INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2017-2020

SG13-TD550/WP3

STUDY GROUP 13

Original: English

Question(s): 16/13 Virtual, 1-12 March 2021

TD

Source: Editors

Title: Draft Recommendation ITU-T Y. QKDN_SDNC: "Quantum Key Distribution Networks - Software Defined Networking Control"

Purpose: Information

Contact:	Yongli Zhao Beijing University of Posts and Telecommunications. China	Tel: +86-10-61198108 E-mail: yonglizhao@bupt.edu.cn
Contact:	Xiaosong Yu Beijing University of Posts and Telecommunications. China	Tel: +86-10-61198108 E-mail: xiaosongyu@bupt.edu.cn
Contact:	Zhangchao Ma CAS Quantum Network Co., Ltd. China	Tel: +86-10-83057625 E-mail: mazhangchao@casquantumnet.com
Contact:	Junsen Lai Ministry of Industry and Information Technology (MIIT). China	Tel: +86-10-62300592 E-mail: laijunsen@caict.ac.cn

Keywords: QKDN (Quantum Key Distribution Network), SDN (Software defined networking), functional architecture, reference point, operational procedure

Abstract: This document includes proposed modifications to the draft Recommendation ITU-T Y.QKDN_SDNC " Software Defined Network Control for Quantum Key Distribution Networks " according to the editor's notes after December 2020 SG13RGM Q16/13 meeting.

Summary

The initial draft Recommendation Y.QKDN_SDNC was created in the last Q16/13 rapporteur meeting in Geneva June 2019 and the base line document was included in TD271-WP3. This output document includes proposed modifications based on the contribution C76 after the December 2020 SG13RGM Q16/13 meeting. The updated texts and editor notes are included.

Annex I

Draft Recommendation ITU-T Y. QKDN_SDNC

Software Defined Networking Control for Quantum Key Distribution Networks

Summary

Recommendation ITU-T Y.QKDN_SDNC specifies the requirements, functional architecture, reference points, hierarchical SDN controller, overall operational procedures of SDN control, and controllable elements for SDN in QKDN and security considerations.

Keywords

QKDN (Quantum Key Distribution Network), SDN (Software defined networking), functional architecture, reference point, operational procedure, SDN controller, hierarchical SDN controller, controllable element, security consideration.

Table of Contents

Draft Recommendation ITU-T Y. QKDN_SDNC

Quantum Key Distribution Networks - Software Defined Networking Control

1. Scope

This recommendation specifies the requirements, functional architecture, reference points, overall operational procedures of software defined networking (SDN) control in QKDN and so on. The scope of this draft recommendation covers:

- Requirements for SDN control in QKDN;
- Functional architecture of SDN control in QKDN;
- Reference points of SDN control in QKDN;
- Hierarchical SDN controller in QKDN;
- Overall operational procedures of SDN control in QKDN;
- Controllable elements for SDN control in QKDN;
- Security Considerations;

Appendix I: use cases of SDN control in QKDN;

Appendix II: comparison of control methods between traditional QKDN and SDN based QKDN;

Appendix III: controllable elements for SDN in QKDN.

2. References

[ITU-T Y.3800] Recommendation ITU-T Y.3800 (2019), *Framework for Networks to support Quantum Key Distribution*.

[ITU-T Y.3801] Recommendation ITU-T Y.3801 (2020), *Functional requirements for quantum key distribution networks*.

[ITU-T Y.3802] Recommendation ITU-T Y.3802 (2020), *Functional architecture of the Quantum Key Distribution network.*

[ITU-T Y.3803] Recommendation ITU-T Y.3803 (2020), *Key management for quantum key distribution network*.

[ITU-T Y.3804] Recommendation ITU-T Y.3804 (2020), *Control and Management for Quantum Key Distribution Network.*

[ITU-T Y.3300] Recommendation ITU-T Y.3300 (2014), *Framework of software-defined networking*

[ITU-T Y.3301] Recommendation ITU-T Y.3301 (2016), *Functional requirements of software-defined networking*

[ITU-T Y.3302] Recommendation ITU-T Y.3302 (2017), *Functional architecture of software-defined networking*

[ITU-T Y.3320] Recommendation ITU-T Y.3320 (2014), *Requirements for applying formal methods to software-defined networking*

[ITU-T Y.3321] Recommendation ITU-T Y.3321 (2015), *Requirements and capability framework for NICE implementation making use of software-defined networking technologies*

[ITU-T Y.3322] Recommendation ITU-T Y.3322 (2016), *Functional architecture for NICE implementation making use of software-defined networking technologies*

[ETSI ISG-QKD] ISG-QKD (2011), *Towards Standardization of Quantum Key Distribution - Use Cases for QKD*

3. Terms and definitions

3.1. Terms defined elsewhere

This recommendation uses the following terms defined elsewhere:

3.1.1. Quantum key distribution (QKD) [b-ETSI GR QKD 007]: Procedure or method for generating and distributing symmetrical cryptographic keys with information theoretical security based on quantum information theory.

3.1.2. Quantum key distribution network (QKDN) [ITU-T Y.3800]: A network comprised of two or more quantum key distribution (QKD) nodes connected through QKD links.

NOTE – A QKDN allows sharing keys between the QKD nodes by key relay when they are not directly connected by a QKD link.

3.1.3. Software-defined networking (SDN) [ITU-T Y.3300]: A set of techniques that enables to directly program, orchestrate, control and manage network resources, which facilitates the design, delivery and operation of network services in a dynamic and scalable manner.

3.2. Terms defined in this Recommendation

This recommendation defines the following terms:

<To be added>

4. Abbreviations and acronyms

This recommendation uses the following abbreviations and acronyms:

QKD	Quantum Key Distribution
QKDN	Quantum Key Distribution Networks
SDN	Software Defined Networking
QoS	Quality of Service

5. Conventions

In this Recommendation:

T “is required to” indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

The keywords “is prohibited from” indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

The keywords “is recommended” indicate a requirement which is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance.

The keywords "is not recommended" indicate a requirement which is not recommended but which is not specifically prohibited. Thus, conformance with this specification can still be claimed even if this requirement is present.

The keywords "can optionally" indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

6. Introduction

Quantum key distribution (QKD) technology has been ready for practical use in the existing and future communications and security infrastructures. [ITU-T Y. 3800] gives an overview on networks supporting QKD, and [ITU-T Y.3802] specifies the functional architecture of quantum key distribution networks (QKDN). In QKDN, network control is one of the most important fundamental functions, and [ITU-T Y.3804] has specified the control and management functions for QKDN. However, the network control proposed in [ITU-T Y.3804] is operated under the distributed architecture. The QKDN controller does not deal with keys themselves and keys are supplied directly from a key manager to a cryptographic application. The control method lacks the operational flexibility and global view of networks.

As one of the most promising control technologies, software defined networking (SDN) [ITU-T Y.3300] has several advantages in traditional communication networks. On the one hand, it supports centralized, programmable, and hierarchical control manner by SDN controller; on the other hand, it can provide services for applications in a fast way by opening northbound interfaces between control layer and service layer. This change of control method in QKDN provides another method to realize control functionalities by introducing logically centralized and programmable control of network resources through standardized interfaces and protocols.

The considerations of introducing SDN into QKDN are as follows:

- The centralized control manner of SDN helps to collect the overall information of QKDN independent of whether QKDN is distributed or not. It is helpful to improve the performance monitoring and routing decision.

