Draft Recommendation ITU-T Y.3805 (formerly Y.QKDN_SDNC)

Software Defined Networking Control for Quantum Key Distribution Networks

Summary

The Recommendation specifies the requirements, functional architecture, reference points, hierarchical SDN controller and overall operational procedures of SDN control.

Keywords

Functional architecture; hierarchical; operational procedure; QKDN (Quantum Key Distribution Network); reference point; SDN (Software-defined networking); SDN controller.

Table of Contents

Draft Recommendation ITU-T Y.3805 (formerly Y.QKDN_SDNC)

Software Defined Networking Control for Quantum Key Distribution Networks

1. Scope

This recommendation specifies the requirements, functional architecture, reference points, hierarchical software-defined networking (SDN) controller and overall operational procedures of SDN control in QKDN. The scope of this 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;

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)/Cor.1 (2020), *Overview on networks supporting 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), *Quantum key distribution networks - Functional architecture.*

[ITU-T Y.3803] Recommendation ITU-T Y.3803 (2020), *Quantum key distribution networks – Key management*.

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

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

3. Terms and definitions

3.1. Terms defined elsewhere

This recommendation uses the following terms defined elsewhere:

3.1.1. key manager (KM) [ITU-T Y.3800]: A functional module located in a quantum key distribution (QKD) node to perform key management in the key management layer.

3.1.2. key management agent (KMA) [ITU-T Y.3802]**:** A functional element to manage keys generated by one or multiple quantum key distribution (QKD) modules in a QKD node (trusted node).

NOTE - KMA acquires keys from one or multiple QKD modules, synchronizes, resizes, formats, and stores them. It also relays keys through key management agent (KMA) links.

3.1.3. key supply agent (KSA) [ITU-T Y.3802]: A functional element to supply keys to a cryptographic application, being located between a key management agent (KMA) and the cryptographic application.

NOTE - Application interfaces for cryptographic applications are installed into the key supply agent (KSA). The KSA synchronizes keys, and verifies their integrity via a KSA link before supplying them to the cryptographic application.

3.1.4. 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.

3.1.5. quantum key distribution module [ITU-T Y.3800]**:** A set of hardware and software components that implements cryptographic functions and quantum optical processes, including quantum key distribution (QKD) protocols, synchronization, distillation for key generation, and is contained within a defined cryptographic boundary.

NOTE – A QKD module is connected to a QKD link, acting as an endpoint module in which a key is generated. These are two types of QKD modules, namely, the transmitters (QKD-Tx) and the receivers (QKD-Rx).

3.1.6. 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.

3.1.7. quantum key distribution network controller [ITU-T Y.3800]: A functional module, which is located in a quantum key distribution (QKD) network control layer to control a QKD network.

3.1.8. quantum key distribution network manager [ITU-T Y.3800]: A functional module, which is located in a quantum key distribution (QKD) network management layer to monitor and manage a QKD network.

3.1.9. 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:

None.

4. Abbreviations and acronyms

This recommendation uses the following abbreviations and acronyms:

KM Key Manager

KMA Key Management Agent

KML Key Management Layer

KSA Key Supply Agent

QKD Quantum Key Distribution

QKDN Quantum Key Distribution Network

QL Quantum Layer

QoS Quality of Service

SDN Software-Defined Networking

5. Conventions

In this Recommendation:

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

6. Overview

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; [ITU-T Y.3801] specifies functional requirements for quantum layer, key management layer, QKDN control layer and QKDN management layer; [ITU-T Y.3802] specifies the functional architecture of QKDN); [ITU-T Y.3803] specifies the key management of 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.

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, SDN controller supports centralized, programmable, and hierarchical control; on the other hand, it can provide fast services for applications by opening northbound interfaces between control layer and service layer. The change of control method by SDN in QKDN provides alternative 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 SDN-based centralized control 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 programmed 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 in a large scale QKDN consisting of multiple, logical sub-QKDN. Under such scenarios, the implementation of the controller for each sub-QKDN is independent of others, which makes the QKDN 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 services provisioning for the customers. The overall operational procedures and its advantages are described in the 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 QKDs in the network partitions by 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 requirements for SDN controller in QKDN control layer.

- Req_1. The SDN controller is required to support the ability of application registration in QKDN, which enables the fast provisioning of cryptographic applications in the service layer.

- Req_2. The 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. The SDN controller is recommended to support the ability of QKDN virtualization, which enables the creation of logically isolated network partitions over physical QKDNs.

- Req_4. The SDN controller is recommended to support the ability of QKDN programmable elements control, when the QKDN consists of programmable elements in the quantum layer.

- Req_5. The SDN controller is recommended to support the ability of communication among multiple SDN controllers which enable the hierarchical SDN control.

8. Functional architecture for SDN control in QKDN

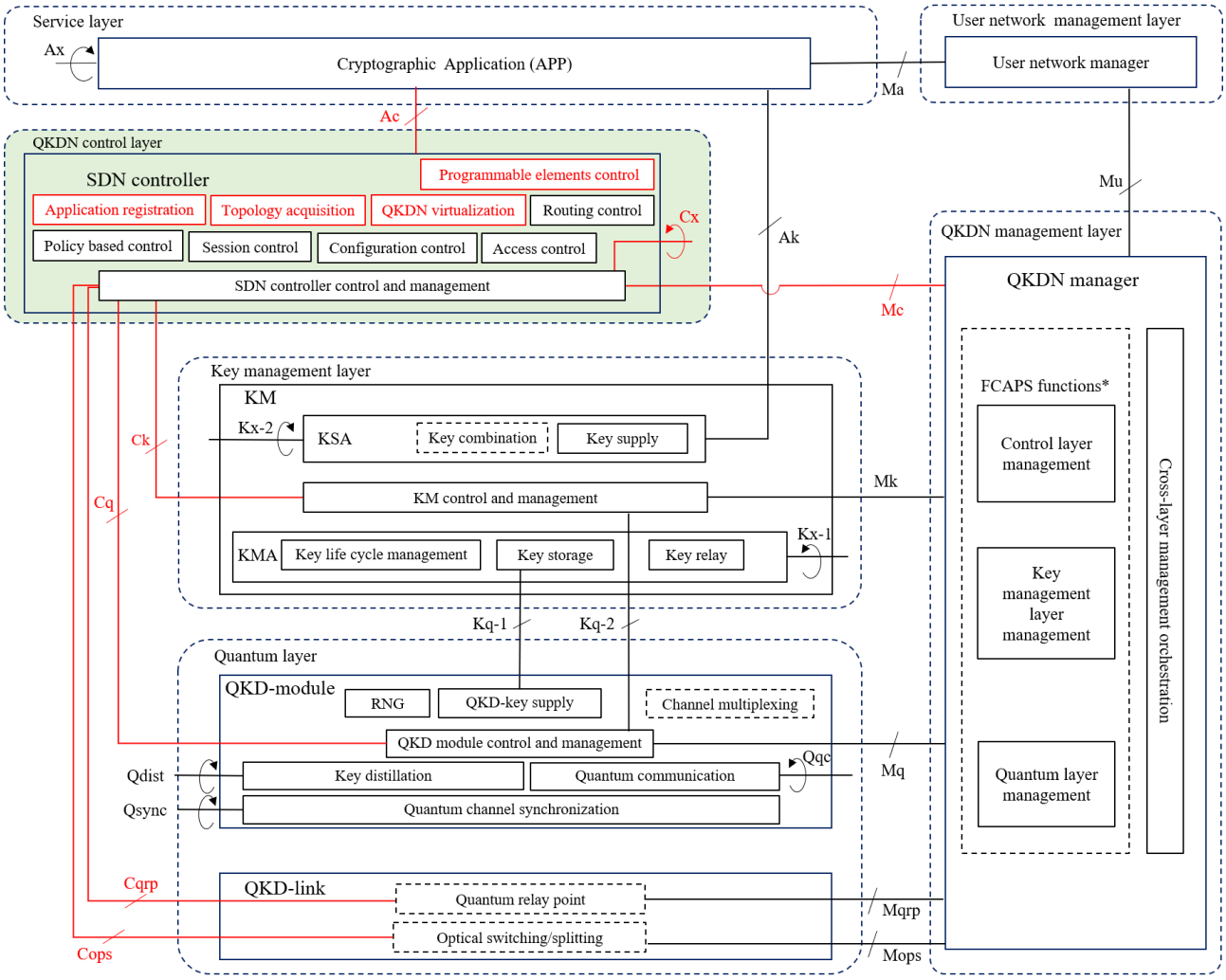

Fig. 1 Functional architecture for SDN control in QKDN
(* FCAPS represents fault, configuration, accounting, performance and security management)

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 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.

