Demonstration of Autonomic End-to-End QoS Assurance over SDN-based QKD-Secured Optical Networks

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

Zihao Wang
State Key Lab of Information Photonics and Optical Communications
Beijing Univ. of Posts and Telecommunications
Beijing, China
wizrhao@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

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

***Abstract*—We demonstrate autonomic end-to-end quality-of-service assurance over quantum-key-distribution-secured optical networks, which enhances software-defined-networking control-loops with knowledge engine and cross-layer collaboration. Its performances are verified on our testbed and achieve millisecond-level latency without human intervention.**

Keywords—autonomic, optical network, quality of service, quantum key distribution, software defined networking

I. INTRODUCTION

With the increasing security threats over optical networks and the growing cryptographic demands of applications, quantum key distribution (QKD)-secured optical networks (QKD-ONs) have emerged as a promising solution for realizing secure communications [1]. The QKD-ONs have optical cross connectors (OXC), QKD modules and key managers in nodes interconnected with optical, QKD and key management (KM) links. The symmetric secret keys are distributed between nodes with information-theoretic security and supplied for cryptographic applications. However, due to the complex network conditions and various application scenarios, QKD-ONs face the challenges of ensuring the end-to-end (E2E) quality of service (QoS) in a stable way for the key generation, distribution and supply [2]. Autonomic control mechanisms can enable the network to adjust to the varying network conditions and service demands in a timely and efficient manner without requiring human intervention. The autonomic ability is essential for E2E QoS assurance, especially in QKD-ONs where current key generation rate is relatively low, because untimely human actions to assure QoS will cause the sensitive data over optical fibers eavesdropped with high risks [3].

The autonomic E2E QoS assurance in QKD-ONs relies on closed control-loops which consist of four main phases, i.e. observation, analysis, decision, and action, as shown in Fig. 1(a). These phases enable the QKD-ON to sense its environment, understand its QoS situation, make QoS policy decisions and take actions accordingly, so as to realize the E2E QoS assurance. We have took the lead recently in developing the ITU-T recommendations to specify the requirements for autonomic QoS assurance in QKD networks [4]. Software defined networking (SDN) plays an important role in autonomic control by providing centralized and programmable network control and management. Several studies have enabled SDN in QKD-ONs for routing and key provisioning for QoS assurance [5-8]. But there has

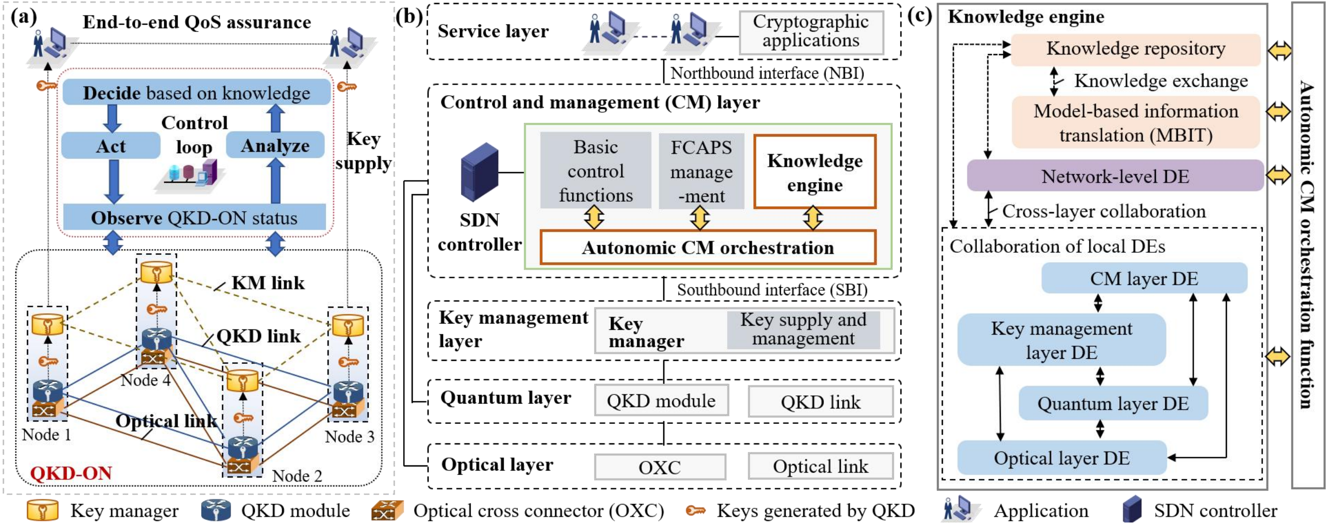


Fig. 1. (a) Autonomic E2E QoS assurance over QKD-ONs; (b) architecture of SDN-based QKD-ONs supporting autonomic E2E QoS assurance; (c) detailed functions in knowledge engine orchestrated by autonomic CM orchestration function.

