ITUPublications
Recommendations

International Telecommunication Union
Standardization Sector

Recommendation

ITU-T Y.3812 (09/2022)

SERIES Y: Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities

Quantum key distribution networks

Quantum key distribution networks – Requirements for machine learning based quality of service assurance

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Enhancements to NGN	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Computing power networks	Y.2500–Y.2599
Packet-based Networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999
FUTURE NETWORKS	Y.3000–Y.3499
CLOUD COMPUTING	Y.3500–Y.3599
BIG DATA	Y.3600–Y.3799
QUANTUM KEY DISTRIBUTION NETWORKS	**Y.3800–Y.3999**
INTERNET OF THINGS AND SMART CITIES AND COMMUNITIES	
General	Y.4000–Y.4049
Definitions and terminologies	Y.4050–Y.4099
Requirements and use cases	Y.4100–Y.4249
Infrastructure, connectivity and networks	Y.4250–Y.4399
Frameworks, architectures and protocols	Y.4400–Y.4549
Services, applications, computation and data processing	Y.4550–Y.4699
Management, control and performance	Y.4700–Y.4799
Identification and security	Y.4800–Y.4899
Evaluation and assessment	Y.4900–Y.4999

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T Y.3812

Quantum key distribution networks – Requirements for machine learning based quality of service assurance

Summary

Recommendation ITU-T Y.3812 specifies high-level and functional requirements of machine learning (ML) based quality of service (QoS) assurance for quantum key distribution networks (QKDNs).

This Recommendation first provides an overview of requirements of ML based QoS assurance for the QKDN. It describes a functional model of ML based QoS assurance which is followed by associated high-level and functional requirements of ML based QoS assurance. Additionally, some use cases are described.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.3812	2022-09-29	13	11.1002/1000/15065

Keywords

Functional model, machine learning, QKDN, QoS assurance, and requirements.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents/software copyrights, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T Y.3812

Quantum key distribution networks – Requirements for machine learning based quality of service assurance

1 Scope

This Recommendation specifies high-level and functional requirements of ML based quality of service (QoS) assurance for quantum key distribution networks. The scope of this Recommendation is as follows:

- Overview of requirements of ML based QoS assurance for QKDNs;
- Functional model of ML based QoS assurance for QKDNs;
- High-level requirements of ML based QoS assurance for QKDNs;
- Functional requirements of ML based QoS assurance for QKDNs;
- Use cases of ML based QoS assurance for QKDNs.

This Recommendation considers ML for QKDN in the context of QoS assurance only. Therefore, any other use of ML is out of the scope of this Recommendation.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.1710] Recommendation ITU-T X.1710 (2020), Security framework for quantum key distribution networks.

[ITU-T Y.2701] Recommendation ITU-T Y.2701 (2007), Security requirements for NGN release 1.

[ITU-T Y.3101] Recommendation ITU-T Y.3101 (2018), Requirements of the IMT-2020 network.

[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.3804] Recommendation ITU-T Y.3804 (2020), *Quantum key distribution networks - Control and management*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 assurance [b-ITU-T X.1500]: The degree of confidence that the process or deliverable meets defined characteristics or objectives.

3.1.2 network performance [b-ITU-T E.417]: The performance of a portion of a telecommunications network that is measured between a pair of network-user or network-network interfaces using objectively defined and observed performance parameters.

3.1.3 quality of experience [b-ITU-T P.10]: The degree of delight or annoyance of the user of an application or service. [b-Qualinet]

NOTE – Recognizing ongoing research on this topic, this is a working definition which is expected to evolve for some time. (This note is not part of the definition.)

3.1.4 quality of service [b-ITU-T Q.1741.1]: The collective effect of service performance which determine the degree of satisfaction of a user of a service. It is characterized by the combined aspects of performance factors applicable to all services, such as:

– Service operability performance;

– Service accessibility performance;

– Service retainability performance;

– Service integrity performance; and

– Other factors specific to service.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

DWDM	Dense Wavelength Division Multiplexing
E2E	End to End
ETL	Extract-Transform-Load
KMA	Key Management Agent
KML	Key Management Layer
KPI	Key Performance Indicator
KSA	Key Supply Agent
ML	Machine Learning
QBER	Quantum Bit Error Rate
QKD	Quantum Key Distribution
QKDN	Quantum Key Distribution Networks
QL	Quantum Layer
QoE	Quality of Experience
QoS	Quality of Service

5 Conventions

The keywords "is required to" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this Recommendation 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

The QKDN is expected to be able to provide optimized support for a variety of different quantum key distribution (QKD) services. The key performance indicators (KPIs) include optimal latency, accuracy, throughput and availability for key distribution.