  NOTE - With SDN technology, QKD-key can be virtualized and stored in the virtual QKD-key storage entities to enhance the 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, QKDN virtualization, programmable elements control, routing control, policy-based control, session control, configuration control and access control. 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 key pairs provided by 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 defines the newly added one and presents the existing ones related to SDN.

NOTE - When SDN controller involves the interaction with other QKDN elements, the existing reference points in [ITU-T Y.3802] are used. The new extended functions of SDN control are implemented by extending the interaction information of reference points.

The newly added reference point is:

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

The existing reference points in [ITU-T Y.3802] related to SDN include:

- **Ck:** reference point between SDN controller and KM control and management. It is responsible for SDN controller to communicate control information with the KM control and management.
- **Cq:** reference point between SDN controller and QKD module. It is responsible for the SDN controller to communicate control information with QKD module.
- **Cops:** a reference point connecting the SDN controller control and management function in the SDN controller with an optical switching/splitting function in a QKD link. It is responsible for the SDN controller to communicate control information on optical switching/splitting with the QKD link.
- **Cqrp:** a reference point connecting the SDN controller control and management function in the SDN controller with a quantum relay point function in a QKD link. It is responsible for the SDN controller to communicate control information on quantum relay point 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.

- **Cx:** reference point connecting two SDN controller control and management functions. It is responsible for communication of control information between the two SDN controllers.

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 adopted. 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 provisioning within its control range. SDN controller of each layer has its northbound interface to communicate with the service layer, and 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.

- **Ac-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.

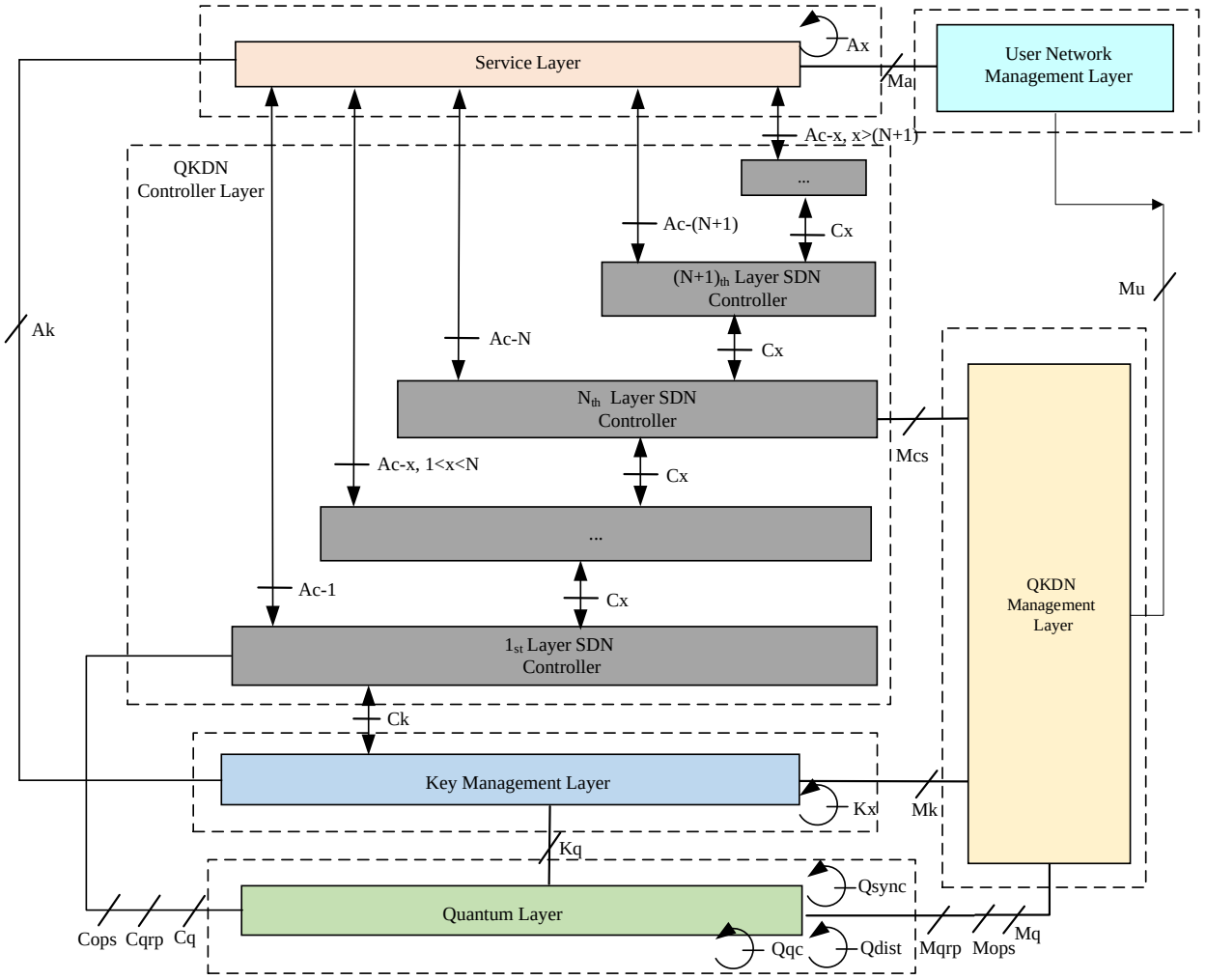

Fig. 2 Hierarchical SDN controller in QKDN

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

NOTE - Different sub-QKDNs in a large scale QKDN can be implemented by multiple vendors but are provided by a same administrative authority. The first layer SDN controllers control different sub-QKDNs respectively, and the higher layer SDN controller is responsible for the inter sub-QKDN cooperation and SDN controller orchestration.

