Draft new Recommendation ITU-T Y.QKDN-TSNfr

Framework for integration of quantum key distribution network and time sensitive network

Summary

This Recommendation specifies the framework for integration of quantum key distribution network (QKDN) and time sensitive network (TSN) including the overview and scenarios of QKDN and TSN integration, the network capabilities to support QKDN and TSN integration, the conceptual structure and basic functions of QKDN and TSN integration, and its overall operational procedures and security considerations.

Keywords

Quantum Key Distribution (QKD); QKD network (QKDN); Time Sensitive Network (TSN)

Table of Contents

Draft new Recommendation ITU-T Y.QKDN-TSNfr

Framework for integration of quantum key distribution network and time sensitive network

1. Scope

This Recommendation specifies the framework for integration of quantum key distribution network (QKDN) and time sensitive network (TSN).

In particular, the Recommendation covers:

- Overview and scenarios of QKDN and TSN integration
- Network capabilities to support QKDN and TSN integration
- The conceptual structure and basic functions of QKDN and TSN integration
- Overall operational procedures for the integration of QKDN and TSN
- Security considerations

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.3805] Recommendation ITU-T Y.3805 (2022), *Quantum Key Distribution Networks - Software Defined Networking Control*

< Others to be added>

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.

Editor's Note: More definitions will be added as work progresses

3.2 Terms defined in this Recommendation

This chapter defines all the terms used in this recommendation.

-TBD

4 Abbreviations and acronyms

This chapters describes all the abbreviations and acronyms used in the recommendation.

API	Application Programming Interface
QKD	Quantum Key Distribution
QKDN	Quantum Key Distribution Network
QoS	Quality of Service
TSN	Time Sensitive Network

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 and scenarios of the integration of QKDN and TSN

The Time-sensitive Networking (TSN) is one widely applied communication standard developed by IEEE to meet stringent latency and timing requirements of the industrial environment.

TSN relies on precise time synchronization and time-aware traffic shaping and scheduling to ensure deterministic and reconfigurable data transmission in Ethernet networks. As a key enabler for IT/OT convergence, TSN is expected to provide new solutions for the next generation industrial networks.

A centralized TSN model is as shown in Fig.1. The control signalling interaction between the centralized network configurator (CNC) and TSN switches, the data delivery between TSN endpoints and switches and the time synchronization messages all need highly secure and real-time security protection measures.

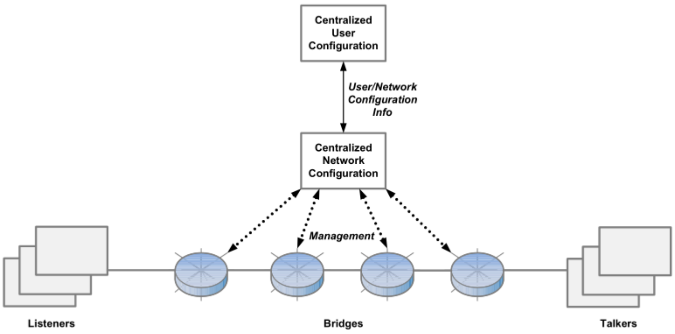
Centralized User Configuration
User/Network Configuration Info
Centralized Network Configuration
Management
Listeners
Bridges
Talkers

Fig. 1 Fully centralized TSN model

Ensuring cybersecurity is an important requirement in life-critical control systems for which industrial TSN will provide communication service. Traditional key exchange methods (i.e., either manually pre-shared keys or public key exchange), which will require more computing resources and cause additional latency, are discouraged for the TSN targeted scenario.

As QKD can generate out-of-band symmetric keys based on quantum physics principle, it is envisioned to be an important solution for TSN security enhancement.

This Recommendation aims to provide a framework to facilitate the integration of QKDN and TSN and to ensure the efficient security enhancement of TSN based on QKDN.

Editor’s Note: Further descriptions will be added for the concept of QKDN and TSN integration as work progresses.

7 Network capabilities to support QKDN and TSN integration

Editor’s Note: network capabilities to support QKDN and TSN integration considering the various integration scenarios, including QKD protected time synchronization and packet delivery, QKD and TSN coordination etc, will be described.

