DESIGN OF EFFICIENT RESOURCE PROVISIONING ALGORITHMS FOR QUANTUM KEY DISTRIBUTION-SECURED OPTICAL NETWORKS

Ph.D. Thesis

by

Purva Sharma

DEPARTMENT OF ELECTRICAL ENGINEERING
INDIAN INSTITUTE OF TECHNOLOGY INDORE

November, 2023

DESIGN OF EFFICIENT RESOURCE PROVISIONING ALGORITHMS FOR QUANTUM KEY DISTRIBUTION-SECURED OPTICAL NETWORKS

A THESIS

Submitted in partial fulfillment of the

requirements for the award of the degree

of

DOCTOR OF PHILOSOPHY

by

Purva Sharma

DEPARTMENT OF ELECTRICAL ENGINEERING
INDIAN INSTITUTE OF TECHNOLOGY INDORE

November, 2023

INDIAN INSTITUTE OF TECHNOLOGY INDORE

CANDIDATE'S DECLARATION

I hereby certify that the work which is being presented in the thesis entitled **DESIGN OF EFFICIENT RESOURCE PROVISIONING ALGORITHMS FOR QUANTUM KEY DISTRIBUTION- SECURED OPTICAL NETWORKS** in the partial fulfillment of the requirements for the award of the degree of **DOCTOR OF PHILOSOPHY** and submitted in the **DEPARTMENT OF ELECTRICAL ENGINEERING, Indian Institute of Technology Indore**, is an authentic record of my own work carried out during the time period from January 2019 to November 2023 under the supervision of Dr. Vimal Bhatia, Professor, Indian Institute of Technology Indore, India and Dr. Shashi Prakash, Professor, Institute of Engineering and Technology, Devi Ahilya University, Indore, India.

The matter presented in this thesis has not been submitted by me for the award of any other degree of this or any other institute.

Purva
06/11/2023

Signature of the student with date
PURVA SHARMA

This is to certify that the above statement made by the candidate is correct to the best of my knowledge.

06.11.2023

Signature of Thesis Supervisor with date
PROF. VIMAL BHATIA

6/11/2023

Signature of Thesis Co-Supervisor with date
PROF. SHASHI PRAKASH

PURVA SHARMA has successfully given her Ph.D. Oral Examination held on 13/02/2025.

13.02.2025

Signature of Thesis Supervisor with date
PROF. VIMAL BHATIA

13/02/2025

Signature of Thesis Co-Supervisor with date
PROF. SHASHI PRAKASH

ACKNOWLEDGMENTS

Though words are seldom sufficient to express gratitude and feelings, it gives me an opportunity to acknowledge those who have been the driving force behind my Ph.D. journey and success.

First and foremost, praises and thanks to the **God**, for his showers of blessings throughout my Ph.D. journey to accomplish the research successfully.

I would like to express my deep and sincere gratitude to my research supervisor, **Prof. Vimal Bhatia** for his sustained support, motivation, encouragement, freedom, and guidance throughout this research tenure. I have been extremely lucky to have a supervisor who cared so much about my work, and who responded to my questions and queries so promptly. I never felt alone in this wonderful journey of accomplishments and it is made possible through his continuous motivation and guidance. I am extremely grateful for what he has offered me. I also thank him for many things that I learnt during this tenure on both personal and professional fronts.

I am also thankful to my thesis co-supervisor **Prof. Shashi Prakash** for the patient guidance, encouragement and advice he has provided throughout my Ph.D. journey. His vision, sincerity and motivation have deeply inspired me. It was a great privilege and honor to work and study under his guidance. I would also like to thank my PSPC committee members **Prof. Mukesh Kumar** and **Prof. Subhendu Rakshit** for theirs insightful suggestions and advice that helped me to enhance my understanding of the material present in this thesis.

I am also privileged to thank Director, **Prof. Suhas Joshi**, all Deans and Head of the Department of Electrical Engineering of Indian Institute of Technology, Indore for all the facilities, support, and help. I extend my sincere thanks to the **Ministry of Education (MoE), Government of India** and **Indo-US Science and Technology Forum (IUSSTF)** (ID: IUSSTF/JC-089/2019) for their financial support to this research work.

I am grateful to my senior **Dr. Anuj Agrawal** for his valuable guidance, encouragement, and support at the early stage of my research work. I would also like to thank my seniors at Signals and Software Group (SaSg), **Dr. Pragya Swami**, **Dr. Uday Kumar Singh**, **Dr. Puneet Singh Thakur**, **Dr. Praveen Kumar Singya**, and **Dr. Arijit Dutta**. They have taught me the lab culture and I would like to acknowledge all their support, friendship, assistance and motivation during entire tenure of my research. I am also thankful to the juniors of my lab, **Mr. Abhinav Singh Parihar**, **Mr. Deepak Kumar**, **Mr. Justin Jose**, **Ms. Vaishali Sharma**, **Mr. Shubham Bisen**, **Ms. Anupma Sharma**, **Mr. Vidya Bhaskar Shukla**, and **Mr. Amit Baghel** for their friendly behavior, support, and all the enjoyable moments throughout this journey. I would like to thank **Mr. Shubham Gupta**, M. Tech Student at SaSg, for his collaboration and supportive nature. A special thanks to my friends and colleagues of the department for their help and constant motivation.

This journey would not have been possible without the support of my family members. Thank you for encouraging me in all of my pursuits and inspiring me to follow my dreams. Especially, I would like to say a heartfelt thank you to my parents, **Mrs. Hansa Sharma** and **Dr. Shaliendra Sharma**, for always believing in me, encouraging me to follow my dreams and helping me in financial crunch situations.

My father always encourage me to do higher studies and my mother makes me confident. I am grateful to my sister **Ms. Prachi Sharma** and my brother **Mr. Vikas Purohit** for their constant support.

I owe thanks to a very special person, my husband, **Dr. Sohit Sharma** for his love, support and understanding during my pursuit of Ph.D degree that made the completion of thesis possible. I greatly value his contribution and deeply appreciate his belief in me. My heart felt regard goes to my father in law, mother in law, and sister in law for their love and moral support. I consider myself the luckiest in the world to have such a lovely and caring family, standing beside me with their love and unconditional support.

Purva Sharma

Dedicated to my parents, my sister, and my husband

ABSTRACT

Increasing incidents of attacks and evolution of quantum computing poses challenges to secure existing information and communication technologies infrastructure. In recent years, quantum key distribution (QKD) is being extensively researched and is widely accepted as a promising technology to realize secure networks. QKD technique provides unconditional theoretical security as it relies on the fundamental principles of quantum mechanics, namely, the Heisenberg's uncertainty principle and the quantum no-cloning theorem, instead of the computational complexity of algorithms. These fundamental principles ensure that a third party trying to eavesdrop on a secret key is easily detected. It generates and distributes secret keys over an insecure communication channel using QKD protocols such as Bennett and Brassard-84 (BB84) and others. The generated secret keys are then used to encrypt/decrypt the information. Optical fiber networks carry a huge amount of information and are widely deployed around the world in the backbone terrestrial, submarine, metro, and access networks. Thus, increasing incidents of lightpath attacks motivated the research and development of QKD-secured optical networks (QKD-ONs).

A QKD-ON involves realization of quantum signal channel (QSCh) for transmission of quantum bits, public interaction channel (PICh) for verification of the exchanged key information (these two channels form a QKD system), as well as the traditional data channel (TDCh) for encrypted data transmission between the sender and the receive. A cost-efficient solution for deployment of QKD-ONs is to integrate QKD (QSCh/PICh) into existing optical networks (TDCh) using wavelength division multiplexing (WDM). However, co-existence of the QSCh and the two classical channels introduces various networking challenges, such as routing, wavelength and time-slot assignment (RWTA), trusted repeater node (TRN) placement, resiliency, quantum key recycling, and QKD for multi-cast service, in QKD-ONs.

The problem of assigning an appropriate path and suitable network resources to establish a lightpath (LP) request is known as routing and wavelength assignment (RWA) in classical WDM optical networks. However, the QKD-ONs consist of three channels, namely, QSCh, PICh, and TDCh, where wavelengths reserved for TDCh are assigned to QKD-secured lightpath request (QKD-LPR) for data transmission and wavelengths reserved for QSCh and PICh are utilized employing optical time division multiplexing (OTDM) for secret key assignment. Thus, the modified problem in QKD-ONs is known as RWTA. The RWTA problem was investigated in traditional OTDM networks. However, different from existing RWTA, the unique feature in QKD-ONs is that the secret key for QKD-LP/LP request transmitted through TDCh must be updated frequently to prevent the data being cracked by the eavesdroppers. Hence, the network resources in QSCh should be reassigned periodically to update the secret key of QKD-LPR with specific security level. This diverse assignment and reassignment of network resources in QSCh make the RWTA or routing and resource assignment (RRA) problem of QKD-ONs different and complex compared to the existing RWA and RWTA. The main focus of this thesis is to address the RRA problem, which is one of the most important networking challenges of the QKD-ONs.

Initially, in this thesis, the effect of blocking is analyzed for different categories of QKD-LPRs (CoQKD-LPRs) during assignment and reassignment of network resources in QKD-ONs. In QKD-ONs, the blocking increases with increase in the

number of QKD-LPRs, as well as with the modifications of secret keys for enhancing the security level of QKD-LPRs. Hence, the blocking affects the QKD-LPRs of different security levels, especially the QKD-LPRs of high and moderate security levels. Such QKD-LPRs require more security (that means secret key of such QKD-LPRs is updated more frequently to prevent the data from eavesdroppers) than the low priority (LP)QKD-LPRs during security breaches. Hence, resources in QSCh for high priority (HP)QKD-LPRs and moderate priority (MP)QKD-LPRs should be reassigned periodically during RRA, and if resources are not available to satisfy the QKD-LPRs requirement, then such QKD-LPRs get rejected. Moreover, if resources are assigned first to LPQKD-LPRs, then maximum resources are occupied by such QKD-LPRs in the network. This leads to lower availability of network resources for HPQKD-LPRs and MPQKD-LPRs, thereby resulting in the blocking of HPQKD-LPRs and MPQKD-LPRs. Thus, the prioritization of QKD-LPRs based on the security level is essential for reducing the impact of blocking in such networks. An efficient secret key assignment priority ordering policy (SKA-POP) for different CoQKD-LPRs is proposed for RRA in QKD-ONs. The performance of the proposed SKA-POP is compared with non-priority order-based RWTA (NP-RWTA), priority order based RWTA (POB-RWTA), partial priority-based RWTA (PP-RWTA), and secret key assignment priority ordering policy with longest route first (SKA-POP-LRF), and the effectiveness of the proposed SKA-POP is examined in terms of success probability *(SP)* and probability of secret key update failure *(P_{SKUF})*.

Fragmentation is one of the most important and serious issues of QKD-ONs during assignment and reassignment. It can be reduced by appropriate management of network resources in order to increase the accommodation of number of QKD-LPRs. The impact of fragmentation in QSCh of QKD-ON is analyzed and the problem of time slot fragmentation is addressed in this thesis. Furthermore, in order to minimize the effect of fragmentation during assignment and reassignment in QSCh of QKD-ONs, a fragmentation-suppressed routing and resource assignment (FS-RRA) approach is proposed. The effect of fragmentation in QSCh is analyzed using two existing resource assignment approaches and a proposed FS-RRA approach in terms of the QSCh fragmentation index *(FI_{QSCh})*, the external fragmentation *($FM_{external}$)*, blocking probability *(BP)*, and resource utilization *(RU)* under two different sizes of network, namely, NSFNET and UBN24. Simulation results indicate that the proposed FS-RRA approach performs better than the other two existing resource assignment approaches.

Inspired by the recent advances in deep reinforcement learning (DRL) for solving complex problems, and because of its capability to learn directly from previous experiences, the DRL method is exploited to solve the RRA problem. The RRA problem of QKD-ONs is a complex decision making problem, where appropriate solutions depend on understanding the networking environment. A DRL-based RRA scheme is proposed, which learns the optimal policy to select an appropriate route and assigns suitable network resources for establishment of QKD-LPRs by using deep neural networks (DNNs). The performance of the proposed scheme is compared with deep-Q network (DQN) method and two baseline schemes, namely, first-fit (FF) and random-fit (RF) for two different networks. Simulation results indicate that the proposed DRL-based RRA scheme considerably outperforms the DQN and the two baseline schemes in terms of both *BP* and *RU*. Moreover, the choice of routing strategy during RRA will depend on factors such as network size, available

resources, and specific security objectives. Therefore, to address the routing part of RRA problem, a DRL-based routing scheme is proposed in QKD-ONs that considers various networking factors while making optimal routing decisions. This thesis raised interest towards addressing the different networking challenges of QKD-ONs and enhancing security of existing and future optical networks using quantum-based technology.

Contents

List of Figures

List of Tables

List of Acronyms

AES Advanced encryption standard.

AG-RWTA Auxiliary graph based-RWTA.

AI Artificial intelligence.

API Application program interface.

B92 protocol Bennett-92 protocol.

BB84 protocol Bennett and Brassard-84 protocol.

BBM92 protocol Bennett Brassard Meermin-92 protocol.

BFT Byzantine fault tolerance.

BP Blocking probability.

Bps Bit per second.

C-band Conventional band.

CAPEX Capital expenditure.

CCh Control channel.

CoQKD-LPR Categories of QKD lightpath request.

COW protocol Coherent one-way protocol.

CV-QKD protocol Continuous-variable QKD protocol.

D Diagonal.

DARPA Defense Advanced Research Project Agency.

DCh Data channel.

DCNs Data communication nodes.

DL Deep learning.

DNNs Deep neural networks.

DPR-QKD protocol Distributed-reference QKD protocol.

DPS protocol Differential phase shift protocol.

DQN Deep-Q networks.

DRL Deep reinforcement learning.

DRL-based RRA Deep reinforcement learning based routing and resource assignment.

DSKRT-SM Distributed subkey-relay-tree based secure multicast.

DSKRT-RKA Distributed subkey-relay-tree-based secure multicast-routing and key assignment.

DV-QKD protocol Discrete-variable QKD protocol.

DWDM Dense wavelength division multiplexing.

E91 protocol Ekert-91 protocol.

EB scheme Entanglement based scheme.

EONs Elastic optical networks.

ETSI European Telecommunications Standards Institute.

ETSI ISG-QKD ETSI Industry Specification Group on QKD.

FF First fit.

$\mathbf{FI_{QSCh}}$ QSCh fragmentation index.

$\mathbf{FM_{external}}$ External fragmentation metric.

FS-RRA Fragmentation suppressed routing and resource assignment.

H Horizontal.

HPQKD-LPRs High priority QKD lightpath requests.

IEEE Institute of Electrical and Electronics Engineers.

IETF/IRTF Internet Engineering Task Force/Internet Research Task Force.

ILP Integer linear programming.

IM Intensity modulator.

ISG Industry Specification Group.

ISO/IEC International Organization for Standardization/International Electrotechnical Commission.

ITU International Telecommunication Union.

ITU-T SG 17 ITU-T Study Group 17.

ITU-T SG 13 ITU-T Study Group 13.

ITU-T International Telecommunication Union-Telecommunications.

JTC Joint Technical Committee.

KaaS Key as a service.

Km Kilometer.

KoD Key on demand.

KP Key pool.

KRT-RKA Key-relay-tree-based routing and key assignment.

LP Lightpath.

LPQKD-LPRs Low priority QKD lightpath requests.

Mbps Megabits per second.

MDI-QKD Measurement-device-independent QKD.

ML Machine learning.

MPQKD-LPRs Moderate priority QKD lightpath requests.

MQON Metro-quantum optical networks.

MRN Multi relay node.

MTKA Multi-tenant key assignment.

MTP Multi-tenant provisioning.

NETCONF protocol Network configuration protocol.

NGNs Next-generation networks.

NP-RWTA Non priority order based routing, wavelength and time slot assignment.

O-band Original band.

Off-MTP Offline multi-tenant provisioning.

OFP OpenFlow protocol.

On-MTP Online multi-tenant provisioning.

OTDM Optical time division multiplexing.

P_{SKUF} Probability of secret key update failure.

P&M Prepare and measure.

PF Polarization filter.

PICh Public interaction channel.

PIN photo-diode Positive-intrinsic-negative photo-diode.

PNS Photon number splitting.

POB-RWTA Priority order based routing, wavelength and time slot assignment.

PP-RWTA Partial-priority based routing, wavelength and time slot assignment.

PPO Proximal policy optimization.

QaaS QKD as a service.

QB Quantum block.

QBER Quantum bit error rate.

QCNs Quantum communication nodes.

QD Quantum detector.

QKD Quantum key distribution.

QKD-LPRs QKD secured lightpath requests.

QKD-ONs Quantum key distribution-secured optical networks.

QKDN Quantum key distribution network.

QKPs Quantum key pools.

QKS Quantum secret key server.

QL Quantum link.

QSCh Quantum signal channel.

QSS Quantum signal source.

Qubits Quantum bits.

R Rectilinear.

RF Random fit.

RL Reinforcement learning.

RNG Random number generator.

RRA Routing and resource assignment.

RU Resource utilization.

RWA Routing and wavelength assignment.

RWKA Routing wavelength and key assignment.

RWTA Routing wavelength and time slot assignment.

SARG04 protocol Scarani Acin Ribordy Gisin-04 protocol.

SBPP Shared backup path protection.

SDN Software-defined networking.

SDON Software-defined optical network.

SDQaaS Software defined network for QKD as a service.

SECOQC Secure Communication based on Quantum Cryptography.

SKA-POP-LRF Secret key assignment priority ordering policy with longest route first.

SKA-POP Secret key assignment priority ordering policy.

SKFM Secret key flow model.

SKRs Secret key rates.

SKRS Secret key recovery strategy.

SLA Service level agreement.

SPc Control channel security probability.

SPd Data channel security probability.

SRSR Service request security ratio.

SSP protocol Six-state protocol.

TDCh Traditional data channel.

TDM Time division multiplexing.

TF-QKD Twin-field QKD.

TRNs Trusted repeater nodes.

TSW Time sliding window.

TWRM Time window-based recovery method.

UTRNs Untrusted relay nodes.

V Vertical.

VKP Virtual key pool.

VOA Variable optical attenuator.

WDM Wavelength division multiplexing.

WG3 Working group 3.

Chapter 1

Introduction

Quantum key distribution (QKD) has emerged as a solution to provide security for the future optical communication networks. Conventional encryption methods enable security against cyber attacks using public-key cryptography [13, 14]. However, the level of security achieved by such methods is based on the computational complexity of the employed mathematical functions. With the development of faster processing chips, it is becoming easier to compromise the security offered by public-key cryptography. Moreover, the evolution of quantum computers [15–21] necessitates the need for QKD to secure the information transmitted over communication networks since the existing encryption methods will not be able to provide security in the era of quantum computing [8, 22, 23].

QKD is based on the fundamental principles of quantum mechanics, namely, the Heisenberg's uncertainty principle and the quantum no-cloning theorem [24–26]. Heisenberg's uncertainty principle states that it is not possible to accurately measure a pair of conjugate properties, i.e., the position and momentum of an object simultaneously [27–29]. Quantum no-cloning theorem states that it is not possible to exactly replicate the arbitrary unknown quantum states carried by the particles such as photons [1, 30–33]. The uncertainty principle and the no-cloning theorem imply that a quantum bit (qubit) cannot be copied and any attempt of copying it can be detected by the sender (referred to as "Alice"), and the receiver (referred to

as "Bob"). QKD generates and distributes secret keys between the sender and the receiver [25, 34]. The generated random secret keys can then be used to encrypt and decrypt the classical data using the conventional encryption algorithms [35] such as one-time pad [36] and advanced encryption standards (AES) [37].

In 1984, Charles H. Bennett and Gilles Brassard developed the first QKD protocol, known as the Bennett and Brassard-84 (BB84) protocol [5, 24], and subsequently, various other QKD protocols were proposed over the years [38–46]. The schemes and families of QKD protocols are described in Section 1.1.2(1.1.2.2) along with a detailed description of the first as well as the most widely used BB84 protocol. Most of the QKD protocols employ single-photon sources and detectors for secret key generation and detection. Since the single-photon sources and detectors are still under development, implementation of QKD has been widely done using weak coherent light sources. However, such devices are imperfect for the implementation of QKD and may cause security loopholes in the system, thereby making the QKD system insecure [47–49]. Thus, to protect the QKD systems from such imperfections, new QKD protocols, namely, the decoy-state QKD protocol [50–52] and the measurement-device independent QKD (MDI-QKD) protocol [7, 53, 54] have been proposed.

QKD can be realized over both the free-space [55–57] and the optical fiber [58–60] media. This thesis focuses on the optical fiber networks secured by QKD. Optical fiber has been usually considered as a secure mode of transmission due to propagation of optical signals inside the guided medium, however, the increasing incidents of lightpath attacks including jamming, eavesdropping, data interception, among others [61–63] motivated the research and development of QKD secured optical fiber communication.

This chapter aims to cover all the relevant aspects of QKD-secured optical networks (QKD-ONs) including the motivation behind the necessity of QKD-ONs. Thus, the important terminologies and concepts of QKD are described first, such as qubits, a basic QKD system, types of attacks in QKD systems, and different

QKD protocols (with a detailed description of BB84 protocol since we use it later to explain the process of QKD-ONs) to develop a basic understanding. However, the readers interested in others important aspects of QKD such as device level research and protocol-specific studies are encouraged to refer to the corresponding literature. The point-to-point QKD over fiber system; architecture of mesh connected QKD-ONs; important networking challenges in QKD-ONs and the existing methods to solve them are described next. Furthermore, some of the most relevant challenges and crucial research aspects addressed in this thesis related to QKD-ONs are highlighted.

1.1 Quantum Key Distribution: Overview

This section gives an overview of QKD including qubits and its representation, and a basic yet complete QKD system. Subsequently, this section describes the underlying QKD process using the BB84 protocol, the schemes for designing QKD protocols, and the quantum hacking attacks along with the method of prevention.

1.1.1 Quantum Bits

A classical bit is the basic entity of the classical computation and information systems. Similarly, a qubit coined by Benjamin Schumacher [64] is the basic entity of the quantum information and quantum computation systems [1].

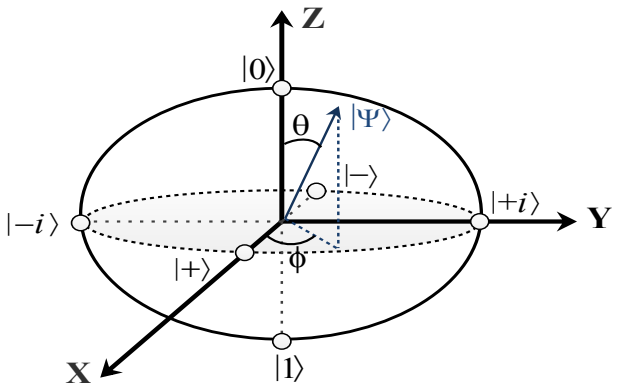


Figure 1.1: Bloch Sphere [1, 2]

.

In a classical system, a bit can be in two states, i.e., 0 or 1. In quantum systems, a qubit has two basis states, represented as $|0\rangle$ or $|1\rangle$, where $|\rangle$ is Dirac or bra-ket notation [1, 65]. However, a qubit can be in a quantum superposition of the basis states $|0\rangle$ and $|1\rangle$ simultaneously [17, 20, 66], which is the key difference between a classical bit and a qubit. Bloch sphere is used to graphically represent the possible quantum states of a qubit, as shown in Figure 1.1 [1]. Figure 1.2 shows the vector representation of the classical bit and the qubit. The representation of qubit states depends on the computational basis. Some examples of qubit states $|\psi\rangle$ in the Bloch sphere are $|0\rangle$, $|1\rangle$, $|+\rangle$, $|-\rangle$, $|+i\rangle$, and $|-i\rangle$.

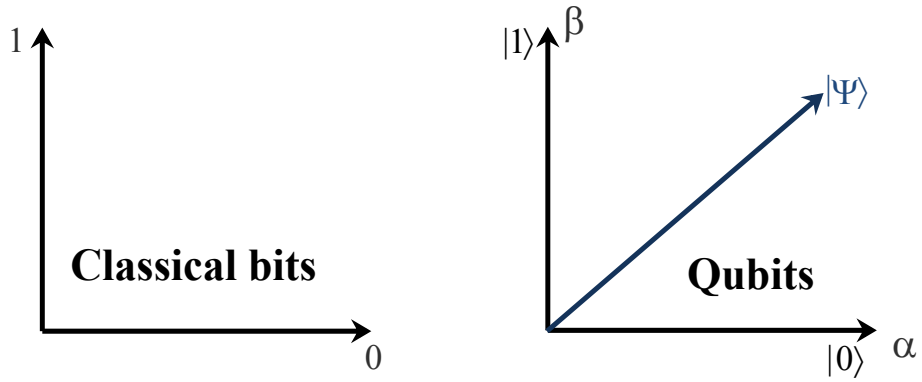


Figure 1.2: Vector representation of classical bit and qubit.

1.1.2 Basic QKD System

This subsection describes a basic QKD system, QKD protocols, and the process of QKD system using BB84 protocol.

1.1.2.1 Components of Basic QKD System and their Functionalities

A QKD system requires two types of channels, viz. quantum signal channel (QSCh) [67] and publich interaction channel (PICh); a QKD protocol; and encryption/ decryption blocks, as shown in Figure 1.3.

- QSCh is used to send the quantum states of light (photons) between the nodes, i.e., Alice and Bob.

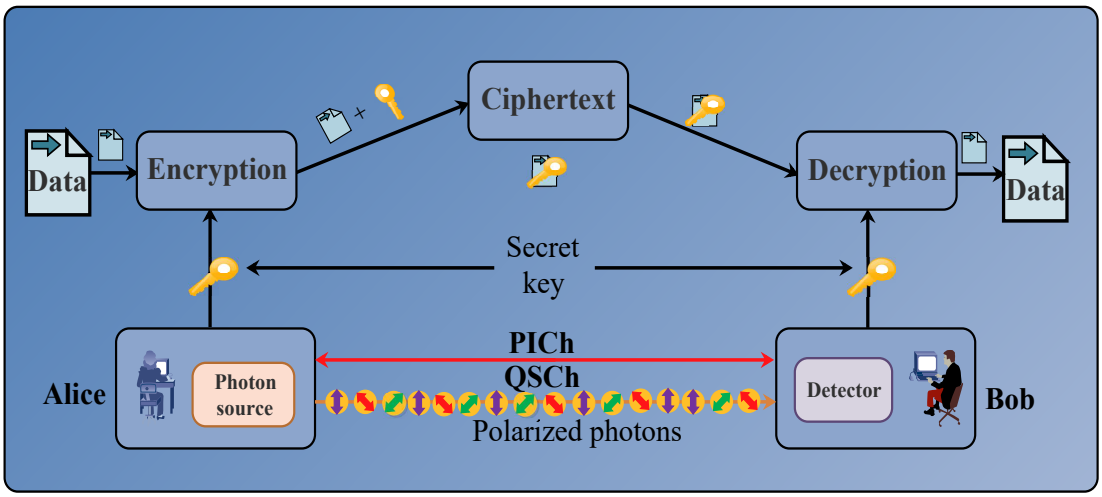


Figure 1.3: Basic QKD system [3].

- PICh is used to transmit the measuring-basis of qubits, and to verify the generated shared secret keys using the post-processing methods [68]. After post-processing, a final random secret key is generated between Alice and Bob.

- A QKD protocol [69] is used in QKD to establish secure connection between Alice and Bob. It generates secret keys and also analyzes the amount of correct information shared between the users during the key generation.

- The encryption and decryption blocks are required to encrypt the information using the secret keys and then to decrypt it back.

1.1.2.2 QKD Protocols

(a) Schemes of QKD Protocols: The two main schemes used to design QKD protocols are Prepare and Measure (P&M) scheme, and Entanglement-Based (EB) scheme [13, 69, 70].

(1) Prepare and Measure Scheme: In the P&M scheme, Alice *prepares* the information in the form of polarized photons and then sends that information to Bob, which is then *measured* by Bob [69, 70], as shown in Figure 1.4. The process of P&M scheme is described in detail in Section 1.1.3(1.1.3.1) using BB84 protocol. The P&M scheme is based on two fundamental laws of quantum mechanics, namely,

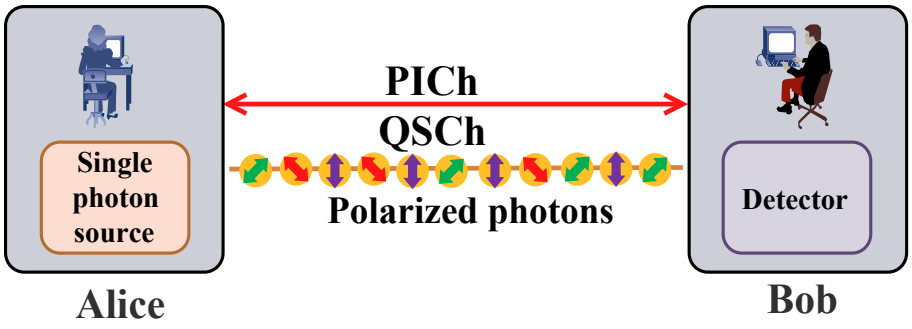


Figure 1.4: Concept of prepare and measure scheme [3].

the Heisenberg's uncertainty principle and the quantum no-cloning theorem [3]. Some of the QKD protocols based on this scheme are BB84 [24], Bennett-92 (B92) [39], Six-State protocol (SSP) [41, 42], Scarani Acin Ribordy Gisin-04 (SARG04) [43], Differential Phase Shift (DPS) [45, 46], and others [7, 71].

(2) Entanglement-Based Scheme: In the EB scheme, a source generates entangled pairs of photons, i.e., the entangled quantum states, and sends them to Alice and Bob [4], as shown in Figure 1.5. Alice and Bob then measure the received quantum states. In this scheme, the quantum states of both the sender and receiver are associated in such a way that the measurement on one affects the other, and both can easily detect any attempt of eavesdropping [70]. The QKD protocols based on this scheme are Ekert-91 (E91) [38] and Bennett Brassard Meermin-92 (BBM92) [40].

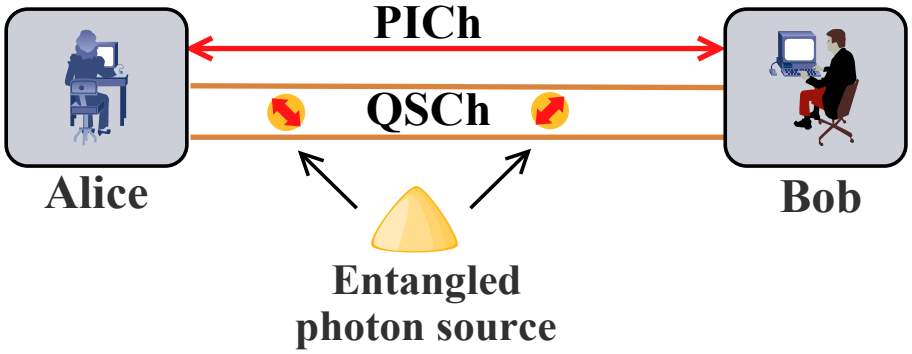


Figure 1.5: Concept of entanglement-based scheme [4].

(b) Families of QKD Protocols: The QKD protocols belong to one of the following three families, namely, discrete variable (DV)-QKD protocols, continuous-variable (CV)-QKD protocols, and distributed-phase-reference (DPR)-QKD proto-

cols [69].

(1) Discrete-Variable QKD Protocols: The DV-QKD protocols generate secret keys between Alice and Bob by using the polarization states of photon or phase to encode the bits. Such protocols utilize the photon counting and post-processing methods for the detection of individual photons to generate the secret keys [69]. The first protocol of this family is the BB84 protocol [24].

(2) Continuous-Variable QKD Protocols: About fifteen years after implementation of the first DV-QKD protocol, an alternative approach, namely, the continuous-variable coding, was introduced by Ralph for secure data transmission [44]. DV-QKD protocols require single photon sources and detectors for implementation. However, CV-QKD protocol uses standard telecommunication devices, such as positive-intrinsic-negative (PIN) photo-diode. The major difference between the DV-QKD and CV-QKD protocol lies in their detection method. CV-QKD protocols replaced the photon counting approach of discrete-variable coding with a coherent detection method, i.e., homodyne detection, which is highly efficient, cost-effective, and fast. The first squeezed state category of BB84 protocol [72–74] with the discrete and Gaussian modulation was implemented by Hillery [72] and Cerf et al. [73], respectively. Later, experimental demonstrations of various CV-QKD protocols were done to check the practicality of these protocols with the coherent states of light [75–81].

(3) Distributed-Phase Reference QKD Protocols: The QKD protocols of this family include DPS-QKD [45, 46, 82] and coherent-one way (COW) protocol [69, 71] which have been developed recently. In DPR-QKD protocols, a sequence of coherent states of weak laser pulses is transmitted from Alice to Bob. In the DPS-QKD protocol, the intensity of the pulses is same; however, their phases modulate. In COW protocol, the phases of all the pulses are same; however, their intensities vary. Table 1.1 summarizes all the aforementioned QKD protocols.

Table 1.1: Summary of QKD Protocols

Protocol Family	Name and Year of Protocol	Protocol Scheme	Principle	Unique Feature	Innovators and References
DV-QKD	BB84 (1984)	P & M	Heisenberg's uncertainty principle	The first quantum cryptography protocol, uses four polarization states of photon	C. H. Bennett and G. Brassard [24]
	E91 (1991)	EB	Quantum entanglement	The first QKD protocol based on the principle of quantum entanglement	A. Ekert [38]
	B92 (1992)	P & M	Heisenberg's uncertainty principle	Identical to the BB84, however, it uses only two non-orthogonal states	C. H. Bennett [39]
	BBM92 (1992)	EB	Quantum entanglement	The BBM92 protocol is the entangled version of BB84 protocol	C. H. Bennett, G. Brassard, and N. D. Mermin [40]
	SSP (1998 & 1999)	P & M	Heisenberg's uncertainty principle	This protocol uses higher number of polarization states of photon (i.e., six) as compared to the BB84 protocol	D. Bruß [41] and H.B-Pasquinucci and N. Gisin[42]
	SARG04 (2004)	P & M	Heisenberg's uncertainty principle	Only the classical phase of SARG04 is different than the BB84 protocol	V. Scarani, A. Acin, G. Ribordy, and N. Gisin [43]
CV-QKD	Discrete modulation protocol (Squeezed-state BB84 (2000))	P & M	Heisenberg's uncertainty principle	A new version of BB84 protocol with the squeezed-state and discrete modulation	M. Hillery [72]
	Gaussian protocol (Squeezed-state BB84 (2001))	P & M	Heisenberg's uncertainty principle	The squeezed-state based BB84 protocol with the Gaussian modulation	N. J. Cerf, M. Levy, G. Van Assche [73]
DPR-QKD	DPS (2003)	P & M	Heisenberg's uncertainty principle	The first DPR based QKD protocol that uses weak coherent sources, and one bit delay circuit to generate, and measure qubits, respectively	K. Inoue, E. Waks, and Y. Yamamoto [45, 46]
	COW (2004)	P & M	Heisenberg's uncertainty principle	The COW protocol uses weak coherent pulses for photon generation and each bit is encoded in a sequence of one non-empty (μ)-pulses (containing the mean number of photons) and one empty (0)-pulses	N. Gisin, G. Ribordy, H. Zbinden, D. Stucki, N. Burnner, and V. Scarani [71]

1.1.3 Basic Process of QKD System

Figure 1.3 shows the components of a QKD system [3] and the process of secure information exchange, as described below.

- A secret key is generated and shared between the Alice and the Bob using a QKD protocol. The process of secret key generation using BB84 protocol is described below.
- After secret key generation, the encryption block encrypts information using some conventional encryption algorithms [3, 36, 37]. The encrypted information is known as ciphertext, which is then transmitted by Alice.
- Bob uses the same secret key to decrypt the ciphertext to recover the original information, i.e., convert the ciphertext into plaintext [35].

1.1.3.1 Process of secret key generation using BB84 Protocol

The BB84 protocol [5, 24] is based on the basic principles of quantum mechanics and is provably secure. For the generation of photons, the BB84 protocol uses pulses of polarized light, where each pulse contains single photon. Single photon is generated by using a single-photon source which reduces the adverse effects of photon number splitting (PNS) attack [83–85]. The BB84 protocol uses two bases, namely, a rectilinear basis (R) with two polarization states of photons (0° and 90°) and a diagonal basis (D) with two polarization states of photons (45° and 135°), as shown in Figure 1.6.

Figure 1.7 shows the bit encoding in BB84 protocol according to the original BB84 protocol proposed in [24]. Here, binary 0 is represented by 0° or horizontal (H) polarization state in R or a 45° polarization state in D. Similarly, binary 1 is represented by a 90° or vertical (V) polarization state in R or 135° polarization state in D [5]. Table 1.2 shows the polarization bases, polarization states, and bit encoding in the BB84 protocol.

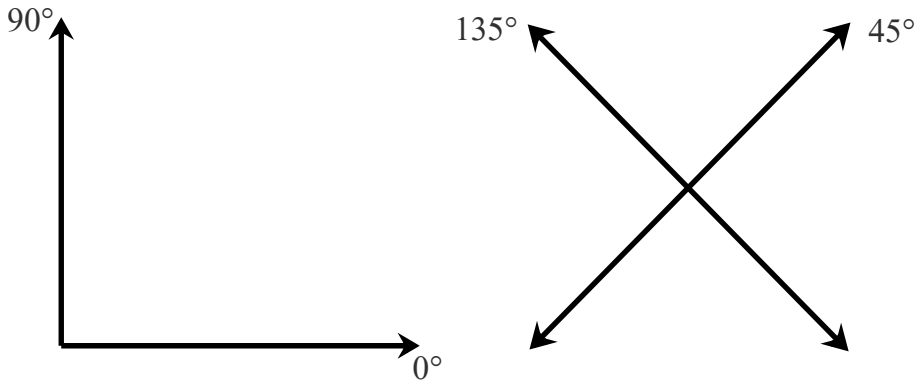


Figure 1.6: Photon polarization states in BB84 protocol (R&D bases) [5].

Table 1.2: Polarization bases, states, and bit encoding in BB84 protocol [5]

Polarization basis	Polarization state	Bit Encoding
Rectilinear (+)	0° or H	Binary 0
	90° or V	Binary 1
Diagonal (×)	45°	Binary 0
	135°	Binary 1

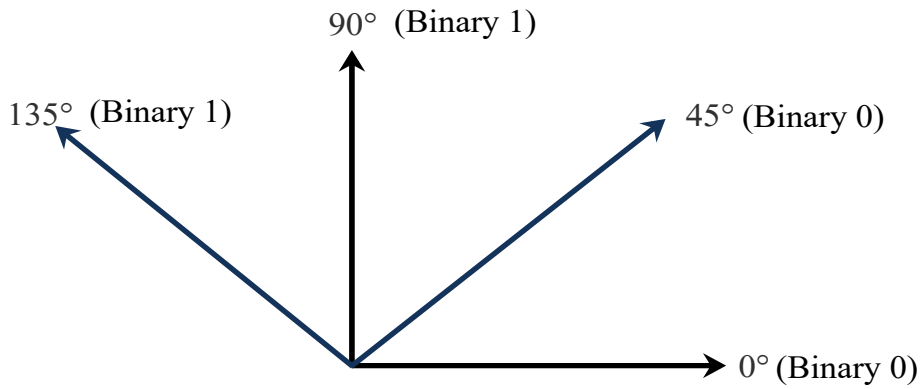


Figure 1.7: Bit encoding in BB84 protocol [5].

The process of a QKD system is explained in the following phases below. Table 1.3 describes the operations involved in different phases with an example as discussed in [5, 24]:

Table 1.3: Example of BB84 protocol process [5]

Alice's random bits	1	1	0	1	0	0	1	1	0	1	0	0
Alice's measuring bases	+	×	×	+	+	×	+	×	×	+	+	×
Photon polarization states	V	135°	45°	V	H	45°	V	135°	45°	V	H	45°
Bob's measuring bases	+	+	+	+	+	×	+	+	×	×	+	×
Bob's bits (Raw key)	1	0	0	1	0	0	1		0		0	0
Bob send his measuring bases to Alice	+	+	+	+	+	×	+		×		+	×
Alice confirm the measuring bases	T	F	F	T	T	T	T		T		T	T
Sifted key	1			1	0	0	1		0		0	0
Bob reveals some bits at random				1		0						
Alice confirm the bits				OK		OK						
Secret key	1				0		1		0		0	0

- Quantum Phase: In the quantum phase, Alice communicates with Bob over the quantum channel in the following steps [70]:
  - Alice generates a random string of bits, and for each bit, she choose a measuring basis randomly, either R or D. The random string of bits along with the polarization states, i.e., the string of qubits is then sent to Bob through the quantum channel.
  - Bob also chooses a measuring basis randomly for each of the received qubit, and using the chosen basis, it starts to measure the received bits. For a bit, if the measuring bases of Alice and Bob match, it results in a perfectly correlated result, otherwise, an uncorrelated result. Sometimes,

due to errors in detection and/or transmission, Bob does not register anything (as shown by blank entry from 5^{th} row onwards in Table 1.3).

  - After measurement of all the bits, Bob records a string of all the received bits, called as *Raw key (K_{raw})* [25].

