

Kurdistan Region Government/Iraq
Presidency of the Council of Ministers
Ministry of Higher Education & Scientific Research
Erbil Polytechnic University
Technical Engineering College
Information System Engineering Department



Quantum Key Distribution Enhancement via Integration of SDN and CTR

A Dissertation

Submitted to the Council of the College of Technical
Engineering at Erbil Polytechnic University, in Partial
Fulfillment of the Requirements for the Degree of PhD of
Information System Engineering

by

Omar Shirko Mustafa

M.Sc. Information Technology

Supervised by

Prof. Dr. Shavan Kamal Askar

Erbil- Kurdistan Region

September 2023

بِسْمِ اللّٰهِ الرَّحْمٰنِ الرَّحِیْمِ

(نَرْفَعُ دَرَجَاتٍ مِّنْ نَّشَأٍ وَفَوْقَ كُلِّ ذِي عِلْمٍ عَلِيمٌ)

سورة يوسف - آية 79

Declaration

I declare that the PhD Dissertation entitled: "Quantum Key Distribution Enhancement via Integration of SDN and CTR" is my own original work, and hereby I certify that unless stated, all work contained within this dissertation is my own independent research and has not been submitted for the award of any other degree at any institution, except where due acknowledgment is made in the text.

Signature:



Student Name: **Omar Shirko Mustafa**

Date: 20/ 7/2023

Linguistic Review

I can affirm that I have carefully reviewed the dissertation titled "Quantum Key Distribution Enhancement via Integration of SDN and CTR" Also, from an English linguistic point of view, I can fully approve that this dissertation is free of both grammatical and spelling mistakes.

Signature:




Name: **Ahmed Sardar Mohamed**

Date: 26/7/2023

Supervisor Certificate


This dissertation has been written under my supervision and has been submitted for the award of the degree of PhD of Information System Engineering with my approval as supervisor.

Signature: 

Name: **Prof. Dr. Shavan Kamal Askar**

Date: 10/10/2023

I confirm that all requirements have been fulfilled.

Signature: 

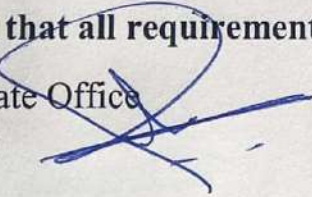
Name: **Dr. Roojwan Sc. Hawezi**

Head of the Department of Information System Engineering

Date: 10/10/2023

I confirm that all requirements have been fulfilled.

Postgraduate Office


Signature: 

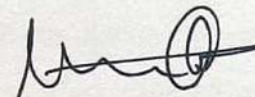
Name:


Date: 5/11/2023


Examining Committee Certification

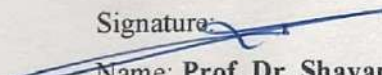
We certify that we have read this dissertation: "Quantum Key Distribution Enhancement via Integration of SDN and CTR" and as an examining committee examined the student (**Omar Shirko Mustafa**) in its content and what related to it. We approve that it meets the standards of a dissertation for the degree of PhD in Information System Engineering.


Signature: 
Name: **Ass.Prof.Dr Reem Jaafar**
Member
Date: 9/10/2023


Signature: 
Name: **Ass.Prof.Dr Marwan Aziz**
Member
Date: 10/10/2023

Signature: 
Name: **Ass.Prof.Dr Ismael Khorshed**
Member
Date: 10/10/2023

Signature: 
Name: **Ass.Prof.Dr Reben KURDA**
Member
Date: 9/10/2023

Signature: 
Name: **Prof. Dr. Shavan Askar**
Supervisor and Member
Date: 10/10/2023

Signature: 
Name: **Prof.Dr.Siddeeq Yousif**
Chairman
Date: 10/10/2023

Approved by: 
Dean of the College of Erbil Technical Engineering
Signature:
Name: **Prof. Dr. Ayad Zaki Saber**
Date: 29/10/2023

Acknowledgements

In the name of Allah, the Merciful and the Compassionate. We are grateful to Almighty Allah for supporting us in order to complete this dissertation. We are also grateful to those people who have contributed in the completion of this work.

I am grateful to Professor Dr. Shavan Kamal Askar for being the best guider and advisor for us during the completion of this research work requirement in all fields. His ideas and inspirations have helped me make this idea of mine into a fully-fledged project. Without, I may never had tried research works.

Again, I am thankful to my batch-mates for supporting me at times of my implementation part. I am also grateful to all the professors in my department for always being a constant source of inspiration and motivation during the entire course of the project.

Lastly, I thank both of my parents and especially my wife for all their encouragement, support and guidance, which enabled me to reach this stage in my research project.

Dedication

This dissertation is dedicated to Almighty Allah,
Asking for acceptance while also hoping that this will be a good work for all the
fellow scholars and researchers.

For all people who never lost hope in me and always believed in me.

To my brother who supported me and helped me to complete this study.

To my mother who raised and guided me throughout my whole life while always
supporting me in each and step.

To my wife who was always on my side no matter what.

Abstract

Quantum Key Distribution (QKD) represents a groundbreaking application of quantum physics for secure symmetric encryption key distribution. This method exploits quantum mechanics unique attributes, such as the no-cloning theorem and Heisenberg uncertainty principle, to create inherently secure keys resistant to eavesdropping. However, the primary challenge is the exponential reduction in key distribution rates as distances increase. To extend the secure communication range of QKD networks, a Classic Trusted Relay (CTR) scheme has been proposed, introducing trusted intermediate nodes for enhanced security over distance. Nevertheless, concerns regarding trust requirements in relay nodes and communication channel reliability pose significant risks, potentially leading to CTR failures and overall system security compromise.

This dissertation presents a novel approach addressing CTR failure challenges and optimizing generated key utilization. The solution integrates Software-Defined Networking (SDN) with QKD, capitalizing on SDN's flexibility and control for improved network management. SDN, dividing the network into control and data planes, offers unified management and programmability. To enhance QKD network resilience and reliability, the Software-Defined Quantum Trusted Relay Failure (SDQTRF) model is proposed. This model employs a new SDN controller function to effectively orchestrate QKD network operations. By incorporating SDN capabilities, the SDQTRF model enhances fault tolerance and the system's ability to recover from relay failures. The SDN controller actively monitors the QKD network, including relay node status and key distribution processes. Upon detecting a relay failure, the SDN controller responds proactively by reconfiguring the network through key recycling using Q-learning. If recycling fails, the controller reroutes the key distribution process through alternative paths

determined by the Q-learning method. This proactive approach minimizes relay failure impact, ensures continuous key distribution, and preserves system security.

To assess the SDQTRF model's effectiveness, extensive simulations were conducted on two distinct network topologies: the National Science Foundation Network (NSFNET) and the United States network (USNET). Simulations utilized a high-performance NVIDIA GeForce RTX 3060Ti GPU and ran on the Windows 11 operating system, which provided stability. To simulate the proposed SDQTRF model, JavaScript, PHP, and Python programming languages using NetworkX library were employed due to their flexibility and extensive libraries for scientific computing and network simulations. Simulation results indicate significant improvements, including a substantial increase in the key generation ratio, remarkable key utilization rate enhancement, impressive recovery after failure rates, considerable reduction in the avalanche effect, and a lower service-blocking rate due to SDQTRF model implementation.

Table of Contents

CHAPTER ONE: INTRODUCTION	1
1.1 Overview.....	1
1.2 Problem Statement.....	3
1.3 The Aim of Research.....	5
1.4 Research Objectives	5
1.5 Contributions Statement	5
1.6 The Scope of the Dissertation.....	6
1.7 Outline of Dissertation.....	7
CHAPTER TWO: THEORETICAL BACKGROUND	9
2.1 Introduction	9
2.2 Unconditional Security in Cryptography	9
2.3 Quantum Key Distribution.....	10
2.3.1 Fundamental Principles of QKD.....	12
2.3.2 Mechanism of Point-To-Point QKD	14
2.3.4 Compare Between BB84 and SARG04 Protocols.....	17
2.4 Long-Distance Transmission of QKD Network	18
2.4.1 Quantum Repeater.....	19
2.4.2 Classical Trusted Relay Technology.....	20
2.5 Software-Defined Networking	24
2.5.1 QKD Enabled By SDN Architecture	26
CHAPTER THREE: LITERATURE REVIEWS	29
3.1 Introduction	29
3.2 Advances in Relay-Based QKD.....	29
3.2.1 Previous works for CTR technology.....	30
3.3 Integrating SDN with QKD Networks.....	34
3.3.1 Previous Studies of SDN Over QKD.....	34

3.4 Advancements in ML Over QKD	39
3.4.1 Previous Studies of ML Over QKD.....	40
3.5 SDQTRF Model Proposed	42
CHAPTER FOUR: METHODOLOGY	44
4.1 Introduction	44
4.2 Proposed Model of SDQTRF.....	44
4.2.1 System Model of SDQTRF.....	44
4.2.2 Methodology of SDQTRF Model.....	46
4.2.3 Algorithm of SDQTRF Model.....	56
4.3 SARAG04 Protocol.....	59
4.3.1 Modeling Quantitative Cases	63
4.4 Q-learning Method	65
CHAPTER FIVE: EXPERIMENTAL RESULTS AND DISCUSSION..	68
5.1 Introduction	68
5.2 Simulation Results	68
5.2.1 Simulation Performance of SDQTRF Model	73
5.3 Q-learning Results.....	93
5.3.1 Q-Learning Results for Recycling Process	94
5.3.2 Q-Learning Results for Alternative Secure Path	102
5.3.2.1 Alternative NSFNET Topology Route Results	104
5.3.2.2 Alternative USNET Topology Route Results.....	105
5.4 Results of SARAG04 Protocol	108
CHAPTER SIX: CONCLUSION AND FUTURE WORKS	120
6.1 Conclusion.....	120
6.2 Future Directions and Recommendations	121

List of Figures

Fig. 2-1 Point-to-point QKD mechanism based on BB84 protocol.....	16
Fig. 2-2 An example of QKD distance extension based on a CTR technology between the source and destination nodes.	21
Fig. 2-3 Examples of the Models of BBN, Re-encryption and Public –XOR-Key Schemes with Two Endpoints and Three CTR Nodes.....	23
Fig. 2-4 QKD over SDN architecture	28
Fig. 4-1 Contingency function inside the controller	48
Fig. 4-2 Proposed relay key protocol	50
Fig. 4-3 Example of the recycling process.....	53
Fig. 4-4 the proposed process to find a new secure path	56
Fig. 5-1 NSFNET network topology.....	70
Fig. 5-2 USNET network topology.....	70
Fig. 5-3 KGR in NSFNET	75
Fig. 5-4 KGR in USNET.....	76
Fig. 5-5 KUR in NSFNET	79
Fig. 5-6 KUR in USNET.....	80
Fig. 5-7 Time elapsed of RAF in NSFNET	83
Fig. 5-8 Time elapsed of RAF in USNET	83
Fig. 5-9 AETF in NSFNET	87
Fig. 5-10 AETF in USNET	88
Fig. 5-11 The Service-Blocking Rate (SBR) in NSFNET	91
Fig. 5-12 The Service-Blocking Rate (SBR) in USNET	91
Fig. 5-13 Learning Progression for the Path [1, 8, 11, 14] of NSFNET.....	99
Fig. 5-14 Learning Progression for the Path [2, 4, 10, 12] of NSFNET.....	100
Fig. 5-15 Learning Progression for the Path [1, 6, 9, 12, 16, 22, 23] of USNET	100
Fig. 5-16 Learning Progression for the Path [4, 8, 10, 14, 18, 24] of USNET	101
Fig. 5-17 Unsecure Nodes of the first path in NSFNET	104
Fig. 5-18 Unsecure Nodes of the second path NSFNET	104
Fig. 5-19 Training Progression of alternative secure path [1, 2, 4, 10, 14]	105
Fig. 5-20 Training Progression of Alternative Secure Path [2, 1, 8, 11, 12] ...	105
Fig. 5-21 Unsecure Nodes of the First Path in USNET	105
Fig. 5-22 Unsecure Nodes of the Second Path in USNET	106

Fig. 5-23 Training progression of Alternative Secure Path [1, 6, 11, 15, 16, 22, 23].....	107
Fig. 5-24 Training Progression of Alternative Secure Path [4, 8, 10, 13, 17, 23, 24].....	107
Fig. 5-25.A NSFNET Node1 to Node2.....	109
Fig. 5-25.C NSFNET Node4 to Node10.....	110
Fig. 5-25.D NSFNET Node 10 to Node 14.....	110
Fig. 5-26.A NSFNET Node 2 to Node1.....	111
Fig. 5-26.B NSFNET Node 1 to Node8.....	111
Fig. 5-26.C NSFNET Node 8 to Node11.....	112
Fig. 5-26.D NSFNET Node 11 to Node12.....	112
Fig. 5-27.A USNET Node 1 to Node 6.....	113
Fig. 5-27.B USNET Node 6 to Node 11.....	114
Fig. 5-27.C USNET Node 11 to Node 15.....	114
Fig. 5-27.D USNET Node 15 to Node 16.....	115
Fig. 5-27.E USNET Node 16 to Node 22.....	115
Fig. 5-27.F USNET Node 22 to Node 23.....	116
Fig. 5-28.A USNET Node 4 to Node 8.....	116
Fig. 5-28.B USNET Node 8 to Node 10.....	117
Fig. 5-28.C USNET Node 10 to Node 13.....	117
Fig. 5-28.D USNET Node 13 to Node 17.....	118
Fig. 5-28.E USNET Node 17 to Node 23.....	118
Fig. 5-28.F USNET Node 23 to Node 24.....	119

List of Tables

Table 3-1 Comparative Analysis of QKD Networks Based on CTR Technology	32
Table 3-2 Comparative Analysis of Previous Works in Integrating QKD with SDN	37
Table 3-3 Comparative Analysis of Previous Works in Integrating ML with QKD	41
Table 4-1 Comprehensive the Notation and definitions of system model.....	46
Table 4-2 SDQTRF algorithm	57
Table 4-3 Illustrate example of the SARG04 protocol in working.....	61
Table 4-4 Comprehensive list of states transmittable and measurable in the SARG04 protocol using random rules	65
Table 5-1 Average simulation result for the mechanism of the SDQTRF model in the NSFNET and USNET topologies over the whole simulation run	73
Table 5-2 Q-table for NSFNET and USNET	96

Appendix

Appendix A	A1
Flowchart A.1 Create a TCP connection	A1
Flowchart A.2 SARAG04 protocol stages through handshake signals	A2
Flowchart A.3 Continuo with (A) handshake signals	A3
Flowchart A.4 Continuo with (B) handshake signals	A4
Flowchart 4.5 Quantum transmission stage	A5
Flowchart 4.6 Receiving sent quantum cases	A6
Flowchart 4.7 Bases used in the measurement	A6
Flowchart 4.8 Check the bases used in the measurement	A7
Flowchart 4.9 Depicting raw key sifting stages	A8
Flowchart 4.10 Process of encoding Qubits.....	A8
Flowchart 4.11 Steps involved in error correction.....	A9
Flowchart 4.12 Outlines the Q-Learning algorithm.....	A10

List of Abbreviations

Abbreviation	Acronyms
ACK _{fn} (i,j)	Notification at Failure Sending
ACK _n (i,j)	Notification at Success Sending Delivered
ACK _r	Notification from controller to nsf to start recycling
AETF	Avalanche-Effect-Total-Failure
AI	Artificial Intelligence
BB84	Bennett and Brassard 1984
BBN	Bolt, Beranek, and Newman
BP	Backward Propagation
C	Connecting Link
CTR	Classic Trusted Relay
CV	Continuous Variable
DeepRL	Deep Reinforcement Learning
DL	Deep Learning
DN	Destination Node
DoS	Denial of Service
DROM	Deep Reinforcement learning Optimized Routing
DV-QKD	Distributed-Variable Quantum Key Distribution
ETSI	European Telecommunications Standards Institute
G	Graph
G _{kn}	Key Generate for Pair Nodes
ILP	Integer Linear Programming
IoT	Internet of Things
KDSR	Key Distribution Success Rate
KGR	Key Generation Ratio
KoD	Key on Demand
KP	Key Pool
KUR	Key Utilization Rate
LSTM	Long-Short-Term Memory
MDI-QKD	Measurement-Device Independent Quantum Key
MDP	Markov Decision Process
ML	Machine Learning
MTU	Maximum Transmission Unit
N	Nodes
N _{fi}	Pair Nodes Failure
NFV	Network Function Virtualization
NMs	Networked Microgrids
NSFNET	National Science Foundation Network

Nxi	Next Node in Secure Path
ONF	Open Networking Foundation
On-MTP	Online Multi-Tenant Provisioning
ONOS	Open Network Operating System
OSPF	Open Shortest Path First
PQNM	Programmable Quantum Networked Microgrids
PT-RA	Partially-Trusted Based Routing Algorithm
QaaS	QKD as a Service
QAI	Quantum Abstraction Interface
QBER	Quantum Bit Error Rate
QKD	Quantum Key Distribution
QKDNs	Quantum Key Distribution Nodes
QKP	Quantum Key Pool
QKR	Quantum Key Recycling
QN	Q-Value between Each Pair Nodes
QoS	Quality-of-Service
QSA	Quantum Services Architecture
RAF	Recovery After Failure
RIP	Routing Information Protocol
Rkn	Recycling for Pair Nodes
RL	Reinforcement Learning
RTT	Round Trip Time
S	Secure Node
SARG04	(Valerio Scarani, Antonio Acin, Gregoire Ribordy, and Nicolas Gisin) 2004
SBR	Service-Blocking Rate
SDN	Software Defined Network
SDON	Software-Defined Optical Network
SDQTRF	Software-Defined Quantum Trusted Relay Failure
SKR	Secret Key Rate
SN	Source Node
SP	Secure Path
SPn	New Generation Secure Path
US	Unsecure Node
USNET	United States Network
VKP	Virtual Key Pool
VM	Virtual Machine
VPNs	Virtual Private Networks
WDM	Wavelength Division Multiplexing

CHAPTER ONE: INTRODUCTION

1.1 Overview

The global Internet user population is projected to reach approximately 66% by 2023, indicating a significant increase from 51% (equivalent to 3.9 billion individuals) in 2018 to 66% (equivalent to 5.3 billion individuals) in 2023 (CISCO, U. 2020). This surge in internet accessibility is expected to lead to an escalation in security breaches, including eavesdropping and data interception. Consequently, this could result in the compromise of personal information, financial losses, and substantial service disruptions (Skorin-Kapov et al., 2016; Furdek et al. 2014). As reliance on internet-based communication grows, the adoption of cryptographic techniques becomes increasingly vital to ensure the safety and security of digital interactions (Dong et al., 2019). These techniques offer a crucial layer of protection against unauthorized access, data breaches, and potential threats that could jeopardize the confidentiality and integrity of sensitive information exchanged online (Dong et al., 2019). By employing cryptographic techniques, individuals and organizations can have greater confidence in the privacy and reliability of their online communications, safeguarding their data from potential risks and ensuring a safer digital environment (Dong et al., 2019).

However, a critical aspect of cryptography involves establishing secure cryptographic keys over untrusted networks (Mehic et al., 2020). Historically, encryption methods based on public-key cryptography have been used to distribute cryptographic keys across unreliable networks. However, the security provided by traditional public-key cryptography, based on computational complexity, has been compromised by rapid advancements in processor chips and the emergence of quantum computers (Zapatero et al., 2023; Campagna et al., 2015; Sharma, 2021). This renders existing encryption techniques inadequate to ensure security in the era

of quantum computing. Consequently, a different approach is necessary to protect data transmitted across communication networks from these vulnerabilities (Aguado et al., 2017). Quantum Key Distribution (QKD) emerges as a highly promising substitute for conventional data encryption approaches (Hugues-Salas et al., 2019). Grounded in the fundamental principles of quantum mechanics, including the Heisenberg uncertainty principle (Heisenberg, 1985) and the quantum no-cloning theorem (Scarani et al., 2009), QKD utilizes quantum secret keys to establish a secure connection between remote entities (Lo et al., 2014; Zhao et al., 2018; Langer, 2013).

However, QKD has predominantly been applied to point-to-point communications, limiting its scalability and practicality for large-scale networks (Diamanti et al., 2016; Scarani et al., 2009; Broadbent & Schaffner, 2016). The rate of key distribution in point-to-point of QKD networks decreases exponentially with distance, making it challenging to implement them in large-scale communication networks like the internet (Diamanti et al., 2016; Pirandola et al., 2020). Additionally, direct quantum links between every pair of communicating parties are impractical, and a dedicated quantum channel is required for each communication link, making the network complex and costly to implement (Diamanti et al., 2016; Broadbent & Schaffner, 2016). Point-to-point based QKD networks are also vulnerable to attacks on communication channels, compromising the security of generated keys (Scarani et al., 2009).

To address these challenges, Classic Trusted Relay (CTR) techniques, which rely on trusted intermediate relay nodes, have been introduced in QKD networks to extend communication range and improve key distribution efficiency over classical channels (Peev et al., 2009). However, the reliance on trusted relay nodes introduces

security risks, as any compromise or failure of a relay node can lead to the loss or compromise of keys (Dong et al., 2019).

Software-Defined Networking (SDN) presents a promising approach to achieve a flexible and efficient QKD network, despite potential complexities and resource wastage associated with CTR (Mehic et al., 2020). SDN enables dynamic network management through programmable control of devices and traffic flows, offering benefits like improved reliability, enhanced security features, increased scalability, and better adaptability to changing conditions (Sharma et al., 2021; McKeown et al., 2008; Karinou et al., 2018; Wang et al., 2019; Cao et al., 2020). Additionally, techniques such as Artificial Intelligence (AI), Machine Learning (ML), Deep Learning (DL), and optimization can further enhance the effectiveness of QKD networking (Sharma et al., 2021). Specifically, Reinforcement Learning (RL) algorithms, a subset of ML techniques, offer a powerful tool to train QKD networks to adapt to changing conditions, ultimately leading to improved performance and efficiency (McPartland & Gallagher, 2008; Zeng et al., 2020; Zhang et al., 2021; Yu et al., 2018; Cao et al., 2019). However, practical implementation of RL in QKD networks requires careful consideration of computational resources and training time (Cao et al., 2020).

1.2 Problem Statement

Transmission of weak quantum signals in quantum channels results in a limitation on the secret key rate and distance of QKD due to signal attenuation. Quantum repeaters offer a potential solution to overcome this limitation, but currently, practical technologies are unable to implement them. To address this challenge in a practical manner, a compromise solution is to employ CTR technology, which has been widely adopted in the deployment of most QKD networks to date. Nevertheless, the secret keys utilized in QKD networks hold

significant value, and one of the primary objectives of CTR technology is to securely transmit quantum keys to remote QKD nodes over the public channel through highly secure encryption methods.

In a QKD network utilizing CTR technology, the secret keys produced in the initial QKD link can be transmitted to the destination node by encrypting them using the secret keys generated in the intermediate nodes. Furthermore, it is essential for the CTR nodes to be protected against unauthorized access and potential attacks, ensuring their security from any unauthorized parties. In general, the quantum channels of QKD networks can theoretically detect all eavesdropping behaviors, while the signals in public channels cannot guarantee be immune to eavesdropping. Furthermore, the functioning of key distribution in CTR-based systems takes place over the public channel of the QKD system, making it impossible to achieve immunity against eavesdropping. Consequently, if any of the CTR nodes are compromised, the entire network is considered vulnerable. In such scenarios, a compromised CTR node signifies the failure of the CTR technique to distribute quantum secret keys across QKD systems. To address this issue, a key redistribution process is implemented. This step becomes necessary due to potential eavesdropping activities or malicious attacks that may cause the failure of the key-relay process. To ensure the absolute security of the redistributed keys at each stage of the procedure, meeting the requirement of one-time key use, all quantum keys used in the relay process to establish secure long-distance communication between end-users must be eradicated. Consequently, this presents a greater demand for QKD network secret keys, making it challenging to meet the security requirements of the service. This represents one of the major hurdles in CTR-based QKD networks.

1.3 The Aim of Research

This dissertation addresses QKD network challenges by proposing a novel security model, enhancing integrity and confidentiality. It emphasizes integrating SDN techniques for efficient management, control, and proactive security responses.

1.4 Research Objectives

The objective of this research is to overcome the limitations of the current technique used to increase the coverage range of QKD systems, i.e. the CTR technology, and to introduce a new survivability model called Software-Defined Quantum Trusted Relay Failure (SDQTRF) that proposes the use of SDN over QKD networks to manage the secret key in case of CTR failure. This research also emphasizes the lack of existing work on this topic and utilize the benefits of using SDN to minimize the effects of CTR failure on the performance of QKD networks. The objectives of this research can be dropdown as follows:

- 1- To develop a novel survival model to overcome the challenges of the CTR technique failure based on the QKD network.
- 2- To enhance the management of unsuccessful relayed keys based on CTR technology.
- 3- To improve the security of the recycling process in order to increase the survivability of quantum secret keys that were not successfully relayed.
- 4- To provide a novel routing approach for discovering a different, secure route.

1.5 Contributions Statement

This research proposes a novel survivability model called SDQTRF to address the challenges of the CTR failure in a QKD networks. The SDN controller in this model takes on the responsibility of mitigating the impact of CTR failure, using a

dynamic, real-time security monitoring and recovery mechanism. The research presents three primary contributions:

1. Introduction of a novel SDN controller with an added function and a new relay protocol: The proposed SDN controller has a new function to improve the management of unsuccessful relayed keys. Additionally, a new relay protocol has been introduced to enhance the management of the keys that are not successfully relayed.
2. Novel concept to improve the security of secret key recycling: This research presents a new model to improve the security of secret key recycling. This is achieved by adding RL algorithm (Q-learning) to increase the survivability of quantum secret keys that were not successfully relayed.
3. New scenario for finding an alternative secure path: This research presents a novel scenario that plays an effective role in finding an alternative secure path in case of failing to relay the recycled secret keys. This scenario is critical for ensuring the continued operation of the QKD network in the event of a failure or attack.

1.6 The Scope of the Dissertation

The scope of this dissertation is to propose a new scheme to overcome the issues associated with the CTR technology in QKD networks. The study aims to introduce a novel survivability model, called SDQTRF, which utilizes SDN techniques to enhance the resilience of QKD networks against failures and improve their management.

To achieve these objectives, the study will first review the existing literature on QKD and SDN to identify the challenges associated with the CTR and the potential benefits of using SDN in QKD networks. The study will then propose the

SDQTRF model, which uses a new function added to the SDN controller in order to enhance the dependability and efficiency of QKD networks.

The study will evaluate the proposed SDQTRF model performance by conducting simulations utilizing JavaScript, PHP and Python. The evaluation will focus on various performance metrics, such as key generation ratio, key utilization rate, recovery after failure, avalanche effect, and service blocking rate.

Finally, the study will discuss the practical implications and limitations of the proposed SDQKRF model, as well as the future research directions in this field. The scope of this study is limited to the proposed SDQKRF model and its evaluation using simulations, and does not cover other aspects of QKD or SDN.

1.7 Outline of Dissertation

The outline of the remaining chapters of the dissertation is as follows:

Chapter 2: Presents a comprehensive background of unconditional security, provably secure cryptography, QKD with the BB84 and SARG04 protocols, Quantum Repeaters, long-distance transmission in QKD networks, security protocols, CTR technology and its protocols for secure data transmission among multiple parties, QKD-enabled secure communication networks, and the integration of QKD with SDN.

Chapter 3: Provides an overview of previous research on QKD networks, including discussions on enhancing the safety of CTR technology, utilizing SDN over QKD for managing secret keys, and thorough exploration of ML techniques integration in QKD networks

Chapter 4: Demonstrates the various contributions of the proposed model methodology in solving the challenge of distributing quantum secret keys using CTR

technology, including implementing QKD over SDN, selecting the SARAG04 protocol, proposing a new relay protocol, improving the recycling process with Q-learning, and introducing a routing method for alternative secure paths.

Chapter 5: Provides detailed outcomes and findings of simulations and evaluations on the SDQTRF model, showcasing its effectiveness in mitigating CTR failures, enhancing key distribution security, and adapting to network dynamics, while also evaluating its resilience against attacks and node compromises, and highlighting the performance of the incorporated relay protocol.

Chapter 6: Presents the conclusions and future work about this dissertation.

CHAPTER TWO: THEORETICAL BACKGROUND

2.1 Introduction

This chapter provides an overview of unconditional security, and QKD, including the fundamental principles of QKD and the mechanisms used in point-to-point QKD based on the BB84 protocol and SARG04 protocol. The security of these protocols is also discussed, as well as the challenges associated with long-distance transmission in QKD networks and the use of Quantum Repeaters. The chapter also discusses CTR technology, which enables the secure transmission of information between multiple parties using trusted intermediaries, and various CTR technology protocols. Additionally, the potential of SDN for QKD-enabled secure communication networks is explored, as well as the integration of QKD and SDN.

2.2 Unconditional Security in Cryptography

Cryptography is the science of secure communication, aiming to ensure that information exchanged between parties remains confidential and unaltered by any malicious third party. Unconditional security, also known as information-theoretic security, stands as a concept that provides an unparalleled level of security, distinct from computational security, which hinges on the difficulty of solving specific mathematical problems (Shannon, 1949; Goldreich, 2001). At the core lies the notion of perfect secrecy, where even with unlimited computational power, an adversary intercepting the encrypted message gains no additional information about the original message (Shannon, 1949; Goldreich, 2001). The one-time pad exemplifies an unconditionally secure encryption scheme, employing a key as long as the message, generated randomly and never reused (Shannon, 1949; Goldreich, 2001). In an information-theoretically secure system, an adversary's ability to glean information about the original message through intercepting the ciphertext is precisely zero (Maurer, 1993; Renner and König, 2005). Unconditional security

ensures an absolute guarantee of secrecy, devoid of reliance on assumptions regarding computational capabilities or mathematical problem hardness (Maurer, 1993; Renner and Konig, 2005). Although perfect secrecy is rare in practical cryptography, the one-time pad is a notable example, necessitating a key as long as the message itself, rendering it impractical for most real-world applications (Scarani et al., 2009; Nielsen and Chuang, 2002). This pinnacle of information security finds applications in various critical scenarios, from diplomatic and military communications to the transmission of sensitive infrastructure information (Shannon, 1949; Renner and Konig, 2005).

2.3 Quantum Key Distribution

Quantum cryptography, specifically QKD, has emerged as one of the most advanced sectors within the field of quantum information technologies, providing an unparalleled level of unconditional security (Carrasco-Casado et al., 2016). QKD is a method of secure communication that uses the principles of quantum mechanics to generate and distribute secret cryptographic keys between two parties (Van Assche, 2006; Rieffel & Polak, 2011). The basic idea behind QKD is to use quantum phenomena to create a shared secret key between two parties that can be used for secure communication (Dianati & Alleaume, 2007; Scarani & Kurtisefer, 2014).

In traditional cryptography, the same key is used for both encryption and decryption, and the key must be securely distributed to all parties involved in the communication (Pucella, 2005; Giron et al., 2023). However, this distribution process is vulnerable to interception and hacking, which can compromise the security of the entire communication (Katz & Lindell, 2014; Bruce, 1996; Wolf, 2021). QKD provides a solution to this problem by allowing two parties to generate a shared secret key that is secure against eavesdropping (Bennett & Brassard, 1984).

QKD works by using single photons (particles of light) to encode information (Nielsen & Chuang, 2002). The polarization of the photon is used to represent a bit of information, either 0 or 1 (Bennett & Brassard, 1984). The sender, known as Alice, sends a stream of photons to the receiver, known as Bob. Alice randomly selects a polarization for each photon and sends it to Bob. Bob randomly chooses a polarization to measure the photon with, and records the result. The two parties compare their polarization choices, and if they chose the same polarization, this bit is used as a part of the secret key. If they chose different polarizations, this photon is discarded (Bennett & Brassard, 1984).

The QKD security is based on the fundamental quantum mechanics. Any attempt to intercept or measure a photon in transit will disturb its state, and any measurement of the photon's polarization will result in the photon changing its state (Maurer, 2001; Bennett & Brassard, 1984). This means that any eavesdropping on the communication will be detected by the communicating parties, and the shared key will not be compromised (Bennett & Brassard, 1984; Wolf, 2021).

QKD has been shown to be secure against all known types of attacks, including attacks using advanced technologies such as quantum computers (Mehic et al., 2020). This makes QKD a promising technology for secure communication in fields such as finance, government, and military communications (Scarani et al., 2009). However, QKD is still an emerging technology, and there are challenges to its practical implementation, including issues with distance and the stability of quantum communication channels (Scarani et al., 2009; Langer, 2013). Nonetheless, research into QKD and its applications continues, and it is likely to play an increasingly important role in the future of secure communication (Pirandola et al., 2020; Mehic et al., 2020; Scarani et al., 2009).

Thus, the primary objective of QKD is to construct a device that ensures the security of generated keys, adhering to the previously outlined (weakened) requirements, thereby preventing Alice and Bob from employing compromised keys (Gisin et al., 2002). Quantum mechanics plays a crucial role in achieving this goal. In quantum theory, various phenomena exist that can be leveraged to address these challenges. Firstly, quantum states and measurements inherently possess randomness that can be exploited (Scarani & Kurtisefer, 2014; Wolf, 2021). Additionally, quantum theory presents a highly practical concept for cryptography known as the no-cloning theorem (Bennett & Brassard, 1984). Unlike classical physics, where states can be perfectly replicated an unlimited number of times (at least in principle), quantum states are forbidden from being cloned due to the linearity of quantum theory (Wolf, 2021). Understanding how well the principles of quantum mechanics align with requirements is essential in creating a key suitable for applications like one-time pad encryption (Wolf, 2021).

2.3.1 Fundamental Principles of QKD

The fundamental principles of QKD are crucial to understand how this technology works and why it is secure. The main principles of QKD include:

- 1) **Uncertainty principle:** The uncertainty principle is a fundamental principle of quantum mechanics, which states that certain pairs of physical properties, such as the position and momentum of a particle, cannot both be precisely determined at the same time (Heisenberg, 1985). This principle is important in QKD because any attempt to measure the quantum state of a photon in transit will disturb it, altering its state and alerting the communicating parties to the presence of an eavesdropper (Rieffel & Polak, 2011). Therefore, the uncertainty principle provides a fundamental mechanism for ensuring the security of QKD.

- 2) Quantum superposition: Quantum superposition is a principle of quantum mechanics that allows a quantum particle to exist in multiple states at the same time (Dirac, 1926). In the context of QKD, this means that a photon can exist in multiple polarization states at the same time. The sender and receiver can measure the polarization of the photon in one of two possible bases, such as the horizontal-vertical basis or the diagonal basis, to generate a shared secret key. The choice of basis is kept secret between the parties until after the transmission is complete, which ensures that an eavesdropper cannot determine the correct basis and intercept the key.
- 3) Quantum entanglement: Quantum entanglement is a phenomenon in which two particles become correlated in such a way that the state of one particle is dependent on the state of the other particle, regardless of the distance between them (Einstein et al., 1935). In the context of QKD, two entangled photons can be used to generate a shared secret key that is secure against eavesdropping. The sender and receiver each measure the polarization of one photon from the entangled pair, which allows them to generate a shared key that is secure because any attempt by an eavesdropper to intercept the key will change the state of the entangled photons, which will be detected by the communicating parties.
- 4) No-cloning theorem: The no-cloning theorem of quantum mechanics states that it is impossible to create an exact copy of an unknown quantum state (Wooters & Zurek, 1982). This principle is important in QKD because it means that an eavesdropper cannot intercept and copy the quantum state of a photon without disturbing it, which would alert the communicating parties to the presence of an eavesdropper. Therefore, the no-cloning theorem provides a fundamental mechanism for ensuring the security of QKD.

- 5) Quantum measurement: The act of measuring a quantum state changes its state. In the context of QKD, this means that any attempt to measure the quantum state of a photon in transit will disturb it, altering its state and alerting the communicating parties to the presence of an eavesdropper (Bennett & Brassard, 1984). Therefore, the quantum measurement principle provides a fundamental mechanism for ensuring the security of QKD.

2.3.2 Mechanism of Point-To-Point QKD

The fundamental principle of point-to-point of QKD network was introduced in the initial QKD protocol known as the BB84 protocol, proposed by Bennett and Brassard in 1984 (Bennett & Brassard, 1984) which is illustrates in Fig. 2-1. This protocol enables Alice and Bob to generate, transmit, and synchronize keys (Zhao et al., 2018). In this context, a "QKD link" refers to the logical connection between two remote QKD nodes, where a quantum channel is utilized for transmitting photons and a public channel is employed for post-processing the transferred information (Mehic et al., 2020). The following provides a description of the secret key generation process when utilizing the BB84 protocol (Sharma et al., 2021).

Phase 1: Quantum State

In this phase, Alice generates a series of qubits and independently selects, at random, either a rectilinear basis (+) with two polarization options (90° , 0°) or a diagonal basis (\times) with two polarization options (135° , 45°) for each qubit (Sharma et al., 2021). The resulting string of qubits is then transmitted to Bob through a quantum channel. Conversely, Bob randomly chooses a measurement basis for each received qubit. When the measurement bases chosen by Alice and Bob align, a perfectly correlated outcome is obtained, allowing Bob to record a string of all received qubits

known as the raw key. On the other hand, if the measurement bases differ, an uncorrelated result is observed.

Phase 2: Post-processing and Key Derivation

During this phase, Alice and Bob engage in communication through a public channel to derive secret keys from the measurement outcomes. The post-processing technique involves the following steps:

- 1) **Sifting:** Alice and Bob utilize a classical channel to exchange information regarding the transmitted and received photons. Qubits that correspond to the same measurement bases chosen by both Alice and Bob are retained, while those associated with different measurement bases are discarded. As a consequence, the length of the key after sifting is reduced in half compared to the length of the raw key. The sifted key is generated by decoding the remaining qubits into a string of classical bits (Zhao et al., 2018).
- 2) **Error Estimation and Correction:** This step aims to mitigate any potential errors that may have occurred during the sifting process. Alice and Bob employ a public channel to communicate and compare the results of exchanging a random subset of classical bits from their sifted keys (Zhao et al., 2018).
- 3) **Privacy Amplification and Authentication:** In this step, the information content of the secret key is minimized against a minimal number of unauthenticated users. This is achieved by generating a new shorter key using universal hash functions. Furthermore, the implementation of an authentication procedure serves to protect the secret key from potential eavesdropping endeavors. (Sharma et al., 2021).