One of the challenges of QKDN is to ensure the network performance and specific QoS /quality of experience (QoE) requirements per application scenario.

To meet such QoS requirements for different applications, QKDN is required to support the following capabilities:

1) QoS related events that happened in the past can be reconstructed automatically and accurately;

2) Current QoS related events can be detected accurately and in a timely manner to trigger automatic and immediate actions;

3) Future QoS related events can be predicted with high confidence.

With the increasing complexity and dynamics of network behaviours, it is very hard for traditional programmers to develop traditional codes to schedule the network resources based on expert knowledge, especially when the mathematical causal relationship between the network events and the QoS anomalies may be dependent on unknown characteristics and may not be known or possible to derive.

ML mechanisms, with the capabilities of teaching a computer to learn knowledge using data without being explicitly programmed, have demonstrated their capabilities to solve complex tasks such as image recognition and speech recognition. ML mechanisms can also be applied to the networking field to intelligently learn the network environment and react to dynamic situations. They can learn from past QoS data against target KPIs and reconstruct relationships between past QoS related data and QoS anomalies automatically and accurately. Using the learned relationships, they can detect current QoS anomalies. They can then trigger automatic mitigation or suggested actions. ML mechanisms can also predict future QoS related anomalies with high confidence. These capabilities are modelled as an ML based QoS assurance functional model.

7 Functional model of ML based QoS assurance for QKDN

ML is based on algorithms, data and computing power. Current communication networks with distributed architecture and limited computing power have not been designed to cope with data analytics and ML.

According to [ITU-T Y.3801], the QKDN is required to support diverse performance requirements of heterogeneous services based on unified and end-to-end (E2E) QoS control mechanisms. To meet such requirements, QKDN QoS assurance ML algorithms need input data which should be collected from the quantum layer and key management layer. They also need QoS KPI data to build a correlation between QoS KPI and QoS related data. However, due to the complexity and dynamics of the QKDN, it will produce massive and heterogeneous data. Therefore, a unified data format is necessary for the functional model of ML based QoS assurance to work efficiently and accurately.

According to [ITU-T Y.3804], the QKDN management and orchestration plane need to detect the QoS fault and anomalous events and perform the management process, aiming at the fulfilment and assurance of QKDN services. Assurance is defined as the degree of confidence that the process or deliverable meets defined characteristics or objectives [b-ITU-T X.1500]. Based on these considerations, this Recommendation specifies a functional model of ML based QoS assurance which is depicted in Figure 1.

The functional model of ML based QoS assurance for QKDN includes functional components such as QoS data collection, pre-processing, modelling and training, QoS anomaly detection, QoS anomaly prediction, QoS decision making, and reporting. The detailed descriptions of the model are for further study.