- The tunable components of QKDN (e.g., tunable laser and tunable optical switch) can be programed and controlled dynamically by SDN controller which has southbound interfaces. For example, tunable optical switch can be controlled dynamically by SDN controller to construct different quantum channels between different nodes.

- SDN supports hierarchical control manner, and it could be adopted in multi-domain or multi-vendor QKDN. Under such scenarios, the implementation of each controller for different domains/vendors are independent of others, which makes the network control much easier. One upper layer controller is in charge of several lower layer controllers.

- By opening the northbound interface which is defined as the application-control interface [ITU-T Y.3300] used for interactions between the service layer and the SDN control layer in QKDN, SDN can provide fast provisions of services for applications. The overall operational procedures and its advantages are given in clause 11 of this recommendation.

- SDN supports QKDN virtualization that combines physical QKDN resources and QKDN functionality into a single software-based administrative entity, a virtual QKDN, according to different demands of specific customers or applications. With the programmability and controllability of southbound interfaces, it enables the creation of logically isolated network

partitions over shared physical QKDNs and realizes QKD in network partitions with sharing the same resources in an efficient way.

NOTE – The QKDN resources that can be virtualized include QKDN topology (nodes and links) and QKD-key resources.

7. Requirements for SDN controller in QKDN control layer

The requirements for QKDN control layer are defined in [ITU-T Y.3801], and this recommendation specifies the extra requirements for SDN controller in QKDN control layer.

- Req_1. SDN controller is required to support the ability of QKDN application registration, which enables the fast provisioning of network applications in the service layer.
- Req_2. SDN controller is required to support the ability of acquiring and updating of network topology information from quantum layer or SDN child controllers (in hierarchical SDN control architecture).
- Req_3. SDN controller is required to support the ability of QKDN virtualization, which can provide a logical isolation of virtual quantum keys from both the network view and the user view.
- Req_4. SDN controller is required to support the ability of QKDN programmable elements control, which enables the control on the programmable elements in the quantum layer.

8. Functional architecture for SDN control in QKDN

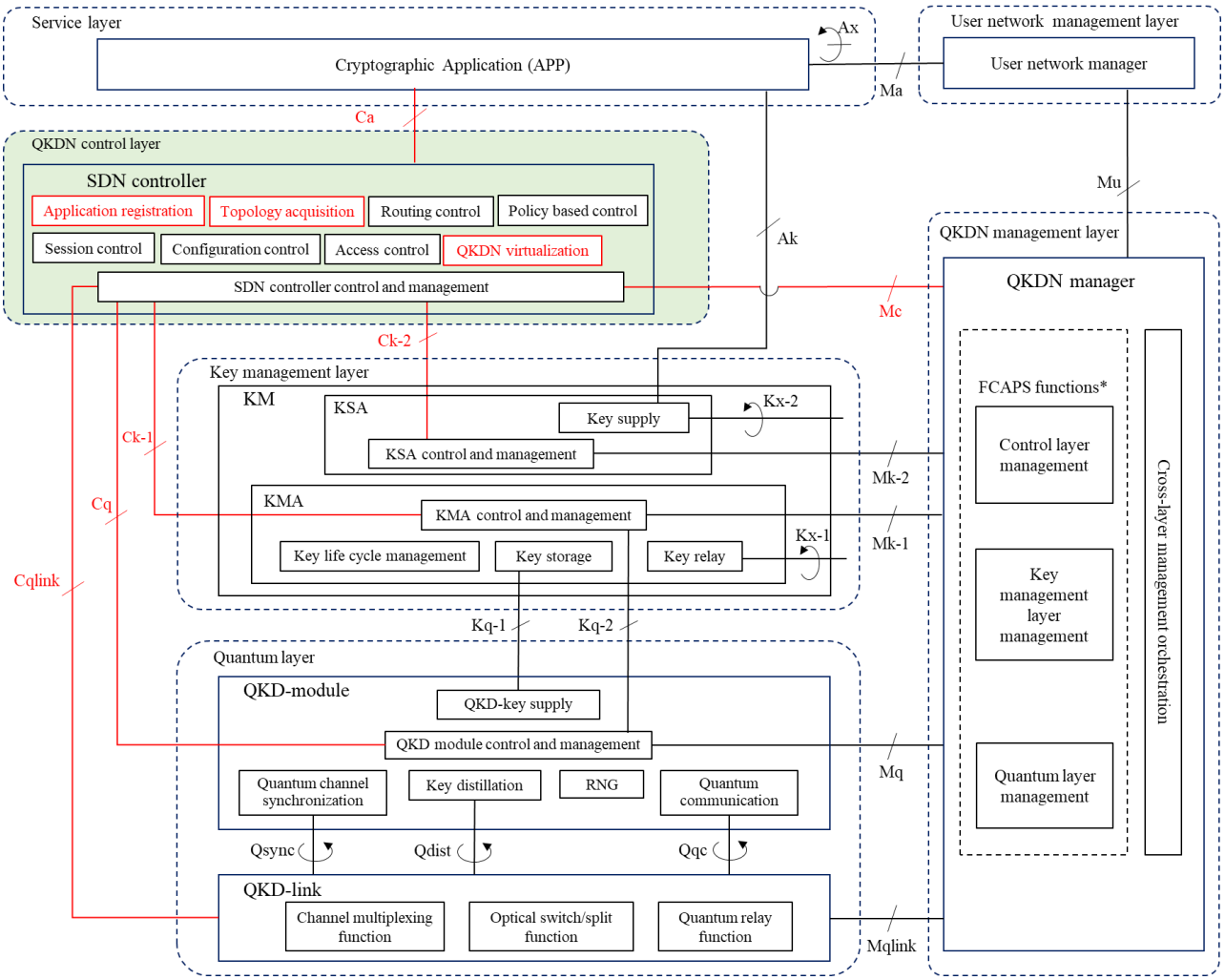

Fig. 1 Functional architecture for SDN control in QKDN
(* FCAPS represents fault, configuration, accounting, performance and security management)

Based on the conceptual structure and functional architecture model for QKDN defined in [ITU-T Y. 3800] and [ITU-T Y.3802] respectively, the functional architecture for SDN control in QKDN is specified in Fig. 1. The detailed description of functional elements as well as the reference points are given in [ITU-T Y.3800] and [ITU-T Y.3802], and this recommendation specifies SDN related functional elements in QKDN.

- Quantum layer: the functional elements in the quantum layer including QKD-link and QKD-module are enabled to communicate with SDN controller conveniently. The parameters of QKD-link and QKD-module such as quantum key generation rate, transition power, receive power, etc., could be adjusted by SDN controller in QKDN control layer.

- Key management layer: the functional elements in the key management layer including key management agent (KMA) and key supply agent (KSA) exchange control and management messages with SDN controller. With SDN technology, virtual quantum key pool (VQKP) could be constructed in QKDN. Here, VQKP is defined to be the virtual QKD-key storage entities for any quantum node pairs in QKDN to enhance the quantum key management.

- QKDN control layer: the functional element in QKDN control layer is SDN controller. It controls the variable resources to ensure secure, stable, efficient, and robust operations of QKDN. The functions of SDN controller include application registration, topology acquisition, routing control, policy-based control, session control, configuration control, access control and QKDN virtualization. In addition, different from traditional QKDN controllers, SDN controllers have northbound interfaces between service layer and QKDN control layer. SDN controller opens northbound interfaces to cryptographic applications in service layer, which enables the fast service provisioning for applications in QKDN.

- Service layer: the cryptographic applications in service layer are to utilize the shared key pairs provided by the QKDN and perform encrypted communication between remote parties. The cryptographic applications could be initialized and provided by SDN controller with its northbound interface. Three typical cryptographic applications in the service layer are point-to-point applications, point-to-multipoint applications, and multipoint-to-multipoint applications.