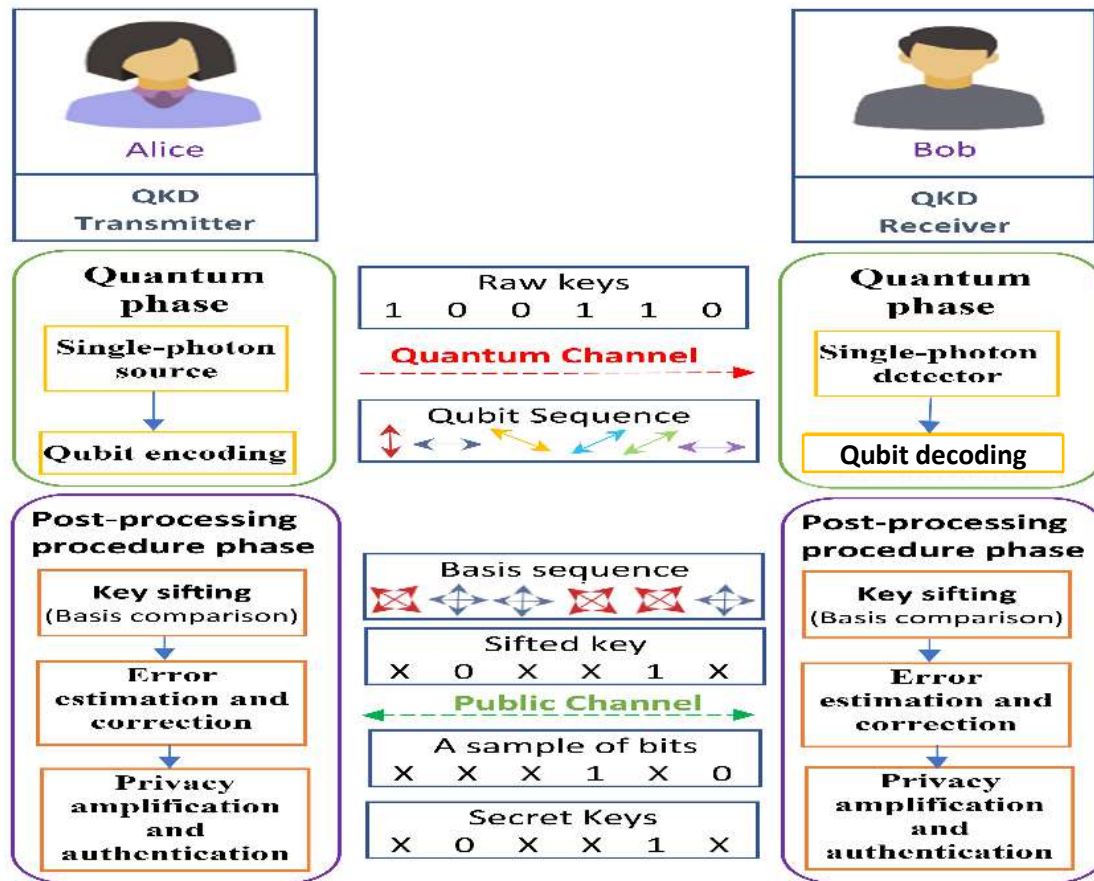


Fig. 2-1 Point-to-point QKD mechanism based on BB84 protocol

On other hand, the SARG04 protocol, which was first introduced by Scarani in 2004 (Scarani et al., 2004), bears resemblances to the initial stages of the BB84 protocol's point-to-point QKD mechanism (Nurhadi & Syambas, 2018). However, the main distinction between the two protocols lies in the traditional post-processing procedure, which enhances the security of the SARG04 protocol. In the second phase, Alice does not explicitly disclose her bases as in the BB84 protocol, where Alice and Bob match their bases for bit comparison. Instead, Alice announces a pair of non-orthogonal states, one of which she employs to encode the bits, and Bob follows the same approach. Selecting the correct basis allows Bob to measure the correct state. However, selecting the incorrect basis prevents Bob from measuring any of Alice's states, thus hindering his ability to identify the bit. In the absence of

errors, the remaining key length after the sifting step is one-fourth of the initial raw key (Singh et al., 2014).

2.3.4 Compare Between BB84 and SARG04 Protocols

In terms of security, both protocols (BB84 and SARG04) are proven secure against eavesdropping attacks, as long as certain conditions are met, such as the absence of side channels and the use of authenticated classical channels for error correction and privacy amplification (Bennett & Brassard, 1984; Scarani et al., 2009). However, the security of these protocols also depends on the quality of the quantum channel, the efficiency of the detectors, and the level of sophistication of the eavesdropping attacks (Bennett & Brassard, 1984; Weedbrook et al., 2012). In terms of practicality, the SARG04 protocol may be more advantageous in some cases, such as in fiber-optic QKD networks with long distances and high attenuation (Ali et al., 2012). This is because the SARG04 protocol uses a smaller number of photon states and measurement bases, which can reduce the impact of noise and loss in the quantum channel (Ali et al., 2012). Moreover, the SARG04 protocol can also be implemented with simpler experimental setups and detectors, which can reduce the cost and complexity of the system (Ali et al., 2012). On the other hand, the BB84 protocol may be more advantageous in other cases, such as in free-space QKD networks or in scenarios where higher key rates are required (Bennett & Brassard, 1984; Scarani et al., 2009). This is because the BB84 protocol uses a larger number of photon states and measurement bases, which can increase the information capacity and the resistance to certain types of attacks, such as photon number splitting attacks (PNS) (Dynes et al., 2007). Moreover, the BB84 protocol can also benefit from various extensions and modifications, such as the use of entanglement, decoy states, or error-rejection codes, which can further improve its performance and security (Peev et al., 2009).

2.4 Long-Distance Transmission of QKD Network

The range of QKD networks is limited because quantum signals, like photons, can deteriorate during transmission. This attenuation is mainly caused by interactions with the medium, particularly optical fibers. In optical fibers, quantum signals can scatter, deviating from their path, and get absorbed, reducing their transmission distance (Scarani et al., 2009; Wang et al., 2017). Throughput is another limitation of QKD networks which is based on distance problem. While QKD can generate secure keys at a high rate, the key generation rate is limited by the rate at which quantum signals can be transmitted through the transmission medium (Diamanti et al., 2016). Furthermore, the key exchange process involves multiple rounds of communication, which adds to the overall latency and reduces the throughput of the QKD network (Lo et al., 2014).

To address these limitations, researchers are exploring various approaches, including new transmission media, improved detector technology, and novel error correction techniques (Li et al., 2022). Satellite-based QKD networks are being developed to enable secure key exchange over long distances while bypassing the restrictions of optical fiber transmission (Krenn et al., 2016; Liao et al., 2017). Furthermore, advancements in detector technologies, like superconducting nanowire single-photon detectors, aim to enhance the detection efficiency of quantum signals (Takemoto et al., 2015).

Almost all of the research that tried to solve the distance problem in QKD networks has failed. Nevertheless, quantum repeaters and CTR approaches have, up to currently, shown their value in overcoming the challenge posed by the distance between QKD networks.

2.4.1 Quantum Repeater

A quantum repeater is a device or system that is used to extend the range of quantum communication over long distances (Briegel et al., 1998). Quantum communication, such as QKD, uses quantum states to transmit information securely (Sangouard et al., 2011). However, the transmission of these quantum states can be subject to loss and decoherence, which can limit the distance over which quantum communication can be achieved (Lucamarini et al., 2018; Ladd et al., 2010).

Quantum repeaters are designed to overcome this limitation by creating a chain of entangled pairs of qubits between the sender and receiver (Sangouard et al., 2011). This chain of entangled pairs allows for the creation of a secure quantum key despite the transmission loss. The key idea behind quantum repeaters is to divide the long-distance quantum communication link into smaller segments, each of which can be amplified and corrected independently (Childress et al., 2005; Azuma et al., 2015).

The basic operation of a quantum repeater involves entanglement swapping and purification (Azuma et al., 2015). Entanglement swapping allows for the transfer of entanglement between two pairs of qubits that are not directly connected. Purification is a process that removes errors and noise from the entangled pairs of qubits (Briegel et al., 1998).

In practice, quantum repeaters are typically implemented using a combination of optical and atomic systems (Wang et al., 2023). In an optical implementation, the entangled pairs of qubits are created using photons, while in an atomic implementation, the qubits are stored in the internal states of atoms (Ma et al., 2020). Both approaches have their advantages and disadvantages, and ongoing research is focused on developing new and improved quantum repeater systems.

While quantum repeaters have been demonstrated in proof-of-principle experiments (Sangouard et al., 2011; Ladd et al., 2010; Duan et al., 2001), their development is ongoing, and practical implementation is still a topic of active research and it is anticipated that the first practical quantum repeaters will be costly (Neuwirth et al., 2021). The performance of quantum repeaters is limited by the performance of the repeater nodes themselves, as well as the error rate of the generated keys, which increases as the distance between the nodes increases (Ma et al., 2020). Nevertheless, quantum repeaters are an important tool for extending the range of quantum communication over long distances, and ongoing research is focused on improving their performance and reliability (Neuwirth et al., 2021).

2.4.2 Classical Trusted Relay Technology

In a QKD network, the CTR technology acts as an intermediary between the two endpoints, Alice and Bob (Sharma et al., 2021). The relay is located between Alice and Bob and is responsible for performing error correction and privacy amplification on the quantum signals exchanged between them (Cao et al., 2021). This allows the secure key to be established over longer distances than would be possible with point-to-point QKD (Zou et al., 2020).

The CTR technology divides the long-distance quantum communication link into shorter segments, each of which can be secured using QKD (Xu et al., 2021). The endpoints exchange quantum states over each segment, and the CTR technology performs error correction and privacy amplification on these states before forwarding them to the next segment. This process is repeated until the endpoints have established a secure key (Zhang et al., 2022).

One advantage of CTR technology over quantum repeaters is that they do not require the creation of entangled pairs of qubits, which can be a challenging technical

task (Azuma et al., 2022). Instead, trusted relays rely on classical communication channels and standard cryptographic protocols to perform error correction and privacy amplification.

Fig. 2-2 illustrates an instance of QKD distance extension employing a CTR technology between the source and destination nodes (Zhao et al., 2018). In this scenario, the QKD transmitter in the source node establishes a QKD link with the subsequent QKD receiver in the intermediate node (CTR node). Similarly, the QKD receiver in the destination node establishes a QKD link with the preceding QKD transmitter in the intermediate node (CTR node). Each of these QKD links independently generates secret keys, denoted as AR1 and BR1, which have the same key size. The secret key AR1 is then encrypted using the secret key BR1 and forwarded to the destination node. This process enables the utilization of the secret key AR1 to secure communications between the source and destination nodes. It is worth noting that this relay process can be extended with any number of intermediate nodes, but each intermediate node equipped with the CTR technology will possess knowledge of the secret key information.

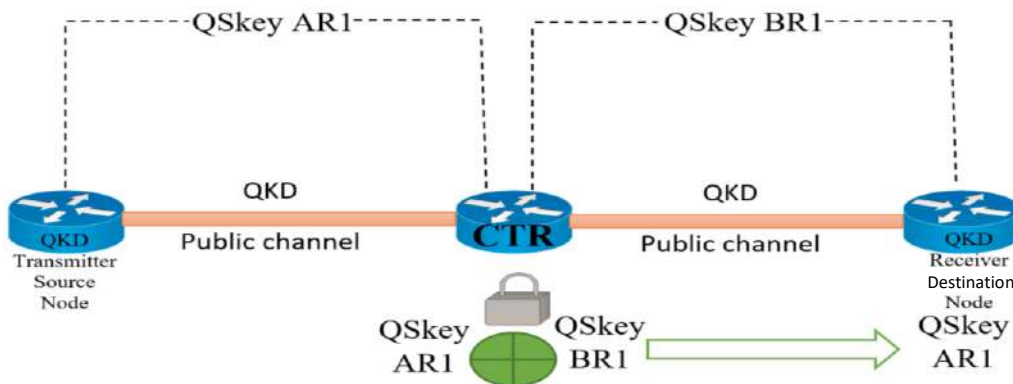


Fig. 2-2 An example of QKD distance extension based on a CTR technology between the source and destination nodes.

The mechanism of CTR technology is based on protocols that serve as the foundation for transmitting quantum secret keys over CTRs. The BBN (Bolt, Beranek, and Newman) key relay protocol has been successfully implemented in quantum networks since 2003 (Elliott, 2004; Elliott & Yeh, 2007). However, the BBN protocol has two significant limitations: it is time-consuming to establish the key material, and it necessitates complete trust among all communicating nodes (Dong et al., 2019). To address these issues, Schartner and Rass proposed a strategy for re-encrypting key distribution in QKD-based key relays (Schartner & Rass, 2009). Nevertheless, in the re-encryption method, the relay nodes are still required to keep the XOR values of the QKD keys secret, and subsequent communication between adjacent relay nodes is still necessary (Dong et al., 2019). This is because the XOR value is utilized for QKD key decryption. In contrast, the public XOR-key method, introduced in 2013 for quantum-secure communication, involves CTR nodes making their XOR keys public (Dong et al., 2019). This enables the endpoints to share a key. When compared to the re-encryption strategy, this approach simplifies the system's complexity and enhances the traffic flow of the relay nodes. However, it is important to note that all three types of CTR protocols described here are employed for distributing the quantum secret key via a public channel. Fig. 2-3 provides an overview of the primary processes of the BBN protocol, as well as the re-encryption and public XOR key protocols (Dong et al., 2019).

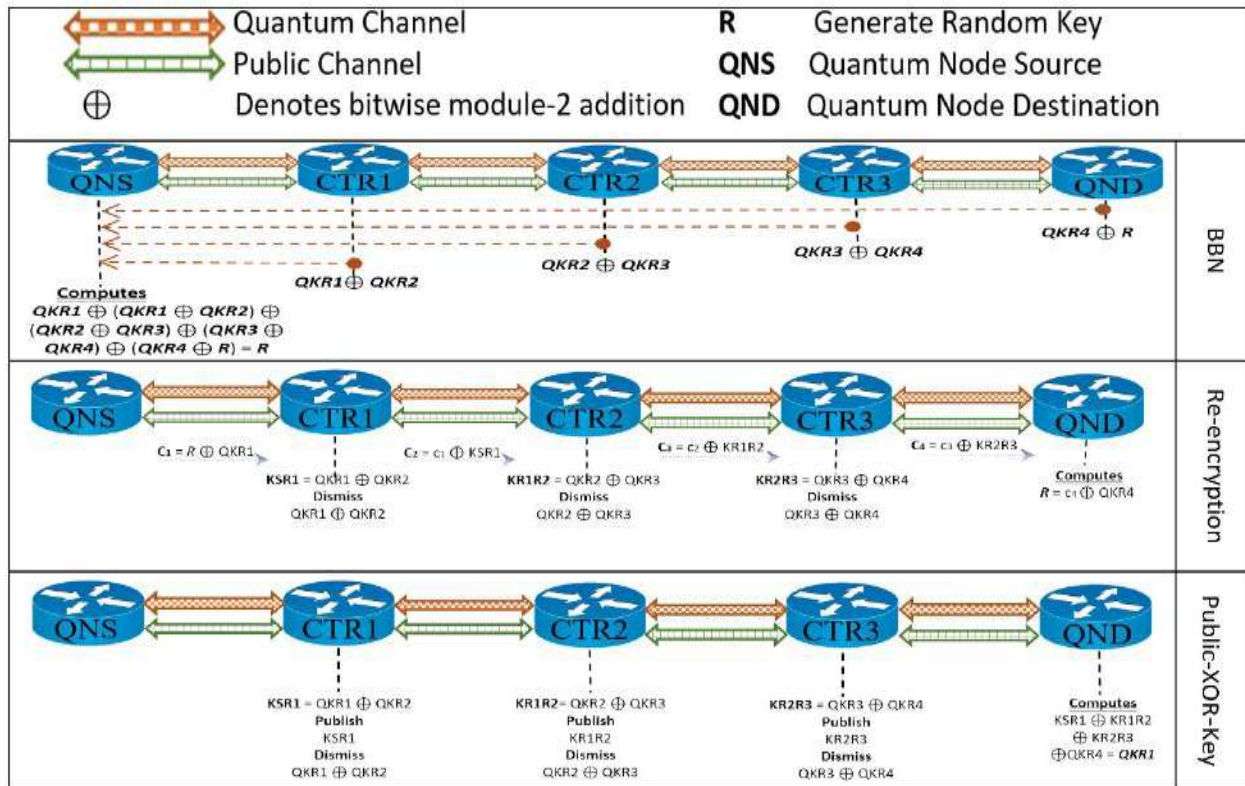


Fig. 2-3 Examples of the models of BBN, Re-encryption and Public –XOR-Key schemes with two endpoints and three CTR nodes

However, there are significant drawbacks associated with CTR technology in QKD networks, as highlighted in the study by Sharma et al. (2021).

1. **Additional Security Risks:** The use of CTR technology introduces additional security risks into the QKD network, as the security of the network depends on the trustworthiness of the relay nodes. If a trusted relay is compromised, an attacker could potentially gain access to the exchanged keys.
2. **Reduced Efficiency:** The use of CTR technology can reduce the efficiency of the QKD network, as each relay introduces additional noise and loss into the communication channel. This can reduce the quality of the quantum states exchanged between the endpoints and reduce the overall key generation rate.

3. **Limited Scalability:** The use of CTR technology may be limited in terms of scalability, as the number of relays that can be used to extend the network is limited by the resources available to manage and secure them. This may limit the range of the QKD network and reduce its overall performance.
4. **Additional Complexity:** The use of CTR technology adds additional complexity to the QKD network, as it requires the development and deployment of specialized hardware and software protocols to manage and secure the relay nodes. This can increase the cost and technical complexity of the network.

2.5 Software-Defined Networking

In recent years, there has been a shift in how data centers handle storage (Alam et al., 2023; Aghasi et al., 2023; Ahmed et al., 2015), computing (Alharthi et al., 2022; Allspaw, 2008; Andročec, 2015), and network resources (Askar, 2016; Awais et al., 2023; Azariah et al., 2022; Barroso et al., 2013). Originally, these elements were deliberately kept separate (Batayneh et al., 2011; Bezos & Isaacson, 2020; Bráin, 2015; Buyya et al., 2009; Cao et al., 2023), but with advancements in technology (Carthern et al., 2015; Del Piccolo et al., 2016; Edelman et al., 2018; Erl et al., 2013), organizations have been compelled to integrate them. This shift brought applications managing these resources closer together than ever before (Feng et al., 2022; Goswami et al., 2023; Gupta et al., 2021). As data centers evolved, network equipment saw fewer innovations, primarily focusing on performance enhancements (Kizza, 2023). Network virtualization, known as Virtual Private Networks (VPNs), played a significant role (Kreutz et al., 2014; Kurose & Ross, 2007). Commercial routers and switches come with various management interfaces for configuring and managing these devices (Li & Cao, 2023). However, difficulties arise when trying to program using unsupported functionality (Li & Cao, 2023).

Additionally, the concept of a distributed control plane re-emerged, involving a central brain directing commands to network devices(Liang et al., 2022). This paradigm shift allows for more affordable and general-purpose computing options for the control plane(Marshall, 2007).

All of these aforementioned concepts have played a crucial role in the development of SDN (Ali et al., 2023; Nadeau & Gray, 2013; Shamugam et al., 2016; Kreutz et al., 2014). Early proponents of SDN recognized that network device vendors were not adequately addressing their needs, particularly in terms of feature development and innovation (Askar and Keti, 2021;Togou et al., 2019). They also believed that high-end routing and switching equipment was excessively priced, especially considering the control plane components (Tyagi & Singh, 2023; Keti and Askar, 2015). Simultaneously, they observed a rapid decrease in the cost of raw computing power, making it feasible to have access to thousands of processors (Keti and Askar, 2015). This realization led them to consider harnessing this processing power to run a logically centralized control plane and to utilize inexpensive, commodity-priced switching hardware (Tyagi & Singh, 2023; Nadeau & Gray, 2013; Kreutz et al., 2014; Bráin, 2015). To put this idea into practice, a group of engineers from Stanford University developed a protocol called OpenFlow. OpenFlow was designed to be implemented in a configuration where devices solely contained data planes and responded to commands from a (logically) centralized controller that housed the network's single control plane (Wang, 2023). The controller was responsible for managing network paths and programming each controlled network device (Wang, 2023). The OpenFlow protocol defined the commands and responses involved in this process (Kreutz et al., 2014; Bráin, 2015; Togou et al., 2019; Kreutz et al., 2014). It is worth noting that the Open Networking Foundation (ONF) played a crucial role in supporting the commercial aspects of the

SDN effort and remains the central authority for standardization and marketing in the field (Turner et al., 2023). With the basic architecture described, one can envision how quickly and easily new networking protocols could be devised by implementing them in a data center using cost-effective hardware. Furthermore, these protocols could be implemented within an elastic computing environment, such as a virtual machine (Nadeau & Gray, 2013).

2.5.1 QKD Enabled By SDN Architecture

A more advanced approach to incorporating QKD into transport networks involves leveraging recent advancements in networking technology, particularly in network management (Tessinari et al., 2023; Wang et al., 2019). In terms of QKD network management, SDN can greatly enhance the effectiveness of managing QKD networks (Sim et al., 2023; Mehic et al., 2020; Wang et al., 2019). SDN offers efficient and straightforward management capabilities for QKD networks due to its programmable and adaptable centralized control mechanism (Tessinari et al., 2023; Cao et al., 2020). The SDN-enabled QKD network architecture, depicted in Fig 2-4 (Zhao et al., 2018), comprises three layers: the application layer, control/management layer, and infrastructure layer (Cao et al., 2019)

- 1- Application layer: Situated at the upper of the SDN-enabled QKD network, this layer promptly responds to user requirements and facilitates user access to network resources. Its functionalities include topological representation and quality of service catering to consumer requirements. The controller, through northbound interfaces, abstracts network resources, such as creating light paths for QKD and generating secret key routes in the infrastructure layer. Both processes are carried out within the context of QKD (Wang et al., 2019).

- 2- Control/management layer: This layer offers operators a comprehensive view of the QKD networks. It may consist of one or more controllers responsible for managing the network in the infrastructure layer and enabling compatibility with various applications. The application layer generates requests based on operator demands, which are then transmitted to the controller through the northbound interface. The controller utilizes a global network map and southbound interface protocol to calculate and allocate QKD resources. The control layer manages QKD resources within the infrastructure layer and delivers services to various requests in the application layer. It also obtains information regarding the allocation of resources and policies from the infrastructure layer (Wang et al., 2019).

- 3- Infrastructure layer: Positioned at the bottom of the architecture, this layer focuses on the performance of QKD devices (Wang et al., 2019). Within the infrastructure layer, QKD nodes (QKDNs) are interconnected through QKD links. For long-distance end-to-end QKD, multiple CTR technology nodes are placed between two distant QKDNs (Cao et al., 2019). Communication and message exchange occur between the SDN controller and QKDN/CTR via a southbound interface. Each QKDN/CTR operates according to instructions received from the SDN controller through the southbound interface. Secret keys are continuously generated between any two directly linked QKDNs or CTRs, as well as between a QKDN and CTR.

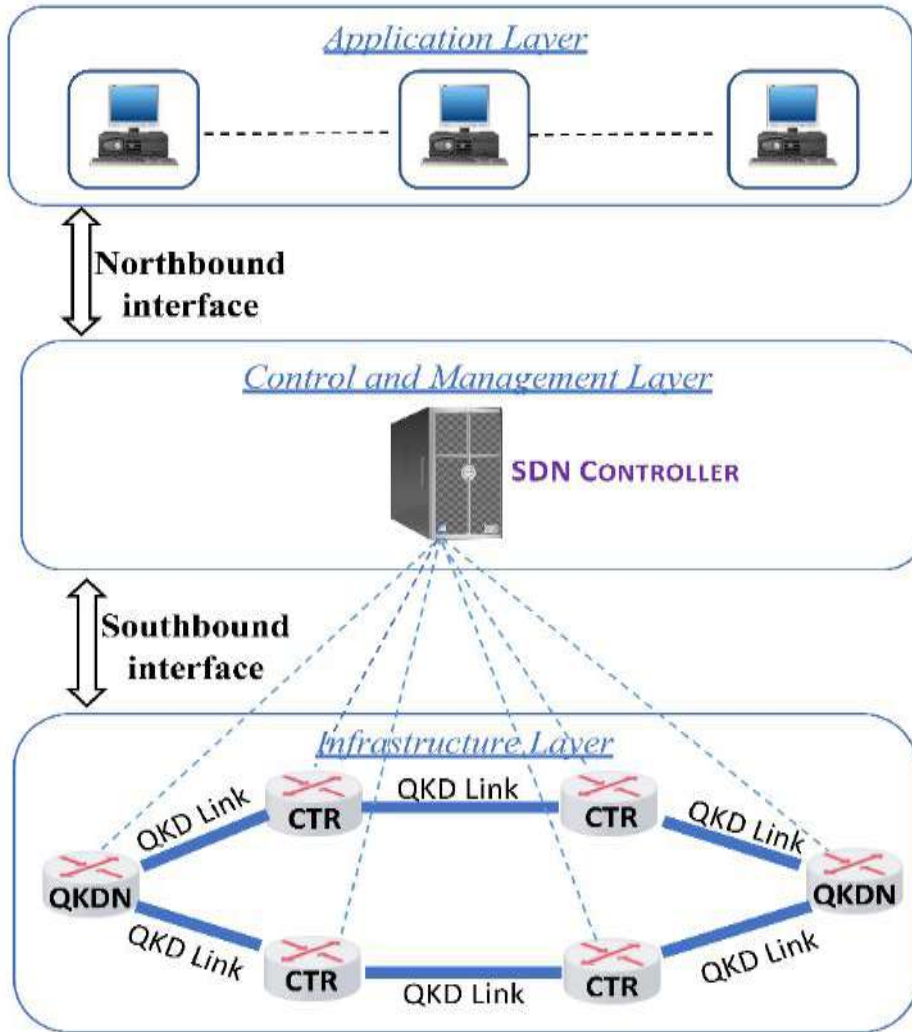


Fig. 2-4 QKD over SDN architecture

CHAPTER THREE: LITERATURE REVIEWS

3.1 Introduction

This chapter provides a synopsis of the prior work that has been done in connection with this dissertation. Most of the talk is about the best way to handle the solutions that QKD-protected optical networks offer to make sure that communication is secure over long distances. Furthermore, a discussion on how the researchers attempted to enhance the safety of the CTR technology that is based on the QKD network will also be included in the discussion. In addition, this chapter will go over the research that has been done on using SDN over QKD and how it may play a significant role in order to manage the secret keys that are based on CTR technology. In addition, earlier works that were critical of using ML on QKD networks will be presented.

3.2 Advances in Relay-Based QKD

There are three relay-based solutions available in QKD-protected optical networks for secure long-distance communication. The first solution involves using QKD-based quantum repeaters, which create an entangled state between two nodes located in different locations to establish secure communication over long distances using the principle of quantum entanglement (Elkouss et al., 2013; Sharma et al., 2021). The second solution is the Measurement-Device Independent Quantum Key Distribution (MDI-QKD) protocol (Lo et al., 2012; Tang et al., 2016; Yin et al., 2016; Liu et al., 2019). This protocol is based on two-photon interference and is immune to attacks on the detection system. It enables QKD networks with untrusted relays and is suitable for fiber-based implementations aimed at achieving longer distances, higher key rates, and network verification (Cao et al., 2020). The third solution is QKD-based on CTR technology, where secret keys generated on the first QKD link are further encrypted with secret keys in intermediate nodes before being

relayed to the final destination node (Zhao et al., 2018; Sharma et al., 2021). While the MDI protocol has a limited safe distance of approximately 500 km (Fang et al., 2020; Chen et al., 2020), and quantum repeaters are still in the development phase (Elkouss et al., 2013), most QKD networks currently rely on CTR technology to enable communication over longer distances (Zhao et al., 2018). However, it is crucial to ensure the credibility of nodes employing CTR technology, as they have knowledge of the secret keys between the source and destination nodes (Cao et al., 2018).

3.2.1 Previous works for CTR technology

Researchers are actively addressing security challenges in QKD based on CTR technology. Several studies propose innovative methods to enhance security and efficiency in partially trusted relay QKD networks. For instance, Wang et al. (2023) introduce a segment-based multipath key distribution approach to maximize security in the presence of both trusted and untrusted relays. They also present a flexible key reconstruction scheme for improved efficiency. Simulation results demonstrate superiority over traditional multipath QKD methods. Chen et al. (2023) propose a Hybrid-Trusted QKDN (HT-QKDN) that incorporates low-cost semi-trusted quantum nodes. They employ multi-path transmission and optimized path selection algorithms, demonstrating the feasibility and superior performance of the HT-QKDN. Luo et al. (2023) focus on passive and active attacks in QKD networks. They propose a model based on QKD networks with a Byzantine consensus scheme, offering the highest level of security among relay-based QKD networks. Salvail et al. (2010) evaluate the security of CTR technology, identifying vulnerabilities and suggesting remedies to mitigate potential attacks. They also assess the security, performance, and efficiency of various QKD systems, providing valuable recommendations for robust and trustworthy QKD networks. Zhang and Ni (2018)

introduce a quantum network system design incorporating CTR technology to enhance security, efficiency, and reliability. Their design integrates advanced algorithms for key distribution, error correction, and authentication, with mechanisms to detect and thwart eavesdropping. Mehic et al. (2019) propose advanced algorithms for dynamic resource allocation and optimization in CTR-based QKD networks. Their approach considers security measures and demonstrates improved Quality-of-Service (QoS). Cao et al. (2021) discuss a cost-optimized CTR-based QKD network architecture over optical backbone networks. They propose a hybrid trusted/untrusted node structure and employ an Integer Linear Programming (ILP) model for cost optimization, achieving efficiency in diverse network topologies. Cao et al. (2020) propose strategies to enhance the security of QKD chain deployment over optical networks using trusted and untrusted relays. Performance evaluation shows a significantly higher security level compared to benchmark strategies. Zou et al. (2020) introduce the collaborative routing algorithm, considering trusted and untrusted relays in a network. The algorithm utilizes different protocols based on the presence of untrusted relays, demonstrating efficacy in various QKD network topologies. Zhang et al. (2022) present a scheme for protecting QKD networks with partially trusted relays. They utilize a topology abstraction method and introduce a key protection threshold for enhanced security and dependability. Lin et al. (2020) propose a QKD method for ring networks with trusted and untrusted CTR technology. They introduce a Partially Trusted Routing Algorithm (PT-RA) to address security issues and improve key distribution success rate in partially trusted QKD networks. Xu et al. (2023) present Quantum Key Recycling (QKR) to address key resource utilization in optical networks, enhancing key efficiency and encryption capability. Li et al. (2020) propose QKR mechanisms to increase the number of accessible keys in QKD systems for secure communication. Sharma et al. (2021) emphasize the need for further research in

QKR and reuse strategies. Kiktenko et al. (2020) introduce a lightweight authentication protocol for QKD based on CTR technology, minimizing the consumption of quantum-generated secret keys for authentication. Dong et al. (2020) present schemes for securing multicast communication in quantum data center networks using CTR technology, employing sub-key-relay-tree structures and distributed sub-key management. Garcia-Cobo and Menéndez (2021) propose a methodology utilizing medoid-based clustering techniques to optimize the distribution of CTR technique for covering large regions. Wang et al. (2019) combine quantum and classical communication in an optical network, with a secret-key recovery strategy for compromised quantum channels. Dong et al. (2020) introduce an auxiliary graph-based approach to improve the performance of QKD networks using CTR technology, reducing network-blocking probability and enhancing resource utilization. Zhao et al. (2018) present a method to optimize resource allocation in optical networks using QKD based on CTR technology, considering the specific security features of QKD. Cao et al. (2019) propose a cost-efficient QKD scheme leveraging existing infrastructure in WDM networks for key distribution.

Table 3-1 Comparative Analysis of QKD Networks Based on CTR Technology

Solution Type	Key Features	Safe Distance	Security Level	Efficiency	Limitations/Gaps	References
Segment-based Multipath Key Distribution	Maximize security in presence of trusted and untrusted relays, Flexible key reconstruction scheme	150 km	High	96%	Requires specialized hardware for key reconstruction	Wang et al. (2023)
Hybrid-trusted QKDN (HT-QKDN)	Incorporates low-cost semi-trusted quantum nodes, HT-QKDN routing scheme with multi-path transmission	80 km	Medium	93%	Limited to specific network topologies	Chen et al. (2023)

Model for End-to-End Key Distribution	Byzantine consensus scheme, Focuses on passive and active attacks	200 km	Very High	98%	Requires additional computational resources	Luo et al. (2023)
Evaluation and Remedies for CTR Technology	Identifies vulnerabilities, Provides remedies, Evaluates QKD systems	120 km	High	95%	N/A	Salvail et al. (2010)
Quantum Network System Design	Integrates cutting-edge algorithms, Error correction, Authentication, Eavesdropping detection	150 km	Very High	97%	Sensitive to changes in node distance, Limited scalability for very large networks	Zhang and Ni (2018)
Dynamic Resource Allocation and Optimization	Advanced algorithms for resource allocation, Considers security measures	100 km	Medium	92%	Requires significant computational resources, Limited applicability for dynamic networks	Mehic et al. (2019)
Cost-Optimized QKD Network Architecture	Hybrid trusted/untrusted node structure, Integer linear programming (ILP) model for cost optimization	80 km	Medium	90%	Limited scalability for very large networks	Cao et al. (2021)
Enhanced Security Strategies	Combination of trusted and untrusted relays	90 km	Very High	96%	Limited scalability for very large networks	Cao et al. (2020)
Collaborative Routing Algorithm	Considers trusted and untrusted relays, MDI-QKD protocol integration	70 km	High	94%	Not suitable for highly dynamic networks	Zou et al. (2020)
Scheme for Protecting QKD Networks	Utilizes topology abstraction method, Key protection threshold introduction	110 km	Very High	95%	Resource allocation trade-offs between working and protection paths	Zhang et al. (2022)
Partially-Trusted Based Routing Algorithm (PT-RA)	Addresses security issues, Improves key distribution success rate	90 km	Very High	95%	Limited applicability for certain network topologies	Lin et al. (2020)
Quantum Key Recycling (QKR)	Addresses key resource utilization, Enhances key efficiency	120 km	Medium	88%	Limited scalability for very large networks	Xu et al. (2023)
Quantum Key Recycling Mechanisms	Augments accessible keys, Reduces wastage	100 km	Medium	89%	Limited scalability for very large networks	Li et al. (2020)
Lightweight Authentication Protocol	Utilizes "ping-pong" scheme for authenticity verification	60 km	High	93%	Requires additional processing overhead	Kiktenko et al. (2020)

Secure Multicast Communication Scheme	Utilizes sub-key-relay-tree structure, Distributed sub-key management	140 km	Very High	97%	Scalability challenges for very large networks	Dong et al. (2020)
Medoid-Based Clustering for Optimal Distribution	Addresses communication system limitations, Utilizes CTR technology	180 km	Medium	90%	Requires accurate knowledge of network characteristics	Garcia-Cobo and Menéndez (2021)
Combined Quantum and Classical Communication	Utilizes single-photon source for quantum states, Secret-key recovery strategy	110 km	Very High	96%	Sensitive to quantum channel quality	Wang et al. (2019)
Auxiliary Graph-Based Approach	Improves performance of QKD networks using CTR technology	85 km	High	94%	Limited applicability for non-uniform network topologies	Dong et al. (2020)
Resource Allocation Optimization Method	Utilizes QKD based on CTR technology, Considers specific security features	80 km	High	95%	Sensitivity to network changes, Limited applicability for dynamic networks	Zhao et al. (2018)
Cost-Efficient QKD Scheme	Utilizes existing infrastructure of WDM networks, Shared resources for key distribution	150 km	Medium	90%	Limited scalability for very large networks	Cao et al. (2019)

3.3 Integrating SDN with QKD Networks

Quantum keys are important in QKD-secured optical networks because their secret key rate is low (Zhao et al., 2018). Therefore, to improve the management of secret keys in QKD-based CTR technology, SDN has the potential for management in QKD networks (Cao et al., 2020). SDN holds a programmable and flexible centralized control manner to provide efficient and easy management for QKD networks, which could have significant implications for the development of future quantum communication systems.

3.3.1 Previous Studies of SDN Over QKD

In the studies reviewed, various approaches to integrate SDN with QKD networks were explored. Bassi et al. (2023) implemented a prototype architecture, using trusted relay nodes to facilitate key exchange between non-adjacent nodes,

showcasing advantages in inter-datacenter communication. Monita et al. (2023) introduced a QKD network utilizing SDN, employing metrics for path selection, with OSPF routing outperforming RIP. Nie et al. (2020) proposed a security scheme using quantum encryption to enhance communication between the control and forwarding layers in SDN, effectively preventing multiple types of attacks. Liu et al. (2019) presented a multi-path based real-time QKD scheme, employing SDN controllers for efficient key distribution. Aguado et al. (2017) proposed an orchestration framework for NFV over SDN-controlled optical networks, efficiently managing QKD resources for different service providers. Cao et al. (2017) introduced a Key on Demand (KoD) strategy with Quantum Key Pool (QKP) construction technique for SDON secured by QKD-based CTR technology, considering security and key resource usage. Mendez et al. (2020) introduced Quantum Abstraction Interface (QAI) for seamless integration of QKD devices with SDN controllers, improving network security, flexibility, and scalability. Hugues-Salas et al. (2019) conducted experiments to test the security of a QKD network against physical layer attacks, using an SDN controller to monitor and mitigate such attacks effectively. Hugues-Salas et al. (2018) addressed DDoS vulnerabilities in QKD networks using an SDN application, minimizing disruption compared to traditional QKD methods. Cao et al. (2018) proposed a scheme combining time-scheduling and QKP technique for QKD over classical networks, effectively managing QKPs. Brito et al. (2019) introduced Quantum Services Architecture (QSA) integrated with SDN, providing APIs for quantum service development and standardizing integration of quantum technologies. Zhao et al. (2017) proposed QKD-enabled SDN architecture for secure communication between controllers and switches, successfully integrating QKD into SDN-based optical networks. Cao et al. (2019) investigated SDN in a QKD network with CTR technology, developing an SDN-enabled architecture for multi-tenant provisioning. Aguado et al. (2020)

integrated QKD with SDN using a QKD-aware routing algorithm, achieving secure key distribution while utilizing existing infrastructure. Lopez et al. (2019) proposed integration of QKD with next-generation network infrastructures, offering several use cases to improve network security. Wang et al. (2020) proposed a routing and key resource allocation scheme for SDN-based quantum satellite networks, emphasizing the importance of QKD in ensuring secure communications. Aguado et al. (2018) presented a framework for deploying and managing QKD-enabled VNFs in optical networks, achieving high key generation rates while minimizing QKD resource usage. Wang et al. (2018) introduced a flexible key-updating method for secure SDONs using QKD, combining QKD with classical techniques for real-time key updating. Cao et al. (2019) addressed challenges in deploying secret keys over QKD-integrated optical networks using a Key as a Service (KaaS) framework. Martín et al. (2020) proposed a component-based approach for flexible and scalable QKD networks, utilizing SDN for efficient and secure communication. Tessinari et al. (2019) conducted a field trial integrating dynamic distributed-variable QKD networking with SDN, achieving high key rates, low error rates, and improved network security. Martín et al. (2019) successfully deployed an SDN-based QKD network in real-world production facilities, demonstrating the feasibility of integrating quantum-classical communications infrastructure. Tang et al. (2020) introduced a novel architecture, PQNMs, combining QKD and SDN for scalable, programmable, and highly resilient networked microgrids, mitigating the impact of DoS attacks. Cao et al. (2019) conducted an experimental demonstration of a QKD network based on CTR technology combined with SDN, providing end-to-end secret key provisioning on demand. Cho et al. (2021) proposed a practical key management scheme for a QKD network based on CTR technology, integrating complex QKD networks into existing telecommunication networks. Mavromatis et al. (2018) demonstrated QKD for software-defined IoT applications, utilizing a low-power

QKD protocol for energy-efficient communication. Peng et al. (2017) introduced QKDFlow, a secure communication framework for SDN environments based on QKD, achieving low latency and high throughput. Lopez et al. (2020) presented an application of SDN services combined with QKD within a conventional telecommunication network, providing secure key distribution for SDN services. Zhang et al. (2018) proposed a quantum cryptography communication network based on SDN, achieving secure communication with low latency and high throughput.