- Classical Phase: In the classical phase, Alice communicates with Bob over the classical channel to extract secret keys from the measurement results. The secret key extraction process, as shown in Figure 1.8 involves of the following steps [35, 68, 86]:

  - Sifting: In this step, Alice and Bob exchange the information related to the sent/received photons over the classical channel. The random measuring bases chosen by Alice and Bob are compared: the bits corresponding to the same bases are kept, and the bits corresponding to different measuring bases are discarded. The remaining string of bits is known as the *sifted key (K_{sifted})* [10, 25].

  - Error estimation: In order to avoid eavesdropping, Alice and Bob decide a threshold value of quantum bit error rate ($QBER_{th}$), when there is no eavesdropper (Eve) on the communication medium. $QBER$ is the ratio of the probability of getting wrong detection to the total probability of detection. Based on that value, they compare a random subset of K_{sifted} bits and calculate the estimated $QBER_{est}$. If $QBER_{est} > QBER_{th}$, the process is terminated and restarted, otherwise continued. [3, 86].

  - Error reconciliation or error correction: This step is used to further remove any chance of error occurred during the sifting process. Different methods of error reconciliation are used to enhance the capability of error correction in the QKD protocols [70]. After this process, the generated key is known as *corrected key ($K_{corrected}$)*.

  - Privacy amplification: Privacy amplification is an important step in this phase, which reduces the information of secret key to a negligible amount

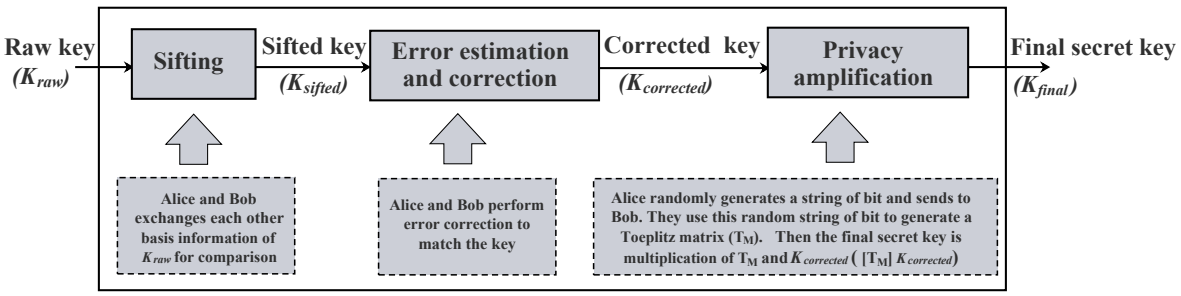


Figure 1.8: Post-processing procedure.

against an unauthenticated user and produces a new shorter key using the universal hash functions. The generated final key is known as the *Secret key* (K_{final}) [68, 86]. Additionally, an authentication process is required to ensure safety of the generated secret key from eavesdropping [25].

- Encryption Phase: In this phase, the generated secret key is then used for encryption and decryption of sensitive information between two legitimate end-users. This phase utilizes the one-time pad encryption [36] and symmetric encryption algorithm, i.e., AES [37] to encrypt and decrypt the data, and establish secure communication between the end-users [3, 87].

1.1.4 Quantum Hacking Attacks and its Prevention

In this subsection, some of the significant and vulnerable quantum hacking attacks or side-channel attacks at both the source and detector sides are discussed [83, 88, 89]. These attacks can be made in the QKD systems during the secret key generation. The security of QKD systems can be affected by such attacks if the devices at user-ends are imperfect. The practically realizable methods to prevent QKD protocols [7, 50] from side-channels attacks are also discussed.

1.1.4.1 Source Side Attack and its Prevention

(a) Source side attack: BB84 protocol has been widely used to generate secret keys for practical QKD systems, however, this QKD protocol uses single-photon

devices (source/detector) at the sender and the receiver side [70]. In practice, it is difficult to design a perfect single-photon transmitter or receiver. Thus, due to device imperfections, side-channel attacks can affect the QKD systems [47, 49]. The most vulnerable attack at the source side is the PNS attack [6, 83]. The PNS attack occurs due to the use of a weak coherent source instead of a single-photon source [90]. For example, when Alice sends single photon to Bob, multiple photons get transmitted instead of single photon due to device imperfections. In the PNS attack, the eavesdropper first measures the number of photons of each transmitted pulse. When s/he notices that multiple photons are being transmitted simultaneously, s/he splits the photons, otherwise, s/he blocks the transmitted pulse. After splitting the photons, the eavesdropper stores one photon and pass the other photons to the Bob via a lossless channel, as shown in Figure 1.9. In order to get the complete information of secret key, the eavesdropper listens to the PICh for Alice's and Bob's bases announcement. Once eavesdropper knows the Alice's and Bob's information related to basis measurement, s/he can get the complete information of the secret key by measuring each of the stored photons in the correct measurement basis. In this way, the eavesdropper can perform the PNS attack, without letting either of the Alice or the Bob realizing the attack.

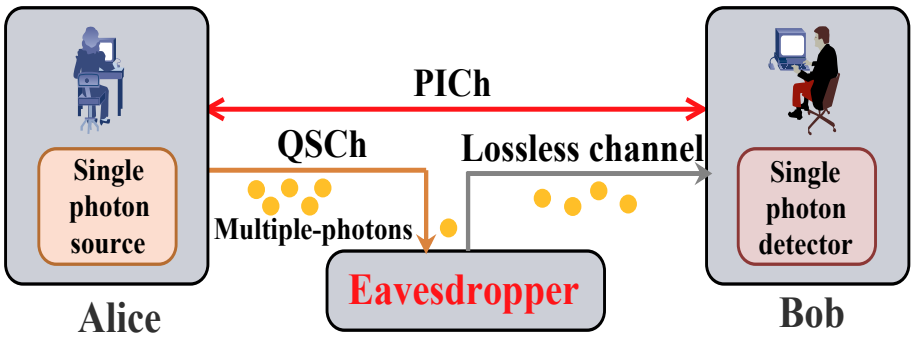


Figure 1.9: PNS attack [6].

(b) Decoy-State QKD method: To prevent the QKD systems from the PNS attacks, a decoy-state method was proposed [50]. This method allows the use of weak laser sources by creating the additional states, known as the decoy states, in

place of single-photon sources. In the decoy-state method [6, 48, 91, 92], the sender chooses the intensity for every transmitted pulse at random from a set of available intensities, and reduces the effect of multi-photon transmission (PNS attack). Out of all the available intensities, one corresponds to the signal states (used for secret key generation) and the rest to the decoy states (having different intensity levels than main signal) [35, 51, 52, 93, 94]. After the announcement of Bob that he has received all the transmitted pulses, Alice announces the intensity level used for each transmitted pulse and estimates the *QBER* and yield (it is the conditional probability that the signal will be detected by Bob (the receiver), given that Alice (the sender) transmits it) of decoy states. By monitoring the *QBER* and yield, Alice and Bob can detect the presence of a PNS attack. The decoy states can be created by using variable optical attenuator (VOA) and intensity modulator (IM) [7], which changes the intensity of signals. The original BB84 protocol [5, 24] integrated with the decoy-state technique is known as the decoy-state BB84 protocol. The first experimental demonstration of decoy-state QKD over a 15 km fiber link achieved a secret key generation rate of 165 bps [91]. Various QKD protocols based on this technique have been experimentally implemented to detect the attacks on the source side [48, 92, 95–98].

1.1.4.2 Detector Side Attacks and its Prevention

(a) Detector side attacks: Decoy-state method [50] secures the source side of the QKD system from the PNS attacks, however, this method cannot be applied at the detector side. Several quantum hacking attacks have been proposed and experimentally demonstrated in [47, 88, 99, 100]. Some of the powerful attacks are the detector blinding attacks [89] and time-shift attacks [88, 101]. In the detector blinding attacks, an eavesdropper sends a bright light at the detector side and forces the detector to enter into the linear operation mode (in which detectors are more sensitive to light). The Eve randomly prepares his/her signal and sends a bright trigger pulse towards the Bob. If the measurement bases of Eve and Bob are same,

then one of the detector produces a *click*, and the Eve can determine which detector produced the *click*. In this way, he/she can know the information of the secret key without any disturbance [89]. Since QKD protocol consists of at least two single-photon detectors for qubit detection, and the detection efficiency of both the detectors are time-dependent, the detectors may not have the same detection efficiency throughout. By taking advantage of this, Eve can shift the arrival time of each pulse and partially gain knowledge of the secret key without any error. Such type of attack is known as the time-shift attack [88, 101].

(b) Measurement-Device-Independent QKD method: Various methods have been proposed to secure the QKD systems against device-imperfection based security loopholes. Some of the methods are slightly complicated [102, 103], and have extremely low key generation rate and transmission reach [104]. Hence, a new MDI-QKD scheme [7] was proposed that removes all the detector side-channel attacks. The initially proposed MDI-QKD relied on the single-photon source, and hence was susceptible the PNS attack [83]. However, the decoy-state method [50] was combined with MDI-QKD to prevent the QKD systems from the imperfect single-photon source based attacks [105, 106]. The idea of decoy-state MDI-QKD has a great importance in the QKD security against all types of device imperfection attacks. Moreover, it improves the transmission distance of quantum signals [54]. In the MDI-QKD method, Alice and Bob (sources) randomly prepare their measurement bases similar to that in the BB84 protocol, and send them to an untrusted node, i.e., Charles (at center) [7], as shown in Figure 1.10. Charles performs measurement test on received bases, and after performing the measurement test, he announces the measurement outcome via the public channel. Alice and Bob keep the information of bits corresponding to the Charles's measurement results and discard the remaining. Charles's measurement results are only used to check the parity of both Alice's and Bob's bits, and it does not provide any information related to his/her bits. Similar to the BB84 protocol, Alice and Bob perform a post-processing operation, i.e., Alice and Bob announce the randomly selected bases and compare them with

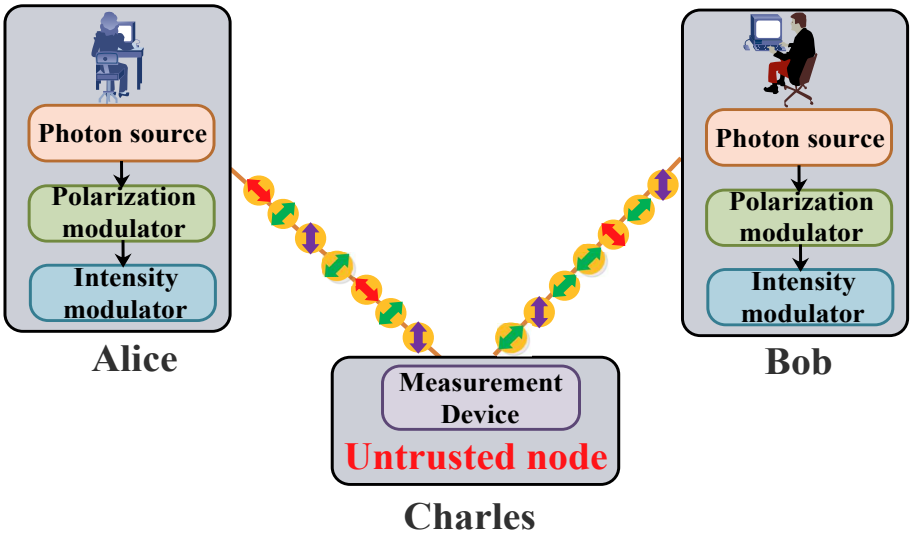


Figure 1.10: Generalized MDI-QKD setup [7].

Charles's measurement outcomes. At the end, either Alice or Bob performs the bit flip operation to achieve a guarantee correlation between the bit strings, and obtain the final secret key [7]. This method is called as MDI-QKD because the detector at the center has no information about the qubits, i.e., he/she does not know the bases and the polarization states used and to which party they belong. The process of MDI-QKD protocol and other aspects related to implementation, key generation rate, etc., are described in detail in [7, 101].

1.2 QKD-Secured Optical Networks

This section discusses the QKD-ONs, the practical demonstration of QKD-ONs, the mechanism of secure communication over a point-to-point [9] optical fiber link using the BB84 QKD protocol, and the basic network architectures of QKD-ONs in detail.

The initial QKD experiments were conducted over separate dark fibers. However, the dark fibers are neither available in abundance to realize quantum communication globally, nor it is cost-effective to deploy a separate global optical network for this purpose. Since optical fibers carry almost all of the global Internet traffic currently, and are deployed widely around the world in the access, metro, terrestrial backbone, and the submarine networks, it is a general consensus to integrate QKD

with the existing optical networks. However, since the quantum signals are weak (consisting of few countable photons per pulse) as compared to the classical signals (consisting of millions of photons per pulse), the coexistence of quantum and classical signals in a common optical fiber is challenging. Moreover, the transmission distance of quantum signals is much lower as compared to the classical signals as they are weak. Furthermore, any interaction between the quantum signals and classical signals might further deteriorate the quality of quantum signals and can also alter the quantum states. Thus, to integrate QKD with the existing optical networks, multiplexing techniques, namely, wavelength division multiplexing (WDM) and time division multiplexing (TDM) have been extensively researched in the recent past to share the available optical bandwidth among the quantum and classical signals. WDM is used to transmit multiple optical signals onto a single fiber using multiple wavelengths, whereas TDM is used to transmit multiple data streams over a common communication channel by separating them into multiple segments, where each independent data stream is demultiplexed at the receiving end in the time domain.

In 1997, Townsend demonstrated the first simultaneous transmission of quantum and classical signals over single fiber using WDM, where original (O)-band (1260-1360 nm) was used for the quantum signals, and conventional (C)-band (1530-1565 nm) for the classical signals [107]. Thus, using WDM in the QKD-ONs, the quantum and classical signals are spaced apart in wavelength, where the optical band used for the quantum signals is referred to as the QSCh, and the optical band used for the transmission of classical signals is referred to as the traditional data channel (TDCh) [8, 34]. Quantum signals are transmitted through the QSCh by using TDM. Besides the QSCh and TDCh, another channel, namely, PICh is also required [34] to transmit the qubit measuring-basis and the information during post-processing between the sender and the receiver [34]. O-band has higher losses as compared to the C-band, hence it restricts the transmission distance of weak quantum signals, and results in lower secret key rate (SKR) [108]. Thus, in the later experiments, all the

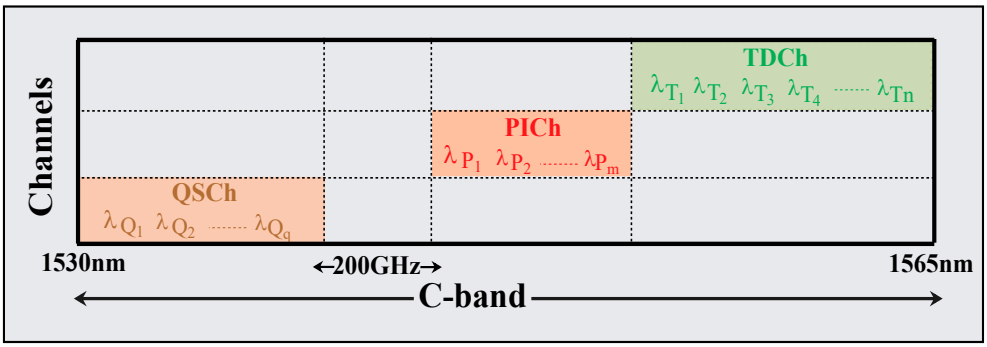


Figure 1.11: Types of channels in QKD-ONs [8].

three types of channels, namely, QSCh, PICh, and TDCh were allocated different wavelengths bands from the C-band, thus bringing the three of them closer. In [109], experimental demonstration of quantum-classical coexistence in C-band was performed using dense WDM (DWDM), where the spacing between the channels was kept as 400 GHz and 800 GHz . This channel spacing is necessary to avoid interaction between the quantum and the classical signals [110, 111]. However, a higher channel spacing results in spectrum wastage. Thus, efforts have been made to further reduce the channel spacing, and an experimental demonstration of quantum-classical coexistence was conducted with 200 GHz channel spacing [60], as shown in Figure 1.11. Several other demonstrations of multiplexing QSCh, PICh, and TDCh in a single fiber have been conducted recently [58, 59, 112–119]. Although several successful demonstrations of quantum-classical coexistence in a single fiber have been conducted for point-to-point links, the QKD-ONs present new challenges to be addressed for practical realization of quantum communication globally over the existing optical networks. Such networking challenges of QKD-ONs, the procedure involved, and detailed explanation of Figure 1.11, i.e., allocation of channels using WDM are given in Section 1.4.

1.2.1 Practical Demonstration of QKD-ONs

Several QKD networks and testbeds have been established in different part of the world to assess their performance in real environment. The world's first quantum cryptography network, namely, Defense Advanced Research Project Agency

(DARPA) quantum network, consisting of 10 nodes was installed between Harvard University, Boston University, and BBN [120, 121]. The European project for Secure Communication based on Quantum Cryptography (SECOQC) combined several QKD systems into a single QKD network considering trusted repeater architecture for long-distance communication in Vienna in 2008 [122]. A QKD network has been established in Tokyo by different organizations of Japan and Europe [123] in 2010. Various long-term performance analyses of QKD networks over the existing regional optical networks have been conducted, namely, the SwissQuantum in Geneva [124] that uses trusted repeaters, the Durban network in South Africa [125], and the Cambridge quantum network [126]. A metropolitan quantum network was demonstrated in Wuhu, China [127]. In 2017, a 2000 km quantum link (QL) was established in China, connecting four cities, namely, Beijing, Shanghai, Jinan, and Hefei [128–130]. Based on the developed technology of quantum-classical signal coexistence, a few companies [131–134] currently provide dedicated QKD services to governments, enterprises, and industrial customers for protection of critical data in transit; and QKD equipments to the research labs. Technological advancements and progress have been made since the beginning of the DARPA quantum network in 2002, and the methods used and the processes involved in the practical QKD testbeds and experiments, such as, key establishment, resource assignment, trusted and untrusted repetition for long-distance communication, among others, are summarized in Section 1.4. Moreover, major practical QKD systems involving the optical networking concepts described in Section 1.3 and 1.4, are summarized in Table 1.4.

1.2.2 Standardization Activities on QKD Systems and Networks

Standardization efforts on QKD systems and networks are also in progress by organizations such as International Telecommunication Union (ITU), European Telecommunications Standards Institute (ETSI), International Organization for Standard-

Table 1.4: Summary of practical demonstrations of QKD secured optical networks

Year and Ref.	Description
2005, [120]	Reports the status of the world's first quantum cryptography network supported by US DARPA
2009, [122]	Describes the SECOQC prototype of QKD network considering trusted repeater architecture for long-distance communication in Vienna in 2008
2009, [135]	Reports a practical realization of metropolitan QKD network without trusted repeater nodes (TRNs) in Beijing
2009, [127]	Demonstrates a user-oriented hierarchical quantum network based on technique of TRN in Wuhu, China
2010, [136]	A metropolitan all-pass quantum communication network was successfully demonstrated in 2009 in China
2010, [137] and 2018, [112]	The successful demostration of the co-existence of quantum signal and classical signal using WDM in different cities in China
2010, [125]	A long-term performance analyses of QKD network over the existing regional optical network was conducted in the Durban in South Africa
2011, [124]	Reports the performance of SwissQuantum QKD network in the field environment in Geneva over a metropolitan area
2011, [123]	Demonstration of the quantum secure communication network in Tokyo by integrating six different QKD system into a mesh network
2014, [138]	A successful demonstration of wide area QKD network was conducted for more than 5000 hours from 2011 to 2012 in three cities, namely, Hefei-Chaohu-Wuhu, in China
2016, [53]	Demonstrates a MDI-QKD network in real field environment with three user nodes and one Untrusted relay node (UTRN)
2016, [54]	Demonstrates the MDI-QKD with decoy-state technique over ultra-low fiber link of 404 km with key rate of 3.2×10^{-4} bps
2016, [139]	The first commercial QKD network in South Korea was deployed in 2016
2016, [128], 2018, [26], and 2019,[140]	China started to build a longest QKD network over a distance of 2000km from Beijing to Shanghai in 2013 and successful established in 2018
2018, [59]	Experimental demonstration of longest conventional QKD over ultra-low loss fiber achieve 421 km with a secret key rate of 0.25 bps
2018, [141]	A TF(Twin field)-QKD scheme was designed and experimentally demonstrated to solve the rate-distance problem of secure QKD network

ization/International Electrotechnical Commission (ISO/IEC), Institute of Electrical and Electronics Engineers (IEEE) and Internet Engineering Task Force/Internet Research Task Force (IETF/IRTF) [142]. Standardization of QKD systems and networks is essential to facilitate interoperability of QKD devices in a multi-vendor environment that will make it possible to integrate QKD technology with the communication networks. Documentation related to QKD standards have been released by different standards developing organizations, and some more are still in progress. The ITU-Telecommunications (ITU-T) Study Group 13 (ITU-T SG 13) "Future Networks" [143] is focusing on next-generation networks (NGNs), network aspects of mobile telecommunications, and standardization of QKD networks (QKDN) and

have published majority of its standards on QKD in the Y-series of ITU-T recommendations. The ITU-T Y.3800-Y.3804 recommendations cover overview of networks supporting QKD; functional requirements and architecture; key management, quality of service aspect; and control and management [144]. The ITU-T Study Group 17 (ITU-T SG 17) "Security" [145] is working on standardization in quantum network security and published its standards in the X-series of ITU-T recommendations. This recommendation series include security considerations [146], security framework, key combination and confidential key supply for QKD networks.

An Industry Specification Group (ISG) on QKD for users at ETSI (ETSI ISG-QKD) [147] is working on various industry specifications and have published several group specification documents on QKD (ETSI GS QKD), such as internal and application interfaces, module security specification, optical characterization of QKD components and QKD system, implementation of security requirements, and a control interface for software-defined networks [148]. A working group-WG3 "Security Evaluation, Testing, and Specification" of ISO and IEC (ISO/IEC Joint Technical Committee (JTC) 1/SC27) is focusing on security requirements, test, and evaluation methods for QKD and have proposed standards for improving the design and implementation security of different QKD devices and evaluating the security of QKD modules [142, 146]. The IEEE P1913 draft standard [149] enables dynamic addition, modification, and removal of quantum protocols or applications by configuring quantum devices in communication networks. In IEEE P1913, a YANG model is presented, whose QKD module, when applied to devices in a communication network, can capture the information such as transceiver rates, QKD protocol, and other QKD-specific characteristics. Although several standardization efforts are ongoing worldwide, consideration of parallel technological advancements in the classical and quantum communication technologies, and harmonization among different standardization organizations is essential to avoid possible contradictions in the standards being published by them.

1.2.3 Point-to-Point QKD System over an Optical Fiber Link

This subsection describes the mechanism of secure communication over a point-to-point [9] optical fiber link using the BB84 QKD protocol. A basic point-to-point mechanism of QKD over optical fiber is shown in Figure 1.12, as described in [8]. Here, Alice's lab consists of a quantum transmitter (quantum signal source (QSS), random number generator (RNG), and polarization filter (PF)) and Bob's lab consists of a quantum receiver (quantum detector (QD), RNG, and PF) [8]. QKD systems consist of various other components and the selection of such components depends on the QKD protocols being used. The steps involved in establishing secure communication between Alice and Bob in Figure 1.12 are described as follows [34]:

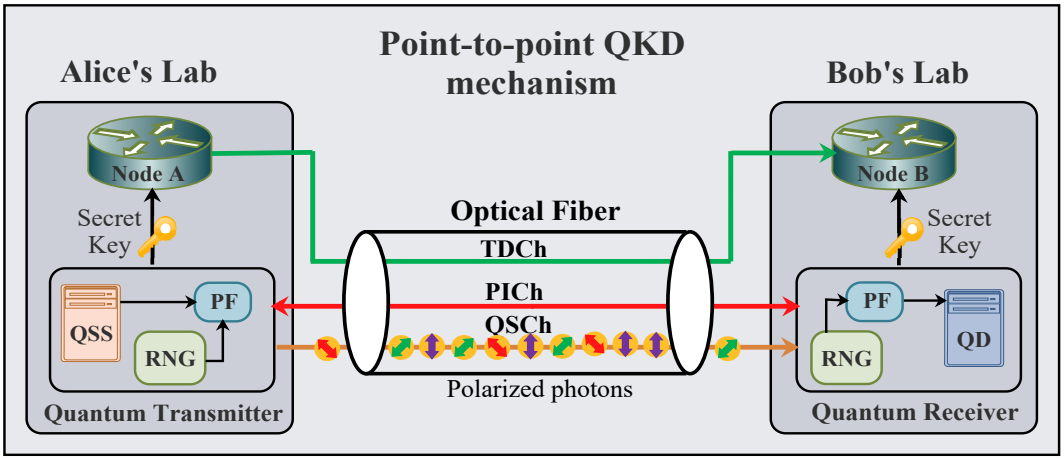


Figure 1.12: Point-to-point QKD mechanism [8, 9].

- In the Alice's lab, the QSS transmits single photons [150] to the PF; and RNG generates random bits and sends them to the PF.
- The single photons are polarized with one of the four polarization states (H, V, 45°, 135°). The bits generated by RNG are encoded with the polarized single photons to obtain qubits.
- Alice sends the qubits to Bob through QSCh, and PICh is required for qubit synchronization between Alice and Bob.

- In Bob's lab, the quantum receiver receives and measures the qubits with randomly selected polarization bases.

- Alice and Bob exchange the measuring bases with each other via PICh and compare them. After comparison, the qubits with the same polarization bases are considered for secret key generation. The sequence of bits obtained after the comparison of bases constitutes the *sifted key*.

- Alice and Bob may not be sure about the correctness of the bits considered for the *sifted key*. Thus, to further ensure the correctness and to improve the safety, error-correction, privacy amplification, and authentication are performed via PICh. The remaining bits obtained after these processes (referred to as post-processing) constitute the *secret key* [86]. Alice uses the generated *secret key* to encrypt the classical data and transmits the encrypted data to Bob through TDCh. Bob uses the same key to decrypt the received data [34].

In the last step, for data encryption, conventional encryption methods, such as one-time pad and AES, are used, however, using the secret key that has been obtained using a QKD protocol via QSCh. A one-time pad encryption method was proposed in [36], however, Shannon [151] found that in this method, the key length has to be at least as long as the data size. Hence, this method is not suitable for high bit rate data encryption as it requires large storage and high execution time, which degrades the performance of the system. To overcome this, an AES algorithm [37] was proposed, where secret keys of different lengths, i.e., 128, 192, and 256 bits are used to encode and decode the data in blocks of 128 bits. AES algorithm can encrypt the data with smaller key size and low execution time [152, 153], however, it is less secure than the one-time pad encryption method [26].

1.3 Network Architecture of QKD-ONs

In this section, network architectures of QKD-ONs are discussed in detail.

1.3.1 Basic Architecture

A basic network architecture of the QKD-ON is shown in Figure 1.13. This architecture comprises of four planes, namely, application plane, control plane, QKD plane, and data plane [8, 34, 154].

1.3.1.1 Application Plane

In the application plane, lightpath requests are generated which include (i) the lightpath requests that require QKD security (hereafter referred to as QKD secured lightpath (QKD-LP)), and (ii) the typical lightpath (LP) requests without QKD security. Both QKD-LP and LP requests are then transferred to the control plane for further processing. The status of QKD-LP and LP request acceptance/rejection is received at the application plane.

1.3.1.2 Control Plane

The control plane consists of the software-defined networking (SDN) controller [155–161] that controls and manages the network resources. The control plane allocates resources to QKD-LP, and LP requests from the QSCh, and TDCh in the QKD plane, and data plane, respectively.

1.3.1.3 QKD plane

The QKD plane consists of quantum communication nodes (QCNs) and the connection among QCNs is established over QSCh and PICh. The implementation of QKD plane is dependent on the QKD protocol being used. The process of secret key generation between each node-pair of the QKD-LP requests (QKD-LPRs) takes place in the QKD plane.

1.3.1.4 Data plane

The LP requests are transferred to the data plane directly without the involvement of QKD plane and are assigned wavelength/frequency resources. The QKD-LPRs

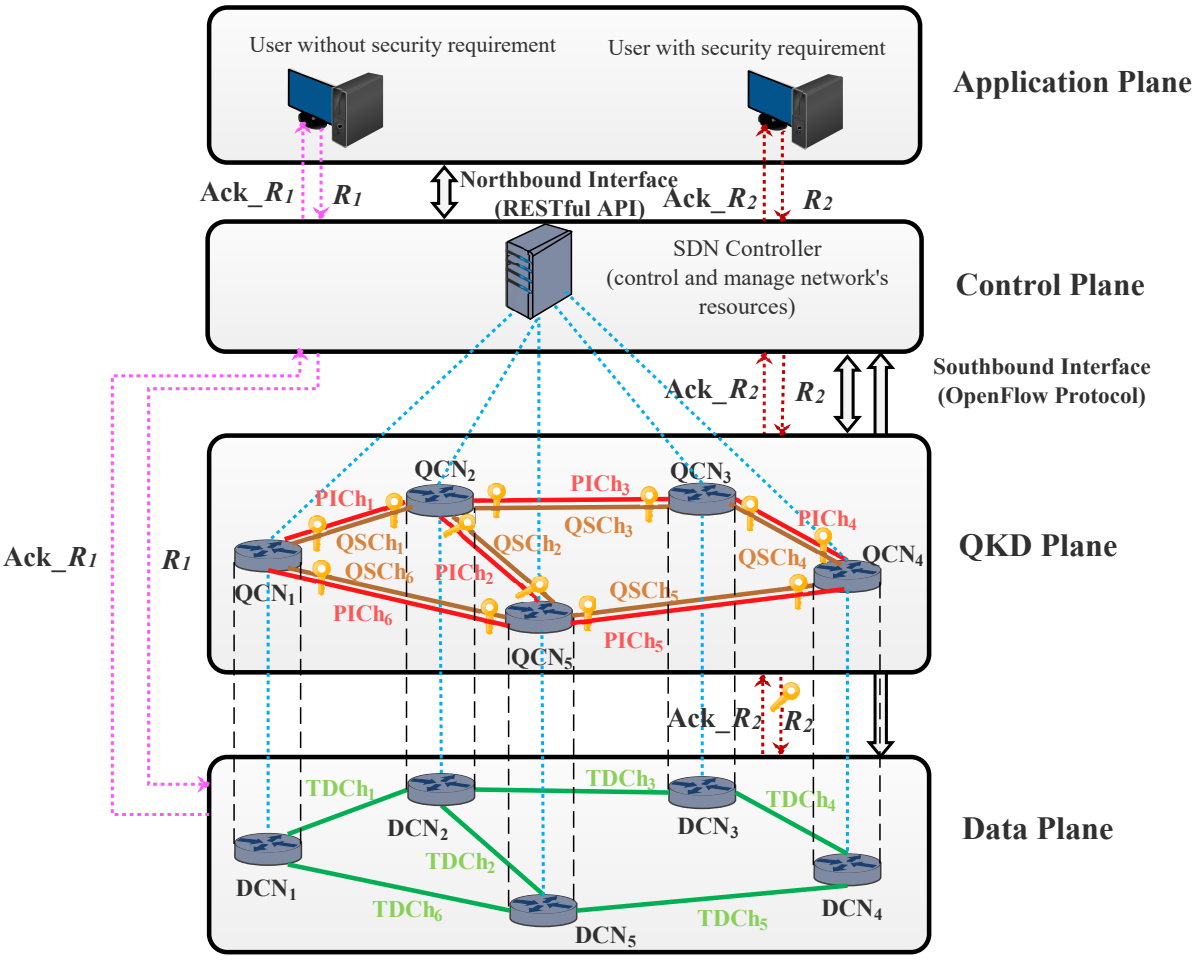


Figure 1.13: Basic network architecture [8].

are also assigned the wavelength/frequency resources in the data plane, however, the data to be transmitted over TDCh is encrypted (using the conventional encryption methods) by the secret keys generated at the QKD plane.

To establish communication among the four planes of the network architecture, different protocols are used. For implementing the southbound interface (between control plane and QKD/data plane), OpenFlow protocol (OFP) or Network Configuration (NETCONF) protocol can be used [162]. The southbound interface is used to transmit the control signals corresponding to the QLP, and LP requests from the SDN controller to the QKD plane, and data plane, respectively. The RESTful application program interface (API) is used to implement the northbound interface (between control plane and application plane) through which the properties (such as nodes, bit rate requirement, etc.) and status (acceptance, rejection, etc.) of LP

and QKD-LP requests are exchanged [8]. The process of serving LP and QKD-LP requests is shown Figure 1.13 for an LP request (R_1, shown in magenta) and a QKD-LPR (R_2, shown in red). On receiving the LP request R_1 from the application plane, the control plane performs routing, and resource allocation from the TDCh, and sends the control directly to the data plane for transmitting the information using the chosen route and the allocated TDCh resources. For the QKD-LPR R_2, the control plane configures the QKD plane to generate the secret keys among the QCNs, i.e., routing, and resource allocation from the QSCh and PICh takes place. It should be noted here that the routes chosen for establishing communication among the QCNs and the data communication nodes (DCNs) do not need to be the same. The control plane then sends the control to the data plane for encrypting the information to be transmitted using the secret keys generated at the QKD plane, and then transmit it over the chosen route and the allocated wavelength/frequency resources from the TDCh. For both the LP and QLP requests, the data plane acknowledges the control plane, where the status of network resources requests is updated accordingly, and the status of QKD-LP/LP requests acceptance/rejection is forwarded to the application plane.

1.4 Networking Challenges in QKD-ONs

In this section, the new networking challenges that have been introduced due to the integration of QKD with the existing optical networks are described. Significant research has been done on the networking aspects of QKD secured WDM optical networks, and various methods have been proposed to address the networking challenges, as described below.

1.4.1 Routing, Wavelength and Time Slot Allocation

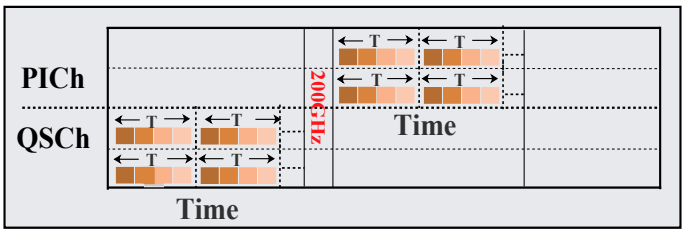
In classical WDM networks, the available optical band is subdivided into a number of fixed wavelengths grids, and for each LP request, after defining a suitable route,

wavelength is assigned. This problem is known as routing and wavelength assignment (RWA). However, in the QKD-ONs, the available optical band is subdivided into QSCh, PICh, and TDCh, as shown in Figure 1.1. The wavelengths reserved for TDCh are allocated to the LP/QKD-LP requests for data transmission in the same way as that used for the classical optical networks. However, the wavelengths allocated for QSCh and PICh are utilized employing the optical time-division multiplexing (OTDM) scheme [8, 34]. For establishing QKD-LPRs, after defining the route, wavelength is assigned on the TDCh, and time slots are assigned on the QSCh/PICh. The modified problem in QKD-ONs is known as routing, wavelength and time slot assignment (RWTA) [186].

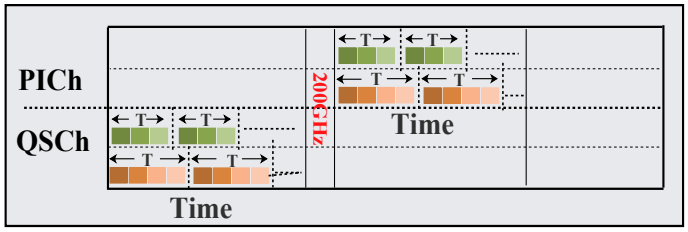
The wavelength resources are limited, and with the integration of QKD, the number of wavelengths available for the classical communication further reduces. Thus, it is necessary to utilize them efficiently such that maximum number of LP/QKD-LP requests can be established with required security levels. Thus, resource (wavelength/time slot) assignment [34, 187–189] for the three types of channels is an important problem in QKD-ONs [8]. Furthermore, currently, in most of the practical QKD networks, the secret key rate is only about $1 \sim 2$ Mbps for 50 km fiber link distance [87, 114, 117, 190]. The secret key resources (time slots) are also limited, whose assignment/reassignment depend on the required security levels, and hence they should also be efficiently utilized for QLPRs using OTDM. OTDM is an optical multiplexing technique in which multiple lower bit-rate data streams are combined to form a high bit-rate data stream, and the multiplexed signals are transmitted, and then demultiplexed at the receiver in time-domain [191]. In QKD-ONs, the reserved wavelengths for QSCh and PICh are subdivided into multiple time slots using OTDM to share the network resources and utilize them efficiently [8, 34]. PICh can reserve the dedicated wavelengths or share the wavelengths with TDCh.

Various strategies have been proposed in the literature to solve the RWTA problem [163, 167, 168, 192–194]. Initially, the RWTA problem was investigated in [8], and an RWTA strategy for resource allocation in a static traffic scenario was pro-

posed. In a static traffic scenario, the set of connection requests is known in advance. An integer linear programming (ILP) model was developed and a heuristic algorithm to solve the resource assignment problem was proposed. To enhance the security level of QKD-LPRs, a concept of key updating period was introduced. In this, the secret key can be updated periodically for data encryption, thereby making it difficult for the Eve. Figure 1.14 shows the time slot assignment scenario for QKD-LPRs with two different security levels that are assigned different key updating periods (T). Figure 1.14(a) shows the security-level scheme with fixed T, i.e., T is fixed (does not vary dynamically) and same for all the wavelengths reserved for QSCh and PICh. In the second scheme, as shown in Figure 1.14(b), the value of T is fixed, however, it is different for different wavelengths. The security level in the first scheme is lower as compared to that of the second scheme because of fixed T (easier to be cracked). A new metric, referred to as service request security ratio (SRSR) was introduced, which is defined as the ratio of the service requests allocated with QSChs successfully to the total unblocked number of service requests [8].



(a) Fixed T



(b) Different fixed T

Figure 1.14: Types of security levels [8].

To improve the security level further, a new key updating period scheme with flexible T, i.e., T with some statistical distribution, was introduced in [34]. In this scheme, T is flexible and changes dynamically, thereby increasing the complexity to

make it harder for an Eve to crack the key, and hence enhancing the security of the QKD-LPRs [164]. In case of dynamic traffic scenario, a time conflict problem arises during resource allocation due to the LP/QKD-LPR requests that arrive at the same time in the network. A concept of time-sliding window (TSW) was introduced to overcome this problem [34], however, a trade-off exists between the security-level and the resource utilization efficiency in QKD-ONs.

To maintain a balance between the security-level and the resource utilization efficiency, a new key on demand (KoD) strategy with the quantum key pool (QKP) construction technique over a software-defined optical network (SDON) was presented in [87] to secure the control channel (CCh) and the data channel (DCh). For QKP construction, the synchronized secret keys between various pairs of QCNs in the network are stored in the respective quantum secret key servers (QKSs) of QCNs. The KoD scheme with QKP assigns secret key resources on demand to the QKD-LPRs. To perform KoD jointly for both the channels, a dynamic routing, wavelength and key assignment (RWKA) algorithm was developed. RWKA algorithm consists of three steps 1) RWA for DCh of each request; 2) key assignment (KA) for CCh of each request; 3) KA for requests via the DCh. Two cases were considered for key assignment in the RWKA problem, namely, key updating based on the time-complexity of the attacks, and key updating based on the data-complexity of the attacks.

To provision adequate secret keys over QKD-ONs, a time-scheduled scheme with QKP technique was introduced in [10]. In this scheme, the RWTA problem is solved by considering three sub-problems, namely, fixed/flexible secret key consumption, uniform/non-uniform time slot allocation, and time slot continuous/discrete QKP construction, for efficient QKP construction. An example of these sub-problems for RWTA in QKD-ONs is shown in Figure 1.15. In secret key consumption, the secret keys in different QKPs (e.g., $QKP_{1\text{-}2}$, $QKP_{1\text{-}3}$, and $QKP_{2\text{-}3}$) are constantly consumed, and may be fixed or flexible, depending on the security requirements of confidential information being transmitted between the QCNs (e.g., QCN_1, QCN_2,

and QCN_3) in the network. In time slot allocation, the number of time slots allocated for different QKPs (e.g., $QKP_{1\text{-}2}$, $QKP_{1\text{-}3}$, and $QKP_{2\text{-}3}$) may be uniform or non-uniform depending on the security (secret key) requirements of QKP construction. For, e.g., let us consider the different QKPs (e.g., $QKP_{1\text{-}2}$, $QKP_{1\text{-}3}$, and $QKP_{2\text{-}3}$) are constructed with the same security (secret key) requirement, and for each QKP construction, a uniform time slot (i.e., one time-slot) is allocated (t_1, t_4, and t_3 are allocated for $QKP_{1\text{-}2}$, $QKP_{1\text{-}3}$, and $QKP_{2\text{-}3}$, respectively), shown in Figure 1.15 (the brown dash line). In Figure 1.15 (the green dash line), different QKPs (e.g. $QKP_{1\text{-}2}$, $QKP_{1\text{-}3}$, and $QKP_{2\text{-}3}$) are constructed with different security (secret key) requirements, and for each QKP construction, non-uniform time slots (i.e., three (t_1, t_2, t_3), three (t_1, t_3, t_5 on QL_1 and t_4, t_5, t_6 on QL_2), and two time-slots (t_2, t_4) for $QKP_{1\text{-}2}$, $QKP_{1\text{-}3}$, and $QKP_{2\text{-}3}$, respectively) are allocated. The construction of different QKPs may occupy continuous time-slots or discrete time slots on the intermediate QLs between the two QCNs depending on QCN without/with secret key cache function. For instance, construction of $QKP_{1\text{-}3}$ depends on the construction of $QKP_{1\text{-}2}$ and $QKP_{2\text{-}3}$ with time slot t_4 on the intermediate QLs (QL_1 and QL_2), i.e., for continuous time slot QKP construction time slot continuity constraint should be followed. For discrete time slot QKP construction, the time slot continuity constraint is not necessary. An example of discrete time-slot QKP construction is shown in Figure 1.15, where the construction of $QKP_{1\text{-}3}$ depends on the construction of $QKP_{1\text{-}2}$ with time slot (t_1, t_3, t_5) on the intermediate QL_1 and $QKP_{2\text{-}3}$ with time slot (t_4, t_5, t_6) on the intermediate QL_2. Efficient deployment and employment of the secret keys are the two new challenges in such networks. To address these challenges, a concept of key as a service (KaaS) has been introduced in [166] with two secret-key virtualization steps, namely, Key pool (KP) assembly and Virtual key pool (VKP) assembly.