- QKDN management layer: the elements in QKDN management layer communicate with SDN controller to get configuration and management information.

- User network management layer: the user network management layer function is the same as that in [ITU-T Y.3802].

9. Reference points

Most of the reference points in Fig. 1 have been defined in [ITU-T Y.3802] , and this recommendation only defines the newly added and different ones.

- **Ca:** reference point between cryptographic application and SDN controller in the QKDN control layer. It is responsible for service provisioning of cryptographic applications.

- **Ck-1:** reference point between SDN controller and KMA. It is responsible for SDN controller to communicate control information with the KMA.

- **Ck-2:** reference point between SDN controller and KSA. It is responsible for SDN controller to communicate control information with the KSA.

- **Cq:** reference point between SDN controller and QKD module. It is responsible for the SDN controller to communicate control information with QKD module.
- **Cqlink:** reference point between SDN controller and QKD link. It is responsible for the SDN controller to communicate control information with the QKD link.
- **Mc:** reference point between QKDN manager and SDN controller. It is responsible for the QKDN manager to communicate management information with the SDN controller.

10. Hierarchical SDN controller in QKDN

Clause 8 describes the basic functional architecture for SDN control in QKDN. However, in certain scenarios, only one single SDN controller is not suitable for the overall control in QKDN, and hierarchical SDN controller could be adopt. Fig. 2 illustrates the hierarchical SDN controller in QKDN. Under such scenario, SDN controllers are organized in a hierarchical way, and the functions and implementations of each SDN controller is independent of each other. The hierarchical controller is responsible for service provision within its control range. Each layer SDN controller has its northbound interface to communicate with the service layer, but only the first layer has a southbound interface for controlling the controllable elements and collecting information from key management layer and quantum layer. Most of the reference points in Fig. 2 have been defined in clause 9, and this recommendation only describes the newly added and updated ones.

- **Ca-x:** reference point between cryptographic application and the x_{th} layer SDN controller under hierarchical SDN control scenarios. It is responsible for service provisioning of network applications using the x_{th} layer SDN controller.
- **I-CPI**: reference point between SDN controllers in adjacent layers under hierarchical SDN control scenarios. It is responsible for the communication between the SDN controllers in adjacent layers.

  NOTE-The reference point needs to be standardized when it is realized by different domains; on the other hand, the reference point doesn’t need the standardization when it is realized by only one domain.

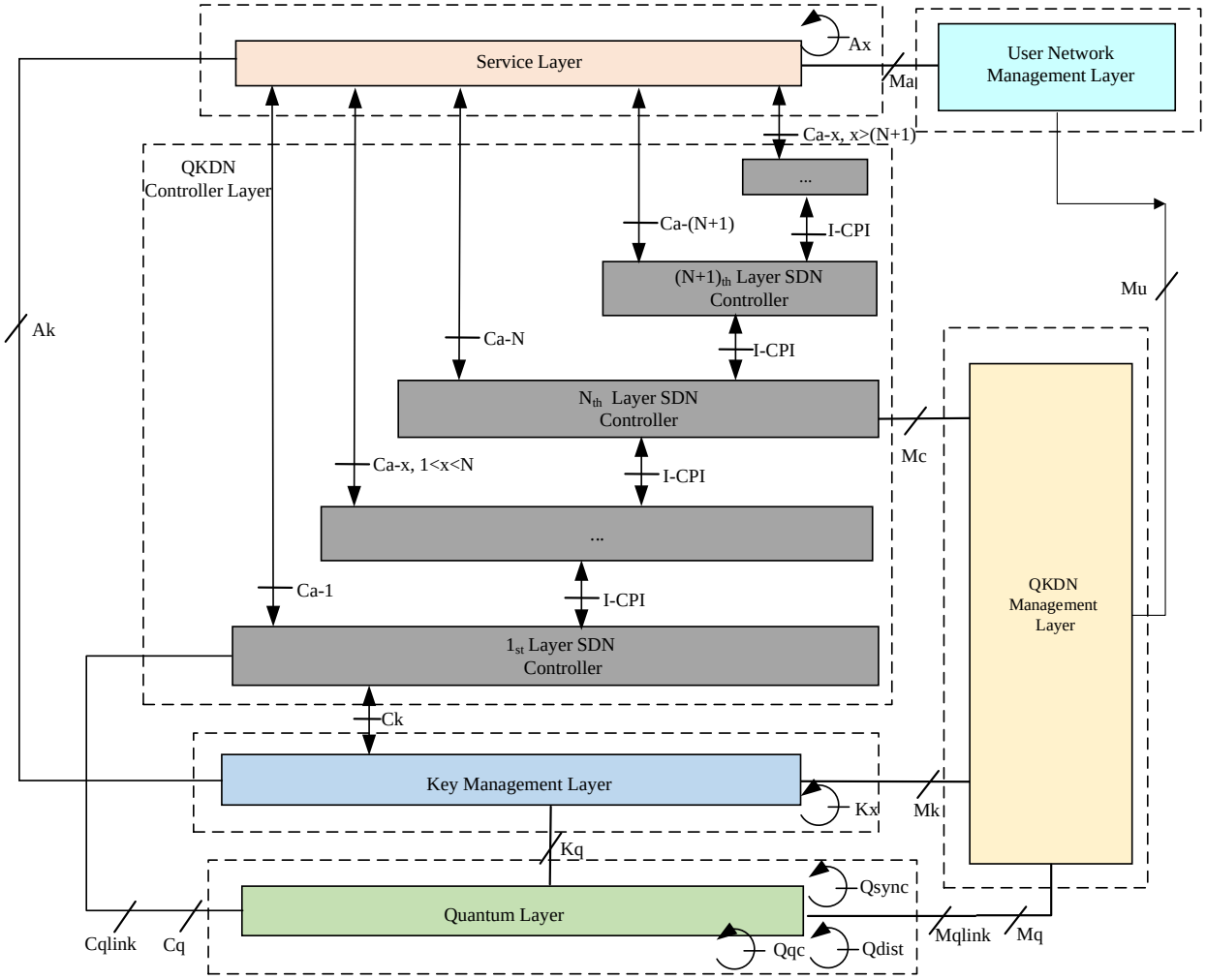

Fig. 2 Hierarchical SDN controller in QKDN

For example, in the multi-domain QKDN as illustrated in Fig. 3, each domain could develop their 1_{st} layer SDN controller that is able to control elements in the domain through southbound interfaces. The 2_{nd} layer SDN controller could be developed to get in charge of the 1_{st} layer SDN controllers and the 3_{rd} layer SDN controller could be developed to get in charge of the 2_{nd} layer SDN controllers. Here, we consider three services: 1) for provisioning the **service within domain A**, it only needs to operate the 1_{st} layer SDN controller C_A; 2) for provisioning the **service across domain A and B**, it needs to operate the 2_{nd} layer SDN controller C_{AB} which controls the 1_{st} layer SDN controller C_A and C_B; 3) for provisioning the **service across domain A and D**, it needs to operate the 3_{rd} layer SDN controller which controls the 2_{nd} layer SDN controller C_{AB} and C_{CD}.

Note that, each domain in QKDN is the domain that a single first layer SDN controller controls. It is implemented by one vendor but is provided with different administrative authority. The first layer SDN controllers control different network domains respectively, and the higher layer SDN controller is responsible for the inter domain cooperation and SDN controller orchestration.