This work is supported by NSFC project (61971068, 62150032, U22B2026), National Key Research and Development Program of China (2020YFE0200600), Science and Technology Innovation 2030- Major Project (2021ZD0300704).

been no autonomic E2E QoS assurance mechanism such as autonomic protection/recovery in QKD-ONs. This paper demonstrates the novel autonomic E2E QoS assurance in SDN-based QKD-ONs, by introducing a knowledge engine with cross-layer-collaborative QoS assurance (CLC-QA) strategy. The overall feasibility and efficiency of the proposed solution is demonstrated on our SDN-based five-node testbed for the first time, in terms of latency, service success ratio and average key consumption.

II. Autonomic E2E QoS Assurance over SDN-based QKD-ONs

A. Network architecture

The architecture of SDN-based QKD-ONs supporting autonomic E2E QoS assurance is proposed, as illustrated in Fig. 1(b). There are five layers including optical layer, quantum layer, KM layer, control and management (CM) layer and service layer. The optical layer has OXCs and optical links to enable classical communication. The quantum layer has QKD modules and QKD links for key generation using QKD technologies. Key managers are located in the KM layer for each node to perform key supply and key management. There is a KM link connecting key managers to perform IT-secure key relay and communications for KM. Cryptographic applications with E2E QoS requirements are in the service layer, consuming keys from KM layer. The CM layer has the enhanced SDN controller, which communicates with service layer using the northbound interface (NBI), and interconnects with optical, quantum and KM layers using southbound interfaces (SBI). To realize the autonomic E2E QoS assurance in QKD-ONs, the knowledge engine and autonomic CM orchestration functions are newly added. They can also be implemented by a knowledge plane, which is not limited in SDN controller.

The new knowledge engine functions, along with basic control functions and traditional fault, configuration, accounting, performance and security (FCAPS) management, are orchestrated together to realize the closed control-loops according to the E2E QoS requirements. The basic CM functions control, monitor and manage the QKD-ON as a whole and can be specific to different layers' QoS assurance. The detailed functions in knowledge engine orchestrated by autonomic CM orchestration function are shown in Fig. 1(c). There are core elements including knowledge repository, model-based information translation (MBIT), network-level decision-making element (DE) and local DEs, where cross-layer collaboration is enabled. The knowledge repository is to store the observed QoS data and the autonomic E2E QoS assurance policy information. It can exchange knowledge with traditional CM functions and different DEs. The MBIT function provides translation of heterogeneous information such as QoS requirements into layer specific provisioning rules. DEs are introduced as the core autonomic software components to realize the closed control-loops, including observation, analysis, decision and action phases, for auto-properties such as auto-configuration, auto-protection/recovery and auto-optimization. The network-level DE provides global autonomic abilities for QKD-ONs such as supporting network-wide autonomic QKD routing. Local DEs are enabled to realize fast closed control-loop for autonomic QoS assurance specific to optical, quantum, KM and CM layers. Local DEs will be cross-layer collaborated to realize network-level autonomic E2E QoS assurance in QKD-ONs.

B. Autonomic E2E QoS assurance procedure

The cross-layer collaborative QoS assurance (CLC-QA) strategy is introduced for autonomic E2E QoS assurance in QKD-ONs as shown in Fig. 2. The E2E service request is firstly sent to basic control functions in the SDN controller through NBI. Then, the autonomic CM functions get QoS requirement information to translate it into autonomic E2E QoS provisioning rules using MBIT function. The QoS related knowledge is exchanged between the autonomic CM functions and knowledge repository as the base of further selecting different DEs to satisfy E2E QoS requirements. The autonomic CM orchestration selects the required DEs for operation and collaboration. If the specific local DE is needed, the local DE procedure specific to different layers will be operated individually; if the collaboration between different local DEs is needed to construct a network-level DE, the DE collaboration operation will be executed. After DE operation, the autonomic QoS assurance result with success or failure is sent to control functions. Lastly, the response for E2E service whether QoS is assured successfully is returned to the cryptographic applications.