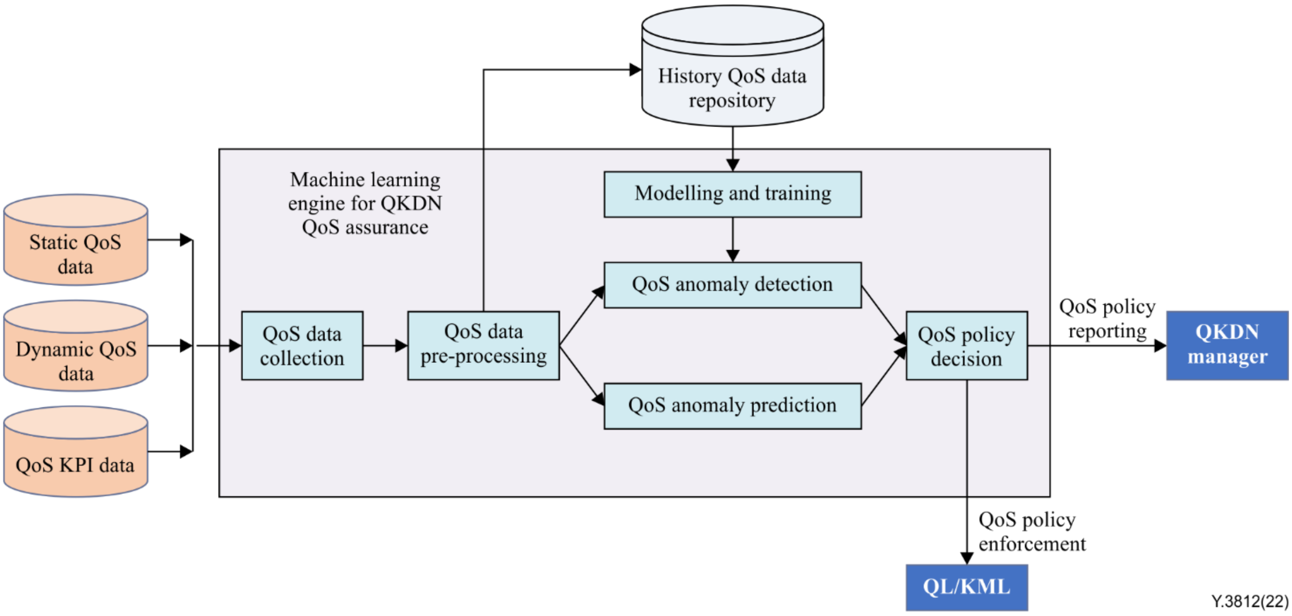

Figure 1 – Functional model of ML based QoS assurance for the QKDN

8 High-level requirements of ML based QoS assurance for the QKDN

The high-level requirements of ML based QoS assurance for QKDN include the requirements of QoS related data collection, data pre-processing, history QoS data storage, ML based modelling and training, QoS anomaly detection and prediction, QoS policy decision making, enforcement and reporting.

- The QKDN is required to collect static QoS data and QoS KPIs from the quantum layer (QL) and key management layer (KML).
- The QKDN is required to collect dynamic QoS data and QoS KPIs from the QL and KML.
- The QKDN is required to pre-process collected raw QoS data.
- The QKDN is required to provide a history QoS data repository.
- The QKDN is required to construct ML models for QoS assurance.
- The QKDN is recommended to provide training in QoS anomaly detection and prediction.
- The QKDN is required to support the detection of QoS related anomalies.
- The QKDN is recommended to support the prediction of QoS related anomalies.
- The QKDN is recommended to support QoS policy decision making.
- The QKDN is recommended to enforce QoS decision policy.
- The QKDN is recommended to report QoS decision policy.

9 Functional requirements of ML based QoS assurance for QKDN

9.1 Functional requirements for QoS data collection

The QoS data can be collected from the QL and KML, either passively or actively.

The functional requirements for QL QoS data collection are as follows.

- The QKDN is required to collect static QoS data from the QL (e.g., history QL QoS data set).
- The QKDN is required to collect dynamic QoS data from the QL (e.g., link distance, link complexity, noise, secret-key rate, quantum bit error rate (QBER), operating frequency).
- The QKDN is required to collect QL QoS KPI data (e.g., QoS KPIs of the quantum and classical channels).

The functional requirements for KML QoS data collection are as follows.

- The QKDN is required to collect static QoS data from the KML (e.g., history KML QoS data set).
- The QKDN is required to collect dynamic QoS data from the KML (e.g., the usage of KML resources, key management agent (KMA) and key supply agent (KSA) links delay, loss rate and throughput).
- The QKDN is required to collect KML QoS KPI data (e.g., QoS KPIs of the KMA and KSA links).

9.2 Functional requirements for QoS data pre-processing

- The QKDN is required to perform extract-transform-load (ETL) and transform the collected multisource, heterogeneous QKDN QoS raw data into understandable, unified and easy-to-use structures.
- The QKDN is required to clean and filter noisy data from the collected multisource, heterogeneous QKDN QoS raw data.
- The QKDN is recommended to normalize and unify the data format of the collected multisource, heterogeneous QKDN QoS raw data for further storage and analysis.

9.3 Functional requirements for history QoS data repository

- The QKDN is required to store the multisource, heterogeneous QKDN QoS pre-processed data.
- The QKDN is recommended to label the QoS related anomalies and the corresponding collected QKDN QoS pre-processed data, if applicable.

9.4 Functional requirements for modelling and training

- The QKDN is required to construct ML models based on the pre-processed QKDN QoS data and QoS KPI parameters (e.g., ML models: supervised learning, unsupervised learning, semisupervised learning, deep learning, reinforcement learning, either alone or in combination).
- The QKDN is recommended to train the ML models be based on the available pre-processed QKDN QoS data and QoS KPIs.

9.6 Functional requirements for QoS application

- The QKDN is required to undertake ML for QoS diagnostics.
- The QKDN is recommended to support the prediction of QoS related anomalies based on ML models.

- The QKDN is recommended to support the assessment of QoS related data based on ML models.
- The QKDN is recommended to support static parameter tuning in the QL and KM layer according to QoS related data based on ML models.
- The QKDN is recommended to support dynamic feedback in the QL and KM layer according to QoS related data based on ML models.

9.7 Functional requirements for QoS policy decision making, enforcement and reporting

- The QKDN is recommended to make decisions on key relay routes in terms of ML based QoS policy.
- The QKDN is recommended to measure QoS parameters in terms of the ML based QoS enforcement policy.
- The QKDN is recommended to (re-)configure the QKD module, QKD links, KM and KM links in terms of the ML based QoS policy.