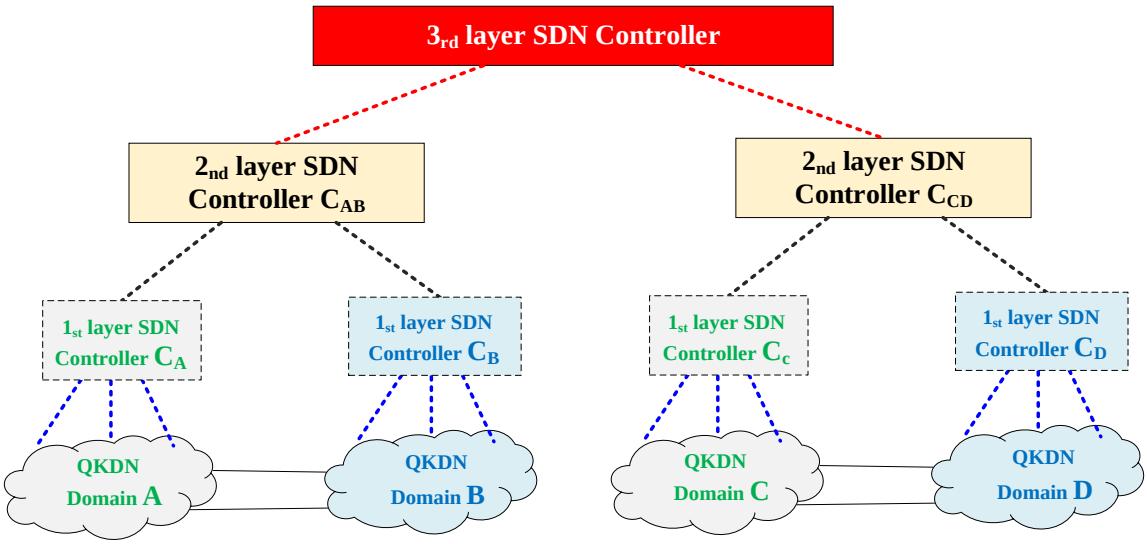

Fig. 3 Hierarchical SDN control in multi-domain QKDN

11. Overall operational procedures of SDN control in QKDN

Different from other traditional operational procedures of QKD network functions without SDN control, the operational procedures of SDN control in QKDN reduce the time for provisioning different services by directly providing keys to the service layer using SDN control through skipping the QKDN manager. The SDN controller can also enable more efficient key resource utilization by deciding the end of key generation and controlling the management monitor in a global view. Apart from that, the SDN technology improves the flexibility of service provisioning and provides services for applications in a fast way by opening the interface between QKDN control layer and service layer. Based on the functional architecture for SDN control defined in clause 8, this clause describes the overall operational procedures of SDN control in QKDN.

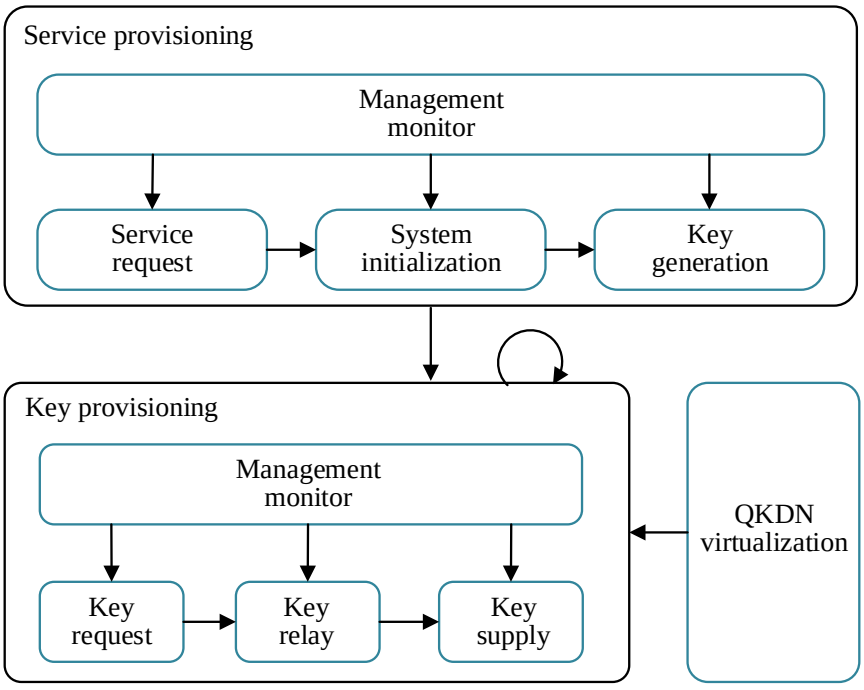

Fig. 4 The overall operational procedures of SDN control in QKDN

The relationship of the overall operational procedures of SDN control in QKDN is shown in Fig. 4. There are two high-level modes in the overall operational procedures, containing service provisioning mode and key provisioning mode. When the service request arrives, the QKDN enters the service

provisioning mode. The system is initialized and quantum keys are generated under the control of the SDN controller. When the key request arrives, the QKDN enters the key provisioning mode, the key request, relay and supply phase decide the route information by using the SDN controller and pushes up quantum keys for the service. At the same time, the real-time network management monitoring will be performed to collect and monitor all the QKD links in the service provisioning phase and analyze the status of key management in the key provisioning phase with the global view enabled by the SDN controller. The QKDN virtualization is the function that can construct multiple logical QKDNs on a physical QKDN. The implementation of QKDN virtualization needs the support of "Key provisioning", so that it remaps the virtual resources and physical QKDN resources to efficiently meet the demands of specific services or applications. The overall operational procedures include:

1) Normal operation mode: Service request and system initialization phase

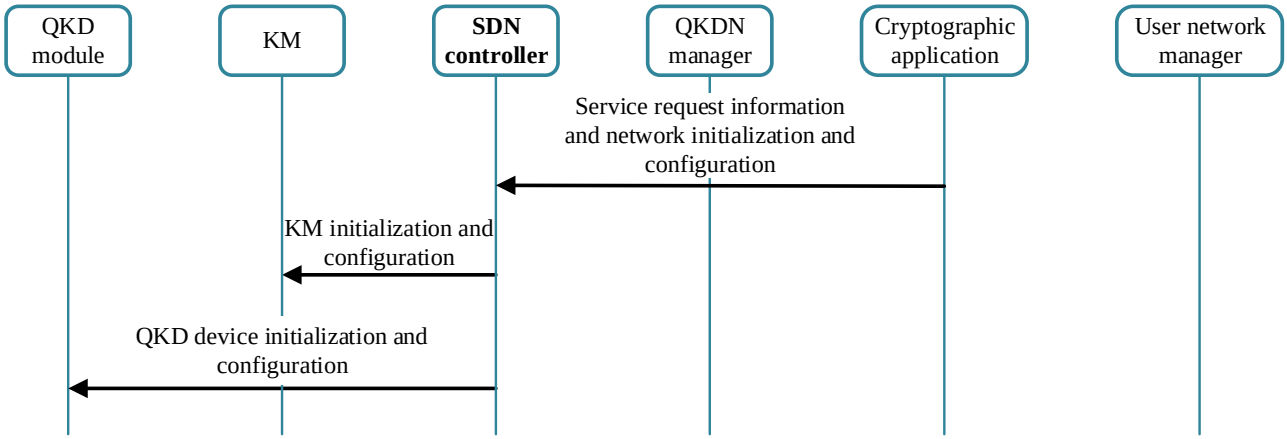

Fig. 5 Service provisioning and system initialization phase

Fig. 5 illustrates procedures of SDN control for service request and system initialization with SDN technology. At this phase, the cryptographic application in the service layer directly provides service request information and network initialization and configuration to the SDN controller, not bothering to provide information to QKDN manager. Then the SDN controller initiates QKDN controller, the KM and QKD module to configure the QKD network.