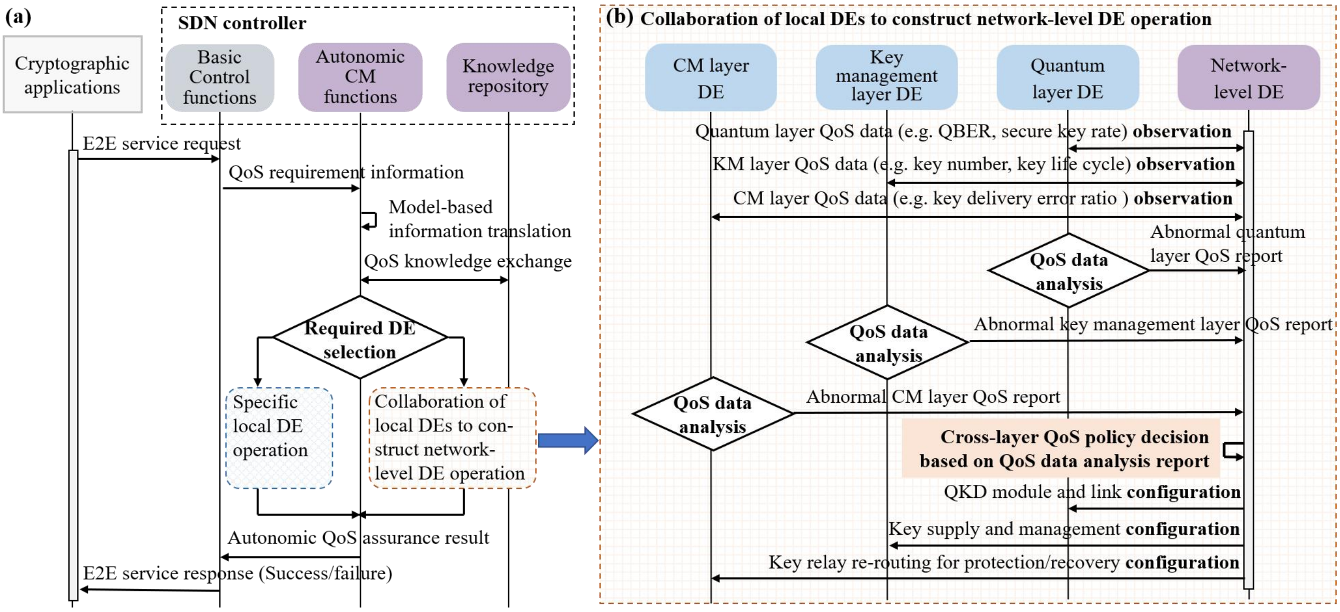

(a)
SDN controller
Cryptographic applications
Basic Control functions
Autonomic CM functions
Knowledge repository
E2E service request
QoS requirement information
Model-based information translation
QoS knowledge exchange
Required DE selection
Specific local DE operation
Collaboration of local DEs to construct network-level DE operation
Autonomic QoS assurance result
E2E service response (Success/failure)
(b) Collaboration of local DEs to construct network-level DE operation
CM layer DE
Key management layer DE
Quantum layer DE
Network-level DE
Quantum layer QoS data (e.g. QBER, secure key rate) observation
KM layer QoS data (e.g. key number, key life cycle) observation
CM layer QoS data (e.g. key delivery error ratio) observation
Abnormal quantum layer QoS report
QoS data analysis
Abnormal key management layer QoS report
QoS data analysis
QoS data analysis
Abnormal CM layer QoS report
Cross-layer QoS policy decision based on QoS data analysis report
QKD module and link configuration
Key supply and management configuration
Key relay re-routing for protection/recovery configuration

Fig. 2. (a) General procedure of autonomic E2E QoS assurance in QKD-ONs; (b) collaboration of local DEs to construct network-level DE operation.