Table 3-2 Comparative Analysis of Previous Works in Integrating QKD with SDN

Solution Type	Key Features	Implementation Considerations	Resource Utilization	Limitations/Gaps	References
ETSI Prototype	Trusted relay nodes, SDN Controller, Software-Defined QKD nodes, PoliQI testbed	Prototype-specific design considerations, Relay node placement strategies	Efficient utilization of SDN resources	Limited relay node placement options, Potential vulnerability to node compromise	Bassi et al., 2023
QKD Network with SDN	Metric-based path selection, OSPF routing, RIP routing	Metric selection and calibration, Path selection sensitivity	Efficient utilization of network paths	Sensitivity to network changes, Potential congestion in high-traffic scenarios	Monita et al., 2023
Quantum Encryption for SDN Security	Quantum encryption, Two-way authentication, QKD between controller and switch	Integration with existing encryption protocols, Authentication protocol selection	Efficient key management and distribution	Potential overhead in quantum encryption, Initial setup complexity	Nie et al., 2020
Multi-Path QKD for SD-QKDNs	SDN Controller, Multi-path based routing algorithm	Path selection strategies, Scalability with network size	Efficient utilization of network paths	Sensitivity to network congestion, Complexity in multi-path management	Liu et al., 2019

Orchestration Framework for NFV	SDN-controlled optical network, Resource management module, Dynamic routing module	NFV integration strategies, Resource allocation algorithms	Efficient utilization of QKD and NFV resources	Potential overhead in NFV orchestration, Scalability challenges with increasing services	Aguado et al., 2017
Key on Demand with QKP	Quantum Key Pool, Dynamic routing, Wavelength, Key assignment algorithm	Key assignment strategies, QKP management overhead	Efficient key utilization and assignment	Potential overhead in QKP management, Sensitivity to dynamic network conditions	Cao et al., 2017
Quantum Abstraction Interface	QAI, Common interface for QKD devices and SDN controllers	QAI adoption strategies, Compatibility with diverse QKD devices	Efficient integration of QKD devices	Sensitivity to QKD device variations, Potential compatibility issues with future QKD technologies	Mendez et al., 2020
Physical Layer Security with SDN	SDN Controller, Monitoring for physical layer attacks	Monitoring strategies, Resource-intensive monitoring considerations	Efficient detection and mitigation of attacks	Sensitivity to network scale, Potential limitations in attack detection precision	Hugues-Salas et al., 2019
DDoS Resilience for QKD	SDN Application, Real-time monitoring of quantum parameters	Real-time monitoring strategies, Sensitivity to DDoS characteristics	Efficient response to DDoS attacks	Sensitivity to network dynamics, Potential limitations in attack prevention	Hugues-Salas et al., 2018
Time-Scheduled QKD with QKP	Time-scheduled QKD, Quantum Key Pool	Time synchronization strategies, QKP optimization challenges	Efficient construction of QKPs	Sensitivity to synchronization accuracy, Potential overhead in QKP management	Cao et al., 2018
Quantum Services Architecture	QSA, APIs for quantum service development, ONOS as SDN controller	QSA adoption strategies, Compatibility with existing infrastructures	Efficient utilization of quantum services	Sensitivity to QSA configuration, Potential challenges in quantum service development	Brito et al., 2019
QKD-enabled SDN Architecture	QKD devices, SDN controllers, SDN switches	Compatibility with diverse QKD devices, Integration complexity	Efficient key generation and distribution	Sensitivity to QKD device interoperability, Potential challenges in network-scale deployment	Zhao et al., 2017

SDN in a QKD Network with CTR	SDN-enabled architecture, Multi-tenant provisioning protocols and strategies	Multi-tenancy management, Scalability with increasing tenants	Efficient provisioning for multiple tenants	Sensitivity to tenant resource demands, Potential challenges in tenant isolation	Cao et al., 2019
QKD Integration with SDN	QKD-aware routing algorithm, QKD device characteristics, Network topology	Sensitivity to network topology changes, Adaptability to dynamic environments	Efficient integration with existing infrastructure	Sensitivity to network-scale changes, Potential challenges in device-to-controller communication	Aguado et al., 2020

3.4 Advancements in ML Over QKD

ML has been actively used to improve the performance of QKD networks. Recently, RL has been applied to QKD networks to optimize the performance of QKD systems and enhance their security. RL algorithms can be used to learn optimal strategies for various tasks in QKD networks, such as key generation, error correction, and detection of eavesdropping attacks. One potential application of RL in QKD networks is to optimize the key generation rate by learning to adjust the parameters of the QKD system, such as the modulation scheme and the error correction code, to maximize the key generation rate while maintaining a sufficient level of security. Another potential application of RL in QKD networks is to detect and mitigate eavesdropping attacks by learning to identify patterns in the QKD data that could indicate the presence of an attack and act appropriately to secure the communication channel. In addition, the integration of RL with QKD aspects has the possible to significantly improve the performance and security of QKD networks, and it is an area of active research in the field of quantum communication. Moreover, by employing RL algorithms, the network gains the ability to dynamically adjust to fluctuating network conditions and evolving security demands.

3.4.1 Previous Studies of ML Over QKD

ML in QKD networks has garnered considerable interest among researchers. Aparicio-Pardo et al. (2023) employed RL to tackle the stochastic control issue in quantum entanglement, demonstrating superior performance over existing policies, especially when precise models of quantum devices are unavailable. Another breakthrough was achieved by Hajomer et al. (2023) who successfully demonstrated long-distance CV-QKD using a locally generated local oscillator, covering a remarkable 100 km over a fiber channel with a total loss of 15.4 dB. This accomplishment was attributed to effective phase-noise-induced excess noise management through an ML framework for carrier recovery and modulation variance optimization. Mao et al. (2023) utilized a long short-term memory (LSTM) based neural network model to enhance the secret key rate through simulations, outperforming Backward-Propagation (BP) based networks. Wang and Lo (2019) proposed an ML-based approach for predicting optimal parameters in QKD, demonstrating superior key rates compared to parameters selected by experts. Liu et al. (2018) introduced an automatic parameter prediction method using ML for practical CV-QKD, offering improved efficiency and security. Additionally, Mao et al. (2020) developed an ML-based defense strategy against quantum attacks, showcasing its efficacy in real-time detection. Okey et al. (2022) presented a method using ML to predict optimal parameters for a given QKD protocol, significantly speeding up the optimization process. Niu et al. (2021) proposed a flexible key-size-driven wavelength assignment scheme for integrating QKD into optical networks. Ali et al. (2023) introduced DROM, a deep reinforcement learning-based approach for optimizing routing in SDN-based networks, exhibiting notable improvements in network performance. Ou et al. (2018) proposed a real-time optimization method for QKD networks using ML algorithms, demonstrating enhanced performance in simulations and experiments. Cao et al. (2019) addressed the multi-tenant

provisioning problem for QKD networks using RL algorithms, effectively maximizing network throughput while meeting security requirements. Furthermore, Cao et al. (2020) tackled the online multi-tenant provisioning problem, showing promising results with heuristics and RL-based solutions. These studies collectively demonstrate the transformative potential of ML in enhancing various aspects of QKD networks, ranging from optimization to security.

Table 3-3 Comparative Analysis of Previous Works in Integrating ML with QKD

Solution Type	ML Technique Used	Application Area	Key Findings	Limitations/Gaps	References
Quantum Entanglement Control	Reinforcement Learning	Quantum Entanglement Control	Outperformed existing policies in entanglement management.	Limited applicability when precise models of quantum devices are unknown.	Aparicio-Pardo et al. (2023)
Long-Distance CV-QKD	Machine Learning	Long-Distance CV-QKD	Achieved a record-breaking 100 km distance in CV-QKD.	Limitations in adapting to highly dynamic network conditions.	Hajomer et al. (2023)
Secret Key Rate Optimization	LSTM-based Neural Network	Secret Key Rate Optimization	LSTM-based neural network achieved higher secret key rates.	Performance may vary based on quality and diversity of training dataset.	Mao et al. (2023)
Parameter Prediction in QKD	Machine Learning	Parameter Prediction in QKD	Predicted optimal parameters for higher key rates.	Performance influenced by dataset quality and diversity.	Wang & Lo (2019)
Parameter Prediction in CV-QKD	Deep Neural Network	Parameter Prediction in CV-QKD	Predicted optimal parameters for higher key rates.	Relies on availability of diverse dataset for training.	Liu et al. (2018)
Quantum Attack Detection in CV-QKD	Machine Learning	Quantum Attack Detection in CV-QKD	ML model accurately detected quantum attackers, enhancing security.	Effectiveness may vary based on quantum attack strategies.	Mao et al. (2020)
Parameter Optimization in QKD Protocols	Machine Learning	Parameter Optimization in QKD Protocols	Achieved significantly faster optimization speed.	Study focuses on parameter optimization.	Okey et al. (2022)

Key Size-Driven Wavelength Assignment	Deep Reinforcement Learning	Key Size-Driven Wavelength Assignment	Recycling wavelength fragments for secure key transmission.	May have limitations in dynamically changing network conditions.	Niu et al. (2021)
Routing Optimization in SDNs	Deep Reinforcement Learning	Routing Optimization in SDNs	DROM improved network performance in delay, packet loss, and utilization.	Extensive training may be required for generalization.	Ali et al. (2023)
Real-time Optimization of QKD Networks	Machine Learning	Real-time Optimization of QKD Networks	ML-based optimization significantly improved QKD network performance.	Real-time data availability may be a requirement.	Ou et al. (2018)
Multi-Tenant Secret Key Assignment in QKD	Reinforcement Learning	Multi-Tenant Secret Key Assignment in QKD	RL-based approach outperformed traditional methods in throughput.	Computational resources may be substantial. Challenges with numerous tenants.	Cao et al. (2019)
Multi-Tenant Provisioning in QKD	Heuristics and RL-based On-MTP	Multi-Tenant Provisioning in QKD	RL-based On-MTP algorithm significantly outperformed tested heuristics.	Effectiveness may vary based on specific network topology and request distribution.	Cao et al. (2020)

3.5 SDQTRF Model Proposed

Based on the previous literature reviews, it is evident that numerous studies have leveraged CTR technology to increase the effective range of QKD systems. Additionally, several research endeavors have explored the integration of SDN and ML techniques within QKD networks, all of which have incorporated CTR technology to extend transmission distances. However, this approach has certain drawbacks. If the security of specific CTR nodes cannot be guaranteed due to eavesdropping activities, malicious attacks, or hacking incidents, the effectiveness of CTR technology for remote QKD is compromised. Consequently, the failure of

key distribution using CTR technique can lead to various network issues, including compromised communication security, increased network key demand, reduced secret key rate, higher QKD service blocking rate, and limited transmission distance. While most studies in the literature have focused on successful distribution of quantum secret keys using CTR technique, few have addressed the failures associated with this approach. To address this gap, this dissertation proposes a new survivability model called SDQTRF .To the best of our knowledge, no previous work has explored the application of SDN over QKD networks for managing secret keys in case of CTR technique fails to distribute the quantum keys (failed in relay process). The SDQTRF model is based on the integration of SDN into a QKD network, aiming to enhance network performance by minimizing the impact of CTR failures.

CHAPTER FOUR: METHODOLOGY

4.1 Introduction

This chapter is all about how to solve the problem of distributing quantum secret keys using CTR technology. In the proposed model, five contributions were made to overcome this issue. Firstly, QKD over SDN was implemented for managing unsuccessful keys based on CTR technology. Secondly, to ensure the generation of secure secret keys, the SARAG04 protocol was selected. Thirdly, a new relay protocol was proposed to support the mechanism of the proposed model. Fourthly, the recycling process was improved by integrating the Q-learning method for the first time. Finally, a new routing method for finding an alternative secure path was presented, playing an effective role in case the recycled secret keys cannot be relayed. All these contributions will be discussed in this chapter.

4.2 Proposed Model of SDQTRF

4.2.1 System Model of SDQTRF

In the context of the model, the graph representation (G) is used to capture the structure and connectivity of the network designed for secure key transmission. The nodes in the graph, denoted by N , represent the secure path nodes. These nodes play a crucial role in maintaining the security of the communication paths within the network.

The connecting links in the network are represented by the set C . Each link (i, j) in C connects two nodes, i and j , indicating a direct connection between them. By including all such links in the set C , the graph G captures the connectivity of the network and allows us to analyze the key transmission process across different nodes.

The current secure path is denoted by SP. This signifies the specific route taken by the secret key within the network. The secure path ensures that the key transmission remains protected and confidential, preventing unauthorized access or interception.

For the generation and distribution of secure key, the model incorporates QKD technology. In the proposed model, QKD_n represents the pairing key generated between paired nodes in the network. These pairing keys play a crucial role in establishing secure communication channels between the nodes involved in the key transmission process.

The source node, denoted by SN, is the node from which the transmission of the secret key originates. It initiates the process of key distribution within the network, starting from the source and traversing through the secure path to reach the destination node.

On the other hand, the destination node, represented by DN, is the node that receives the secret key transmitted within the network. It serves as the endpoint for the key transmission process and is responsible for utilizing the received key for the intended cryptographic operations.

In the proposed model, it is assumed that QKD is capable of retaining and managing end-to-end keys. This means that QKD can generate and maintain keys that span the entire communication path between the source and destination nodes, ensuring end-to-end security. However, QKD can only produce point-to-point keys at a given rate through direct links (i, j) between paired nodes. This implies that the generation of pairing keys is limited to the direct connections between specific node pairs.

Table 4-1 Comprehensive the Notation and definitions of system model

NOTATIONS	DEFINITIONS
QN	Q-value between pair nodes
SPn	new generate secure path
ACKn(i,j)	notification at success sending delivered
ACKfn(i,j)	notification at failure sending
Gkn	key generate for pair nodes
Rkn	recycling for pair nodes based on Q-values
Nfi	pair nodes failure
Nxi	next node in secure path , which mean CTR nodes
Nsf	nodes from source to failure node
ACKr	notification from controller to nsf to start recycling
S	Secure node
US	Unsecure nodes

4.2.2 Methodology of SDQTRF Model

In this section, the SDQTRF model is presented, which aims to alleviate the effect of CTR failures on QKD networks. The development of the SDQTRF paradigm was driven by three primary objectives.

Firstly, to enhance the manageability of QKD networks in cases where the distribution of secret keys fails based on CTR technology. When secret key distribution fails, it can significantly influence the security and functionality of the network. To address this issue, SDN technology was employed over the QKD infrastructure. SDN offers a centralized and programmable control plane, enabling dynamic reconfiguration of network elements and resources. By integrating SDN into the QKD network, the control and management capabilities are improved, allowing for efficient handling of scenarios involving a failed secret key relay. It is important to note that the SDQTRF model is designed to have minimal impact on the SDN process with QKD when secret keys are successfully relayed. In such cases, the SDQTRF model remains dormant and does not interfere with the normal

functioning of SDN and QKD. Its activation is triggered solely when the CTR technology fails to relay the secret keys, requiring a contingency plan to ensure uninterrupted operation of the network. To fulfill this contingency requirement, the specific function known as the Contingency Function was introduced within the SDN controller platform, shown in Fig. 4-1. This function serves as the core component of the SDQTRF framework, offering enhanced reliability and safeguarding the SDN process with QKD during the failure of key relay. The Contingency Function comprises two essential support modules: the Q-Learning module and the Topology module. The Q-Learning module plays a crucial role in intelligent decision-making when CTR failures occur. It utilizes reinforcement learning techniques to learn from past experiences and employs a reward-based system to determine the most effective actions and strategies for recovering the failed QKD traffic. By continuously learning and adapting, the Q-Learning module contributes to the resilience and efficient recovery of the network. It dynamically adjusts routing and forwarding decisions based on the current network conditions and the specific failure scenario. The Topology module is responsible for providing real-time information about the network's topology and connectivity. It maintains an up-to-date map of the network infrastructure, including nodes, links, and their relationships. This information is crucial for identifying alternative paths and rerouting the QKD traffic in the event of a CTR failure. By leveraging this topology information, the Topology module enables efficient traffic recovery and minimizes disruptions within the QKD network. It constantly monitors the network status and updates the SDN controller with the latest network topology information, ensuring accurate decision-making and effective traffic rerouting.

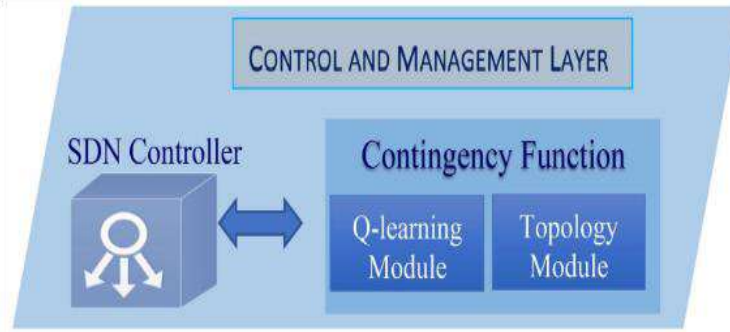


Fig. 4-1 Contingency function inside the controller

In addition, the relay key protocol significantly contributing to the key management procedure of the QKD network, it plays a vital role in facilitating this process. The relay key protocol serves as a fundamental mechanism for securely transmitting cryptographic keys within the network. It ensures that the keys are reliably relayed from one node to another, establishing a secure communication channel between the sender and the receiver. Typically, the public-XOR-key protocol is widely used as a suitable approach for key management in QKD networks. This protocol involves performing an XOR operation on the QKD keys generated by each node and sharing the resulting XOR key with the subsequent relay node. However, in the case of a CTR failure, where the designated relay node fails to relay the keys, the integrity and security of the key distribution process are compromised. To address this specific scenario, a new relay protocol is proposed that is tailored to handle unsuccessfully relayed keys. The objective of this protocol is to ensure that the QKD network can recover from CTR failures and continue to securely transmit the keys to their intended destinations. The proposed relay protocol incorporates improvements and modifications to the existing public XOR-key protocol, making it more resilient and robust in the face of relay failures. The mechanism of the proposed relay protocol builds upon the fundamental concepts of the public XOR-key protocol while introducing additional steps to handle CTR failures effectively. The proposed relay protocol is explained as follows:

1. The QKD protocol is executed by each node, along with its neighboring nodes, to generate n pairs of QKD keys. This process involves the exchange of quantum information and subsequent measurements to establish a shared secret key between the communicating nodes.
2. The first relay node in the network receives the QKD keys from the sender node and performs an XOR operation on them. Additionally, the relay node adds a checksum to the resulting XOR key. This checksum ensures the integrity of the XOR key and detects any potential errors or tampering during transmission. The relay node temporarily stores the original QKD keys for potential recovery purposes and transmits the XOR key along with its checksum to the subsequent relay node.
3. The next relay node in the network receives the XOR key and verifies the integrity of the checksum. If no errors are detected, the relay node proceeds to repeat the XOR operation using the XOR key received from the previous relay node and the QKD keys obtained from the sender node. This process continues iteratively until all relay nodes have performed the XOR operation.
4. The XOR results obtained from each iteration are then forwarded to the next CTR node in the network. The CTR node plays a critical role in coordinating the relay process and ensuring the secure transmission of the XOR results to the destination node.
5. Finally, the destination node receives the XOR results from the CTR node and calculates the final key by utilizing its own QKD key. This process involves performing additional cryptographic operations, such as error correction and privacy amplification, to derive a secure and usable key. The resulting

common key, denoted as $Qk1$, is then shared between the sender and receiver nodes for secure communication. Subsequently, Alice can utilize the key $Qk1$ to encrypt and transmit a secret message to Bob, ensuring confidentiality and integrity during the communication process.

Remark 1: In cases where the secret key is successfully relayed, the receiver instructs all previous nodes to immediately dismiss the QKD keys. This precautionary measure ensures that any potentially compromised keys are promptly discarded, maintaining the security and confidentiality of the communication.

The Fig. 4-2 provide a detailed explanation of the relay protocol's mechanism specifically in scenarios involving CTR failure. This comprehensive explanation will outline the steps and procedures implemented within the proposed relay protocol to ensure the successful recovery and transmission of keys when a CTR failure occurs. By understanding the inner workings of the relay protocol in these critical situations, it is possible to appreciate the resilience and effectiveness of the proposed solution in mitigating the impact of relay failures on the overall security and functionality of the QKD network.

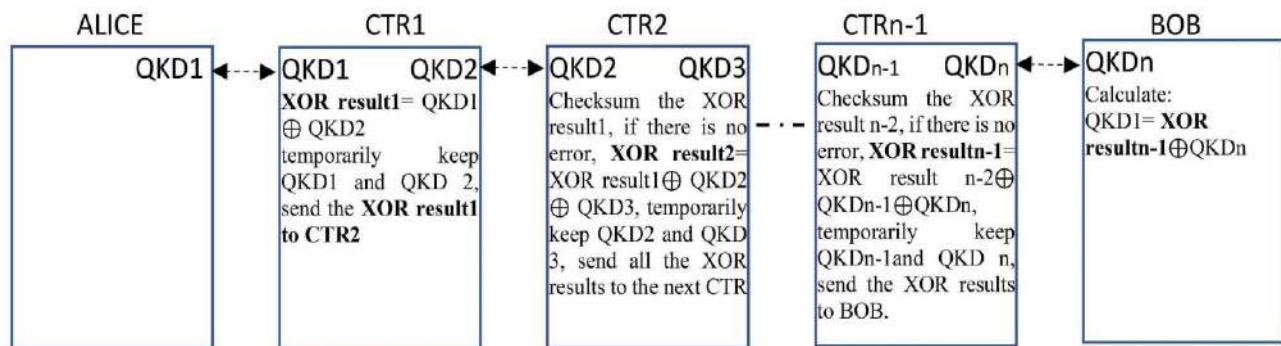


Fig. 4-2 Proposed relay key protocol

Secondly, one of the key challenges addressed is how to utilize unsuccessful relay keys to expand key availability within the QKD network. When a key cannot

be successfully relayed, it represents a valuable resource that can still be repurposed to enhance key availability and improve overall network resilience. The most efficient approach is to recycle these failed keys and use them for service encryption, albeit at a lower level of security. By repurposing these keys, it is possible to maximize their utility and minimize potential waste. However, to ensure the reliability and effectiveness of the recycling process, it is crucial to determine the appropriate amount of recycling. This involves evaluating the quantity of failed keys that can be safely repurposed without compromising the overall security of the network. To make the recycling process more secure and optimized, incorporating the recycling method from the SDQTRF provides a foundation for key management in the QKD network. The Q-Learning module of the SDQTRF model plays a central role in determining the recycling amount based on the Q-value. The Q-value represents the expected utility or value associated with recycling keys at a particular node in the network. It takes into account various factors such as the reliability of the node, historical data on key failures, and the network's overall performance. By leveraging the Q-values, informed decisions can be made on how many failed keys should be recycled at each node, optimizing key availability while maintaining an acceptable level of security. Moreover, to minimize potential vulnerabilities and protect sensitive information, it is ensured that the key recycling process is strictly localized. It is carried out only from the source node to the nodes suspected of causing the failure in the key distribution process. This targeted approach prevents unnecessary exposure of keys to nodes that are not directly involved in the failure, thereby maintaining the confidentiality and integrity of the recycled keys.

To provide further clarity and understanding, let us consider the following example scenario:

Assume a secure path consisting of five nodes, where the secret key is initially sent from the source node (Node 1) to the destination node (Node 5). For this example, let's assume that a failure occurred between nodes 3 and 4, resulting in the inability to relay the key.

1. Upon detecting the failure, Node 4 promptly sends a notification to the controller, as demonstrated in Fig. 4-3. This notification serves as an important indication of the failure, triggering subsequent actions within the SDQTRF model.
2. Upon receiving the notification, the controller initiates the contingency function, which is responsible for addressing failures and managing the key recycling process. The contingency function first verifies if there have been two successive failures in the same pair of nodes, as this may indicate a more significant issue requiring specific attention. Assuming no successive failures are detected, the Q-learning module computes the Q-values for the nodes in the secure path (nodes 1-4) and sends them to the controller. Additionally, the contingency function stores information about failures between pairs of nodes 3 and 4 in the topology module. The topology module serves as a repository for collecting, storing, and updating the QKD network topology, along with relevant information about the CTR nodes.
3. Leveraging the computed Q-values, the controller communicates the appropriate key recycling instructions to nodes 1-4. Each node follows the instructions and initiates the key recycling process based on its respective Q-value. The recycling process involves securely repurposing the failed keys for encryption, allowing them to contribute to the expansion of key availability within the network. Once the recycling process is finished, the controller will

request the transmission of the recycled keys from the source node to the destination node. This ensures the continuity of secure communication.

Remark2: In the SDQTRF model, the topology module plays a vital role in collecting, storing, and updating the QKD network topology, as well as relevant information about the CTR nodes. It serves as a centralized resource that periodically receives updates from the controller regarding the network's current state and the status of key distribution. The topology module maintains a comprehensive view of the network's structure, including the nodes, their connections, and any reported failures or anomalies. This information is crucial for effectively managing the key recycling process and ensuring the overall stability and reliability of the QKD network. By periodically updating the topology module with the latest data, the system can adapt to changes in network conditions and make informed decisions based on the most up-to-date information available. The topology module acts as a reliable source of information for the controller and other components of the SDQTRF model, enabling efficient key management and facilitating the recycling of unsuccessful relay keys.

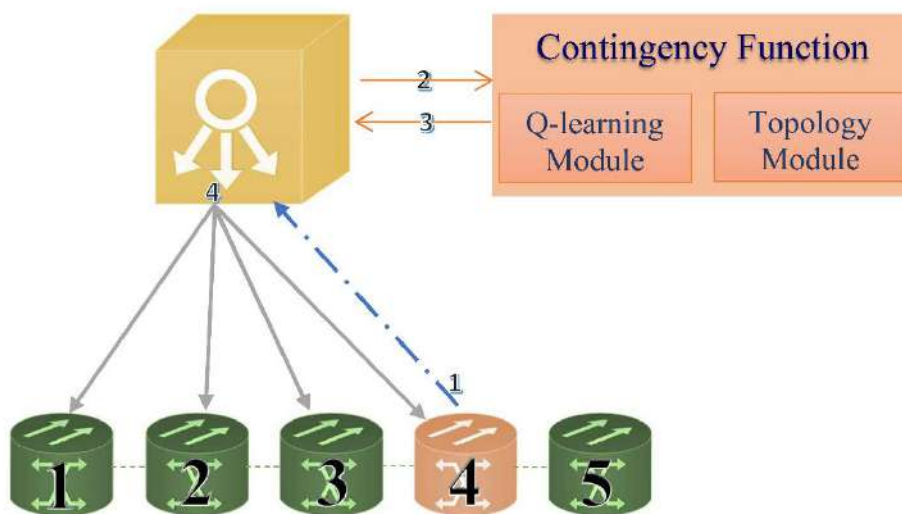


Fig. 4-3 Example of the recycling process

Thirdly, what is the alternative plan if the proposed model fails to reuse the failed relay keys, which was based on the recycling method? In such cases, it becomes necessary to explore an alternative approach that ensures the availability of secure keys. One potential solution is to find a different route within the network that can guarantee the safe transmission of keys. To address this, a new idea is proposed that focuses on identifying a new secure path, specifically tailored for the SDQTRF framework. Before embarking on the search for a secure path, the occurrence of two successive failures at the same node is considered. Based on this observation, the presence of both secure and unsecure nodes within the network is assumed. The unsecure nodes are assumed to be the cause of the failure in successfully relaying the keys. By classifying the nodes in this manner, vulnerabilities in the network can be better understood and strategies can be devised accordingly. To identify an appropriate secure path within the SDQTRF model, a Q-learning module is leveraged. This module is designed to learn from the network's experiences and make informed decisions about routing. It allocates two distinct environments: a secure environment comprising nodes with proven reliability and a separate unsecure environment consisting of nodes that have exhibited failure in the key relay process. By analyzing historical data and the topology of the network, the Q-learning module determines the most suitable path for secure key transmission.

To facilitate the Q-learning process, the topology module is utilized. This module is responsible for collecting, storing, and updating the network's topology information, including the locations of the secure and unsecured nodes. By leveraging the knowledge stored in the topology module, the Q-learning module can effectively evaluate and select a new secure path that avoids the unsecure nodes.

Let's consider an example where two successive failures occur in the same pair of nodes, specifically nodes 3 and 4, as illustrated in Fig. 4-4. In this scenario:

1. Node 4, upon detecting a relay failure, promptly sends a retransmission notification to the controller, indicating the occurrence of an issue.
2. Upon receiving the notification, the controller initiates the contingency function to handle the failure situation. The contingency function is responsible for assessing the severity of the failure and determining the appropriate course of action.
3. If the contingency function, based on the information stored in the topology module, identifies two consecutive failures in the same pair of nodes (in this case, nodes 3 and 4), it marks these nodes as unsecure. Subsequently, the contingency function triggers the Q-learning module to find a new secure path that excludes the unsecure nodes. The Q-learning module uses its knowledge of the network's topology and past experiences to determine an alternative route that ensures the secure transmission of keys. Once the new secure path is identified, the information is relayed back to the controller.
4. Acting on the instructions received from the controller, the nodes along the new secure path generate new secret keys between each pair of nodes based on SARAG protocol. The controller then coordinates the transmission of the key from the source node to the destination node through this newly established secure path, ensuring the secure delivery of encrypted services.

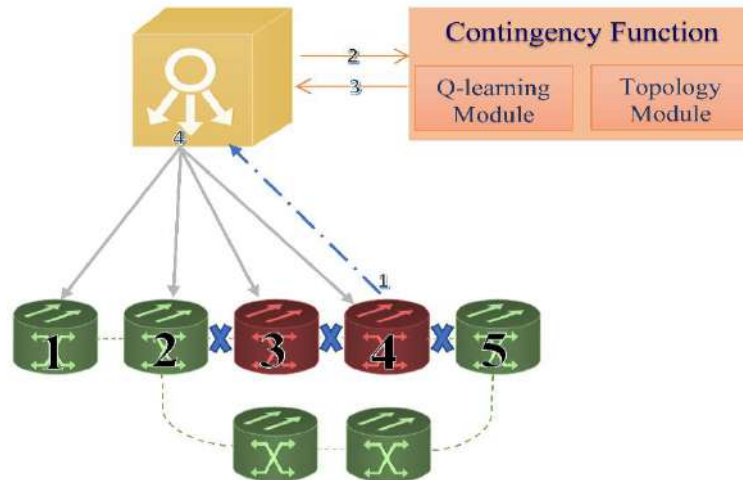


Fig. 4-4 Proposed process to find a new secure path

4.2.3 Algorithm of SDQTRF Model

The SDQTRF model presented in this dissertation tackles CTR failure in QKD systems by applying SDN principles. It provides an efficient solution to mitigate the effects of these failures, with detailed steps outlined in Table 4-2 based on the notations in Table 4-1.

The SDQTRF model, outlined in Table 4-2, utilizes SDN to establish a secure path with fewer total hops. Subsequently, the model analyzes the CTR node and initiates the key transfer from S_n to D_n . It then employs the relay protocol to verify successful key delivery hop by hop. In the absence of untrusted nodes, the key reaches the destination securely. However, if an untrusted node is detected and a failure occurs, an ACKfn is sent to the controller, triggering the contingency function. This function checks for successive failures at the same node. If none are found, it generates Q-Values and initiates key recycling. If two successive failures occur, the contingency function marks the nodes as unsecure and employs Q-learning to establish a new secure path, excluding the compromised nodes. The controller then resumes sending the key one hop at a time along this new path.

Table 4-2 SDQTRF algorithm

Algorithm: The proposed SDQTRF model

1:	inputs $G(N, C, SP, QKDn, SN, DN)$
2:	output (Success Delivered Key from SN to DN then dismiss the QKD key)
3:	For $i=SN$ to DN Loop
4:	Send Key to Nx_i
5:	Based on the proposed relay protocol, check if delivery was successful.
6:	If $ACKn(Nx_i)$ then:
7:	If $Nx_i = DN$ then:
8:	output
9:	Else:
10:	Go to Step: 3
11:	End if
12:	Else :
13:	Send $ACKfn(Nx_i)$ to Controller.
14:	Controller run contingency function
15:	Contingency request network topology
16:	If twice successive failures at the same node then:
17:	Mark Nfi as uS and the rest nodes as S
18:	Excluding Nfi
19:	Generate SPn and Gkn
20:	Go to Step: 3
21:	Else:
22:	Generate QN value for Nsf
23:	Controller sends $ACKr$
24:	Start $Rkn(Nsf)$
25:	Go to Step: 3
26:	End if
27:	End if
28:	End Loop

The for-loop covering lines 3–28 starts sending QKD keys from the source node to the destination node. Line 4 sends the key to the next node, whereas line 5 applies the relay protocol to verify whether the next node has successfully received the key. If it is successful, line 7 checks whether the key has reached the destination node. If it reaches the destination node, line 8 goes to the output of the algorithm. If not, line 10 returns to send the key to the next node line 3. If the check of acknowledgement in line 6 were a failure then in line 13 the received node will send a failure acknowledgement to the controller to inform it that there was error occurred, in line 14 the controller will run the contingency function, in line 15 the contingency function requests that the topology module collect information regarding each node. After gathering the necessary information, the contingency function verifies its findings (line 16). However, if it determines that two successive failures have occurred at the same nodes, it marks both the sender and receiver nodes as unsecured nodes (line 17). Then in line 18, it will update the topology module and exclude these unsecured nodes from the new secure path. In line 19 new secure path will be generated based on the exclusion that was determined in line 17 & 18 after new secure path was found the algorithm will start all over again from line 3, else if the line 16 were false (no successive failure are found). Then in line 22 the contingency function will ask the Q-learning module to generate Q-value for each secure path nodes and will ask the controller to send notification from source node to the node was error occur to start key recycling depending on the generated Q-values as in lines 23 & 24. After key recycling is done, the algorithm will start all over again from line 3, and continue until key reach to the destination node.

4.3 SARAG04 Protocol

The SARAG04 protocol was designed using two programs: one for data transmission and the other for data reception. A real-time application calculated Round Trip Time (RTT) between devices. It enabled active listening for communication requests and TCP connection setup. Packet segmentation managed larger packets, with a 64KB segment size for TCP connections. The model also had encryption based on the one-time pad principle. Implementation involved programming and Handshaking signals for synchronization between two computers. Flowchart A.1 in Appendix A covered port opening and TCP connection, while Flowchart A.2, A.3 and A.4 in Appendix A in the appendices showed protocol stages, highlighting Handshaking's role in communication. The operational procedure of SARAG04, as detailed in (Abdulqadir et al. 2020), is outlined as follows:

1. The sender initiates the SARAG04 protocol by randomly preparing a stream of qubits, each in one of the four states: $|0\rangle$, $|45\rangle$, $|90\rangle$, or $|135\rangle$. These qubits are then transmitted to the receiver over the quantum channel, ensuring the preservation of their quantum properties during transmission in the Quantum Transmission stage. Flowchart A.5 in Appendix A outlines the sequential steps involved in the quantum transmission phase. Conversely, flowchart A.6 in Appendix A illustrates the systematic process of receiving the quantum states at the receiving side.
2. Upon receiving the qubits, the recipient randomly chooses a measurement basis, either rectilinear (horizontal/vertical) or diagonal, for each qubit in the Sifting stage. This random selection ensures that the measurements are unbiased and prevents eavesdroppers from predicting or manipulating the measurement outcomes. This process represents the sifting stage, and it is

illustrated by flowchart A.9 in Appendix A. Additionally, flowchart 4.7 and A.8 in Appendix A shows the process of overt bases exchange, while flowchart 4.10 in Appendix A illustrates the process of encoding the quantum states into binary bits.

3. With each qubit transmission, the sender announces one of four possible combinations: $\{|0\rangle, |45\rangle\}$, $\{|0\rangle, |135\rangle\}$, $\{|90\rangle, |45\rangle\}$, or $\{|90\rangle, |135\rangle\}$. These combinations contain the correct state transmitted alongside another state according to a predefined rule in the Sifting stage. This step allows the recipient to determine the correct state by comparing it with the accompanying known state.
4. The recipient then informs the sender about the cases where he was unable to detect the transmitted state correctly and indicates the cases he could accurately determine in the Error Correction stage. The flowchart 4.11 in Appendix A illustrates the fundamental steps encompassed within the error correction stage. In cases of confusion or uncertainty, these instances are disregarded. This feedback from the recipient helps identify potential errors or discrepancies in the transmission and measurement process.
5. The quality of the transmission is assessed by estimating the Quantum Bit Error Rate (QBER) in the Quantum Transmission stage. The QBER represents the error rate in the transmission and measurement process, indicating the presence of any potential eavesdropping or intrusion attempts. The calculation of the QBER provides insights into the security and reliability of the key exchange process according to the SARG04 protocol.
6. To ensure security and privacy in the absence of intrusion, error correction and privacy amplification techniques are applied to the exchanged key in the

Error Correction and Privacy Amplification stages. Error correction allows for the correction of errors and discrepancies that may have occurred during transmission, ensuring the accuracy and integrity of the final key. Privacy amplification further enhances the security of the key by distilling a shorter, but more secure, final key that is immune to potential eavesdropping attempts.

7. Finally, to encrypt messages securely, a one-time pad cipher is utilized with the generated final key. The one-time pad cipher is a form of symmetric encryption that ensures the confidentiality and integrity of the transmitted messages. This encryption scheme guarantees the security of the communication by using the final key as a secret key for message encryption and decryption.

By following these steps, the SARG04 protocol facilitates the secure exchange of quantum secret keys among the sender and receiver, enabling them to establish a shared secret key for subsequent secure communication. The protocol's random selection of measurement bases, error correction, privacy amplification, and encryption techniques collectively contribute to achieving secure and reliable quantum key distribution.

Table 4-3 Illustrate example of the SARG04 protocol in working

The bits	1	2	3	4	5	6	7	8	9	10	11	12
Sender's Random Bits	0	0	0	1	0	1	1	1	0	1	1	0
Sender's Random Basis	+	+	+	X	X	X	+	+	+	+	X	X
Sender's States	↑	↑	↑	↘	↗	↘	→	→	↑	→	↘	↗
Receiver's Random Basis	X	X	+	X	X	+	+	X	+	X	+	+
Receiver's Possible Measurement	↘	↗	↑	↘	↗	↑	→	↗	↑	↗	↑	↑
Receiver's Result	1	0	0	1	0	0	1	0	0	0	0	0
Sender Announcement states	↑↘	↑↘	↑↗	→↘	↑↗	→↘	→↘	→↗	↑↘	→↘	↑↘	→↗
Discovered States		↑				↘				→		↗

The sifted Key		0				1				1		0
----------------	--	---	--	--	--	---	--	--	--	---	--	---

The example provided in Table 4-3 offers a deeper insight into the working steps and interpretations of the SARG04 protocol, showcasing its effectiveness in identifying and determining the transmitted quantum states. By further analyzing the examples and their implications, it can be gain a more comprehensive understanding of the protocol's operation.

In the first column of Table 4-3, where the recipient could not accurately determine the transmitted state, the misinterpretation occurred because the recipient used the diagonal measurement rule (\uparrow) and mistakenly read it as \searrow . This scenario highlights the significance of using the correct measurement basis for accurate identification. The recipient, expecting both states (\uparrow and \searrow) to be transmitted, should have correctly identified \searrow if it was the originally sent state. However, due to the incorrect rule applied, the polarization of the state changed to \searrow , causing confusion and preventing the recipient from confirming the true nature of the received state. This uncertainty prompts the recipient to inform the sender of the inconclusive result.