Deployment of a dedicated QKD network for each high security organization such as banking, finance, and intelligence is expensive. Hence, a multi-tenant QKD network was implemented in [173, 174] where multiple tenants can share a same

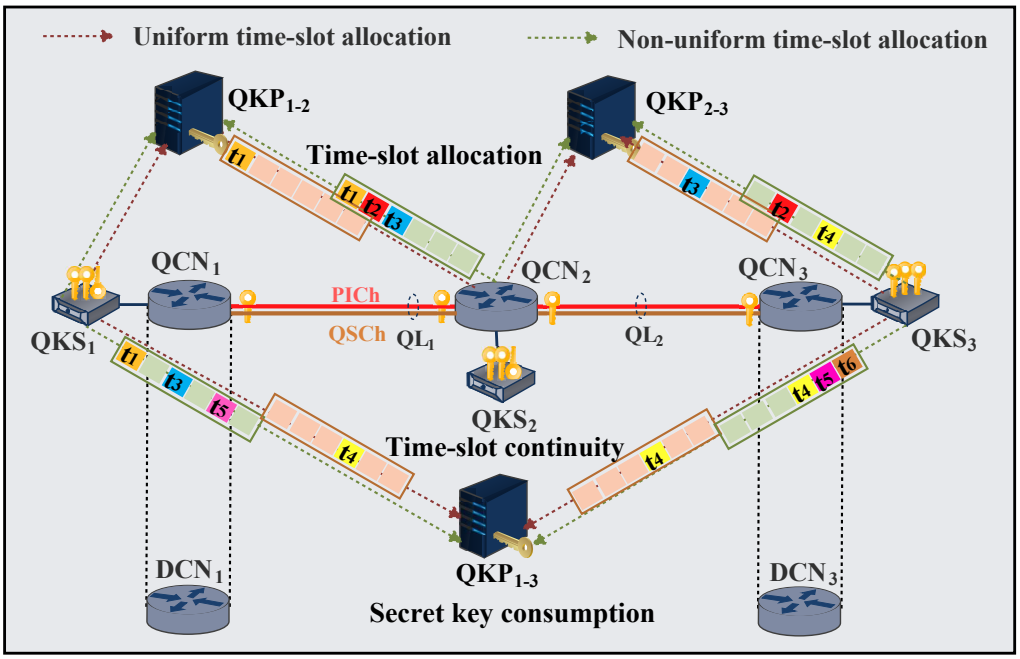


Figure 1.15: An example of three sub-problems (fixed/flexible secret key consumption, uniform/non-uniform time slot allocation, and time slot continuous/discrete QKP construction) for RWTA [10].

QKD network infrastructure to satisfy their requirements. However, efficient and flexible provisioning of multiple-tenant over a QKD network is challenging. Generally, multi-tenant provisioning (MTP) can be divided into two problems, i.e., offline (static) MTP (Off-MTP), where tenant requests are known in advance, and online (dynamic) MTP (On-MTP), where tenant requests arrive without any prior knowledge. The Off-MTP problem was addressed in [173] to improve cost efficiency by sharing a QKD network infrastructure among multiple tenant requests. An SDN-enabled metropolitan area QKD network [195] architecture was introduced, and various multi-tenancy operations for establishing multi-tenant requests over the new architecture were experimentally demonstrated. In the laboratory, an experimental testbed was established for demonstrating a workflow, protocol extension, and an on-demand secret key resource allocation strategy for providing multi-tenant services. In QKD-ONs, the secret key resources are limited. Thus, a SKR sharing scheme was presented in [173] for efficient multi-tenant secret key assignment (MTKA). A new concept of QKD as a service (QaaS) was introduced in [172] for multiple users to access their required SKRs from the same QKD network infrastructure. In this

study, a new architecture of SDN for QaaS (SDQaaS) was developed. Additionally, the protocol extension and intercommunication workflow to create, update, and delete the QKD-LPRs were presented; and a routing and SKR assignment strategy for implementing QaaS was proposed. In [175, 176], an On-MTP problem was addressed, where the On-MTP includes the scheduling of multiple-tenant requests and assignment of non-reusable secret keys to multiple tenant requests. In [175], a reinforcement learning (RL)-based MTKA strategy was proposed for QKD-ONs. Moreover, to implement efficient On-MTP, a comparative analysis of heuristics and an RL-based On-MTP was performed to examine the efficiency of On-MTP [176]. Furthermore, in [170], a problem of efficient distribution of keys over metro-quantum optical networks (MQON) was addressed by designing a novel node structure. Based on this structure, two new RWTA schemes were proposed for MQON. Along with the routing and resource assignment, a summary of various networking challenges of QKD-ONs addressed in the existing works, is given in Table 1.5.

1.4.2 Fragmentation

In QKD-ONs, for efficient utilization of network resources, OTDM [186] has been adopted to construct QSCh and PICh [8]. Hence, the process of resource assignment in QKD-ONs is termed as RWTA [8, 34]. Moreover, in such networks, a unique secret key updating feature has been introduced to enhance the security level of QKD-LPRs [8] and resource reassignment is performed to satisfy the security requirements of QKD-LPRs. This diverse assignment and reassignment of network resources during the creation and modification of QKD-LPRs introduces fragmentation in QSCh and generates several small-sized isolated, discontinuous, and fragmented time-slots that cannot be further used for future incoming QKD-LPRs. Thus, fragmentation in QKD-ONs is critical and different problem than the existing fragmentation problem of elastic optical networks (EONs) and computer storage.

Figure 1.16 illustrates the effect of fragmentation in QKD-ONs. In order to show the effect of fragmentation in QSCh, a network topology, as shown in Figure

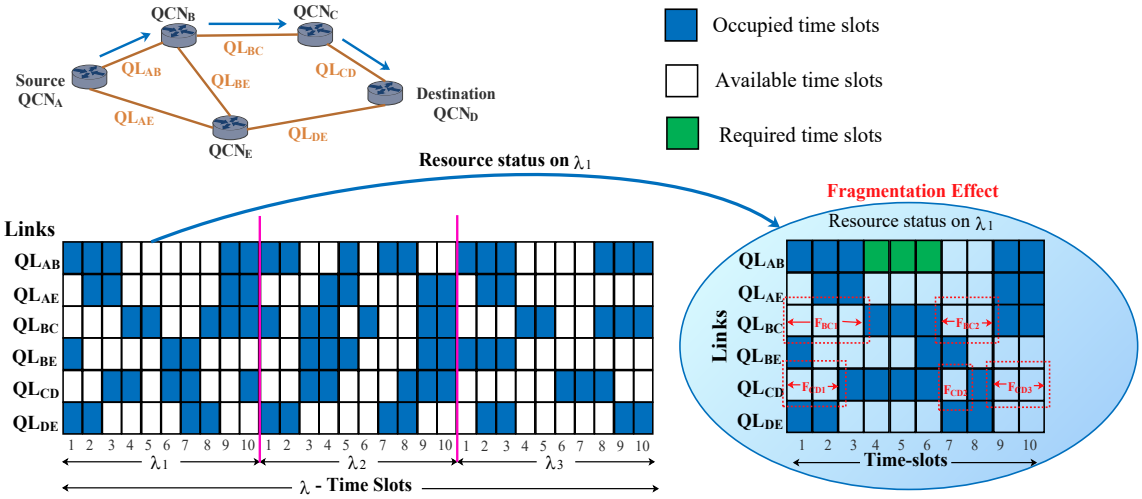


Figure 1.16: Illustration of the effect of fragmentation in QKD-ONs

1.16, consists of five QCNs and six QLs is considered. Moreover, an example of time-slot fragmentation in QSCh during RWTA on λ_1 and the resource status on λ_1 are illustrated in Figure 1.16. Each QL consists of ten time slots. Suppose a QKD-LPRs AD selects a route A-B-C-D and requires three time slots on selected route to establish a secure connection between the QCN_A and QCN_D. A QKD-LPR AD first searches the availability of time slots on corresponding QLs, i.e., QL_{AB}, QL_{BC} , and QL_{CD} to satisfy the QKD-LPR security requirement. Let us consider time slots {4, 5, 6} are selected as the occupied time-slots on QL_{AB} for a QKD-LPR AD (filled with green) as per their security requirement. A QKD-LPR AD searches the same time-slots {4, 5, 6} on QL_{BC} and QL_{CD} in order to meet the time slot continuity constraint. For QKD-LPR AD, on QL_{BC} and QL_{CD} the unused time slots are available, however the available time slots are fragmented slots (F_{BC1} and F_{BC2} on QL_{BC} and F_{CD1}, F_{CD2}, and F_{CD3} on QL_{CD}), i.e., the sufficient time-slots are unavailable on the corresponding QLs. Hence, because of these fragmented time-slots, a QKD-LPR AD get rejected, results in higher blocking of QKD-LPRs. Thus, it is important to consider the impact of fragmentation while allocating network resources to QKD-LPRs with security requirements.

1.5 Securing Optical Networks Using Quantum-Secured Blockchain: An Overview

This section moves towards a new technology known as quantum-secured blockchain. Blockchain is one of the most promising solutions because of its decentralized and distributed ledger technology. However, the security of blockchain relies on the computational complexity of certain mathematical functions, and because of the evolution of quantum computers, its security may be breached in real-time in the near future. Therefore, researchers are focusing on combining QKD with blockchain to enhance blockchain network security. This section provides a brief overview of blockchain technology with its security loopholes, the quantum-secured blockchain technology, and focused on the current research efforts in developing secure and robust optical networks.

1.5.1 Blockchain

Blockchain is an innovative and unique technology for transferring and sharing confidential information among untrusted nodes in the network. It is a distributed database that consists of non-erasable records of information [196]. In blockchain, the records are managed by a group of network nodes, not by a single centralized authority. Hence, it is tamper-resistant [197, 198]. Blockchain security is based on two cryptographic tasks, i.e., a cryptographic hash function for encryption and a digital signature for authentication, which makes blockchain more secure [11]. In blockchain [199], each block is connected with its previous block using the previous block's hash value. In addition, each node in the blockchain network has a copy of the ledger. Hence, if an eavesdropper wants to break the security of a blockchain, he/she has to solve a large mathematical problem of each node in the network at the same time, which is expensive and requires more computational power [200]. Hence, the security of blockchain technology is currently almost unbreakable. A blockchain has the following characteristics [201] that make it attractive for various types of

applications:

- Blockchain technology has a decentralized structure [201, 202], where there is no central node/authority to store data. Moreover, in blockchain technology, transactions are not validated and authorized by a centralized authority as in a centralized system.

- The blockchain is immutable [203], i.e., the previously stored data cannot be changed. All of the valid transactions are immutably stored in blocks of blockchain. In blockchain, each block is connected with the previous block using its hash value generated by a cryptographic hash function. If an attacker tries to alter any previous block record, it will affect all of the succeeding blocks of the blockchain, and the attack can be easily detectable.

- The blockchain system itself validates and authenticates transactions. Hence, it is transparent in recording new data and also in updating them. In blockchain, the valid transaction is added to the block after the validation process using consensus protocols. In addition, the ledger of each node is updated, and this process is publicly visible. Hence, a third party cannot add false transactions to the ledger. This visibility ensures the transparency and security of blockchain [203].

- All of the nodes in the blockchain network hold identical copies of the ledger records, and update when the transaction is valid. Hence, blockchain is resistant to attacks and information leakage [201]. This feature of blockchain contributes to the network's resilience and data integrity.

1.5.2 Quantum-secured Blockchain

This subsection describes the quantum-secured blockchain technology along with its underlying process. Blockchain technology is strong enough to provide security within the blockchain network between the nodes by leveraging asymmetric cryptography and hashing algorithms. Asymmetric cryptography generates a pair of keys

to provide security between the nodes and authenticate transactions by generating a digital signature. The most widely used digital signature schemes are Rivest, Shamir, Adleman (RSA) [14], or elliptic curve cryptography [204]. Hashing algorithms also play a crucial role in providing security by hashing the transaction data and linking blocks of a blockchain by generating block hash values. However, the security of both asymmetric cryptography and hash algorithms relies on the computational complexity of certain mathematical functions that quantum computers can easily attack shortly [11, 205]. Hence, blockchain will release all of its security features and become insecure. If quantum attack-aware schemes are not designed to enhance blockchain security, then the existing and future blockchain networks will become vulnerable and put blockchain at risk.

Post-quantum cryptography schemes were proposed to overcome the blockchain security problem [204]. However, currently, their security is questionable. Hence, they do not provide guaranteed security against threats. The most prominent way to provide complete security in blockchain against quantum attacks is QKD. The security of QKD relies on the fundamental laws of quantum mechanics [35]. QKD generates and distributes random secret keys between the authenticated users in the network using the QKD protocol through QSCh and PICh to encrypt confidential information. Hence, there is a huge research interest in protecting the blockchain network against quantum attacks by integrating QKD into blockchain [206]. A quantum-secured blockchain platform was developed and experimentally demonstrated, which uses QKD for authentication and the original Byzantine fault tolerance (BFT) consensus protocol for validation [11]. The security of the quantum-safe blockchain is practically realizable and scalable for different government and commercial services. However, a major drawback of the proposed quantum-secured blockchain is the use of a consensus protocol. The limitation of the BFT consensus protocol is that, if a large number of nonoperational nodes are present in the blockchain network, it becomes data-intensive. Hence, a new quantum-secured consensus protocol was designed to limit the problem of the traditional consensus pro-

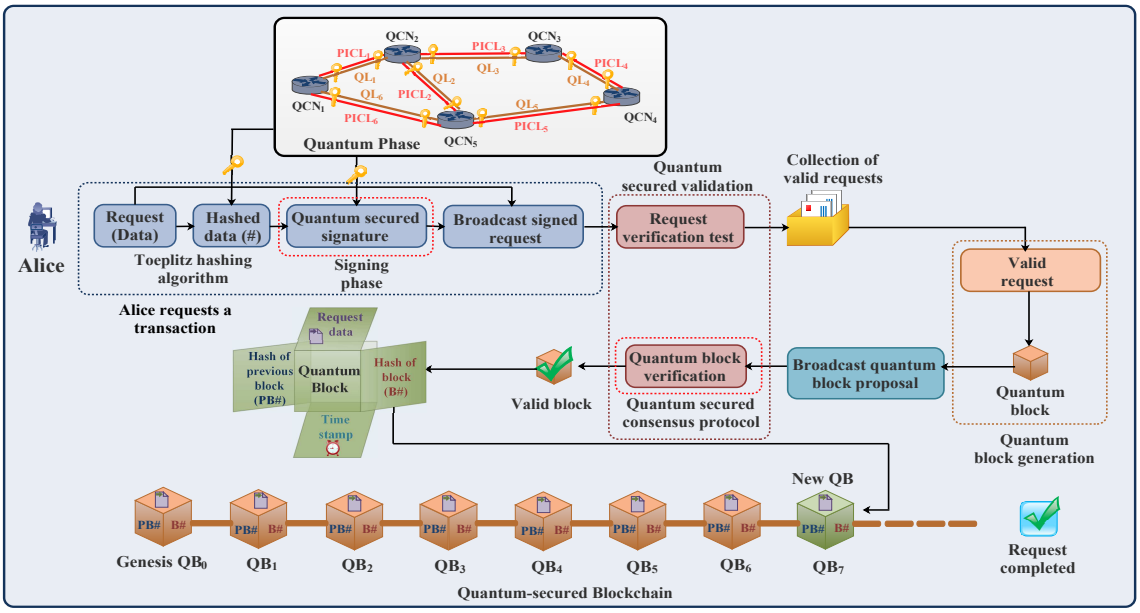


Figure 1.17: Process of quantum-secured blockchain [11, 12].

.

tocol in [12]. However, not many protocols have been implemented to improve the security of blockchain networks using QKD. Therefore, further research is urgently needed to design secure consensus protocols using quantum technologies.

1.5.3 Process of Quantum-secured Blockchain

This subsection discusses the process of quantum-secured blockchain. In quantum-secured blockchain, the QKD technique is used to generate and distribute secret keys and provide authentication, which makes blockchain networks robust against the attacking capabilities of quantum computers [15, 207]. Quantum-secured blockchain uses the same components as the traditional blockchain, discussed in Section 5.1.1.1 However, a major difference is that, instead of conventional cryptography and hashing algorithms, it utilizes quantum techniques to secure the network against security breaches. Figure 1.17 shows the workflow of a quantum-secured blockchain [11, 12]. The workflow consists of the quantum phase, transaction proposal phase, transaction validation phase, and quantum block proposal and validation phase. A detailed description of the phases is discussed below.

1.5.3.1 Quantum Phase

A quantum phase consists of a QKD network [120–123, 128, 130], as shown in Figure 1.17. In this phase, random secret keys between the two authenticated users in the network are generated using QKD protocols, such as BB84 [5, 24] and others [38, 40, 42, 45, 46, 69], [7, 50–53, 141], through QSCh and PICh, discussed in Section 1.1.3(1.1.3.1). The generated secret keys are then used for encryption and authentication.

1.5.3.2 Transaction Proposal Phase

In the transaction proposal phase, Alice requests a transaction and hashed data by using hashing algorithms for encryption, as shown in Figure 1.17. The most widely used scheme is Toeplitz hashing [208], in which a Toeplitz matrix is generated by shared random keys between the sender and receiver. This scheme, along with one-time pad encryption, helps in transferring transaction data securely. The generated secret keys using QKD in the quantum phase are used in generating a quantum-secured signature to sign a transaction in a signing phase. After the signing phase, the transaction data and the signature are broadcasted to the nodes in the quantum blockchain network.

1.5.3.3 Transaction Validation Phase

In this phase, upon receiving the transaction data and signature, the blockchain participants perform a specific test, detailed in [12], to validate the transaction. After validation, only the valid transactions are collected in a block of valid requests, as shown in Figure 1.17.

1.5.3.4 Quantum Block Proposal and Validation Phase

After the transaction validation phase, the quantum block (QB) of valid requests is created and broadcasted to peer nodes in the quantum blockchain network for validation. The QB is validated using quantum-secured consensus protocols consisting

of proposing, voting, and decision phases, as explained in [12]. When the QB is validated, it is then added to the quantum blockchain to form a quantum-secured blockchain. After that, the ledger of each node in the quantum blockchain network is updated, and the transaction is securely received.

1.6 Thesis Outline and Contributions

This thesis consists of Chapters 1 to 6, whose brief description with their contribution is as follows.

Chapter 1. Introduction: This chapter gives a brief overview of QKD including qubits and its representation, and a basic yet complete QKD system. Subsequently, it describes the underlying QKD process using the BB84 protocol, the schemes for designing QKD protocols, and the quantum hacking attacks along with the method of prevention. Further, this chapter discusses the co-existence of QKD in optical networks, some practical demonstrations of QKD-ONs, the QKD standardization activities, and the mechanism of secure communication over a point-to-point optical fiber link using the BB84 QKD protocol. Besides, the architecture and various networking challenges of QKD-ONs are discussed. Apart from this, the chapter provides an overview of new quantum-secured blockchain technology. The motivation and contribution of the work are also presented.

Chapter 2. Efficient Provisioning of Network Resources for Different CoQLRs in QKD-ONs: In this chapter, a RWTA or routing and resource assignment (RRA) problem of QKD-ONs for different categories of QKD-LPR (CoQKD-LPRs) is addressed. The QKD-LPRs are categorized into three different types, namely high prioriy QKD-LPRs (HPQKD-LPRs), moderate priority QKD-LPRs (MPQKD-LPRs), and low priority QKD-LPRs (LPQKD-LPRs), on the basis of their security requirements. To minimize the impact of blocking for different CoQKD-LPRs of QKD-ONs, an efficient key assignment priority ordering policy for RRA is

proposed. The performance of the proposed policy is investigated under two different sizes of networks and compared with different existing baseline policies in terms of considered metrics.

Chapter 3. Impact of Fragmentation in Quantum Signal Channel of QKD-ONs: This chapter is focused on the fragmentation issue of QKD-ONs caused by the isolated slots in the network. A fragmentation-suppressed routing and resource assignment (FS-RRA) approach is proposed to minimize the effect of fragmentation during assignment and reassignment in QSCh. The effect of time-slot fragmentation in QSCh is analyzed by using two existing resource assignment approaches and a proposed FS-RRA in terms of the QSCh fragmentation index *(FI_{QSCh})*, the external fragmentation *($FM_{external}$)*, blocking probability *(BP)*, and resource utilization *(RU)*.

Chapter 4. Deep Reinforcement Learning Based Routing and Resource Assignment in QKD-ONs: In this chapter, a deep reinforcement learning (DRL)-based method is exploited to address the RRA problem of QKD-ONs. The RRA problem of QKD-ONs is a complex decision making problem, where appropriate solutions depend on understanding the networking environment. Motivated by the recent advances in DRL for complex problems and also because of its capability to learn directly from experiences, this chapter exploits DRL to solve the RRA problem and proposes a DRL-based RRA scheme. The performance of the proposed DRL-based RRA scheme is compared with the deep-Q network (DQN) method and the two baseline schemes, namely, First Fit (FF) and Random Fit (RF) in terms of *BP*, and *RU*.

Chapter 5. Routing based on Deep Reinforcement Learning in QKD-ONs: This chapter is focused on the routing sub-problem of RRA in QKD-ONs. Routing is a challenging problem in QKD-ONs and involves the selection of an ap-

propriate route that establishes a secure path between the QKD nodes for secret key distribution. A DRL-based solution for routing in QKD-ONs is proposed in this chapter that enables the routing agent to learn and adapt to changing network conditions by understanding the networking environment. The effectiveness of the proposed scheme is compared with two baseline routing schemes, namely, shortest path (ShP) and fixed alternate routing based on hop count (HC), in terms of *BP*.

Chapter 6. Conclusion and Future Work: The contributions of the thesis are summarized in this chapter, and important insights and conclusions are presented. Further, the scope for future work is also discussed.

Table 1.5: Summary of existing works that address various networking challenges in QKD-ONs

Networking Challenge	Year, and Ref.	Description
RWTA	2017, [154]	Develops a QKD-ON architecture with SDN, address RWTA problem, and develop a static RWTA strategy
	2017, [87]	Introduces a novel concept of KoD for efficient provisioning of network resources with QKP technique
	2017, [163]	Proposes a soft-reservation strategy to avoid time-conflict based on resource allocation
	2018, [164]	Develops RWTA algorithm with flexible key updation period in a dynamic traffic scenario and introduces the concept of TSW to reduce time conflicting
	2018, [10]	Proposes a new time-scheduled scheme to assign resources efficiently for three types of channels with QKP technique
	2018, [165]	Proposes a secret key generation scheme to provide security in the physical layer based on feature extraction of the optical channel and experimentally verified the proposed scheme over 200 km fiber loop
	2019, [166]	Presents the concept of KaaS that provides sufficient secret keys in proper time to satisfy the lightpath requests
	2019, [167]	Proposes an auxiliary graph-based RWTA (AG-RWTA) algorithm to save quantum key resources
	2019, [168]	A new node structure was designed for the distribution of global quantum keys to secure multicast services
	2020, [169]	Proposes a novel key-relay tree-based routing and key assignment(KRT-RKA) scheme based on the multi relay node (MRN) structure for efficient distribution of quantum keys as per the user demands in a multicast service scenario
	2020, [170]	Two RWTA schemes was designed based on auxiliary graph in MQON with new node structure
	2020, [171]	A novel distributed subkey-relay tree-based routing and key assignment (DSKRT-RKA) algorithm was proposed based on DSKRT-SM scheme for efficient distribution of secret keys for multicast services
Multi tenant provisioning problem	2019, [172]	Introduces a new concept of QaaS and develop routing and SKR assignment strategy for multiple users
	2019, [173]	Develops a multi-tenant QKD network in which multiple users can use the same network infrastructure for securing their lightpath requests, proposes a MTKA strategy and experimentally verified the proposed strategy
	2019, [174]	Demonstrates the multi-tenant provisioning over SDN-based metropolitan area network and design an on-demand secret key resource allocation strategy for providing access to multiple users
	2019, [175] and 2020, [176]	The On-MTP problem was addressed and a heuristic and RL-based key assignment strategies were designed for QKD networks
Resiliency	2019, [177]	Focuses on protecting the secret keys against network failure and develop two new survivable schemes
	2019, [178]	A secret key flow model (SKFM) was constructed to design SKRS to strength the resiliency against failure in QKD network
	2019, [179]	A novel shared backup path protection (SBPP) scheme based on dynamic time window plane was proposed in TDM based QKD-ONs
	2020, [180]	A new dynamic wavelength and key resource adjustment algorithm was proposed to solve the mixed/hybrid resource allocation problem in the existing backup QKD-ONs
Trusted repeater node placement, cost-minimized approach, and key recycling approach	2020, [170]	A novel quantum node structure with the ability of bypass was designed, if the distance between the two nodes in the network is within a certain range
	2020, [181], 2020, [182], and 2021, [183]	A new hybrid trusted/untrusted relay based QKD network architecture which consists of TRNs/UTRNs was proposed
	2019, [184]	The cost minimized problem was addressed, a novel cost-oriented model was constructed and a cost-efficient QKD networking algorithms were designed to solve the cost-minimized problem
	2020, [185]	Quantum key recycling mechanisms, namely, partial recycling, all recycling, and mixed recycling, were proposed to increase the number of available keys in the QKD system for secure communication

Chapter 2

Efficient Provisioning of Network Resources for Different CoQKD-LPRs in QKD-ONs

2.1 Introduction

In optical communication networks, the problem of assigning an appropriate route and suitable network resources to a LP request is known as RWA. However, in QKD-ONs, for efficient utilization of network resources in such networks, OTDM has been adopted for construction of the QSCh and PICh. Hence, the modified RWA problem of QKD-ONs is termed as RWTA [8]. In context of RWTA or RRA, different researchers have developed various strategies for efficient utilization of network resources for three types of channels in both static [8] and dynamic traffic scenarios [34]. Almost all the proposed strategies in the literature focus on efficient utilization of network resources because of the limited network resources in the existing optical networks.

It has also been observed from the literature, discussed in Chapter 1, that the availability of network resources' is essential for QKD-LPRs in order to reduce the effect of blocking in the network. The unavailability of network resources increases

blocking and degrades the network performance. In QKD-ONs, blocking increases because of the increase in traffic load, and the number of times modifications are required to update the secret key of QKD-LPRs. Additionally, the financial, defence, and other government services, whose security is paramount during security attacks, require sufficient network resources during resource assignment and reassignment to satisfy the service demand with full security. Hence, blocking is a severe problem for HPQKD-LPRs and MPQKD-LPRs in such networks. Therefore, in this chapter a secret key assignment priority ordering policy (SKA-POP) is proposed for RRA to improve the success probability *(SP)* of QKD-LPRs.

In this chapter, QKD-LPRs are categorized into three types, namely, HPQKD-LPRs, MPQKD-LPRs, and LPQKD-LPRs. The QKD-LPRs with the highest security level are categorized as HPQKD-LPRs. In HPQKD-LPRs category, secret keys of such requests are updated more frequently than the other two CoQKD-LPRs. The HPQKD-LPRs include defence services, financial services, and other government applications, which are at the highest priority during RRA [8]. The QKD-LPRs with moderate security levels come under the category of MPQKD-LPRs. The secret keys of MPQKD-LPRs are updated moderately, i.e., the QKD-LPR modifications required to update the secret keys of such requests are lower than the HPQKD-LPRs, however more than the LPQKD-LPRs. Confidential business information such as emails, etc. are examples of MPQKD-LPRs. Online gaming, a normal conversation between two users, downloading movies, and web-series, etc., are examples of LPQKD-LPRs. For LPQKD-LPRs, the secret keys of such category of QKD-LPRs are updated slowly than the HPQKD-LPRs and MPQKD-LPRs. The priority order of QKD-LPRs based on the security level is HPQKD-LPRs $>$ MPQKD-LPRs $>$ LPQKD-LPRs. Hence, the number of times the secret key reassignment process required to establish a QKD-LPR with full security is more for HPQKD-LPRs, moderate for MPQKD-LPRs, and fewer for LPQKD-LPRs. Thus, availability of network resources is essential for HPQKD-LPRs and MPQKD-LPRs, which are at high risk during security threats. The main contributions of the work are as follows:

(i) This chapter addresses the RRA problem of QKD-ONs for different CoQKD-LRs.

(ii) A SKA-POP for RRA is proposed to improve the *SP* of QKD-LPRs.

(iii) The performance of the proposed ordering policy is evaluated on two different networks, namely, NSFNET and UBN24 and compared with non-priority based RWTA (NP-RWTA), priority order based RWTA (POB-RWTA) [209], partial-priority based RWTA (PP-RWTA), and a version of SKA-POP, i.e., SKA-POP with the longest route first (SKA- POP-LRF) schemes in terms of the *SP* and the probability of secret key update failure (P_{SKUF}).

2.2 Proposed Secret Key Assignment Priority Ordering Policy

2.2.1 Network Model

This subsection describes the system model used in this chapter to evaluate performance of the proposed priority ordering policy in comparison with the NP-RWTA, POB-RWTA, PP-RWTA, and SKA-POP-LRF. Let us consider a physical network topology of a QKD-ON represented by a connected graph $G(V_Q, E_Q, T_Q, W_T, W_Q)$, where, V_Q represents the set of QCNs, T_Q represents the set of TRNs, and E_Q represents the set of QLs. W_T represents the total number of available wavelengths on each fiber link, and W_Q represents the total number of reserved wavelengths for QSCh and PICh on each QL. Let us assume Q is set of incoming QKD-LPRs. A QKD-LPR is represented by $Q_t(o_t, d_t, q_l, C_r, Z^c_{t,k}, T, N^m_{t,k}, z^c_{t,k}, Z^m_{t,k})$, $Q_t \in Q$, where o_t and d_t are the source and destination QCNs of a QKD-LPR, respectively. The q_l is the number of QLs between source QCN and destination QCN pair, the $C_r(H_{QKD\text{-}LPR}, M_{QKD\text{-}LPR}, L_{QKD\text{-}LPR})$ represents the CoQKD-LPRs, where, $H_{QKD\text{-}LPR}$, $M_{QKD\text{-}LPR}$, and $L_{QKD\text{-}LPR}$ are set of incoming HPQKD-LPRs, MPQKD-LPRs, and LPQKD-LPRs, respectively. $Z^c_{t,k}$ is the required number of initial secret

key time-slots during creation of a QKD-LPR, T is period after which a secret key of QKD-LPR has to be updated or modified. $N^m_{t,k}$ is the number of times secret key modification required to update a QKD-LPR. $z^c_{t,k}$ is the change in the number of time-slots for modifying secret key of a QKD-LPR, and $Z^m_{t,k}$ is the required number of modifying secret key time-slots of a QKD-LPR. QSCh and PICh reserved an equal number of wavelengths on each QL is considered in this chapter. Also, TRNs between the QCNs for establishing a secured long-distance communication in the QKD network is assumed. OTDM is employed in QKD-ON for efficient utilization of network resources, which segments the reserved wavelengths of QSCh and PICh into several time-slots. For analyzing the performance of the proposed ordering policy, the K-shortest path algorithm is utilized for routing computation and selection to compute the k-alternate paths between the source and destination QCNs of a QKD-LPR. Then, for secret key assignment and reassignment during RRA, the FF resource assignment policy is utilized in this chapter because of its simplicity and low computational complexity.

2.2.2 Secret Key Assignment Priority Ordering Policy

This subsection discusses concept of the proposed SKA-POP for reducing the impact of blocking in QKD-ONs.

In a non-priority based ordering policy, resources are randomly assigned in the network without any priority order. If resources are assigned first to LPQKD-LPRs, then the resources are occupied by such QKD-LPRs in the network. This leads to lower availability of network resources for HPQKD-LPRs and MPQKD-LPRs, resulting in increased blocking of HPQKD-LPRs and MPQKD-LPRs in the network. Similarly, in POB-RWTA scheme the QKD-LPRs with higher security level are served first and in PP-RWTA scheme some of the QKD-LPRs from each CoQKD-LPR (which have higher priority within the CoQKD-LPR) are served first and other QKD-LPRs are randomly served in the network. However, using these schemes the overall blocking of QKD-LPRs does not reduce because of the assignment of

network resources without any proper ordering policy. Therefore, for improving establishment of the HPQKD-LPRs and MPQKD-LPRs, and for reducing the overall blocking of QKD-LPRs, a priority ordering policy for RRA in QSCh of QKD-ONs is proposed. Using the proposed SKA-POP, the requested resources are available for HPQKD-LPRs and MPQKD-LPRs. Additionally, it has been observed that by using SKA-POP, sufficient resources are also available for LPQKD-LPRs after the successful assignment of resources for HPQKD-LPRs and MPQKD-LPRs during the secret key assignment and reassignment.

The objective of the proposed SKA-POP is to assign the network resources for QKD-LPRs according to the order of priority to reduce blocking in QSCh of QKD-ONs. The proposed policy consists of three steps with two priority criteria. In *Step 1*, the QKD-LPRs with different security levels are categorized into three different types, namely, HPQKD-LPRs, MPQKD-LPRs, and LPQKD-LPRs. Based on the first priority criterion, the different CoQKD-LPRs are arranged in decreasing order of their security level, i.e., from HPQKD-LPRs to LPQKD-LPRs, to maximize the establishment of high and moderate security level QKD-LPRs. In the *Step 2*, within a category, the QKD-LPRs are arranged in increasing order of $Z^c_{t,k}$, which is the second priority criterion. That means in the category of HPQKD-LPRs, the QKD-LPR which requires the least initial secret key time-slots, will be served first in the network. Similarly, the same priority criterion of *Step 2* is followed by the other two CoQKD-LPRs. By using the above mentioned criterion more number of resources are available for future QKD-LPRs because QKD-LPR with least $Z^c_{t,k}$ is served first in the network. Additionally, for each category of QKD-LPRs, the proposed SKA-POP uses the shortest route first (based on the hop-counts) so that less number of links and resources are utilized by QKD-LPR to serve the request. In *Step 3*, the RRA is performed using the proposed priority criteria. Therefore, by using the proposed priority ordering policy, blocking of the QKD-LPRs due to limited number of network resources can be reduced.

The motivation behind prioritization of QKD-LPRs is to serve the HPQKD-

LPRs and MPQKD-LPRs before any LPQKD-LPRs in the network such that the maximum number of HPQKD-LPRs and MPQKD-LPRs are established successfully. Hence, SP is improved and P_{SKUF} is reduced by introducing the concept of prioritization for RRA in such networks. The priority order of each category of QKD-LPRs is based on the $Z^c_{t,k}$ and their route length. Using these criteria, in each QKD-LPR category, the QKD-LPRs with least $Z^c_{t,k}$ and with the shortest route receive highest priority.

In this work, our objective is to enhance the availability of network resources for HPQKD-LPRs and MPQKD-LPRs in order to reduce the blocking of such requests and the network's overall blocking. However, in a non-priority ordering policy, the QKD-LPRs are served randomly, in POB-RWTA, only the HPQKD-LPRs are served first and all other QKD-LPRs are served randomly, and in PP-RWTA, within the CoQKD-LPRs some of the QKD-LPRs are served first and others are served randomly in the network, as discussed above. Hence, the availability of resources is not guaranteed for the upcoming QKD-LPRs. Thus, using the concept of non-priority ordering policy, POB-RWTA, and, PP-RWTA for RRA in QSCh, the QKD-LPRs with high and moderate security levels may be rejected due to unavailability of network resources during secret key assignment and reassignment which increases blocking in the network. However, in the proposed SKA-POP, the secret key assignment and reassignment for RRA are based on a different priority criteria. Hence, the possibility of the availability of network resources is more for HPQKD-LPRs and MPQKD-LPRs. Therefore, the proposed priority ordering policy minimizes the impact of blocking as compared to NP-RWTA, POB-RWTA, and PP-RWTA in such networks which leads to better performance of QKD-ONs in terms of higher SP and lower P_{SKUF}. The complete algorithm of SKA-POP for RRA is shown in Algorithm 1.

The proposed SKA-POP for RRA is explained with an illustration, where a network topology with 5 QCNs and 7 QLs is assumed, as shown in Figure 2.1. Consider that different QKD-LPRs, i.e., AC, BC, AB, BD, AD, with different security require-

Algorithm 1 The proposed SKA-POP

Inputs: $G(V_Q,\ E_Q,\ T_Q,\ W_T,\ W_Q)$, Q, $Q_t(o_t,\ d_t,\ q_l,\ C_r,\ Z^c_{t,k},\ T,\ N^m_{t,k},\ z^c_{t,k},\ Z^m_{t,k})$, *k-routes*

Output: *SP* and P_{SKUF}.

for $Q_{\mathrm{t}} \leftarrow 1$ to Q **do**

Divide the QKD-LPRs into three CoQKD-LPRs on the basis of security level

Arrange the different CoQKD-LPRs in decreasing order of their security level (Prioritize the CoQKD-LPRs on the basis of security level)

Search the route for each category of QKD-LPRs using *K-shortest path algorithm*

Select the first *k-routes* as *fixed routes*

Arrange the QKD-LPRs (within the CoQKD-LPR) and their routes in increasing order of $Z^c_{t,k}$ and route length, respectively

if resources are available **then**

Perform secret key assignment using *FF algorithm* for individual CoQKD-LPR based on the priority criteria

if secret key assignment is successful **then**

Request is accepted

Update the status of request on each QL

else

Request is rejected

end if

end if

if request requires modification **then**

if resources are available **then**

Perform re-assignment for modifying secret key using *FF algorithm*

if secret key re-assignment is successful **then**

Request is accepted

Update the status of request on each QL

else

Request is rejected

end if

else

Request is rejected

end if

else

No re-assignment

end if

if more modification is required **then**

follow *Step 18* to *Step 32*

end if

return output parameters

end for

ments arrive in the network. The routes of the QKD-LPRs are shown in Table 2.1. The arrangement of QKD-LPRs with their requirements and QKD-LPR acceptance status is shown in Table 2.2 using NP-RWTA, POB-RWTA and PP-RWTA.

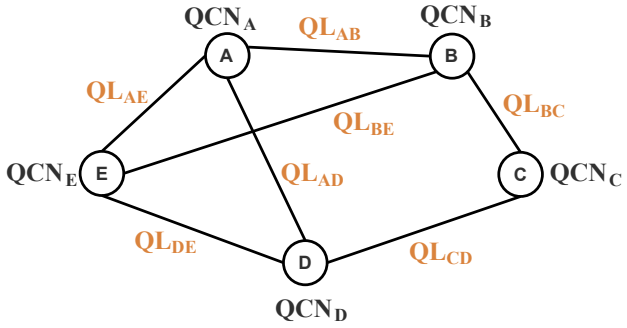


Figure 2.1: A network topology.