Fig. 2(b) shows an example of collaboration procedures of local quantum, KM and CM DEs to construct network-level DE operation, with the objective of auto-protection/recovery for services in QKD-ONs. In the observation phase, the network-level DE observes the quantum layer QoS data such as quantum bit error rate (QBER) and secure key rate from quantum layer DE, the KM layer QoS data such as available key number and key life cycle in key managers from KM layer DE, and the CM layer QoS data such as key delivery error ratio from CM layer DE. Then in the analysis phase, the observed QoS data is analyzed to find if there are abnormal quantum, KM and CM layer QoS status needing to be reported to network-level DE. Based on the QoS data analysis report, network-level DE decides the cross-layer QoS policy, including the wavelength allocation, key formatting and key relay re-routing. In the action phase, the configuration information is sent for specific local DEs and acted using basic control functions of the SDN controller.

III. Performance Evaluation

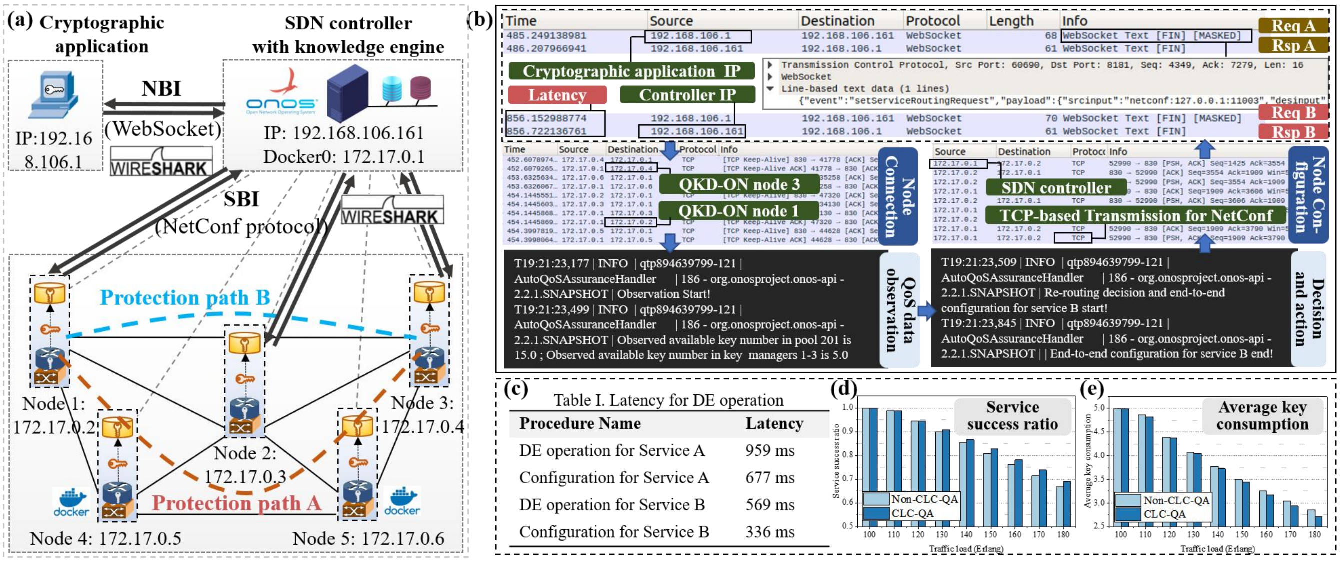
To experimentally evaluate the proposed architecture and procedures, we set up SDN-based QKD-ONs for supporting autonomic E2E QoS assurance, as shown in Fig. 3(a). In KM, quantum and optical layers, five NetConf-enabled QKD-ON nodes are interconnected in a mesh topology. They are realized on Docker containers with data modeling language YANG implementation running on a PC with Intel Core i7-10510U CPU 795@1.80 GHz 2.30 GHz and 16-GB memory. Docker is a platform that allows developers to easily create, deploy, and run applications in containers. Hence, the configured Docker containers according to the QKD-ON parameters can be considered as real nodes and links. QKD and optical links are wavelength division multiplexed. QKD keys are generated in ~10 Kbps using BB84 and stored in key managers [1]. For CM layer, the NetConf-based SDN controller with knowledge engine is built on the open network operating system (ONOS) platform, to realize autonomic control-loops in QKD-ONs. The service layer with cryptographic applications are deployed in a PC and communicates with controller through WebSocket NBI.