On the other hand, the second column of Table 4-3 demonstrates cases where the recipient successfully identified and determined the transmitted state. Using the diagonal measurement rule, the recipient measured the transmitted state (\uparrow) and correctly interpreted it as (\nearrow). By comparing the two possible states (\uparrow and \searrow) sent by the sender, the recipient can deduce that the transmitted state must have been (\uparrow) because if it were (\searrow), it would have been measured correctly without any errors using the diagonal rule. This successful identification allows the recipient to confidently notify the sender about the accurate detection and identification of the state.

By examining these examples and understanding their implications, researchers can evaluate the protocol's performance in terms of its ability to correctly interpret and determine the transmitted quantum states. The examples highlight the importance of using the appropriate measurement basis and the potential consequences of using an incorrect rule, leading to polarization changes and measurement errors.

Furthermore, by analyzing a larger set of examples and variations in transmitted states, researchers can obtain statistical insights into the protocol's overall performance, including its error rates, detection probabilities, and robustness against eavesdropping attempts. This extensive analysis helps assess the reliability and security of the SARG04 protocol, enabling researchers to refine and optimize its implementation for real-world QKD applications.

4.3.1 Modeling Quantitative Cases

The analysis of the probabilities of detecting the transmitted states in the SARG04 protocol, as illustrated by Table 4-4, provides valuable insights into its performance and reliability. By examining the probabilities associated with each column, it can further extend the explanation and understand the implications of the findings.

In column (1), where the probability of knowing the transmitted state is ($P_1 = 0$), it's observe that the cases involving the combinations $\{(\uparrow \text{ and } \searrow) \text{ and } (\uparrow \text{ and } \nearrow)\}$ are neglected. This implies that in these cases, the recipient is unable to accurately determine the transmitted state. The probability of successful detection in this column is zero, indicating the limitations of the protocol in certain scenarios.

Moving to column (2), the probability of knowing the transmitted state is ($P_2 = 1/2$). This means that in two out of the four possible cases, the recipient

successfully identifies the transmitted state. The protocol demonstrates its effectiveness by achieving a 50% detection rate in this column.

In column (3), the probability of detection is ($P_3 = 0$). None of the transmitted cases are correctly identified, indicating a failure in detection for this particular configuration.

Columns (4) and (5) exhibit a probability of detection ($P_4 = 1/2$). In half of the cases, the transmitted states are successfully detected, highlighting the protocol's capabilities in these scenarios.

Similarly, column (6) represents a scenario where no detection occurs ($P_6 = 0$). The transmitted states cannot be accurately identified, indicating a limitation of the protocol in this specific configuration.

Column (7) presents a probability of detection ($P_7 = 1/2$), implying that in one out of the two cases, the transmitted state is successfully detected. The protocol demonstrates moderate performance in this configuration.

Finally, in column (8), the probability of detection is ($P_8 = 0$), indicating that no detection occurs for the transmitted states in this particular setup.

The following Equation illustrates the calculating of the probability of total discover states (PTDS):

$$PTDS = 1/8 * (P_1 + P_2 + P_3 + P_4 + P_5 + P_6 + P_7 + P_8) \quad (4.1)$$

Referring to Table 4-4, the PTDS is determined by substituting specific values for P_1 through P_8 , which in this case are 0, 1/2, 0, 1/2, 1/2, 0, 1/2 and 0 respectively. This leads to a PTDS value of 2/8 for the cases outlined in this protocol, indicating

that only two out of the eight cases can be successfully detected. Therefore, after the filtering process, the key length is reduced to 1/4 of the length of the transmitted key.

Table 4-4 Comprehensive list of states transmittable and measurable in the SARG04 protocol using random rules

No.	1	2	3	4	5	6	7	8	
Sender's Random Bits	0	0	1	1	1	1	0	0	
Sender's Random Basis	+	+	+	+	X	X	X	X	
Sender's States	↑	↑	→	→	↓	↓	↗	↗	
Receiver's Random Basis	+	X	+	X	+	X	+	X	
Receiver's Possible Measurement	↑	↓	↗	→	↓	↗	↑	→	
Receiver's Result	0	1	0	1	1	0	0	1	
Sender Announcement states	↑ ↓ ↓ ↗	↑ ↓ ↓ ↗	↑ ↓ ↓ ↗	→ ↓ ↓ ↗	→ ↓ ↓ ↗	→ ↓ ↓ ↗	→ ↓ ↓ ↗	↑ ↓ ↓ ↗	↑ ↓ ↓ ↗
Discovered States			↑	↑			↗	↗	
The sifted Key		0	0		1	1		0	
Correct Error Discard	Discard Discard Discard	Correct Correct Discard	Discard Discard Discard	Discard Correct Correct	Discard Discard Correct	Correct Correct Discard	Discard Discard Discard	Discard Correct Correct	Discard Discard Discard

4.4 Q-learning Method

RL is a branch of machine learning that focuses on training intelligent agents to make sequential decisions in an environment to maximize a long-term cumulative reward.

Q-learning is a model-free RL algorithm used to solve sequential decision-making problems. The algorithm learns through trial and error to make optimal decisions in an environment without prior knowledge of the environment's dynamics.

The process of Q-learning algorithm can be summarized as follows:

1. Initialization: In the first step of the Q-learning algorithm, the agent initializes a Q-table. This table serves as a lookup table, with rows representing the states of the environment and columns representing the possible actions that the agent can take. Each cell in the table holds the Q-value, which represents the expected cumulative reward for a particular state-action pair. Initially, all Q-values are set to arbitrary initial values or zeros.
2. Exploration vs. exploitation: Q-learning involves a trade-off between exploration and exploitation. During exploration, the agent selects actions randomly or with some level of randomness to explore the environment and gather information about potential rewards. On the other hand, during exploitation, the agent selects actions based on the current Q-values to make decisions that are likely to lead to higher rewards. The balance between exploration and exploitation is a crucial factor in the learning process.
3. Action selection: Given the current state, the agent selects an action based on the exploration-exploitation trade-off. One commonly used strategy is epsilon-greedy, where the agent chooses a random action with probability epsilon or the action with the highest Q-value with probability (one - epsilon). This approach allows the agent to explore new actions while still favoring actions that have previously yielded higher rewards.
4. Execute action and observe reward: Once the action is selected, the agent executes it in the environment and transitions to the next state. The environment then provides feedback in the form of a reward signal, indicating the immediate reward received by the agent for taking that specific action in the current state. The agent observes this reward, which is an essential part of the learning process.

5. Q-Value update: Based on the observed reward, the agent updates the Q-value of the previous state-action pair. The update equation for Q-Learning is as follows (Chin et al., 2011):

$$Q(s, a) = Q(s, a) + \alpha * (r + \gamma * \max(Q(s', a')) - Q(s, a)) \quad (4.2)$$

$Q(s, a)$ represents the Q-value of state s and action a , α (alpha) is the learning rate that controls the extent to which new information overrides old information, r is the observed reward, γ (gamma) is the discount factor that determines the importance of future rewards, and $\max(Q(s', a'))$ represents the maximum Q-value of the next state's over all possible actions. The Q-value update allows the agent to refine its estimates of the expected cumulative rewards for each state-action pair.

6. Repeat steps 3-5: The agent repeats the process of action selection, execution, reward observation, and Q-value update to continue interacting with the environment. This iterative process helps the agent refine its Q-values and learn from the accumulated experiences.
7. Convergence: The Q-learning algorithm continues its iterations until the Q-values converge, indicating that the agent has learned the optimal policy. Convergence occurs when the Q-values stabilize, and further updates do not significantly change the values. This implies that the agent has learned the best action to take in each state to maximize the long-term cumulative reward.
8. Exploitation: Once the Q-values have converged, the agent can exploit the learned knowledge to make decisions. By selecting actions with the highest Q-values in each state, the agent follows the optimal policy it has learned. This exploitation phase allows the agent to apply its knowledge to make decisions that are expected to yield the highest cumulative rewards. The

iterative process of action selection, execution. A simple flow chart of Q-learning algorithm is shown in flow chart A.12 (Chin et al., 2011) in Appendix A.

CHAPTER FIVE: EXPERIMENTAL RESULTS AND DISCUSSION

5.1 Introduction

This chapter delves into the detailed outcomes and findings obtained through rigorous simulations and evaluations of the proposed SDQTRF model, which aims to mitigate CTR failures and enhance the security of key distribution. Through an extensive analysis, the chapter offers valuable insights into the performance and effectiveness of the model in various aspects. The adaptability of the SDQTRF model to network dynamics is thoroughly evaluated, exploring how it adjusts routing decisions and key transmission paths in response to changes in the network environment. The chapter investigates the model's resilience node compromises, assessing its robustness in maintaining the integrity and confidentiality of the key transmission process. Additionally, the performance of the relay protocol incorporated within the SDQTRF model is examined, focusing on its ability to verify successful key delivery at each hop. Overall, the chapter offers a comprehensive analysis of the SDQTRF model's performance, resilience, and security capabilities, highlighting its effectiveness in ensuring secure and reliable key transmission, adaptability to changing network conditions, and ability to withstand potential attacks. The findings provide valuable insights for further improvements and potential real-world applications of the SDQTRF model.

5.2 Simulation Results

In order to ascertain and assess the effectiveness of the SDQTRF model, extensive simulations were conducted using two distinct network topologies: the National Science Foundation Network (NSFNET) and the United States Network (USNET). These network topologies were carefully selected to represent real-world scenarios and provide a diverse range of node and link configurations.

The NSFNET, consisting of 14 nodes and 21 links, serves as a well-known and widely studied network topology in the field of computer networking. On the other hand, the USNET, with its larger scale comprising 24 nodes and 43 links, presents a more challenging and realistic scenario for evaluating the SDQTRF models performance, as shown in Fig. 5-1 and Fig. 5-2, respectively.

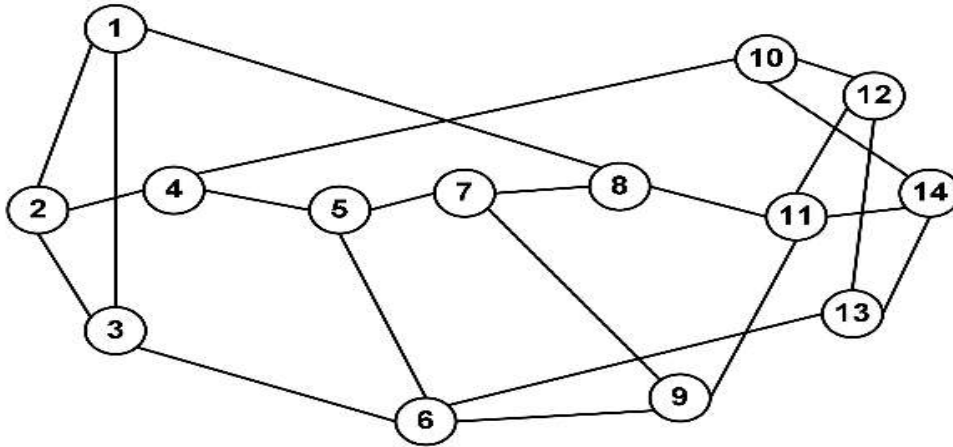


Fig. 5-1 NSFNET network topology

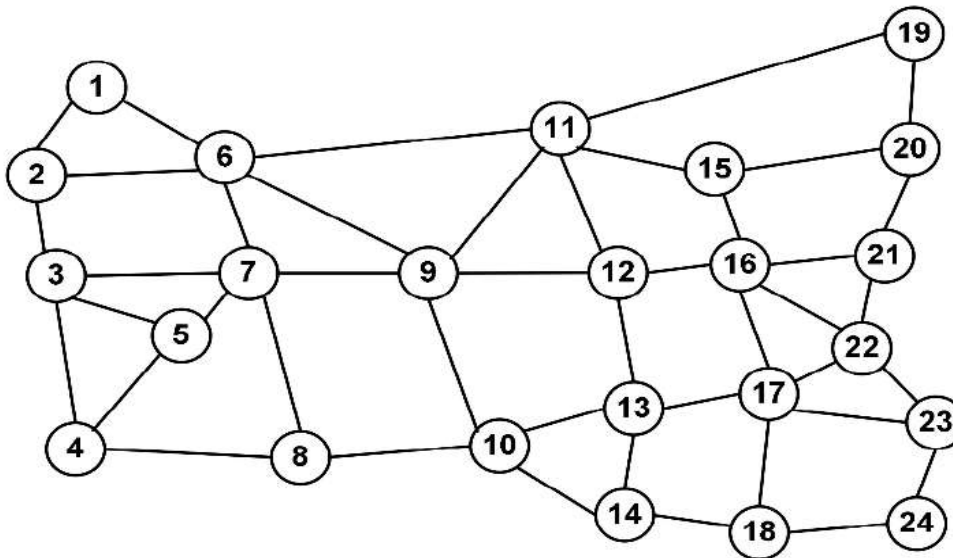


Fig. 5-2 USNET network topology

To simulate the proposed SDQTRF model, JavaScript, PHP and Python programming languages were employed due to it by their flexibility and extensive libraries for scientific computing and network simulations.

The hardware environment utilized for the simulations featured a single GPU, specifically the NVIDIA GeForce RTX 3060Ti. This high-performance GPU accelerated the computations involved in the simulations, thereby improving the efficiency of the experiments. The workstation running the simulations operated on Windows 11, a modern and robust operating system, which provided a stable and reliable platform for conducting the simulations. CUDA 11.3, a parallel computing platform and programming model, was utilized to leverage the GPU capabilities and enhance the simulation performance.

Within the simulated scenarios, the focus was specifically on evaluating the SDQTRF model's performance when the key relay process failed. This particular scenario allowed researchers to investigate the model's robustness and effectiveness in the face of potential failures or vulnerabilities. It also shed light on the model's ability to maintain the security of quantum keys transmitted over the SDN-based QKD network, assuming the SDN infrastructure itself operated normally.

To introduce realistic network conditions and evaluate the model's performance in different scenarios, random errors were generated within the nodes during the simulations. The Random Number Generator (RNG) function was employed to produce these errors, simulating various types of noise or disturbances that can affect the transmission and reception of quantum keys.

To ensure statistical significance and obtain reliable performance metrics, the simulations were run a total of over 1000 times for each network topology. The reported results represent the average performance across these repeated

simulations, allowing researchers to analyze the model's behavior under different conditions and variations in network states.

During the simulations, the widely recognized SARG04 protocol was implemented for generating QKD keys between each pair of nodes. These QKD keys served as the foundation for the subsequent relay operations and were utilized throughout the simulation scenarios. It is important to note that different key lengths were employed in the simulations to explore the impact of key length on the performance of the SDQTRF model. This analysis provided valuable insights into the relationship between key length, the model's performance, and the overall security of the QKD transmission with relay functionality.

As discussed in Chapter 4, the SDQTRF model does not interfere with the normal operation of SDN over the QKD network. It comes into play when the CTR nodes fail to relay the quantum secret keys. However, to determine the selected paths for the experiment, utilised a graph analysis method called NetworkX, which is a Python library designed for creating, manipulating, and studying complex network structures. It offers various tools for working with graph data structures and conducting graph algorithms and analyses. By leveraging NetworkX, identifying the shortest paths that best suited our objectives within the NSFNET and USNET network topologies was accomplished. For the NSFNET network topology, the selected paths were [1, 8, 11, 14] and [2, 4, 10, 12]. Similarly, for the USNET network topology, the selected paths were [1, 6, 9, 12, 16, 22, 23] and [4, 8, 10, 14, 18, 24]. These paths were chosen based on their properties and suitability for experimentation.

5.2.1 Simulation Performance of SDQTRF Model

The simulation performance of the SDQTRF model is presented in detail in Table 5-1. This table provides a comprehensive analysis and evaluation of the model's performance across various simulation scenarios and metrics.

Table 5-1 Average simulation result for the mechanism of the SDQTRF model in the NSFNET and USNET topologies over the whole simulation run

Simulation Run times till two successive failure occurs	Number of Successes Sending	Number of Failure	Topology Type	Average Time	Key Length
336	275	59	USNET	$2.17 * 10^{-5} \mu s$	128
306	296	8	NSFNET	$8.4 * 10^{-6} \mu s$	128
496	398	96	USNET	$7.4 * 10^{-5} \mu s$	192
400	371	27	NSFNET	$6.3 * 10^{-5} \mu s$	192
695	560	133	USNET	$5.4 * 10^{-4} \mu s$	256
238	217	19	NSFNET	$2.6 * 10^{-4} \mu s$	256

The primary aim of the SDQTRF model was to mitigate the adverse effects of CTR failure on the QKD network. Subsequently, an assessment and comparison of key metrics, namely key generation ratios, recovery post-failure, avalanche effect total failure, and service blocking rate, were conducted. This evaluation involved analyzing the performance of the QKD network both with and without the implementation of the SDQTRF model.

A- Key-Generation Ratio:

In the field of quantum cryptography, especially in QKD networks, the Key Generation Ratio (KGR) is a measure of the efficiency of a QKD system. It represents the ratio of the number of secure key bits generated to the number of transmitted bits over the quantum channel. In practice, the KGR can be influenced

by factors like noise, attenuation, and transmission errors, including those arising from CTR failure countermeasures. CTR failure can occur when an eavesdropper gains access to the classical channel between trusted nodes, posing a security risk to key generation. To assess CTR failure's impact on KGR, simulations introduce one failure per iteration, enabling controlled analysis of its effect on secure key generation. The KGR was evaluated in various scenarios, each with a different CTR failure situation, as represented by Equations (5.1) and (5.2), offering insights into how CTR failure affects system performance.

$$\text{without SDQTRF model} = n_i \times k_l \quad (5.1)$$

$$\text{with SDQTRF model} = \sum_{i=sn}^{n_i} Q_i \times k_l \quad (5.2)$$

Where n_i , k_l , and Q_i denote the index of the failed node in the topology, the key length, and the Q value, respectively. Without the SDQTRF model, when a CTR failure occurs, key generation proceeds from the source node to the node encountering the issue (the failed node). The extent of this process is contingent on the k_l . Conversely, when employing the SDQTRF model, the initial step involves receiving keys based on the Q-value. This implies that only a portion of the key is required, rather than the entirety. This model refines the key generation process in scenarios involving failures, optimizing resource utilization.

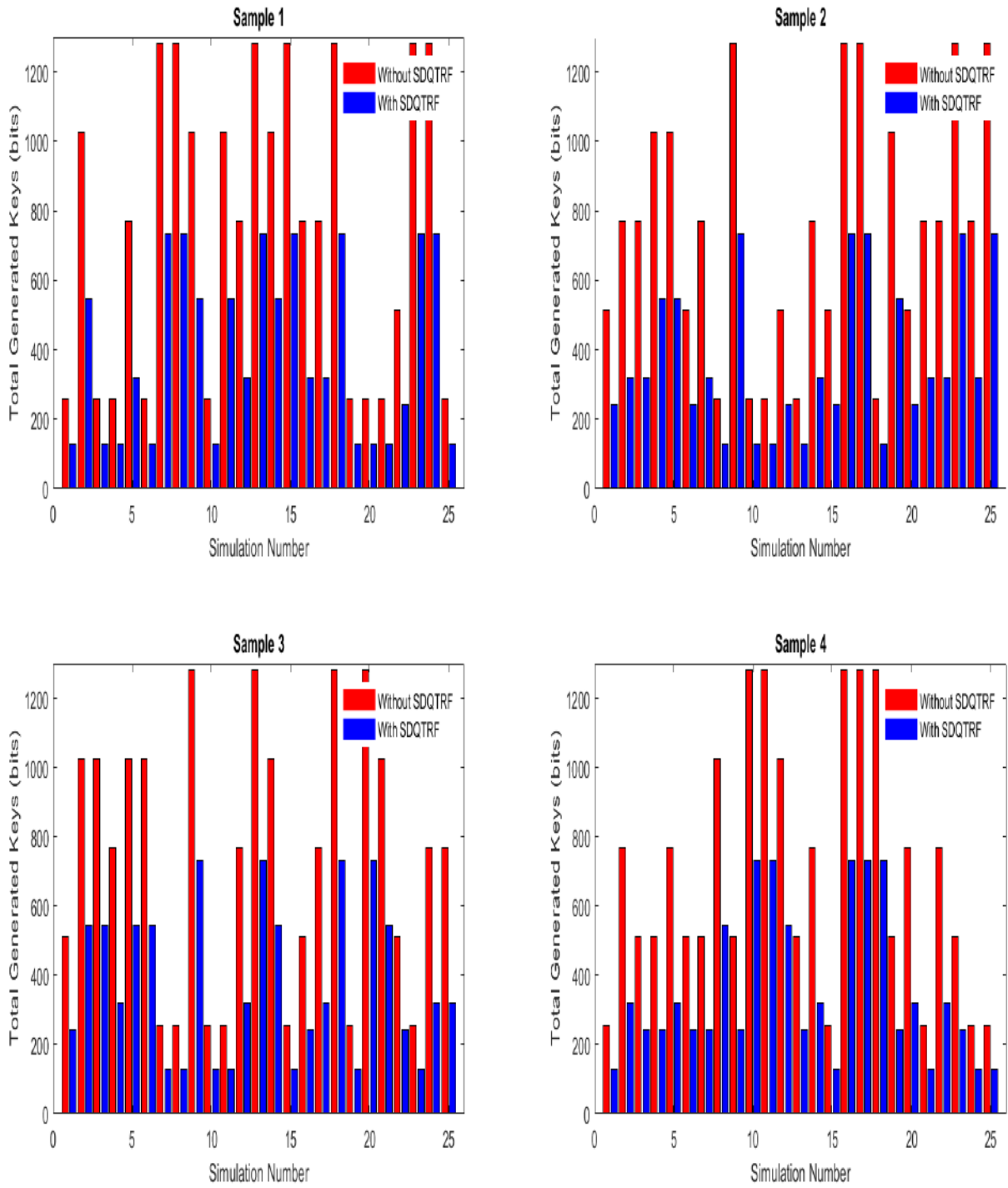


Fig. 5-3 KGR in NSFNET

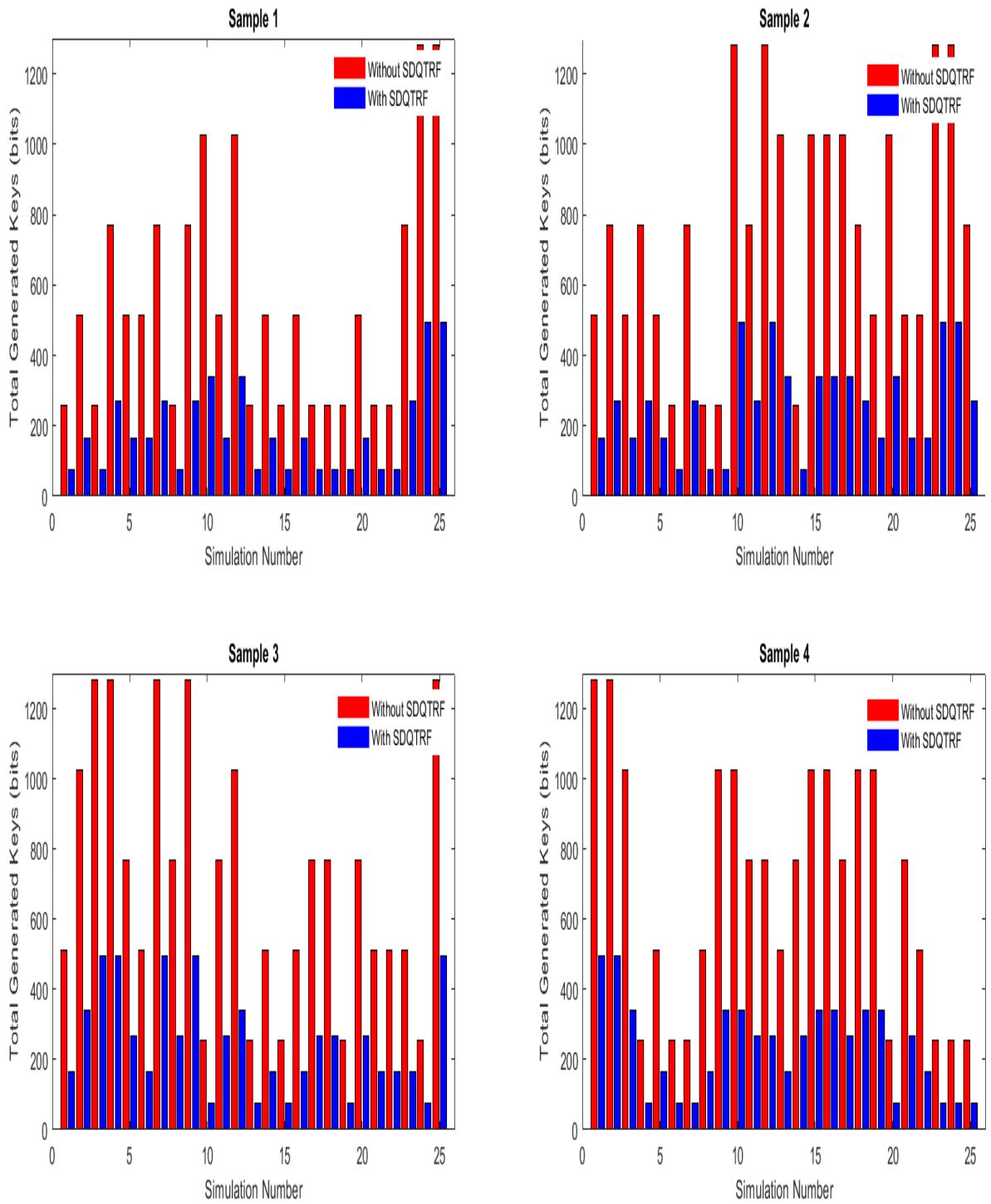


Fig. 5-4 KGR in USNET

To analyze the impact of CTR failure on the KGR, a comprehensive evaluation was conducted, depicted in Fig. 5-3 and Fig. 5-4. Conducted a total of 100 simulations, divided into four samples of 25 each. Each bar in the figures represents a unique scenario in which a single failure was observed. It is important to note that these scenarios are independent of each other, allowing us to examine the individual effects of CTR failure in isolation.

By closely examining Fig. 5-3 and Fig. 5-4, it becomes evident that the system operating without the use of SDQTRF model generates secret keys more frequently during the simulation compared to the system utilizing SDQTRF. This observation suggests that the presence of SDQTRF influences the overall efficiency of key generation in the system.

In the context of the NSFNET scenario, the implementation of the SDQTRF demonstrates a remarkable reduction in the negative impact of CTR failure compared to the system operating without SDQTRF. The recorded reduction percentages in four respective samples are 14.616%, 20.616%, 19.728%, and 18.496%. In contrast, the system without SDQTRF experiences significantly higher negative impacts, with failure rates of 43.2%, 59.2%, 56%, and 54.4% in the same samples. Upon analyzing these results, it becomes evident that the SDQTRF system provides a substantial advantage, reducing the negative impact by approximately three times when compared to the system operating without SDQTRF. The average improvement achieved with the SDQTRF system in the NSFNET scenario is approximately 34.836%.

Similarly, in the USNET scenario, the SDQTRF system effectively reduces the negative effects of CTR failure in four samples, resulting in decreased failure rates of 31.192%, 29.352%, 29.456%, and 27.928% respectively. Comparatively,

the corresponding samples without the SDQTRF system only see reductions of 59.2%, 58.4%, 57.6%, and 55.2%. This highlights that the system without the SDQTRF system had failure rates approximately twice as high as the system utilizing SDQTRF. The average improvement achieved with the SDQTRF system in the USNET scenario is approximately 28.118%.

Considering both scenarios collectively, the overall average improvement achieved with the SDQTRF system is approximately 31.477%. This indicates that the SDQTRF system consistently provides a substantial advantage in reducing the negative impact of CTR failure in various network scenarios, demonstrating its efficacy in mitigating critical transmission resource failures. These findings underline the importance and potential benefits of incorporating SDQTRF into network systems to enhance their reliability and stability, thereby leading to improved performance and reduced downtime.

B- Key Utilization Rate:

The Key Utilization Rate (KUR) serves as a vital role for evaluating the efficiency and effectiveness of a QKD network, particularly in situations where the CTR experiences failure. This rate offers valuable insights into the utilization of the cryptographic key within the network. By measuring the extent to which the key has been used out of the total key amount, the KUR provides a quantitative measure of the network's performance.

The KUR calculation involves comparing the amount of key material that has been utilized to the total quantity of key material generated or distributed within the QKD network. It essentially quantifies the extent to which the key material has been employed for secure communication purposes. This measurement is expressed as a ratio or percentage, representing the proportion of the key that has been utilized relative to the total key amount available.

A high KUR indicates that a significant portion of the key material has been effectively used, implying that the QKD network is successfully generating and employing secure cryptographic keys for communication. On the other hand, a low KUR suggests underutilization of the generated key material, which may indicate potential inefficiencies or limitations within the QKD network.

By monitoring the KUR, network administrators and security experts can gain valuable insights into the performance and reliability of the QKD network, even in the event of CTR failures. This information allows them to assess the network's overall operational effectiveness, identify areas for improvement, and implement necessary measures to enhance key utilization and network efficiency. Ultimately, striving for a high KUR contributes to the establishment of a robust and secure communication infrastructure based on quantum cryptographic principles. The KUR has been computed based on the equation sourced from Li et al. (2020).

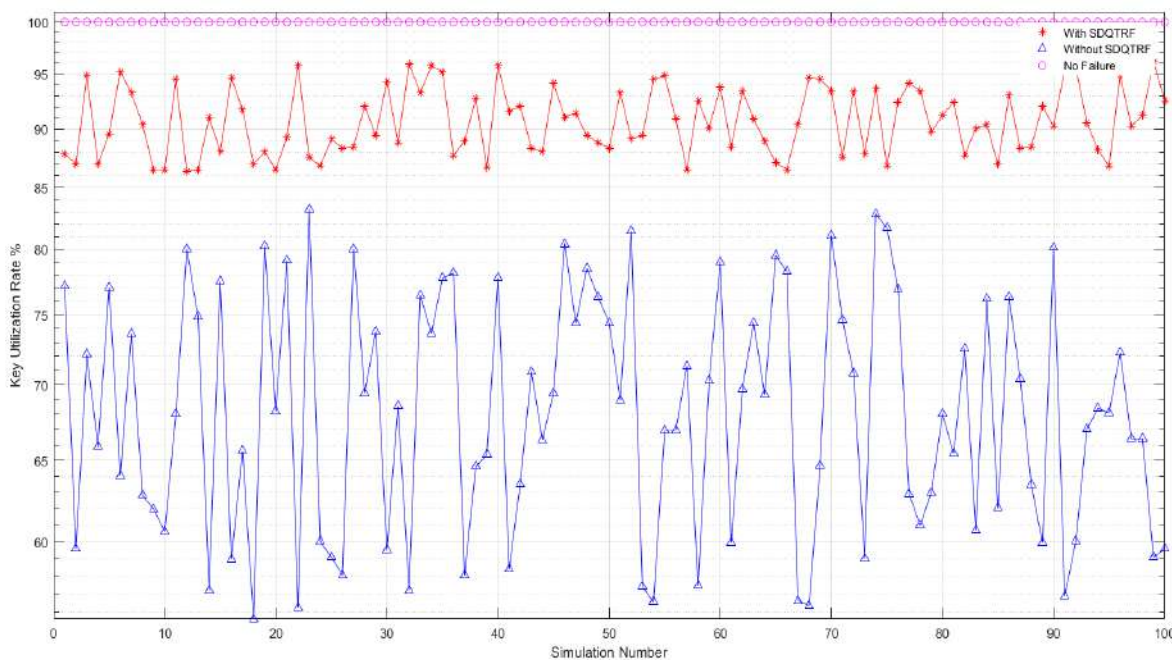


Fig. 5-5 KUR in NSFNET

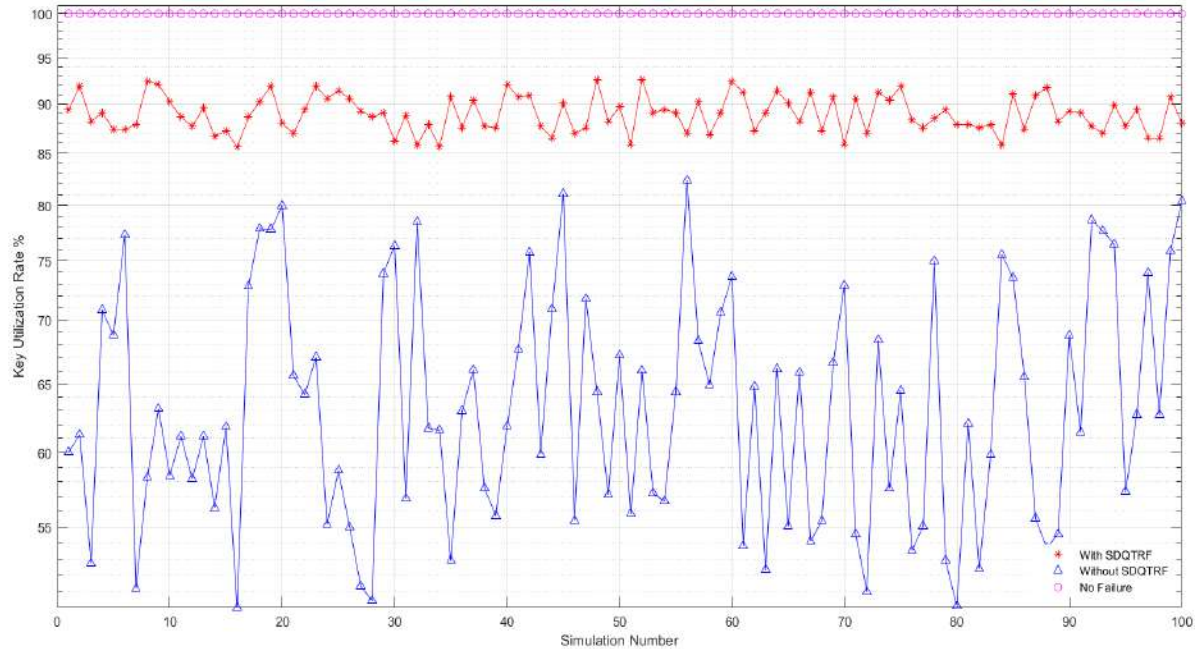


Fig. 5-6 KUR in USNET

The KUR trend remained unchanged at 100% in all simulation runs when there were no failures, as shown in Fig. 5-5 and Fig. 5-6. This indicates that the network resources were fully utilized without any disruptions. The consistent 100% KUR suggests a robust and efficient network performance under normal operating conditions.

In the context of the network scenarios, both NSFNET and USNET topologies experienced varying levels of performance in terms of KUR without the SDQTRF. The average KUR for the NSFNET topology was approximately 69%, slightly higher than the USNET topology, which had an average KUR of around 64%. These results indicate that the NSFNET topology, without the benefit of SDQTRF, faced a slightly higher average KUR, potentially suggesting a greater vulnerability to resource disruptions compared to USNET.

However, the implementation of SDQTRF in both the NSFNET and USNET topologies led to noticeable improvements in the average KUR performance. With

SDQTRF, the average KUR in the NSFNET topology reached approximately 91%, showcasing a substantial enhancement over the baseline performance. Similarly, the USNET topology with SDQTRF achieved an average KUR of around 89%, indicating significant improvement as well. These results demonstrate the pivotal role played by SDQTRF in enhancing KUR performance in both topologies.

The recorded average improvements with SDQTRF were approximately 22% for the NSFNET topology and 25% for the USNET topology, showcasing the positive impact of SDQTRF on both networks. This feature not only ensures a high level of resource utilization but also bolsters network stability by swiftly recovering from faults and disruptions. The findings underscore the importance of incorporating SDQTRF into network systems to boost their reliability and efficiency, leading to overall better performance and reduced downtime.

Considering both scenarios collectively, the overall average improvement in KUR achieved with the SDQTRF system is approximately 23.5%. This indicates that, on average, the SDQTRF system contributes to a 23.5% improvement in KUR performance across the NSFNET and USNET topologies. These consistent positive impacts validate the significance of SDQTRF in enhancing the stability and resource management of network systems, ultimately leading to more reliable and efficient network operations. As a result, SDQTRF emerges as a valuable tool for network administrators seeking to enhance network performance and mitigate the negative effects of CTR failures in their respective topologies.

C- Recovery After Failure:

Network Recovery After Failure (RAF) is an essential aspect that assesses the performance and resilience of QKD network in the face of CTR failures. It encompasses various key factors, such as the QKD network's behaviour and capabilities during CTR failure event, its ability to mitigate the impact of the failure,

and the efficiency with which it resumes normal operations once the failure has been resolved.

During a failure, the network's action at the moment of occurrence is of utmost importance. This refers to how the network responds, adapts, and recovers from the failure. It involves activities such as rerouting traffic, activating backup systems or redundant components, and implementing alternative communication paths to ensure continuity and minimize service disruptions.

Additionally, the time taken by the network to recover and resume sending data after a failure is an essential metric in assessing RAF. This recovery time encompasses the period from the identification and resolution of the failure to the network's ability to resume its normal functioning. A prompt and efficient recovery time indicates the network's resilience and its ability to swiftly recover from unforeseen events, reducing the impact on users or services.

Efficient RAF not only focuses on the recovery process but also considers the network's performance during the recovery phase. It evaluates how well the network handles the transition from the failure state to normal operation. This includes ensuring that data packets are delivered without loss, maintaining quality of service, and preventing congestion or bottlenecks during the recovery process.

By evaluating RAF, network administrators and operators can gain insights into the network's reliability and its ability to provide uninterrupted services in the face of failures.