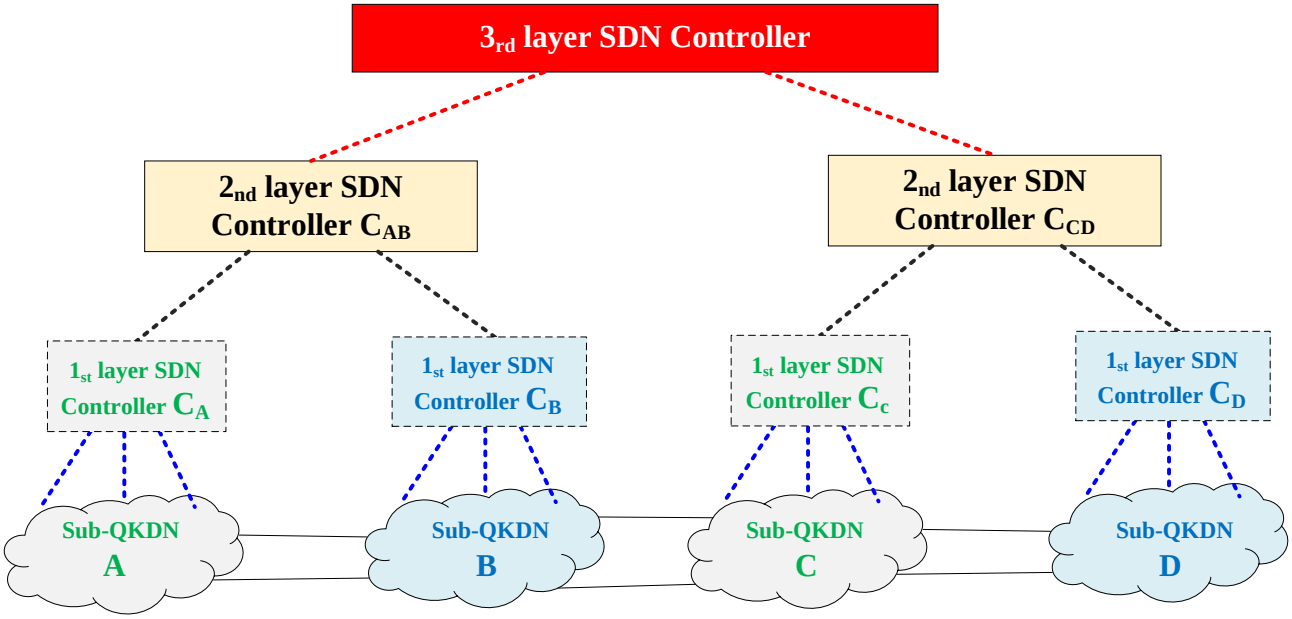

Fig. 3 Hierarchical SDN control in a large scale QKDN

11. Overall operational procedures of SDN control in QKDN

Unlike 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 using SDN control by skipping the QKDN manager. The SDN controller can also provide more efficient key resource utilization by deciding the end of key generation and controlling the management monitor in a global view. In addition, the SDN technology improves the flexibility of service provisioning and provides services for applications in a fast way by opening the north-bound interface between QKDN control layer and service layer. Based on the functional architecture for SDN control defined in the clause 8, this clause describes the overall operational procedures of SDN control in QKDN.

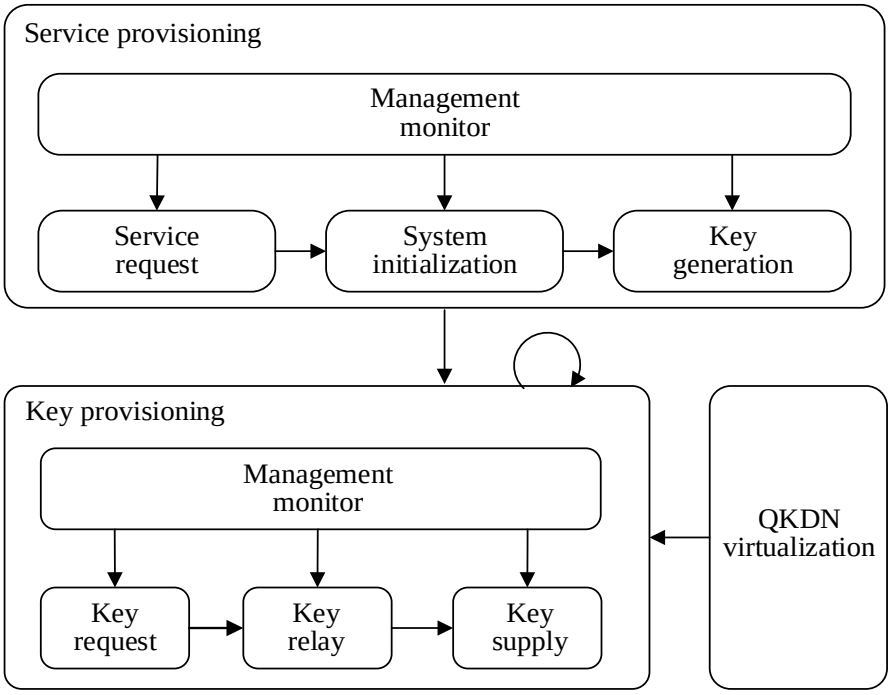

Fig. 4 The overall operational procedures of SDN control in QKDN

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: service provisioning mode and key provisioning mode. When a 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 a 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 the supplied keys for the key request. At the same time, the real-time network monitoring operation is performed to collect and monitor all the QKD links in the service provisioning phase and analyze the status of keys in the key provisioning phase with the global view provided 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. Apart from these, a control action procedure is specified, which includes hierarchical SDN control associated with QKDN management. The overall typical operational procedures include:

11.1. Normal operation mode: Service request and system initialization phase

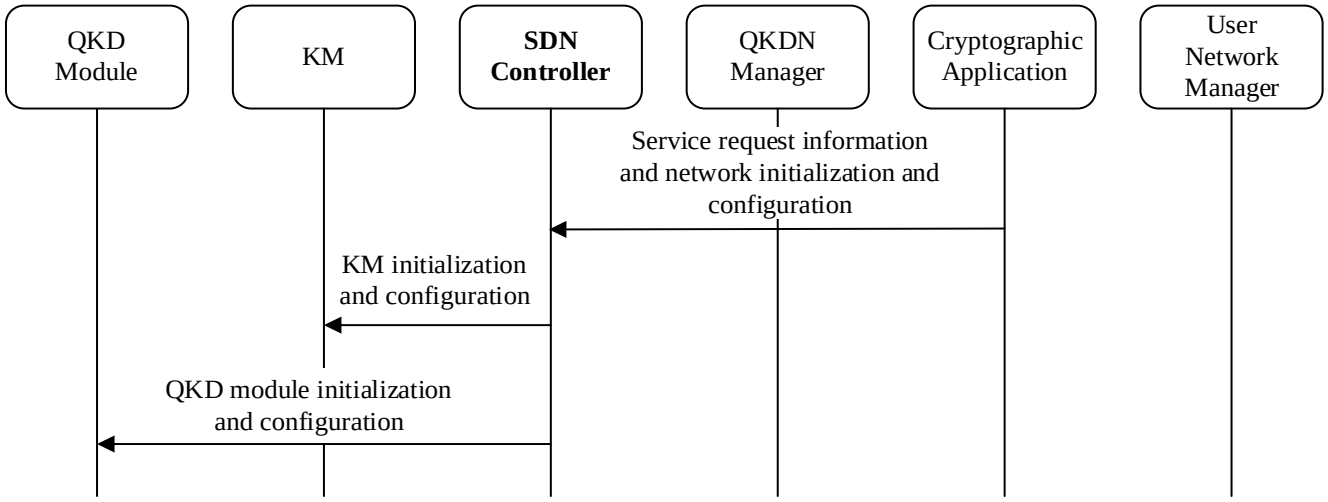

Fig. 5 An example of service provisioning and system initialization phase

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.