2) Normal operation mode: Key generation phase

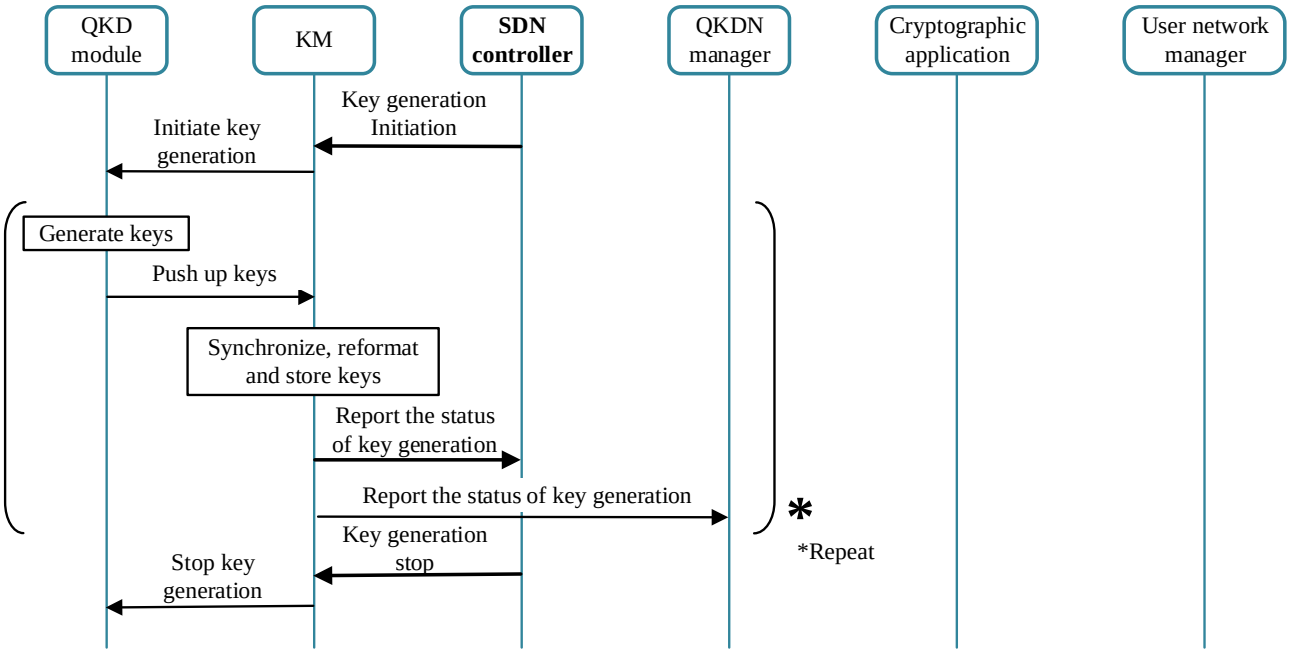

Fig. 6 Key generation phase

Fig. 6 illustrates procedures of SDN control for key generation with SDN technology. In the phase, the SDN controller sends the initiation of key generation to the QKD module directly. Then, the physical key generation procedures are repeated until the SDN controller sends the instruction to stop it. The status of key generation is reported to both SDN controller and QKDN manager for future control and management requirements.

3) Normal operation mode: Key request, relay and supply phase

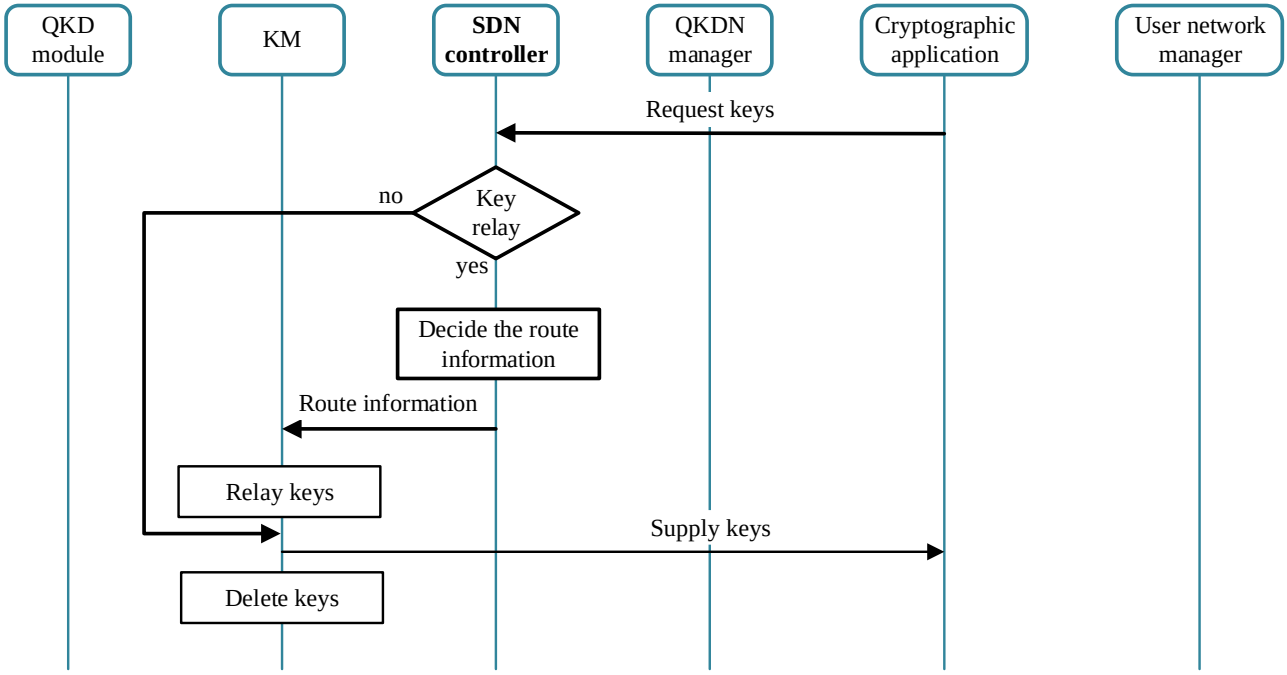

Fig. 7 Key request and supply phase

Fig. 7 illustrates procedures of SDN control for key request and supply. For that the SDN controller knows the whole key resource status of each node, a cryptographic application in the user network sends IT-secure key request information to the SDN controller in the QKD network. Then SDN controller checks the need to relay keys. If it needs to relay keys for service provisioning, the SDN controller will decide the routing information. Based on the routing information, the KM initiates the key relay procedures between the originating QKD node and the destination QKD node and executes key relay according to the control by the SDN controller; if it doesn't need key relay, the KM supplies keys to the requesting cryptographic application directly. Finally, the KM pushes up keys to the requesting cryptographic application.