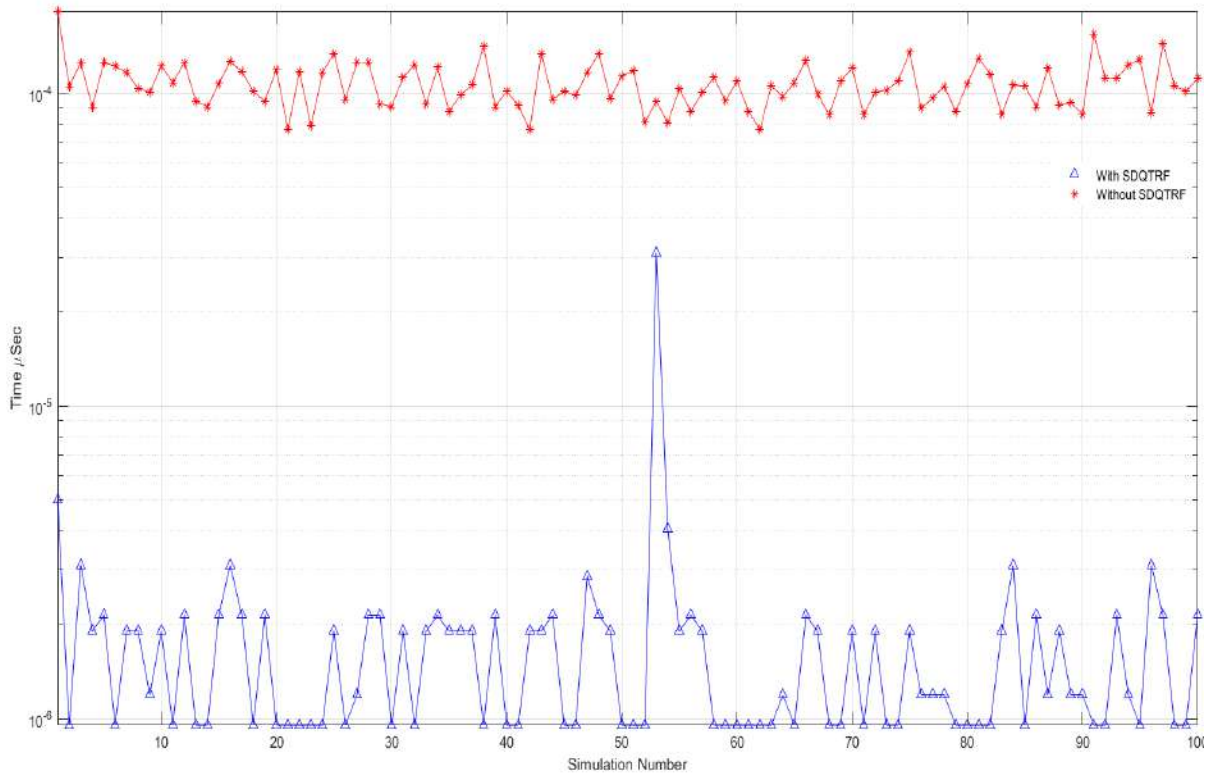


Fig. 5-7 Time elapsed of RAF in NSFNET

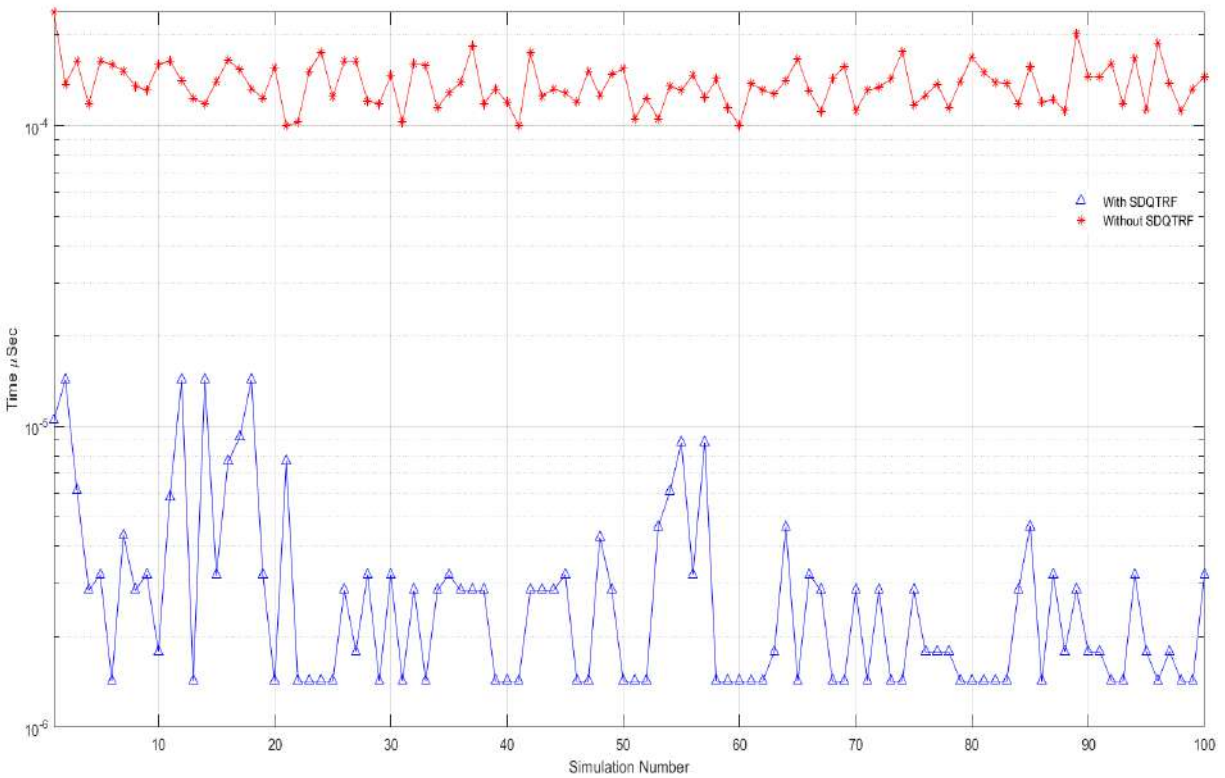


Fig. 5-8 Time elapsed of RAF in USNET

The significant time difference between the RAF process with and without SDQTRF highlights the effectiveness of SDQTRF in improving network recovery and data transmission. The utilization of SDQTRF enables a more efficient and rapid resumption of operations after a disruption or failure within the network. In Fig. 5-7 and Fig. 5-8, it is evident that the RAF process without SDQTRF experiences considerably longer delays. This delay can be attributed to the additional time required for the system to recover and resume data transmission without the aid of SDQTRF. On the other hand, when SDQTRF is employed, the network demonstrates enhanced resilience, swiftly recovering from disruptions and promptly resuming its data sending operations.

In the context of both the NSFNET and USNET scenarios, the average RAF time without the implementation of SDQTRF is recorded as approximately 1×10^{-4} μs in the NSFNET and just above 1×10^{-4} μs in the USNET. These figures indicate that a considerable time overhead is incurred in the absence of SDQTRF, potentially leading to slower network recovery after failures.

However, with the integration of SDQTRF, there is a noticeable improvement in the average RAF times in both scenarios. In the NSFNET topology, the average RAF time with SDQTRF is approximately 1.5×10^{-6} μs , showcasing a remarkable enhancement compared to the systems without SDQTRF. Similarly, in the USNET topology, the average RAF time with SDQTRF is around 2.5×10^{-6} μs , further highlighting the efficiency of SDQTRF in accelerating network recovery.

The recorded average improvements with SDQTRF were approximately 9.85×10^{-5} μs for the NSFNET and 9.75×10^{-5} μs for the USNET. These results demonstrate the pivotal role played by SDQTRF in significantly reducing the average RAF time in both network scenarios. The average RAF times with SDQTRF

are remarkably lower compared to those without it, indicating that SDQTRF efficiently accelerates network recovery after failures. The findings underscore the importance of incorporating SDQTRF into network systems to reduce time overhead and enhance network resilience, ultimately leading to improved network performance and reliability.

Considering both scenarios collectively, the overall average improvement in RAF time achieved with the SDQTRF system is approximately 9.8×10^{-5} μ s. This indicates that, on average, the SDQTRF system contributes to a significant reduction in network recovery time across the NSFNET and USNET topologies. The reduced RAF time emphasizes the effectiveness of SDQTRF in swiftly recovering from network failures and disruptions, underscoring its importance in enhancing the stability and resource management of network systems. As a result, SDQTRF emerges as a valuable tool for network administrators seeking to improve network performance and mitigate the negative effects of CTR failures in their respective topologies.

D- Avalanche-Effect-Total-Failure:

The Avalanche Effect Total Failure (AETF) is a fundamental requirement for all cryptographic algorithms. It plays a fundamental role in ensuring the security and strength of these algorithms. The term "avalanche" metaphorically captures the idea that even a slight change in the input, such as a single bit alteration in the secret key, can lead to a cascade of significant changes throughout the entire encryption process. This property makes cryptographic systems more resistant to attacks and enhances their ability to conceal sensitive information.

In this dissertation, the focus was on exploring the impact of the avalanche effect by employing the AETF. Specifically, the aim was to compare the avalanche quantity of the secret key under two scenarios: with and without the SDQTRF

model, particularly in the event of a CTR failure. By analysing the extent of the avalanche effect, insights were sought into the effectiveness of the SDQTRF model in mitigating and managing the avalanche phenomenon.

Interestingly, rather than directly resolving the avalanche effect, the choice was made to utilize the SDQTRF model. The SDQTRF model was implemented to minimize the adverse effects of avalanches on the secret key after failures occur. This approach offered an alternative strategy to dealing with the avalanche effect, aiming to maintain the integrity of the key while reducing the risk of key destruction. Without incorporating the SDQTRF model, the occurrence of a failure, such as a CTR failure, would result in the destruction of the key, rendering it unusable. Consequently, a new key would need to be generated, leading to a high avalanche effect. The destruction and regeneration of the key pose significant security concerns, as it increases the potential for unauthorized access and compromises the confidentiality and integrity of the encrypted data.

By introducing the SDQTRF model, the aim was to address these concerns and maintain the stability of the encryption system. The SDQTRF model provides a mechanism to recover and restore the key's integrity after a failure, minimizing the need for complete key regeneration. This proactive approach not only reduces the impact of avalanches on the key but also improves the overall efficiency and performance of the cryptographic algorithm.

Through research, the role of the SDQTRF and SDQTRF models in managing the avalanche effect during failures, such as CTR failures, has been explored. By employing these models, the goal is to strike a balance between ensuring the robustness of the encryption system and minimizing the disruptions caused by the avalanche effect. The findings contribute to the advancement of cryptographic

techniques and offer potential solutions to enhance the security and resilience of encrypted data transmission and storage. The AETF has been computed based on the equation sourced from (Raghunandan et al., 2020).

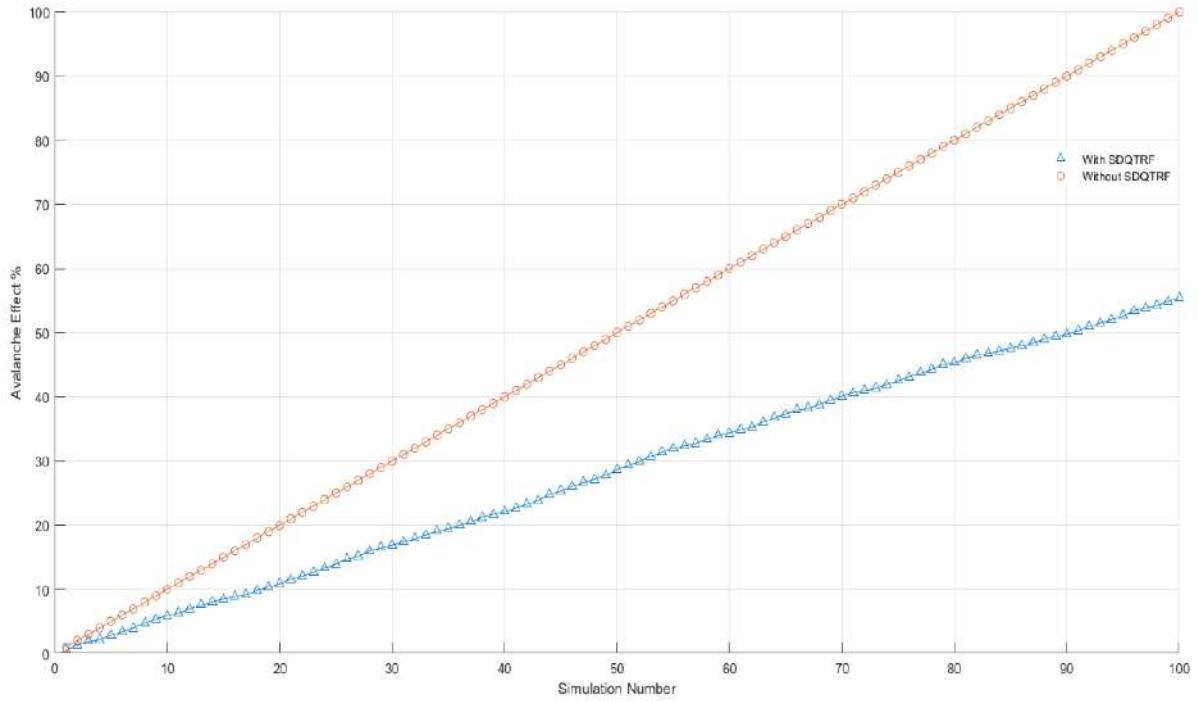


Fig. 5-9 AETF in NSFNET

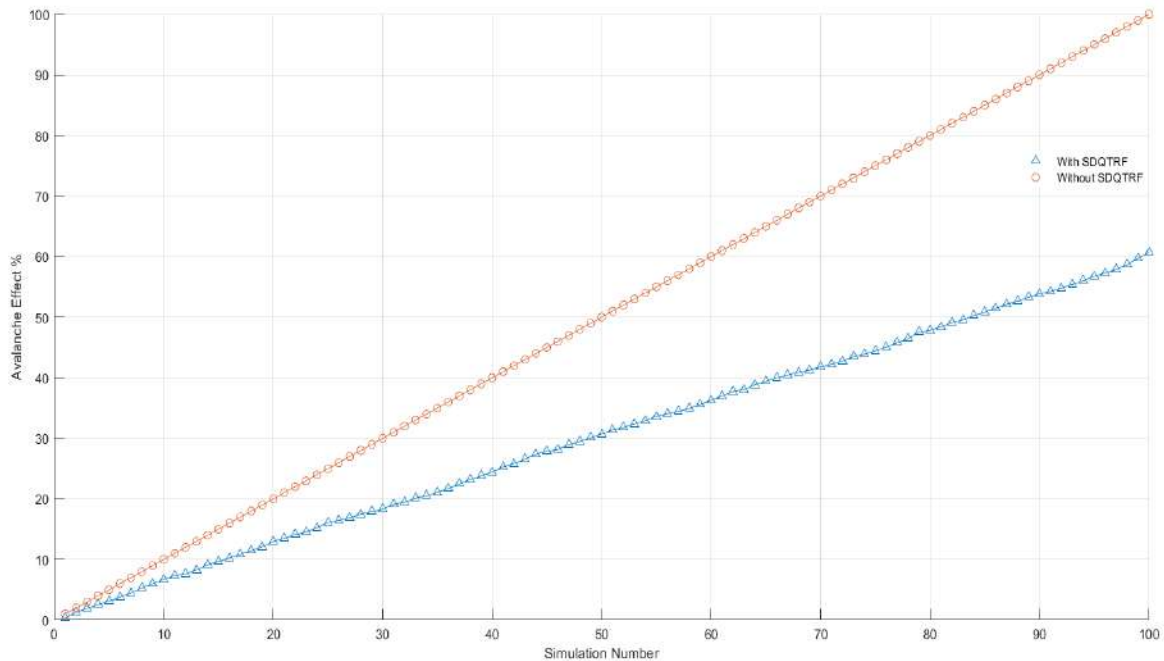


Fig. 5-10 AETF in USNET

In both the NSFNET and USNET topologies, the incorporation of the SDQTRF model plays a crucial role in mitigating the negative effects of avalanches on network key resources. As the simulation progressed, it was observed that the proportion of the key affected by avalanches gradually increased, eventually reaching nearly 100% in scenarios where SDQTRF was not utilized. This indicates that without the SDQTRF model, the network experienced cascading failures, causing a significant impact on key resources.

In both NSFNET and USNET topologies, when examining the incorporation of the SDQTRF model, as depicted in Fig. 5-9 and Fig. 5-10, the initial simulation results indicated that about 0% of the key experienced avalanches in both (with and without SDQTRF). However, as the simulation progressed, the proportion of the key affected by avalanches gradually increased, eventually reaching nearly 100% without utilizing the SDQTRF model. On the other hand, when the SDQTRF model

was employed, the percentage steadily rose from 55% in NSFNET to 60% in USNET.

The recorded average improvements in the proportion of the key affected by avalanches were approximately 45% for the NSFNET and 40% for the USNET. These results demonstrate that the SDQTRF model significantly reduces the proportion of the key affected by avalanches in both scenarios. The average improvements emphasize the effectiveness of SDQTRF in enhancing network stability and resilience, leading to improved network performance and reduced vulnerability to cascading failures.

Considering both scenarios collectively, the overall average improvement achieved with the SDQTRF model is approximately 42.5%. This indicates that, on average, the SDQTRF model contributes to a significant reduction in the proportion of the key affected by avalanches across the NSFNET and USNET topologies. The reduced impact of avalanches underscores the importance of incorporating SDQTRF as a valuable tool for network administrators seeking to enhance network reliability and mitigate the negative effects of avalanches in their respective topologies. The findings highlight the positive impact of SDQTRF in ensuring network stability and improving overall network performance, making it an essential component in enhancing the resilience of modern network systems.

E- Service-Blocking Rate:

For evaluating the performance of the QKD service, the employed performance criterion is called the success probability of QKD service requests. This criterion serves as a measure of efficiency by calculating the ratio of the total accepted QKD service requests to the overall incoming QKD service requests. By

analyzing this ratio, insights are gained into the effectiveness of the QKD system in successfully accommodating the service demands.

In addition to the success probability, another significant metric that contributes to the evaluation is the blocking probability. The success probability can be determined by the blocking probability because the sum of the success and blocking probabilities is equal to one (Parkinson, 2002). The blocking probability represents the proportion of QKD service requests that are denied or blocked due to specific reasons. In our case, there are two primary reasons for blocking: failure in secret key rate assignment or failure in secret key rate reassignment. These failures can be identified during the creation or modification of QKD services, allowing us to pinpoint areas where improvements are necessary.

To simulate the performance of the QKD service, a loss system known as the Engest system (Parkinson, 2002) was utilized. It is important to note that this loss system typically operates without queuing, meaning that incoming requests are either accepted or blocked immediately based on the availability of resources and the system's capacity. By examining the arrival and departure rates of QKD service requests within this loss system, one can determine the traffic load. The traffic load is calculated by dividing the arrival rate of QKD service requests by the departure rate, providing us with a valuable indicator of the workload and resource utilization within the QKD system.

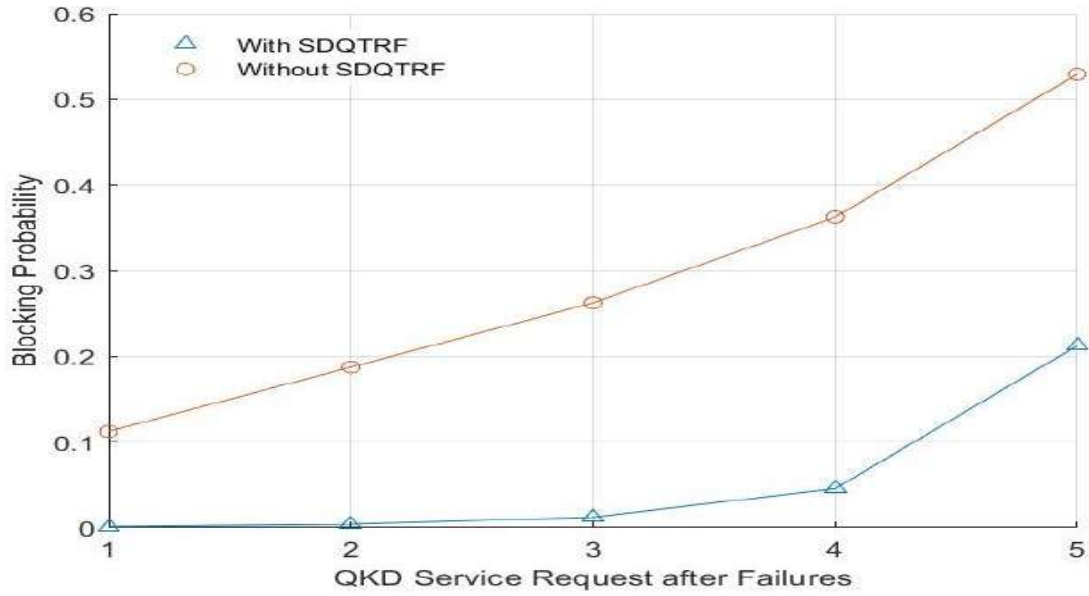


Fig. 5-11 The Service-Blocking Rate (SBR) in NSFNET

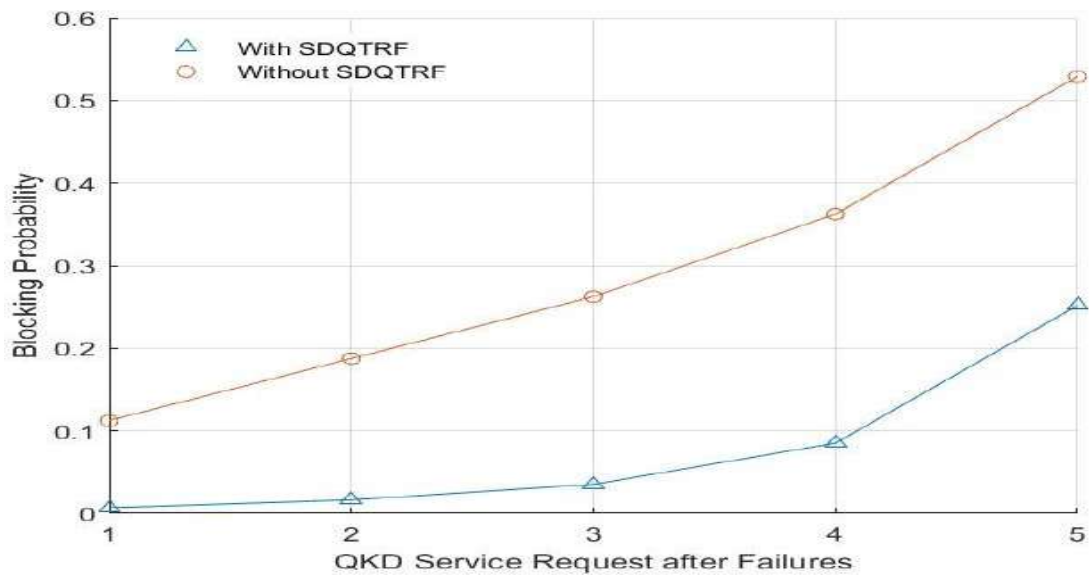


Fig. 5-12 The Service-Blocking Rate (SBR) in USNET

Upon examining the graphical representations provided in Fig. 5-11 and Fig. 5-12, a notable distinction emerges when considering the influence of SDQTRF on the SBR. The SBR, which indicates the proportion of service requests that are unable

to be accommodated by the system, exhibits significant variations based on the utilization of SDQTRF.

In the context of a single failure, the SBR remains relatively low regardless of the presence of SDQTRF. This suggests that the system possesses the capability to swiftly rectify issues that arise after an isolated failure event. However, as multiple failures occur consecutively, the SBR gradually increases, implying that the system's ability to handle service requests diminishes. This can be attributed to the cumulative effect of failures, which strain the system's resources and impede its capacity to effectively address subsequent requests. Consequently, the likelihood of service requests being blocked rises, resulting in a higher SBR.

Analyzing Fig. 5-11 and Fig. 5-12, it is evident that the systems operating without the SDQTRF model exhibit a distinct trend in their SBR values. These systems commence with an initial SBR slightly above 0.1, indicating a relatively small proportion of blocked service requests. However, as failures accumulate, the SBR steadily climbs and surpasses 0.5 towards the end of the observed period. This escalating trend underscores the system's decreasing efficacy in meeting service demands as failures persist.

Conversely, the introduction of the SDQTRF model in the NSFNET topology yields a different outcome. During the first two failure events, the SBR remains unchanged, effectively staying at zero. This implies that the SDQTRF model successfully mitigates the impact of these initial failures, allowing the system to continue operating without any blocked service requests. However, as subsequent failures occur, the SBR gradually rises, reaching slightly above 0.2 by the final failure. This signifies a noteworthy improvement compared to the without SDQTRF systems, suggesting that the routing framework contributes to the system's resilience

and its ability to cope with failures, ultimately leading to reduced blocked service requests.

Similarly, a comparison can be drawn with the USNET topology, where the SBR follows a distinct trajectory. With the implementation of SDQTRF, the SBR begins at zero and progressively climbs throughout the observed period, ultimately reaching approximately 0.26 by the end. This upward trend highlights the system's diminishing performance as failures accumulate, leading to a significant proportion of service requests being blocked.

Considering both scenarios collectively, the average improvement achieved with the SDQTRF model is approximately 0.27. This indicates that, on average, the SDQTRF model contributes to a significant reduction in the Service Blocking Ratio across the NSFNET and USNET topologies. The reduced SBR underscores the effectiveness of SDQTRF in enhancing the resilience and performance of network systems, ultimately leading to improved service delivery and availability. These findings highlight the importance of incorporating SDQTRF as a valuable tool for network administrators seeking to enhance network reliability and mitigate the negative impact of service blocking in their respective topologies. The consistent positive impact of SDQTRF in reducing SBR further emphasizes its significance in improving the overall efficiency and quality of network services. As a result, SDQTRF emerges as a critical component in enhancing the overall resilience and responsiveness of network systems, making it an essential framework in modern network management.

5.3 Q-learning Results

As mention in the previous chapter, the utilization of the Q-learning method in the proposed model serves two crucial goals. Firstly, it aims to determine the optimal amount of recycling for the secret quantum keys by leveraging the Q-value

associated with the selected path. The Q-value represents the expected reward or utility of choosing a particular action (in this case, recycling a certain amount of quantum keys) in a given state (corresponding to a specific path). By compute the Q-value for each possible action-state pair, the Q-learning algorithm enables the model to make informed decisions regarding the amount of recycling required to maximize key utilization while ensuring security. Secondly, the Q-learning method is applied to discover alternative secure paths in the network. After identifying the unsecure nodes through an initial analysis, the model employs Q learning to search for alternative routes that avoid these vulnerable points. The Q-values associated with different paths are calculated based on their potential to provide a secure communication channel. By iteratively updating and refining these Q-values through the learning process, the proposed model becomes adept at identifying the most secure and reliable paths for QKD network.

By integrating the Q-learning method into the proposed model, it becomes possible to address the key challenges of recycling quantum keys and identifying secure paths effectively. The extended explanation emphasizes the significance of the Q-learning approach in achieving the desired objectives of the research, setting the stage for the subsequent discussion of the process results.

5.3.1 Q-Learning Results for Recycling Process

The provided implementation represents a series of procedures aimed at improving the recycling method of quantum secret keys by obtaining Q-values using the Q-learning algorithm. Here is an explanation of how these procedures work:

The procedures begin by initializing the necessary variables and libraries required for the task. Next, the initialization step involves creating and populating the R-matrix. This matrix captures the rewards associated with different state-action

pairs in the selected topology. The goal state and available paths are taken into account when assigning rewards.

Following the R-matrix initialization, the procedures create an empty Q-matrix, which will store the expected future rewards for each state-action pair. This Q-matrix plays a crucial role in guiding the recycling process.

Several helper procedures are defined to facilitate the training and improvement process. These procedures assist in selecting the next action to take based on the available actions in a given state and updating the Q-matrix according to the observed rewards and future expected rewards.

The training phase starts by initializing the current state, followed by a loop that repeats a specified number of iterations based on the selected method. Within each iteration, a random current state is selected, and the available actions in that state are determined. An action is then chosen, and the Q-matrix is updated accordingly based on the current state and the selected action.

Throughout the training process, the procedures keep track of the scores obtained after each iteration. These scores reflect the cumulative rewards obtained during the training and serve as an indication of the improvement in the recycling method.

Once the training phase is completed, the procedures generate a plot displaying the scores obtained during the number of training iterations. This plot provides a visual representation of the progress made in enhancing the recycling method of quantum secret keys.

Finally, the procedures employ the trained Q-matrix. Starting from an initial state, the procedures iteratively select the action associated with the highest Q-value

in each state. This process continues until the goal state is reached, and the sequence of states taken to reach the goal is recorded.

Table 5-2 Q-table for NSFNET and USNET

<p><i>Type of topology</i></p>	<p>NSFNET Network Topology: Sending Process from Node 1 to 14</p>	<p>([[0., 51.2, 40.96, 0., 0., 0., 0., 64., 0., 0., 0., 0., 0., 0.], [51.2, 0., 40.44125638, 64., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0.], [51.2, 51.2, 0., 0., 0., 50.55157047, 0., 0., 0., 0., 0., 0., 0., 0.], [0., 51.2, 0., 0., 51.2, 0., 0., 0., 80., 0., 0., 0., 0., 0.], [0., 0., 0., 64., 0., 50.55157047, 51.2, 0., 0., 0., 0., 0., 0., 0.], [0., 0., 40.96, 0., 51.2, 0., 0., 0., 63.18946309, 0., 0., 0., 0., 0.], [0., 0., 0., 0., 51.2, 0., 0., 64., 64., 0., 0., 0., 0., 0.], [51.2, 0., 0., 0., 0., 0., 51.2, 0., 0., 0., 80., 0., 0., 0.], [0., 0., 0., 0., 0., 50.55157047, 51.2, 0., 0., 0., 80., 0., 0., 0.], [0., 0., 0., 64., 0., 0., 0., 0., 0., 0., 62.17629195, 0., 100.], [0., 0., 0., 0., 0., 0., 0., 64., 63.18946309, 0., 0., 64., 0., 100.], [0., 0., 0., 0., 0., 0., 0., 0., 80., 80., 0., 80., 0., 0.], [0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 64., 0., 100.], [0., 0., 0., 0., 0., 0., 0., 0., 80., 80., 0., 80., 98.73353608]])</p>
<p><i>Type of topology</i></p>	<p>NSFNET Network Topology: Sending Process from Node 2 to 12</p>	<p>([[0., 50.72135271, 40.57708217, 0., 0., 0., 0., 63.40169089, 0., 0., 0., 0., 0., 0.], [50.72135271, 0., 40.57708217, 63.40169089, 0., 0., 0., 0., 0., 0., 0., 0., 0., 0.], [50.72135271, 50.72135271, 0., 0., 0., 50.72135271, 0., 0., 0., 0., 0., 0., 0., 0.], [0., 50.72135271, 0., 0., 50.72135271, 0., 0., 0., 79.25211361, 0., 0., 0., 0., 0.], [0., 0., 0., 63.40169089, 0., 50.72135271, 50.72135271, 0., 0., 0., 0., 0., 0., 0.], [0., 0., 40.57708217, 0., 50.72135271, 0., 0., 0., 63.40169089, 0., 0., 0., 0., 0.], [0., 0., 0., 0., 49.37515721, 0., 0., 63.40169089, 63.40169089, 0., 0., 0., 0., 0.], [50.72135271, 0., 0., 0., 0., 50.72135271, 0., 0., 0., 79.25211361, 0., 0., 0., 0.], [0., 0., 0., 0., 0., 50.72135271, 50.72135271, 0., 0., 0., 79.25211361, 0., 0., 0.], [0., 0., 0., 63.40169089, 0., 0., 0., 0., 0., 0., 100., 0., 63.40169089], [0., 0., 0., 0., 0., 0., 0., 63.40169089, 63.40169089, 0., 0., 99.06514202, 0., 63.40169089], [0., 0., 0., 0., 0., 0., 0., 0., 79.25211361, 79.25211361, 99.06514202, 79.25211361, 0.], [0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 99.06514202, 0., 63.40169089], [0., 0., 0., 0., 0., 0., 0., 0., 79.25211361, 79.25211361, 0., 79.25211361, 0.]]</p>
<p><i>Type of topology</i></p>	<p>USNET Network Topology: Sending Process from Node 1 to 23</p>	<p>[[0., 25.85885287, 0., 0., 0., 32.56154236, 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0.], [25.85885287, 0., 25.85885287, 0., 0., 32.32356609, 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0.], [0., 25.85885287, 0., 32.32356609, 26.04923389, 0., 32.32356609, 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0.], [0., 0., 25.85885287, 0., 25.85885287, 0., 0., 40.40445761, 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0.], [0., 0., 25.85885287, 32.32356609, 0., 0., 32.56154236, 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0.], [0., 0.]]</p>

<i>Type of topology</i>	<p>[25.85885287, 25.85885287, 0., 0., 0., 0., 32.32356609, 0., 40.70192795, 0., 40.70192795, 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0.]</p> <p>[0., 0., 25.85885287, 0., 26.04923389, 32.56154236, 0., 40.40445761, 40.70192795, 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0.]</p> <p>[0., 0., 32.32356609, 0., 0., 32.56154236, 0., 0., 50.50557202, 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0.]</p> <p>[0., 0., 0., 0., 32.56154236, 32.32356609, 0., 0., 50.50557202, 40.70192795, 50.87740994, 0., 0., 0., 0., 0., 0., 0., 0.]</p> <p>[0., 0., 0., 0., 0., 0., 40.40445761, 40.70192795, 0., 0., 0., 63.13196502, 50.87740994, 0., 0., 0., 0., 0., 0., 0.]</p> <p>[0., 0., 0., 0., 30.96726144, 0., 0., 40.70192795, 0., 0., 50.87740994, 0., 0., 50.50557202, 0., 0., 0., 40.40445761, 0., 0., 0., 0.]</p> <p>[0., 0., 0., 0., 0., 0., 38.7090768, 0., 38.7090768, 0., 63.13196502, 0., 63.59676243, 0., 0., 0., 0., 0., 0.]</p> <p>[0., 0., 0., 0., 0., 0., 50.50557202, 0., 50.87740994, 0., 50.87740994, 0., 80., 0., 0., 0., 0., 0., 0.]</p> <p>[0., 0., 0., 0., 0., 0., 50.50557202, 0., 63.13196502, 0., 0., 63.59676243, 0., 0., 0., 0., 0., 0.]</p> <p>[0., 0., 0., 0., 0., 0., 40.70192795, 0., 0., 63.13196502, 0., 0., 51.2, 0., 0., 0.]</p> <p>[0., 0., 0., 0., 0., 0., 50.87740994, 0., 50.50557202, 0., 79.49595304, 0., 63.59676243, 79.49595304, 0., 0.]</p> <p>[0., 0., 0., 0., 0., 0., 63.13196502, 0., 63.59676243, 0., 63.59676243, 0., 79.49595304, 100., 0.]</p> <p>[0., 0., 0., 0., 0., 0., 50.87740994, 0., 79.49595304, 0., 0., 0., 79.49595304]</p> <p>[0., 0., 0., 0., 0., 0., 40.70192795, 0., 0., 0., 0., 50.87740994, 0., 0., 0., 0.]</p> <p>[0., 0., 0., 0., 0., 0., 50.50557202, 0., 0., 40.40445761, 0., 64., 0., 0., 0.]</p> <p>[0., 0., 0., 0., 0., 0., 63.59676243, 0., 50.87740994, 0., 80., 0., 0.]</p> <p>[0., 0., 0., 0., 0., 0., 63.59676243, 79.49595304, 0., 64., 0., 100., 0.]</p> <p>[0., 0., 0., 0., 0., 0., 80., 0., 79.49595304, 99.8347387, 80.]</p> <p>[0., 0., 0., 0., 0., 0., 63.59676243, 0., 0., 100., 0.]</p>
<i>Type of topology</i>	<p>[[[0., 26.14761074, 0., 0., 32.68451342, 0.]],</p> <p>[26.14761074, 0., 26.01716297, 0., 32.68451342, 0.]],</p> <p>[0., 25.26476339, 0., 32.52145371, 26.01716297, 0., 32.52145371, 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0.]],</p> <p>[0., 26.01716297, 0., 26.01716297, 0., 40.65181713, 0.]],</p> <p>[0., 26.01716297, 32.52145371, 0., 32.52145371, 0.]],</p> <p>[26.14761074, 25.6318592, 0., 0., 32.039824, 0., 40.85564178, 0., 32.68451342, 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0.]],</p> <p>[0., 26.01716297, 0., 26.01716297, 32.68451342, 0., 40.65181713, 40.04978, 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0.]],</p> <p>[0., 0., 32.52145371, 0., 32.52145371, 0., 50.81477142, 0.]],</p>

```

[0.,0.,0.,0.,0.,32.68451342,32.52145371,0.,0.,51.06955223,32.68451342,40.85564178,0.,
0.,0.,0.,0.,0.,0.,0.,0.,0.,0.,0.],
[0.,0.,0.,0.,0.,0.,0.,40.65181713,40.85564178,0.,0.,0.,50.81477142,63.83694028,0.,0.,0.,0.,
0.,0.,0.,0.,0.],
[0.,0.,0.,0.,0.,32.68451342,0.,0.,40.85564178,0.,0.,40.04978,0.,0.,40.85564178,0.,0.,0.,32.
52145371,0.,0.,0.,0.,0.]
[0., 0., 0., 0., 0., 0., 0., 0., 40.85564178, 0., 32.68451342, 0., 51.06955223, 0., 0.,
51.06955223, 0., 0., 0., 0., 0., 0., 0.],
[0., 0., 0., 0., 0., 0., 0., 0., 51.06955223, 0., 40.65181713, 0., 63.83694028, 0., 0.,
63.83694028, 0., 0., 0., 0., 0., 0., 0.],
[0., 0., 0., 0., 0., 0., 0., 0., 50.81477142, 0., 0., 51.06955223, 0., 0., 0., 0., 79.79617535,
0., 0., 0., 0., 0., 0.],
[0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 32.68451342, 0., 0., 0., 51.06955223, 0., 0., 0.,
40.65181713, 0., 0., 0., 0.],
[0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 40.65181713, 0., 0., 40.85564178, 0., 63.83694028, 0.,
0., 0., 50.81477142, 63.51846427, 0., 0.],
[0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 51.06955223, 0., 0., 51.06955223, 0., 79.79617535,
0., 0., 0., 63.51846427, 79.39808034, 0.],
[0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 63.83694028, 0., 0., 63.83694028, 0., 0., 0., 0.,
0., 0., 99.93317225],
[0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 32.68451342, 0., 0., 0., 0., 0., 0., 0., 40.65181713, 0.,
0., 0., 0.],
[0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 40.85564178, 0., 0., 0., 32.52145371, 0.,
50.81477142, 0., 0., 0.],
[0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 51.06955223, 0., 0., 0., 40.65181713, 0.,
63.51846427, 0., 0.],
[0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 51.06955223, 63.51846427, 0., 0., 0.,
50.81477142, 0., 79.39808034, 0.],
[0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 63.83694028, 0., 0., 0., 0., 0., 63.51846427, 0.,
100.],
[0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 0., 79.39808034, 0., 0., 0., 0.,
79.9465378, 99.93317225]

```

In Table 5-2, all the values are expressed in percentage format. To illustrate, let's examine the first route within the NSFNET network topology, where the selected nodes are [1, 8, 11, 14]. Referring to the Q-table, the initial one-dimensional array [0., 51.2, 40.96, 0., 0., 0., 0., 64., 0., 0., 0., 0., 0.] represents the first node (source node) along with its connections. A value of zero indicates no connection. Following the Q-learning principle, the highest Q-value is selected, which in this case is 64, corresponding to node number 8. Therefore, if we consider the highest

Q-values along the path, we have: from node 1 to node 8, the value is 64%; from node 8 to node 11, the value is 80%; and from node 11 to node 14, the value is 100%. To provide further clarity, when moving from node 1 to node 8, the recycling rate is 64% of the key length. To provide further clarity, it's important to note that the table indexes nodes from [0], while the figure of NSFNET network topology in Fig. 5-1 starts indexing from [1].

The training and testing function in iteration process it was differ based on the selected topology. However, the following figures are going to explain the number of iterations.