11.2. Normal operation mode: Key generation phase

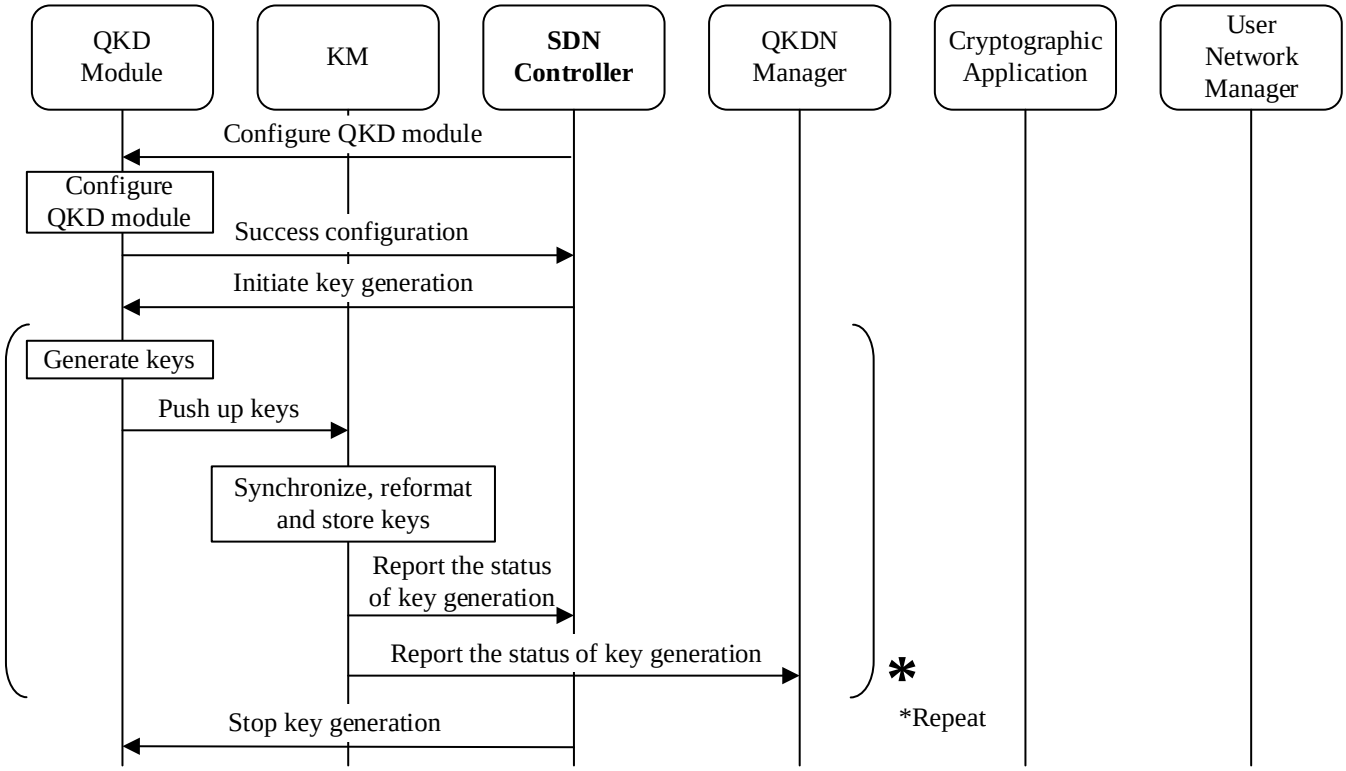

Fig. 6 An example of key generation phase

Fig. 6 illustrates procedures of SDN control for key generation with SDN technology. In the phase, SDN controller firstly sends the configuration of QKD module to QKD modules. After the QKD

modules are configured successfully, 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.

11.3 Normal operation mode: Key request, relay and supply phase

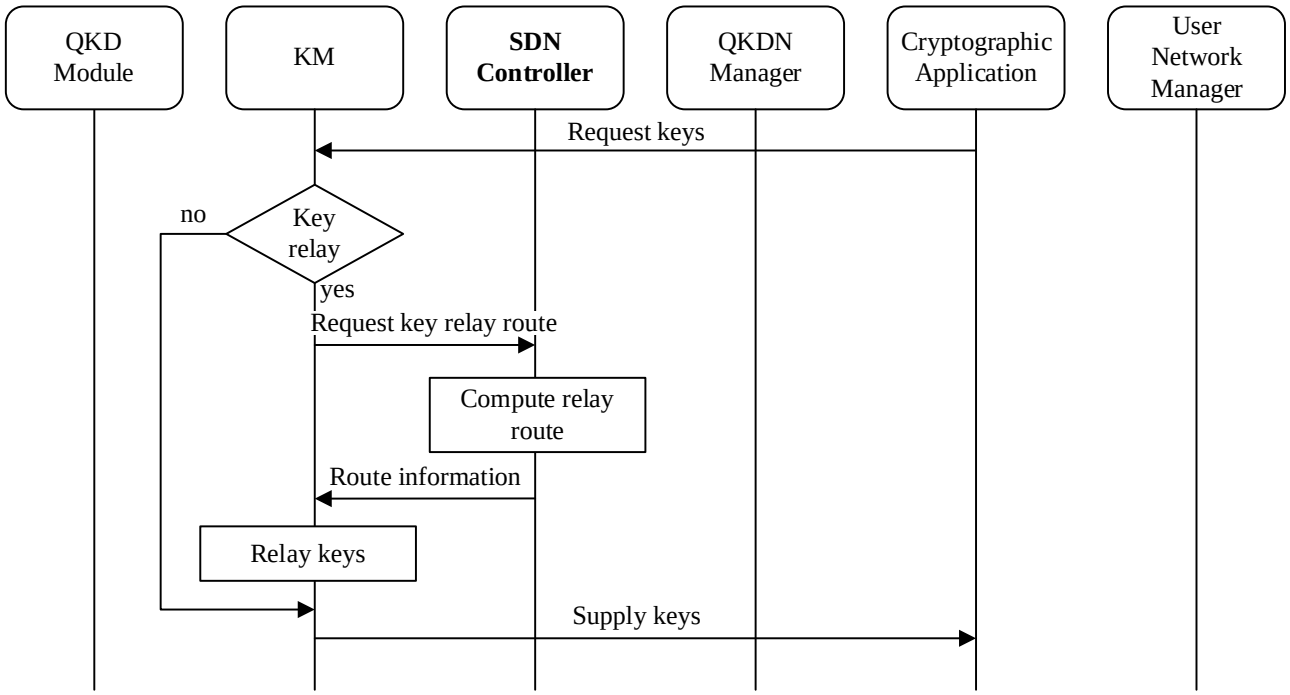

Fig. 7 An example of key request, relay and supply phase

Fig. 7 illustrates procedures of SDN control for key request, relay and supply. A cryptographic application in the user network sends key request information to the KM in the QKD network. Then KM checks the need to relay keys to the SDN controller. If it needs to relay keys for service provisioning, the SDN controller will compute relay route and 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.

11.3.1. A key relay control procedure including hierarchical SDN control

A key relay control procedure including multiple sub-QKDNs hierarchical SDN control is shown in Fig. 8.

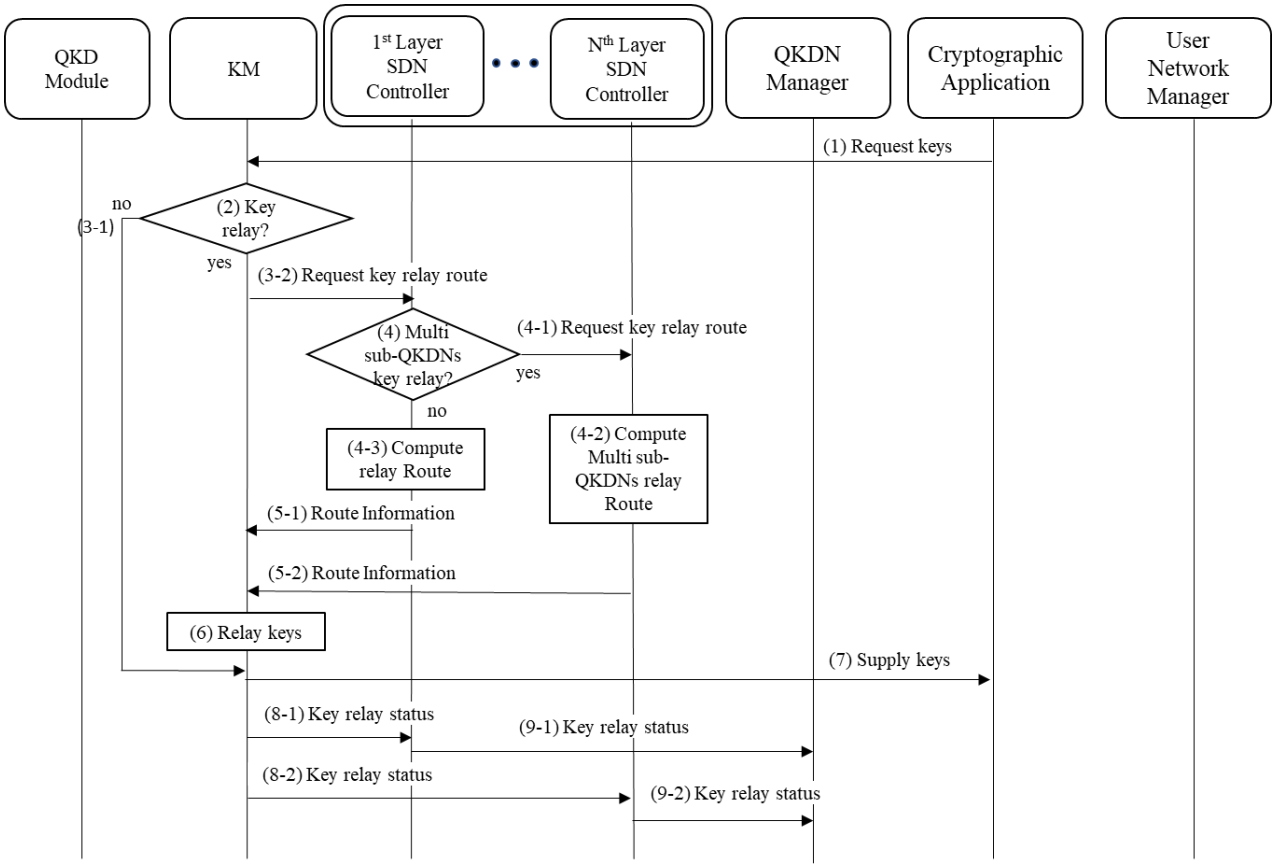

Fig. 8 An example of a key relay procedure including hierarchical SDN control

1) A cryptographic application requests a key to the KM.

