Draft new Supplement Y.Supp.QKDN_sync

Analysis of Synchronization in Quantum Key Distribution Networks

Summary

Y.Supp.QKDN_sync to ITU-T Y.3800-series Recommendations provides instructive information on time synchronization solution, function, and implementation in quantum key distribution networks (QKDN), including time synchronization function in quantum, key management, network management, and control layers of QKDN.

Keywords

Quantum Key Distribution (QKD); QKD network (QKDN); Time synchronization

Table of Contents

Draft new Supplement Y.Supp.QKDN_sync

Analysis of Synchronization in Quantum Key Distribution Networks

1. Scope

This Supplement provides instructive information on time synchronization solution, function, and implementation in QKDN. It addresses the following subjects:

- Overview of synchronization function in QKDN
- Time synchronization 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.*

[ETSI GR QKD 003] ETSI GR QKD 003 (2018), *Quantum Key Distribution (QKD); Components and Internal Interfaces*

[ETSI GR QKD 007] ETSI GR QKD 007 (2018), *Quantum Key Distribution (QKD)*; *Vocabulary*

3. Terms and definitions

3.1 Terms defined elsewhere

This Supplement uses the following terms defined elsewhere:

3.1.1 **quantum key distribution (QKD)** [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.

3.2 Terms defined in this Supplement

None.

4 Abbreviations and acronyms

This Supplement uses the following abbreviations and acronyms:

QKD	Quantum Key Distribution
QKDN	Quantum Key Distribution Network

< TBD>

5 Conventions

None.

6 Overview of synchronization function in QKDN

[Editor's Note]: Clause 6 contain synchronization technology overview, illustrative synchronization solutions in QKDN, and functional model example of QKDN synchronization, instead of requirement.

6.1 Synchronization technology overview

Synchronization technology including frequency and time synchronization, is considered to play a fundamental supporting role in ICT networks, including quantum key distribution network (QKDN). When any events happen in QKDN, the order in which they happen, and how that data is then collected and logged depends almost entirely on devices being in synchronization. Key areas where time synchronization directly affects QKDN operations include: quantum key file time stamps, log file auditing and monitoring, fault diagnosis and recovery, distributed routing control and management operations, etc. Time synchronization is also something that needs to be constantly maintained. No time-keeping device is truly accurate, so without proper synchronization, the natural drift of between devices' internal time-keeping will ultimately lead to issues.

There are several ways to implement time synchronization in ICT networks. Currently in widespread use is the Network Time Protocol (NTP), a well-established protocol that has been around for decades and is currently in its fourth version (NTPv4). NTP's accuracy is about several milliseconds, but NTPv4 can achieve sub-millisecond accuracy if the network is carefully designed and a dedicated Stratum 1 clock is used. Another commonly used time synchronization protocol is Precision Time Protocol (PTP), or IEEE 1588. which is capable of synchronizing clocks to sub-microsecond accuracy. However, it is more complicated to deploy and not universally available on network equipment.

NTP protocol adopts the client and server structure, using universal time coordinated (UTC) as the time standard, establishes hierarchical time distribution model, with considerable flexibility and practicality, can adapt to a variety of sizes, rates and link conditions of network environment. NTP not only corrects the current time, but also continuously tracks changes in time and can automatically adjust to maintain time stability even when the network fails. Furthermore, NTP incurs little network overhead and has countermeasures to ensure network security. These advantages allow NTP to obtain reliable and accurate time synchronization, and it has become the most widely used time synchronization tool in ICT networks.

In the NTP protocol synchronization process, the server and client exchange of data packets to obtain time information, using the timestamp carried by the data packets to calculate the time offset between client and server as well as the path delay introduced by transmission of data packets. Based on the above results of calculation, the time of server and client could be synchronized.

NTP is a hierarchical protocol. The source clock is called Stratum 1, which is usually a NTP time server using global navigation satellite system (GNSS) to receive timing signals through antennas, also known as satellite timing. Satellite timing has the advantages of lower propagation signal attenuation, larger coverage and higher synchronization accuracy. The ground time synchronization server measures the pseudo-distance signal through the timing antennas from satellite, in which loaded with high-performance and high-precision atomic clocks, then calculates the pseudo-distance to get the accurate time. There are many kinds of GNSS systems, for example Global Positioning System (GPS), GLONASS, Galileo, and Beidou Navigation Satellite System (BDS).

6.2 Synchronization solution in QKDN

In the quantum layer of QKDN, merely NTP-based time synchronization is not sufficient. In a typical prepare-and-measurement-based discrete variable QKD system, the transmitter for synchronization will send optical pulses synchronized to the quantum signal through a synchronization channel to the receiver. The detected synchronization signal with frequency-and-phase recovery is used as the trigger of a single photon detector (SPD) in the receiver. For typical continuous variable QKD, which is based on transmitter with gaussian modulation and a receiver with coherent detection, a physical layer synchronization channel is optional.