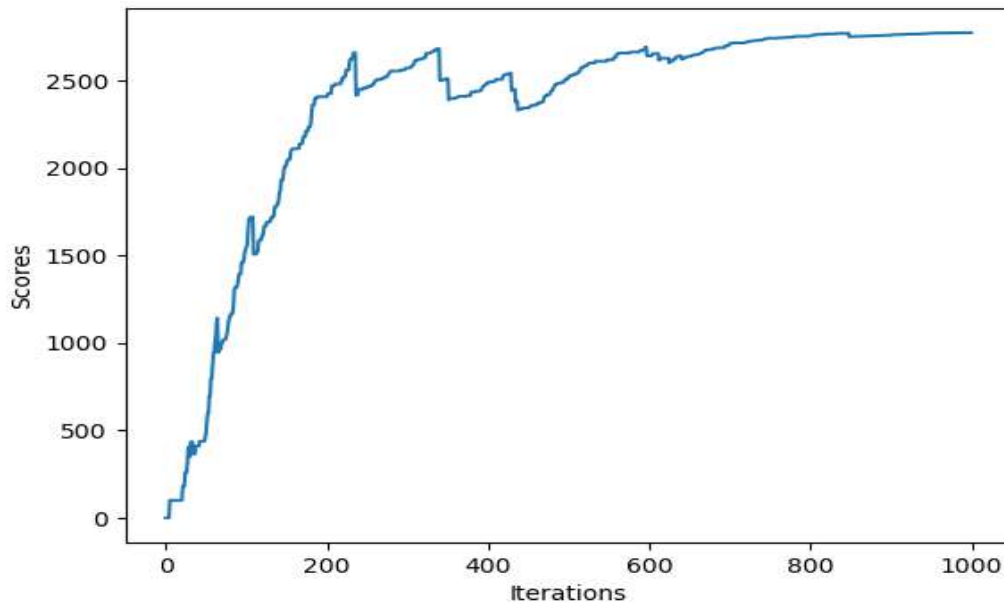


Fig. 5-13 Learning progression for the path [1, 8, 11, 14] of NSFNET

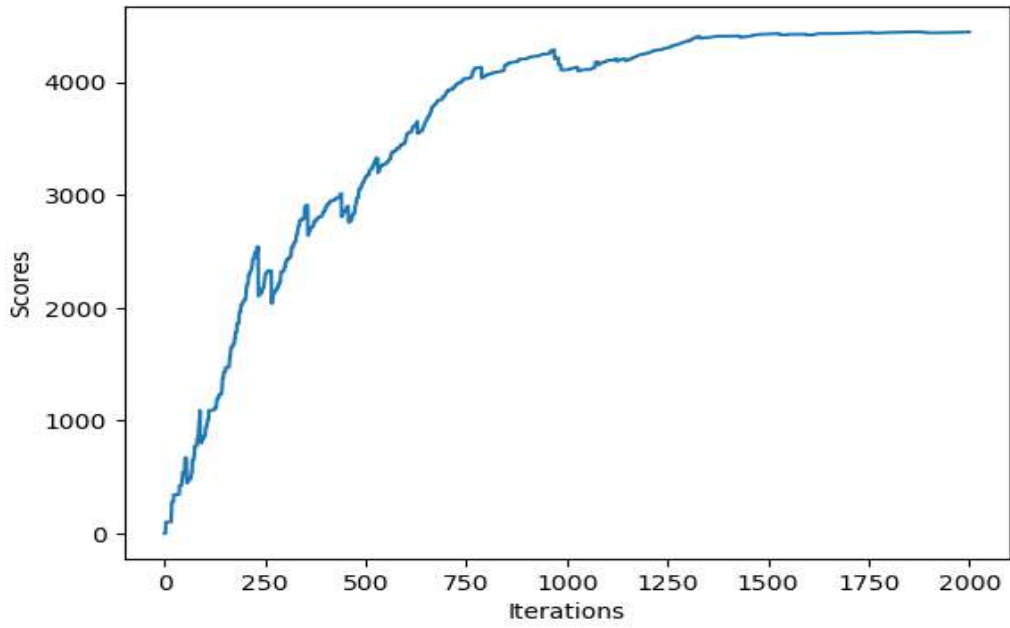


Fig. 5-14 Learning progression for the path [2, 4, 10, 12] of NSFNET

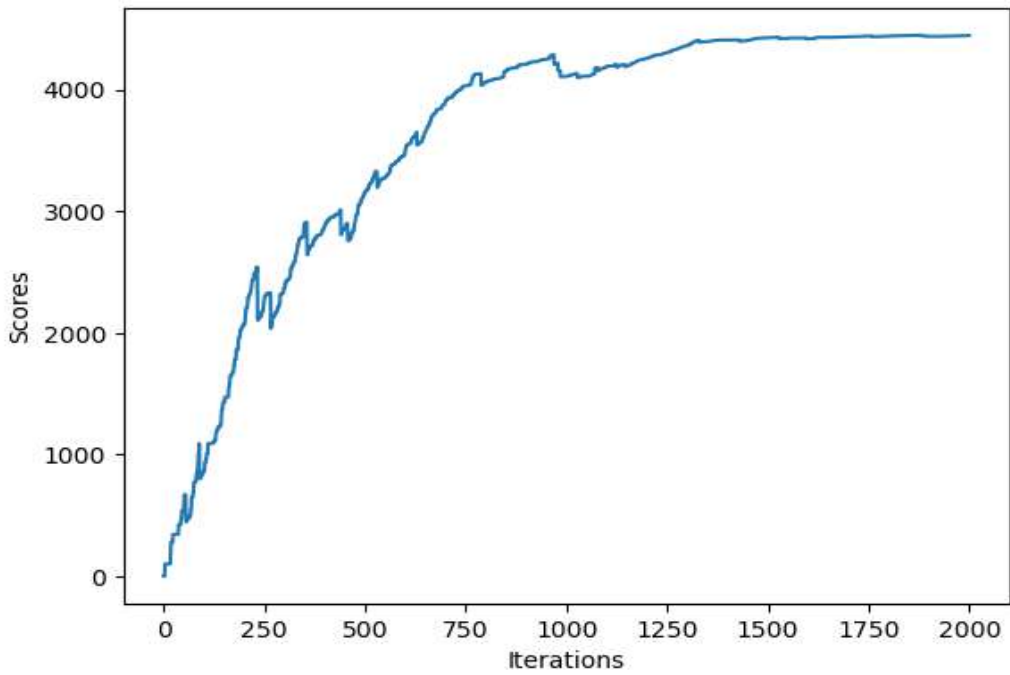


Fig. 5-15 Learning progression for the path [1, 6, 9, 12, 16, 22, 23] of USNET

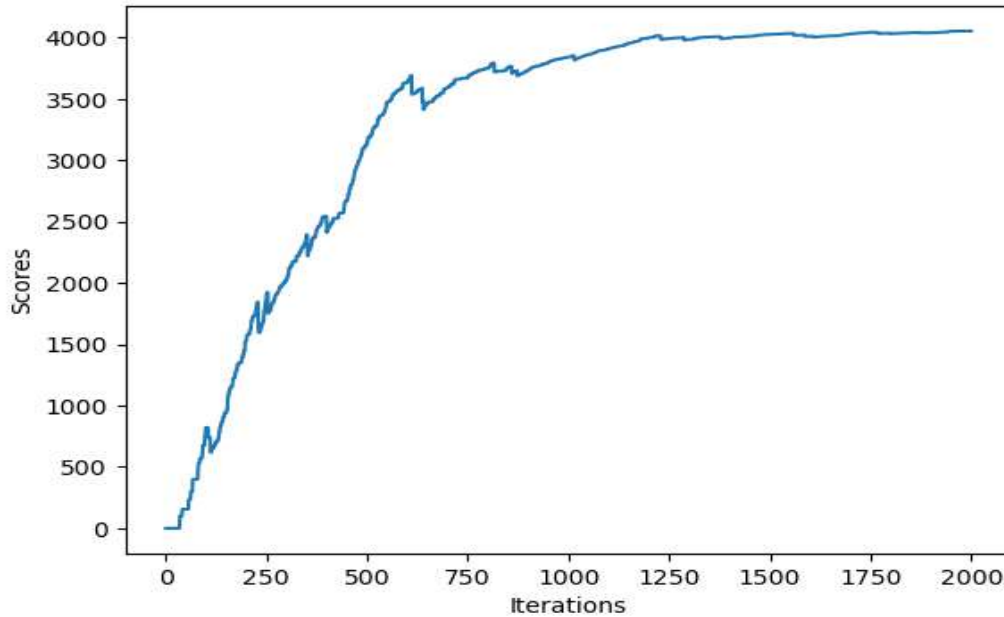


Fig. 5-16 Learning progression for the path [4, 8, 10, 14, 18, 24] of USNET

Remark 1: In the previous figures, the term "score" (sometimes referred to as "steps") denotes the performance assessment after each iteration, ultimately providing an overall evaluation of the agent's proficiency. Essentially, it signifies the number of steps taken per episode. However, it's crucial to note that the score is contingent on the updating function and reward matrix, which influence the values it yields. In actuality, the score doesn't wield significant influence over the agent's learning process; its primary purpose is to gauge how many steps or points the agent achieves in each iteration and to facilitate result visualization. It's worth mentioning that the term 'iterations' may also pertain to the number of episodes, so understanding the context is imperative. Throughout the training regimen, the procedures meticulously record the scores accrued after every iteration, offering insight into the cumulative rewards attained during training and serving as an indicator of the enhancement in the recycling method. Consequently, it can be regarded as a form of cumulative rewards, as it encapsulates various factors related to the update function.

5.3.2 Q-Learning Results for Alternative Secure Path

The search for an alternative secure path relies on Q-learning methods, which share similarities with the procedures described earlier. However, there are key differences that distinguish this approach. The following steps outline the implementation of the Q-learning algorithm to discover the alternative secure path in a graph containing secure and unsecure nodes. The graph is represented by an adjacency matrix, where each row and column corresponds to a node.

Firstly, a Q-matrix is initialized to store the Q-values for each state-action pair. Additionally, two environmental matrices, `enviro_Securenode` and `enviro_Unsecurenode`, are established to track the occurrences of secure and unsecure nodes during the learning process.

To determine the feasible actions in a given state, the available actions function is employed. It identifies the indices in the rewards matrix where the value is non-negative, indicating a potential action from the current state.

The sample next action function randomly selects the next action from the available actions. This randomization encourages exploration of different paths during action selection.

The `collect_environmental_data` function aids in gathering information about the environment when an action is taken. If the action corresponds to a secure node, it is recorded as 'Secure.' Conversely, if it corresponds to an unsecure node, it is recorded as 'Unsecure.' This information helps in analyzing the encountered environments during the learning process.

The update function serves as the core of the Q-learning algorithm. It updates the Q-matrix based on the current state, the action taken, and the maximum Q-value of the next state. The update equation incorporates the reward received from the

action and discounted future rewards. Additionally, the function updates the environmental matrices based on the environment of the action. The Q-matrix is iteratively updated to enhance the learned values.

Subsequently, the code proceeds to train the Q-learning algorithm for a specified number of episodes. In each episode, a random initial state is chosen, and the next action is sampled using the sample next action function. The update function is called to update the Q-matrix and environmental matrices based on the selected action. The score, representing the sum of the normalized Q-matrix, is recorded to monitor the learning progress.

Upon completion of training, the code visualizes the scores over the episodes to observe the learning curve. It then utilizes the trained Q-matrix to identify the most alternative secure path. Starting from an initial state, the code iteratively selects the action with the maximum Q-value until it reaches the goal state. The sequence of actions taken represents the identified most alternative secure path.

Finally, the algorithm's performance is evaluated after training. It randomly selects an initial state, chooses the next action using the sample next action function, updates the Q-matrix and environmental matrices, and records the score. The scores are plotted to provide insight into the algorithm's performance during evaluation.

By leveraging the Q-learning algorithm, the code enables efficient navigation within the graph and the identification of the most alternative secure path based on rewards and environmental information. The learned Q-values offer valuable guidance for finding secure routes in a network.

5.3.2.1 Alternative NSFNET Topology Route Results

The simulation analyzed the NSFNET Topology to check the security of different nodes. After examining the first path [1, 8, 11, 14] and the second path [2, 4, 10, 12], it was found that nodes (8, 11) and (4, 10) were unsecure.

Fig. 5-17 and Fig. 5-18 emphasize the presence of unsecure nodes along the selected paths. Furthermore, these unsecure nodes have been identified as the vulnerable points along the route.

#	Node Name	Status
1	1;8	Secure
2	8;11	Not Secure
3	11;14	Secure

Fig. 5-17 Unsecure nodes of the first path in NSFNET

#	Node Name	Status
1	2;4	Secure
2	4;10	Not Secure
3	10;12	Secure

Fig. 5-18 Unsecure nodes of the second path NSFNET

Taking into account the information provided earlier, the system has reached a point where it needs to find alternative path that ensures security and avoids unsecure nodes.

To achieve this objective, the system initiates a series of simulations represented by iteration numbers. These iterations involve testing various possible paths and evaluating their suitability in terms of security and efficiency. The system iteratively explores different combinations of nodes, assessing their potential to provide a secure connection.

After multiple iterations, as shown in Fig. 5-19 and Fig. 5-20, the system successfully discovers a path that satisfies the security requirements. These paths, labeled as [1, 2, 4, 10, 14] and [2, 1, 8, 11, 12], which is represents a sequence of nodes that the system can traverse to establish a secure communication channel. By carefully avoiding nodes (8, 11) and (4, 10), the system has been able to bypass potential vulnerabilities and ensure the safety of the data transmitted along the alternative paths.

Remark1: Note that these two selected paths are in different situations with different source and destination nodes. Each path has been tested separately. When the simulation eliminated the (8, 11) nodes from the first path and then found the alternative secure path [1, 2, 4, 10, 14], this round of the simulation does not have any relation with the second round for the second different situation to find the alternative second path. In more precise terms, if checking the second alternative path, the (8, 11) nodes exist in the path.

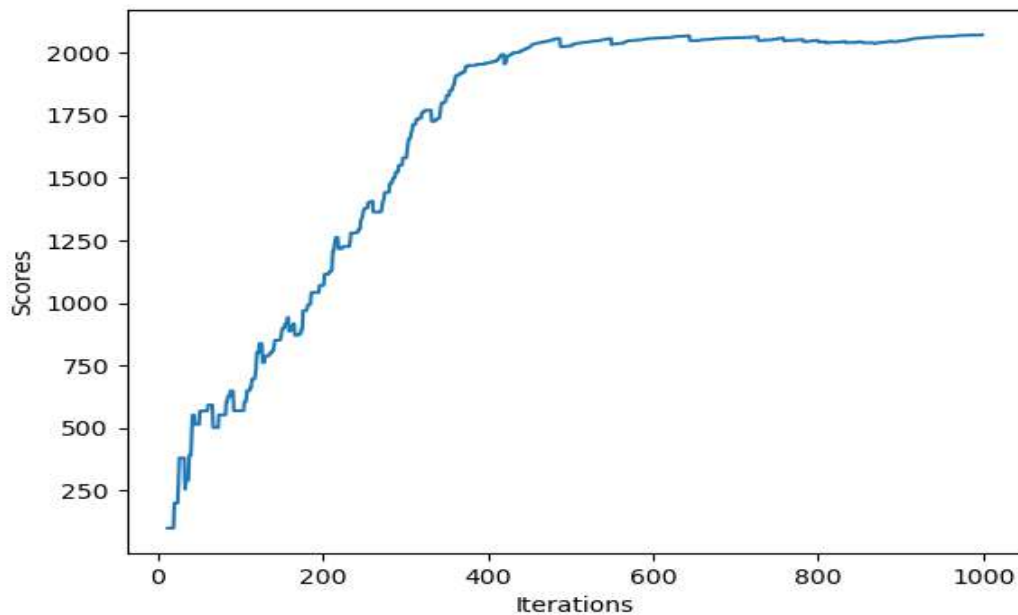


Fig. 5-19 Training progression of alternative secure path [1, 2, 4, 10, 14]

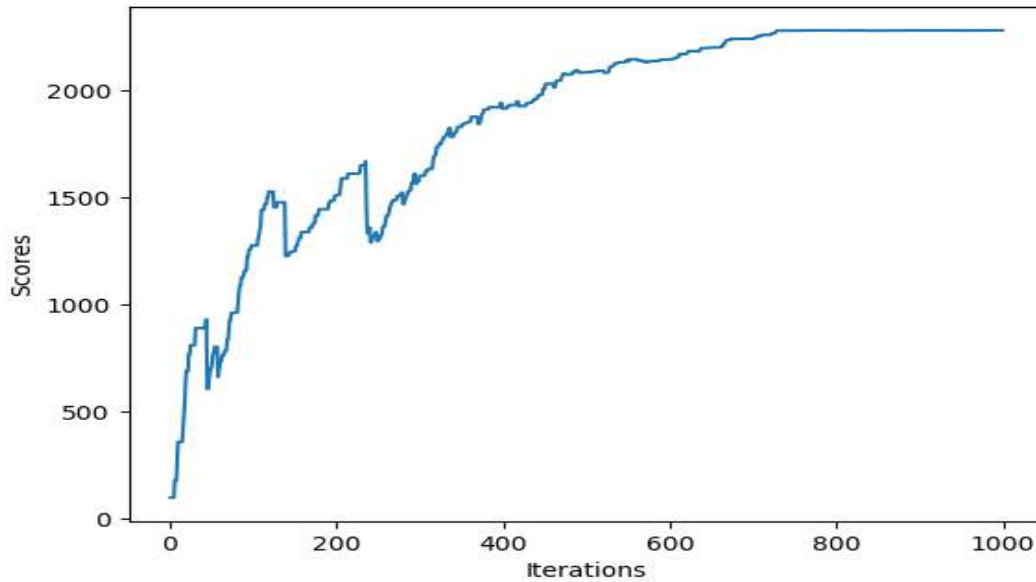


Fig. 5-20 Training progression of alternative Secure Path [2, 1, 8, 11, 12]

5.3.2.2 Alternative USNET Topology Route Results

The security of various nodes in the USNET Topology was assessed through a simulation. By analyzing the first path [1, 6, 9, 12, 16, 22, 23] and the second path [4, 8, 10, 14, 18, 24], it was discovered that nodes (9, 12) and (14,18) were determined to be insecure. Fig. 5- 21 and Fig.5-22 highlight the existence of these insecure nodes along the specified routes, and it has been identified that these nodes serve as vulnerable points along the route.

#	Node Name	Status
1	1,6	Secure
2	6,9	Secure
3	9,12	Not Secure
4	12,16	Secure
5	16,22	Secure
6	22,23	Secure

Fig. 5-21 Unsecure nodes of the first path in USNET

#	Node Name	Status
1	4;8	Secure
2	8;10	Secure
3	10;14	Secure
4	14;18	Not Secure
5	18;24	Secure

Fig. 5-22 Unsecure nodes of the second path in USNET

Based on the information provided earlier, the system has reached a stage where it must seek an alternative route that guarantees security while avoiding insecure nodes.

To accomplish this goal, the system initiates a series of simulations denoted by iteration numbers. These iterations involve the testing of different potential paths, evaluating their suitability in terms of both security and efficiency. The system systematically explores various combinations of nodes, assessing their capacity to establish a secure connection.

Following multiple iterations, as illustrated in Fig. 5- 23 and Fig.5-24, the system successfully identifies a path that meets the security requirements. These paths, labeled as [1, 6, 11, 15, 16, 22, 23] and [4, 8, 10, 13, 17, 23, 24], represent sequences of nodes that the system can traverse to establish a secure communication channel. By carefully avoiding nodes (9, 12) and (14, 18), the system has managed to circumvent potential vulnerabilities and ensure the safety of the transmitted data along these alternative routes.

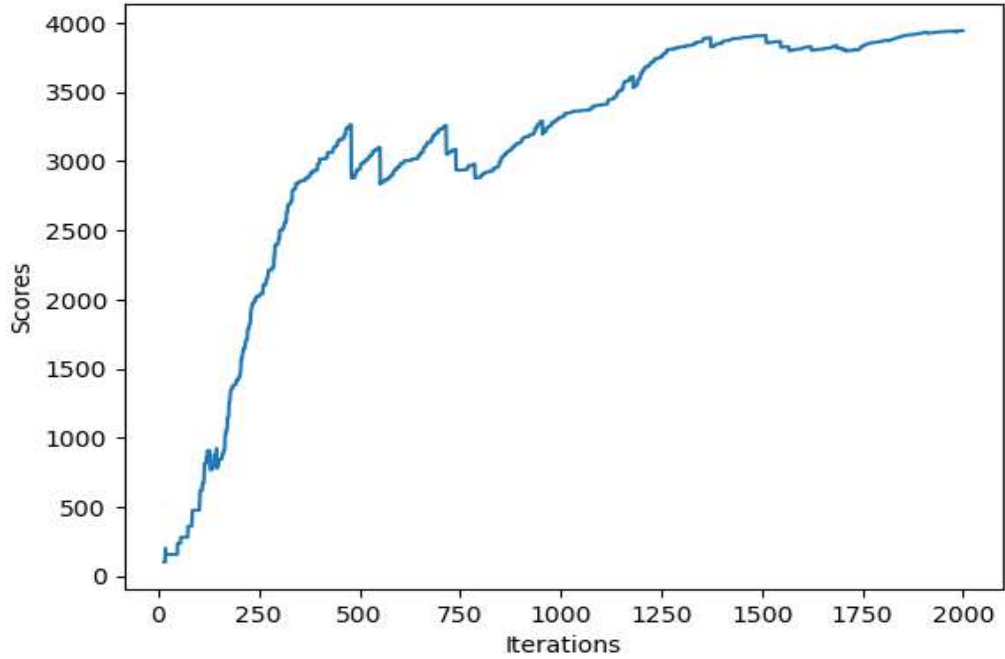


Fig. 5-23 Training progression of alternative secure path [1, 6, 11, 15, 16, 22, 23]

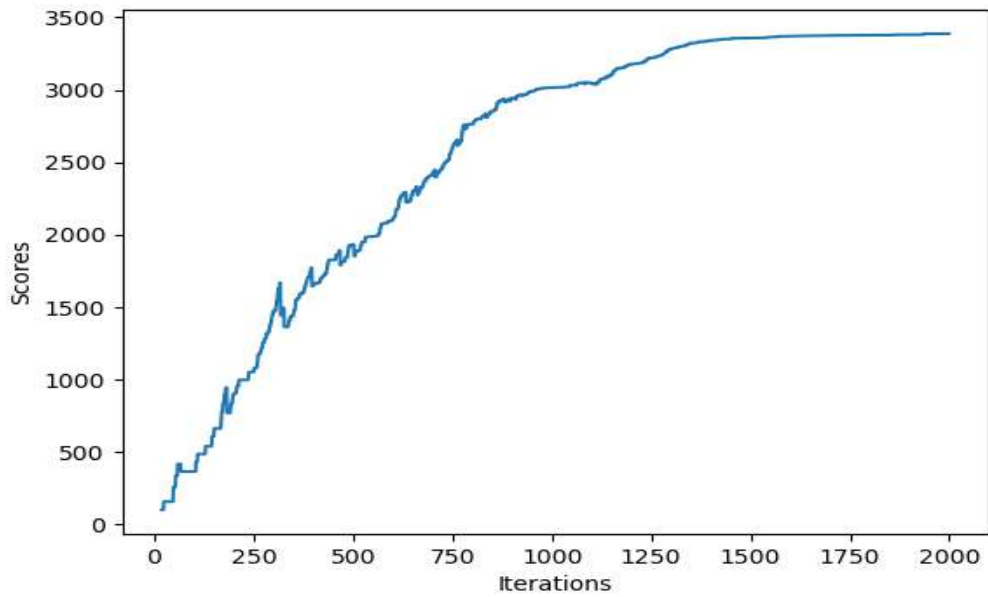


Fig. 5-24 Training progression of alternative secure path [4, 8, 10, 13, 17, 23, 24]

5.4 Results of SARAG04 Protocol

The quantum key generation in this dissertation is based on the SARAG04 protocol, which is implemented on specific paths (*alternative routes*) within the mentioned network topologies.

The following Fig. 5-25.A, B, C and D and Fig.5-26.A,B,C and D offer illustrative examples of the SARAG04 generation pertaining to the secret keys associated with the first and second alternative paths of the NSFNET network topology [1, 2, 4, 10, 14] and [2, 1, 8, 11, 12], respectively. These figures serve to showcase the specific values and patterns that arise during the SARAG04 generation process for the secret keys along this particular path. By examining these examples, one can gain insights into the underlying mechanisms and characteristics of the SARAG04 algorithm as it operates on the secret keys within the context of the NSFNET network topology. These figures contribute to a comprehensive understanding of the SARAG04 generation and its impact on the security and functionality of the network.

4-10


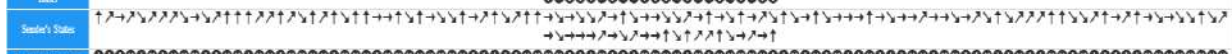
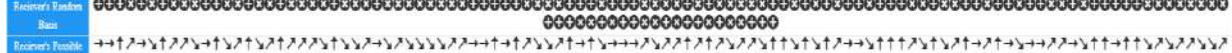

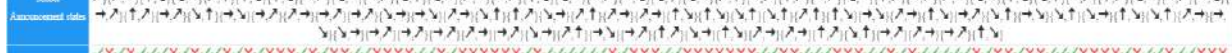

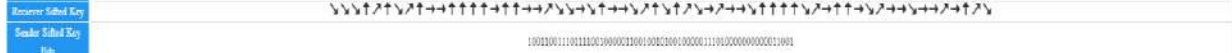

Sender's Random Bits	
Sender's States	
Receiver's Random Bits	
Receiver's Possible Measurement	
Sender Announcement states	
Discovered States	
Sender Sifted Key	
Receiver Sifted Key	
Sender Sifted Key Bits	10010001110011100100001000100010001110100000000001001
Receiver Sifted Key Bits	00010100111111100010011000000100101110011001101000
Sender Key After 4 th Round of Error Correction	0011110010000010010000001001000000000000000110000
Receiver Key After 4 th Round of Error Correction	1001111110001110000000100100000000000000000000000000
Sender Final Key after Error Correction	00110001011001000000001011110001010001110011000110010
Receiver Final Key after Error Correction	00110001011001000000001011110001010001110011000110010

Fig. 5-25.C NSFNET node 4 to node 10

10-14


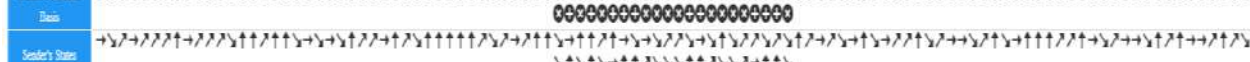

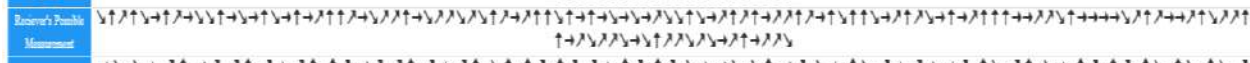
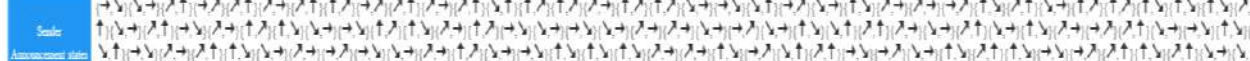



Sender's Random Bits	
Sender's States	
Receiver's Random Bits	
Receiver's Possible Measurement	
Sender Announcement states	
Discovered States	
Sender Sifted Key	
Receiver Sifted Key	
Sender Sifted Key Bits	0011100111000010001001001001100001010011001100110010000011
Receiver Sifted Key Bits	001100001000100111100011001000010000000000000000000000
Sender Key After 4 th Round of Error Correction	1111100011111000110100000010000111110001100010001000110011
Receiver Key After 4 th Round of Error Correction	1111100011111000110100000010000111100001000011000111000110011
Sender Final Key after Error Correction	11111000111110001101000000100001111000000000001000000000011
Receiver Final Key after Error Correction	11111000111110001101000000100001111000000000001000000000011

Fig. 5-25.D NSFNET node 10 to node 14

The following Fig. 5-27.A, B, C, D, E and F and Fig.5-28.A, B, C, D, E and F offer illustrative examples of the SARAG04 generation pertaining to the secret keys associated with the first and second alternative paths of the USNET network topology [1, 6, 11, 15, 16, 22, 23] and [4, 8, 10, 13, 17, 23, 24] respectively. These figures serve to showcase the specific values and patterns that arise during the SARAG04 generation process for the secret keys along this particular path. By examining these examples, one can gain insights into the underlying mechanisms and characteristics of the SARAG04 algorithm as it operates on the secret keys within the context of the USNET network topology. These figures contribute to a comprehensive understanding of the SARAG04 generation and its impact on the security and functionality of the network.



Fig. 5-27.A USNET node 1 to node 6

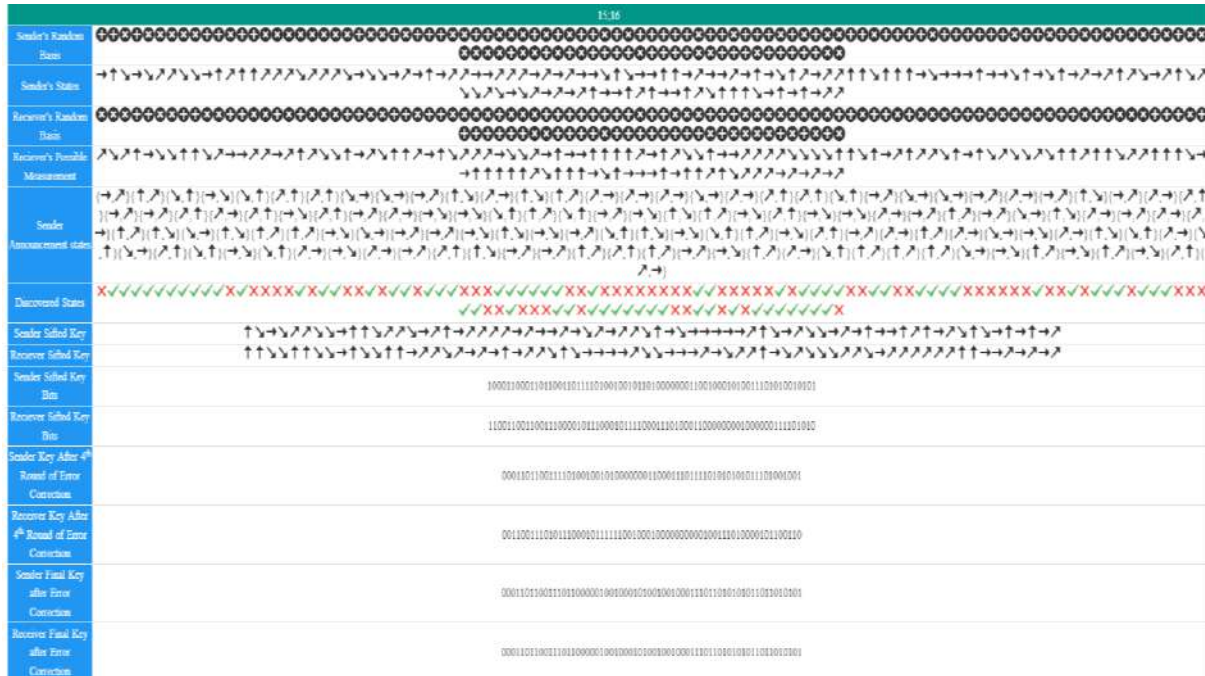


Fig. 5-27.D USNET node 15 to node 16

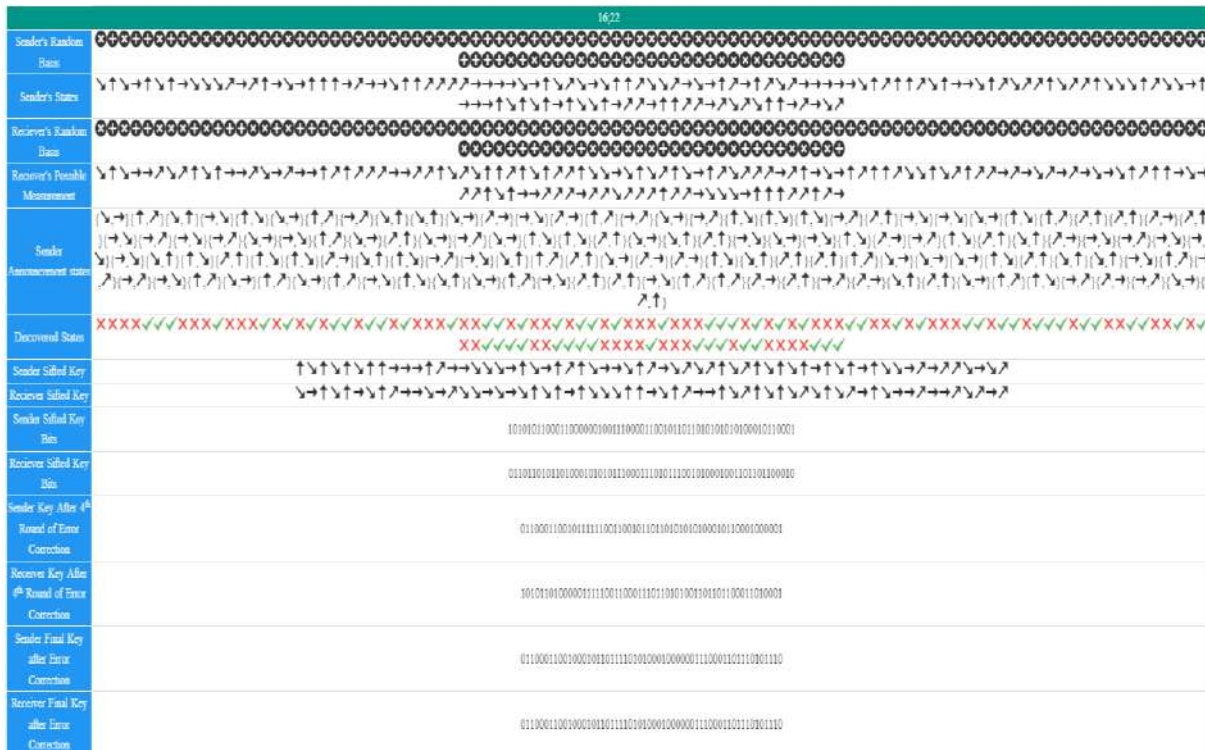


Fig. 5-27.E USNET node 16 to node 22

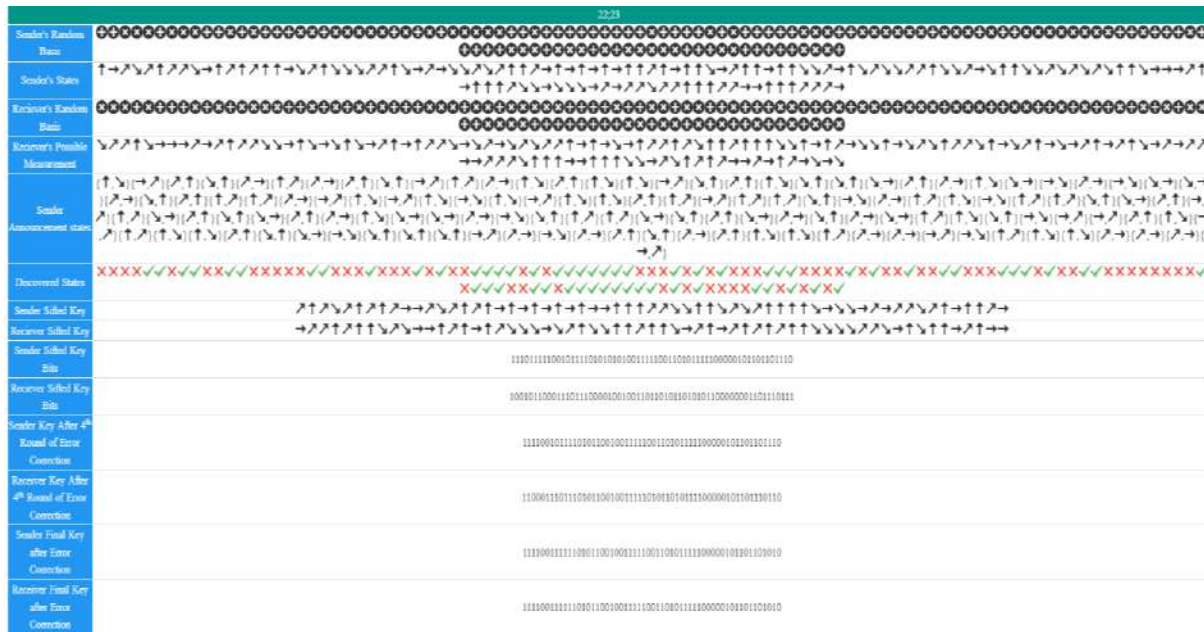


Fig. 5-27.F USNET node 22 to node 23



Fig. 5-28.A USNET node 4 to node 8

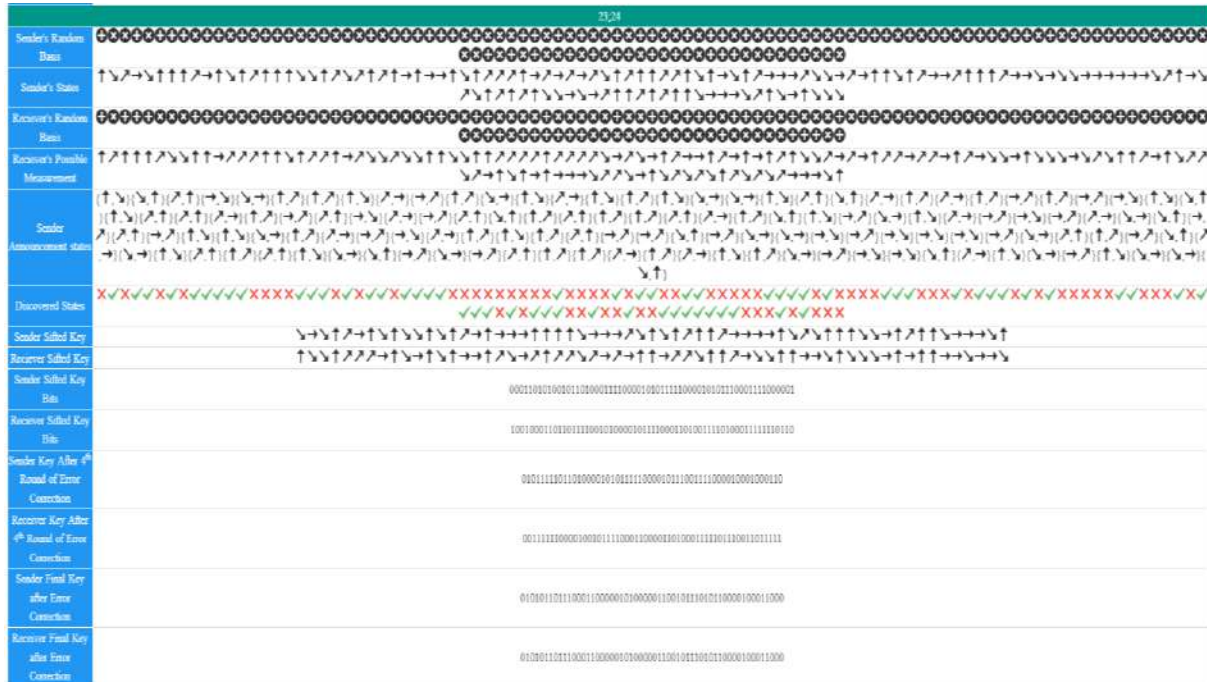


Fig. 5-28.F USNET node 23 to node 24

CHAPTER SIX: CONCLUSION AND FUTURE WORKS

6.1 Conclusion

In this chapter, the research objectives were effectively realized. The primary objective, which was to address the challenges associated with the reliability and security of CTR technology within QKD networks, was successfully accomplished. A comprehensive analysis of the limitations inherent to CTR nodes revealed significant hurdles in ensuring the consistent reliability of the CTR technique for remote QKD applications.

To address these concerns, the SDQTRF model was introduced as a robust survivability solution. Central to this model is the integration of a novel relay mechanism, housing a "Contingency Function" within the SDN controller. This innovative feature substantially enhances key management, especially in scenarios where the relay key transmission experiences setbacks, guaranteeing uninterrupted secure communication even in the face of CTR failures.