9.8 Reference point requirements

- The QKDN is required to support QoS data collection by the QKDN reference points Mc, Mk, Mq, Mqrp, Mops, Mu and Ma.
- The QKDN is required to support QoS data feedback based on the QoS policy decision by the QKDN reference points Mc, Mk, Mq, Mqrp, Mops, Mu and Ma.
- The QKDN is required to support the adjustment of the key-distribution strategy based on QoS data assessing in the KM layer by QKDN reference points Mc and Mk.
- The QKDN is required to support parameter tuning based on QoS data assessing in the QL by QKDN reference points Mc, Mq, Mqrp and Mops.
- The QKDN is required to support data communication for QoS/QoE correlation by the QKDN reference points Mc, Mu and Ma.
- The QKDN is required to support reference points between the QoS policy decision functional component and the user plane.
- The QKDN is required to support reference points between the QoS policy decision functional component and the management plane.

10 Security considerations

This Recommendation describes the high-level and functional requirements of ML based QoS assurance for QKDNs; therefore, security requirements described in [ITU-T X.1710], [ITU-T Y.3801] and [ITU-T Y.3802] and general network security requirements and mechanisms in IP based networks described in [ITU-T Y.2701] and [ITU-T Y.3101] should be applied. Details are outside the scope of this Recommendation.

Appendix I

Use cases of machine learning based QoS assurance for QKDN

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

Some use cases of ML based QoS assurance for the QKDN are described in this Recommendation.

I.1 Quantum channel performance

Integrating QKD with existing traditional dense wavelength division multiplexing (DWDM) fibre-optical networks is critical to the realization and commercialization of quantum networks. When solving the problem of mixed transmission of quantum signal and classical signal, the main challenge is the impact of noise, which has a significant impact on the QoS of quantum signal. It is difficult for the traditional method to estimate the noise in the quantum band in practical networks, because a large number of classical channels is distributed at different wavelengths and different channel spacing, modulated by mixed formats and carrying different data rates.

Therefore, it is proposed to apply the ML method to estimate the performance of the quantum channel (e.g., noise, secret-key rate, and QBER) to achieve better QoS. ML can be used to make accurate predictions. Selecting the quantum channel with the best transmission performance based on the prediction results can reduce the influence of noise and improve the QoS.

I.2 QoS fault diagnosis and prediction

The QoS fault will lead to the decline of QoS and QoE in the QKDN. As the size of the QKDN continues to grow, it is urgently necessary to develop an automatic and efficient data mining analysis tool to realize the QoS fault diagnosis of the QKDN and to predict the QoS fault of the QKDN by combining the historical data of equipment operation and external data.

The QoS fault diagnosis model of the QKDN needs the ability to quickly identify the type of QoS fault and accurately locate the QoS fault. The types of device in a QKDN are cumbersome, and some of them are very complex and crucial. We can use the advantages of ML to extract the QoS faults of the collected QKDN. This information and various data are based on deep learning methods, which can establish the characteristics of the QKDN more accurately and perform QoS fault diagnosis in the QKDN more effectively.

The QoS fault prediction model of the QKDN needs the ability to predict QoS faults in advance according to historical data and external data. The amount of historical data and external data in the QKDN are numerous, and the data types are complex and diverse. It is difficult to find the internal patterns through these QoS data. Machine learning can be used to find hidden patterns in QoS data, and the ML model can accurately predict the impending QoS fault through these inherent patterns so as to handle the QoS faults of the QKDN more accurately.

Bibliography

[b-ITU-T E.417] Recommendation ITU-T E.417 (2005), *Framework for the network management of IP-based networks.*

[b-ITU-T P.10] Recommendation ITU-T P.10/G.100 (2017), *Vocabulary for performance, quality of service and quality of experience*.

[b-ITU-T Q.1741.1] Recommendation ITU-T Q.1741.1 (2002), *IMT-2000 references to release 1999 of GSM evolved UMTS core network with UTRAN access network*.

[b-ITU-T X.1500] Recommendation ITU-T X.1500 (2011), *Overview of cybersecurity information exchange.*

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

[b-ITU-T Y.3806] Recommendation ITU-T Y.3806 (2021), *Quantum key distribution networks – Requirements for quality of service assurance*.

[b-ITU-T Y.3807] Recommendation ITU-T Y.3807 (2021), *Quantum key distribution networks - Quality of service parameters*.

[b-Qualinet] Qualinet White Paper on Definitions of Quality of Experience (2013), Output from the fifth Qualinet meeting, Novi Sad, March 12. http://www.qualinet.eu/index.php?option=com_content&view=article&id=45&Itemid=52

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	**Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities**
Series Z	Languages and general software aspects for telecommunication systems

Published in Switzerland
Geneva, 2022