needed to supply end-to-end secret keys with key relay. An example of SFP is shown in Fig. 1. The SFC request is from Node A to Node B, and requires VNF1 and VNF2 to process data. The selected DCs with VNF1 and VNF2 are connected with Node D and Node C respectively. To construct the SFP, the communication path A → D → C → B is established with bandwidth allocation; the QKD path A→D→C→B is selected with secret key supply.

III. 4C Resource Coordination (4CRC) Algorithm

In the quantum cloud, the 4CRC algorithm is proposed to satisfy the 4C requirements of SFC requests. The network topology is denoted by $G(V \cup D, E)$, where V refers to the set of network nodes, D denotes the set of DCs, E is the set of fiber links. The network nodes are equipped with QKD modules and optical transceivers. B_l is the available spectrum resources in fiber link, $l \in E$; C_n is the available computing and caching resources in the DCs connected with the node $n \in V$; K_l is the available secret keys generated by QKD with a key generation rate g in the fiber link l; F_n is the deployed VNFs in the node n. The SFC request is $r(s, d, S_{vnf}, S_c, S_b, S_k)$, where s and d are source and destination nodes; $S_{vnf} = \{f_i\}$ is the required VNF set; $S_c = \{c_i\}$ is the set of the computing and caching resources required on VNFs; $S_b = \{b_i\}$ is the set of the required bandwidth; $S_k = \{k_i\}$ is the set of the required secret keys.

The 4CRC algorithm consists of three main parts, i.e. VNF selection, SFP calculation, and 4C resource allocation. The detailed procedures are shown in TABLE I. In the first part (Lines 1-11), all the candidate DCs deployed with the required VNFs are checked to find the appropriate DCs for providing VNFs. Two VNF selection strategy strategies I and II are designed considering that the location of VNFs will influence the final SFP and the resource consumption. Strategy I gives a high priority of the DCs containing all $f_i \in S_{vnf}$; strategy II considers the DCs over the K-shortest-paths from s to d first. Based on the new ordered S_{DC}^i, the available computing and caching resources are checked one by one to achieve the selected node set $\mathcal{N}_r$. In the second part (Lines 12-23), SFP is calculated for each SFC request. The SFP must go through the selected DCs as required. In an SFP, the selected node connecting a DC is called anchor node (AN). The ANs will split an SFP into multiple segments. For each segment, among the candidate paths, if the available spectrum resources can satisfy the bandwidth requirements of the SFC request, the communication path is selected; if the available secret keys are not smaller than key requirement in this segment, the QKD

TABLE I. Detailed Procedures of 4CRC Algorithm

4CRC Algorithm

Input: $G(V \cup D, E)$, B_l, C_n, K_l, F_n, $r(s, d, S_{vnf}, S_c, S_b, S_k)$
Output: 4C resource allocation on the service function path

1: **for** $\forall f_i \in S_{vnf}$
2: get the DC set S_{DC}^i hosting VNF f_i;
sort all DCs in S_{DC}^i according to specific VNF selection strategy:
3: **I:** the DCs containing all $f_i \in S_{vnf}$ rank first;
II: the DCs over the K-shortest-paths from s to d rank first;
4: **for** each $DC_n \in S_{DC}^i$
5: **if** $C_n \geq c_i$
6: select DC_n to use VNF f_i;
7: add the node n_i connecting DC_n into $\mathcal{N}_r$;
8: **break;**
9: **end**
10: **end**
11: **end**
12: add s before the first element and d after the last element in $\mathcal{N}_r$;
13: **for** $\forall n_i \in \mathcal{N}_r$
14: calculate the K-shortest-paths P_i, from $n_i \in \mathcal{N}_r$ to $n_{i+1} \in \mathcal{N}_r$;
15: **for** $\forall p_i \in P_i$
16: **if** B_l over p_i can satisfy the bandwidth requirement $b_i \in S_b$
17: add p_i into communication path set $\mathcal{P}_r^b$; **break;**
18: **end**
19: **if** K_l over p_i can satisfy the secret key requirement $k_i \in S_k$
20: Add p_i into QKD path set $\mathcal{P}_r^k$; **break;**
21: **end**
22: **end**
23: **end**
24: **if** $\mathcal{N}_r$, $\mathcal{P}_r^b$ and $\mathcal{P}_r^k$ can be found to satisfy the 4C requirements of r
25: allocate 4C resources based on $\mathcal{N}_r$, $\mathcal{P}_r^b$ and $\mathcal{P}_r^k$ for r;
26: **else** $r(s, d, S_{vnf}, S_c, S_b, S_k)$ is blocked;
27: **end**