2) The KM checks if a key relay is needed.

3-1) If no, then key is supplied via KM to the application.

3-2) If yes, KM then sends the key relay request to the SDN controller

4) SDN controller checks whether multiple sub-QKDNs key relay is needed.

4-1) If not, then it computes a relay route for a QKDN.

5-1) The computed relay route is sent to KM.

4-2) If yes, N^{th}-layer SDN controller computes multiple sub-QKDNs key relay route with support of underlying layer's SDN controllers.

5-2) The computed multiple sub-QKDNs relay route is sent to KM

6) KM then relays keys on the computed relay route

7) KM also supply keys to the cryptographic application

8-1) The status of key relay is reported to the 1^{st}-layer SDN controller for logging purpose

9-1) The status of key relay is reported to the QKDN manager for logging purpose

8-2) The status of key relay is reported to the N^{th}-layer SDN controller for logging purpose

9-2) The status of key relay is reported to the QKDN manager for logging purpose

11.3.2. A key relay rerouting procedure including hierarchical SDN control

A key relay rerouting procedure including multiple sub-QKDNs hierarchical SDN control is shown in Fig.9.

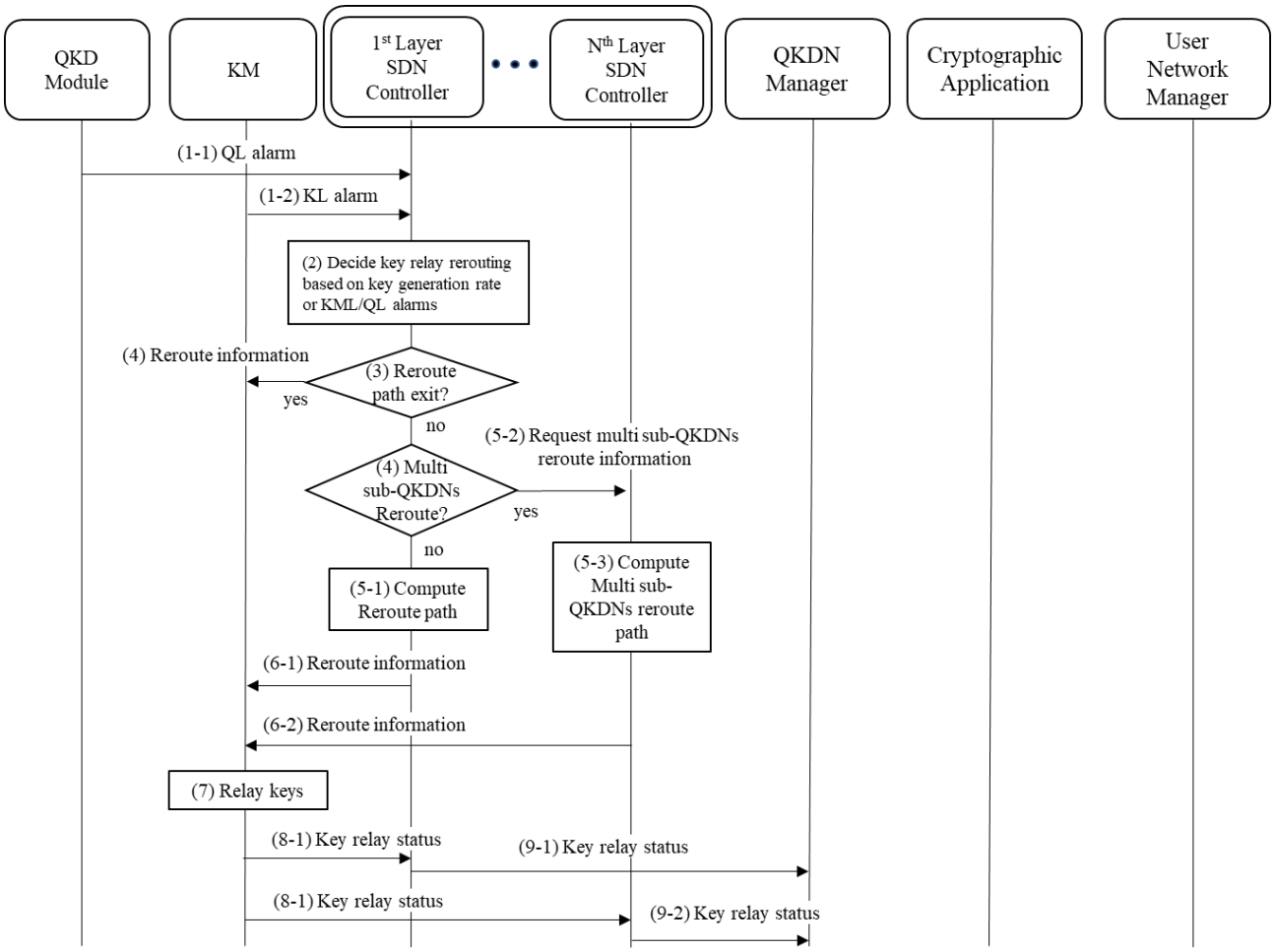

Fig. 9. An example of a key relay rerouting procedure including hierarchical SDN control

1-1) SDN controller receives alarms from QL such as quantum channel failure.

1-2) SDN controller receives alarms from KML such as key generation rate falling below a defined threshold.

2) SDN controller decides whether key relay rerouting is needed due to the alarms received.

3) If a reroute path for the failure exists, it returns the information to KM for rerouting

4) If not, it checks if a reroute path involves multiple sub-QKDNs route computation

5-1) If no, it computes a QKDN reroute path

6-1) Then it returns the computed reroute path to KM

5-2) If yes, it request multiple sub-QKDNs reroute path computation to the Nth-layer SDN controller

5-3) Nth-layer SDN controller compute the reroute path with support of underlying layer's SDN controllers.

6-2) Then it returns the computed reroute path to KM

7) KM then relays keys on the computed relay route

8-1) The status of key relay is reported to the 1st-layer SDN controller for logging purpose

9-1) The status of key relay is reported to the QKDN manager for logging purpose

8-2) The status of key relay is reported to the Nth-layer SDN controller for logging purpose