The basic network capabilities to support QKDN-TSN integration ~~may~~ include:

- ~~QKDN secured time synchronization message delivery between TSN grandmaster clock and slave clocks;~~
- ~~QKDN-secured TSN control signalling interaction between CNC/CUC and endpoint/bridges.~~
- ~~QKDN-secured packet transportation between talker and listeners.~~
- ~~TSN controller aware of QKDN key resource to schedule data paths with security guarantee;~~
- ~~QKDN controller aware of TSN requirements to generate key resource along TSN links.~~

● **End-to-end encryption of TSN services**

The TSN endpoints has a capability to obtain keys from the associated QKDN user nodes.

● **QKDN awareness to TSN**

The TSN controller has a capability to be aware of the latency caused by QKDN key supply, relay and consumption to ensure the link delay budget of TSN data flows to be satisfied while protected by QKDN.

● **Encryption of synchronization signals**

All TSN nodes have a capability to obtain keys from QKDN for message authentication between neighboring TSN nodes to ensure the security of network synchronization.

● **Encryption of control plane data signals**

The CNC/CUC of TSN has a capability to obtain keys from the connected QKD nodes to ensure the secure signaling delivery between CNC/CUC and the associated TSN endpoints or switches.

8 Conceptual structures for QKDN and TSN integration

Editor’s Note: The conceptual structures of QKDN and TSN integration will be described.

The TSN as a user network can be secured by QKDN. The conceptual structure for the integration of QKDN and TSN is as shown in Fig. 2.

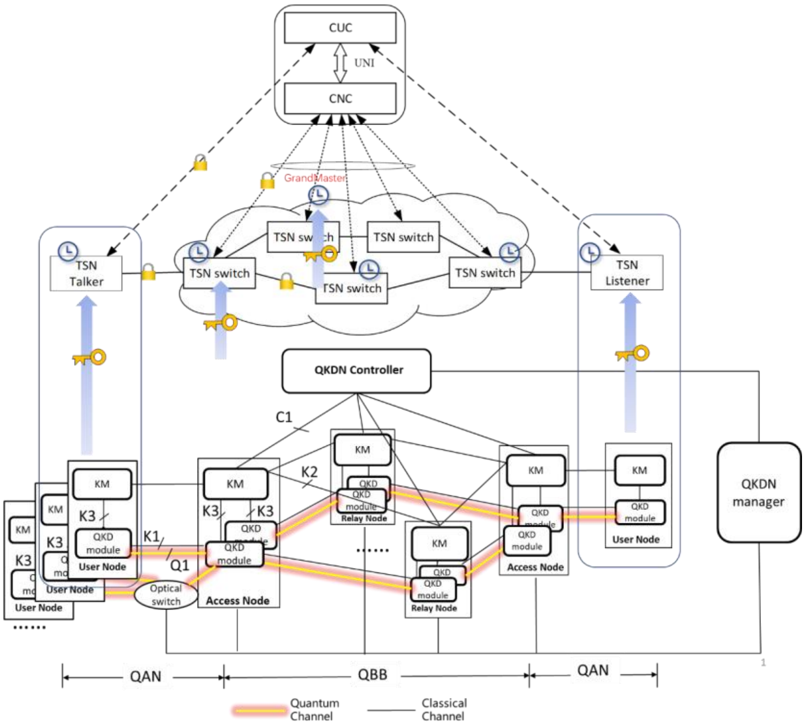

Fig. 1 Conceptual structure of TSN integrated with QKDN as a user network

9 Basic functions of QKDN and TSN integration

Editor’s Note: Basic functions and relevant functional entities to implement the integration of QKDN and TSN will be described.

- **QKDN-based encryption for TSN data flows**

For any two TSN endpoints delivering deterministic data flows, both the talker and listener need to be connected to QKDN user nodes, in order to obtain encryption and decryption keys in a timely manner, which can ensure the encrypted service flow based on QKD-keys can arrive at the destination and decrypted within the required delay bound, as shown in Figure 3-1.