The evaluation results of autonomic E2E QoS assurance procedures are in Fig. 3(b) mainly captured by Wireshark network protocol analyzer. The E2E service request and response (WebSocket messages) between the application and SDN controller represent the beginning and end of autonomic QoS assurance, during which controller checks node connection status, observes QoS data, analyzes QoS data, decides QoS policies and configures QKD-ON nodes via NetConf messages (transmitted based on TCP protocol). The services A (security-priority) and B (latency-priority) are carried using CLC-QA strategy in the testbed, which request the E2E key-relay protection between node 1 and 3 to avoid accident key provisioning failure. Based on the observed quantum, KM and CM layer QoS data, the knowledge engine in SDN controller makes decisions as follows: setting the protection path A 1-2-3 for service A with required keys in AES 256-bit format, and setting the protection path B 1-3 for service B with required keys in AES 128-bit format, where the former QoS policy provides the higher security while the latter QoS policy achieves the lower latency.

Fig. 3(c) summarizes the latency for DE operation. The overall DE operation latency achieves millisecond level, and is 959 ms and 569 ms for services A and B respectively. The configuration latency after decision for services A and B is 677 ms and 336 ms respectively. The reason is that the configuration times of one-hop path are smaller than that of two-hop path. We also evaluate network-level QoS performances of CLC-QA strategy under heavy traffic load scenario for autonomic protection, and compared with non-cross-layer-collaborative QoS assurance (non-CLC-QA) strategy in terms of service success ratio (SSR) and average key consumption (AKC) shown in Figs. 3(d-e). The E2E key requirements of 10^5 services are randomly in the range [1.28, 6.40] kbits. We can find that CLC-QA strategy achieves the higher SSR and lower AKC. Its performance advantages increase when the traffic load becomes heavier. This is because the CLC-QA strategy can adapt to the network resource status and make protection decisions with the cross-layer collaborative perspective to adjust the key formats and routes under different E2E QoS requirements autonomically.

IV. Conclusion

In this paper, we present the autonomic E2E QoS assurance over the SDN-based QKD-ONs. Our experiments demonstrate DEs in knowledge engine can utilize the cross-layer-collaborative strategy while realizing millisecond-level control-loops, improving the QKD-ON autonomic ability.



```
Time            Source           Destination      Protocol   Length  Info
485.249138981   192.168.106.1    192.168.106.161  WebSocket      68  WebSocket Text [FIN] [MASKED]
486.207966941   192.168.106.161  192.168.106.1    WebSocket      61  WebSocket Text [FIN]
  ▸ Transmission Control Protocol, Src Port: 60690, Dst Port: 8181, Seq: 4349, Ack: 7279, Len: 16
  ▸ WebSocket
  ▾ Line-based text data (1 lines)
      {"event":"setServiceRoutingRequest","payload":{"srcinput":"netconf:127.0.0.1:11003","desinput"
856.152988774   192.168.106.1    192.168.106.161  WebSocket      70  WebSocket Text [FIN] [MASKED]
856.722136761   192.168.106.161  192.168.106.1    WebSocket      61  WebSocket Text [FIN]
```

```
Time           Source      Destination  Protocol Info
452.6078974…   172.17.0.4  172.17.0.1   TCP      [TCP Keep-Alive] 830 → 41778 [ACK] Se
452.6079265…   172.17.0.1  172.17.0.4   TCP      [TCP Keep-Alive ACK] 41778 → 830 [ACK
453.6325634…   172.17.0.6  172.17.0.1            35258 [ACK] Se
453.6326067…   172.17.0.1  172.17.0.6            258 → 830 [ACK
454.1445551…   172.17.0.2  172.17.0.1   TCP      [TCP Keep-Alive] 830 → 47320 [ACK] Se
454.1445603…   172.17.0.3  172.17.0.1            34130 [ACK] Se
454.1445868…   172.17.0.1  172.17.0.3            130 → 830 [ACK
454.1445869…   172.17.0.1  172.17.0.2   TCP      [TCP Keep-Alive ACK] 47320 → 830 [ACK
454.3997819…   172.17.0.5  172.17.0.1   TCP      [TCP Keep-Alive] 830 → 44628 [ACK] Se
454.3998064…   172.17.0.1  172.17.0.5   TCP      [TCP Keep-Alive ACK] 44628 → 830 [ACK
```

```
Source      Destination  Protocc Info
172.17.0.1  172.17.0.2   TCP     52990 → 830 [PSH, ACK] Seq=1425 Ack=3554
172.17.0.2  172.17.0.1   TCP     830 → 52990 [ACK] Seq=3554 Ack=1909 Win=5
172.17.0.2                       → 52990 [PSH, ACK] Seq=3554 Ack=1909
172.17.0.1                       → 830 [ACK] Seq=1909 Ack=3606 Win=5
172.17.0.2  172.17.0.1   TCP     830 → 52990 [PSH, ACK] Seq=3606 Ack=1909
172.17.0.1
172.17.0.2
172.17.0.1  172.17.0.2   TCP     52990 → 830 [ACK] Seq=1909 Ack=3790 Win=5
172.17.0.1  172.17.0.2   TCP     52990 → 830 [PSH, ACK] Seq=1909 Ack=3790
```

```
T19:21:23,177 | INFO  | qtp894639799-121 |
AutoQoSAssuranceHandler      | 186 - org.onosproject.onos-api -
2.2.1.SNAPSHOT | Observation Start!
T19:21:23,499 | INFO  | qtp894639799-121 |
AutoQoSAssuranceHandler      | 186 - org.onosproject.onos-api -
2.2.1.SNAPSHOT | Observed available key number in pool 201 is
15.0 ; Observed available key number in key  managers 1-3 is 5.0
```

```
T19:21:23,509 | INFO  | qtp894639799-121 |
AutoQoSAssuranceHandler      | 186 - org.onosproject.onos-api -
2.2.1.SNAPSHOT | Re-routing decision and end-to-end
configuration for service B start!
T19:21:23,845 | INFO  | qtp894639799-121 |
AutoQoSAssuranceHandler      | 186 - org.onosproject.onos-api -
2.2.1.SNAPSHOT | | End-to-end configuration for service B end!
```