4) Normal operation mode: Management monitor phase

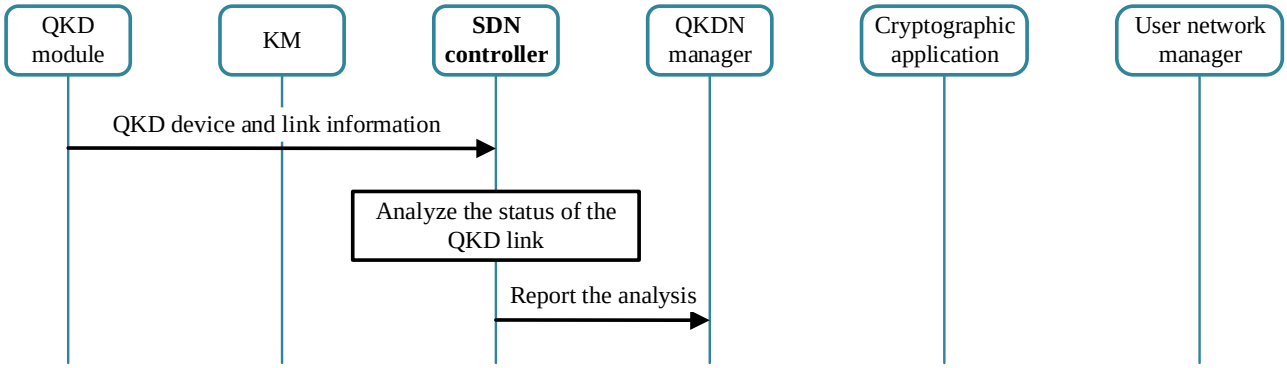

Fig. 8 Management monitor phase in the service provisioning mode

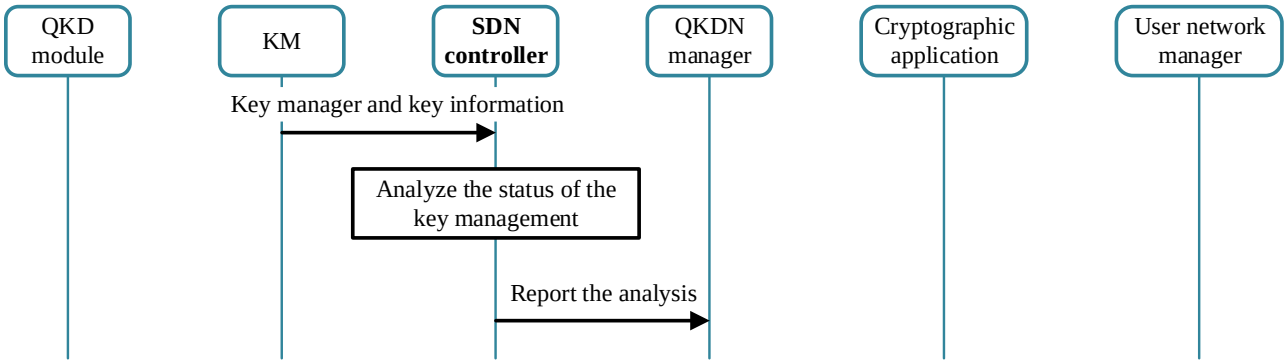

Fig. 9 Management monitor phase in the key provisioning mode

Fig. 8 and Fig.9 illustrate the procedures for management monitor with the SDN controller. In the service provisioning mode, the QKD device and link information are sent to the SDN controller through its south interface. In the key provisioning mode, the SDN controller collects the key manager and key information from KM. The status of the QKD link and key management are analysed by the SDN controller. Then the SDN controller reports the analysis to the QKDN manager.

5) Normal operation mode: QKDN virtualization phase

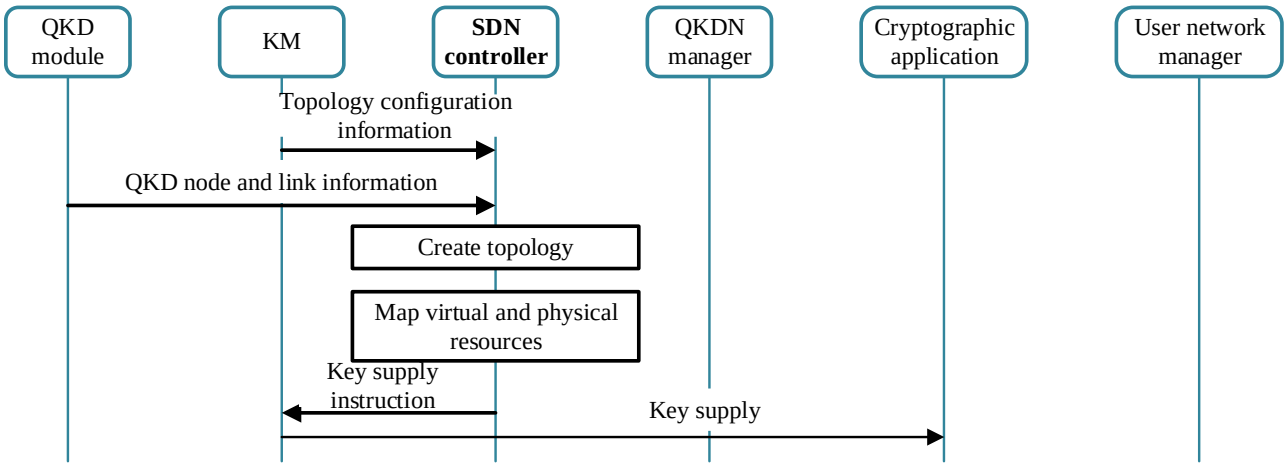

Fig. 10 QKDN virtualization phase

Fig. 10 illustrates procedure of SDN control in QKDN virtualization phase. First of all, the SDN controller uses the southbound interfaces to collect topology configuration information from KM and QKD node and link information from QKD module. Then, the SDN controller creates the virtual topology based on the collected information. To meet the demand of specific services or applications, the SDN control map the virtual and physical QKDN resources. Finally, the SDN controller sends the key supply instruction to KM and the KM supplies keys to cryptographic application.

12. Controllable elements for SDN in QKDN

One of the most important advantages of introducing SDN technology into QKDN, is that SDN controller can support the programmable control of QKDN elements. These elements include:

- Laser.
- Intensity modulator.
- Phase modulator.
- Single photon detector.
- Main control unit.
- Post processing unit.

- Key pool.

13. Security Considerations

In SDN control based QKDN, the security of SDN controller is very important. For one thing, authority for SDN controller should be well designed; for another thing, the control channel of SDN controller could be encrypted with quantum keys provided by QKDN itself. Also note that the compatibility between SDN controller and other controllers should be considered. Details are outside the scope of this recommendation.

Appendix I:

Use cases of SDN control in QKDN

(This Appendix does not form an integral part of this Recommendation)

[Editor's note: any update of the use cases of SDN control in QKDN is invited.]

Following are several potential use cases for SDN control in QKDN:

- **Data centers**

  With the rise of cloud services, data centers will become the assets of enterprise competition, and their data security issues are receiving more and more attention. By combining SDN and QKDN, the centralized network control mode is adopted, and each data center is provided with a QKD node, specifically including QKD devices and a KM. Routing relay between data centers, the configuration of KMSs and QKD devices is the responsibility of the QKDN controller. The QKDN controller utilizes the advantages of centralized SDN control to efficiently manage the key resources of each data center node and provide an open interface for third-party applications, which can greatly improve the security of data transmission and meet the requirements of service encryption between different data centers, as shown in Fig. I.1.