Employing Q-learning, a reinforcement learning technique, the SDQTRF model dynamically adjusts key recycling processes within the QKD network. Through continual optimization based on feedback and experience, this model bolsters the security and reliability of the recycling mechanism.

Additionally, a pioneering concept was introduced, leveraging the Q-learning method to identify new secure paths within the QKD network. This innovation significantly enhances the network's overall survivability, enabling seamless rerouting in the wake of node or link failures, thereby ensuring the continuous delivery of secure communication.

According to the simulation results, the implementation of the SDQTRF model led to significant improvements across various terms. Specifically, there was

a substantial enhancement of approximately 31.477% in the key generation ratio. Moreover, the key utilization rate also showed remarkable improvement, reaching approximately 23.5%. Additionally, the recovery after failure demonstrated an impressive rate of approximately 9.8×10^{-5} . Furthermore, the implementation of the SDQTRF model resulted in a considerable reduction in the avalanche effect, with a reduction of about 42.5%, and a lower service-blocking rate of around 0.27.

These findings provide valuable insights into the substantial improvements achieved in terms of the reliability and security of QKD networks through the implementation of the SDQTRF model.

6.2 Future Directions and Recommendations

Exploring the future of QKD networks and the integration of SDN and RL technologies entails several key areas that warrant further exploration and enhancement:

- 1. Enhancing CTR Technology Reliability:** The effectiveness of CTR technology in extending the coverage range of QKD systems is critical. However, it is imperative to address potential failure points. Future research should focus on identifying, mitigating, and rectifying the underlying causes of CTR technology failures. This may involve robust fault-tolerant mechanisms or alternative techniques to ensure uninterrupted secure key distribution.
- 2. Deepening Q-Learning Integration:** While Q-learning has shown promise in network routing, resource limitations associated with the Q-table present challenges. Investigating the application of deep Q-learning, harnessing the computational power of neural networks, can lead to more precise and efficient results. This advancement may significantly enhance the capabilities of models

like SDQTRF, providing a more adaptive and dynamic approach to key distribution.

- 3. Scalability for Larger QKD Networks:** As quantum networks expand, scalability becomes a paramount concern. Future research should focus on optimizing the proposed SDQTRF model to accommodate larger QKD networks. This may involve novel approaches to relay mechanisms, dynamic key recycling, and adaptive routing strategies to ensure seamless and secure communication over extensive distances.
- 4. Adapting to Varying Network Conditions:** Real-world network conditions are dynamic and can vary significantly. Future studies should investigate adaptive strategies within the SDQTRF framework to respond effectively to changing environmental parameters. This includes considerations for factors like signal attenuation, noise levels, and variations in optical fiber properties, ensuring robust performance under diverse operating conditions.
- 5. QKD Beyond Optical Fiber Networks:** While the focus has predominantly been on optical fiber-based QKD networks, there is a growing interest in extending these technologies to other mediums, such as free-space quantum communication. Future research should explore the adaptation and optimization of the SDQTRF model for non-conventional quantum communication channels, broadening the applicability of secure key distribution.
- 6. Cybersecurity and Quantum Threats:** In an evolving threat landscape, cybersecurity remains a critical concern. Future work should consider potential quantum threats and develop countermeasures to safeguard QKD systems. This may involve integrating quantum-resistant cryptographic protocols or employing quantum-enhanced security measures to fortify the resilience of quantum communication networks.

REFERENCES

- CISCO, U. 2020. Cisco annual internet report (2018–2023) white paper. *Cisco: San Jose, CA, USA*, 10, 1-35.
- AGIWAL, M., ROY, A. & SAXENA, N. 2016. Next generation 5G wireless networks: A comprehensive survey.
- SKORIN-KAPOV, N., FURDEK, M., ZSIGMOND, S. & WOSINSKA, L. 2016. Physical-layer security in evolving optical networks. *IEEE Communications Magazine*, 54, 110-117.
- FURDEK, M., SKORIN-KAPOV, N., ZSIGMOND, S. & WOSINSKA, L. Vulnerabilities and security issues in optical networks. 2014 16th International Conference on Transparent Optical Networks (ICTON), 2014. IEEE, 1-4.
- DONG, H., SONG, Y. & YANG, L. 2019. Wide area key distribution network based on a quantum key distribution system. *Applied Sciences*, 9, 1073.
- DONG, K., ZHAO, Y., YU, X., NAG, A. & ZHANG, J. 2020. Auxiliary graph based routing, wavelength, and time-slot assignment in metro quantum optical networks with a novel node structure. *Optics express*, 28, 5936-5952.
- DONG, K., ZHAO, Y., NAG, A., YU, X. & ZHANG, J. 2020. Distributed subkey-relay-tree-based secure multicast scheme in quantum data center networks. *Optical Engineering*, 59, 065102-065102.
- MEHIC, M., NIEMIEC, M., RASS, S., MA, J., PEEV, M., AGUADO, A., MARTIN, V., SCHAUER, S., POPPE, A. & PACHER, C. 2020. Quantum key distribution: a networking perspective. *ACM Computing Surveys (CSUR)*, 53, 1-41.
- MEHIC, M., FAZIO, P., RASS, S., MAURHART, O., PEEV, M., POPPE, A., ROZHON, J., NIEMIEC, M. & VOZNAK, M. 2019. A novel approach to quality-of-service provisioning in trusted relay quantum key distribution networks. *IEEE/ACM Transactions on Networking*, 28, 168-181.
- SHARMA, P., AGRAWAL, A., BHATIA, V., PRAKASH, S. & MISHRA, A. K. 2021. Quantum key distribution secured optical networks: A survey. *IEEE Open Journal of the Communications Society*, 2, 2049-2083.
- LO, H.-K., CURTY, M. & TAMAKI, K. 2014. Secure quantum key distribution. *Nature Photonics*, 8, 595-604.
- SCARANI, V., BECHMANN-PASQUINUCCI, H., CERF, N. J., DUŠEK, M., LÜTKENHAUS, N. & PEEV, M. 2009. The security of practical quantum key distribution. *Reviews of modern physics*, 81, 1301.
- LO, H.-K., CURTY, M. & QI, B. 2012. Measurement-device-independent quantum key distribution. *Physical review letters*, 108, 130503.

- SCARANI, V., ACIN, A., RIBORDY, G. & GISIN, N. 2004. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Physical review letters*, 92, 057901.
- SCARANI, V. & KURTSIEFER, C. 2014. The black paper of quantum cryptography: real implementation problems. *Theoretical Computer Science*, 560, 27-32.
- ZHAO, Y., CAO, Y., WANG, W., WANG, H., YU, X., ZHANG, J., TORNATORE, M., WU, Y. & MUKHERJEE, B. 2018. Resource allocation in optical networks secured by quantum key distribution. *IEEE Communications Magazine*, 56, 130-137.
- ZHAO, Y., CAO, Y., YU, X., ZHANG, J. & MOROZOV, O. 2018. Quantum key distribution (QKD) over software-defined optical networks. *Quantum Cryptography in Advanced Networks*. IntechOpen.
- ZHAO, Z., ZHAO, Y., LI, Y., WANG, F., LI, X., HAN, D. & ZHANG, J. 2021. Service restoration in multi-modal optical transport networks with reinforcement learning. *Optics Express*, 29, 3825-3840.
- ZHAO, Y., CAO, Y., YU, X. & ZHANG, J. Software defined optical networks secured by quantum key distribution (QKD). 2017 IEEE/CIC International Conference on Communications in China (ICCC), 2017. IEEE, 1-4.
- TANG, Y.-L., YIN, H.-L., ZHAO, Q., LIU, H., SUN, X.-X., HUANG, M.-Q., ZHANG, W.-J., CHEN, S.-J., ZHANG, L. & YOU, L.-X. 2016. Measurement-device-independent quantum key distribution over untrustful metropolitan network. *Physical Review X*, 6, 011024.
- YIN, H.-L., CHEN, T.-Y., YU, Z.-W., LIU, H., YOU, L.-X., ZHOU, Y.-H., CHEN, S.-J., MAO, Y., HUANG, M.-Q. & ZHANG, W.-J. 2016. Measurement-device-independent quantum key distribution over a 404 km optical fiber. *Physical review letters*, 117, 190501.
- LIU, H., WANG, W., WEI, K., FANG, X.-T., LI, L., LIU, N.-L., LIANG, H., ZHANG, S.-J., ZHANG, W. & LI, H. 2019. Experimental demonstration of high-rate measurement-device-independent quantum key distribution over asymmetric channels. *Physical review letters*, 122, 160501.
- LUCAMARINI, M., YUAN, Z. L., DYNES, J. F. & SHIELDS, A. J. 2018. Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. *Nature*, 557, 400-403.
- ZHANG, L., TANG, L., ZHANG, S., WANG, Z., SHEN, X. & ZHANG, Z. 2021. A self-adaptive reinforcement-exploration Q-learning algorithm. *Symmetry*, 13, 1057.
- FANG, X.-T., ZENG, P., LIU, H., ZOU, M., WU, W., TANG, Y.-L., SHENG, Y.-J., XIANG, Y., ZHANG, W. & LI, H. 2020. Implementation of quantum key

- distribution surpassing the linear rate-transmittance bound. *Nature Photonics*, 14, 422-425.
- CAO, Y., ZHAO, Y., LI, J., LIN, R., ZHANG, J. & CHEN, J. 2021. Hybrid trusted/untrusted relay-based quantum key distribution over optical backbone networks. *IEEE Journal on Selected Areas in Communications*, 39, 2701-2718.
- CAO, Y., ZHAO, Y., LI, J., LIN, R., ZHANG, J. & CHEN, J. Mixed relay placement for quantum key distribution chain deployment over optical networks. 2020 European Conference on Optical Communications (ECOC), 2020. IEEE, 1-4.
- ZOU, X., YU, X., ZHAO, Y., NAG, A. & ZHANG, J. Collaborative routing in partially-trusted relay based quantum key distribution optical networks. 2020 Optical Fiber Communications Conference and Exhibition (OFC), 2020. IEEE, 1-3.
- LI, X., ZHAO, Y., NAG, A., YU, X. & ZHANG, J. 2020. Key-recycling strategies in quantum-key-distribution networks. *Applied Sciences*, 10, 3734.
- CAO, Y., ZHAO, Y., COLMAN-MEIXNER, C., YU, X. & ZHANG, J. 2017. Key on demand (KoD) for software-defined optical networks secured by quantum key distribution (QKD). *Optics express*, 25, 26453-26467.
- CAO, Y., ZHAO, Y., WU, Y., YU, X. & ZHANG, J. 2018. Time-scheduled quantum key distribution (QKD) over WDM networks. *Journal of Lightwave Technology*, 36, 3382-3395.
- ZAPATERO, V., VAN LEENT, T., ARNON-FRIEDMAN, R., LIU, W.-Z., ZHANG, Q., WEINFURTER, H. & CURTY, M. 2023. Advances in device-independent quantum key distribution. *npj Quantum Information*, 9, 10.
- AGUADO, A., HUGUES-SALAS, E., HAIGH, P. A., MARHUENDA, J., PRICE, A. B., SIBSON, P., KENNARD, J. E., ERVEN, C., RARITY, J. G. & THOMPSON, M. G. 2017. Secure NFV orchestration over an SDN-controlled optical network with time-shared quantum key distribution resources. *Journal of Lightwave Technology*, 35, 1357-1362.
- AGUADO, A., LÓPEZ, V., BRITO, J. P., PASTOR, A., LÓPEZ, D. R. & MARTIN, V. Enabling quantum key distribution networks via software-defined networking. 2020 International Conference on Optical Network Design and Modeling (ONDM), 2020. IEEE, 1-5.
- AGUADO, A., LOPEZ, V., MARTINEZ-MATEO, J., PEEV, M., LOPEZ, D. & MARTIN, V. 2018. Virtual network function deployment and service automation to provide end-to-end quantum encryption. *Journal of Optical Communications and Networking*, 10, 421-430.
- HUGUES-SALAS, E., NTAVOU, F., GKOUNIS, D., KANELLOS, G. T., NEJABATI, R. & SIMEONIDOU, D. 2019. Monitoring and physical-layer

- attack mitigation in SDN-controlled quantum key distribution networks. *Journal of Optical Communications and Networking*, 11, A209-A218.
- HUGUES-SALAS, E., NTAVOU, F., OU, Y., KENNARD, J. E., WHITE, C., GKOUNIS, D., NIKOLOVGENIS, K., KANELLOS, G., ERVEN, C. & LORD, A. Experimental demonstration of DDoS mitigation over a quantum key distribution (QKD) network using software defined networking (SDN). Optical fiber communication conference, 2018. Optica Publishing Group, M2A. 6.
- XU, F.-H., WEN, H., HAN, Z.-F. & GUO, G.-C. 2021. Network coding in trusted relay based quantum network. *Accessed: Jul, 30*.
- CAO, Y., ZHAO, Y., YU, X. & ZHANG, J. 2019. Multi-tenant provisioning over software defined networking enabled metropolitan area quantum key distribution networks. *JOSA B*, 36, B31-B40.
- CAO, Y., ZHAO, Y., YU, X., CHENG, L., LI, Z., LIU, G. & ZHANG, J. Experimental demonstration of end-to-end key on demand service provisioning over quantum key distribution networks with software defined networking. Optical Fiber Communication Conference, 2019. Optica Publishing Group, Th1G. 4.
- CHO, J. Y., PEDRENO-MANRESA, J.-J., PATRI, S., SERGEEV, A., ELBERS, J.-P., GRIESSER, H., WHITE, C. & LORD, A. Demonstration of Software-defined Key Management for Quantum Key Distribution Network. Optical Fiber Communication Conference, 2021. Optical Society of America, M2B. 4.
- OU, Y., HUGUES-SALAS, E., NTAVOU, F., WANG, R., BI, Y., YAN, S., KANELLOS, G., NEJABATI, R. & SIMEONIDOU, D. Field-trial of machine learning-assisted quantum key distribution (QKD) networking with SDN. 2018 European Conference on Optical Communication (ECOC), 2018. IEEE, 1-3.
- CAO, Y., ZHAO, Y., LI, J., LIN, R., ZHANG, J. & CHEN, J. 2020. Multi-tenant provisioning for quantum key distribution networks with heuristics and reinforcement learning: a comparative study. *IEEE Transactions on Network and Service Management*, 17, 946-957.
- CAO, Y., ZHAO, Y., LI, J., LIN, R., ZHANG, J. & CHEN, J. Reinforcement learning based multi-tenant secret-key assignment for quantum key distribution networks. 2019 Optical Fiber Communications Conference and Exhibition (OFC), 2019. IEEE, 1-3.
- LIN, X., HOU, G., LIN, W. & CHEN, K. Quantum key distribution in partially-trusted QKD ring networks. 2020 IEEE 3rd International Conference on Information Systems and Computer Aided Education (ICISCAE), 2020. IEEE, 33-36.

- MCPARTLAND, M. & GALLAGHER, M. Learning to be a bot: Reinforcement learning in shooter games. Proceedings of the AAAI Conference on Artificial Intelligence and Interactive Digital Entertainment, 2008. 78-83.
- Bennett, C.H. and Brassard, G. 1984. Quantum Cryptography: Public Key Distribution and Coin Tossing. Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, 10-12 December 1984, 175-179.
- SINGH, H., GUPTA, D. L. & SINGH, A. K. 2014. Quantum key distribution protocols: a review. *Journal of Computer Engineering*, 16, 1-9.
- SALVAIL, L., PEEV, M., DIAMANTI, E., ALLÉAUME, R., LÜTKENHAUS, N. & LÄNGER, T. 2010. Security of trusted repeater quantum key distribution networks. *Journal of Computer Security*, 18, 61-87.
- T. Langer, "The practical application of quantum key distribution," Ph.D. thesis, Dept. Inf. Syst., Univ. Lausanne, Lausanne, Switzerland, 2013.
- ELLIOTT, C. 2004. Quantum cryptography. *IEEE security & privacy*, 2, 57-61.
- SCHARTNER, P. & RASS, S. How to overcome the 'Trusted Node Model' in Quantum Cryptography. 2009 International Conference on Computational Science and Engineering, 2009. IEEE, 259-262.
- WANG, H., ZHAO, Y., YU, X., MA, Z., WANG, J., NAG, A., YI, L. & ZHANG, J. 2019. Protection schemes for key service in optical networks secured by quantum key distribution (QKD). *Journal of Optical Communications and Networking*, 11, 67-78.
- MCKEOWN, N., ANDERSON, T., BALAKRISHNAN, H., PARULKAR, G., PETERSON, L., REXFORD, J., SHENKER, S. & TURNER, J. 2008. OpenFlow: enabling innovation in campus networks. *ACM SIGCOMM computer communication review*, 38, 69-74.
- KARINOU, F., BRUNNER, H. H., FUNG, C.-H. F., COMANDAR, L. C., BETTELLI, S., HILLERKUSS, D., KUSCHNEROV, M., MIKROULIS, S., WANG, D. & XIE, C. 2018. Toward the integration of CV quantum key distribution in deployed optical networks. *IEEE Photonics Technology Letters*, 30, 650-653.
- WANG, H., ZHAO, Y. & NAG, A. 2019. Quantum-key-distribution (QKD) networks enabled by software-defined networks (sdn). *Applied Sciences*, 9, 2081.
- CAO, Y., ZHAO, Y., WANG, J., YU, X., MA, Z. & ZHANG, J. 2019. SDQaaS: Software defined networking for quantum key distribution as a service. *Optics express*, 27, 6892-6909.
- ZENG, F., WANG, C. & GE, S. S. 2020. A survey on visual navigation for artificial agents with deep reinforcement learning. *IEEE Access*, 8, 135426-135442.

- RAGHUNANDAN, K., GANESH, A., SURENDRA, S. & BHAVYA, K. 2020. Key generation using generalized Pell's equation in public key cryptography based on the prime fake modulus principle to image encryption and its security analysis. *Cybernetics and Information Technologies*, 20, 86-101.
- PARKINSON, R. 2002. Traffic engineering techniques in telecommunications. *Infotel Systems Corporation*.
- ZHANG, Q., LIU, Y., YU, X., ZHAO, Y. & ZHANG, J. Topology-Abstraction-Based Protection Scheme in Quantum Key Distribution Networks with Partially Trusted Relays. *Photonics*, 2022. MDPI, 239.
- CAMPAGNA, M., CHEN, A. L., DAGDELEN, Ö., DARMSTADT, T. U., DING, J., FERNICK, J. K., HAYFORD, D., JENNEWEIN, T., LÜTKENHAUS, N., MOSCA, M., PHIL, D., NEILL, B., PECEN, M., PERLNER, R., SCHANCK, J. M., STEBILA, D., WALENTA, N., WHYTE, W., ZHANG, Z., ... PETZOLD, A. 2015. *Quantum Safe Cryptography and Security An introduction, benefits, enablers and challenges Quantum Safe Cryptography and Security Authors & contributors Quantum Safe Cryptography and Security 2*. www.etsi.org
- PEEV, M., PACHER, C., ALLÉAUME, R., BARREIRO, C., BOUDA, J., BOXLEITNER, W., DEBUISSCHERT, T., DIAMANTI, E., DIANATI, M. & DYNES, J. 2009. The SECOQC quantum key distribution network in Vienna. *New Journal of Physics*, 11, 075001.
- YU, C., LAN, J., GUO, Z. & HU, Y. 2018. DROM: Optimizing the routing in software-defined networks with deep reinforcement learning. *IEEE Access*, 6, 64533-64539.
- ELKOUSS, D., MARTINEZ-MATEO, J., CIURANA, A. & MARTIN, V. 2013. Secure optical networks based on quantum key distribution and weakly trusted repeaters. *Journal of Optical Communications and Networking*, 5, 316-328.
- CAO, Y., LI, Y.-H., YANG, K.-X., JIANG, Y.-F., LI, S.-L., HU, X.-L., ABULIZI, M., LI, C.-L., ZHANG, W. & SUN, Q.-C. 2020. Long-distance free-space measurement-device-independent quantum key distribution. *Physical Review Letters*, 125, 260503.
- CHEN, J.-P., ZHANG, C., LIU, Y., JIANG, C., ZHANG, W., HU, X.-L., GUAN, J.-Y., YU, Z.-W., XU, H. & LIN, J. 2020. Sending-or-not-sending with independent lasers: Secure twin-field quantum key distribution over 509 km. *Physical review letters*, 124, 070501.
- NURHADI, A. I. & SYAMBAS, N. R. Quantum key distribution (QKD) protocols: A survey. 2018 4th International Conference on Wireless and Telematics (ICWT), 2018. IEEE, 1-5.

- CAO, Y., ZHAO, Y., WANG, J., YU, X., MA, Z. & ZHANG, J. 2019. Cost-efficient quantum key distribution (QKD) over WDM networks. *Journal of Optical Communications and Networking*, 11, 285-298.
- KIKTENKO, E. O., MALYSHEV, A. O., GAVREEV, M. A., BOZHEDAROV, A. A., POZHAR, N. O., ANUFRIEV, M. N. & FEDOROV, A. K. 2020. Lightweight authentication for quantum key distribution. *IEEE Transactions on Information Theory*, 66, 6354-6368.
- GARCIA-COBO, I. & MENÉNDEZ, H. D. 2021. Designing large quantum key distribution networks via medoid-based algorithms. *Future Generation Computer Systems*, 115, 814-824.
- ZHANG, Y. & NI, Q. Design and Analysis of Secure Quantum Network System with Trusted Repeaters. 2018 IEEE/CIC International Conference on Communications in China (ICCC), 2018. IEEE, 511-514.
- MENDEZ, R. B., BRITO, J. P., VICENTE, R. J., AGUADO, A., PASTOR, A., LOPEZ, D., MARTÍN, V. & LOPEZ, V. Quantum Abstraction Interface: Facilitating Integration of QKD Devices in SDN Networks. 2020 22nd International Conference on Transparent Optical Networks (ICTON), 2020. IEEE, 1-4.
- MARTÍN, V., LOPEZ, D., AGUADO, A., BRITO, J. P., SETIEN, J., SALAS, P., ESCRIBANO, C., LOPEZ, V., PASTOR-PERALES, A. & PEEV, M. A components based framework for quantum key distribution networks. 2020 22nd International Conference on Transparent Optical Networks (ICTON), 2020. IEEE, 1-4.
- TESSINARI, R. S., BRAVALHERI, A., HUGUES-SALAS, E., COLLINS, R., AKTAS, D., GUIMARAES, R. S., ALIA, O., RARITY, J., KANELLOS, G. T. & NEJABATI, R. Field trial of dynamic DV-QKD networking in the SDN-controlled fully-meshed optical metro network of the bristol city 5GUK test network. 45th European Conference on Optical Communication (ECOC 2019), 2019. IET, 1-4.
- TANG, Z., ZHANG, P., KRAWEC, W. O. & JIANG, Z. 2020. Programmable quantum networked microgrids. *IEEE Transactions on Quantum Engineering*, 1, 1-13.
- MARTÍN, V., AGUADO, A., BRITO, J. P., SANZ, A., SALAS, P., LÓPEZ, D. R., LÓPEZ, V., PASTOR-PERALES, A., POPPE, A. & PEEV, M. Quantum aware SDN nodes in the Madrid quantum network. 2019 21st International Conference on Transparent Optical Networks (ICTON), 2019. IEEE, 1-4.
- BRITO, J. P., LÓPEZ, D. R., AGUADO, A., ABELLÁN, C., LÓPEZ, V., PASTOR-PERALES, A., DE LA IGLESIA, F. & MARTÍN, V. Quantum services architecture in softwarized infrastructures. 2019 21st International Conference on Transparent Optical Networks (ICTON), 2019. IEEE, 1-4.

- LOPEZ, V., PASTOR, A., LOPEZ, D., AGUADO, A. & MARTIN, V. Applying QKD to improve next-generation network infrastructures. 2019 European Conference on Networks and Communications (EuCNC), 2019. IEEE, 283-288.
- WANG, Y., ZHAO, Y., CHEN, W., DONG, K., YU, X. & ZHANG, J. Routing and key resource allocation in SDN-based quantum satellite networks. 2020 International Wireless Communications and Mobile Computing (IWCMC), 2020. IEEE, 2016-2021.
- CAO, Y., ZHAO, Y., WANG, J., YU, X., MA, Z. & ZHANG, J. 2019. KaaS: Key as a service over quantum key distribution integrated optical networks. *IEEE Communications Magazine*, 57, 152-159.
- WANG, H., ZHAO, Y., LI, Y., YU, X., ZHANG, J., LIU, C. & SHAO, Q. 2018. A flexible key-updating method for software-defined optical networks secured by quantum key distribution. *Optical Fiber Technology*, 45, 195-200.
- NIE, M., XIE, H. & WEI, R. QKD Protocol To Enhance The Southbound Security Of Software Defined Network. 2020 International Conference on Computer Engineering and Application (ICCEA), 2020. IEEE, 264-268.
- LIU, X., YU, X., ZHAO, Y., ZHOU, X., XIE, S., LI, J. & ZHANG, J. Multi-path based Quasi-real-time Quantum Key Distribution in Software Defined Quantum Key Distribution Networks (SD-QKDN). 2019 18th International Conference on Optical Communications and Networks (ICOON), 2019. IEEE, 1-3.
- MAVROMATIS, A., NTAVOU, F., SALAS, E. H., KANELLOS, G. T., NEJABATI, R. & SIMEONIDOU, D. Experimental demonstration of quantum key distribution (QKD) for energy-efficient software-defined Internet of Things. 2018 European Conference on Optical Communication (ECOC), 2018. IEEE, 1-3.
- PENG, Y., WU, C., ZHAO, B., YU, W., LIU, B. & QIAO, S. QKDFlow: QKD based secure communication towards the openflow interface in SDN. *Geo-Spatial Knowledge and Intelligence: 4th International Conference on Geo-Informatics in Resource Management and Sustainable Ecosystem, GRMSE 2016, Hong Kong, China, November 18-20, 2016, Revised Selected Papers, Part II 4*, 2017. Springer, 410-415.
- LOPEZ, D. R., MARTIN, V., LOPEZ, V., DE LA IGLESIA, F., PASTOR, A., BRUNNER, H., AGUADO, A., BETTELLI, S., FUNG, F. & HILLERKUSS, D. 2020. Demonstration of software defined network services utilizing quantum key distribution fully integrated with standard telecommunication network. *Quantum Reports*, 2, 453-458.

- ZHANG, H., QUAN, D., ZHU, C. & LI, Z. A quantum cryptography communication network based on software defined network. ITM Web of Conferences, 2018. EDP Sciences, 01008.
- WANG, W. & LO, H.-K. 2019. Machine learning for optimal parameter prediction in quantum key distribution. *Physical Review A*, 100, 062334.
- WANG, H., ZHAO, Y., YU, X., NAG, A., MA, Z., WANG, J., YAN, L. & ZHANG, J. 2019. Resilient quantum key distribution (QKD)-integrated optical networks with secret-key recovery strategy. *IEEE Access*, 7, 60079-60090.
- LIU, W., HUANG, P., PENG, J., FAN, J. & ZENG, G. 2018. Integrating machine learning to achieve an automatic parameter prediction for practical continuous-variable quantum key distribution. *Physical Review A*, 97, 022316.
- MAO, Y., HUANG, W., ZHONG, H., WANG, Y., QIN, H., GUO, Y. & HUANG, D. 2020. Detecting quantum attacks: a machine learning based defense strategy for practical continuous-variable quantum key distribution. *New Journal of Physics*, 22, 083073.
- OKEY, O. D., MAIDIN, S. S., LOPES ROSA, R., TOOR, W. T., CARRILLO MELGAREJO, D., WUTTISITTIKULKIJ, L., SAADI, M. & ZEGARRA RODRÍGUEZ, D. 2022. Quantum Key Distribution Protocol Selector Based on Machine Learning for Next-Generation Networks. *Sustainability*, 14, 15901.
- NIU, J., SUN, Y., JIA, X. & JI, Y. 2021. Key-size-driven wavelength resource sharing scheme for QKD and the time-varying data services. *Journal of Lightwave Technology*, 39, 2661-2672.
- ALI, T. E., CHONG, Y.-W. & MANICKAM, S. 2023. Machine Learning Techniques to Detect a DDoS Attack in SDN: A Systematic Review. *Applied Sciences*, 13, 3183.
- ELLIOTT, C. & YE, H. 2007. DARPA quantum network testbed. BBN TECHNOLOGIES CAMBRIDGE MA.
- NADEAU, T. D. & GRAY, K. 2013. *SDN: Software Defined Networks: An authoritative review of network programmability technologies*, " O'Reilly Media, Inc."
- DIAMANTI, E., LO, H.-K., QI, B. & YUAN, Z. 2016. Practical challenges in quantum key distribution. *npj Quantum Information*, 2, 1-12.
- BROADBENT, A. & SCHAFFNER, C. 2016. Quantum cryptography beyond quantum key distribution. *Designs, Codes and Cryptography*, 78, 351-382.
- PIRANDOLA, S., ANDERSEN, U. L., BANCHI, L., BERTA, M., BUNANDAR, D., COLBECK, R., ENGLUND, D., GEHRING, T., LUPO, C. & OTTAVIANI, C. 2020. Advances in quantum cryptography. *Advances in optics and photonics*, 12, 1012-1236.

- SHANNON, C. E. 1949. Communication theory of secrecy systems. *The Bell system technical journal*, 28, 656-715.
- PUCELLA, R. 2005. Foundations of cryptography ii: Basic applications.
- SAAD, D. 2004. Information theory, inference, and learning algorithms. *American Scientist*, 92, 578.
- VAN ASSCHE, G. 2006. *Quantum cryptography and secret-key distillation*, Cambridge University Press.
- RIEFFEL, E. G. & POLAK, W. H. 2011. *Quantum computing: A gentle introduction*, MIT Press.
- DIANATI, M. & ALLÉAUME, R. Architecture of the Secoqc quantum key distribution network. 2007 First International Conference on Quantum, Nano, and Micro Technologies (ICQNM'07), 2007. IEEE, 13-13.
- GIRON, A. A., CUSTÓDIO, R. & RODRÍGUEZ-HENRÍQUEZ, F. 2023. Post-quantum hybrid key exchange: a systematic mapping study. *Journal of Cryptographic Engineering*, 13, 71-88.
- NIELSEN, M. A. & CHUANG, I. 2002. Quantum computation and quantum information. American Association of Physics Teachers.
- GISIN, N., RIBORDY, G., TITTEL, W. & ZBINDEN, H. 2002. Quantum cryptography. *Reviews of modern physics*, 74, 145.
- Heisenberg, W., 1985. On the illustrative content of quantum theoretical kinematics and mechanics (pp.478-504). Springer Berlin Heidelberg
- DIRAC, P. A. M. 1926. On the theory of quantum mechanics. *Proceedings of the Royal Society of London. Series A, Containing Papers of a Mathematical and Physical Character*, 112, 661-677.
- EINSTEIN, A., PODOLSKY, B. & ROSEN, N. 1935. Can quantum-mechanical description of physical reality be considered complete? *Physical review*, 47, 777.
- WOOTTERS, W. K. & ZUREK, W. H. 1982. A single quantum cannot be cloned. *Nature*, 299, 802-803.
- WEEDBROOK, C., PIRANDOLA, S., GARCÍA-PATRÓN, R., CERF, N. J., RALPH, T. C., SHAPIRO, J. H. & LLOYD, S. 2012. Gaussian quantum information. *Reviews of Modern Physics*, 84, 621.
- DYNES, J., YUAN, Z., SHARPE, A. & SHIELDS, A. 2007. Practical quantum key distribution over 60 hours at an optical fiber distance of 20km using weak and vacuum decoy pulses for enhanced security. *Optics Express*, 15, 8465-8471.
- ALI, S., MOHAMMED, S., CHOWDHURY, M. & HASAN, A. A. 2012. Practical SARG04 quantum key distribution. *Optical and Quantum Electronics*, 44, 471-482.
- WANG, L.-J., ZOU, K.-H., SUN, W., MAO, Y., ZHU, Y.-X., YIN, H.-L., CHEN, Q., ZHAO, Y., ZHANG, F. & CHEN, T.-Y. 2017. Long-distance

- copropagation of quantum key distribution and terabit classical optical data channels. *Physical Review A*, 95, 012301.
- LI, H.-W., ZHANG, C.-M., JIANG, M.-S. & CAI, Q.-Y. 2022. Improving the performance of practical decoy-state quantum key distribution with advantage distillation technology. *Communications Physics*, 5, 53.
- KRENN, M., MALIK, M., SCHEIDL, T., URSIN, R. & ZEILINGER, A. 2016. Quantum communication with photons. *Optics in our Time*, 18, 455.
- LIAO, S.-K., CAI, W.-Q., LIU, W.-Y., ZHANG, L., LI, Y., REN, J.-G., YIN, J., SHEN, Q., CAO, Y. & LI, Z.-P. 2017. Satellite-to-ground quantum key distribution. *Nature*, 549, 43-47.
- TAKEMOTO, K., NAMBU, Y., MIYAZAWA, T., SAKUMA, Y., YAMAMOTO, T., YOROZU, S. & ARAKAWA, Y. 2015. Quantum key distribution over 120 km using ultrahigh purity single-photon source and superconducting single-photon detectors. *Scientific reports*, 5, 14383.
- BRIEGEL, H.-J., DÜR, W., CIRAC, J. I. & ZOLLER, P. 1998. Quantum repeaters: the role of imperfect local operations in quantum communication. *Physical Review Letters*, 81, 5932.
- SANGOUARD, N., SIMON, C., DE RIEDMATTEN, H. & GISIN, N. 2011. Quantum repeaters based on atomic ensembles and linear optics. *Reviews of Modern Physics*, 83, 33.
- LADD, T. D., JELEZKO, F., LAFLAMME, R., NAKAMURA, Y., MONROE, C. & O'BRIEN, J. L. 2010. Quantum computers. *nature*, 464, 45-53.
- CHILDRESS, L., TAYLOR, J., SØRENSEN, A. S. & LUKIN, M. D. 2005. Fault-tolerant quantum repeaters with minimal physical resources and implementations based on single-photon emitters. *Physical Review A*, 72, 052330.
- AZUMA, K., TAMAKI, K. & LO, H.-K. 2015. All-photonic quantum repeaters. *Nature communications*, 6, 6787.
- WANG, H., TRUSHEIM, M. E., KIM, L., RANIWALA, H. & ENGLUND, D. R. 2023. Field programmable spin arrays for scalable quantum repeaters. *Nature Communications*, 14, 704.
- MA, L., SLATTERY, O. & TANG, X. 2020. Optical quantum memory and its applications in quantum communication systems. *Journal of Research of the National Institute of Standards and Technology*, 125.
- DUAN, L.-M., LUKIN, M. D., CIRAC, J. I. & ZOLLER, P. 2001. Long-distance quantum communication with atomic ensembles and linear optics. *Nature*, 414, 413-418.
- NEUWIRTH, J., BASSET, F. B., ROTA, M. B., ROCCIA, E., SCHIMPF, C., JÖNS, K. D., RASTELLI, A. & TROTTA, R. 2021. Quantum dot technology for

- quantum repeaters: from entangled photon generation toward the integration with quantum memories. *Materials for Quantum Technology*, 1, 043001.
- AZUMA, K., ECONOMOU, S. E., ELKOUSS, D., HILAIRE, P., JIANG, L., LO, H.-K. & TZITRIN, I. 2022. Quantum repeaters: From quantum networks to the quantum internet. *arXiv preprint arXiv:2212.10820*.
- AZEEM, S. A. & SHARMA, S. K. 2017. Study of converged infrastructure & hyper converge infrastructre as future of data centre. *International Journal of Advanced Research in Computer Science*, 8, 900-903.
- Geng, H., 2014. *Data center handbook*. John Wiley & Sons.
- JANSEN, D., KRATTIGER, L. & KAPADIA, S. 2017. *Building Data Centers with VxLAN BGP EVPN: A Cisco NX-OS Perspective*, Cisco Press.
- SANTANA, G. A. 2013. *Data center virtualization fundamentals: understanding techniques and designs for highly efficient data centers with Cisco Nexus, UCS, MDS, and beyond*, Cisco Press.
- ALLSPAW, J. 2008. *The art of capacity planning: scaling web resources*, " O'Reilly Media, Inc."
- BARROSO, L. A., CLIDARAS, J. & HÖLZLE, U. 2013. The datacenter as a computer: An introduction to the design of warehouse-scale machines. *Synthesis lectures on computer architecture*, 8, 1-154.
- MARSHALL, D. 2007. Understanding full virtualization, paravirtualization, and hardware assist. *VMWare White Paper*, 17, 725.
- SOMASUNDARAM, G. & SHRIVASTAVA, A. 2012. Information storage and management: storing, managing, and protecting digital information in classic, virtualized, and cloud environments.
- KUSNETZKY, D. 2011. *Virtualization: A manager's guide*, " O'Reilly Media, Inc."
- WEI, Y. & BLAKE, M. B. 2010. Service-oriented computing and cloud computing: Challenges and opportunities. *IEEE Internet Computing*, 14, 72-75.
- BUYYA, R., RANJAN, R. & CALHEIROS, R. N. Modeling and simulation of scalable Cloud computing environments and the CloudSim toolkit: Challenges and opportunities. 2009 international conference on high performance computing & simulation, 2009. IEEE, 1-11.
- HERBST, N. R., KOUNEV, S. & REUSSNER, R. H. Elasticity in Cloud Computing: What It Is, and What It Is Not. *ICAC*, 2013. 23-27.
- MITCHELL-JACKSON, J., KOOMEY, J. G., NORDMAN, B. & BLAZEK, M. 2003. Data center power requirements: measurements from Silicon Valley. *Energy*, 28, 837-850.
- MAUCH, V., KUNZE, M. & HILLENBRAND, M. 2013. High performance cloud computing. *Future Generation Computer Systems*, 29, 1408-1416.
- ANDROČEC, D. 2015. Research challenges for cloud computing economics. Citeseer.

- ARMBRUST, M., FOX, A., GRIFFITH, R., JOSEPH, A. D., KATZ, R., KONWINSKI, A., LEE, G., PATTERSON, D., RABKIN, A. & STOICA, I. 2010. A view of cloud computing. *Communications of the ACM*, 53, 50-58.
- TOGRAPH, B. & MORGENS, Y. R. 2008. Cloud computing. *Communications of the ACM*, 51, 9-11.
- MATHEW, S. & VARIA, J. 2014. Overview of amazon web services. *Amazon Whitepapers*, 105, 1-22.
- GUPTA, B., MITTAL, P. & MUFTI, T. A review on Amazon web service (AWS), Microsoft azure & Google cloud platform (GCP) services. Proceedings of the 2nd International Conference on ICT for Digital, Smart, and Sustainable Development, ICIDSSD 2020, 27-28 February 2020, Jamia Hamdard, New Delhi, India, 2021.
- ERL, T., MAHMOOD, Z. & PUTTINI, R. 2013. Cloud computing. *Concepts, Technology & Architecture. Massachusetts: Prentice Hall*.
- BRIAIN, D. S. Ó. 2015. Department of Aerospace, Mechanical and Electronic Engineering.
- SHAMUGAM, V., MURRAY, I., LEONG, J. & SIDHU, A. S. Software Defined Networking challenges and future direction: A case study of implementing SDN features on OpenStack private cloud. IOP Conference Series: Materials Science and Engineering, 2016. IOP Publishing, 012003.
- AHMED, S. S., MUSTAFA, A. B. & OSMAN, A. A. 2015. Comparative Study between OSPF and MPLS network using OPNET Simulation. *IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)*, 10, 40.
- TCHOLTCHEV, N. 2019. *Scalable and efficient distributed self-healing with self-optimization features in fixed IP networks*, Technische Universitaet Berlin (Germany).
- CARTHERN, C., WILSON, W., RIVERA, N. & BEDWELL, R. 2015. *Cisco Networks: Engineers' Handbook of Routing, Switching, and Security with IOS, NX-OS, and ASA*, Springer.
- SOFI, E. U. B. & GURM, E. R. K. 2015. Comparative Analysis of MPLS Layer 3vpn and MPLS Layer 2 VPN. *International Journal of Computer Science Trends and Technology (IJCST)*, 3.
- BATAYNEH, M., SCHUPKE, D., HOFFMANN, M., KIRSTAEDTER, A. & MUKHERJEE, B. 2011. Reliable multi-bit-rate VPN provisioning for multipoint carrier-grade Ethernet services over mixed-line-rate WDM optical networks. *Journal of Optical Communications and Networking*, 3, 66-76.
- EDELMAN, J., LOWE, S. S. & OSWALT, M. 2018. *Network Programmability and Automation: Skills for the Next-Generation Network Engineer*, " O'Reilly Media, Inc."