9-2) The status of key relay is reported to the QKDN manager for logging purpose

11.4. Normal operation mode: Management monitor phase

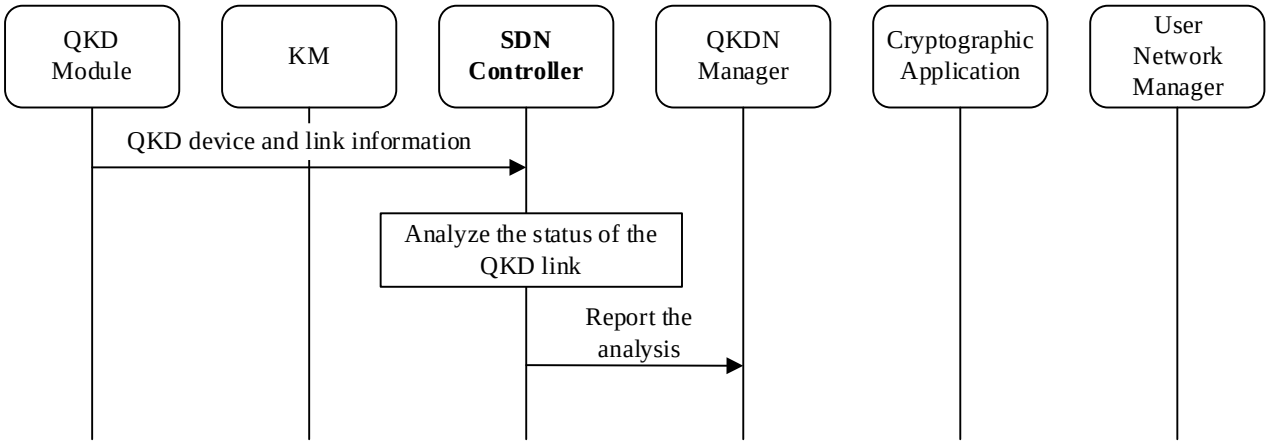

Fig. 10 An example of management monitor phase in the service provisioning mode

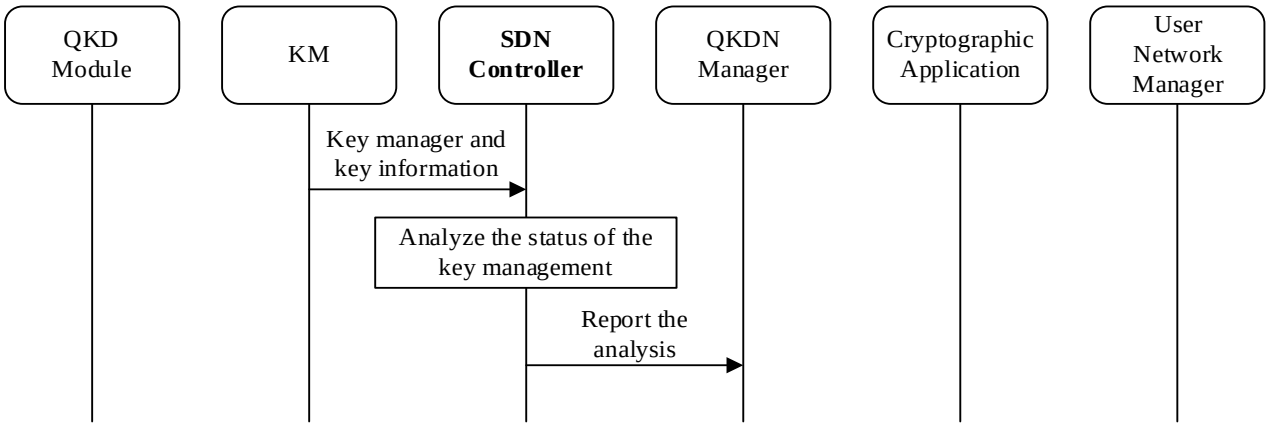

Fig. 11 An example of management monitor phase in the key provisioning mode

Fig. 10 and Fig.11 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.

11.5. Normal operation mode: QKDN virtualization phase

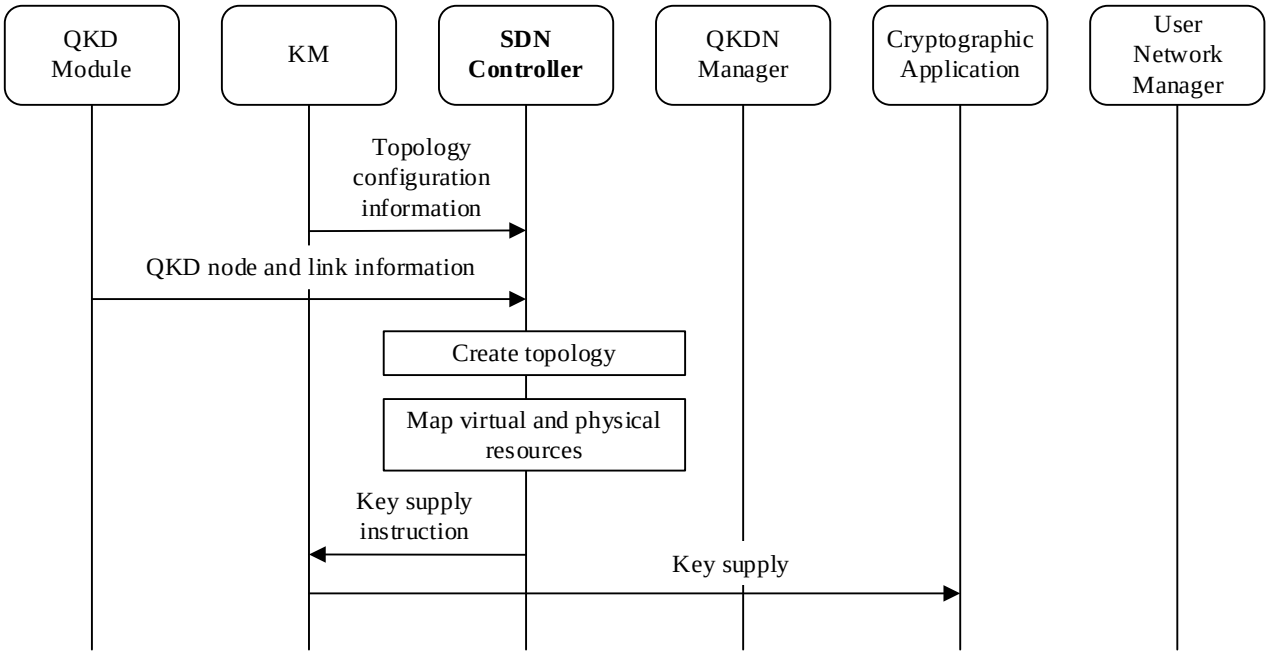

Fig. 12 An example of QKDN virtualization phase

Fig. 12 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.