Table 2.1: QKD lightpath requests routes

QKD-LPR	Route
AC	A-B-C, A-D-C, A-E-B-C, A-E-D-C
BC	B-C, B-A-D-C, B-E-D-C, B-A-E-D-C
AB	A-B, A-E-B, A-D-C-B, A-E-D-C-B
BD	B-C-D, B-A-D, B-E-D, B-A-E-D
AD	A-D, A-E-D, A-B-C-D, A-B-E-D

Table 2.2: Concept of NP-RWTA, POB-RWTA, and PP-RWTA

QKD-LPR	Security Level	$Z^c_{t,k}$	QKD-LPR Order According to NP-RWTA	QKD-LPR Order According to POB-RWTA	QKD-LPR Order According to PP-RWTA	$Z^m_{t,k}$	QKD-LPR Acceptance Status for NP-RWTA/ POB-RWTA/ PP-RWTA
AC	low	2	AC	BD	BD	$3...N^c_{t,k}$	ACC/ACC/ACC
BC	moderate	3	BC	AD	BC	$4,2...N^c_{t,k}$	REJ/ACC/ACC
AB	low	3	AB	AC	AC	$4...N^c_{t,k}$	REJ/REJ/REJ
BD	high	4	BD	BC	AB	$5,3,4...N^c_{t,k}$	REJ/REJ/REJ
AD	high	3	AD	AB	AD	$4,2,3...N^c_{t,k}$	REJ/REJ/REJ

According to the Step 1 of the proposed SKA-POP different QKD-LPRs, i.e., AC, BC, AB, BD, AD with different security requirements, are arranged in decreasing

Table 2.3: Concept of SKA-POP and SKA-POP-LRF

QKD-LPR Priority Order Based on Security Level	QKD-LPR Priority Order According to SKA-POP-LRF	QKD-LPR Priority Order According to SKA-POP	QKD-LPR Acceptance Status for SKA-POP-LRF/SKA-POP	$Z^m_{t,k}$	Request Acceptance Status for SKA-POP -LRF/SKA-POP
BD (high)	AD(3 and A-B-C-D)	AD(3 and A-D)	ACC/ACC	4,2,3...$N^c_{t,k}$	ACC/ACC
AD (high)	BD(4 and B-A-E-D)	BD(4 and B-C-D)	ACC/ACC	5,3,4...$N^c_{t,k}$	ACC/ACC
BC (moderate)	BC(3 and B-A-E-D-C)	BC(3 and B-C)	ACC/ACC	4,2...$N^c_{t,k}$	ACC/ACC
AC (low)	AC(2 and A-E-D-C)	AC(2 and A-B-C)	ACC/ACC	3...$N^c_{t,k}$	REJ/ACC
AB (low)	AB(3 and A-E-D-C-B)	AB(3 and A-B)	ACC/ACC	4...$N^c_{t,k}$	REJ/ACC

order of their security level, i.e., from HPQKD-LPRs to LPQKD-LPRs, shown in Table 2.3. According to the Step 2 of the proposed ordering policy, each category of QKD-LPRs is arranged in increasing order of their requested initial secret key time-slots with the shortest route, shown in Table 2.3. Additionally, the proposed SKA-POP is compared with a SKA-POP-LRF for complete analysis. Table 2.3 shows arrangement of the QKD-LPRs with their requirements and QKD-LPR acceptance status using the proposed SKA-POP and SKA-POP-LRF. In this chapter, aim of the proposed SKA-POP is to assign an appropriate path and suitable network resources for QKD-LPRs according to the priority criteria. The K-shortest path algorithm is used for routing in QSCh. Thus, the first k-routes are selected from the K-routes. The fixed alternate routes obtained for the QKD-LPRs are shown in Table 2.1. After route computation and selection, the resources are assigned along the selected path of the QKD-LRPs using the FF resource assignment policy. If resources for initial secret key time-slots are available during resource assignment, then the QKD-LPR is treated as accepted. Moreover, suppose the QKD-LPR requires modification to improve the security, in that case, resource reassignment is performed using the same resource assignment policy in order to assign requested time-slots for QKD-LPR modification. If resources during assignment and reassignment are available, then QKD-LPRs are accepted, otherwise rejected. The acceptance status of QKD-LPRs for SKA-POP and SKA-POP-LRF is shown in Table 2.3.

2.3 Performance Evaluation

In this section, the impact of blocking in QSCh is analyzed by evaluating performance of the proposed SKA-POP in comparison with the NP-RWTA, POB-RWTA, PP-RWTA, and the SKA-POP-LRF. In this chapter, two different sizes of optical networks, namely, NSFNET (14 nodes and 22 links) and UBN24 (24 nodes and 43 links) to test performance of the proposed SKA-POP are used, as shown in Figure 2.2 and Figure 2.3, respectively. For three types of channel in QKD-ONs, 80 wavelengths with 50 GHz channel spacing is considered [8]. The number of wavelengths reserved for QSCh and PICh is the same. Hence, this chapter analyzes the performance of RRA using the proposed priority ordering policy and the existing schemes only for QSCh. For the performance evaluation of the proposed SKA-POP, different W_Q for QSCh, i.e., 2 and 4, and different ranges of $Z^c_{t,k}$, i.e., $Z^c_{t,k} \in$ [4,6] and $Z^c_{t,k} \in$ [4,8] are assumed. Depending on W_Q, the total number of available time-slots for QSCh also varies. In this chapter, a static traffic scenario is considered, and the QKD-LPRs are randomly generated with different security levels in the network. The sequence of arrival of QKD-LPRs is different for each simulation run. In this work, the performance of the proposed SKA-POP for different ratios of the QKD-LPRs, i.e., $H_{QKD\text{-}LPR}$: $M_{QKD\text{-}LPR}$: $L_{QKD\text{-}LPR}$ = 1:1:1 and $H_{QKD\text{-}LPR}$: $M_{QKD\text{-}LPR}$: $L_{QKD\text{-}LPR}$ = 1:2:3 is analyzed. The results are averaged over 100 simulations for different network topologies. Two metrics, namely, SP and P_{SKUF}, are used for evaluating performance of the proposed SKA-POP. The implementation of QKD network model, QKD-LPR model, and simulations are performed in MATLAB.

2.3.1 Success Probability (SP)

The SP is defined as the ratio of accepted QKD-LPRs to the total incoming QKD-LPRs in the QKD-ON.

$$SP = \frac{\sum Q_{accepted}}{Q_{total}(\sum C_r)} \tag{2.1}$$

where, $Q_{accepted}$ is the accepted QKD-LPR and Q_{total} $(\sum C_r)$ is the total incoming

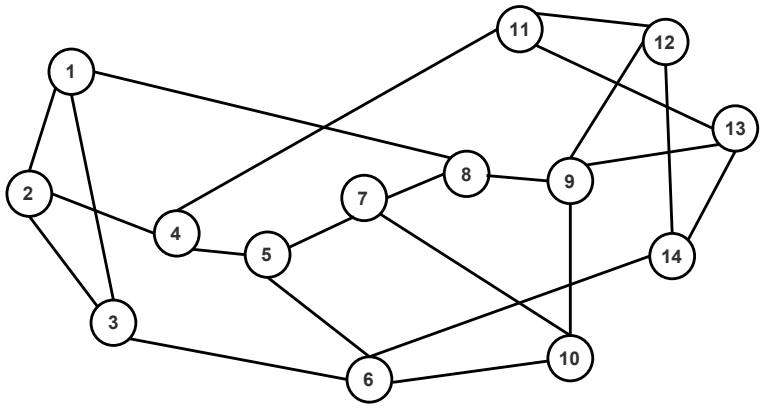


Figure 2.2: NSFNET network topology.

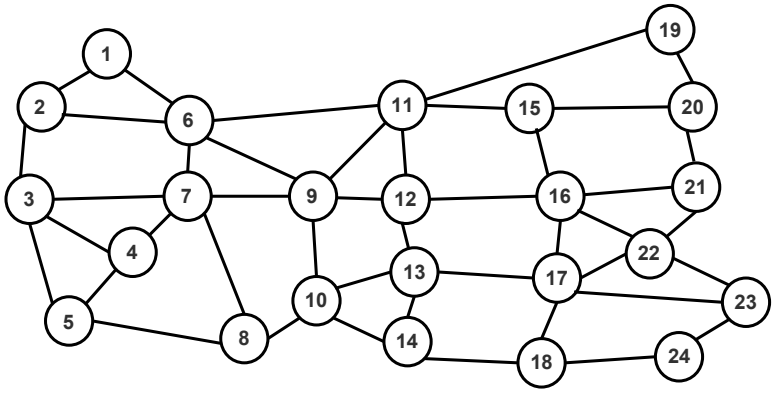


Figure 2.3: UBN24 network topology.

QKD-LRs.

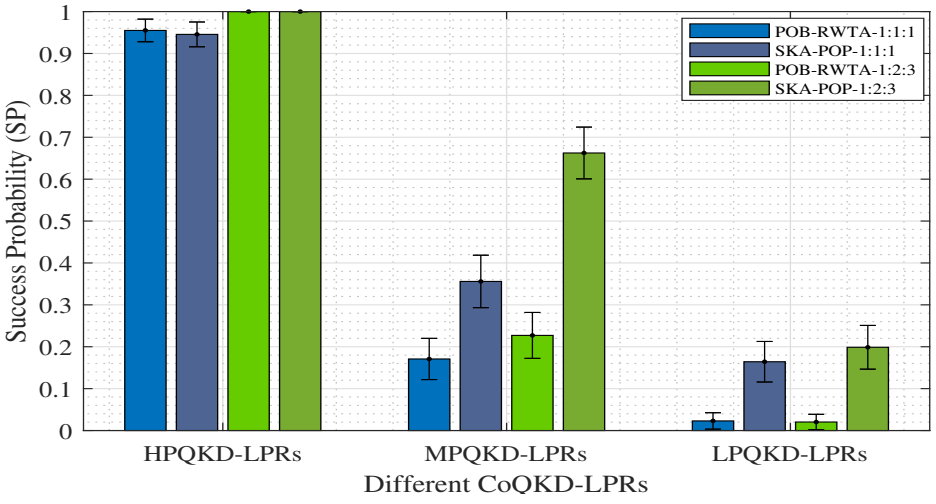
2.3.2 Probability of secret key update failure (P_{SKUF})

The P_{SKUF} is defined as the ratio of QKD-LPRs with secret key update failure to the total incoming QKD-LPRs.

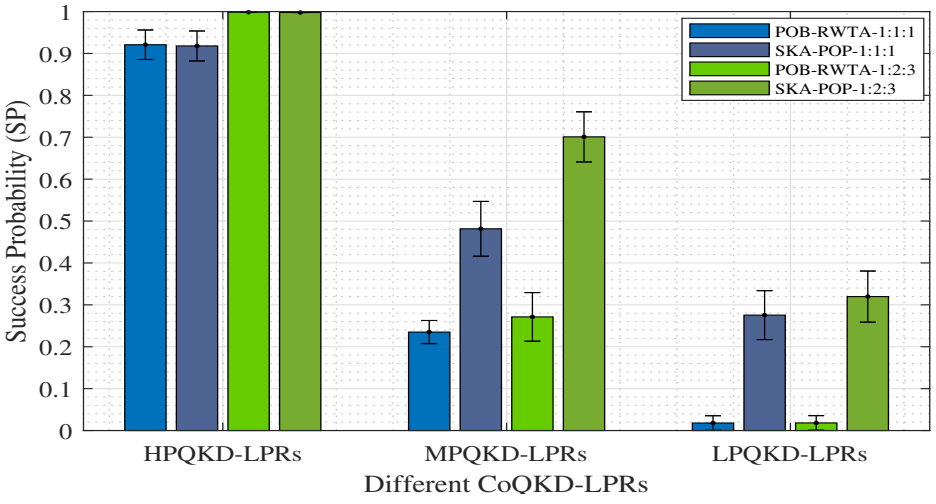
$$P_{SKUF} = \frac{\sum Q_{SKU\ failure}}{Q_{total}(\sum C_r)} \tag{2.2}$$

where, $Q_{SKU\ failure}$ is QKD-LPR with secret key update failure and Q_{total} $(\sum C_r)$ is the total incoming QKD-LRs.

Figure 2.4 shows the *SP* of QKD-LPRs for different CoQKD-LPRs individually with different ratios of QKD-LPRs, i.e., $H_{QKD\text{-}LPR}$: $M_{QKD\text{-}LPR}$: $L_{QKD\text{-}LPR}$ = 1:1:1 and $H_{QKD\text{-}LPR}$: $M_{QKD\text{-}LPR}$: $L_{QKD\text{-}LPR}$ = 1:2:3 with 95% confidence interval. In this work, a standard 95% confidence interval is used to estimate the range of values of



(a)



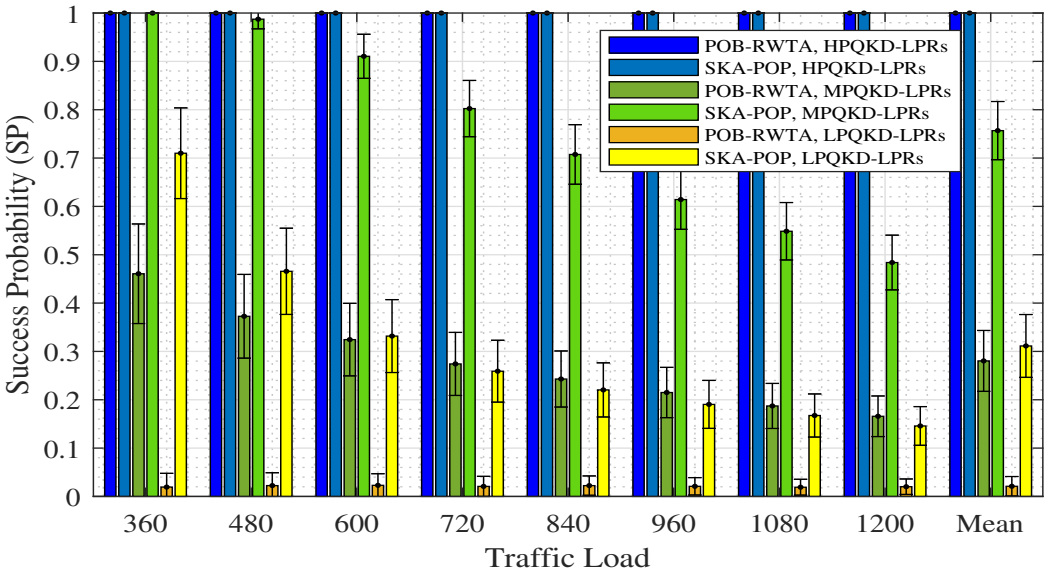
(b)

Figure 2.4: Success Probability (SP) for different CoQKD-LPRs with different QKD-LPR ratios ($H_{QKD\text{-}LPR}$: $M_{QKD\text{-}LPR}$: $L_{QKD\text{-}LPR}$ = 1:1:1 and $H_{QKD\text{-}LPR}$: $M_{QKD\text{-}LPR}$: $L_{QKD\text{-}LPR}$ = 1:2:3) (a) in the NSFNET and (b) in the UBN24.

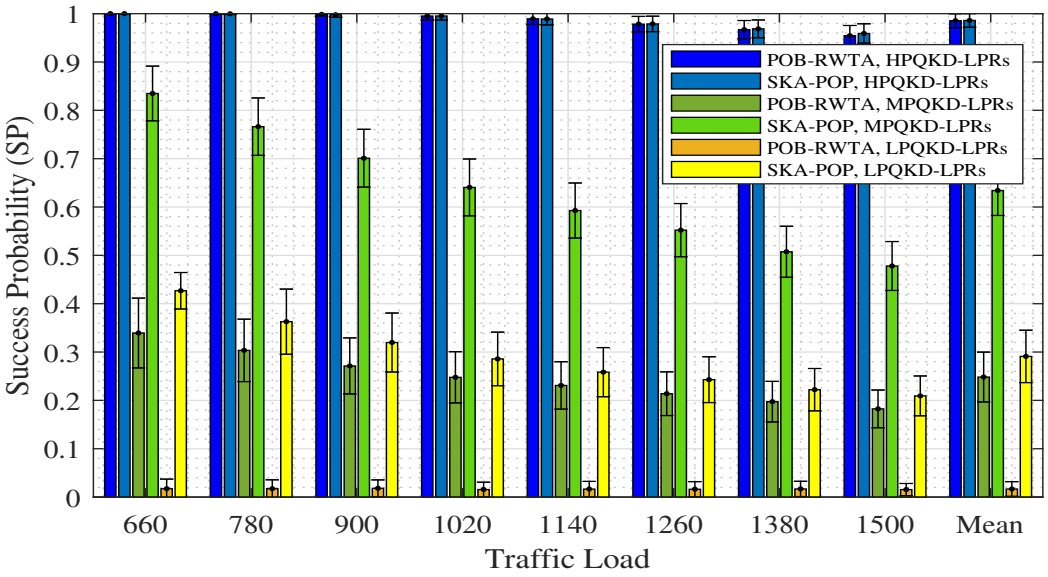
different metrics. The error bars represent 95% confidence interval. The performance of the proposed SKA-POP and the existing POB-RWTA scheme for NSFNET and UBN24 in terms of SP for different ratios of QKD-LPRs is shown in Figure 2.4. The results indicate that the SP is less for $H_{QKD\text{-}LPR}$: $M_{QKD\text{-}LPR}$: $L_{QKD\text{-}LPR}$ = 1:1:1 as compared to $H_{QKD\text{-}LPR}$: $M_{QKD\text{-}LPR}$: $L_{QKD\text{-}LPR}$ = 1:2:3 for MPQKD-LPRs and LPQKD-LPRs. The reason is that as the percentage of HPQKD-LPRs increases, the availability of network resources for other two categories of QKD-LPR decreases. Hence, fewer QKD-LPRs are established for the MPQKD-LPRs and LPQKD-LPRs for QKD-LPR ratio $H_{QKD\text{-}LPR}$: $M_{QKD\text{-}LPR}$: $L_{QKD\text{-}LPR}$ = 1:1:1. It can be observed

from Figure 2.4 that the *SP* for HPQKD-LPRs for different QKD-LPR ratios is almost same using SKA-POP and POB-RWTA. It can also be observed from Figure 2.4(a) that the improvement in *SP* as compared to POB-RWTA is 52% and 86% for MPQKD-LPRs and LPQKD-LPRs for $H_{QKD\text{-}LPR}$: $M_{QKD\text{-}LPR}$: $L_{QKD\text{-}LPR}$ = 1:1:1 and for $H_{QKD\text{-}LPR}$: $M_{QKD\text{-}LPR}$: $L_{QKD\text{-}LPR}$ = 1:2:3 the average improvement of *SP* as compared to POB-RWTA is 65.72% and 89.77% for MPQKD-LPRs and LPQKD-LPRs, respectively. Similarly, for UBN24, it can observed from Figure 2.4(b) that the *SP* for MPQKD-LPRs and LPQKD-LPRs using the SKA-POP compared to POB-RWTA increased by 51.19% and 93.50% for $H_{QKD\text{-}LPR}$: $M_{QKD\text{-}LPR}$: $L_{QKD\text{-}LPR}$ = 1:1:1, respectively. The average improvement of 61.30% and 94.33% has been obtained using SKA-POP for MPQKD-LPRs and LPQKD-LPRs with $H_{QKD\text{-}LPR}$: $M_{QKD\text{-}LPR}$: $L_{QKD\text{-}LPR}$ = 1:2:3 as compared to POB-RWTA. It can also be observed from Figure 2.4(a) that the average improvement in *SP* of the proposed SKA-POP for $H_{QKD\text{-}LPR}$: $M_{QKD\text{-}LPR}$: $L_{QKD\text{-}LPR}$ = 1:2:3 for HPQKD-LPRs, MPQKD-LPRs and LPQKD-LPRs is 5.75%, 86.15% and 21% as compared to $H_{QKD\text{-}LPR}$: $M_{QKD\text{-}LPR}$: $L_{QKD\text{-}LPR}$ = 1:1:1, as shown in Figure 2.4(a) for NSFNET, respectively. Similarly, in Figure 2.4(b) for UBN24, the average improvement of 8.70%, 45.58% and 16.06% has been obtained using SKA-POP for HPQKD-LPRs, MPQKD-LPRs and LPQKD-LPRs with $H_{QKD\text{-}LPR}$: $M_{QKD\text{-}LPR}$: $L_{QKD\text{-}LPR}$ = 1:2:3 as compared to $H_{QKD\text{-}LPR}$: $M_{QKD\text{-}LPR}$: $L_{QKD\text{-}LPR}$ = 1:1:1, respectively. It can also be observed from the Figure 2.4 that with 95% confidence interval, the *SP* for different Co-QKD-LPRs with different ratios of QKD-LPRs, i.e., $H_{QKD\text{-}LPR}$: $M_{QKD\text{-}LPR}$: $L_{QKD\text{-}LPR}$ = 1:1:1 and $H_{QKD\text{-}LPR}$: $M_{QKD\text{-}LPR}$: $L_{QKD\text{-}LPR}$ = 1:2:3 is somewhere between the upper and lower values of the confidence interval.

Figure 2.5 shows the *SP* of QKD-LPRs for different CoQKD-LPRs with different traffic loads with 95% confidence interval. Different ratios of QKD-LPRs for each CoQKD-LPR have been considered for simulation. The performance of SKA-POP for NSFNET and UBN24 in terms of *SP* for QKD-LPRs ratio $H_{QKD\text{-}LPR}$: $M_{QKD\text{-}LPR}$: $L_{QKD\text{-}LPR}$ = 1:2:3 is shown in Figure 2.5. The results indicate that the *SP* is more



(a)



(b)

Figure 2.5: Success Probability (SP) for different CoQKD-LPRs with traffic load (a) in the NSFNET and (b) in the UBN24 for QKD-LPR ratio ($H_{QKD\text{-}LPR}$: $M_{QKD\text{-}LPR}$: $L_{QKD\text{-}LPR}$ = 1:2:3).

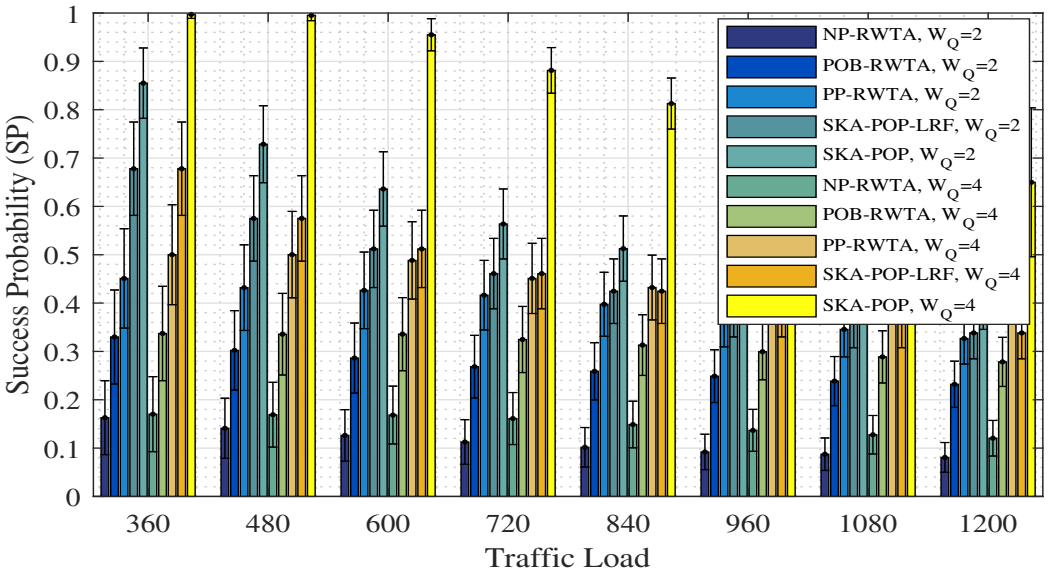
for SKA-POP as compared to POB-RWTA because of the proposed priority criteria. Using the proposed criteria, the availability of network resources for different CoQKD-LPRs increases in the network. Hence, more QKD-LPRs are established in the network using the SKA-POP scheme. It has been seen from Figure 2.5 that the SP for HPQKD-LPRs is almost same. For NSFNET, it has been observed that the improvement in SP for MPQKD-LPRs and LPQKD-LPRs for $H_{QKD\text{-}LPR}$: $M_{QKD\text{-}LPR}$

: $L_{QKD\text{-}LPR}$ = 1:2:3 is 62.95% and 93.24% as compared to POB-RWTA, shown in Figure 2.5(a), respectively. Similarly, for UBN24, the *SP* for MPQKD-LPRs and LPQKD-LPRs using SKA-POP for $H_{QKD\text{-}LPR}$: $M_{QKD\text{-}LPR}$: $L_{QKD\text{-}LPR}$ = 1:2:3 is improved by 60.84% and 94.27% as compared to POB-RWTA, shown in Figure 2.5(b), respectively. It has also been observed from the Figure 2.6 that with 95% confidence interval, the estimate of*SP* of QKD-LPRs for different Co-QKD-LPRs will lie between the upper and lower values of the confidence interval.

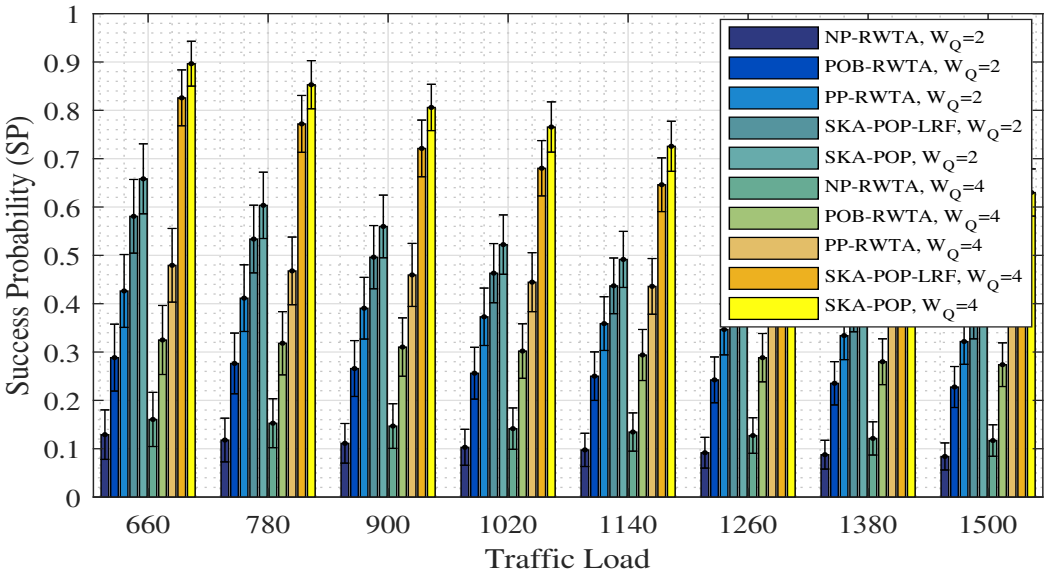
Figure 2.6 shows the *SP* of different ordering policies, i.e., NP-RWTA, POB-RWTA, PP-RWTA, SKA-POP-LRF, and SKA-POP for total QKD-LPRs with different W_Q and QKD-LPR ratio $H_{QKD\text{-}LPR}$: $M_{QKD\text{-}LPR}$: $L_{QKD\text{-}LPR}$ = 1:2:3 with 95% confidence interval. It has been observed from plotted graphs that the SKA-POP performs better than the other four ordering policies under QKD-LPR ratio $H_{QKD\text{-}LPR}$: $M_{QKD\text{-}LPR}$: $L_{QKD\text{-}LPR}$ = 1:2:3 in terms of *SP* for total QKD-LPRs with increasing traffic load. From Figure 2.6(a), it can be seen that an average improvement of 80.31%, 52.89%, 31.11%, and 18.50% in *SP* for total QKD-LPRs with W_Q=2 has been obtained using SKA-POP as compared to NP-RWTA, POB-RWTA, PP-RWTA, and SKA-POP-LRF for NSFNET, respectively. It can also be seen that an average improvement in *SP* with W_Q=4 of the proposed SKA-POP is 82.13%, 62.67%, 46%, and 44.34% as compared to NP-RWTA, POB-RWTA, PP-RWTA, and SKA-POP-LRF, respectively. Similarly, for UBN24 the *SP* of SKA-POP with W_Q=2 is increased by 80.28%, 51.01%, 28.93%, and 11.37% and with W_Q=4 is increased by 81.70%, 60.29%, 41.20%, and 10.29% as compared to NP-RWTA, POB-RWTA, PP-RWTA, and SKA-POP-LRF, respectively.

It has also been observed from the Figure 2.6 that with 95% confidence interval, the *SP* of different ordering policies, i.e., NP-RWTA, POB-RWTA, PP-RWTA, SKA-POP-LRF, and SKA-POP for total QKD-LPRs with different W_Q and QKD-LPR ratio $H_{QKD\text{-}LPR}$: $M_{QKD\text{-}LPR}$: $L_{QKD\text{-}LPR}$ = 1:2:3 is somewhere between the upper and lower values of the confidence interval.

Figure 2.7 and Figure 2.8 show P_{SKUF} with increasing traffic load under different



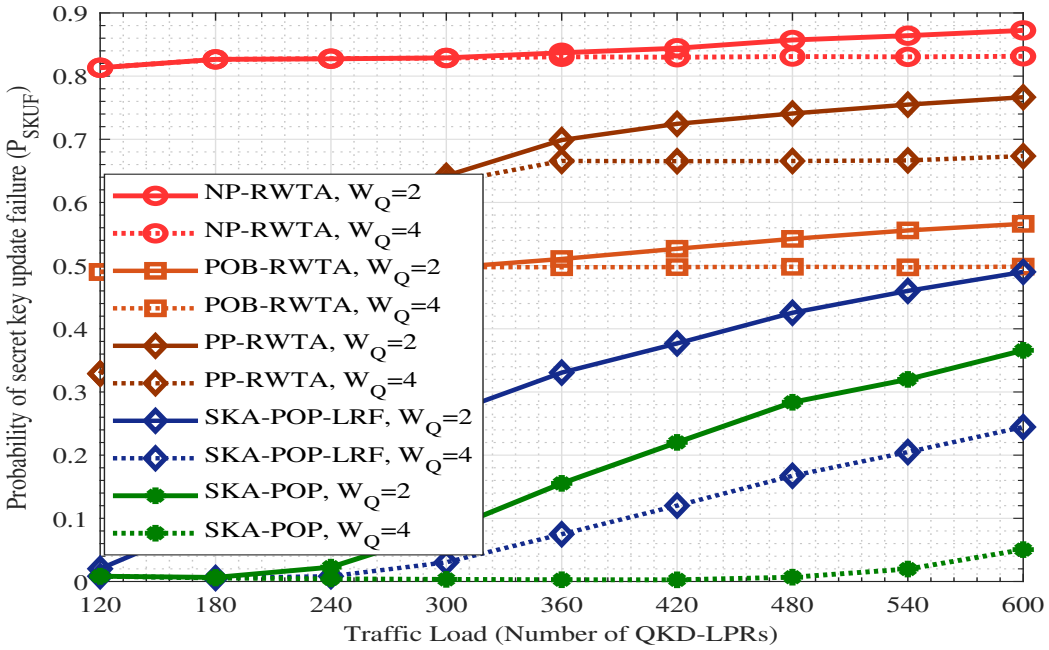
(a)



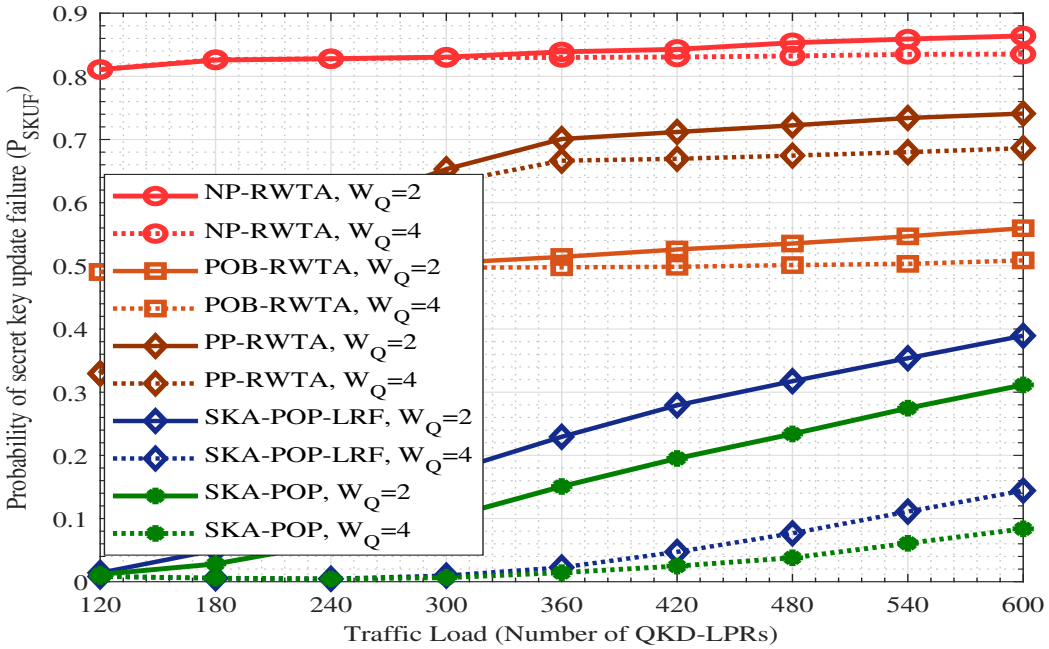
(b)

Figure 2.6: Success Probability (SP) for total QKD-LPRs with different W_Q and QKD-LPR ratio ($H_{QKD\text{-}LPR}$: $M_{QKD\text{-}LPR}$: $L_{QKD\text{-}LPR}$ = 1:2:3) in (a) the NSFNET and (b) the UBN24.

parameters, i.e., W_Q and $Z^c_{t,k}$. P_{SKUF} is the probability of QKD-LPR failure during secret key re-assignment, i.e., the requested resources during secret key assignment are available, however, requested resources during reassignment are not available for QKD-LPR modification and hence, the QKD-LPR is rejected. In this case, the QKD-LPR requires modification to improve the security level; hence, the secret key reassignment process will occur. Therefore, the availability of network resources is



(a)



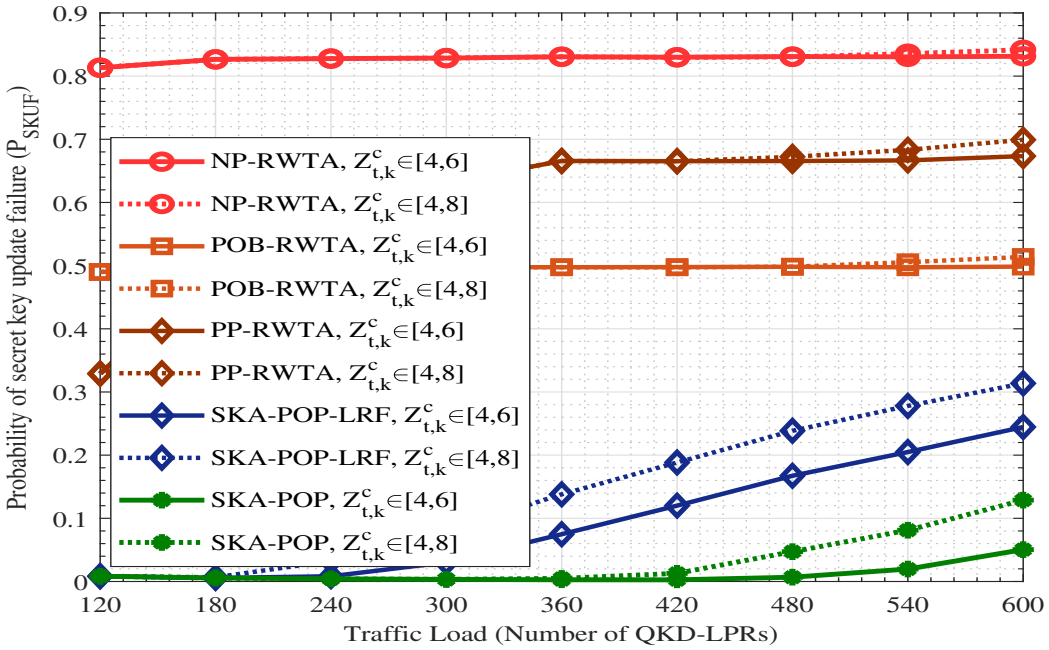
(b)

Figure 2.7: Probability of secret key update failure (P_{SKUF}) for total QKD-LPRs with different W_Q and $H_{QKD\text{-}LPR}$: $M_{QKD\text{-}LPR}$: $L_{QKD\text{-}LPR}$ = 1:1:1 QKD-LPR ratio in (a) the NSFNET and (b) the UBN24.

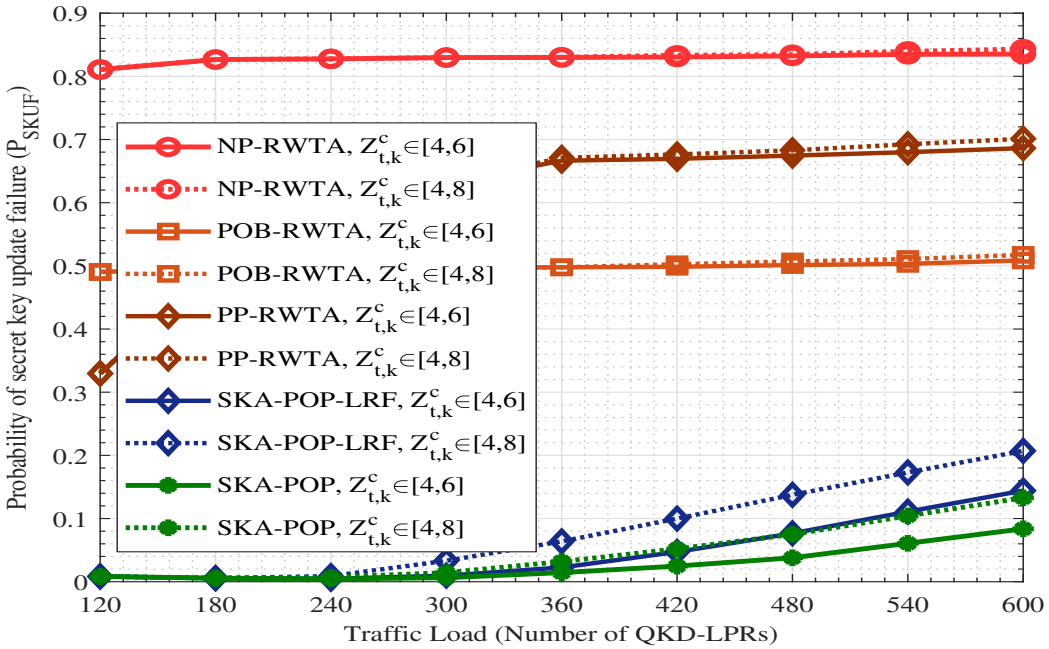
necessary for each modification in order to establish the QKD-LPR with full security. P_{SKUF} obtained for each of the two networks with different W_Q is shown in Figure 2.7. It has been observed that the increase in the value of W_Q increases the QKD-LPR establishment because it increases the availability of network resources.

Thus, it minimizes the effect of blocking in QSCh during secret key assignment and reassignment. It is evident from Figure 2.7 that P_{SKUF} with different W_Q is more for the NP-RWTA, POB-RWTA, PP-RWTA, and SKA-POP-LRF as compared to the proposed SKA-POP for both the networks. In Figure 2.7(a), for NSFNET, an average reduction of 80.66%, 68.73%, 74.48%, and 44.73% in P_{SKUF} with W_Q=2 has been obtained using SKA-POP as compared to the other four ordering policies, namely, NP-RWTA, POB-RWTA, PP-RWTA, and SKA-POP-LRF with QKD-LPR ratio $H_{QKD\text{-}LPR}$: $M_{QKD\text{-}LPR}$: $L_{QKD\text{-}LPR}$ = 1:1:1, respectively. It can also be seen that an average reduction in P_{SKUF} with W_Q=4 of the proposed SKA-POP is 98.60%, 97.67%, 98.06%, and 87.99% as compared to NP-RWTA, POB-RWTA, PP-RWTA, and SKA-POP-LRF, respectively. Similarly, Figure 2.7(b) for UBN24, shows an average reduction of 81.89%, 70.70%, 75.93%, and 28.62% in P_{SKUF} using the proposed SKA-POP with W_Q=2 as compared to NP-RWTA, POB-RWTA, PP-RWTA, and SKA-POP-LRF, respectively. It can also be observed that an average reduction of 96.69%, 94.51%, 95.45%, and 42.69% in P_{SKUF} with W_Q=4 has been obtained for the proposed SKA-POP as compared to NP-RWTA, POB-RWTA, PP-RWTA, and SKA-POP-LRF, respectively.

Figure 2.8, shows P_{SKUF} with different ranges of $Z^c_{t,k}$ for NSFNET and UBN24. It can be observed from the plotted graphs that as the range of $Z^c_{t,k}$ increases, P_{SKUF} increases because more resources get occupied during secret key assignment and reassignment. However, from Figure 2.8, it is evident that P_{SKUF} for the proposed SKA-POP is lower with different ranges of k_{tr}. Thus, using the proposed SKA-POP, maximum number of QKD-LPRs are established successfully. It has been seen from Figure 2.8(a) that the proposed SKA-POP reduces the effect of blocking in QSCh and shows an average reduction of 98.60%, 97.67%, 98.06%, and 87.99% with $Z^c_{t,k} \in$ [4,6] in P_{SKUF} as compared to NP-RWTA, POB-RWTA, PP-RWTA, and SKA-POP-LRF for NSFNET, respectively. Similarly, the minimization in P_{SKUF} of the proposed SKA-POP is 96.02%, 93.40%, 94.53%, and 76.90% with $Z^c_{t,k} \in$ [4,8] as compared to NP-RWTA, POB-RWTA, PP-RWTA, and SKA-POP-LRF for



(a)



(b)

Figure 2.8: Probability of secret key update failure (P_{SKUF}) for total QKD-LPRs with different $Z^c_{t,k}$ and $H_{QKD\text{-}LPR}$: $M_{QKD\text{-}LPR}$: $L_{QKD\text{-}LPR}$ = 1:1:1 QKD-LPR ratio in (a) the NSFNET and (b) the UBN24.

NSFNET, respectively. In Figure 2.8(b), for UBN24, an average reduction of 96.69%, 94.51%, 95.45%, and 42.69% in P_{SKUF} with $Z^c_{t,k} \in$ [4,6] using SKA-POP has been obtained as compared to NP-RWTA, POB-RWTA, PP-RWTA, and SKA-POP-LRF, respectively. It can also be observed from Figure 2.8(b) that an average reduction

in P_{SKUF} of the proposed SKA-POP is 94.22%, 90.44%, 92.10%, and 41.50% with $Z^c_{t,k} \in$ [4,8] as compared to NP-RWTA, POB-RWTA, PP-RWTA, and SKA-POP-LRF, respectively. Thus, the SKA-POP performs better than the other policies to minimize the impact of blocking in the QSCh of QKD-ONs.