Table I. Latency for DE operation

Procedure Name	Latency
DE operation for Service A	959 ms
Configuration for Service A	677 ms
DE operation for Service B	569 ms
Configuration for Service B	336 ms

Fig. 3. (a) SDN-based QKD-ON setup; (b) evaluation results of autonomic QoS assurance procedures; (c) latency for DE operation; (d) SSR; (e) AKC.

REFERENCES

[1] P. Sharma, A. Agrawal, V. Bhatia, S. Prakash and A. K. Mishra, "Quantum Key Distribution Secured Optical Networks: A Survey," IEEE Open Journal of the Communications Society, vol. 2, pp. 2049-2083, August, 2021.

[2] M. Park, K. Lee, K. Seol, M. Lee and H. Kim, "Quality of Service Evaluation over a 496 km Quantum Key Distribution Network," in 2022 International Conference on Software, Telecommunications and Computer Networks (SoftCOM), Split, Croatia, 2022, pp. 1-3.

[3] Draft Recommendation ITU-T Y.QKDN-amc, "Quantum key distribution networks - requirements and architectural model for autonomic management and control", [Online] https://www.itu.int/md/T22-SG13-230313-TD-WP3-0235.

[4] Draft Recommendation ITU-T Y.QKDN-qos-auto-rq, "Quantum key distribution networks - Requirements for autonomic quality of service assurance", [Online] https://www.itu.int/md/T22-SG13-230313-TD-WP1-0344.

[5] A. Aguado et al., "Secure NFV Orchestration Over an SDN-Controlled Optical Network With Time-Shared Quantum Key Distribution Resources," in Journal of Lightwave Technology, vol. 35, no. 8, pp. 1357-1362, 15 April, 2017.

[6] O. Alia, R. S. Tessinari, E. Hugues-Salas, G. T. Kanellos, R. Nejabati and D. Simeonidou, "Dynamic DV-QKD Networking in Trusted-Node-Free Software-Defined Optical Networks," in Journal of Lightwave Technology, vol. 40, no. 17, pp. 5816-5824, 1 Sept, 2022.

[7] Y. Cao, Y. Zhao, J. Zhang, and Q. Wang, "Software-Defined Heterogeneous Quantum Key Distribution Chaining: An Enabler for Multi-Protocol Quantum Networks," IEEE Communications Magazine, vol. 60, no. 9, pp. 38-44, 2022.

[8] R. S. Tessinari et al., "Demonstration of a Dynamic QKD Network Control Using a QKD-Aware SDN Application Over a Programmable Hardware Encryptor," in 2021 Optical Fiber Communications Conference and Exhibition (OFC), San Francisco, CA, USA, 2021, pp. 1-3.