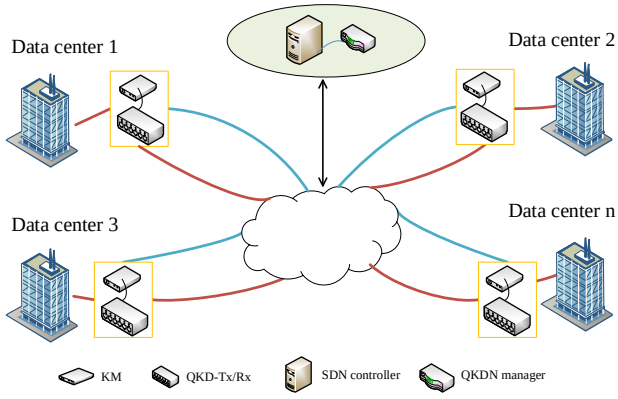

Fig. I.1 Data backup in data centers

- **Enterprise private networks**

  Enterprises or government agencies usually require communication services to provide a high degree of confidentiality and authenticity, requiring mandatory use of dedicated security systems. The QKDN controller can utilize the features of centralized SDN control to globally manage key information such as key resources, QKD devices, and routing policies of different private networks. The SDN controller in QKDN performs key resource allocation, rerouting, and key generation among user nodes more quickly and efficiently. Thereby, the security key distribution of the enterprise private network is realized, as shown in Fig. I.2.

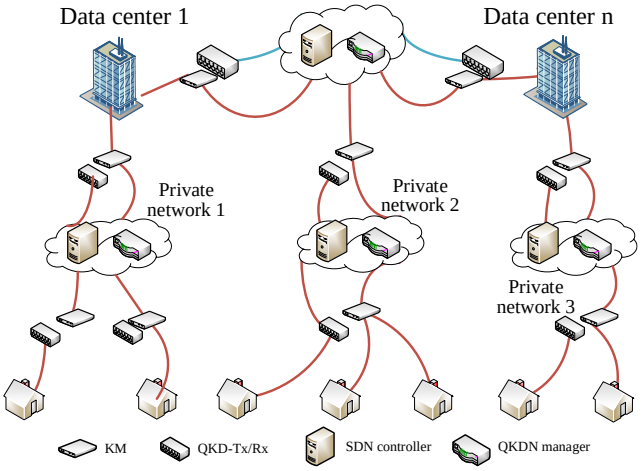

Fig. I.2 QKD private network

- **Backbone networks**

At present, the backbone network nodes communicate with each other through optical fibers, and the technology of quantum signal and classical optical signal co-fiber transmission is gradually mature, which provides a good infrastructure for the layout of QKD system. Each node of backbone network is equipped with QKD nodes, including QKD devices and a KM. Using centralized network control mode, the QKDN controller based on SDN can control the key resources, topology, routing and other information of each node in the backbone network. When a link fault occurs, the key requirements between nodes can be guaranteed through rerouting, as shown in Fig. I.3.

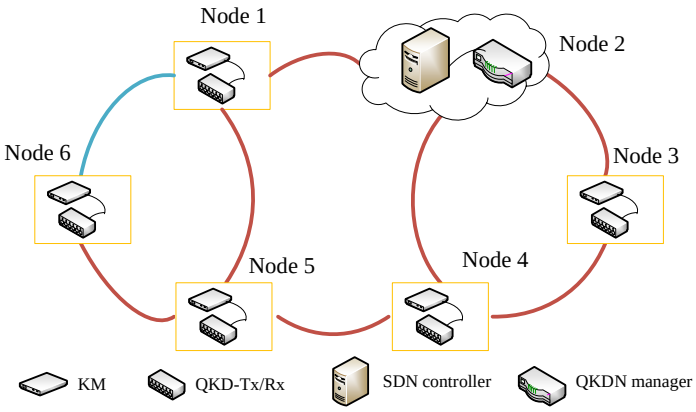

Fig. I.3 QKD backbone network

- **Access networks**

Each ONU receives all downlink signals of OLT. Therefore, encryption measures must be used to prevent ONU from eavesdropping on unsuitable content. By combining SDN and QKDN, each ONU is equipped with QKD nodes, including QKD devices and a KM, OLT is equipped with SDN controller and QKDN manager, using centralized network control mode to achieve one-to-many QKD. Utilizing the centralized control features of SDN, QKDN can flexibly respond to user increases or decreases and meet user dynamic key requirements. Thus, the encrypted transmission of ONU user data is realized.

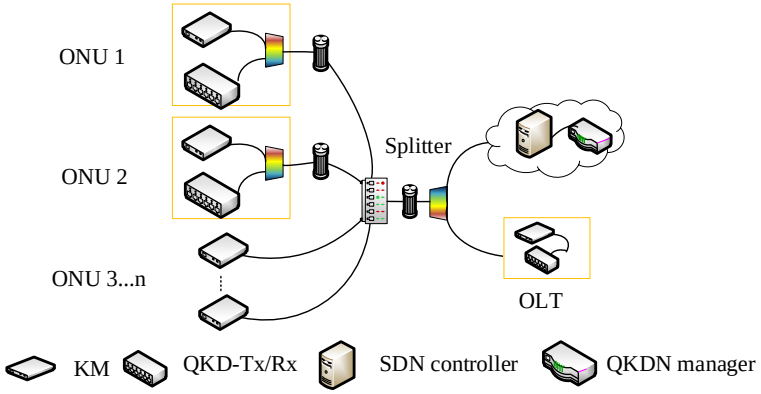

Fig. I.4 QKD access network

- **Mobile terminal communication**

As shown in Fig. I.6, the QKDN based on the SDN manages the resource allocation, path selection, and troubleshooting in the quantum key distribution process through the SDN controller when a secure communication service arrives. The SDN based QKDN is combined with the quantum key update terminal device close to the user. The aim is to charge the symmetric quantum key generated by the QKDN to the secure storage medium of the terminal for authentication and session encryption in the communication process. Thus, secure communication services between mobile terminals or between mobile terminals and servers are provided.

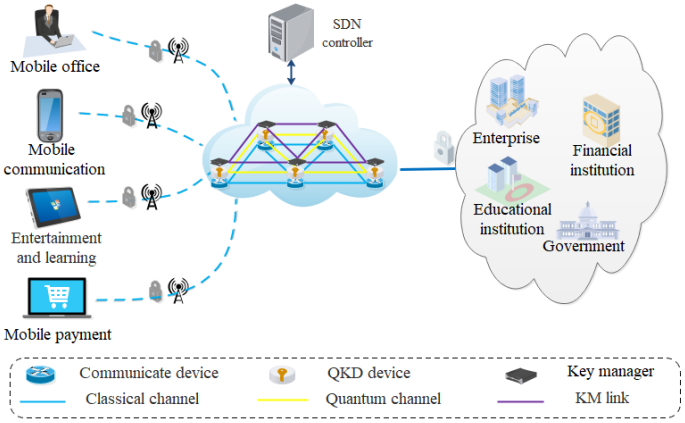

Fig. I.5 Mobile terminal communication

- **Others**

Other use cases can be applied such as secure finance, blockchain application, stable and reliable service environment for the purpose of key change and management, smart grid, intelligent transport system, mashup or convergence applications for control and management.

Appendix II

Comparison of control methods between traditional QKDN and SDN based QKDN

(This Appendix does not form an integral part of this Recommendation)

To better understand SDN control in QKDN, we compare the control method in QKDN with that in SDN based QKDN by analyzing examples. In Fig. II. 1-3, red arrows show control flows and green arrows show key flows. Note that, interfaces are simplified in the figures, and the interfaces related to the control layer is highlighted. In the following three scenarios, there are the same key flows for key relay and key supply, but there are different control flows.