2.4 Conclusion

In this chapter, to minimize the impact of blocking in QSCh, an efficient SKA-POP for RRA has been proposed. In the proposed SKA-POP, the QKD-LPRs are categorized into three types, and the different CoQKD-LPRs are prioritized based on their security level, i.e., from HPQKD-LPRs to LPQKD-LPRs (HPQKD-LPRs > MPQKD-LPRs > LPQKD-LPRs). In addition to this, the QKD-LPRs within the CoQKD-LPR are arranged in increasing order of the requested initial secret key time-slots ($Z^c_{t,k}$). The proposed SKA-POP aims to reduce the blocking of QKD-LPRs while maintaining the overall network performance in terms of SP and P_{SKUF}. The performance of the proposed SKA-POP in comparison with the NP-RWTA, POB-RWTA, PP-RWTA, and SKA-POP-LRF is evaluated with different number of wavelengths reserved for QSCh (W_Q) and different ranges of $Z^c_{t,k}$. In order to examine the proposed SKA-POP effectiveness, simulations are performed on two different networks, namely, NSFNET and UBN24. Simulation results indicate that the proposed SKA-POP shows a significant improvement compared to the NP-RWTA, POB-RWTA, PP-RWTA, and SKA-POP-LRF in terms of higher SP and lower P_{SKUF}. However, in QKD-ON, the assignment and reassignment of network resources generate fragmented slots and introduce fragmentation problem, which is critical during RRA. Hence, in the next chapter, the impact of fragmentation while assigning resources during RRA in QKD-ONs is analyzed.

Chapter 3

Impact of Fragmentation in Quantum Signal Channel of QKD-ONs

3.1 Introduction

In the previous chapter, a RRA problem was addressed and a priority ordering policy for different CoQKD-LPRs was designed. In QKD-ONs, to improve the security of the encrypted data, the quantum key should be updated/modified periodically (where the resources in QSCh should be reassigned periodically to update/modify the quantum key of QKD-LPRs). Therefore, the availability of network resources at each updation/ modification during resource reassignment is essential to establish the QKD-LPR with security requirements. However, it has been observed that this diverse assignment and reassignment of network resources of QKD-LPRs generates isolated time-slot(s) and introduces time-slot fragmentation in QSCh of QKD-ONs. In QKD-ONs, fragmentation is one of the serious issues while assigning network resources and can be mitigated through appropriate management of network resources in such networks. Various existing studies [8, 10, 34, 87, 210] addressed the resource assignment problem and developed different RRA strategies for efficient resource

utilization in the QKD-ONs, discussed in Chapter 1. However, time-slot fragmentation has not been given much consideration in accommodating QKD-LPRs with security requirements in QKD-ONs. Furthermore, only a few studies have been conducted on fragmentation [193], which is a new and different problem compared to the memory fragmentation in computer storage [211], and bandwidth fragmentation in elastic optical networks [212, 213]. Time-slot fragmentation in QKD-ONs increases the number of discontinuous time-slots, which are not used for the future incoming QKD-LPRs. Hence, it increases the blocking of QKD-LPRs, thereby minimizing the security of QKD-ONs. Thus, the fragmentation problem in QSCh for QKD-LPRs is necessary to be considered in such networks. Furthermore, efficient assignment of network resources is important to reduce the effect of fragmentation in QSCh of QKD-ONs. In this chapter, the fragmentation problem in QSCh is addressed and a new fragmentation-suppressed routing and resource assignment (FS-RRA) approach is proposed to minimize the effect of fragmentation in QSCh of QKD-ONs. The main contributions of this chapter are as follows:

(i) In this chapter, the issue of time-slot fragmentation in QSCh is addressed, which is a new and important issue in QKD-ONs.

(ii) A FS-RRA approach is proposed to minimize the effect of fragmentation during assignment and reassignment in QSCh.

(iii) The effect of time-slot fragmentation in QSCh is analyzed by using two existing resource assignment approaches and a proposed FS-RRA in terms of the FI_{QSCh}, the $FM_{external}$, BP, and RU.

(iv) Simulation results indicate that the proposed FS-RRA approach performs better than the two existing resource assignment approaches.

3.2 Fragmentation in QSCh of QKD-ONs

Figure 3.1 illustrates an example of time-slot fragmentation in QSCh of the QKD-ONs. Let us assume a scenario where QKD-LPRs of different security levels dynamically arrive and depart from the QKD-ONs. The status of the QLs after diverse resource assignment and reassignment of QKD-LPRs is shown in Figure. 3.1.

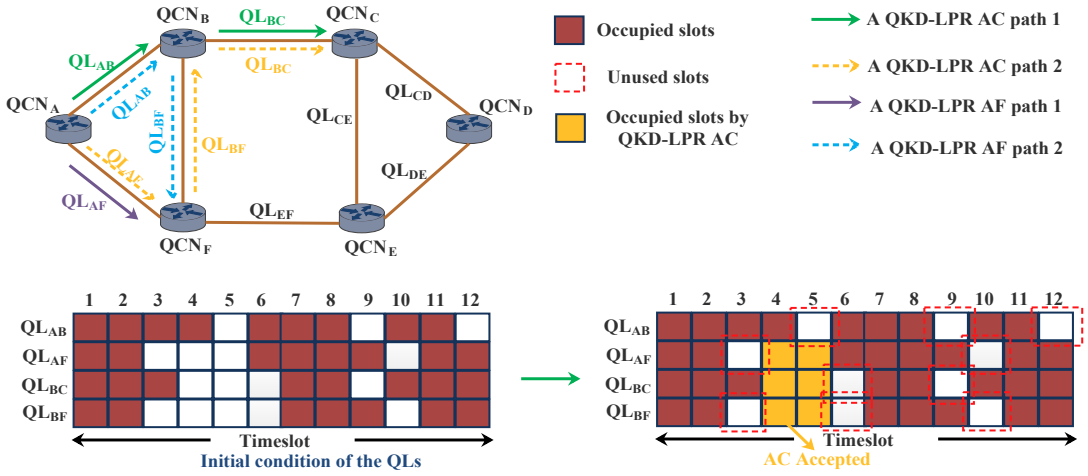


Figure 3.1: An example of time-slot fragmentation in QSCh of the QKD-ONs

Assuming two QKD-LPRs, AC from A (source node) to C (destination node), and AF from A (source node) to F (destination node), arrive in the QKD-ONs. Suppose a QKD-LPR AC selects the shortest path A-B-C from the pre-calculated paths (K_{o_t}, $_{d_t}$) assuming ($K = 2$). It starts performing resource assignment/ reassignment with 2 time-slots requirements on the selected path using the FF resource assignment approach. The requested time-slots on QL_{AB} and QL_{BC} are available; however, the available time-slots on QL_{AB} are fragmented and discontinuous slots {5}, {9}, {12}. Hence, a QKD-LPR AC gets rejected on path A-B-C. Therefore, in order to reduce blocking in the network, a QKD-LR AC selects an alternate path A-F-B-C and checks the availability of time-slots on corresponding QLs to satisfy the requirement. On path A-F-B-C, the requested time-slots without any fragmented slots {4, 5} are available, and hence a QKD-LPR AC is accepted. Furthermore, the assignment/reassignment of network resources for the QKD-LPR AC generates fragmented slots on the corresponding QLs. Specifically, on QL_{AF}, the fragmented

slots are {3}, {10}; on QL_{BF}, the fragmented slots are {3}, {6}, {10} and on QL_{BC}, the fragmented slots are {6}, {9}, shown in Figure 3.1. Due to the presence of these fragmented slots, the upcoming QKD-LPR AF (requires 2 time-slots) gets rejected on both the available paths, namely A-F and A-B-F. Thus in order to improve the acceptance of QKD-LPRs in the network, it is important to consider the effect of fragmentation during the assignment and reassignment.

3.3 Fragmentation-suppressed Routing and Resource Assignment

3.3.1 Network Model

This section describes the QKD network model to evaluate performance of the proposed FS-RRA approach by considering the fragmentation problem in QSCh of QKD-ONs in terms of various performance metrics. Let the physical topology of a connected network be represented by $G(V_Q,\ E_Q,\ W_T,\ W_Q,\ Z_T)$, where V_Q and E_Q represent the QCNs and QLs in the QKD-ON, respectively. Z_T represents the total number of available time-slots on each QL. The W_Q, i.e., the reservation of wavelengths for both the channels (QSCh/PICh) is the same for resource assignment in this work. Moreover, the number of available time-slots, i.e. Z_T, is the same on each QL in the QKD-ONs. A QKD-LPR is modeled as $Q_t(o_t,\ d_t,\ t_{arr},\ t_{upd},\ t_{dep},\ T,\ Z^c_{t,k},\ N^m_{t,k},\ Z^m_{t,k})$, $Q_t \in Q$, where o_t and d_t represents the source and destination QCNs of a QKD-LPR in the QKD-ONs, respectively. $t_{arr},\ t_{upd}$, and t_{dep} represent the arrival time, update time and departure time of a QKD-LPR, respectively. T is the secret key update period of a QKD-LPR. The set of total incoming QKD-LPRs over the QKD-ONs is represented by Q. Let $Z^c_{t,k}$ represents the required number of secret key time-slots for a QKD-LPR creation. The number of times modification required to modify the secret keys of a QKD-LPR is represented by $N^m_{t,k}$. The required number of secret key time-slots for a QKD-LPR modification is represented by $Z^m_{t,k}$ [173]. To

establish QKD-LPR, it is necessary to compute and choose an end-to-end routing path $P_{o_t,\ d_r}$ from source-destination QCNs, and then allocate network resources on each QL along the path $P_{o_t,\ d_t}$ using the proposed resource assignment approach. During assignment and reassignment, QKD-LPR is served if network resources are available on one of the pre-calculated paths ($K_{o_t,\ d_t}$). Otherwise, the QKD-LPR is blocked.

3.3.2 Fragmentation-suppressed Routing and Resource Assignment Approach

This section explains the concept of the proposed fragmentation suppressed routing and resource assignment/ reassignment approach based on the closest available time-slots criterion. The proposed approach is intended to reduce the number of unused time-slots, which prevents the time-slot fragmentation problem in QSCh of the QKD-ON.

In the proposed FS-RRA approach, the K-shortest path routing algorithm is used to find and compute all the possible shortest paths from the source node to the destination node of the QKD-LPR. For routing, the proposed approach selects a shortest path from all the possible available paths based on the QL counts $QL_j \epsilon E_Q$, where QKD-LPR will utilize less number of QLs to establish the connection from source to destination node. This results in the establishment of more QKD-LPRs in the QKD-ONs. However, in order to reduce blocking in the network, if sufficient resources during resource assignment and reassignment are not available on the first shortest path, then the next shortest path is selected from the pre-calculated paths ($K_{o_t,\ d_t}$). For simplicity, let us assume that a QKD-LPR AC arrives in the network and the $K_{o_t,\ d_t}$ (assume $K = 3$) of AC are *A-B-C*, *A-F-B-C*, and *A-F-E-C*. According to the abovementioned routing criterion, a path *A-B-C* is selected because it contains fewer QLs than the other two pre-calculated paths. However, if sufficient resources on $P_{o_t,\ d_t}$ during resource assignment and reassignment are not available, then a path from other two $K_{o_t,\ d_t}$, i.e., *A-F-B-C*, and *A-F-E-C* is selected.

Algorithm 2 The Proposed FS-RRA Approach

Input: $G(V_Q,\ E_Q,\ W_T,\ W_Q,\ Z_T)$, Q, $Q_t(o_t,\ d_t,\ t_{arr},\ t_{upd},\ t_{dep},\ Z^c_{t,k},\ N^m_{t,k},\ Z^m_{t,k})$, *k-paths*

Output: FI_{QSCh}, $FM_{external}$, BP, RU

initialize $FI_{QSCh} = 0$, $FM_{external} = 0$, $BP = 0$, $RU = 0$;
for $Q_t \leftarrow 1$ to $|Q|$ **do**
    Find all possible available paths between o_t to d_t
    Select the first *k-paths*, where $k \in K_{o_t,\ d_t}$, as fixed paths from pre-calculated paths
    Arrange the selected paths in increasing order of their path length
    Search a routing path ($P_{o_t,\ d_t}$) for Q_t from selected paths
    Search the available resources on each QL along the $P_{o_t,\ d_t}$
    if $P_{o_t,\ d_t}$ of Q_t contains resources **then**
        Perform resource assignment using Algorithm 2
        if resource assignment is successful **then**
            Q_t is ACCEPTED
        else
            Q_t is REJECTED
        end if
    end if
    if Q_t requires modification **then**
        Search the available resources on each QL along the $P_{o_t,\ d_r}$
        if $P_{o_t,\ d_t}$ of Q_t contains resources during modification **then**
            Perform resource reassignment using Algorithm 2
            if resource reassignment is successful **then**
                Q_t is ACCEPTED
            else
                Q_t is REJECTED
            end if
        end if
    else
        No resource reassignment
        if more modification is required **then**
            follow *Step 16*
        end if
    end if
    return FI_{QSCh}, $FM_{external}$, BP, RU
end for

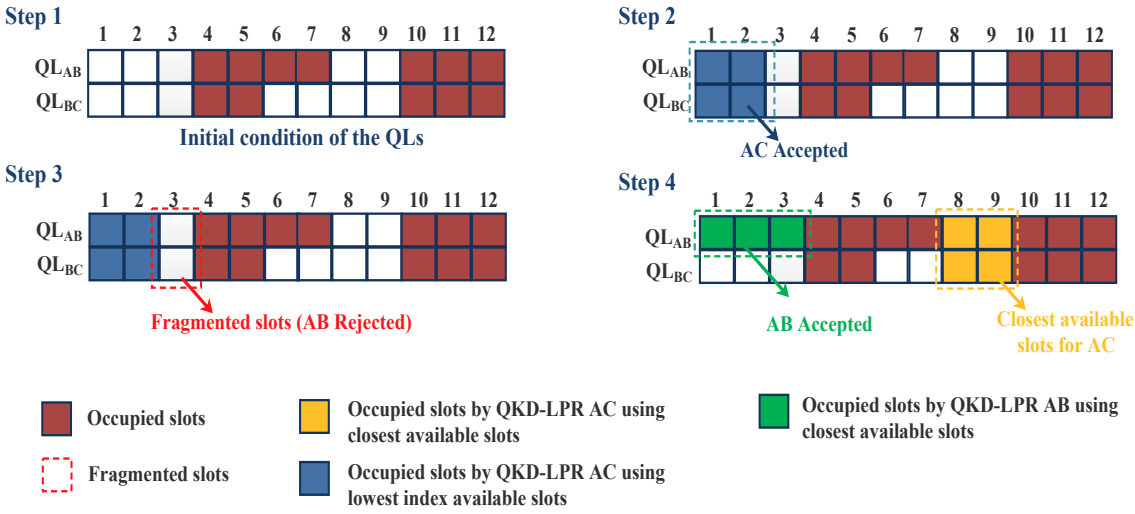


Figure 3.2: The concept and motivation of using the closest slots for resource assignment and reassignment

Algorithm 3 QKD-LPR Assignment/Reassignment

Input: QKD-LPR ($Q_t(o_t,\ d_t,\ t_{arr},\ t_{upd},\ t_{dep},\ Z^c_{t,k},\ N^m_{t,k},\ Z^m_{t,k})$)
Output: Resource assignment/reassignment

1: Check the QKD-LPR resource requirement during assignment/reassignment
2: Search the requested available slots on $P_{o_t,\ d_t}$ and find out the initial indices of the available slots
3: **if** closest or equal available slots are found to the $Z^c_{t,k}$, and $Z^m_{t,k}$ demand **then**
4: Assigned the available slots to the QKD-LPR
5: **else**
6: Q_t is REJECTED
7: **end if**

Besides path computation, the proposed FS-RRA performs resource assignment and reassignment during the creation and modification of QKD-LPRs, respectively. In this approach, the QKD-LPR utilizes the closest available time-slot criterion to search for the availability of resources on the corresponding QLs. In this proposed resource assignment criterion, the QKD-LPR searches the requested available time-slots on the selected routing path $P_{o_t,\ d_t}$ and finds the initial indices of the available time-slots. If the closest time- slots to $Z^c_{t,k}$ during assignment, and $Z^m_{t,k}$ during reassignment are available on the selected routing path $P_{o_t,\ d_t}$, then the resources are assigned to the QKD-LPR. The motivation behind selecting this criterion is to prevent small discontinuous or isolated available resources that might be difficult to

use for future QKD-LPRs.

Figure 3.2 illustrates the concept and motivation of using the closest slots for resource assignment and reassignment. The initial condition of the QLs (QL_{AB} and QL_{BC}) after diverse resource assignment and reassignment is shown in *Step 1* of Figure 3.2. Suppose a QKD-LPR AC arrives in the network, selects a path A-B-C from the $K_{o_t,\ d_t}$ and requires 2 time-slots for establishment. After path selection, the AC searches for available time-slots on the corresponding QLs to establish a connection between source node A and destination node C, as shown in *Step 2* of Figure 3.2. However, it has been observed that assigning time-slots based on the criterion of lowest index availability creates fragmented slots on the selected routing path $P_{o_t,\ d_t}$ of the AC, as shown in *Step 3*. This results in increasing blocking of future QKD-LPRs in the QKD-ONs and degrade the network performance. For example, if QKD-LPR AB arrives after QKD-LPR AC in the network and requires 3 time-slots for establishment. However, due to the presence of discontinuous/isolated time-slots in the corresponding QL of the selected path A-B, QKD-LPR AB gets rejected, as shown in *Step 3* of Figure 3.2. Therefore, in the proposed approach, the resources are assigned using the closest available time-slots criterion to suppress the effect of fragmentation during assignment/reassignment in QKD-ONs. In *Step 4* of Figure 3.2, the closest available time-slots criterion is used to assign resources for QKD-LPR AC that prevents the small discontinuous or isolated available resources. Furthermore, the requested time-slots for the future QKD-LPR AB are available. Hence, both the QKD-LPRs AC and AB gets accepted using the proposed criterion.

The complete algorithm of FS-RRA approach for routing and resource assignment/reassignment in QSCh of QKD-ONs is shown in Algorithm 2 and Algorithm 3.

3.4 Performance Evaluation

In this section, the effect of time-slot fragmentation in the QSCh is analyzed by comparing two existing resource assignment approaches with the proposed FF-RRA approach in terms of the FI_{QSCh}, $FM_{external}$, BP, and RU. In this chapter, two network topologies viz, NSFNET (14 nodes and 22 links) and UBN24 (24 nodes and 43 links) are used for simulations. A short-distance QKD network, where the maximum distance between the two end nodes in the QKD network is less than the distance that can accomplish the point-to-point QKD mechanism is considered.

Assume 80 wavelengths with 50 GHz channel spacing for TDCh, QSCh, and PICh. Consider a specific number of wavelengths reserved for QSCh, and according to reserved wavelengths, the available secret key time-slots (Z_T) on each QL are varied. For QSCh, less number of resources are reserved because if the number of resources is increased for security in QSCh, then there will be fewer resources available for data transmission in TDCh. In this chapter, the dynamic traffic scenario is considered in which QKD-LPRs of different security levels are randomly generated between the source QCN and destination QCN following Poisson distribution in QKD-ONs for each simulation run. The implementation of QKD network model, QKD-LPR model, and simulations are performed in Python.

3.4.1 Measurement of Security-Level Dependent Time-Slot Fragmentation (Fragmentation Metrics)

Previously, file system fragmentation in computer storage [211] and bandwidth fragmentation in EONs [212] were calculated by using the bandwidth fragmentation ratio defined in [211]. This subsection discusses the metrics, i.e., FI_{QSCh}, $FM_{external}$, BP, and RU that are used to measure time-slot fragmentation in QSCh of QKD-ONs.

3.4.1.1 QSCh Fragmentation Index (FI_{QSCh})

Let F_{QL_b} be a slot block of isolated/discontinuous time-slots and $S_{F_{QL_b}}$ be the number of available time-slots in a slot block F_{QL_b}, in each QL. The QL fragmentation index (FI_{QL}) is defined as the ratio of the sum of available slot blocks to the sum of time-slots in all the available slot blocks in each QL. The QL fragmentation index (FI_{QL}) is expresses as:

$$FI_{QL} = \frac{\sum_{b=1}^{i} F_{QL_b}}{\sum_{b=1}^{i} S_{F_{QL_b}}} \tag{3.1}$$

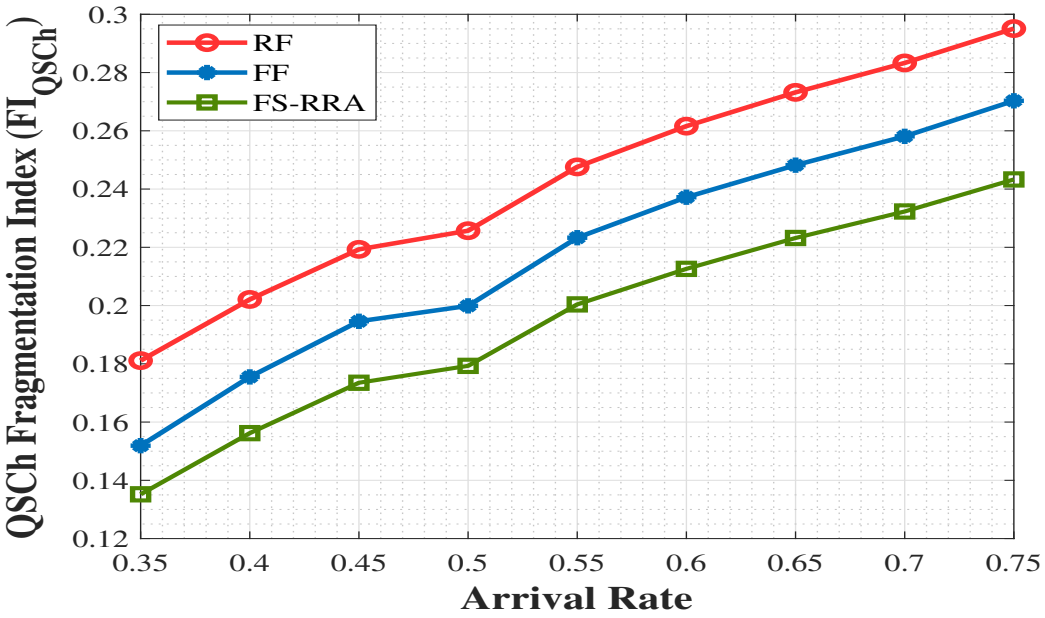
where i is the largest number of a F_{QL_b}. The QSCh fragmentation index (FI_{QSCh}) is determined by calculating the mean of FI_{QL} and can be express as:

$$FI_{QSCh} = mean(FI_{QL}) \tag{3.2}$$

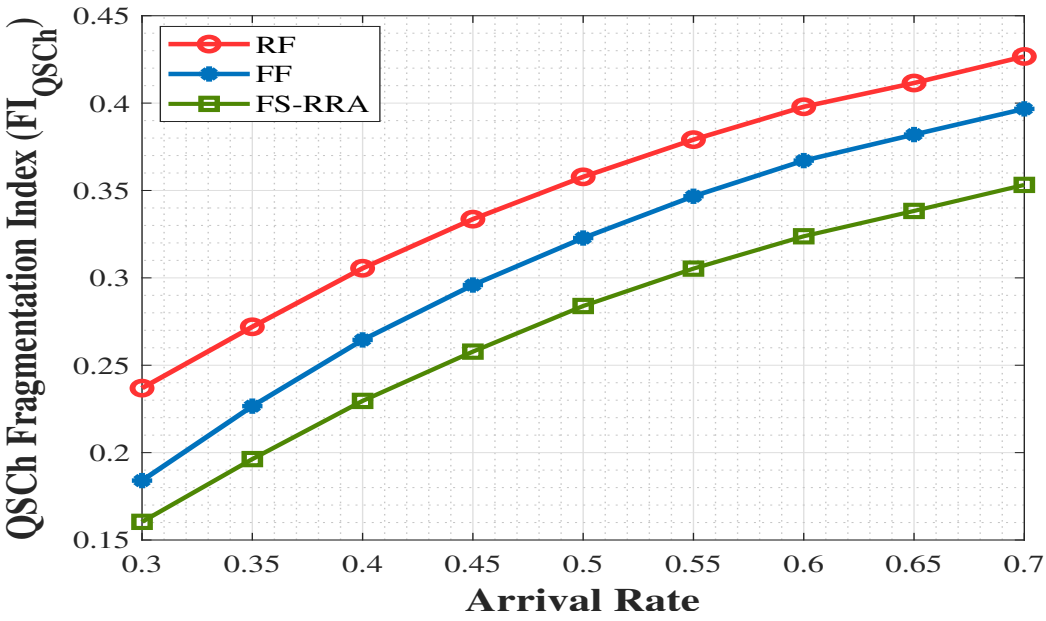
Figure 3.3 (a) and Figure 3.3 (b) show performance of the proposed FS-RRA approach and the two existing approaches in terms of the FI_{QSCh} versus traffic arrival rate for NSFNET and UBN24, respectively. FI_{QSCh} indicates the availability of non-isolated time-slots for QKD-LPRs. A lower FI_{QSCh} value means that more non-isolated time-slots are available to establish QKD-LPR. The FI_{QSCh} increases with an increase in traffic arrival rate. This is because as traffic arrival rate increases, the availability of time-slots decreases. However, the proposed FS-RRA shows the lowest FI_{QSCh} among the two existing approaches, shown in Figure 3.3. In Figure 3.3 (a), for NSFNET, the average reduction in FI_{QSCh} for the proposed FS-RRA is 12.11% and 21.54% compared to the FF and RF, respectively. Similarly, in Fig 3.3 (b), for UBN24, the average FI_{QSCh} of the proposed approach is reduced by 10.34% and 19.77% as compared to FF and RF, respectively.

3.4.1.2 External Fragmentation ($FM_{external}$)

Let $max(S_{F_{QL_b}})$ be the maximum number of available contiguous time-slot and S be the total number of available contiguous time-slot, in each QL. The QL external



(a)



(b)

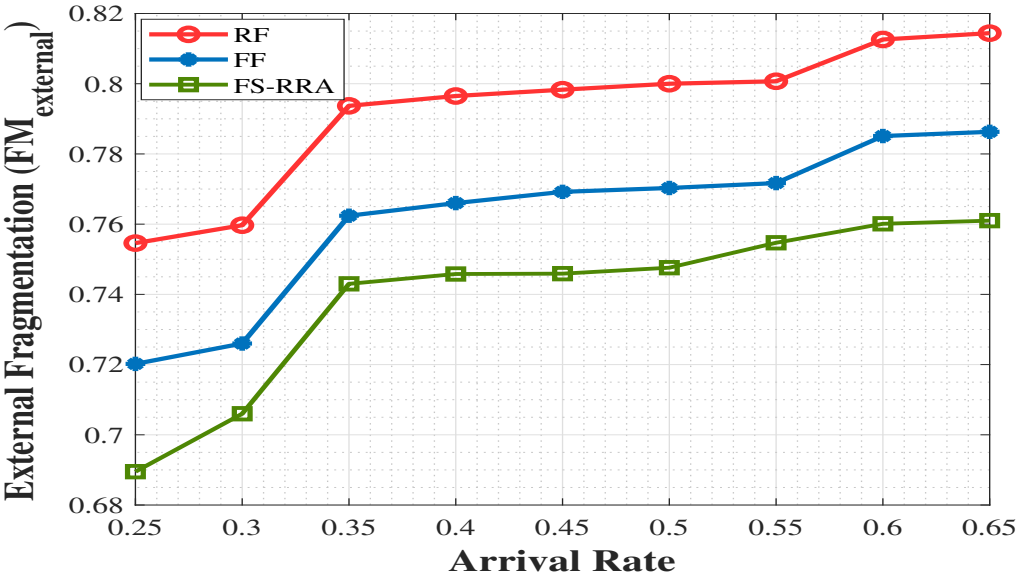
Figure 3.3: QSCh fragmentation index (FI_{QSCh}) versus traffic arrival rate (a) in the NSFNET and (b) in the UBN24.

fragmentation metric ($FM_{external_{QL}}$) is defined as:

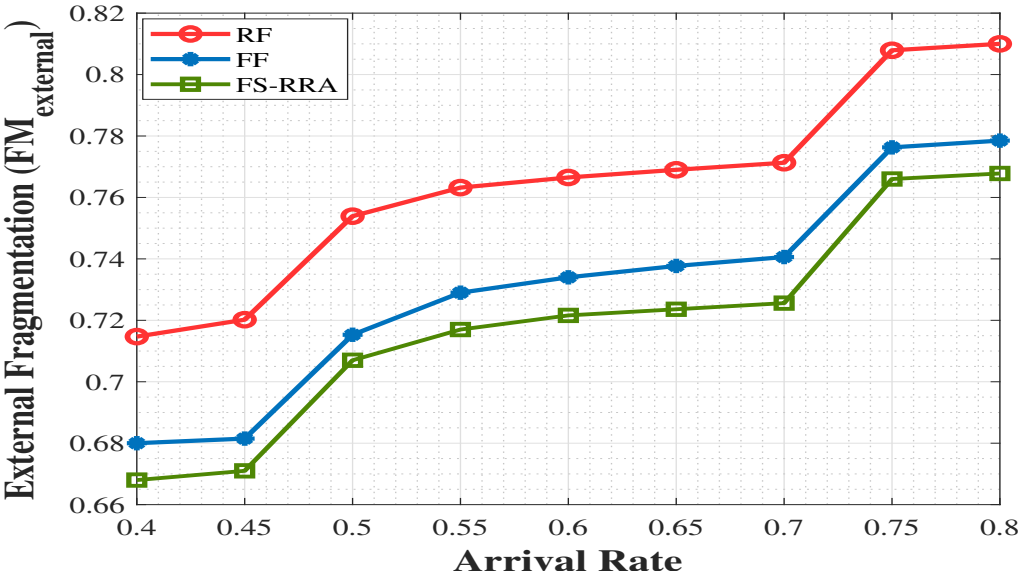
$$FM_{external_{QL}} = 1 - \frac{max(S_{F_{QL_b}})}{S} \tag{3.3}$$

The External Fragmentation Metric ($FM_{external}$) is determined by calculating the mean of $FM_{external_{QL}}$ and can be express as:

$$FM_{external} = mean(FM_{external_{QL}}) \tag{3.4}$$



(a)



(b)

Figure 3.4: External Fragmentation Metric ($EF_{external}$) versus traffic arrival rate (a) in the NSFNET and (b) in the UBN24.

Figure 3.4 (a) and Figure 3.4 (b) show the $FM_{external}$ versus arrival rate for NSFNET and UBN24, respectively. It can be observed from Figure 3.4 that the proposed FS-RRA outperforms the two existing approaches in terms of $FM_{external}$, reducing the number of unused time-slots in the network. The lower value of

$FM_{external}$ indicates a lower time-slot fragmentation in QSCh of QKD-ONs. The value of $FM_{external}$ increases with an increase in arrival rate. However, from Figure 3.4 (a), it has been observed that the proposed reduces the average $FM_{external}$ by 2.97% and 6.69% compared to FF and RF for NSFNET, respectively. Similarly, for UBN24, the average reduction in $FM_{external}$ for the proposed approach is 1.77% and 5.91% compared to FF and RF, respectively, shown in Figure 3.4 (b).

3.4.1.3 Blocking Probability (*BP*)

The ratio of total rejected QKD-LPRs during resource assignment and reassignment ($Q_{t_{REJ}}$) to the total incoming QKD-LPRs in the QKD-ONs is *BP*.

$$BP = \frac{Q_{t_{REJ}}}{\sum_{n=1}^{N} Q_{t_n}} \tag{3.5}$$

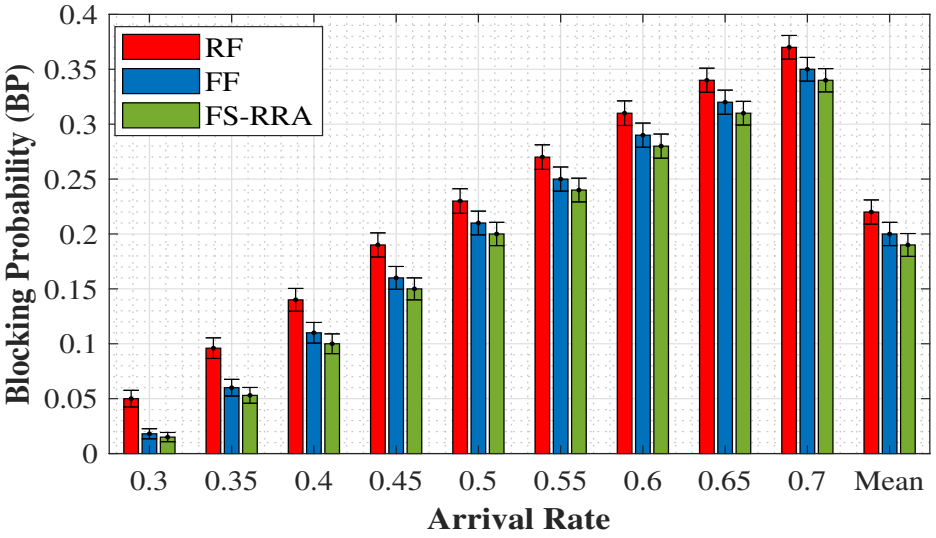
where N is the maximum value of the QKD-LR.

3.4.1.4 Resource Utilization (*RU*)

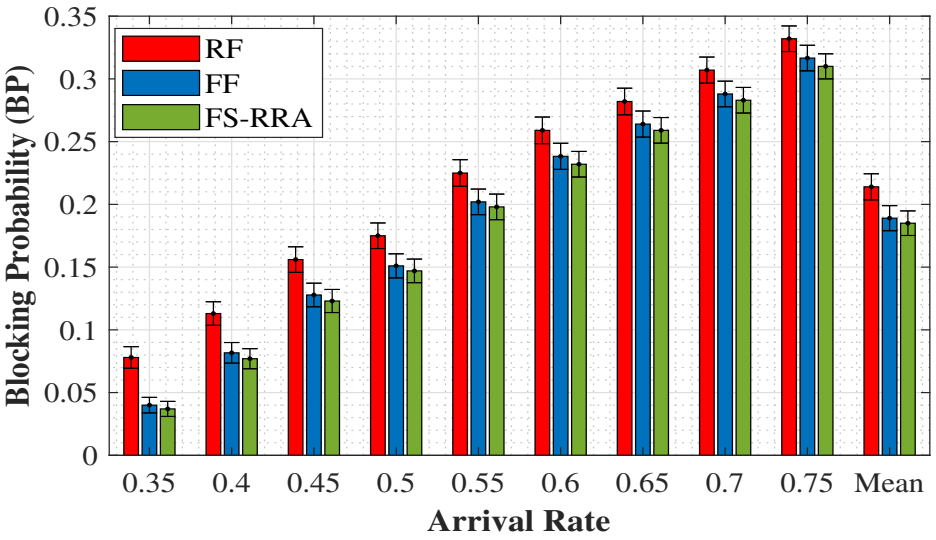
The ratio of total resource utilized by QKD-LPRs during resource assignment and reassignment (z_{UTL}) to the total resources available in the QKD-ONs is *RU*.

$$RU = \frac{z_{UTL}}{Z_T} \tag{3.6}$$

Figure 3.5 (a) and Figure 3.5 (b) show the *BP* of QKD-LPRs versus traffic arrival rate for NSFNET and UBN24 with 95% confidence interval, respectively. The *BP* of QKD-LPRs increases as traffic load increases in the network. This is because of the fact that as traffic load increases, the availability of network resources decreases for the future incoming QKD-LPRs. However, the *BP* of the proposed FS-RRA approach is lower than the two existing approaches. For NSFNET, the proposed FS-RRA approach achieved an average reduction in *BP* of 4.03% and 14.28% compared to FF and RF, respectively, as shown in Figure 3.5 (a). Similarly, for UBN24, the average *BP* of the proposed approach is reduced by 2.61% and 13.44% as compared



(a)

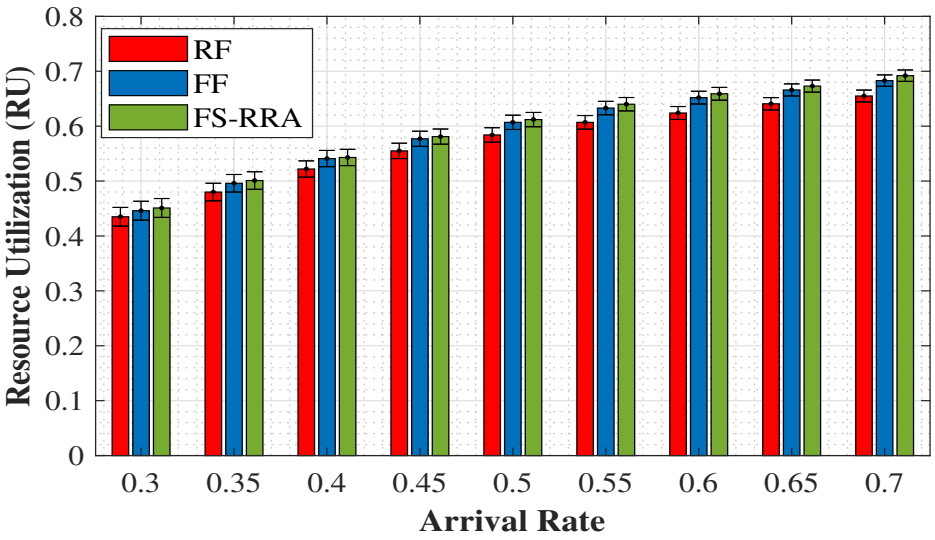


(b)

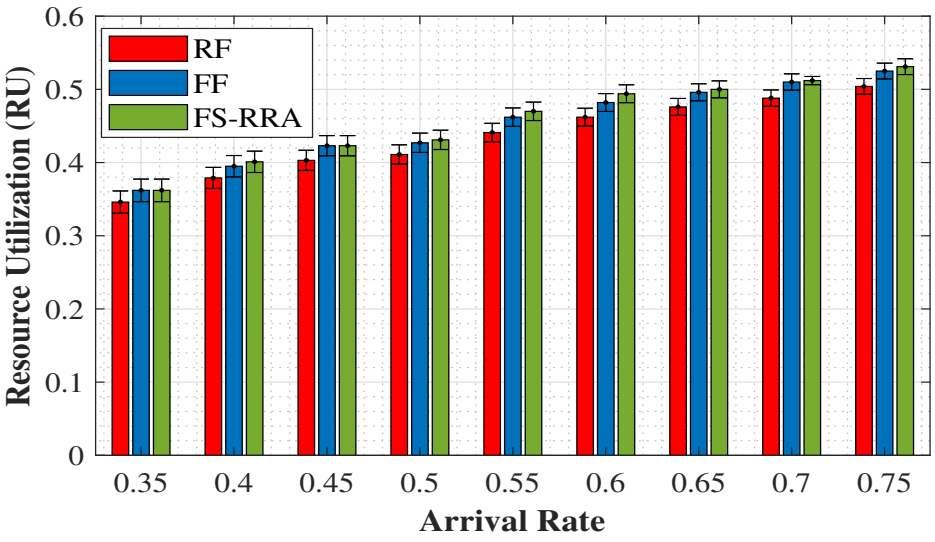
Figure 3.5: Blocking Probability (BP) versus traffic arrival rate (a) in the NSFNET and (b) in the UBN24.

to FF and RF, respectively as shown in Figure 3.5 (b). It can be observed from the Figure 3.5 (a) and Figure 3.5 (b) that with 95% confidence interval, the BP for the proposed FS-RRA, FF, and RF approaches is somewhere between the upper and lower values of the confidence interval.

Figure 3.6 (a) and Figure 3.6 (b) illustrate the performance of the proposed FS-RRA approach and the two existing approaches in terms of RU versus traffic arrival rate for NSFNET and UBN24 with 95% confidence interval, respectively. The RU of the proposed approach as well as the existing approaches increases with the in-



(a)



(b)

Figure 3.6: Resource Utilization (RU) versus traffic arrival rate (a) in the NSFNET and (b) in the UBN24.

crease in the traffic load. This is because as traffic load increases, more resources are occupied/utilized by the QKD-LPRs in the network, resulting in less blocking. Compared to the FF and RF, the proposed approach achieves an average improvement in RU of 3.44% and 5.96% for NSFNET, respectively, shown in Figure 3.6 (a). Similarly, for UBN24, the average improvement in RU of 3.08% and 7.64% is achieved by the proposed approach compared to FF and RF, respectively, shown in Figure 3.6 (b). It can be observed from the Figure 3.6 (a) and Figure 3.6 (b) the estimate of RU for proposed FS-RRA, FF, and RF approaches will lie between the

upper and lower values of the confidence interval.

3.5 Conclusion

In this chapter, the impact of QSCh fragmentation problem in the QKD-ONs is analyzed and a FS-RRA approach for QSCh of QKD-ONs is proposed. The proposed FS-RRA approach aims to reduce the blocking of QKD-LPRs by suppressing the effect of fragmentation due to diverse resource assignment and re-assignment in QSCh. Simulations have been performed on two different networks, namely NSFNET and UBN24, to examine the effectiveness of the proposed FS-RRA approach. The proposed FF-RRA approach has been compared with two existing resource assignment approaches, i.e., the FF and the RF. Simulation results indicate that the proposed FS-RRA approach performs better than the other two existing resource assignment approaches in terms of the FI_{QSCh}, $FM_{external}$, BP, and RU. However, such heuristics focus only on local conditions, which does not allow the algorithm to make more informed decisions that take the entire network into consideration. Hence, the next chapter addresses the RRA problem of QKD-ONs in dynamic traffic scenarios by leveraging DRL, which can intelligently solve decision-making problems in complex networking environments.