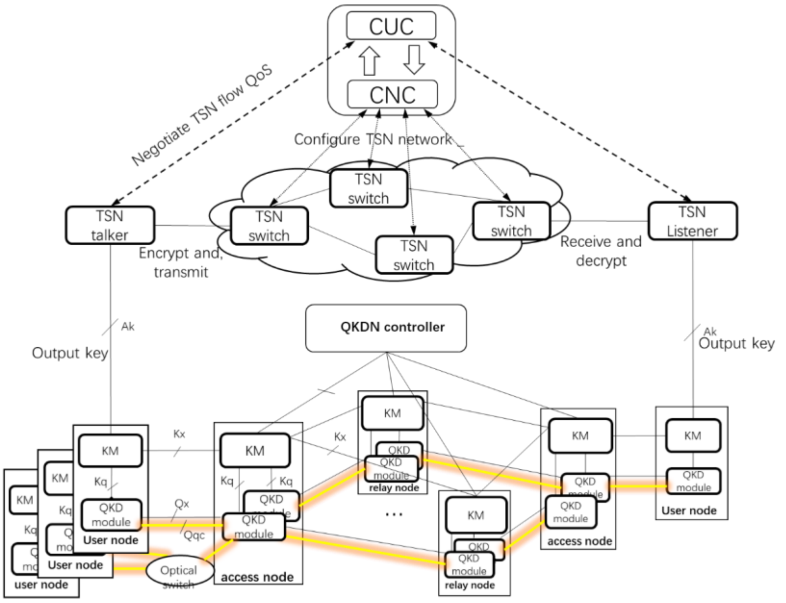

Figure 3-1 Conceptual diagram for TSN data flow secured by QKDN

- **QKDN awareness to TSN**

In addition, as TSN is designed to be dynamically reconfigurable, there is a CNC (Centralized Network Configurator) to determine the route real-timely and schedule the gate control parameters on each TSN switch along the route. Thus, when the TSN route is rescheduled under the instruction of CNC, the QKDN side needs to be aware of the network change via either the CNC or endpoints and regenerate keys accordingly.

- **QKDN-based encryption of synchronization signals**

TSN adopts the 802.1AS protocol to ensure network wide precise time synchronization. All the TSN nodes need to transmit PTP (Precision Time Protocol) messages between any neighboring nodes containing time stamps based on the White Rabbit algorithm, to achieve ns-level synchronization performance within the entire network. Thus, it is necessary to ensure the integrity of the PTP messages delivery. In order to secure the PTP messages by QKD-keys, all the TSN nodes with clocks need to be connected to QKDN nodes and obtain QKD-keys for message authentication between neighboring TSN nodes, as shown in Figure 3-2.

Formatted: Font: (Asian) Chinese (Simplified, Mainland China)

Formatted: Centered

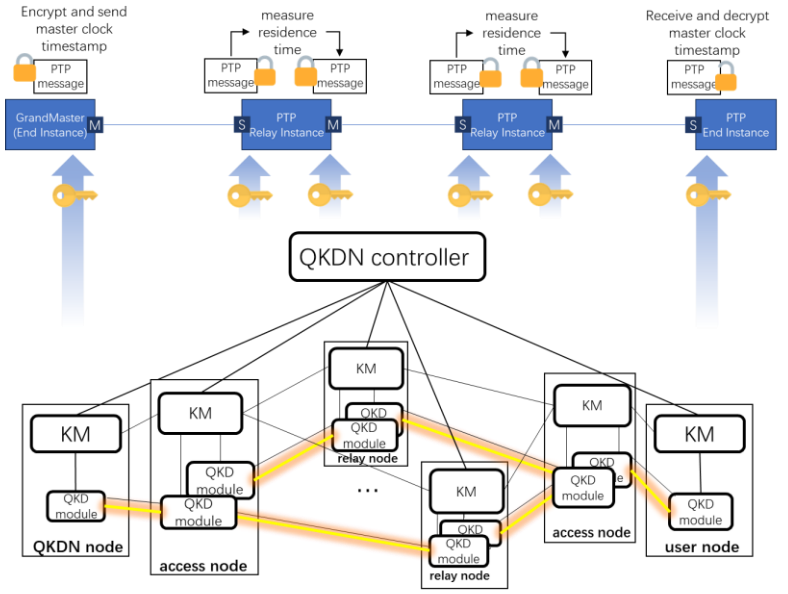

Figure 3-2 Conceptual diagram for TSN synchronization messages secured by QKDN

Formatted: Centered

- **QKDN-based encryption for TSN control plane signals**

The TSN control plane data including the data flow between CNC and TSN switches for scheduling and control signals, and data flow between CUC (Centralized User Configurator) and TSN endpoints for service requests and QoS negotiation, need to be protected especially with integration guarantee. Thus, the CNC/CUC need to be connected with QKD nodes to obtain keys between CNC/CUC and the associated TSN endpoints or switches, as shown in Figure 3-3.