path is selected. After traversing all the segments, the final communication path $\mathcal{P}_r^b$ and QKD path $\mathcal{P}_r^k$ from s to d are achieved. In the third part (Lines 24-27), the 4C resources are allocated according to $\mathcal{N}_r$, $\mathcal{P}_r^b$ and $\mathcal{P}_r^k$. The end-to-end secret keys are supplied per segment. If the SFP cannot be found, the SFC request will be blocked. The time complexity of the 4CRC algorithm is $O(K|V||S_{vnf}|(|E|+|V|log|V|))$.

IV. Simulation Results

Simulation is conducted based on the network topology with 6 nodes and 9 links where 3 nodes are connected with DCs [8]. There are 30 types of VNFs each of which is deployed in two DCs. Each DC can accommodate 5000 computing and caching units; each fiber link has 80 spectrum slots each of which is 50GHz to carry 40Gbps. Each pair of QKD modules has QKPs with 800 keys and key generation rate 32 keys per seconds. AES-256 algorithm is applied to supply cipher resources and a key can encrypt 1 Gbps. One computing unit can process 2 Gbps. Simulation results are obtained by averaging 10 experiments, where 10000 requests are generated following Poisson distribution each time. The VNF number of each request is 2. The initial data rate is [10,40] Gbps which is assumed to change in a specific rate [0.1,2] after steering the traffic from a specific VNF. The proposed two 4CRC algorithms are compared with the baseline algorithm which considers the VNF selection in a random order.

Figs. 3 (a-c) show the simulation results versus traffic load in terms of SFC success ratio, key consumption ratio and spectrum occupation ratio. We can find that the 4CRC-I (4CRA-II) algorithm has 33.61% (35.03%) higher SFC success ratio than the baseline at the 450 Erlang. The reason is that the proposed algorithms consider the 4C resource status and prefer to select SFPs with low resource cost. It can be observed that the success ratio of the 4CRC-I algorithm is higher than that of the 4CRC-II algorithm. This is because the selected SFPs in the 4CRC-I algorithm have the fewer hops than that in the 4CRC-II algorithm. In Fig. 3(b), we can find that the key consumption ratio of the 4CRC-I (4CRC-II) algorithm is 26.05% (23.67%) lower than that of the baseline at 100 Erlang, while the key consumption ratio of the baseline is higher after 300 Erlang. This is because the VNF selection will influence the SFP calculation, and therefore affect the 4C resource consumption. Furthermore, the fewer hops of SFPs have, the fewer secret keys will be likely to be consumed when the success ratio is in a high level. Fig. 3(c) shows that the 4CRC-I (4CRC-II) algorithm has the 27.14% (23.16%) lower spectrum occupation ratio than the baseline at 100 Erlang. The reason is that the hotpots of DCs will emerge with intensive request arrival and the VNFs interconnected with the fewer available communication resources will be selected.

V. Conclusion

The concept of the quantum cloud is illustrated and its 4C-oriented control architecture is designed. The 4CRC problem has been studied for SFC in the quantum cloud for the first time. The 4CRC algorithms considering two VNF selection strategies are designed. The performance of the proposed algorithms is assessed in terms of success ratio, key consumption ratio and spectrum occupation ratio and achieve the higher success ratio compared with the baseline.

Acknowledgment

This work is supported by National Key Research and Development Program of China (2020YFE0200600), NSFC project (62150032, 61971068, 62021005, U22B2026), and BUPT Excellent Ph.D. Students Foundation (CX2021139).