Chapter 4

Deep Reinforcement Learning Based Routing and Resource Assignment in QKD-ONs

4.1 Introduction

In the previous chapters, a priority ordering policy for different CoQKD-LPRs was designed, the impact of fragmentation in QSCh of QKD-ONs was analyzed and a new approach was proposed to suppress the effect of fragmentation. However, the conventional schemes (baseline schemes) rely on fixed policies and use the predetermined algorithms to find the path and allocate resources on the selected path. Hence, such schemes are not suitable for solving complex decision making problems. Therefore, in this chapter, the DRL method is exploited to solve the RRA problem and a DRL-based RRA scheme is proposed. The proposed scheme learns the optimal policy to select an appropriate route and assign suitable network resources for establishment of QKD-LPRs by using deep neural networks (DNNs).

In the recent years, comprehensive research has been conducted on different networking challenges of QKD-ONs [34, 170, 171, 214]. To solve the RRA problem of QKD-ONs various schemes have been proposed in the literature [8, 34], discussed

in Chapter 1. However, as the dynamicity increases, performance of the existing strategies becomes inefficient as these rely on fixed policies that focus on the immediate optimization goals for the current network state and are unable to achieve the optimal solution to solve the dynamic RRA problem of QKD-ONs. Inspired by the recent advances in artificial intelligence (AI) /machine learning (ML), which allow systems/machines to learn from historical data and make predictions to solve decision-making problems, this work explored the capability of different options available in AI/ML. Typically, ML requires data labeling to identify the raw data, and add meaningful and informative labels that help the ML model to learn. In ML, the aim of training or validating the model with a labeled dataset is sometimes referred to as "ground truth." However, in this chapter, the RRA problem is a complex decision-making problem (because of the diverse assignment and reassignment (during QKD-LPR modification because of unique key updation/modification feature) of network resources for establishment of QKD-LPR) and also the mapping of input and output variables or labeling of data is not feasible as it is based on the observation of QKD-ON's environment conditions.

Recently, reinforcement learning (RL), one of the most important subfields of ML, has received extensive research attention as it is a feedback-based ML method. In RL, an agent continuously interacts with the environment to make decisions, observe the results of decisions, and then automatically adjust its strategy based on the feedback of the previous decision to achieve the optimal/best policy. However, RL, a learning process, is inapplicable and unsuitable for large and complex networks because it takes a lot of time to reach the optimal/best policy as it has to explore and learn about the whole system. As a result, RL's applications are quite limited in practice. Deep learning (DL) has recently been introduced as a new groundbreaking method and has potential to overcome the limitations of RL. DL helps to design complex environments and extract important features, thereby reducing computation complexity. DL is implemented using Neural Networks, thus opening a new era for improving the RL algorithms' learning process. This combined form of

RL and DNNs is known as DRL. DRL has ability to approximate optimal policy by employing DNNs for complex decision-making problems and improves the learning speed and performance of the reinforcement learning algorithms. As a result, the application of DRL [215, 216] has received intensive research interest in communication and networking to solve the complex decision-making problems [217] and has become one of the most active areas of research in ML. However, in QKD-ONs limited works have been reported using the application of DRL to address the RRA problem [176, 218]. The main contributions of this chapter are as follows:

(i) The DRL method is exploited to address the RRA problem in QSCh of QKD-ONs.

(ii) A RRA scheme based on DRL to select an optimal route and allocate suitable network resources during assignment and reassignment is proposed in this chapter.

(iii) The performance of the proposed DRL-based RRA scheme is compared with the deep-Q network (DQN) method and the two baseline schemes, namely, FF and RF.

(iv) Simulation results demonstrated that the proposed DRL-based RRA scheme outperforms the DQN and the two baseline schemes in terms of BP and RU for both the considered networks.

4.2 DRL-based Routing and Resource Assignment in QKD-ON

4.2.1 Network Model

The network topology of QKD-ON is modeled as $G(V_Q, E_Q, W_T, W_Q, Z_T)$, where V_Q and E_Q are the sets of QKD-ON nodes and links, respectively. W_T and W_Q denotes the total attainable wavelengths on each link and the number of wavelengths

reserved for QSCh in the QKD-ONs, respectively. The total number of attainable time-slots on each QL is denoted by Z_T. Moreover, the number of attainable time-slots, i.e., Z_T, is the same on each QL in the QKD-ONs for this chapter. A QKD-LPR is modeled as $Q_t(o_t,\ d_t,\ t_{arr},\ t_{upd},\ t_{dep},\ T,\ Z^c_{t,k},\ Z^m_{t,k},\ Z^a_{t,k,i},\ Z^b_{t,k,i})$, $Q_t \in Q$. o_t and d_t denote the source and destination node of a QKD-LPR, respectively. The arrival, update and departure time of a QKD-LPR are represented by t_{arr}, t_{upd} and t_{dep}, respectively. T is the secret key update period of a QKD-LPR. A set of total incoming QKD-LPRs over the QKD networks is represented by Q. Then, the number of specific QKD-LPRs (Q_s) can be determined by the expression as:

$$|Q_s| = \frac{|V_Q| * (|V_Q| - 1)}{2} \tag{4.1}$$

where $|V_Q|$ represents the total number of QKD-ON nodes in the network.

Let $Z^c_{t,k}$ and $Z^m_{t,k}$ denote the required number of secret key time-slots for a QKD-LPR creation and modification, respectively. $Z^a_{t,k,i}$ and $Z^b_{t,k,i}$ represent the sizes and initial indices of all the available I time-slot blocks on the corresponding QLs. To establish Q_t, it is required to compute and select an end-to-end routing path P_{o_t,d_t} from source-destination QKD-ON nodes and allocate network resources on each QL along the selected path P_{o_t,d_t} using the proposed DRL-based RRA scheme. QKD-LPR is served if network resources are available on one of the pre-calculated paths $(K_{o_t,\ d_t})$ during assignment and reassignment, else QKD-LPR is blocked.

4.2.2 DRL-based Routing and Resource Assignment Scheme

This subsection discusses the concept of a proposed DRL-based RRA scheme, where the objective is to maximize the number of QKD-LPRs, while reducing blocking and efficiently utilizing network resources.

The proposed DRL-based RRA scheme jointly addresses the routing and resource assignment problem of QSCh. In this scheme, for routing, the DRL agent selects an optimal path based on the hop counts $H_t \in H$, where QKD-LPR will utilize less number of links, thereby resulting in more accommodation of QKD-LPRs in QKD-

ONs. The resources on the selected path $P_{o_t,\ d_t}$ will be assigned using I candidate of DRL-based RRA scheme. In this chapter, I candidate describes the process of assigning resources to QKD-LPR on the selected path $P_{o_t,\ d_t}$ during assignment and reassignment. The I candidate of DRL-based RRA scheme selects the closest available time-slots to $Z^c_{t,k}$ during assignment (for QKD-LPR creation) and $Z^m_{t,k}$ during reassignment (for QKD-LPR modification). The reason is that the selection of the closest available time-slots reduces the wastage of network resources and enhances the possibilities of the available resources for the upcoming QKD-LPRs in the QKD-ONs, hence results in lower blocking of QKD-LPRs.

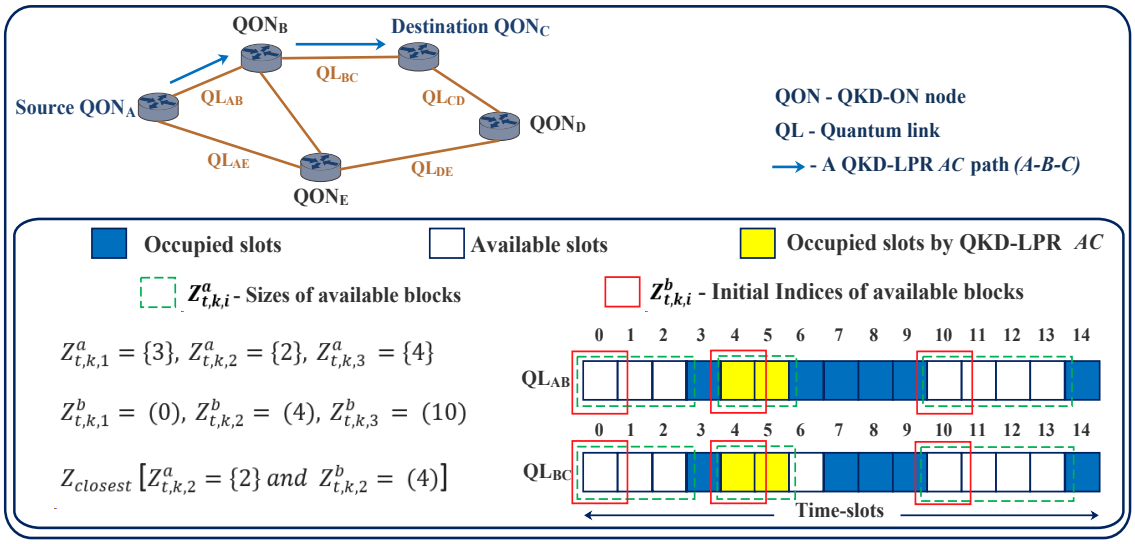


Figure 4.1: An illustration of I candidate of the proposed DRL-based RRA

For ease of understanding, Figure 4.1 depicts the steps of I candidate of the proposed DRL-based RRA scheme during assignment. Consider a scenario in which a QKD-LPR AC arrives in the QKD-ON from the source node A to the destination node C, requires two time-slots for assignment, and selects the best path A-B-C out of the pre-calculated K paths (Assume K=3, then $K_{o_t,\ d_t}$ for a QKD-LPR AC $(K_{A,\ C})$ are A-B-C, A-E-D-C, A-E-B-C), as shown in Figure 4.1. The I candidate of the proposed DRL-based RRA scheme first calculates the size and initial index of the all the available of all the available I time-slot blocks on the corresponding QLs, i.e., $Z^a_{t,k,i}$ and $Z^b_{t,k,i}$, where i represents the number of available I time-slot blocks of

the selected path *A-B-C*, respectively. As shown in Figure 4.1, the calculated sizes ($Z^{a}_{t,k,i}$ (represented with the green dashed box in Figure 4.1)) and initial indices ($Z^{b}_{t,k,i}$ (represented with the red box in Figure 4.1)) of all the available I time-slot blocks are $Z^{a}_{t,k,1}$={3}, $Z^{a}_{t,k,2}$={2}, $Z^{a}_{t,k,3}$={4}, and $Z^{b}_{t,k,1}$= (0), $Z^{b}_{t,k,2}$= (4), $Z^{b}_{t,k,3}$=(10), respectively. Based on the above mentioned criterion of the resource assignment and reassignment, the I candidate finds one of the closest I time-slot blocks represented by $Z_{closest}$, and assigns it to the QKD-LPR AC on the selected path *A-B-C*. In the above example, the $Z_{closest}$ on the basis of size, is $Z^{a}_{t,k,2}$={2}, and its initial index is $Z^{b}_{t,k,2}$= (4) for the assignment of QKD-LPR AC (time slots filled with yellow colour), as shown in Figure 4.1. During reassignment, similar steps of I candidate of the proposed DRL-based RRA have been followed to improve the security level of QKD-LPR in QKD-ONs.

4.2.3 DRL Framework for Routing and Resource Assignment

This subsection describes the working principle of DRL framework to address the RRA problem of QKD-ONs.

Figure 4.2 illustrates the working principle of DRL-based RRA scheme for QKD-ONs. When the SDN controller receives a QKD-LPR Q_t, it fetches the state representation, which includes the in-service QKD-LPRs, network topology, and resource utilization information. The fetched information is fed into the DRL through a feature engineering module *(represented with a dashed red line in Figure 4.2)*, which generates customized state s_t, where s_t represents the environment's state *(Step 1)*. The DNN of DRL-based RRA reads the generated customized state data and takes action $a_t \in A$, where A is a definite action space. The DRL agent takes action according to the RRA policy $\pi_t(A|s_t, \theta)$, where A in this case is a set of RRA schemes for Q_t (where resources are assigned using the steps of I candidate of DRL-based RRA scheme (discussed in Section 4.2 (4.2.2))) and set of DNNs' parameters is represented by θ. A policy π_t of RRA scheme generates a probability distribution over

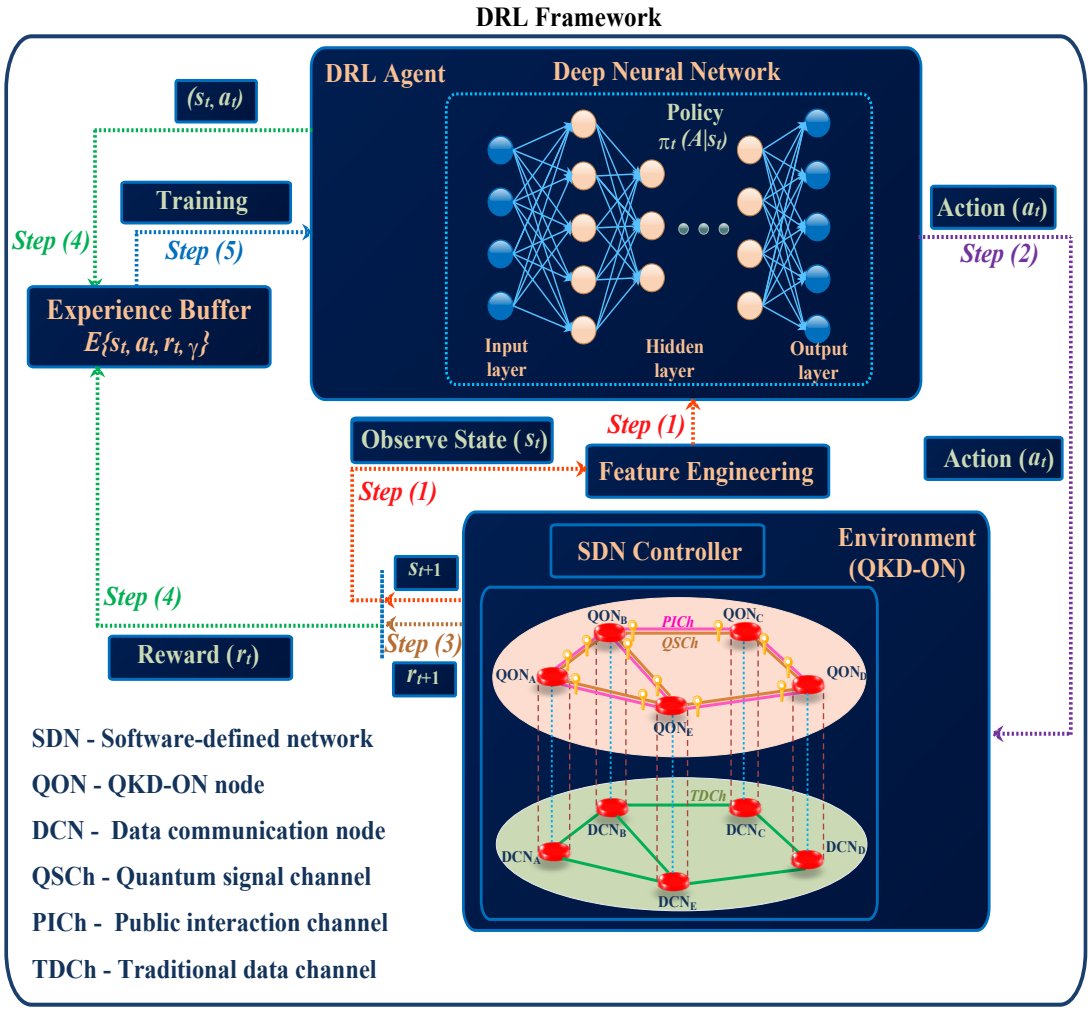


Figure 4.2: An illustration of the proposed DRL framework for RRA in QKD-ONs

A. The SDN controller selects an action $a_t \in A$ based on the probability distribution and sets up the corresponding Q_t *(represented with a dashed purple line in Figure 4.2) (Step 2).* A reward system produces an immediate reward r_t for DRL-based RRA by receiving feedback from the previous RRA operation *(represented with a dashed brown line in Figure 4.2) (Step 3).* An experience E, a tuple $\{s_t, a_t, r_t, \gamma\}$ is stored in an experience buffer *(a dashed green line represents this action in Figure 4.2) (Step 4)* which will be used for training the DNN *(represented with a dashed blue line in Figure 4.2) (Step 5)* in order to achieve the optimal policy, where $\gamma \in [0, 1]$ is a discount factor. The objective of DRL framework for RRA is to maximize

the discounted cumulative reward G_t, which is defined as:

$$G_t = \sum_{j=0}^{\infty} \gamma^j \cdot \pi(a|\ s_{t+j})\ R(s_{t+j},\ a) \tag{4.2}$$

4.3 Modeling and Training

This section first introduces DRL-based RRA modeling which includes definitions of state representation, action, and reward, and then explains the training mechanism.

4.3.1 Modeling

4.3.1.1 State

The state s_t is defined as a vector, expressed in Eq. (4.3). It contains information of Q_t and the current network resource utilisation state, as well as key feature of the I candidate of DRL-based RRA to provision Q_t during assignment and reassignment. When the number of possible pre-calculated paths $(K_{o_t,\ d_t})$ between o_t and d_t is smaller than K, assign $\{\{Z^a_{t,k,i},\ Z^b_{t,k,i}\}|_{i\in[1,I]},\ Z^c_{t,k},\ Z^m_{t,k},\ Z^{Total}_{t,k}|_{k\in[1,K]}\}$ as an array of -1 $(\forall k > K_{o_t,\ d_t})$ in order to maintain the state's s_t format consistent.

$$s_t = \{o_t,\ d_t,\{\{Z^a_{t,k,i},\ Z^b_{t,k,i}\}|_{i\in[1,I]},\ Z^c_{t,k},\ Z^m_{t,k},\ Z^{Total}_{t,k}|_{k\in[1,K]}\}\} \tag{4.3}$$

4.3.1.2 Action

For each Q_t to be served, the DRL agent selects a routing path from the pre-calculated candidate paths (K) and performs resource assignment and reassignment according to the I candidate of DRL-based RRA on the selected path. Therefore, the action space A includes $K.I$ actions.

4.3.1.3 Reward

The designed reward function $R(s_t,\ a_t)$, depends on two factors, i.e., successful provision of Q_t and hop counts of selected path P_{o_t,d_t}. DRL-based RRA receives

an immediate positive reward r_t=+X on successful provisioning of Q_t, otherwise r_t=−X. Additionally, more positive rewards will be received if agent selects a path having less hop counts.

4.3.2 Training

In this chapter, DRL algorithm, namely, proximal policy optimization (PPO) [219], is used for training RRA. A DQN method [220] is also utilized to compare the proposed DRL-based RRA scheme based on PPO. DQN algorithms employ Q-learning to determine the best action to be taken in a given state, and a deep neural network to estimate the Q-value function. PPO is a first-order policy gradient optimization algorithm, which ensures that the policy update is not too large. A large step in a policy update results in learning a bad policy and may lead to instability during training.

In general, DRL environments are modeled as Markov Decision Process attributed to their finite state transitions [215]. However, DRL-based RRA comprehends infinite possible state transitions based on incoming Q. Hence it is difficult to model it as Markov Decision Process. Therefore, in this chapter, an experience buffer has been created of length N, where the experience $E\{s_t,\ a_t,\ r_t,\ \gamma\}$ generated after provisioning of each Q_t will be stored. The proposed DRL-based RRA has the following steps: (1) During initialization, the experience buffer is cleared, (2) the QKD-ON state updates by releasing the network resources of the expired Q_t and the previous Q_t for reassignment, (3) the state model of Q_t modeled as s_t defined in Section 4.3 (4.3.1.1), (4) when the experience buffer is filled with N samples, DRL-based RRA invokes training based on the working principle of DRL framework for RRA as discussed in Section 4.2 (4.2.3). During the training process, a ϵ-greedy strategy has been employed for exploration and exploitation, and (5) At the end, discounted cumulative reward G_t has been calculated using Eq. (4.2), and the buffer will be emptied.

4.4 Performance Evaluation

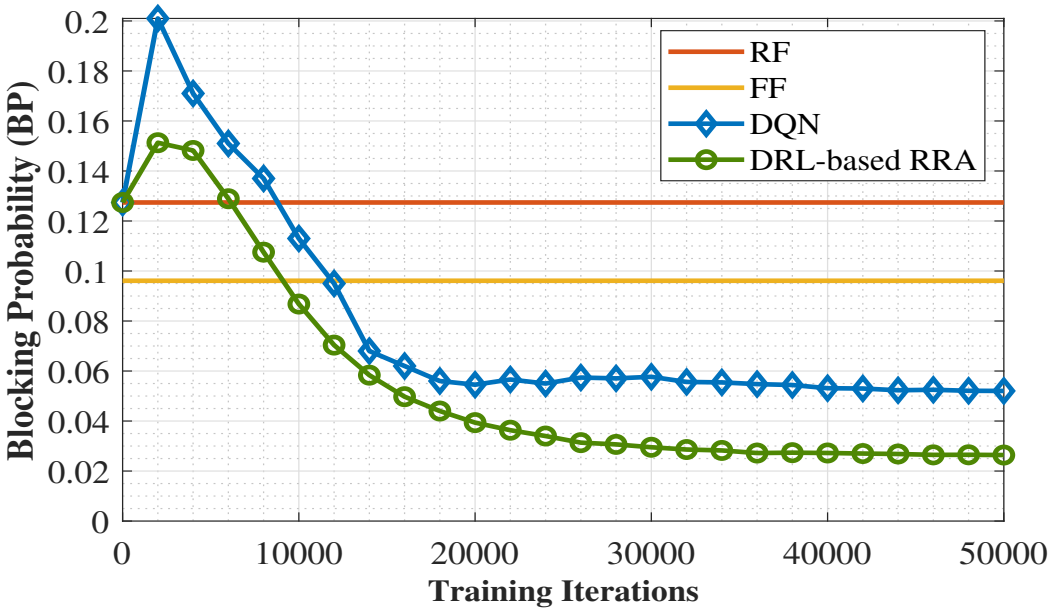
4.4.1 Simulation Setup

In this chapter, two popularly used different sizes of network, namely 14-node NSFNET and 24-node UBN24 [221], are used to evaluate the performance of DRL-based RRA in comparison with the DQN method and the baseline schemes, namely FF and RF. A short-distance QKD network, where the maximum distance between the two end nodes is less than the distance that can accomplish the point-to-point QKD mechanism is assumed. In this chapter, 80 wavelengths with 50 GHz channel spacing for three types of channels in QKD-ONs are considered. Same number of wavelengths are reserved for both the QSCh and the PICh [8]. Therefore, the performance of DRL-based RRA, DQN, and the baseline schemes is analyzed only for the QSCh. In this chapter, a dynamic RRA problem is considered in which QKD-LPRs are randomly generated according to Poisson distribution between source and destination nodes following uniform traffic distribution.

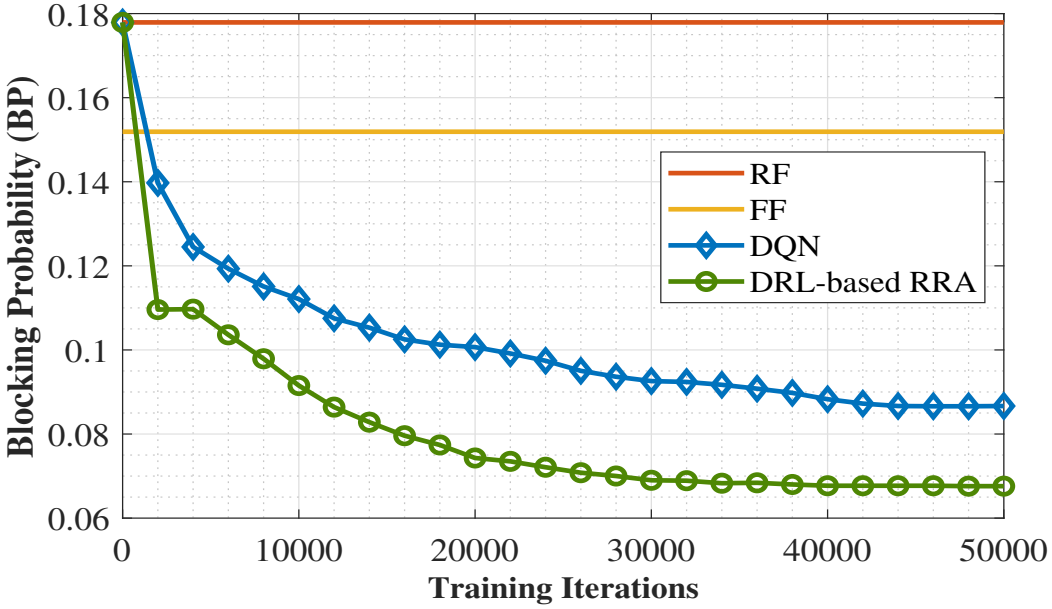
During the training, the hyper-parameters γ (determines how much DRL agents care about rewards, $\gamma \in [0, 1]$) and the learning rate (controls how quickly the model is adapted to the RRA problem) are set to 0.95 and 10^{-3}, respectively. DNNs used ReLU as an activation function in the hidden layers because it allows models to learn faster and perform better. Adam algorithm [222] is used as an optimizer because of its fast computation time, simple parameter tuning, and is considered as a default optimizer for most applications. The simulations of the proposed DRL-based RRA, DQN, and baseline schemes are performed with a customized Python-based simulator. This simulator uses NetworkX to design the graph representation of network model and Pytorch-based PFRL library for the DRL algorithms. The implementation of QKD-ON system model, QKD-LPR model, and simulations are performed using Python.

4.4.2 Training

The training results of *BP* and average reward *(AR)* versus training iterations for the proposed DRL-based RRA, DQN, FF, and RF for both the considered networks are illustrated in Figure 4.3 and Figure 4.4, respectively.

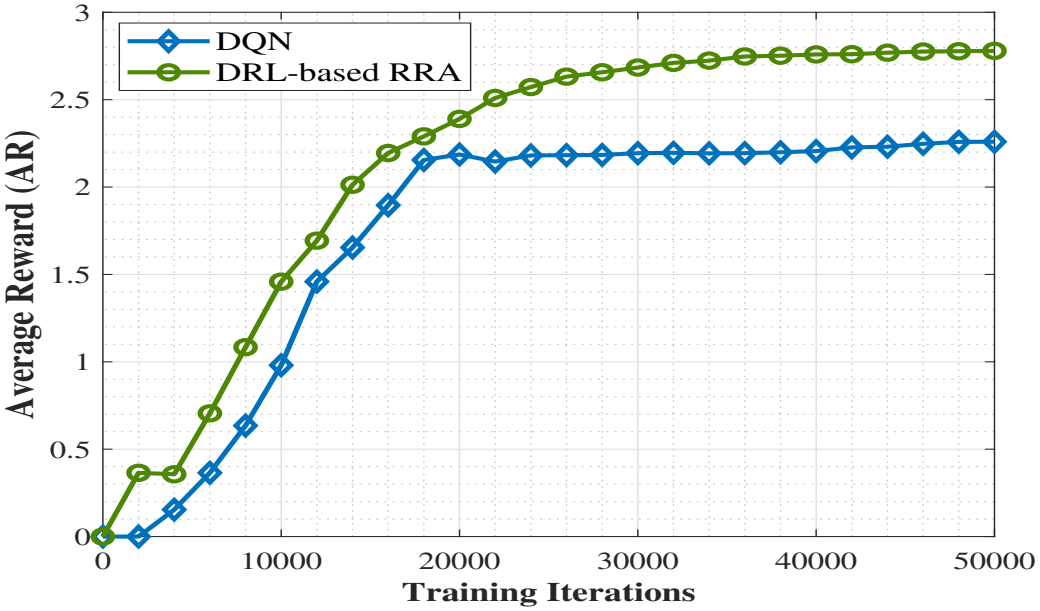


(a)

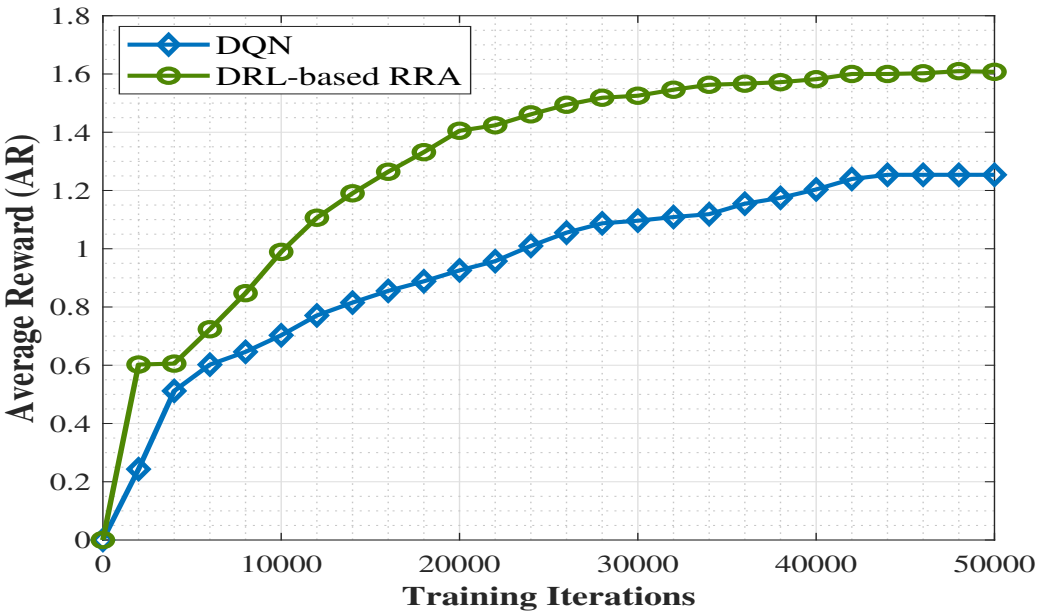


(b)

Figure 4.3: Training results of *BP* versus training iterations for (a) the NSFNET and (b) the UBN24.



(a)



(b)

Figure 4.4: Training results of AR versus training iterations for (a) the NSFNET and (b) the UBN24.

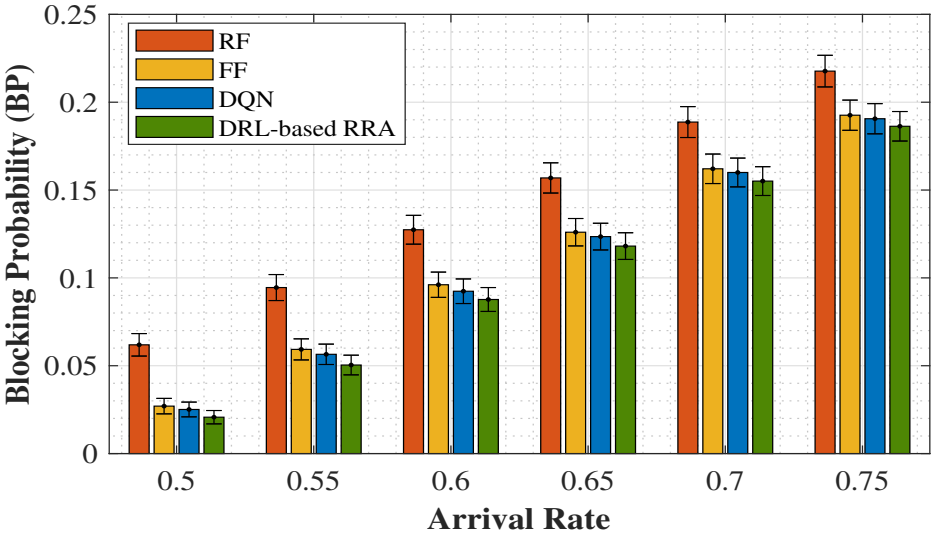
BP is defined in Chapter 3. AR is the average of total rewards after each training iteration. At initial training iteration, the BP of the proposed DRL-based RRA and DQN is equal or higher than the two baseline schemes represented with the straight line, and the AR is minimum, as shown in Figure 4.3 and Figure 4.4, respectively. The performance metrics, i.e., BP and AR, of DRL-based RRA and DQN improve with the number of training iterations during training. However, BP and AR of

DRL-based RRA using PPO are much better than the DQN method because PPO has smaller policy updates, which help to obtain an optimal solution with better training stability, as shown in Figure 4.3 and Figure 4.4, respectively.

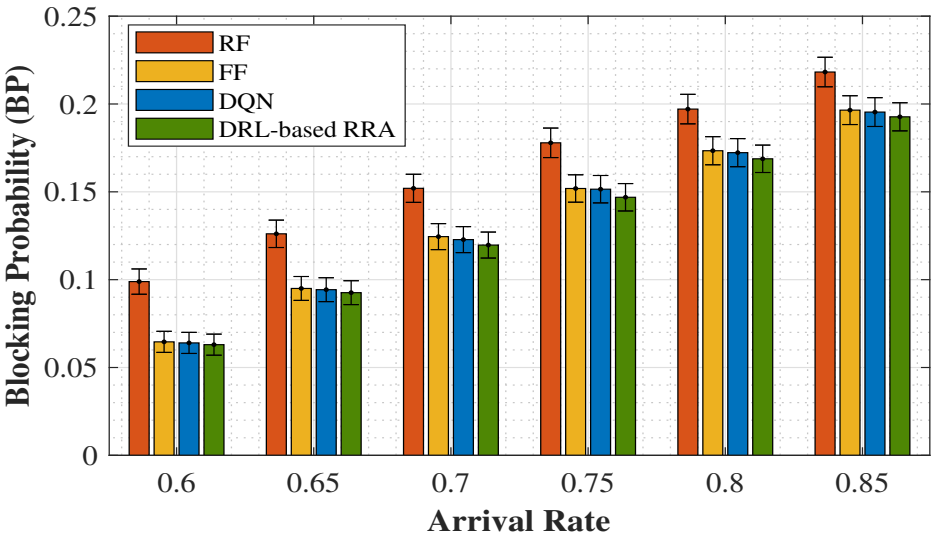
The *BP* of the proposed DRL-based RRA surpassed RF and FF after 6000^{th} and 8000^{th} training iterations, respectively, whereas the *BP* of DQN surpassed RF and FF after 8000^{th} and 10000^{th} training iterations for NSFNET, respectively. Similarly, for UBN24, the *BP* of the proposed DRL-based RRA and DQN surpassed RF and FF at 2000^{th} training iterations. The *BP* of DRL-based RRA and DQN reaches its minimum value, and the training performance becomes stable after 40000^{th} and 42000^{th} training iterations for NSFNET and 38000^{th} and 42000^{th} training iterations for UBN24, respectively. The size of network topology can have a significant impact on network performance, as large size networks tend to be more complex. However, it has been observed that the proposed DRL-based RRA performs better than the DQN method and the two baseline schemes, for the considered networks of different sizes and connectivity.

4.4.2.1 Blocking Probability *(BP)*

Figure 4.5 illustrates the performance of the DRL-based RRA compared to the DQN method and the two baseline schemes, namely, FF and RF, for NSFNET and UBN24 in terms of *BP* under different average arrival rates of traffic with 95% confidence interval. The average arrival rate is the mean number of arrivals of QKD-LPRs per unit time. It can be observed from Figure 4.5 that the *BP* of QKD-LPRs increases with the rise in traffic arrival rate for the proposed DRL-based RRA as well as for the DQN and the two baseline schemes because more resources get occupied during assignment and reassignment in the QKD-ONs. With the approximation capability of DNN, the DRL agent is able to build an optimal policy in order to minimize the blocking of QKD-LPRs, and the proposed scheme outperforms the DQN method and the two baseline schemes in terms of *BP*. Compared to the DQN, FF, and RF, the proposed DRL-based RRA achieves an average reduction in *BP* of 7.19%,



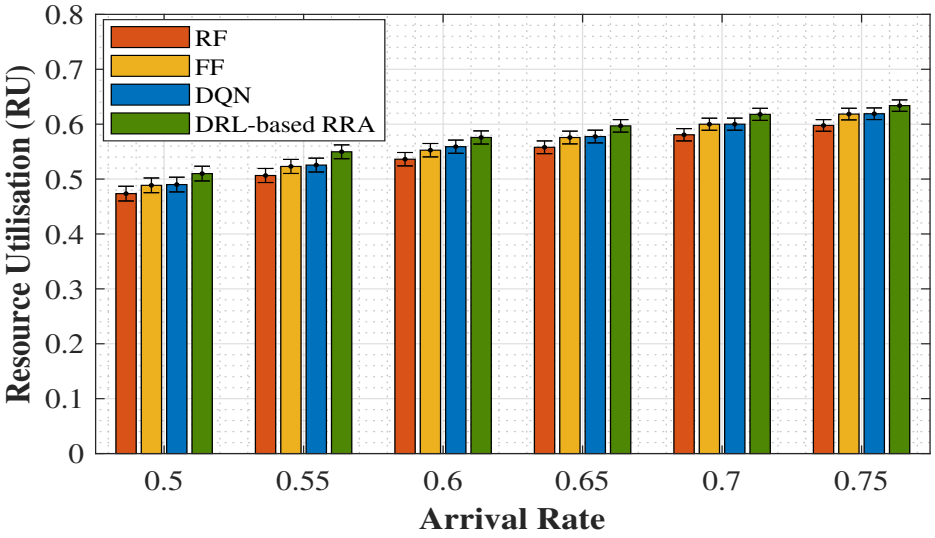
(a)



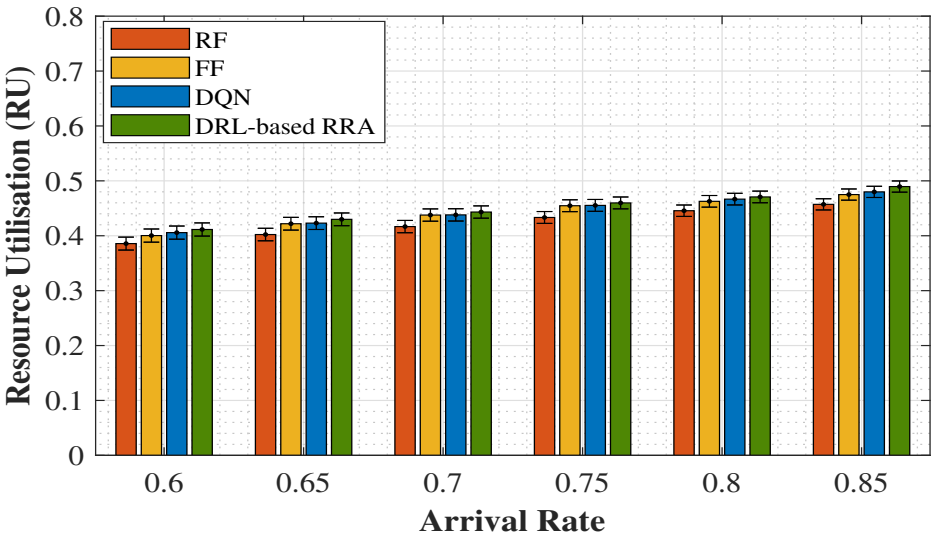
(b)

Figure 4.5: Test results of *BP* versus average traffic arrival rate for (a) the NSFNET and (b) the UBN24.

10.11%, and 33.50% for NSFNET, shown in Figure 4.5 (a) and 2.47%, 3.20%, and 19.60% for UBN24, shown in Figure 4.5 (b), respectively. It can also be observed from the Figure 4.5 that with 95% confidence interval, the *BP* for the proposed DRL-based RRA, DQN, FF, and RF schemes is somewhere between the upper and lower values of the confidence interval.



(a)



(b)

Figure 4.6: Test results of RU versus average traffic arrival rate for (a) the NSFNET and (b) the UBN24.

4.4.2.2 Resource Utilization *(RU)*

RU for different average traffic arrival rate is an important metric and shown in Figure 4.6 (a) and Figure 4.6 (b) for NSFNET and UBN24 with 95% confidence interval, respectively. RU is defined as the ratio of resources (time-slots) utilized by the QKD-LPRs to the total resources available in QKD-ONs. It can be seen from Figure 4.6 that the RU for proposed DRL-based RRA, DQN, FF, and RF schemes increases with the increase in the arrival rate of traffic due to the accommodation of more QKD-LPRs in the QKD-ONs. The proposed DRL-based RRA achieved an

average improvement in RU of 3.40%, 4.33%, and 7.18% for NSFNET and 1.34%, 1.96%, and 6.44% for UBN24 because of the acceptance of more QKD-LPRs (reduction in BP at each corresponding arrival rate, shown in Figure 4.5) as compared to the DQN, FF, and RF, respectively. It can also be seen from Figure 4.6 that the estimate of RU for proposed DRL-based RRA, DQN, FF, and RF schemes will lie between the upper and lower values of the confidence interval.

4.5 Conclusion

In this chapter, the RRA problem in QSCh of QKD-ONs is addressed by exploiting the DRL technique. A DRL-based RRA scheme using PPO to select an optimal route and efficient utilization of network resources to satisfy the resource requirements of QKD-LPRs in QSCh of QKD-ONs is proposed. The simulation results indicate that the proposed DRL-based RRA scheme considerably outperforms the DQN and the two baseline schemes, namely FF and RF, for the considered networks in terms of both BP and RU. However, it has been observed that the routing part of RRA is challenging in QKD-ONs. Hence, in the next chapter, the sub-problem of RRA, i.e., routing is investigated and a DRL-based routing scheme is proposed.