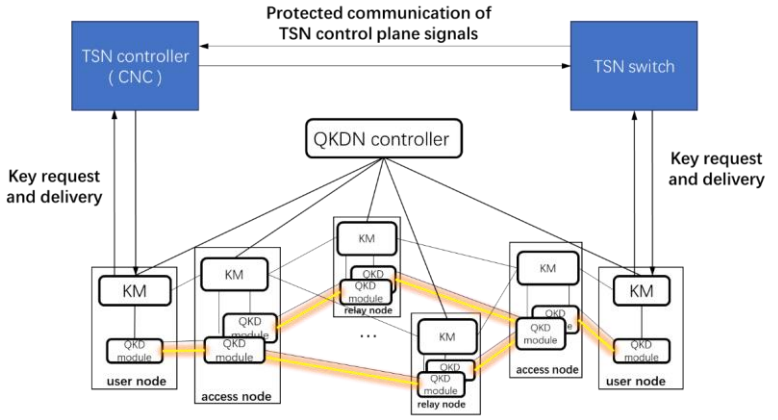

Figure 3-3 Conceptual diagram for TSN control plane signal communication secured by QKDN

10 Overall operational procedures of QKDN and TSN integration

Editor's Note: Operational procedures to implement the coordination and integration of the QKDN and TSN for use cases will be described.

11 Security considerations

Editor's Note: General security perspective are addressed here for QKDN and TSN integration, however, the details of security are outside of scope of this recommendation

Appendix I:

The motivation for TSN and QKDN integration

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

As required by Industry 4.0, the traditional hierarchical factory networks is going to evolve into the future fully inter-connected industrial networks, which can carry the factory level best effort IT (Information Technology) traffic and field level deterministic OT (Operation Technology) traffic in a unified network. In this way, instead of small groups of I/O devices being controlled by separate PLCs (Programmable Logic Controller), all the I/O devices can be controlled in a globally optimized and on-demand reconfigurable manner, in order to achieve highly efficient, customized and intelligent manufacturing envisioned by industry 4.0.

As shown in Fig. 1, the TSN is developed to fulfil the mission for IT/OT converged industrial network. Unlike the traditional industrial networks where most critical industrial data (e.g., I/O signals to control the motors) is delivered within closed workshops, the TSN needs to carry the deterministic and critical OT services across large scale factory networks (campus level at least). This will expose more security holes for the sensitive OT services which made cyber security guarantee as a must.

However, traditional cyber security measures, e.g., asymmetric crypto algorithms for key distribution, will introduce additional latency, which will cause difficulty to fulfil the deterministic and hard real-time (lowed than 1ms end-to-end delay and 100ns jitters in certain cases) requirements of OT services.

QKDN can generate symmetric key flows in a physically out-band and information theoretically secure manner. In addition, the OT traffic, e.g., I/O control signals, usually require very low data rate (e.g., 1bit for a ON/OFF switch control, Tens of bits per cycle for a motor control). The current QKD key rate is enough for OTP encryption of OT service flows. Thus, the OT service data can be encrypted in an extremely simple manner via OTP XOR operation only which will require very low latency compared to traditional cryptographies.

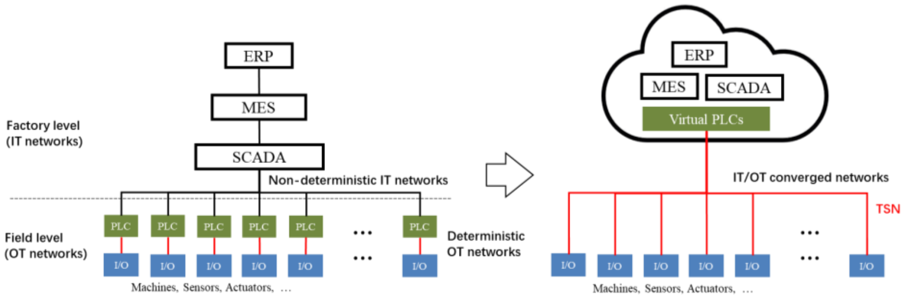

Fig. 1 Evolution of industrial networks with TSN

Bibliography

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