References

[1] S. Wang, H. Cao and L. Yang, "A survey of service function chains orchestration in data center networks," *in 2020 IEEE Globecom Workshops*, pp. 1-6, 2020.

[2] Use cases of computing-aware service function chaining (SFC), IETF draft-zhang-computing-aware-sfc-usecase-01. [Online]. Available: https://datatracker.ietf.org/doc/draft-zhang-computing-aware-sfc-usecase/.

[3] Yajie Li, Yongli Zhao, Bo Li, Xiaosong Yu, Hui Yang, Xinbo Wang, and Jie Zhang, "Joint balancing of IT and spectrum resources for selecting virtualized network function in inter-datacenter elastic optical networks," *Opt. Express*, vol. 27, pp. 15116-15128, 2019.

[4] M. Zhu, J. Gu, T. Shen, J. Zhang and P. Gu, "Delay-aware and resource-efficient service function chain mapping in inter-datacenter elastic optical networks," *J. Commun. Netw.*, vol. 14, no. 10, pp. 757-770, October 2022.

[5] I. Pedone, A. Atzeni, D. Canavese and A. Lioy, "Toward a complete software stack to integrate quantum key distribution in a cloud environment," *IEEE Access*, vol. 9, pp. 115270-115291, 2021.

[6] A. Aguado et al., "Secure NFV orchestration over an SDN-controlled optical network with time-shared quantum key distribution resources," *J. Light. Technol.*, vol. 35, no. 8, pp. 1357-1362, 2017.

[7] A. Aguado et al., "Quantum cryptography networks in support of path verification in service function chains," *J. Commun. Netw.*, vol. 12, no. 4, pp. B9-B19, April 2020.

[8] Q. Zhu, X. Yu, Y. Zhao, A. Nag and J. Zhang, "Resource allocation in quantum-key-distribution-secured datacenter networks with cloud-edge collaboration," *IEEE Internet Things J.*, early access, doi: 10.1109/JIOT.2023.3242725.

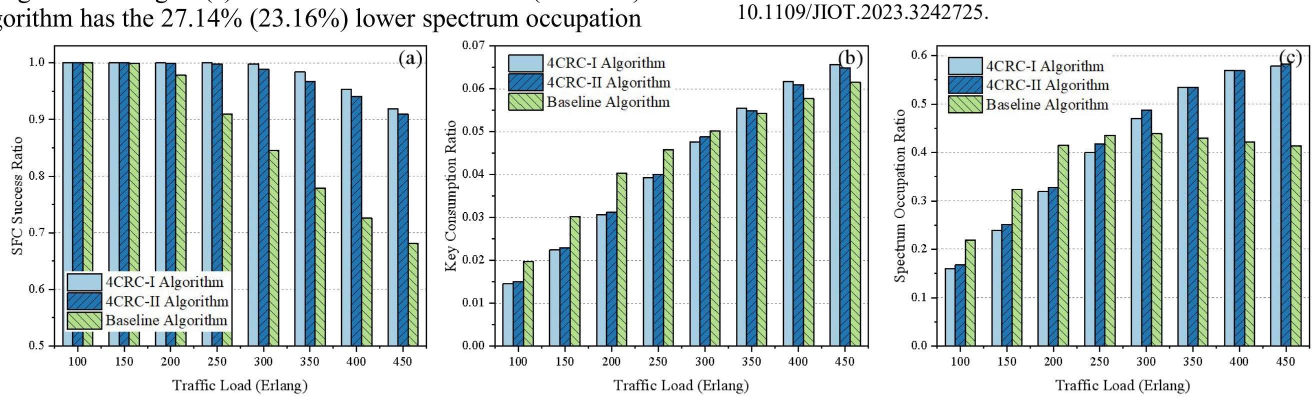

Fig. 2. Simulation results versus traffic load in terms of (a) SFC success ratio; (b) key consumption ratio; (c) spectrum occupation ratio.