For example, in typical preparation-measurement QKD System such as BB84 protocol, pulse width of the quantum signal and effective SPD detection response time window are at about the hundreds picosecond level, the jitter of these signals and responses are usually limited to tens of picoseconds, which means the precision requirement of frequency/phase synchronization between transmitter and receiver need to achieve tens of picoseconds level. The current network-based frequency synchronization solutions cannot fulfil this requirement of the QKD link, and thus point-to-point synchronization channel for phase synchronization is practical solution.

In key management layer, a KM stores point-to-point key pairs generated by QKD modules and provides end-to-end keys through a key relay function. Based on the point-to-point key pairs generated in each round of protocol post-processing in the QKD module, key IDs are assigned with information such as device ID and generation time, which serve as the basis for key synchronization in the key management. The ID of each quantum key pair has uniqueness in the whole QKDN, which serves as reference identification in key storage and service, and also provides guarantee for key relaying, and ultimately forms synchronized end-to-end key.

In key storage and relay procedures, key life cycle needs to be managed according to security requirements, such as key authentication, backup, destruction, and storage time management. NTP-based network time synchronization information can be attached to the QKD-key metadata to indicate timestamp information such as generation time, relay time, storage time, provisioning time, and destruction time. For monitoring and reporting of alarm and performance information of the KM, it is also necessary to support NTP-based time synchronization information in the control unit, so that the QKDN can realize unified time domain management of the entire network.

For key supply of the user network, the QKD-key generation time information needs to be attached to the corresponding key metadata with other necessary information such as device ID. The QKD-key generation rate of current commercial QKD systems is usually at several tens kbit/s, which means QKD-key generation time information will be updated at the tens of milliseconds level and thus NTP-based network frequency synchronization could be adequate. If the QKD-key generation rate could be significantly enhanced in the future, the timing precision of these keys should be improved accordingly, other kinds of network time and synchronization solutions such as PTP could be used. Furthermore, absolute time information provided by NTP can also be used by a QKDN control unit for alarm and performance monitoring.

In the control and management layer of QKDN, a master clock can be co-located within a QKDN management. It can provide the reference timing information to the other functions to implement unified time domain management of the QKDN. On this basis, the QKDN manager and/or controller can monitor the alarm information and performance parameters of the QKD module and KM in the QKDN, as well as the diagnosis and identification of the network link status and faults, and further provide the necessary time reference information for the interaction between the QKDN and a user network.

6.3 Synchronization functional model of QKDN

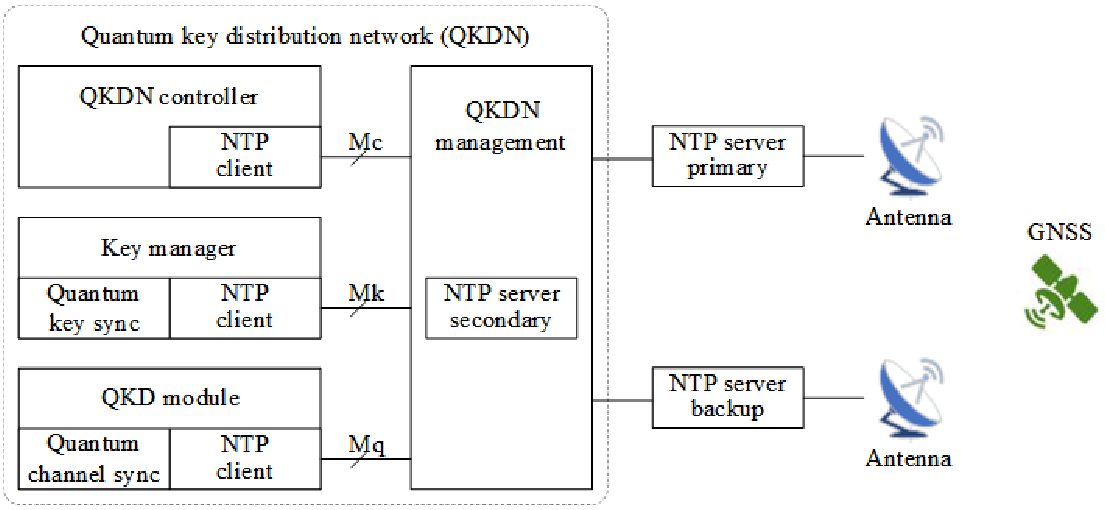

Figure 1 – Functional model example of QKDN synchronization

Based on the functional architecture model and reference points of QKDN illustrated in Figure 1 of [ITU-T Y.3802], a functional model example of QKDN synchronization is shown in Figure 1, which includes some functional elements such as:

– GNSS: Constellations of multiple satellites operating at different orbital altitudes over the earth, such as GPS, BDS, etc. Based on the atomic clocks on the satellites, it realizes the broadcasting of precise time signals that can be traced back to UTC, and it has the advantages of high timing accuracy and wide coverage. Ground subscribers receive time signals from GNSS satellites in the L1/L5 frequency bands through on-demand deployment of antennas and timing modules, to generate high-precision timing signals through automatic synchronization measurements and time-delay compensation, which can usually achieve timing accuracy of tens of nanoseconds.

– Antenna: GNSS antenna systems receive and amplify satellite signals. The amplified signal is passed to the GNSS receiver, which uses the information to calculate the time. GNSS polarized antennas only receive signals vertically or horizontally polarized. It has noise amplifiers that allow the GPS receiver to filter out noise and interference from other sources. Multi-GNSS antenna can receive L1 /L5 signals with high gain from multi constellation, such as GPS, BDS, GLONASS, and Galileo. Active antennas have a built-in amplifier that boosts the signal before being sent to the receiver. Passive antennas do not have a built-in amplifier and rely on the receiver to amplify the signal. Passive antennas are typically smaller and lighter, which may not perform as well in areas with signal challenges. Active antennas need an external power supply, but passive antennas don't.

– NTP server: GNSS-based satellite timing reduces the cost of building dedicated physical channels and has satisfactory accuracy, has become widly-used means for network operators to disseminate public time sources.Primary NTP time server (Stratum 1) receives time signals from multiple GNSS satellites through an antenna, calculates its own position and time information, converts the GNSS time to a standard time format, such as UTC, and after calibration, transmits the time signals to other devices in the network via the NTP protocol. In order to guarantee the accuracy and reliability of network timing, an independent backup NTP time server and antenna are usually configured as a backup for the GNSS satellite timing system. NTP protocol is hierarchical network system of stepped interconnections. secondary NTP time servers are usually configured and backed up in the network management system (NMS) closest to the primary NTP time server and to provide timing services to all the devices in the QKDN.

– NTP client: The timing process of NTP protocol is realized in the form of mutual information transfer between the NTP server and client. The NTP client periodically sends a time synchronization request to the server, which is an NTP protocol packet, and when the server receives the packet, it will return an answer packet to the client after processing. Both packets have timestamp information, which records essential time information in the interaction process, including originate timestamp, receive timestamp, transmit timestamp, destination timestamp, round-trip packet delay, and time offset between the client and server. The time deviation can be synchronized between the NTP client and server by calculating the above interactive process time information.

– Quantum channel synchronization: There are several QKD protocols and implementations including decoy state BB84, Gaussian modulated coherent state, twin field (TF), and measurement device independent (MDI). In QKD systems, optical signal detection, quantum state measurement and basis comparison require the transmitter and receiver to maintain high-precision synchronization, especially frequency and phase synchronization. The pulse width of quantum optical signals is usually less than hundreds of picoseconds, and the requirement for synchronization accuracy reaches sub-nanoseconds, which is unattainable by network-based synchronization schemes. Therefore, QKD systems usually adopts point-to-point optical signals transmission, combining with phase-locked and clock recovery to fulfill the frequency and phase synchronization requirement. In preparation-measurement QKD systems, for example decoy state BB84 and Gaussian modulated coherent state, synchronization optical signals can co- existence with quantum state optical signals in the same fiber based on time-division multiplexing and/or wavelength-division multiplexing. In middle-point measurement QKD systems, for example TF and MDI., the implementation of synchronization optical signals is usually more complicated.

– Quantum key synchronization: QKD system generates point-to-point quantum keys through quantum state optical signal transmission and detection, combined with protocol post-processing such as basis comparison, QBER calculation and privacy amplification. Using the time information obtained by the QKD system through NTP protocol, combined with authentication information such as device ID, the quantum key is encapsulated and cached, and output to key management or user network in form of quantum key pairs. Quantum key pairs contain meta-data such as unique key ID and time information, which are used to support their storage, relaying, and lifecycle management in QKDN, as well as cross-domain key internetworking, and ultimately realize end-to-end key generation and provide responses to symmetric key services initiated in the user network.

7 Time synchronization in QKDN

[Editor’s Note]: The function, performance, implementation, and procedures of different time synchronization functional elements in QKDN will be discussed.

< TBD>

Bibliography

< TBD>

____