- **QKDN with distributed QKDN controllers**: As shown in Fig. II. 1, when terminals need keys to encrypt data, the terminal in source node requests keys from KM locally and gets keys from local KM. If QKD needs key relay, the local KM will send key relay request to the local QKDN controller for getting calculated routing paths. Finally, KM in destination node pushes keys to another terminal.

- **QKDN with a centralized QKDN controller**: As shown in Fig. II. 2, the control method is the same as that in QKDN with distributed QKDN controllers, except that the centralized QKDN controller calculates routing paths for terminals.

- **SDN based QKDN with an SDN controller**: As shown in Fig. II. 3, when terminals need keys to encrypt data, the key request information is directly sent to an SDN controller to provision services. It is the SDN controller to judge whether to relay keys and calculate the routing path if it needs key relay. It means that the SDN controller is the core brain in operational procedures in SDN based QKDN. The control method avoids the operations between users and KM and saves the time for service provisioning.

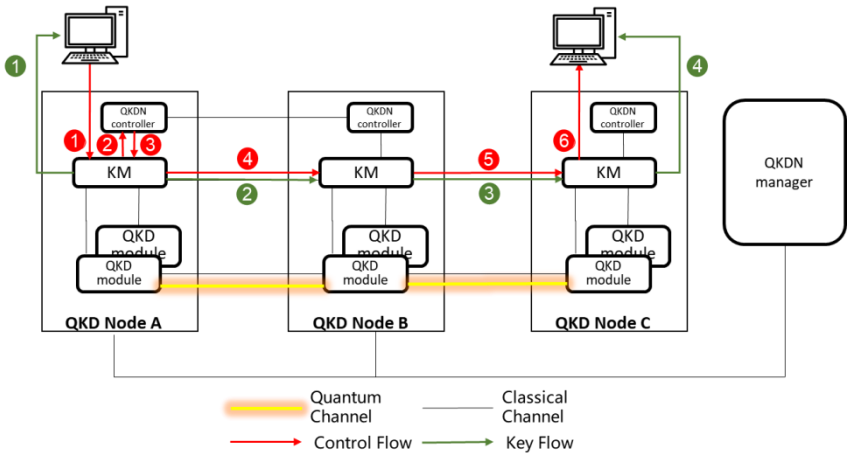

Fig. II.1 Diagram of control method in QKDN with distributed QKDN controllers

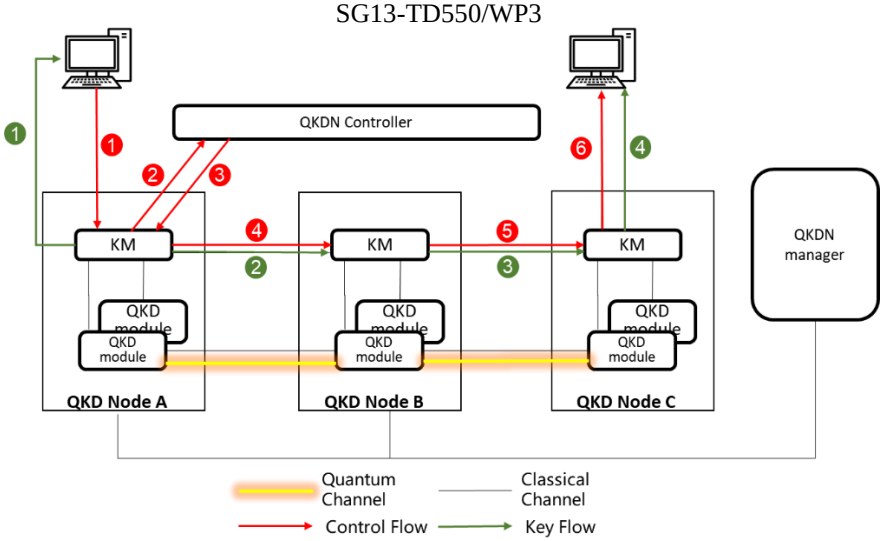

Fig. II.1 Diagram of control method in QKDN with a centralized QKDN controller

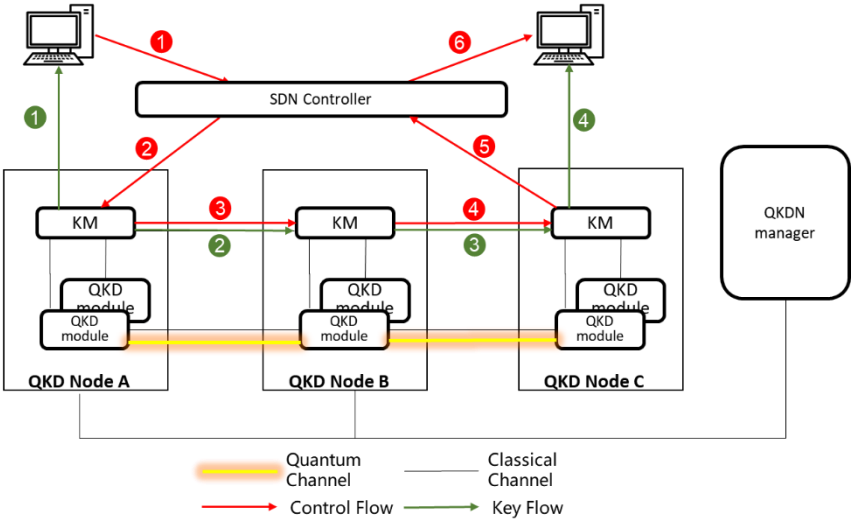

Fig. II.3 Diagram of control method in SDN based QKDN with an SDN controller

Appendix III

Controllable elements for SDN in QKDN

(This Appendix does not form an integral part of this Recommendation)

[Editor's note: the elements that might be available for programmable control by the SDN controller captured in this draft appendix remain under discussion. It has not been agreed that the elements listed will be included.]

One of the most important advantages of introducing SDN technology into QKDN, is that SDN controller can supporting the programmable control of QKDN elements. Meanwhile, QKD network with SDN controller is more flexible and variable, SDN controller can control some functions of programmable elements when QKD network needs.

With the diversity and complexity of various services, the programmable requirements of underlying programmable elements become more and more important. When a certain service needs to replace a certain parameter of the underlying programmable elements, the SDN controller can calculate and control the necessary parameters of a programmable element, which is not only convenient and fast, but also can save a lot of human and material resources. Therefore, it is necessary for SDN to control the programmable elements in QKDN.

Appendix III describes the programmable elements that can be controlled by the SDN controller and the controllable functions.

The following will list the functions of the programmable elements that can be controlled by SDN control in QKD system (currently the components of Decoy state BB84 QKD are taken for example).

Laser: SDN controller can control the launch power and wavelength of optical laser according to different requirements.

Intensity modulator: SDN controller can control the intensity modulator, thus to change the repetition rate of the light pulse (the upper bound is limited by the bandwidth of the intensity modulator) , the time domain width of the light pulse, the intensity of signal state and decoy states in each period cycle, and the probability distribution of signal state and decoy states.

Phase modulator: SDN controller can control the repetition rate of phase modulator, and the phase shift introduced by the phase modulator.

Single photon detector: SDN controller can control the dead time, detection efficiency and repetition rate of single photon detector.

Main control unit: SDN controller can change QKD protocols by modifying the workflow/logic of modulators and single photon detectors, for example change from BB84 protocol to COW protocol.

Post processing unit: SDN controller monitors the parameters such as gain, error rate and error correction efficiency to ensure the system is doing "honest" privacy amplification according to specific QKD security model.

Key pool: SDN controller monitors each symmetric key resource state in each link in and network topology in the whole network.

Bibliography