Chapter 5

Routing Based on Deep Reinforcement Learning in QKD-ONs

5.1 Introduction

In the previous chapters, a priority ordering policy for different CoQKD-LPRs was designed, the impact of fragmentation in QSCh of QKD-ONs was analyzed, and the DRL method was exploited to address the problem of RRA in QSCh of QKD-ONs. This chapter provides a DRL-based solution for routing in QKD-ONs that enables the routing agent to learn and adapt to changing network conditions by understanding the networking environment.

In QKD-ONs, routing involves the process of determining the paths to establish secure communication between the nodes in the network. The choice of routing strategy will depend on factors such as network size, available resources, and specific security objectives. Therefore, this chapter focuses on the routing part of the RRA problem of QKD-ONs. In [182], a collaborative routing algorithm was proposed to complete key distribution in partially-trusted relay-based QKD-ONs by considering both the trusted relays and untrusted relays. A key-on-demand scheme was designed

to allocate keys according to security requirements in QKD-ONs [87]. Additionally, some of the heuristic routing schemes [209, 210] based on certain priority criteria for different types of QKD-LPRs were proposed in the literature. However, heuristic-based routing algorithms rely on predefined algorithms to make routing decisions. These algorithms may not be able to adapt well to changing network conditions or dynamic traffic patterns. As a result, heuristics may face difficulties in optimizing routing decisions in complex networking environments. Therefore, in this chapter, DRL is exploited to solve the routing problem in QKD-ONs. The main contributions of this chapter are as follows:

(i) A DRL method is used to address the routing problem in QKD-ONs.

(ii) A DRL-based routing scheme is proposed to make the routing decision in QKD-ONs.

(iii) Performance of the proposed scheme is compared with the two baseline routing schemes.

(iv) Simulation results indicate that the proposed scheme outperforms the two baseline schemes.

5.2 DRL-based Routing in QKD-ONs

This section explains the working operation, modeling (state s_t, action a_t, reward r_t), and training of DRL-based framework for routing in QKD-ONs. The proposed DRL-based routing scheme learns the optimal routing policy to select an appropriate route based on the condition of network states and feedback from the environment using DRL method. This chapter focuses only on the routing sub-problem of RRA in QKD-ONs. The resources for QKD-LPRs on a selected path are allocated using FF resource allocation approach.

Figure 5.1 represents the schematic of DRL-based routing in QKD-ONs. (1) When a new QKD-LPR Q_t is received in the network, the state representation

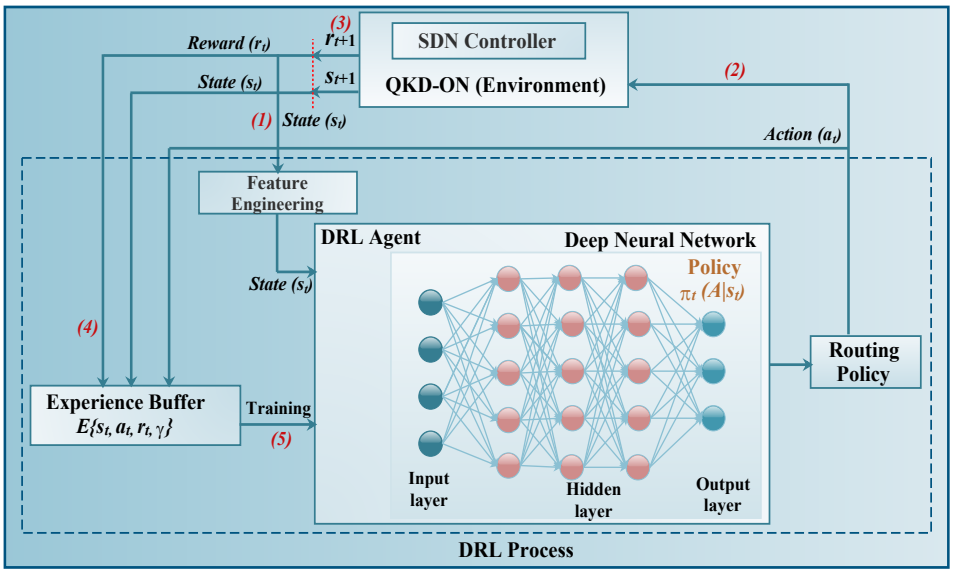


Figure 5.1: DRL framework for Routing in QKD-ONs

of a network, including the in-service QKD-LPRs, network topology, and resource utilization information, is fetched by the SDN controller. The SDN controller evokes a feature engineering module to generate a customized network environment state s_t. The state s_t is expressed as:

$$s_t = \{o_t,\ d_t, \{Z^c_{t,k},\ Z^m_{t,k},\ Z^{Total}_k|_{k\in[1,K]}\}\} \tag{5.1}$$

This customized state s_t will be input to the DNN model of DRL-based routing framework. (2) The DRL agent selects an action $a_t \in A$, where A is a definite action space that makes an optimal routing decision to establish a new QKD-LPR (output a routing policy $\pi_t(A|s_t, \theta)$, where θ represents a set of DNN parameters). The DRL agent selects a path from the pre-calculated K paths. Hence, the action space A includes K actions. Based on π_t, the SDN controller selects an action $a_t \in A$ and establishes the corresponding QKD-LPR. (3) An immediate reward r_t is produced by a reward system for DRL-based routing after receiving feedback from previous routing operation. In this case, $r_t = 1$, if QKD-LPR served successfully, else $r_t =$ -1. (4) In order to achieve an optimal solution, a reward r_t, along with state s_t and action a_t are stored in an experience buffer as a tuple $E\ \{s_t,\ a_t,\ r_t,\ \gamma\}$, where $\gamma \in$

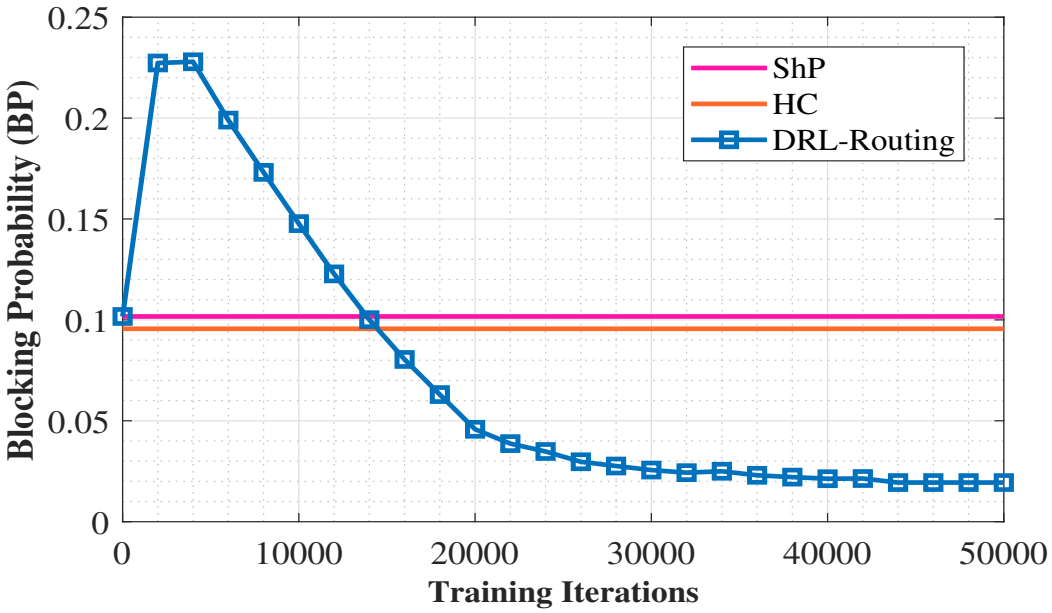
$[0, 1]$ is a discount factor. (5) In this work, an experience buffer of length N has been created, where experience will be stored after provisioning of each QKD-LPR and is used for training the DNN of DRL-based routing framework. The objective of DRL-based routing is to learn the routing policy and maximize the cumulative reward in long-term. The DRL-based routing scheme consists of the following steps: (i) the experience buffer is initially emptied, (ii) the state s_t of the environment, i.e., QKD-ON is updated after releasing the network resources of expired QKD-LPR during assignment and reassignment, (iii) the customized state s_t for a QKD-LPR is modeled as s_t (expressed by Eq. (5.1)), (iv) based on the process of DRL framework for routing in QKD-ON, the proposed DRL-based routing scheme call for training upon filling the experience buffer with N samples, and (v) After completion of the training process, the cumulative reward is calculated and the experience buffer will be cleared.

5.3 Simulation Results and Discussion

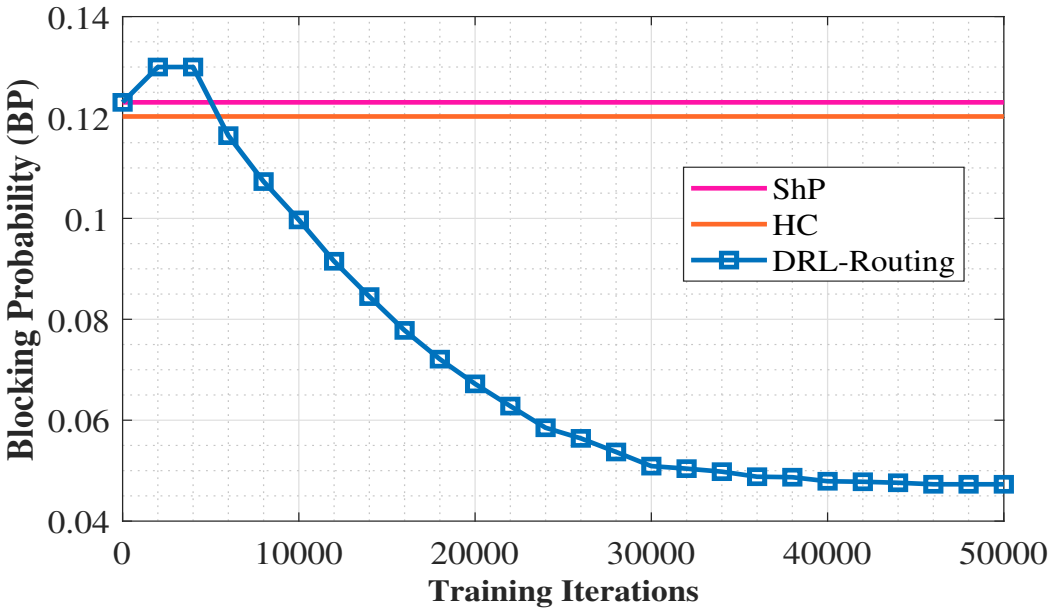
To evaluate the performance of DRL-based routing in comparison with the two baseline schemes, namely shortest-path (ShP) and fixed-alternate routing based on hop count (HC), NSFNET and UBN24 are used. In this chapter, the dynamic QKD-LPRs are generated according to Poisson distribution between the source node and the destination node following uniform traffic distribution. A DRL agent of DRL-based routing framework is trained using the PPO algorithm [219] and for training, γ and the learning rate are set to 0.90 and 10^{-3}, respectively. DNNs used ReLU as an activation function in the hidden layers, and Adam algorithm is used as an optimizer for training. The simulations of the proposed DRL-based routing and baseline schemes (ShP and HC) are performed with a customized Python-based simulator. The QKD-ON system model and QKD-LPR model are implemented, and simulations are performed using Python.

5.3.1 Training Results

The training results of BP and AR as a function of training iterations for both DRL-based routing as well as baseline schemes are shown in Figure 5.2 and Figure 5.3, respectively.

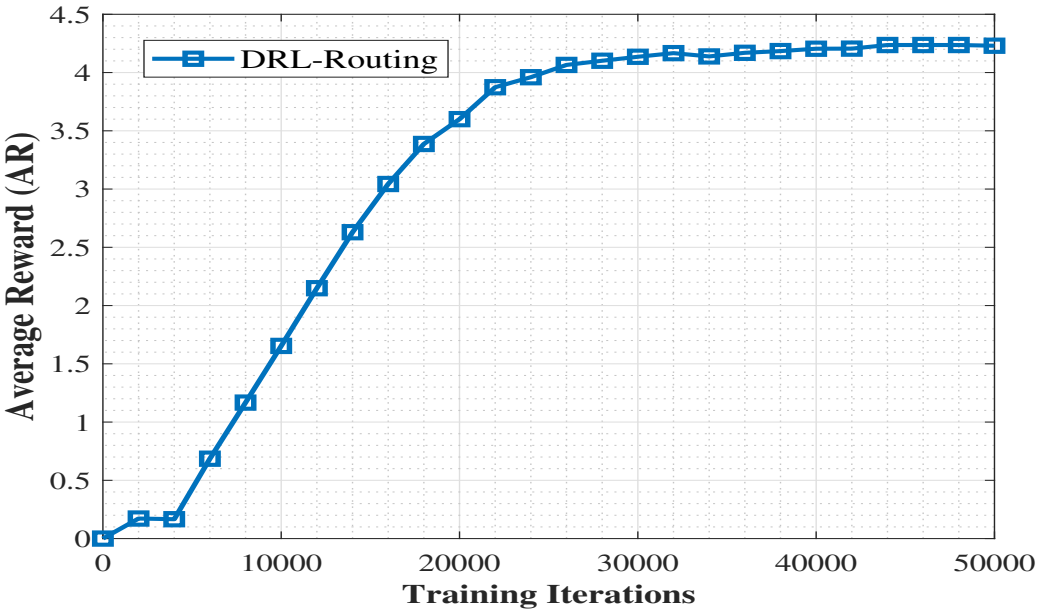


(a)

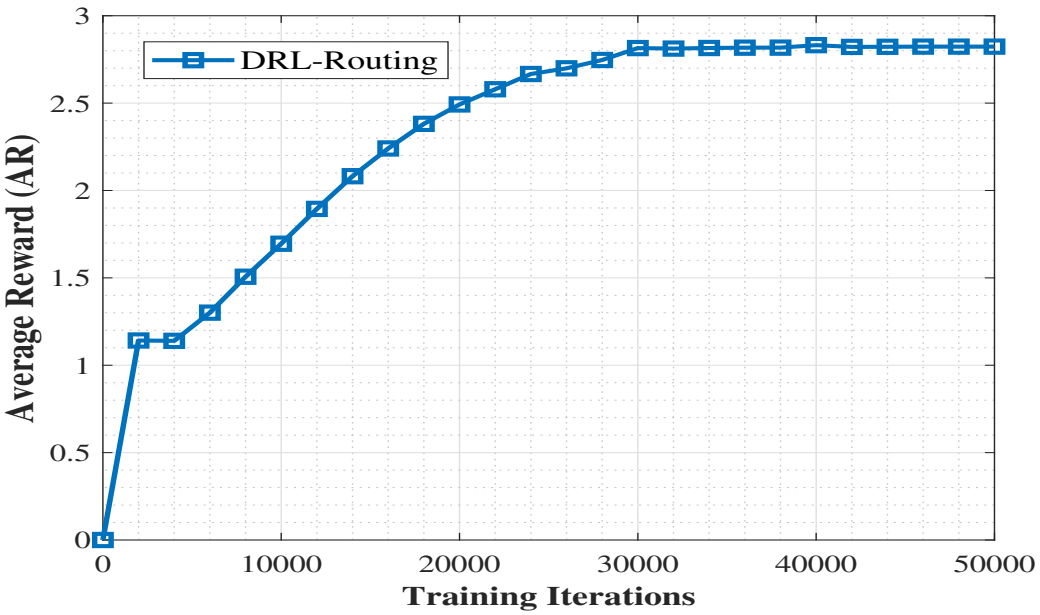


(b)

Figure 5.2: Training results of BP versus training iterations for (a) the NSFNET and (b) the UBN24.



(a)



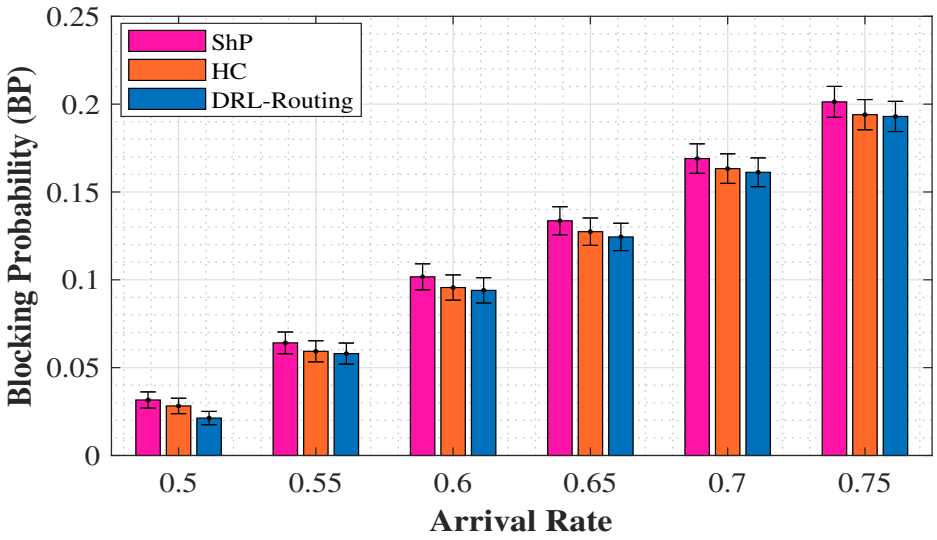
(b)

Figure 5.3: Training results of AR versus training iterations for (a) the NSFNET and (b) the UBN24.

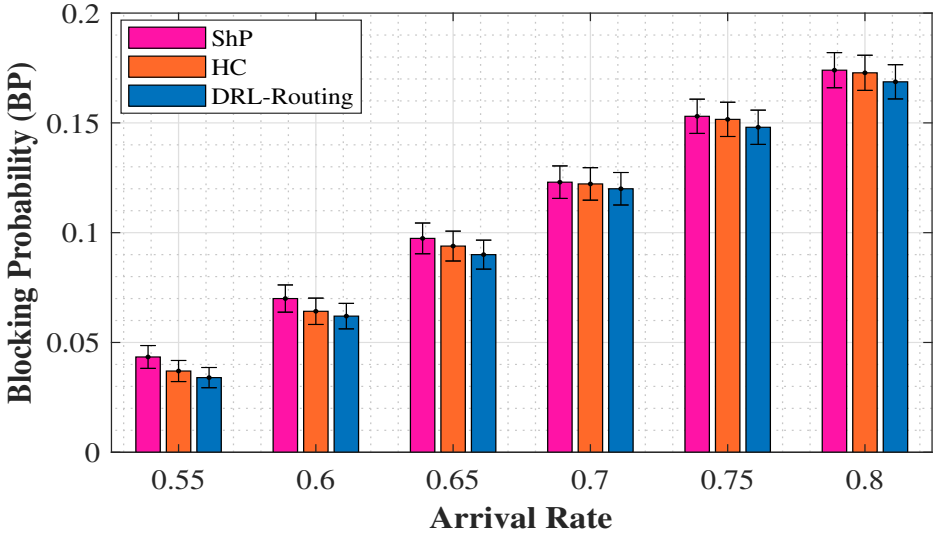
From Figure 5.2 and Figure 5.3, it has been seen that at initial training iterations, BP of the DRL-based routing is higher as compared to the two baseline schemes and correspondingly the values of average reward is minimum. However, as the training iteration increases, performance of the DRL-based routing scheme improves in terms of BP and AR. It has been seen from Figure 5.2 (a) that the BP of DRL-based routing scheme surpassed ShP and HC after 12000th and 14000th iterations

of training for NSFNET, respectively. Similarly, for UBN24, the *BP* of DRL-based routing scheme surpassed ShP and HC after 4000th iterations of training, shown in Figure 5.2 (b). *BP* of DRL-based routing reaches its minimum value, and the training performance becomes stable after 40000th training iterations for both the considered networks.

5.3.2 Test Result



(a)



(b)

Figure 5.4: Test results of *BP* versus average traffic arrival rate for (a) the NSFNET and (b) the UBN24.

Figure 5.4 illustrates the test result of *BP* versus average arrival traffic rate for

the proposed DRL-based routing and the two baseline schemes with 95% confidence interval. It has been observed from plotted graph that the *BP* of the DRL-based routing and the two baseline schemes increases as traffic arrival rate increases because more resources get occupied in the QKD-ONs during RRA. The DRL agent of DRL framework for routing is able to build an optimal routing policy by leveraging the capability of DNN in order to reduce the impact of blocking, and the proposed DRL-based routing outperforms the two baseline schemes in terms of *BP*. The proposed DRL-based routing achieves an average reduction in *BP* of 14.31% and 8% for NSFNET, shown in Fig. 5.4 (a), and 6.45% and 3.74% for UBN24, shown in Fig. 5.4 (b) compared to ShP and HC, respectively. It has also been observed from the Figure 5.4 that with 95% confidence interval, the *BP* for the proposed DRL-based routing and the two baseline schemes is somewhere between the upper and lower values of the confidence interval.

5.4 Conclusion

This chapter explored the application of DRL and proposed a DRL-based solution for routing in QKD-ONs. In this chapter an intelligent routing scheme is designed that considers various networking factors while making optimal routing decisions. The results highlight the considerable potential of employing the DRL approach for routing in QKD-ONs and indicate that the proposed DRL-based routing scheme outperforms the baseline schemes.

Chapter 6

Conclusions and Future Works

This section summarizes the main contributions and findings of the thesis. Furthermore, the scope for future work is discussed.

6.1 Conclusions

Quantum communication opens a new era that has potential to revolutionize secure communication by leveraging the unique properties of quantum mechanics. QKD is one of the most important concepts of quantum communication, enabling two users to generate a secret key between them with information-theoretic security. Thus, this concept solves the key distribution problem of conventional cryptography methods. Optical fiber has been usually considered as a secure mode of transmission, however, the increasing incidents of lightpath attacks inspired researchers to integrate QKD into optical networks. The integration of QKD into optical networks introduces different networking challenges that need to be addressed. The main objective of this thesis is to cover the relevant aspects of QKD-ONs and concentrate on the development of efficient resource provisioning schemes to solve the RRA problem of QKD-ONs.

As an initial step, in this thesis, the integration of QKD into the optical networks to secure the data transmission between the users has been studied. Initially, dark fibers were used to conduct the QKD experiments, however, it is not a cost-

effective solution to deploy a separate global optical network for this purpose. Thus, instead of using separate dark fibers for QKD system (consisting of QSCh and PICh), integration of QKD with the existing classical optical networks has been proposed. Based on this study, it has been observed that the co-existence of QSCh and the two classical channels into the single optical fiber introduces RRA problem in QKD-ON due to limited network resources, which needs to be addressed to enhance the network performance. Furthermore, while accommodating QKD-LPRs in QKD-ONs, the diverse assignment and reassignment of network resources generated fragmented/isolated slots that cannot be used for future incoming QKD-LPRs. Therefore, in this thesis, the RRA problem and the impact of fragmentation in QSCh of QKD-ON have been investigated.

Several research efforts have been made in the literature for efficient utilization of network resources while accommodating QKD-LPRs in QKD-ONs. However, the existing RRA methods do not fit for the scenario, where QKD-LPRs of different security requirements, such as HPQKD-LPRs, MPQKD-LPRs, and LPQKD-LPRs, arrive in the network. Thus, the prioritization of QKD-LPRs based on the specific security requirements is essential in such networks. It has been observed that the existing RRA methods did not consider the effect of fragmentation in QSCh caused by the diverse assignment and reassignment of network resources in QSCh of QKD-ONs. Hence, it increases the blocking of QKD-LPRs, thereby minimizing the security of QKD-ONs. Thus, the effect of fragmentation in QSCh for QKD-LPRs is required to be considered in such networks during RRA. It has also been observed that the conventional schemes use the pre-determined algorithms to find an optimal path and allocate resources on the selected path. Hence, the performance of the conventional schemes becomes inefficient as the dynamicity in the network increases. Inspired by the recent advances in DRL for solving complex problems, and also because of its capability to learn directly from experiences, DRL is exploited to solve the RRA problem. DRL adapts to changing network conditions by understanding the networking environment and considering various factors while making routing

and resource assignment decisions, which include in-service QKD-LPRs, network topology, and resource utilization information. It has also been observed that the routing part of RRA in QKD-ONs is challenging as it depends on factors such as network size, available resources, and specific security objectives. Hence, by leveraging the capability of DRL, an intelligent routing scheme has also been designed in this thesis. Thus, in order to improve the network performance compared to the existing RRA methods, the effect of blocking on different CoQKD-LPRs and the impact of fragmentation in QSCh of QKD-ON have been analyzed, and the capabilities of DRL methods have been explored to propose different resource provisioning schemes.

Different networking parameters and constraints of QKD-ON have been considered in the QKD network model for performance evaluation. To examine the performance of the baseline and the proposed schemes, two different sizes of networks have been considered for simulations. For performance evaluation of the baseline and proposed methods, the QKD-ON model and QKD-LPR model have been developed in MATLAB and Python for simulations. In order to compare the performance of the proposed and the baseline schemes, the performance evaluation has been done in terms of BP, RU, and P_{SKUF}. Furthermore, the effect of fragmentation in QSCh of QKD-ONs has been analyzed on the basis of two metrics, i.e., FI_{QSCh} and $FM_{external}$.

This thesis concludes that the proposed resource provisioning schemes have potential to significantly improve network performance in terms of blocking, resource utilization, and fragmentation. It is expected that the research directions and insights obtained from this thesis will help researchers to solve the networking challenges of existing and future QKD-ONs.

6.2 Future Works

This section discusses some of the future networking aspects that are possible extensions of the work presented in this thesis. These research directions may be explored

to enhance network performance further. Suggestions for the future work are listed below:

- Fragmentation-aware approaches for efficient provisioning of network resources during RRA in QKD-ONs using DRL methods can be developed.

- A failure in QKD-ONs will cause a huge amount of data loss during data transmission and secret key loss during QKD process. Therefore, survivability, i.e., protection of data and secret keys against failure, is an important issue. Hence, different protection mechanisms (i.e., adding backup / redundant network resources) and recovery mechanisms (i.e., restoring services as soon as possible after a disaster) can be developed for three types of channels in QKD-ONs based on severity.

- As QKD is a point-to-point technology, in order to exchange keys across remote nodes, an intermediate node has been considered as a TRN between the source and destination. However, the placement of TRNs increases the infrastructure cost and deployment difficulty. Hence, the placement of TRNs in QKD-ONs is of great importance. Therefore, strategies for optimal placement of TRNs in a metro area network to reduce the capital expenditure (CAPEX) without affecting the security level can be designed.

- Blockchain is an emerging technology used in various applications, including but not limited to the Internet of Things, wireless communication networks, healthcare networks, financial systems, supply chains, and voting systems. However, the evolution of quantum computers will easily break the security of blockchain technology and destroy the existing and next-generation blockchain networks. Inspired by recent advancements in quantum technology, researchers and developers are increasing their interest in combining one of the most promising quantum communication techniques, i.e., QKD, with blockchain to secure blockchain against quantum attacks. However, integrating quantum with blockchain introduces various challenges. Hence, significant

research efforts are required to develop new strategies to enhance blockchain security in optical networks.

- AI/ML has the capability to take decisions and automate and optimize the system for better performance. For an improved security, speed, and scalability, AI/ML can help to construct an intelligent system on the quantum-secured blockchain. Additionally, recent advances in AI/ML, such as DL and RL, can be exploited to propose a secure and robust consensus in quantum-secured blockchain. A new combination of quantum-secured blockchain and AI/ML techniques will be able to build more robust and trusted optical networks against various security breaches. However, such a combination of security and intelligence is not currently developed and also might face various challenges in this domain. Hence, efforts are needed to combine quantum-assisted blockchain with AI/ML/DL/RL and design more secure, trusted, and intelligent optical networks.

References

[1] M. A. Nielsen and I. L. Chuang, "Fundamental concepts," in *Quantum Computation and Quantum Information*. UK: Cambridge University Press, 2010, ch. 1. [Online]. Available: http://mmrc.amss.cas.cn/tlb/201702/W020170224608149940643.pdf

[2] S. Wehner and N. Ng, "edX Quantum Cryptography: Week 0," 2016. [Online]. Available: http://users.cms.caltech.edu/~vidick/notes/QCryptoX/LN_Week0.pdf

[3] L. O. Mailloux, M. R. Grimaila, D. D. Hodson, G. Baumgartner, and C. McLaughlin, "Performance evaluations of quantum key distribution system architectures," *IEEE Secur. Priv.*, vol. 13, no. 1, pp. 30–40, Jan.-Feb. 2015.

[4] T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger, "Quantum cryptography with entangled photons," *Phys. Rev. Lett.*, vol. 84, no. 20, pp. 4729–4732, May 2000.

[5] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theor. Comput. Sci.*, vol. 560, no. 12, pp. 7–11, 2014.

[6] L. O. Mailloux, D. D. Hodson, M. R. Grimaila, R. D. Engle, C. V. Mclaughlin, and G. B. Baumgartner, "Using modeling and simulation to study photon number splitting attacks," *IEEE Access*, vol. 4, pp. 2188–2197, May 2016.

[7] H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 108, no. 13, pp. 130 503(1–5), Mar. 2012.

[8] Y. Cao, Y. Zhao, X. Yu, and Y. Wu, "Resource assignment strategy in optical networks integrated with quantum key distribution," *IEEE/OSA J. Opt. Commun. Netw.*, vol. 9, no. 11, pp. 995–1004, Nov. 2017.

[9] P. Eraerds, N. Walenta, M. Legré, N. Gisin, and H. Zbinden, "Quantum key distribution and 1 Gbps data encryption over a single fibre," *New J. Phys.*, vol. 12, no. 6, pp. 063 027(1–15), Jun. 2010.

[10] Y. Cao, Y. Zhao, Y. Wu, X. Yu, and J. Zhang, "Time-scheduled quantum key distribution (QKD) over WDM networks," *IEEE/OSA J. Lightw. Technol.*, vol. 36, no. 16, pp. 3382–3395, Aug. 2018.

[11] E. O. Kiktenko, N. O. Pozhar, M. N. Anufriev, A. S. Trushechkin, R. R. Yunusov, Y. V. Kurochkin, A. Lvovsky, and A. Fedorov, "Quantum-secured blockchain," *Quantum Sci. Technol.*, vol. 3, no. 3, pp. 035 004(1–8), 2018.

[12] X. Sun, M. Sopek, Q. Wang, and P. Kulicki, "Towards quantum-secured permissioned blockchain: Signature, consensus, and logic," *Entropy*, vol. 21, no. 9, pp. 887(1–15), 2019.

[13] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, no. 1, pp. 145–195, Mar. 2002.

[14] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978.

[15] S. Debnath, N. M. Linke, C. Figgatt, K. A. Landsman, K. Wright, and C. Monroe, "Demonstration of a small programmable quantum computer with atomic qubits," *Nature*, vol. 536, no. 7614, pp. 63–66, Aug. 2016.

[16] M. Caleffi, A. S. Cacciapuoti, and G. Bianchi, "Quantum internet: From communication to distributed computing!" in *Proc. ACM NANOCOM*, Reykjavik, Iceland, 2018, pp. 1–4.

[17] A. S. Cacciapuoti, M. Caleffi, F. Tafuri, F. S. Cataliotti, S. Gherardini, and G. Bianchi, "Quantum internet: networking challenges in distributed quantum computing," *IEEE Netw.*, vol. 34, no. 1, pp. 137–143, Nov. 2019.

[18] M. Caleffi, D. Chandra, D. Cuomo, S. Hassanpour, and A. S. Cacciapuoti, "The rise of the quantum internet," *Computer*, vol. 53, no. 6, pp. 67–72, Jun. 2020.

[19] D. Cuomo, M. Caleffi, and A. S. Cacciapuoti, "Towards a distributed quantum computing ecosystem," *IET Quantum Commun.*, vol. 1, no. 1, pp. 3–8, Jul. 2020.

[20] A. S. Cacciapuoti, M. Caleffi, R. Van Meter, and L. Hanzo, "When entanglement meets classical communications: Quantum teleportation for the quantum internet," *IEEE Trans. Commun.*, vol. 68, no. 6, pp. 3808–3833, Mar. 2020.

[21] N. K. Kundu, S. P. Dash, M. R. McKay, and R. K. Mallik, "MIMO terahertz quantum key distribution," *arXiv preprint arXiv:2105.03642*, 2021.

[22] N. Wolchover, "A tricky path to quantum-safe encryption," *Quanta Mag.*, Sep. 2015.

[23] K. A. Fisher, A. Broadbent, L. Shalm, Z. Yan, J. Lavoie, R. Prevedel, T. Jennewein, and K. Resch, "Quantum computing on encrypted data," *Nat. Commun.*, vol. 5, no. 1, pp. 3074(1–7), Jan. 2014.

[24] C. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE Int. Conf. Computers, Systems & Signal Processing*, Bangalore, India, 1984, pp. 175–179.

[25] Y. Zhao, Y. Cao, X. Yu, and J. Zhang, "Quantum key distribution (QKD) over software-defined optical networks," in *Quantum Cryptography in Advanced Networks*, O. G. Morozov, Ed. Rijeka: IntechOpen, 2019, ch. 2. [Online]. Available: https://doi.org/10.5772/intechopen.80450

[26] Q. Zhang, F. Xu, Y.-A. Chen, C.-Z. Peng, and J.-W. Pan, "Large scale quantum key distribution: Challenges and solutions," *Opt. Express*, vol. 26, no. 18, pp. 24 260–24 273, Sep. 2018.

[27] W. Heisenberg, "The physical content of quantum kinematics and mechanics," in *Quantum Theory and Measurement*, J. A. Wheeler and W. H. Zurek, Eds. Princeton University Press: Princeton, 1927. [Online]. Available: http://www.informationphilosopher.com/solutions/scientists/heisenberg/Heisenberg_Uncertainty.pdf

[28] ——, *Physical principles of the quantum theory*. Dover Publications, Inc., 1930.

[29] C. A. Fuchs and A. Peres, "Quantum-state disturbance versus information gain: Uncertainty relations for quantum information," *Phys. Rev. A*, vol. 53, no. 4, pp. 2038–2045, Apr. 1996.

[30] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, no. 5886, pp. 802–803, Oct. 1982.

[31] D. Dieks, "Communication by EPR devices," *Phys. Lett. A*, vol. 92, no. 6, pp. 271–272, Nov. 1982.

[32] J. Ortigoso, "Twelve years before the quantum no-cloning theorem," *Am. J. Phys*, vol. 86, no. 3, pp. 201–205, Mar. 2018.

[33] H.-K. Lo and H. F. Chau, "Unconditional security of quantum key distribution over arbitrarily long distances," *Science*, vol. 283, no. 5410, pp. 2050–2056, Mar. 1999.

[34] Y. Zhao, Y. Cao, W. Wang, H. Wang, X. Yu, J. Zhang, M. Tornatore, Y. Wu, and B. Mukherjee, "Resource allocation in optical networks secured by quantum key distribution," *IEEE Commun. Mag.*, vol. 56, no. 8, pp. 130–137, Aug.2018.

[35] H.-K. Lo, M. Curty, and K. Tamaki, "Secure quantum key distribution," *Nat. Photon.*, vol. 8, no. 8, pp. 595–604, Jul. 2014.

[36] G. S. Vernam, "Cipher printing telegraph systems: For secret wire and radio telegraphic communications," *IEEE J. AIEE*, vol. 45, no. 2, pp. 109–115, Feb. 1926.

[37] M. Dworkin, E. Barker, J. Nechvatal, J. Foti, L. Bassham, E. Roback, and J. JFD, "Advanced encryption standard (AES)," *Federal Inf. Process. Stds. (NIST FIPS)*, vol. 197, Nov. 2001. [Online]. Available: https://www.nist.gov/publications/advanced-encryption-standard-aes

[38] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Phys. Rev. Lett.*, vol. 67, no. 6, pp. 661–663, Aug. 1991.

[39] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," *Phys. Rev. Lett.*, vol. 68, no. 21, pp. 3121–3124, May 1992.

[40] C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without Bell's theorem," *Phys. Rev. Lett.*, vol. 68, no. 5, pp. 557–559, Feb. 1992.

[41] D. Bruß, "Optimal eavesdropping in quantum cryptography with six states," *Phys. Rev. Lett.*, vol. 81, no. 14, pp. 3018–3021, Oct. 1998.

[42] H. Bechmann-Pasquinucci and N. Gisin, "Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography," *Phys. Rev. A*, vol. 59, no. 6, pp. 4238–4248, Jun. 1999.

[43] V. Scarani, A. Acin, G. Ribordy, and N. Gisin, "Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations," *Phys. Rev. Lett.*, vol. 92, no. 5, pp. 057 901(1–4), Feb. 2004.

[44] T. C. Ralph, "Continuous variable quantum cryptography," *Phys. Rev. A*, vol. 61, no. 1, pp. 010 303(1–4), Dec. 1999.

[45] K. Inoue, E. Waks, and Y. Yamamoto, "Differential phase shift quantum key distribution," *Phys. Rev. Lett.*, vol. 89, no. 3, pp. 037 902(1–3), Jul. 2002.

[46] ——, "Differential-phase-shift quantum key distribution using coherent light," *Phys. Rev. A*, vol. 68, no. 2, pp. 022 317(1–4), Aug. 2003.

[47] H. Weier, H. Krauss, M. Rau, M. Fürst, S. Nauerth, and H. Weinfurter, "Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors," *New J. Phys.*, vol. 13, no. 7, pp. 073 024(1–10), Jul. 2011.

[48] Y.-L. Tang, H.-L. Yin, X. Ma, C.-H. F. Fung, Y. Liu, H.-L. Yong, T.-Y. Chen, C.-Z. Peng, Z.-B. Chen, and J.-W. Pan, "Source attack of decoy-state quantum key distribution using phase information," *Phys. Rev. A*, vol. 88, no. 2, pp. 022 308(1–9), Aug. 2013.

[49] Z. Yuan, J. Dynes, and A. Shields, "Avoiding the blinding attack in QKD," *Nat. Photon.*, vol. 4, no. 12, pp. 800–801, Dec. 2010.

[50] W.-Y. Hwang, "Quantum key distribution with high loss: Toward global secure communication," *Phys. Rev. Lett.*, vol. 91, no. 5, pp. 057 901(1–4), Aug. 2003.

[51] X.-B. Wang, "Beating the photon-number-splitting attack in practical quantum cryptography," *Phys. Rev. Lett.*, vol. 94, no. 23, pp. 230 503(1–4), Jun. 2005.

[52] H.-K. Lo, "Quantum key distribution with vacua or dim pulses as decoy states," in *Proc. IEEE ISIT*, Chicago, USA, 2004, p. 137.

[53] Y.-L. Tang, H.-L. Yin, Q. Zhao, H. Liu, X.-X. Sun, M.-Q. Huang, W.-J. Zhang, S.-J. Chen, L. Zhang, L.-X. You *et al.*, "Measurement-device-independent quantum key distribution over untrustful metropolitan network," *Phys. Rev. X*, vol. 6, no. 1, pp. 011 024(1–8), Mar. 2016.

[54] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang *et al.*, "Measurement-device-independent quantum key distribution over a 404 km optical fiber," *Phys. Rev. Lett.*, vol. 117, no. 19, pp. 190 501(1–5), Nov. 2016.

[55] W. Buttler, R. Hughes, P. G. Kwiat, S. Lamoreaux, G. Luther, G. Morgan, J. Nordholt, C. Peterson, and C. Simmons, "Practical free-space quantum key distribution over 1 km," *Phys. Rev. Lett.*, vol. 81, no. 15, pp. 3283–3286, Oct. 1998.

[56] C.-Z. Peng, T. Yang, X.-H. Bao, J. Zhang, X.-M. Jin, F.-Y. Feng, B. Yang, J. Yang, J. Yin, Q. Zhang *et al.*, "Experimental free-space distribution of entangled photon pairs over 13 km: towards satellite-based global quantum communication," *Phys. Rev. Lett.*, vol. 94, no. 15, pp. 150 501(1–4), Apr. 2005.

[57] S.-K. Liao, H.-L. Yong, C. Liu, G.-L. Shentu, D.-D. Li, J. Lin, H. Dai, S.-Q. Zhao, B. Li, J.-Y. Guan *et al.*, "Long-distance free-space quantum key distribution in daylight towards inter-satellite communication," *Nat. Photon.*, vol. 11, no. 8, pp. 509–513, Jul. 2017.

[58] R. J. Hughes, G. L. Morgan, and C. G. Peterson, "Quantum key distribution over a 48 km optical fibre network," *J. Mod. Opt.*, vol. 47, no. 2-3, pp. 533–547, Jul. 2000.

[59] A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussières, M.-J. Li *et al.*, "Secure quantum key distribution

over 421 km of optical fiber," *Phys. Rev. Lett.*, vol. 121, no. 19, pp. 190 502(1–4), Nov. 2018.

[60] N. Peters, P. Toliver, T. Chapuran, R. Runser, S. McNown, C. Peterson, D. Rosenberg, N. Dallmann, R. Hughes, K. McCabe *et al.*, "Dense wavelength multiplexing of 1550 nm QKD with strong classical channels in reconfigurable networking environments," *New J. Phys.*, vol. 11, no. 4, pp. 045 012(1–17), Apr. 2009.

[61] M. P. Fok, Z. Wang, Y. Deng, and P. R. Prucnal, "Optical layer security in fiber-optic networks," *IEEE Trans. Inf. Forensics Secur.*, vol. 6, no. 3, pp. 725–736, Sep. 2011.

[62] M. Furdek, N. Skorin-Kapov, S. Zsigmond, and L. Wosinska, "Vulnerabilities and security issues in optical networks," in *Proc. IEEE ICTON*, Graz, Austria, 2014, pp. 1–4.