11.6. A control action procedure including hierarchical SDN control associated with QKDN management

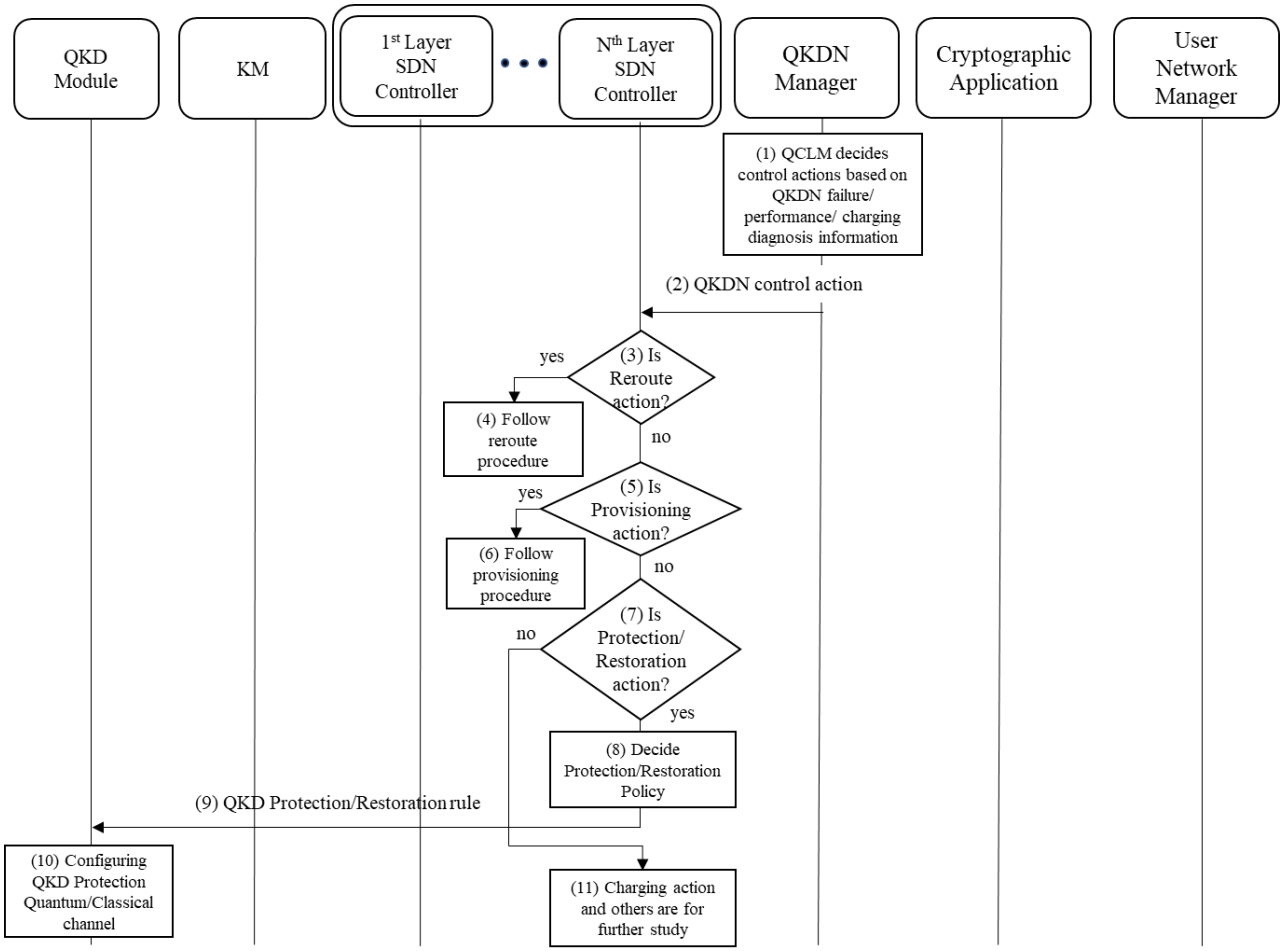

Fig 13. An example of a QKDN control action procedure including hierarchical SDN control associated with QKDN management

A control action procedure including hierarchical SDN control associated with QKDN management is shown in Fig. 13.

1) QKDN manager decides QKDN control actions based on various factors: QKDN failure, performance degradation, and charging policy.
2) QKDN manager then sends the determined QKDN control action information.
3) SDN controller checks if it is key relay reroute control action.
4) If yes, it invokes the reroute procedure.
5) SDN controller further checks if the control action type is provisioning action.
6) If yes, SDN controller invokes the provisioning procedure.
7) SDN controller further checks if the control action type is protection/restoration action
8) SDN controller decides a protection and restoration policy based on the information received from QKDN manager.
9) SDN controller then sends the protection/restoration action rules to QKD module. If the protection/restoration involves multiple sub-QKDNs, the SDN controller orchestrates protection/restoration.
10) QKD module (or multiple QKD modules if multiple sub-QKDNs are involved) configures protection channels based on the received action rules.

11) If the control action types are others including charging control action, the detailed control procedure needs to be further defined.

12. Security Considerations

In SDN control based QKDN, the security of SDN controller is very important. On the one hand, the authority for SDN controller should be well designed; on the other hand, the control channel of SDN controller could be encrypted with QKD 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 SDN-based 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.

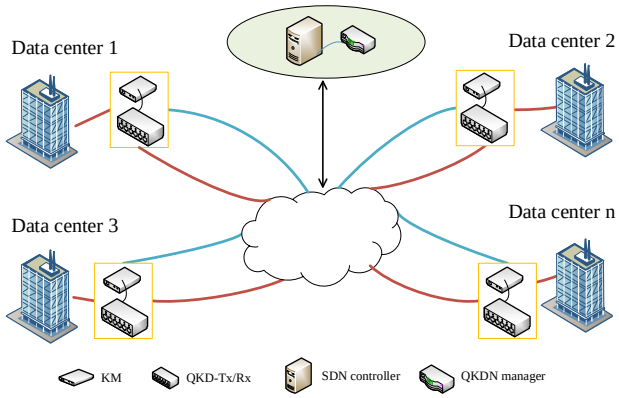

Fig. I.1 Data backup in data centers

- **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 secure key distribution of the enterprise private network is realized, as shown in Fig. I.2.

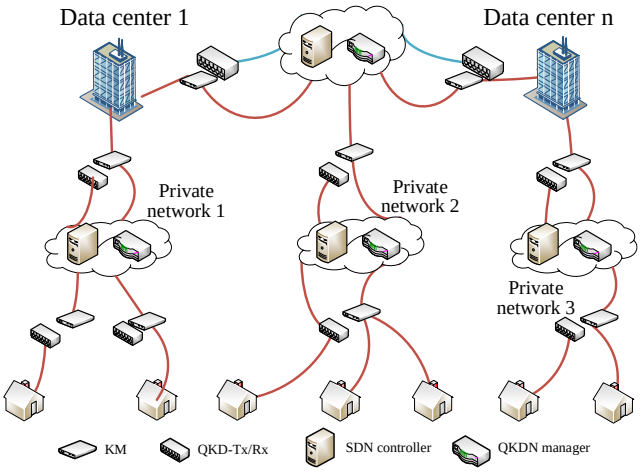

Fig. I.2 QKD private network

- **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 modules and a KM. Using SDN-based centralized network control mode, the SDN controller 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.

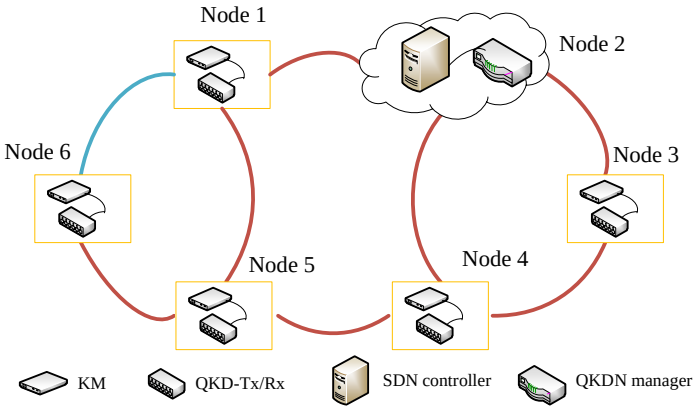

Fig. I.3 QKD backbone network

- **Access networks**

Each optical network unit (ONU) receives all downlink signals of optical line terminal (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.

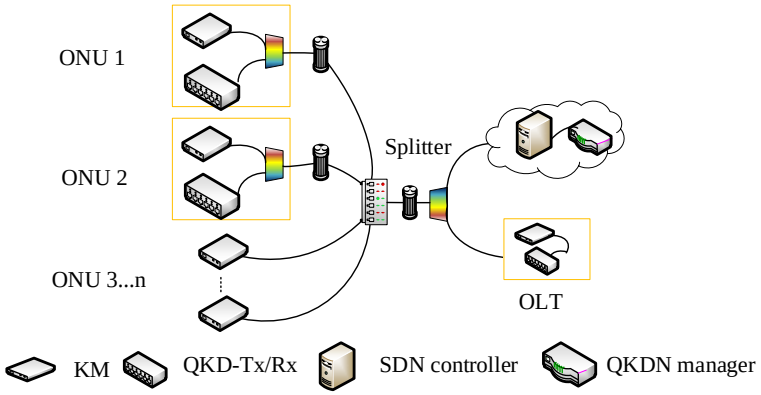

Fig. I.4 QKD access network

- **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 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.

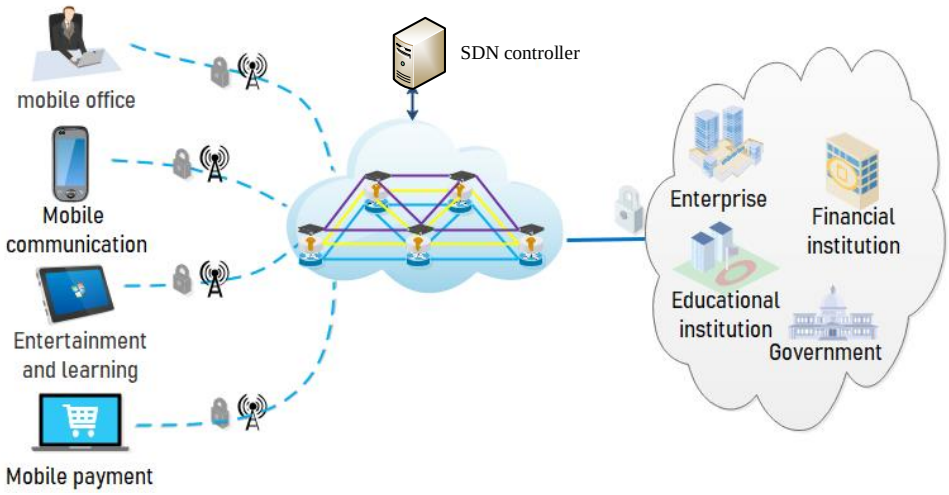

Fig. I.5 Mobile terminal communication

- **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 sent to KM and then the KM sends key relay route request to an SDN controller to provision services. The SDN controller is the core brain in operational procedures of SDN based QKDN.