[63] N. Skorin-Kapov, M. Furdek, S. Zsigmond, and L. Wosinska, "Physical-layer security in evolving optical networks," *IEEE Commun. Mag.*, vol. 54, no. 8, pp. 110–117, Aug. 2016.

[64] B. Schumacher, "Quantum coding," *Phys. Rev. A*, vol. 51, no. 4, pp. 2738–2747, Apr. 1995.

[65] D. Bouwmeester and A. Zeilinger, "The physics of quantum information: Basic concepts," in *The physics of quantum information*. Springer, 2000, pp. 1–14.

[66] R. Van Meter, "Quantum Background," in *Quantum Networking*. Hoboken, NJ, USA: Wiley, 2014, ch. 2.

[67] L. Gyongyosi, S. Imre, and H. V. Nguyen, "A survey on quantum channel capacities," *IEEE Commun. Surv. Tuts.*, vol. 20, no. 2, pp. 1149–1205, 2nd Quart. 2018.

[68] C.-H. F. Fung, X. Ma, and H. Chau, "Practical issues in quantum-key-distribution postprocessing," *Phys. Rev. A*, vol. 81, no. 1, pp. 012 318(1–15), Jan. 2010.

[69] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Rev. Mod. Phys.*, vol. 81, no. 3, pp. 1301–1350, Sep. 2009.

[70] M. Mafu and M. Senekane, "Security of quantum key distribution protocols," in *Advanced Technologies of Quantum Key Distribution*, S. Gnatyuk, Ed. Rijeka: IntechOpen, 2018, ch. 1. [Online]. Available: https://doi.org/10.5772/intechopen.74234

[71] N. Gisin, G. Ribordy, H. Zbinden, D. Stucki, N. Brunner, and V. Scarani, "Towards practical and fast quantum cryptography," *arXiv preprint quant-ph/0411022*, Nov. 2004.

[72] M. Hillery, "Quantum cryptography with squeezed states," *Phys. Rev. A*, vol. 61, no. 2, pp. 022 309(1–8), Jan. 2000.

[73] N. J. Cerf, M. Levy, and G. Van Assche, "Quantum distribution of Gaussian keys using squeezed states," *Phys. Rev. A*, vol. 63, no. 5, pp. 052 311(1–5), Apr. 2001.

[74] M. D. Reid, "Quantum cryptography with a predetermined key, using continuous-variable Einstein-Podolsky-Rosen correlations," *Phys. Rev. A*, vol. 62, no. 6, pp. 062 308(1–6), Nov. 2000.

[75] F. Grosshans and P. Grangier, "Continuous variable quantum cryptography using coherent states," *Phys. Rev. Lett.*, vol. 88, no. 5, pp. 057 902(1–4), Jan. 2002.

[76] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, "Quantum key distribution using Gaussian-modulated coherent states," *Nature*, vol. 421, no. 6920, pp. 238–241, Jan. 2003.

[77] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, "Quantum cryptography without switching," *Phys. Rev. Lett.*, vol. 93, no. 17, pp. 170 504(1–4), Oct. 2004.

[78] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, "Experimental demonstration of long-distance continuous-variable quantum key distribution," *Nat. Photonics*, vol. 7, no. 5, pp. 378–381, Apr. 2013.

[79] T. Wang, P. Huang, Y. Zhou, W. Liu, H. Ma, S. Wang, and G. Zeng, "High key rate continuous-variable quantum key distribution with a real local oscillator," *Opt. Express*, vol. 26, no. 3, pp. 2794–2806, Feb. 2018.

[80] D. Huang, P. Huang, D. Lin, and G. Zeng, "Long-distance continuous-variable quantum key distribution by controlling excess noise," *Sci. Rep.*, vol. 6, no. 1, pp. 19 201(1–9), Jan. 2016.

[81] D. B. Soh, C. Brif, P. J. Coles, N. Lütkenhaus, R. M. Camacho, J. Urayama, and M. Sarovar, "Self-referenced continuous-variable quantum key distribution protocol," *Phys. Rev. X*, vol. 5, no. 4, pp. 041 010(1–15), Oct. 2015.

[82] K. Inoue, "Differential phase-shift quantum key distribution systems," *IEEE J. Sel. Top. Quantum Electron.*, vol. 21, no. 3, pp. 109–115, Sep. 2014.

[83] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, "Limitations on practical quantum cryptography," *Phys. Rev. Lett.*, vol. 85, no. 6, pp. 1330–1333, Aug. 2000.

[84] A. Acin, N. Gisin, and V. Scarani, "Coherent-pulse implementations of quantum cryptography protocols resistant to photon-number-splitting attacks," *Phys. Rev. A*, vol. 69, no. 1, pp. 012 309(1–16), Jan. 2004.

[85] A. Gleim, V. Egorov, Y. V. Nazarov, S. Smirnov, V. Chistyakov, O. Bannik, A. Anisimov, S. Kynev, A. Ivanova, R. Collins *et al.*, "Secure polarization-independent subcarrier quantum key distribution in optical fiber channel using

BB84 protocol with a strong reference," *Opt. Express*, vol. 24, no. 3, pp. 2619–2633, Feb. 2016.

[86] E. Kiktenko, A. Trushechkin, Y. Kurochkin, and A. Fedorov, "Post-processing procedure for industrial quantum key distribution systems," in *J. Phys. Conf. Ser.*, vol. 741, no. 1. IOP Publishing, 2016, pp. 012 081(1–6).

[87] Y. Cao, Y. Zhao, C. Colman-Meixner, X. Yu, and J. Zhang, "Key on demand (KoD) for software-defined optical networks secured by quantum key distribution (QKD)," *Opt. Express*, vol. 25, no. 22, pp. 26 453–26 467, Oct. 2017.

[88] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, "Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems," *Phys. Rev. A*, vol. 78, no. 4, pp. 042 333(1–5), Oct. 2008.

[89] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, "Hacking commercial quantum cryptography systems by tailored bright illumination," *Nat. photonics*, vol. 4, no. 10, pp. 686–689, Aug. 2010.

[90] B. Huttner, N. Imoto, N. Gisin, and T. Mor, "Quantum cryptography with coherent states," *Phys. Rev. A*, vol. 51, no. 3, pp. 1863–1869, Mar. 1995.

[91] Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, "Experimental quantum key distribution with decoy states," *Phys. Rev. Lett.*, vol. 96, no. 7, pp. 070 502(1–4), Feb. 2006.

[92] M. Lucamarini, K. Patel, J. Dynes, B. Fröhlich, A. Sharpe, A. Dixon, Z. Yuan, R. Penty, and A. Shields, "Efficient decoy-state quantum key distribution with quantified security," *Opt. Express*, vol. 21, no. 21, pp. 24 550–24 565, Oct. 2013.

[93] H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," *Phys. Rev. Lett.*, vol. 94, no. 23, pp. 230 504(1–4), Jun. 2005.

[94] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, "Practical decoy state for quantum key distribution," *Phys. Rev. A*, vol. 72, no. 1, pp. 012 326(1–15), Jul. 2005.

[95] F. Grünenfelder, A. Boaron, D. Rusca, A. Martin, and H. Zbinden, "Simple and high-speed polarization-based QKD," *Appl. Phys. Lett.*, vol. 112, no. 5, pp. 051 108(1–3), Jan. 2018.

[96] D. Rosenberg, J. W. Harrington, P. R. Rice, P. A. Hiskett, C. G. Peterson, R. J. Hughes, A. E. Lita, S. W. Nam, and J. E. Nordholt, "Long-distance decoy-state quantum key distribution in optical fiber," *Phys. Rev. Lett.*, vol. 98, no. 1, pp. 010 503(1–4), Jan. 2007.

[97] Y. Liu, T.-Y. Chen, J. Wang, W.-Q. Cai, X. Wan, L.-K. Chen, J.-H. Wang, S.-B. Liu, H. Liang, L. Yang *et al.*, "Decoy-state quantum key distribution with polarized photons over 200 km," *Opt. Express*, vol. 18, no. 8, pp. 8587–8594, Apr. 2010.

[98] C.-Z. Peng, J. Zhang, D. Yang, W.-B. Gao, H.-X. Ma, H. Yin, H.-P. Zeng, T. Yang, X.-B. Wang, and J.-W. Pan, "Experimental long-distance decoy-state quantum key distribution based on polarization encoding," *Phys. Rev. Lett.*, vol. 98, no. 1, pp. 010 505(1–4), Jan. 2007.

[99] A. Lamas-Linares and C. Kurtsiefer, "Breaking a quantum key distribution system through a timing side channel," *Opt. Express*, vol. 15, no. 15, pp. 9388–9393, Jul. 2007.

[100] M.-S. Jiang, S.-H. Sun, G.-Z. Tang, X.-C. Ma, C.-Y. Li, and L.-M. Liang, "Intrinsic imperfection of self-differencing single-photon detectors harms the security of high-speed quantum cryptography systems," *Phys. Rev. A*, vol. 88, no. 6, pp. 062 335(1–5), Dec. 2013.

[101] F. Xu, M. Curty, B. Qi, and H.-K. Lo, "Measurement-device-independent quantum cryptography," *IEEE J. Sel. Top. Quantum Electron.*, vol. 21, no. 3, pp. 148–158, Dec. 2014.

[102] Ø. Marøy, L. Lydersen, and J. Skaar, "Security of quantum key distribution with arbitrary individual imperfections," *Phys. Rev. A*, vol. 82, no. 3, pp. 032 337(1–7), Sep. 2010.

[103] T. F. da Silva, G. B. Xavier, G. P. Temporão, and J. P. von der Weid, "Real-time monitoring of single-photon detectors against eavesdropping in quantum key distribution systems," *Opt. Express*, vol. 20, no. 17, pp. 18 911–18 924, Aug. 2012.

[104] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, "Device-independent security of quantum cryptography against collective attacks," *Phys. Rev. Lett.*, vol. 98, no. 23, pp. 230 501(1–4), Jun. 2007.

[105] X.-B. Wang, "Three-intensity decoy-state method for device-independent quantum key distribution with basis-dependent errors," *Phys. Rev. A*, vol. 87, no. 1, pp. 012 320(1–8), Jan. 2013.

[106] X.-L. Hu, Y. Cao, Z.-W. Yu, and X.-B. Wang, "Measurement-device-independent quantum key distribution over asymmetric channel and unstable channel," *Sci. Rep.*, vol. 8, no. 1, pp. 1–7, Dec. 2018.

[107] P. D. Townsend, "Simultaneous quantum cryptographic key distribution and conventional data transmission over installed fibre using wavelength-division multiplexing," *Electron. Lett.*, vol. 33, no. 3, pp. 188–190, Jan. 1997.

[108] S. Bahrani, M. Razavi, and J. A. Salehi, "Optimal wavelength allocation in hybrid quantum-classical networks," in *Proc. IEEE EUSIPCO*, Budapest, Hungary, 2016, pp. 483–487.

[109] T. J. Xia, D. Z. Chen, G. Wellbrock, A. Zavriyev, A. C. Beal, and K. M. Lee, "In-band quantum key distribution (QKD) on fiber populated by high-speed classical data channels," in *Proc. IEEE/OSA OFC*. Optical Society of America, Anaheim, California United States, 2006, p. OTuJ7.

[110] H. Kawahara, A. Medhipour, and K. Inoue, "Effect of spontaneous Raman scattering on quantum channel wavelength-multiplexed with classical channel," *Opt. Commun.*, vol. 284, no. 2, pp. 691–696, Jan. 2011.

[111] L. He, J. Niu, Y. Sun, and Y. Ji, "The four wave mixing effects in quantum key distribution based on conventional WDM network," in *Proc. IEEE COIN*, Jeju, South Korea, 2014, pp. 1–2.

[112] Y. Mao, B.-X. Wang, C. Zhao, G. Wang, R. Wang, H. Wang, F. Zhou, J. Nie, Q. Chen, Y. Zhao *et al.*, "Integrating quantum key distribution with classical communications in backbone fiber network," *Opt. Express*, vol. 26, no. 5, pp. 6010–6020, Mar. 2018.

[113] I. Choi, Y. R. Zhou, J. F. Dynes, Z. Yuan, A. Klar, A. Sharpe, A. Plews, M. Lucamarini, C. Radig, J. Neubert *et al.*, "Field trial of a quantum secured 10 Gb/s DWDM transmission system over a single installed fiber," *Opt. Express*, vol. 22, no. 19, pp. 23 121–23 128, Sep. 2014.

[114] K. Patel, J. Dynes, M. Lucamarini, I. Choi, A. Sharpe, Z. Yuan, R. Penty, and A. Shields, "Quantum key distribution for 10 Gb/s dense wavelength division multiplexing networks," *Appl. Phys. Lett.*, vol. 104, no. 5, pp. 051 123(1–4), Feb. 2014.

[115] L.-J. Wang, L.-K. Chen, L. Ju, M.-L. Xu, Y. Zhao, K. Chen, Z.-B. Chen, T.-Y. Chen, and J.-W. Pan, "Experimental multiplexing of quantum key distribution with classical optical communication," *Appl. Phys. Lett.*, vol. 106, no. 8, pp. 081 108(1–4), Feb. 2015.

[116] B. Korzh, C. C. W. Lim, R. Houlmann, N. Gisin, M. J. Li, D. Nolan, B. Sanguinetti, R. Thew, and H. Zbinden, "Provably secure and practical quantum key distribution over 307 km of optical fibre," *Nat. Photon.*, vol. 9, no. 3, pp. 163–168, Feb. 2015.

[117] J. F. Dynes, W. W. Tam, A. Plews, B. Fröhlich, A. W. Sharpe, M. Lucamarini, Z. Yuan, C. Radig, A. Straw, T. Edwards *et al.*, "Ultra-high bandwidth quantum secured data transmission," *Sci. Rep.*, vol. 6, pp. 35 149(1–6), Oct. 2016.

[118] J. Dynes, A. Wonfor, W.-S. Tam, A. Sharpe, R. Takahashi, M. Lucamarini, A. Plews, Z. Yuan, A. Dixon, J. Cho *et al.*, "Cambridge quantum network," *npj Quantum Inf.*, vol. 5, no. 101, pp. 1–8, Nov. 2019.

[119] X. Tang, A. Wonfor, R. Kumar, R. V. Penty, and I. H. White, "Quantum-safe metro network with low-latency reconfigurable quantum key distribution," *IEEE/OSA J. Lightw. Technol.*, vol. 36, no. 22, pp. 5230–5236, Nov. 2018.

[120] C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, and H. Yeh, "Current status of the DARPA quantum network," in *Quantum Information and Computation III*, E. J. Donkor, A. R. Pirich, and H. E. Brandt, Eds., vol. 5815, International Society for Optics and Photonics. SPIE, 2005, pp. 138 – 149. [Online]. Available: https://doi.org/10.1117/12.606489

[121] C. Elliott, "Building the quantum network," *New J. Phys.*, vol. 4, no. 1, pp. 46.1–46.12, Jul. 2002.

[122] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. Dynes *et al.*, "The SECOQC quantum key distribution network in Vienna," *New J. Phys.*, vol. 11, no. 7, pp. 075 001(1–37), Jul. 2009.

[123] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka *et al.*, "Field test of quantum key distribution in the Tokyo QKD network," *Opt. Express*, vol. 19, no. 11, pp. 10 387–10 409, May 2011.

[124] D. Stucki, M. Legre, F. Buntschu, B. Clausen, N. Felber, N. Gisin, L. Henzen, P. Junod, G. Litzistorf, P. Monbaron *et al.*, "Long-term performance of the

SwissQuantum quantum key distribution network in a field environment," *New J. Phys.*, vol. 13, no. 12, pp. 123 001(1–18), Dec. 2011.

[125] A. Mirza and F. Petruccione, "Realizing long-term quantum cryptography," *J. Opt. Soc. Am. B*, vol. 27, no. 6, pp. A185–A188, Jun. 2010.

[126] Z. Yuan and A. Shields, "Continuous operation of a one-way quantum key distribution system over installed telecom fibre," *Opt. Express*, vol. 13, no. 2, pp. 660–665, Jan. 2005.

[127] F. Xu, W. Chen, S. Wang, Z. Yin, Y. Zhang, Y. Liu, Z. Zhou, Y. Zhao, H. Li, D. Liu *et al.*, "Field experiment on a robust hierarchical metropolitan quantum cryptography network," *Chin. Sci. Bull.*, vol. 54, no. 17, pp. 2991–2997, Aug. 2009.

[128] R. Courtland, "China's 2,000-km quantum link is almost complete [News]," *IEEE Spectr.*, vol. 53, no. 11, pp. 11–12, Nov.2016.

[129] Z. Zhihao, "Beijing-Shanghai quantum link a 'new era'," *China Daily*, Sep. 2017. [Online]. Available: https://www.chinadaily.com.cn/china/2017-09/30/content_32669593.htm

[130] M. Razavi, A. Leverrier, X. Ma, B. Qi, and Z. Yuan, "Quantum key distribution and beyond: introduction," *OSA J. Opt. Soc. Am. B*, vol. 36, no. 3, pp. QKD1–QKD2, Mar. 2019.

[131] "ID Quantique." [Online]. Available: https://www.idquantique.com/

[132] "MagiQ Technologies, Inc." [Online]. Available: https://www.magiqtech.com/

[133] "Quantum Communications Hub." [Online]. Available: https://www.quantumcommshub.net/

[134] "QuintessenceLabs Pty Ltd." [Online]. Available: https://www.quintessencelabs.com/

[135] W. Chen, Z.-F. Han, T. Zhang, H. Wen, Z.-Q. Yin, F.-X. Xu, Q.-L. Wu, Y. Liu, Y. Zhang, X.-F. Mo *et al.*, "Field experiment on a "star type" metropolitan quantum key distribution network," *IEEE Photon. Technol. Lett.*, vol. 21, no. 9, pp. 575–577, Feb. 2009.

[136] T.-Y. Chen, J. Wang, H. Liang, W.-Y. Liu, Y. Liu, X. Jiang, Y. Wang, X. Wan, W.-Q. Cai, L. Ju *et al.*, "Metropolitan all-pass and inter-city quantum communication network," *Opt. Express*, vol. 18, no. 26, pp. 27 217–27 225, Dec. 2010.

[137] S. Wang, W. Chen, Z.-Q. Yin, Y. Zhang, T. Zhang, H.-W. Li, F.-X. Xu, Z. Zhou, Y. Yang, D.-J. Huang *et al.*, "Field test of wavelength-saving quantum key distribution network," *Opt. Lett.*, vol. 35, no. 14, pp. 2454–2456, Jul. 2010.

[138] S. Wang, W. Chen, Z.-Q. Yin, H.-W. Li, D.-Y. He, Y.-H. Li, Z. Zhou, X.-T. Song, F.-Y. Li, D. Wang *et al.*, "Field and long-term demonstration of a wide area quantum key distribution network," *Opt. Express*, vol. 22, no. 18, pp. 21 739–21 756, Sep. 2014.

[139] "SK Telecom." [Online]. Available: https://www.fiercewireless.com/wireless/sk-telecom-develops-advanced-quantum-repeater

[140] Q. Zhang, F. Xu, L. Li, N.-L. Liu, and J.-W. Pan, "Quantum information research in china," *Quantum Sci. Technol.*, vol. 4, no. 4, pp. 040 503(1–7), Nov. 2019.

[141] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, "Overcoming the rate–distance limit of quantum key distribution without quantum repeaters," *Nature*, vol. 557, no. 7705, pp. 400–403, May 2018.

[142] M. Loeffler, T. Länger, A. Neumann, M. Legré, I. Khan, C. Chunnilall, D. López, M. Lucamarini, and V. Martin, "Current Standardisation Landscape and existing Gaps in the Area of Quantum Key Distribution," *OpenQKD*, Dec. 2020. [Online].

Available: https://openqkd.eu/wp-content/uploads/2021/03/OPENQKD_CurrentStandardisationLandscapeAndExistingGapsInTheAreaOfQuantumKeyDistribution.pdf

[143] "ITU-T Study Group 13 - Future networks, with focus on IMT-2020, cloud computing and trusted network infrastructure," *International Telecommunication Union*. [Online]. Available: https://www.itu.int/en/ITU-T/about/groups/Pages/sg13.aspx

[144] ITU-T Recommendation Y.3804, "Quantum key distribution networks-Control and management," *International Telecommunication Union*, Geneva, Switzerland, Sep. 2020. [Online]. Available: https://www.itu.int/rec/T-REC-Y.3804-202009-I/en

[145] "ITU-T Study Group 17 – Security," *International Telecommunication Union*. [Online]. Available: https://www.itu.int/en/ITU-T/about/groups/Pages/sg17.aspx

[146] ITU-T XSTR-SEC-QKD, "Security consideration for quantum key distribution," *International Telecommunication Union*, Mar. 2020. [Online]. Available: https://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-QKD-2020-1-PDF-E.pdf

[147] "ETSI Quantum Key Disrtibution," *European Telecommunications Standards Institute*. [Online]. Available: https://www.etsi.org/technologies/quantum-key-distribution

[148] "Industry Specification Group (ISG) on Quantum Key Distribution Key (QKD) for Users ," *European Telecommunications Standards Institute*. [Online]. Available: https://www.etsi.org/committee/1430-qkd

[149] P1913 - Software-Defined Quantum Communication [Online]. Available: https://standards.ieee.org/project/1913.html.

[150] A. Beveratos, R. Brouri, T. Gacoin, A. Villing, J.-P. Poizat, and P. Grangier, "Single photon quantum cryptography," *Phys. Rev. Lett.*, vol. 89, no. 18, pp. 187 901(1–4), Oct. 2002.

[151] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[152] M. Taha and P. Schaumont, "Key updating for leakage resiliency with application to AES modes of operation," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 3, pp. 519–528, Mar. 2015.

[153] P. Derbez, P.-A. Fouque, and J. Jean, "Improved key recovery attacks on reduced-round AES in the single-key setting," in *Advances in Cryptology – EUROCRYPT 2013*, T. Johansson and P. Q. Nguyen, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 371–387.

[154] Y. Cao, Y. Zhao, X. Yu, H. Wang, C. Liu, B. Li, and J. Zhang, "Resource allocation in software-defined optical networks secured by quantum key distribution," in *Proc. IEEE OECC/PGC*, Singapore, 2017, pp. 1–3.

[155] M. Channegowda, R. Nejabati, and D. Simeonidou, "Software-defined optical networks technology and infrastructure: enabling software-defined optical network operations," *IEEE/OSA J. Opt. Commun. Netw.*, vol. 5, no. 10, pp. A274–A282, Oct. 2013.

[156] D. B. Rawat and S. R. Reddy, "Software defined networking architecture, security and energy efficiency: A survey," *IEEE Commun. Surv. Tuts.*, vol. 19, no. 1, pp. 325–346, 1st Quart. 2017.

[157] A. Aguado, E. Hugues-Salas, P. A. Haigh, J. Marhuenda, A. B. Price, P. Sibson, J. E. Kennard, C. Erven, J. G. Rarity, M. G. Thompson *et al.*, "Secure NFV orchestration over an SDN-controlled optical network with time-shared quantum key distribution resources," *IEEE/OSA J. Lightw. Technol.*, vol. 35, no. 8, pp. 1357–1362, Apr. 2017.

[158] A. Aguado, V. Lopez, J. Martinez-Mateo, T. Szyrkowiec, A. Autenrieth, M. Peev, D. Lopez, and V. Martin, "Hybrid conventional and quantum security for software defined and virtualized networks," *IEEE/OSA J. Opt. Commun. Netw.*, vol. 9, no. 10, pp. 819–825, Oct. 2017.

[159] Y. Zhao, Y. Cao, X. Yu, and J. Zhang, "Software defined optical networks secured by quantum key distribution (QKD)," in *Proc. IEEE/CIC ICCC*, Qingdao Shi, Shandong Sheng, China, 2017, pp. 1–4.

[160] E. Hugues-Salas, F. Ntavou, D. Gkounis, G. T. Kanellos, R. Nejabati, and D. Simeonidou, "Monitoring and physical-layer attack mitigation in SDN-controlled quantum key distribution networks," *IEEE/OSA J. Opt. Commun. Netw.*, vol. 11, no. 2, pp. A209–A218, Feb. 2019.

[161] S. Gringeri, N. Bitar, and T. J. Xia, "Extending software defined network principles to include optical transport," *IEEE Commun. Mag.*, vol. 51, no. 3, pp. 32–40, Mar. 2013.

[162] A. Aguado, V. Lopez, J. Martinez-Mateo, M. Peev, D. Lopez, and V. Martin, "Virtual network function deployment and service automation to provide end-to-end quantum encryption," *IEEE/OSA J. Opt. Commun. Netw.*, vol. 10, no. 4, pp. 421–430, Apr. 2018.

[163] X. Ning, Y. Zhao, X. Yu, Y. Cao, Q. Ou, Z. Liu, X. Liao, and J. Zhang, "Soft-reservation based resource allocation in optical networks secured by quantum key distribution (QKD)," in *Proc. OSA ACP*, Guangzhou, Guangdong China, 2017, pp. Su2A–66.

[164] H. Wang, Y. Zhao, Y. Li, X. Yu, J. Zhang, C. Liu, and Q. Shao, "A flexible key-updating method for software-defined optical networks secured by quantum key distribution," *Opt. Fiber Technol.*, vol. 45, pp. 195–200, Nov. 2018.

[165] X. Yang, Y. Li, G. Gao, Y. Zhao, H. Zhang, and J. Zhang, "Demonstration of

key generation scheme based on feature extraction of optical fiber channel," in *Proc. IEEE ACP*, Hangzhou, China, 2018, pp. 1–3.

[166] Y. Cao, Y. Zhao, J. Wang, X. Yu, Z. Ma, and J. Zhang, "KaaS: Key as a Service over quantum key distribution integrated optical networks," *IEEE Commun. Mag.*, vol. 57, no. 5, pp. 152 – 159, May 2019.

[167] K. Dong, Y. Zhao, X. Yu, J. Zhang, H. Yu, and Z. Li, "Auxiliary graph based routing, wavelength and time-slot assignment in metro quantum optical networks," in *Proc. IEEE OECC/PSC*, Fukuoka, Japan, 2019, pp. 1–3.

[168] K. Dong, Y. Zhao, X. Yu, J. Zhang, H. Yu, and Y. Zhang, "Auxiliary topology based global quantum key distribution for secure multicast service," in *Proc. IEEE OECC/PSC*, Fukuoka, Japan, 2019, pp. 1–3.

[169] K. Dong, Y. Zhao, T. Yang, Y. Li, A. Nag, X. Yu, and J. Zhang, "Tree-topology-based quantum-key-relay strategy for secure multicast services," *IEEE/OSA J. Opt. Commun. Netw.*, vol. 12, no. 5, pp. 120–132, Apr. 2020.

[170] K. Dong, Y. Zhao, X. Yu, A. Nag, and J. Zhang, "Auxiliary graph based routing, wavelength, and time-slot assignment in metro quantum optical networks with a novel node structure," *Opt. Express*, vol. 28, no. 5, pp. 5936–5952, Mar. 2020.

[171] K. Dong, Y. Zhao, A. Nag, X. Yu, and J. Zhang, "Distributed subkey-relay-tree-based secure multicast scheme in quantum data center networks," *Opt. Eng.*, vol. 59, no. 6, pp. 065 102(1–11), Jun. 2020.

[172] Y. Cao, Y. Zhao, J. Wang, X. Yu, Z. Ma, and J. Zhang, "SDQaaS: Software defined networking for quantum key distribution as a service," *Opt. Express*, vol. 27, no. 5, pp. 6892–6909, Mar. 2019.

[173] Y. Cao, Y. Zhao, R. Lin, X. Yu, J. Zhang, and J. Chen, "Multi-tenant secret-key assignment over quantum key distribution networks," *Opt. Express*, vol. 27, no. 3, pp. 2544–2561, Feb. 2019.

[174] Y. Cao, Y. Zhao, X. Yu, and J. Zhang, "Multi-tenant provisioning over software defined networking enabled metropolitan area quantum key distribution networks," *OSA J. Opt. Soc. Am. B*, vol. 36, no. 3, pp. B31–B40, Mar. 2019.

[175] Y. Cao, Y. Zhao, J. Li, R. Lin, J. Zhang, and J. Chen, "Reinforcement learning based multi-tenant secret-key assignment for quantum key distribution networks," in *Proc. IEEE/OSA OFC*, San Diego, CA, USA, 2019, pp. M2A–7.

[176] ——, "Multi-tenant provisioning for quantum key distribution networks with heuristics and reinforcement learning: A comparative study," *IEEE Trans. Netw. Service Manag.*, vol. 17, no. 2, pp. 946–957, Jan. 2020.

[177] H. Wang, Y. Zhao, X. Yu, Z. Ma, J. Wang, A. Nag, L. Yi, and J. Zhang, "Protection schemes for key service in optical networks secured by quantum key distribution (QKD)," *IEEE/OSA J. Opt. Commun. Netw.*, vol. 11, no. 3, pp. 67–78, Mar. 2019.

[178] W. Hua, Y. Zhao, X. Yu, A. Nag, Z. Ma, J. Wang, L. Yan, and J. Zhang, "Resilient quantum key distribution (QKD)- integrated optical networks with secret-key recovery strategy," *IEEE Access*, vol. 7, pp. 60 079– 60 090, May 2019.

[179] Y. Wang, X. Yu, J. Li, Y. Zhao, X. Zhou, S. Xie, and J. Zhang, "A novel shared backup path protection scheme in time-division-multiplexing based qkd optical networks," in *Proc. OSA ACP*, Chengdu, China, 2019, pp. M4C–6.

[180] L. Lu, X. Yu, Y. Zhao, and J. Zhang, "Dynamic wavelength and key resource adjustment in wdm based QKD optical networks," in *Proc. OSA ACP*, Beijing, China, 2020, pp. M4A–184.

[181] Y. Cao, Y. Zhao, J. Li, R. Lin, J. Zhang, and J. Chen, "Mixed relay placement for quantum key distribution chain deployment over optical networks," in *Proc. ECOC*. IEEE, 2020, pp. 1–4.

[182] X. Zou, X. Yu, Y. Zhao, A. Nag, and J. Zhang, "Collaborative routing in partially-trusted relay based quantum key distribution optical networks," in *Proc. OSA OFC*. Optical Society of America, San Diego, California, USA, 2020, pp. M3K–4.

[183] Y. Cao, Y. Zhao, J. Li, R. Lin, J. Zhang, and J. Chen, "Hybrid trusted/untrusted relay based quantum key distribution over optical backbone networks," *IEEE J. Sel. Areas Commun.*, Mar. 2021.

[184] Y. Cao, Y. Zhao, J. Wang, X. Yu, Z. Ma, and J. Zhang, "Cost-efficient quantum key distribution (QKD) over WDM networks," *IEEE/OSA J. Opt. Commun. Netw.*, vol. 11, no. 6, pp. 285–298, Jun. 2019.

[185] X. Li, Y. Zhao, A. Nag, X. Yu, and J. Zhang, "Key-recycling strategies in quantum-key-distribution networks," *Appl. Sci.*, vol. 10, no. 11, pp. 3734(1–19), Jan. 2020.

[186] B. Wen and K. M. Sivalingam, "Routing, wavelength and time-slot assignment in time division multiplexed wavelength-routed optical WDM networks," in *Proc. IEEE INFOCOM*, vol. 3, New York, NY, USA, 2002, pp. 1442–1450.

[187] S. Bahrani, M. Razavi, and J. A. Salehi, "Wavelength assignment in hybrid quantum-classical networks," *Sci. Rep.*, vol. 8, no. 1, pp. 3456(1–13), Feb. 2018.

[188] Y. Zhao, Z. Chen, J. Zhang, and X. Wang, "Dynamic optical resource allocation for mobile core networks with software defined elastic optical networking," *Opt. Express*, vol. 24, no. 15, pp. 16 659–16 673, Jul. 2016.

[189] D. Banerjee and B. Mukherjee, "A practical approach for routing and wavelength assignment in large wavelength-routed optical networks," *IEEE J. Sel. Areas Commun.*, vol. 14, no. 5, pp. 903–908, Jun. 1996.

[190] A. R. Dixon, Z. Yuan, J. Dynes, A. Sharpe, and A. Shields, "Continuous operation of high bit rate quantum key distribution," *Appl. Phys. Lett.*, vol. 96, no. 16, pp. 161 102(1–3), Apr. 2010.

[191] R. S. Tucker, G. Eisenstein, and S. K. Korotky, "Optical time-division multiplexing for very high bit-rate transmission," *IEEE/OSA J. Lightw. Technol.*, vol. 6, no. 11, pp. 1737–1749, Nov. 1988.

[192] W. Yu, B. Zhao, and Z. Yan, "Software defined quantum key distribution network," in *Proc. IEEE ICCC*, Chengdu, China, 2017, pp. 1293–1297.

[193] X. Yu, X. Ning, Q. Zhu, J. Lv, Y. Zhao, H. Zhang, and J. Zhang, "Multi-dimensional routing, wavelength, and timeslot allocation (RWTA) in quantum key distribution optical networks (QKD-ON)," *Appl. Sci.*, vol. 11, no. 1, pp. 348(1–14), 2021.

[194] H. Wang, Y. Zhao, Y. Li, X. Yu, J. Zhang, C. Liu, and Q. Shao, "A flexible key-updating method for software-defined optical networks secured by quantum key distribution," *Opt. Fiber Technol.*, vol. 45, pp. 195–200, 2018.

[195] S. Aleksic, F. Hipp, D. Winkler, A. Poppe, B. Schrenk, and G. Franzl, "Perspectives and limitations of QKD integration in metropolitan area networks," *Opt. Express*, vol. 23, no. 8, pp. 10 359–10 373, Apr. 2015.

[196] L. Ismail and H. Materwala, "A review of blockchain architecture and consensus protocols: Use cases, challenges, and solutions," *MDPI Symmetry*, vol. 11, no. 10, p. 1198, 2019.

[197] M. Belotti, N. Božić, G. Pujolle, and S. Secci, "A vademecum on blockchain technologies: When, which, and how," *IEEE Commun. Surv. Tuts.*, vol. 21, no. 4, pp. 3796–3838, 4th Quart. 2019.

[198] J. H. Park and J. H. Park, "Blockchain security in cloud computing: Use cases, challenges, and solutions," *MDPI Symmetry*, vol. 9, no. 8, p. 164, 2017.

[199] S. Nakamoto. (2008. Available Online:) Bitcoin: A peer-to-peer electronic cash system. 2008. available online:. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[200] U. Agarwal, V. Rishiwal, S. Tanwar, R. Chaudhary, G. Sharma, P. N. Bokoro, and R. Sharma, "Blockchain technology for secure supply chain management: A comprehensive review," *IEEE Access*, pp. 85 493–85 517, 2022.

[201] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, "Applications of blockchains in the internet of things: A comprehensive survey," *IEEE Commun. Surv. Tuts*, vol. 21, no. 2, pp. 1676–1717, 2nd Quart. 2018.

[202] A. Rahman, M. J. Islam, Z. Rahman, M. M. Reza, A. Anwar, M. P. Mahmud, M. K. Nasir, and R. M. Noor, "Distb-condo: Distributed blockchain-based iot-sdn model for smart condominium," *IEEE Access*, vol. 8, pp. 209 594–209 609, 2020.

[203] J. Sengupta, S. Ruj, and S. D. Bit, "A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT," *J. Netw. Comput.*, vol. 149, p. 102481, 2020.

[204] T. M. Fernández-Caramés and P. Fraga-Lamas, "Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks," *IEEE Access*, pp. 21 091–21 116, 2020.

[205] B. Schneier, *Applied cryptography*. Wiley (New York, NY), 1996.

[206] F. Toudeh-Fallah, M. Pistoia, Y. Kawakura, N. Moazzami, D. H. Kramer, R. I. Woodward, G. Sysak, B. John, O. Amer, A. O. Polychroniadou *et al.*, "Paving the way towards 800 gbps quantum-secured optical channel deployment in mission-critical environments," *arXiv preprint arXiv:2202.07764*, 2022.

[207] A. K. Fedorov, E. O. Kiktenko, and A. I. Lvovsky, "Quantum computers put blockchain security at risk," *Nature*, vol. 563, pp. 465–467, 2018.

[208] H. Krawczyk, "New hash functions for message authentication," in *EUROCRYPT*. Springer, 1995, pp. 301–310.

[209] P. Sharma, V. Bhatia, and S. Prakash, "Priority order-based key distribution in QKD-secured optical networks," in *Proc. IEEE Int. Conf. Adv. Netw. Telecommun. Syst. (ANTS)*, 2020, pp. 1–6 (New Delhi, India).

[210] ——, "Efficient ordering policy for secret key assignment in quantum key distribution-secured optical networks," *Opt. Fiber Technol.*, vol. 68, p. 102755, 2022.

[211] R. Van Gray, "To BLOB or not to BLOB: Large object storage in a database or a filesystem?" cs/0701168, Tech. Rep., 2007.

[212] W. Shi, Z. Zhu, M. Zhang, and N. Ansari, "On the effect of bandwidth fragmentation on blocking probability in elastic optical networks," *IEEE Trans. Commun.*, vol. 61, no. 7, pp. 2970–2978, 2013.

[213] B. C. Chatterjee, S. Ba, and E. Oki, "Fragmentation problems and management approaches in elastic optical networks: A survey," *IEEE Commun. Surv. Tutor.*, vol. 20, no. 1, pp. 183–210, 2018.

[214] P. Sharma, A. Agrawal, V. Bhatia, S. Prakash, and A. K. Mishra, "Quantum key distribution secured optical networks: A survey," *IEEE Open J. Commun. Soc.*, vol. 2, pp. 2049–2083, 2021.

[215] R. S. Sutton and A. G. Barto, *Reinforcement learning: An introduction*. MIT press, 2018.

[216] K. Arulkumaran, M. P. Deisenroth, M. Brundage, and A. A. Bharath, "Deep reinforcement learning: A brief survey," *IEEE Signal Process. Mag.*, vol. 34, no. 6, pp. 26–38, 2017.

[217] N. C. Luong, D. T. Hoang, S. Gong, D. Niyato, P. Wang, Y.-C. Liang, and D. I. Kim, "Applications of deep reinforcement learning in communications

and networking: A survey," *IEEE Commun. Surv. Tutor.*, vol. 21, no. 4, pp. 3133–3174, 2019.

[218] Y. Zuo, Y. Zhao, X. Yu, A. Nag, and J. Zhang, "Reinforcement learning-based resource allocation in quantum key distribution networks," in *ACP*, Beijing China, 2020, pp. T3C–6.

[219] J. Schulman, F. Walski, P. Dhariwal, A. Radford, and O. Klimov, "Proximal policy optimization algorithms," *arXiv preprint arXiv:1707.06347*, pp. 1–12, 2017.

[220] V. Mnih, K. Kavukcuoglu, D. Silver, A. A. Rusu, J. Veness, M. G. Bellemare, A. Graves, M. Riedmiller, A. K. Fidjeland, G. Ostrovski *et al.*, "Human-level control through deep reinforcement learning," *Nature*, vol. 518, no. 7540, pp. 529–533, 2015.

[221] A. Agrawal, V. Bhatia, and S. Prakash, "Spectrum efficient distance-adaptive paths for fixed and fixed-alternate routing in elastic optical networks," *Optical Fiber Technology*, vol. 40, pp. 36–45, 2018.

[222] D. P. Kingma and J. Ba, "Adam: A method for stochastic optimization," *arXiv preprint arXiv:1412.6980*, pp. 1–15, 2014.

List of Publications

Journal Papers:

1. Purva Sharma, Anuj Agrawal, Vimal Bhatia, Shashi Prakash, and Amit Kumar Mishra, "Quantum Key Distribution Secured Optical Networks: A Survey", *IEEE Open Journal of Communications Society*, vol. 2, pp. 2049-2083, 2021.

2. Purva Sharma, Vimal Bhatia, and Shashi Prakash, "Efficient Ordering Policy for Secret Key Assignment in Quantum Key Distribution-secured Optical Networks", *Optical Fiber Technology*, vol. 68, pp. 102755(1-9), 2021.

3. Purva Sharma, Kwonhue Choi, Ondrej Krejcar, Pavel Blazek, Vimal Bhatia, and Shashi Prakash, "Securing Optical Networks using Quantum-secured Blockchain: An Overview", *Sensors*, vol. 23, no. 3, pp. 1228(1-20), 2023.

4. Purva Sharma, Shubham Gupta, Vimal Bhatia, and Shashi Prakash, "Deep Reinforcement Learning-based Routing and Resource Assignment in Quantum Key Distribution-secured Optical Networks", *IET Quantum Communication*, vol. 4, no. 3, pp. 136-145, 2023.

5. Purva Sharma, Vimal Bhatia, and Shashi Prakash, "Impact of Fragmentation in Quantum Signal Channel of Quantum Key Distribution Enabled Optical Networks", *IET Quantum Communication*, vol. 5, no. 2, pp. 164-172, 2024.

Conference Papers:

1. Purva Sharma, Vimal Bhatia, and Shashi Prakash, "Priority Order Based Key Distribution in QKD-secured Optical Networks," *14th IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, Dec. 2020, New Delhi, India.

2. Purva Sharma, Vimal Bhatia, and Shashi Prakash, "Routing and Scheduling of Key Assignment in Quantum Key Distribution-secured Optical Networks," *15th IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, Dec. 2021, Hyderabad, India.

3. Purva Sharma, Vimal Bhatia, and Shashi Prakash, "Routing Based on Deep Reinforcement Learning in Quantum Key Distribution-secured Optical Networks," *17th IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, Dec. 2023, Jaipur, India.