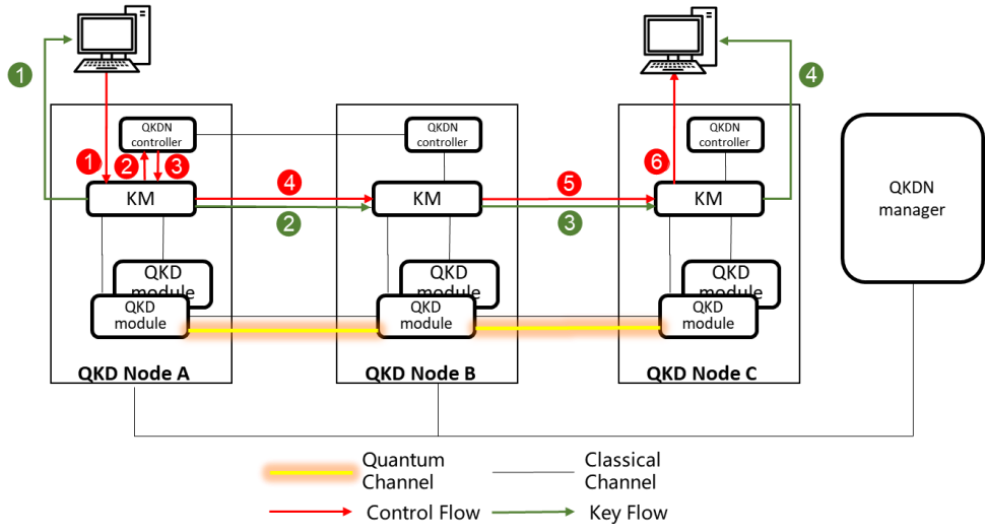

Fig. II.1 Diagram of control method in QKDN with distributed QKDN controllers

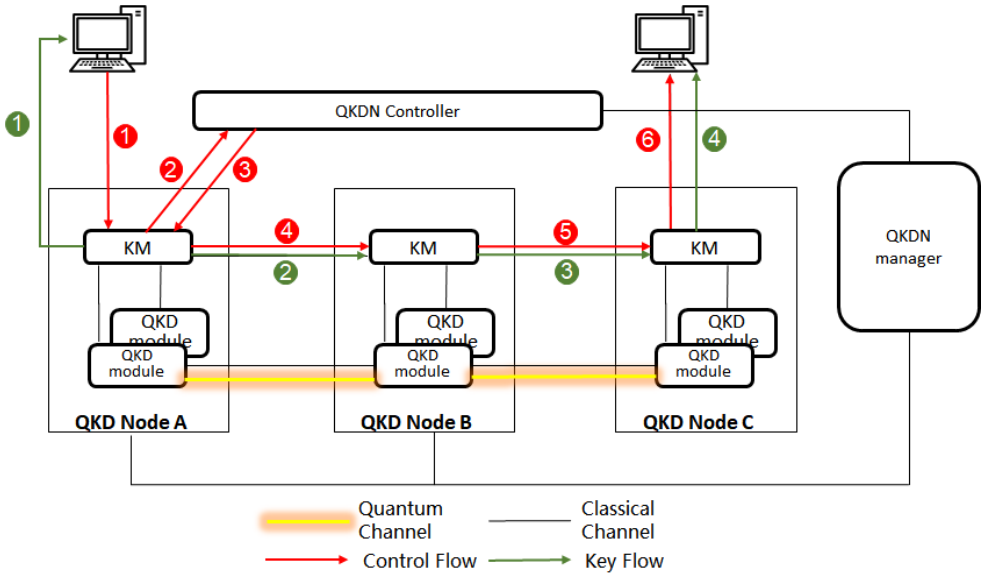

Fig. II.2 Diagram of control method in QKDN with a centralized QKDN controller

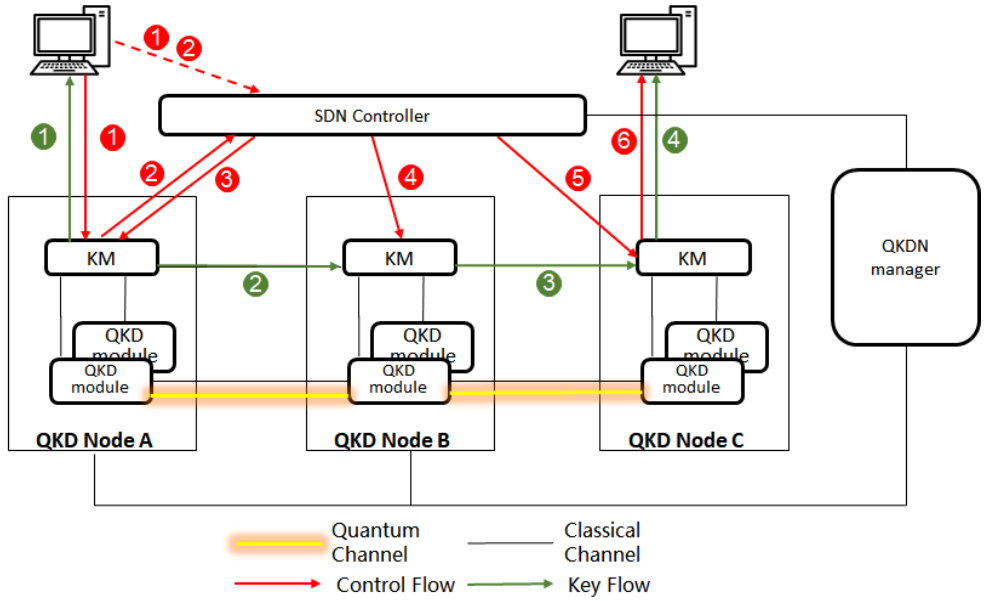

Fig. II.3 Diagram of control method in SDN based QKDN with an SDN controller

Appendix III

Controllable elements for SDN in QKDN

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

One of the most important advantages of introducing SDN technology into QKDN, is that SDN controllers include capabilities to support the programmable control of network elements. In a QKD network the SDN controller can control functions of programmable elements, where required by the QKDN.

As the diversity and complexity of various services increase, the programmability of underlying elements become more important. When a service needs to change certain parameters of underlying programmable elements, the SDN controller can calculate and control the necessary parameters of programmable elements.

Many parameters of a QKDN, such as parameters of QKD modules, are critical for the secure operation of the QKDN. Making QKDN elements remotely programmable can introduce security concerns and additional requirements are likely to be necessary. Such security considerations are outside the scope of this document. Examples of functions of programmable elements in the quantum layer that might be considered for control by an SDN controller after consideration of related security issues include:

- Laser: launch power and wavelength according to different requirements.
- Intensity modulator: repetition rate of light pulses (limited by the bandwidth of the intensity modulator and any other restrictions), duration of light pulse, intensities of the signal state and decoy states.
- Phase modulator: repetition rate and phase shifts.
- Single photon detector: dead time, detection efficiency and repetition rate for gated detectors.
- Main control unit: switching QKD protocols by modifying the workflow/logic of modulators and single photon detectors.
- Post processing unit: monitoring parameters such as gain, error rate and error correction efficiency to ensure the system is doing “honest” privacy amplification according to the specified QKD security model.

Bibliography

[b-ETSI GR QKD 007] ETSI GR QKD 007 (2018), *Quantum Key Distribution (QKD) – Vocabulary*

_____