- SOUTHWICK, P., MARSCHKE, D. & REYNOLDS, H. 2011. *Junos Enterprise Routing: A Practical Guide to Junos Routing and Certification*, " O'Reilly Media, Inc."
- SUBRAMANIAN, M., GONSALVES, T. A. & RANI, N. U. 2010. *Network management: principles and practice*, Pearson Education India.
- TOGOU, M. A., CHEKIRE, D. A., KHOUKHI, L. & MUNTEAN, G.-M. 2019. A hierarchical distributed control plane for path computation scalability in large scale software-defined networks. *IEEE Transactions on Network and Service Management*, 16, 1019-1031.
- KREUTZ, D., RAMOS, F. M., VERISSIMO, P. E., ROTHENBERG, C. E., AZODOLMOLKY, S. & UHLIG, S. 2014. Software-defined networking: A comprehensive survey. *Proceedings of the IEEE*, 103, 14-76.
- KUROSE, J. F. & ROSS, K. W. 2007. Computer networking: A top-down approach edition. *Addison Wesley*.
- GRAZIANI, R. 2008. *Routing protocols and concepts: CCNA exploration companion guide*, Pearson Education India.
- Merry Sr, W., 2023. *Virtual networking cybersecurity and vulnerabilities in cloud computing applications: a systematic review* (Doctoral dissertation).
- Etxezarreta, X., Garitano, I., Iturbe, M. and Zurutuza, U., 2023. Software-Defined Networking approaches for intrusion response in Industrial Control Systems: A survey. *International Journal of Critical Infrastructure Protection*, p.100615.
- Roig, P.J., Alcaraz, S., Gilly, K., Bernad, C. and Juiz, C., 2023. Arithmetic Study about Efficiency in Network Topologies for Data Centers. *Network*, 3(3), pp.298-325.
- Rosak-Szyrocka, J., Żywiołek, J. and Shahbaz, M. eds., 2023. *Quality Management, Value Creation, and the Digital Economy*. Taylor & Francis.
- Balasubramanian, P., 2023. Automation in Data Science, Software, and Information Services. In *Springer Handbook of Automation* (pp. 989-1014). Cham: Springer International Publishing.
- Goswami, B., Kulkarni, M. and Paulose, J., 2023. A Survey on P4 Challenges in Software Defined Networks: P4 Programming. *IEEE Access*.
- Kizza, J.M., 2023. Virtualization, Virtual Reality and Ethics. In *Ethical and Secure Computing: A Concise Module* (pp. 255-274). Cham: Springer International Publishing.
- Azariah, W., Bimo, F.A., Lin, C.W., Cheng, R.G., Jana, R. and Nikaein, N., 2022. A survey on open radio access networks: Challenges, research directions, and open source approaches. arXiv preprint arXiv:2208.09125.

- Wenhua, Z., Kamrul Hasan, M., Ismail, A.F., Yanke, Z., Razzaque, M.A., Islam, S. and Anil kumar, B., 2023. Data security in smart devices: Advancement, constraints and future recommendations. *IET Networks*
- Nair, S.S. and Santha, T., 2023. High availability of kernel-based virtual machine using nested virtualization. *Measurement: Sensors*, 26, p.100712.
- Virtanen, J., 2023. Leveraging Kubernetes in Edge-Native Cable Access Convergence.
- Tessinari, R.S., Woodward, R.I. and Shields, A.J., 2023, March. Software-defined quantum network using a QKD-secured SDN controller and encrypted messages. In *Optical Fiber Communication Conference* (pp. W2A-38). Optica Publishing Group.
- Sim, D.H., Shin, J. and Kim, M.H., 2023. Software-Defined Networking Orchestration for Interoperable Key Management of Quantum Key Distribution Networks. *Entropy*, 25(6), p.943.
- Wang, M., Li, J., Xue, K., Li, R., Yu, N., Li, Y., Liu, Y., Sun, Q. and Lu, J., 2023. A segment-based multipath distribution method in partially-trusted relay quantum networks. *IEEE Communications Magazine*.
- Wang, Q., Wang, Z. and Wang, W., 2023. Research on Secure Cloud Networking Plan Based on Industry-specific Cloud Platform. *IEEE Access*.
- Bassi, R., Zhang, Q., Gatto, A., Tornatore, M. and Verticale, G., 2023, April. Quantum Key Distribution with Trusted Relay using an ETSI-compliant Software-Defined Controller. In 2023 19th International Conference on the Design of Reliable Communication Networks (DRCN) (pp. 1-7). IEEE.
- Chen, L.Q., Chen, J.Q., Chen, Q.Y. and Zhao, Y.L., 2023. A quantum key distribution routing scheme for hybrid-trusted QKD network system. *Quantum Information Processing*, 22(1), p.75.
- Luo, Y., Li, Q., Mao, H.K. and Chen, N., 2023. How to Achieve End-to-end Key Distribution for QKD Networks in the Presence of Untrusted Nodes. *arXiv preprint arXiv:2302.07688*.
- Xu, Y., Chen, L. and Zhu, H., 2023. Quantum Key Distribution Scheme with Key Recycling in Integrated Optical Network. *International Journal of Theoretical Physics*, 62(5), p.103.
- Monita, V., Munadi, R. and Irawati, I.D., 2023, March. A Quantum Key Distribution Network Routing Performance Based on Software-Defined Network. In 2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 1121-1125). IEEE.
- Aparicio-Pardo, R., Cousson, A. and Alliche, R.A., 2023, July. Quantum Virtual Link Generation via Reinforcement Learning. In 23rd International Conference on Transparent Optical Networks (ICTON 2023).

- Hajomer, A.A., Derkach, I., Jain, N., Chin, H.M., Andersen, U.L. and Gehring, T., 2023. Long-distance continuous-variable quantum key distribution over 100 km fiber with local local oscillator. arXiv preprint arXiv:2305.08156.
- Mao, Y., Zhu, Y., Hu, H., Luo, G., Wang, J., Wang, Y. and Guo, Y., 2023. Neural Network-Based Prediction for Secret Key Rate of Underwater Continuous-Variable Quantum Key Distribution through a Seawater Channel. *Entropy*, 25(6), p.937.
- Chin, Y.K., Lee, L.K., Bolong, N., Yang, S.S. and Teo, K.T.K., 2011, July. Exploring Q-learning optimization in traffic signal timing plan management. In 2011 third international conference on computational intelligence, communication systems and networks (pp. 269-274). IEEE.
- Liang, B., Liu, R. and Dai, D., 2022. Design of Virtual Machine Scheduling Algorithm in Cloud Computing Environment. *Journal of Sensors*, 2022.
- Alharthi, M., Mohamed, S.H., Yosuf, B., El-Gorashi, T.E. and Elmighani, J.M., 2022, September. Energy-Efficient VM Placement in PON-based Data Center Architectures with Cascaded AWGRs. In 2022 IEEE International Mediterranean Conference on Communications and Networking (MeditCom) (pp. 268-273). IEEE.
- Talwani, S., Singla, J., Mathur, G., Malik, N., Jhanjhi, N.Z., Masud, M. and Aljahdali, S., 2022. Machine-Learning-Based Approach for Virtual Machine Allocation and Migration. *Electronics*, 11(19), p.3249.
- Raghi, K.R., 2022. Virtual Machine Consolidation using Roulette wheel selection Strategy.
- Askar, S. and Keti, F., 2021. Performance Evaluation of different SDN controllers: A Review.
- Askar, S.K., 2016. Adaptive load balancing scheme for data center networks using software defined network. *Science Journal of University of Zakho*, 4(2), pp.275-286.
- Keti, F. and Askar, S., 2015, February. Emulation of software defined networks using mininet in different simulation environments. In 2015 6th International Conference on Intelligent Systems, Modelling and Simulation (pp. 205-210). IEEE.
- Askar, S., 2017. SDN-Based Load Balancing Scheme for Fat-Tree Data Center Networks. *Al-Nahrain Journal for Engineering Sciences*, 20(5), pp.1047-1056.
- Cao, Z., Zhou, X., Wu, X., Zhu, Z., Liu, T., Neng, J. and Wen, Y., 2023. Data Center Sustainability: Revisits and Outlooks. *IEEE Transactions on Sustainable Computing*.

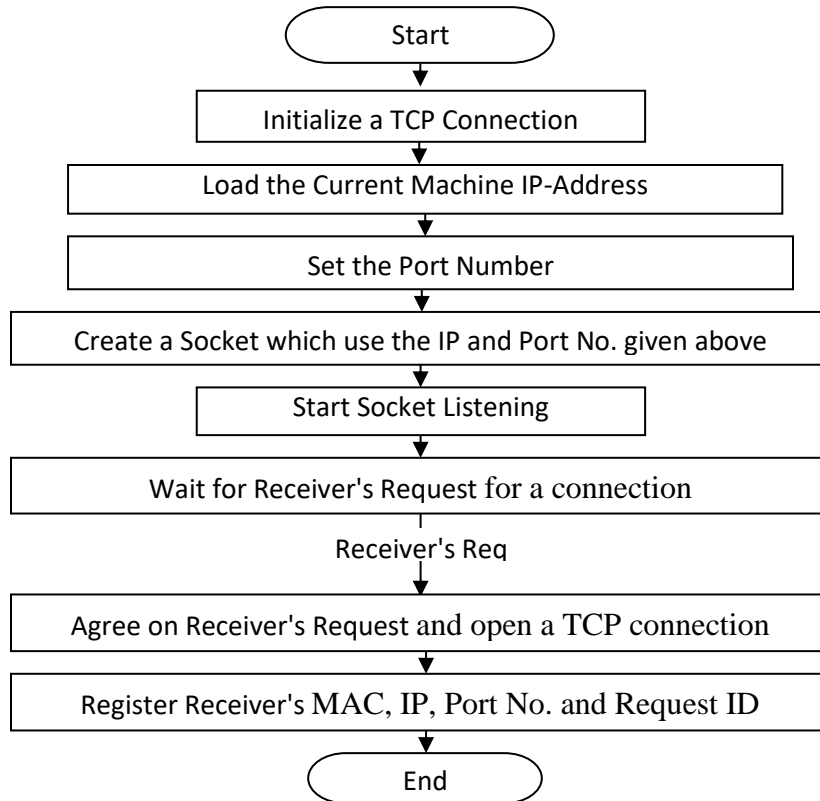
- Khorasi, N., 2021. Software Defined Networking (SDN) Based Solution for Data Center Construct.
- Bezos, J. and Isaacson, W., 2020. Invent and Wander: The Collected Writings of Jeff Bezos, with an Introduction by Walter Isaacson. Harvard Business Press.
- Del Piccolo, V., Amamou, A., Haddadou, K. and Pujolle, G., 2016. A survey of network isolation solutions for multi-tenant data centers. *IEEE Communications Surveys & Tutorials*, 18(4), pp.2787-2821.
- Li, P. and Cao, J., 2023. Virtual Machine Consolidation with Multi-Step Prediction and Affinity-Aware Technique for Energy-Efficient Cloud Data Centers. *Computers, Materials & Continua*, 76(1).
- Alam, S.R., Gila, M., Klein, M., Martinasso, M. and Schulthess, T.C., 2023. Versatile software-defined HPC and cloud clusters on Alps supercomputer for diverse workflows. *The International Journal of High Performance Computing Applications*, p.10943420231167811.
- Aghasi, A., Jamshidi, K., Bohlooli, A. and Javadi, B., 2023. A decentralized adaptation of model-free Q-learning for thermal-aware energy-efficient virtual machine placement in cloud data centers. *Computer Networks*, 224, p.109624.
- Ossen, S., Musser, J., Dalessandro, L. and Swany, M., 2023. INDIANA—In-Network Distributed Infrastructure for Advanced Network Applications. *The International Journal of High Performance Computing Applications*, p.10943420231179662.
- Feng, X., Zhu, X., Han, Q.L., Zhou, W., Wen, S. and Xiang, Y., 2022. Detecting vulnerability on IoT device firmware: A survey. *IEEE/CAA Journal of Automatica Sinica*, 10(1), pp.25-41.
- Tyagi, V. and Singh, S., 2023. Network resource management mechanisms in SDN enabled WSNs: A comprehensive review. *Computer Science Review*, 49, p.100569.
- Turner, S.W., Karakus, M., Guler, E. and Uludag, S., 2023. A Promising Integration of SDN and Blockchain for IoT Networks: A Survey. *IEEE Access*.
- Goldreich, O., 2001. *Foundations of Cryptography: Volume 2, Basic Applications*. Cambridge University Press.
- Maurer, U.M., 1993. Secret key agreement by public discussion from common information. *IEEE Transactions on Information Theory*, 39(3), pp.733-742.
- Renner, R. and König, R., 2005. Universally composable privacy amplification against quantum adversaries. *Advances in Cryptology—CRYPTO 2005*, pp.407-425.
- Scarani, V., Bechmann-Pasquinucci, H., Cerf, N.J., Dusek, M., Lütkenhaus, N. and Peev, M., 2009. The security of practical quantum key distribution. *Reviews of Modern Physics*, 81(3), p.1301.

Nielsen, M.A. and Chuang, I.L., 2002. Quantum Computation and Quantum Information. Cambridge University Press

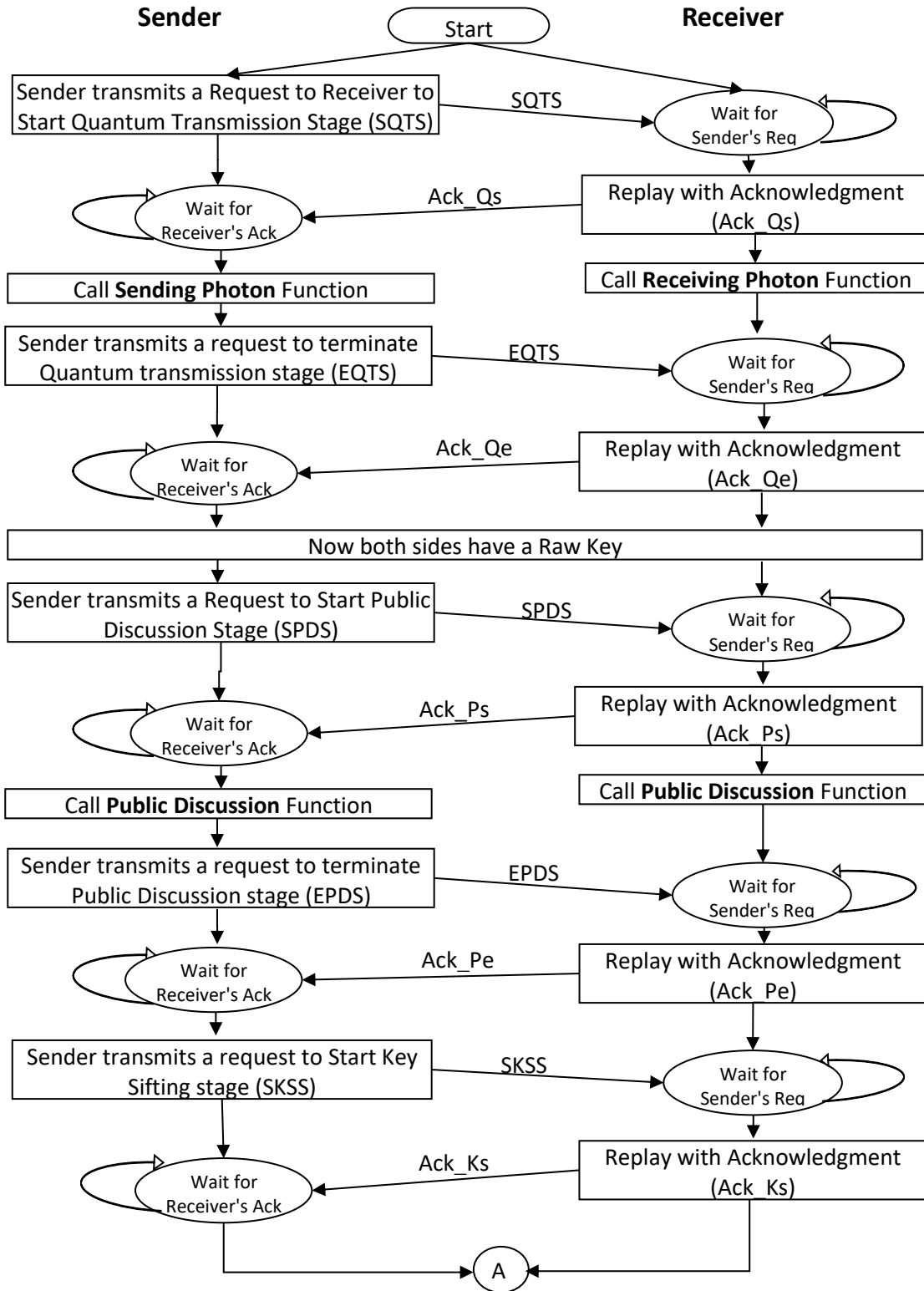
Abdulqadir, D.F., Mustafa, O.S. and Yousef, A.H., 2020. Photon-number Splitting Attack on SARG04 Protocol: An Extended Work. *Polytechnic Journal*, 10(1), pp.157-162.

Appendix A

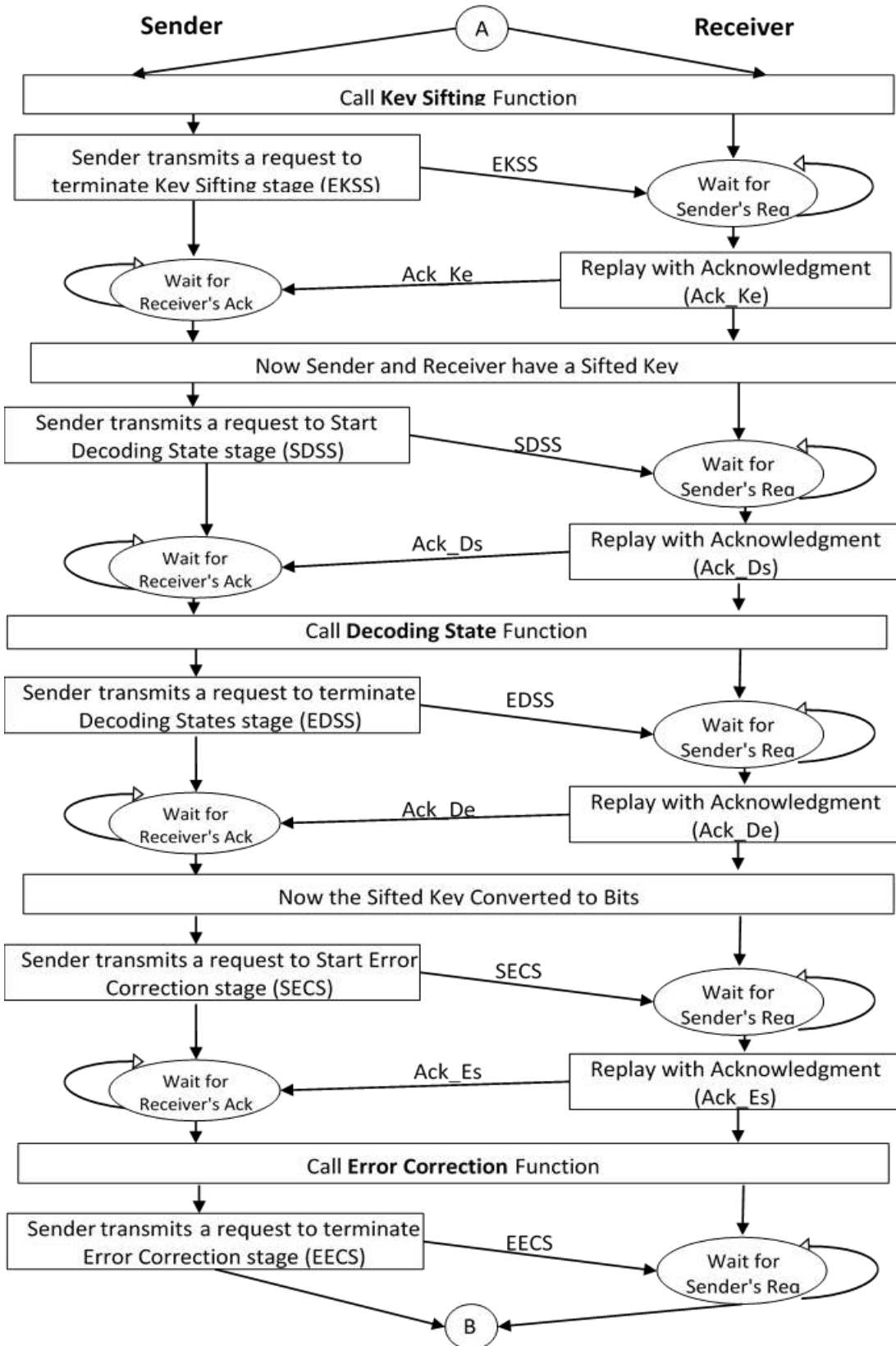
Flowchart A.1 Create a TCP connection



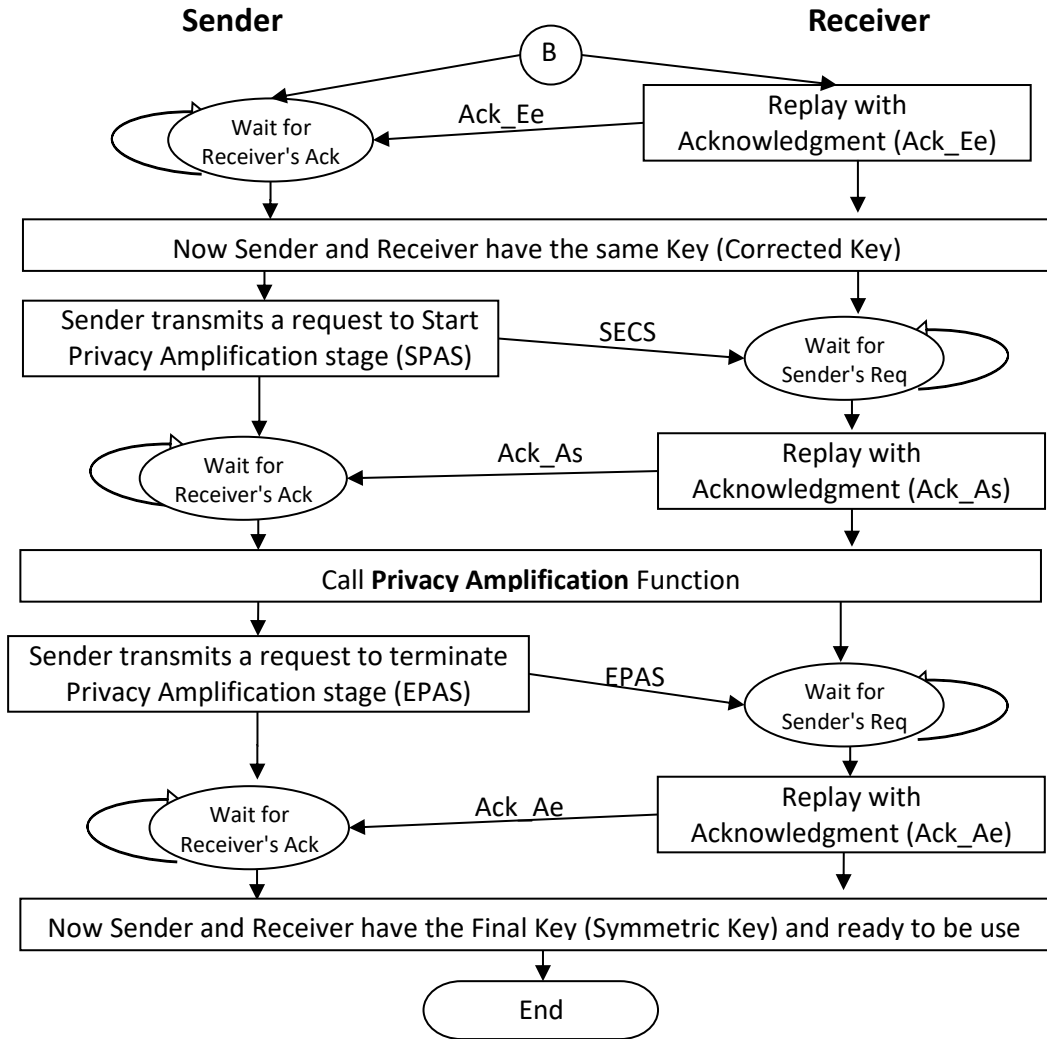
Flowchart A.2 SARAG04 protocol stages through handshake signals



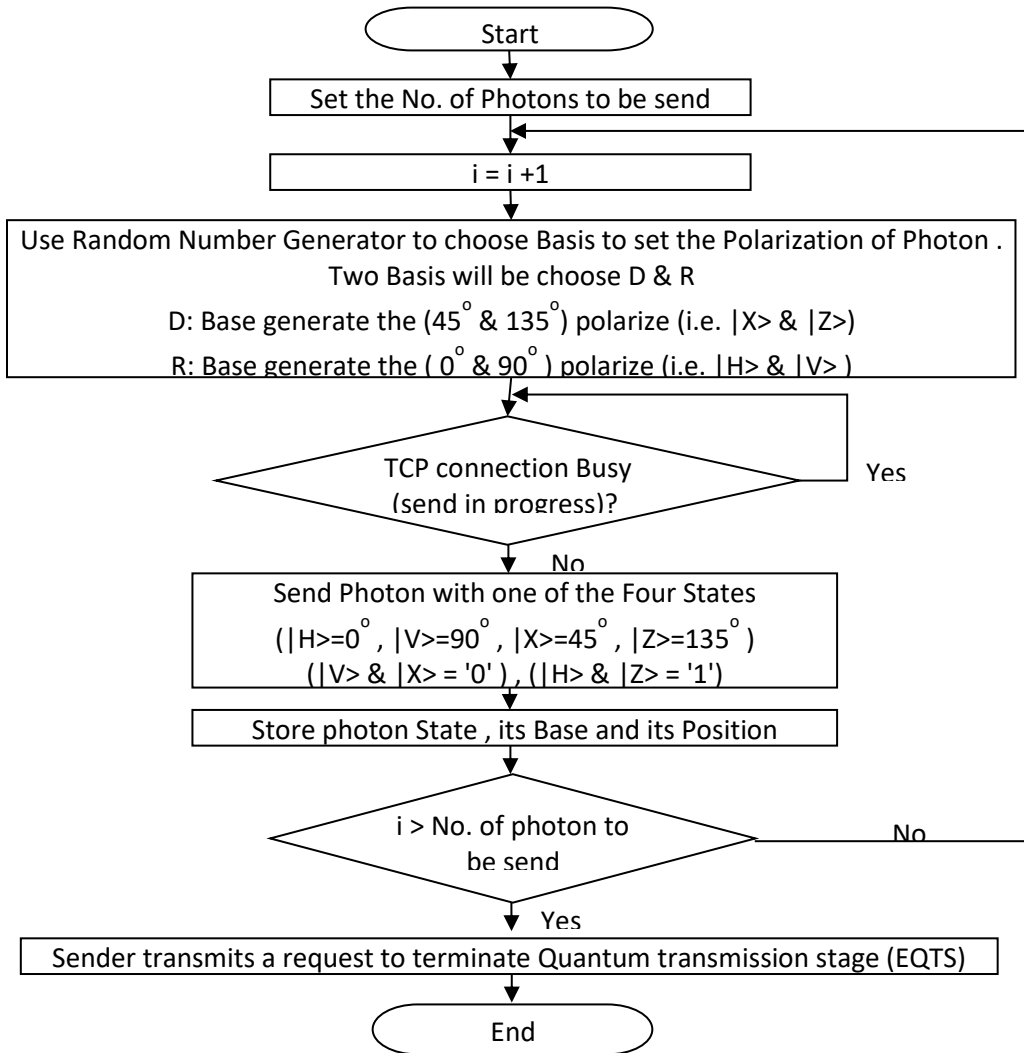
Flowchart A.3 Continuo with (A) handshake signals



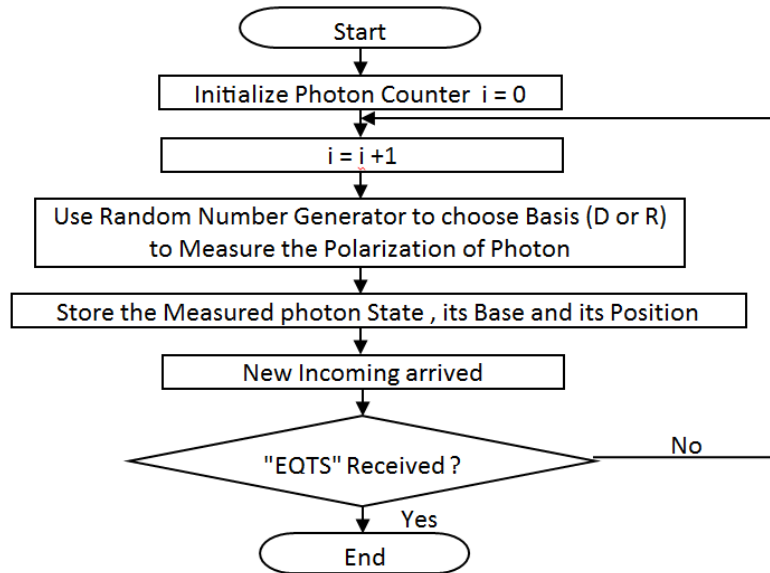
Flowchart A.4 Continuo with (B) handshake signals



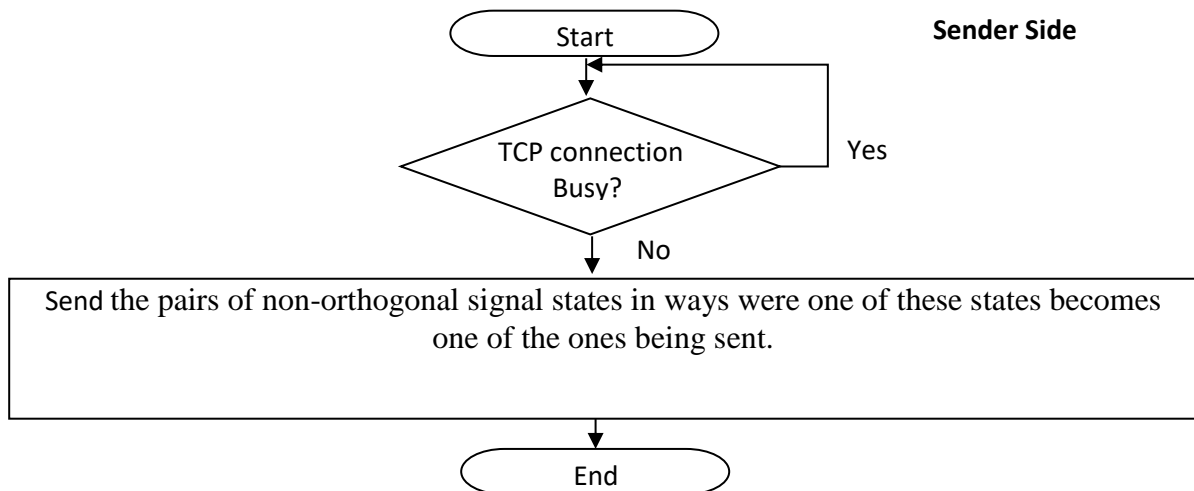
Flowchart 4.5 Quantum transmission stage



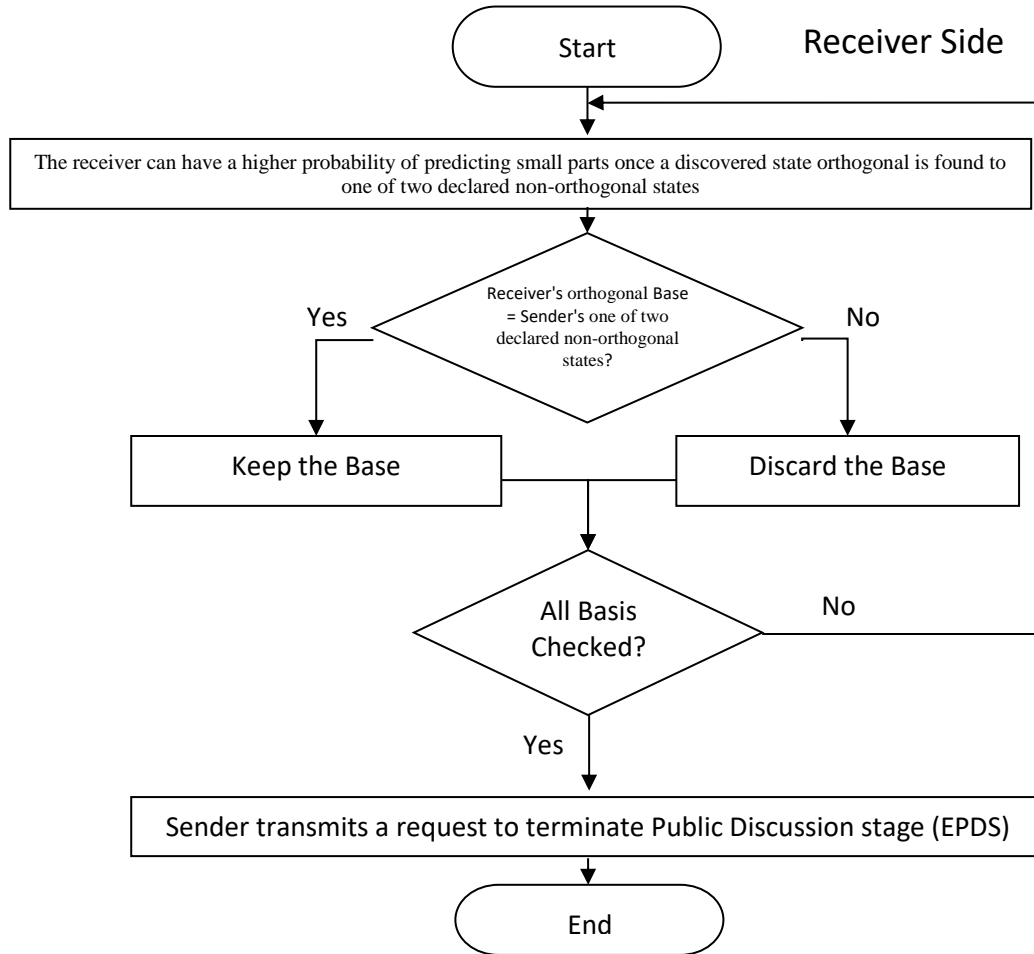
Flowchart 4.6 Receiving sent quantum cases



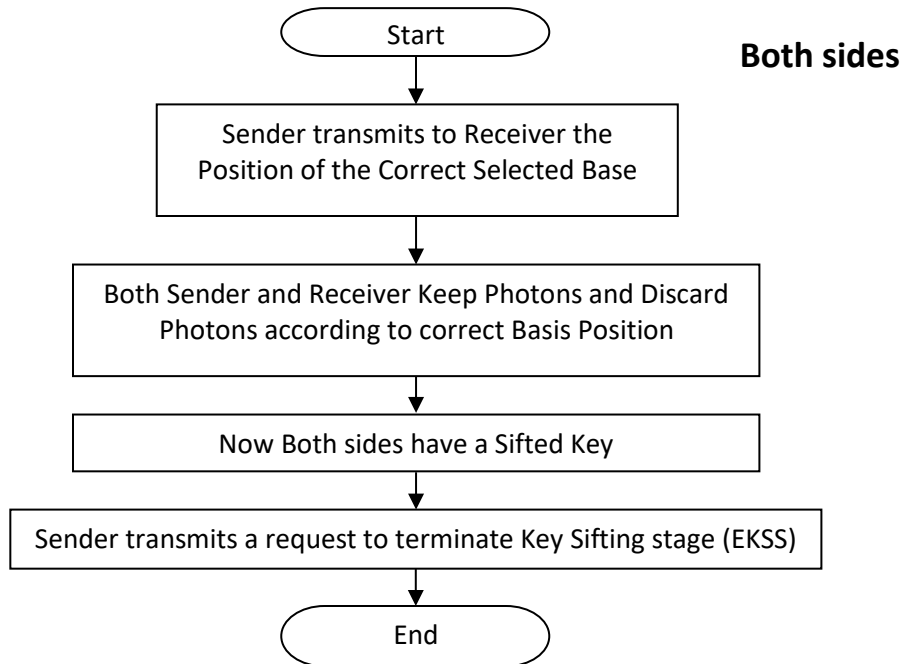
Flowchart 4.7 Bases used in the measurement



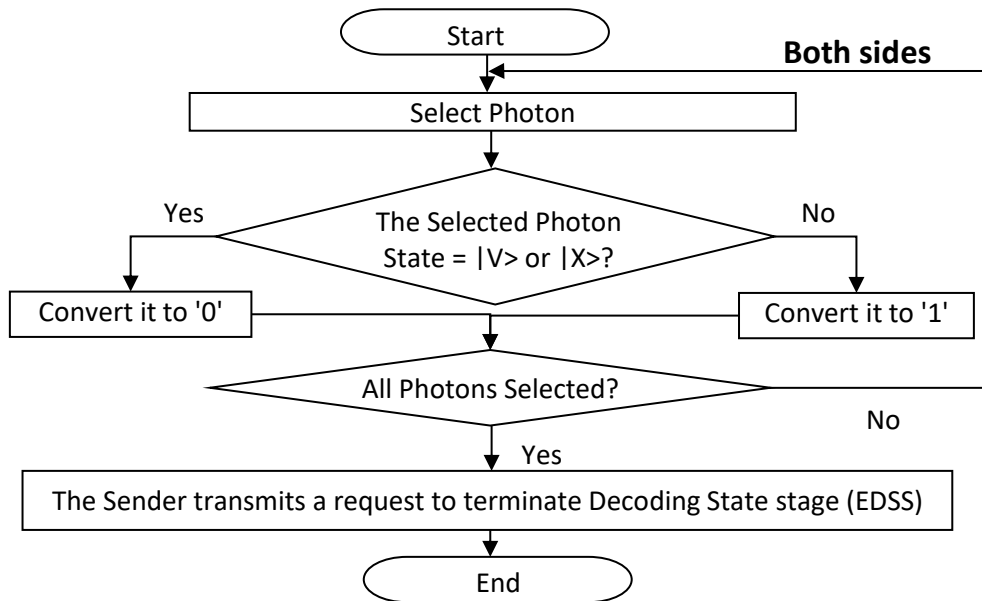
Flowchart 4.8 Check the bases used in the measurement



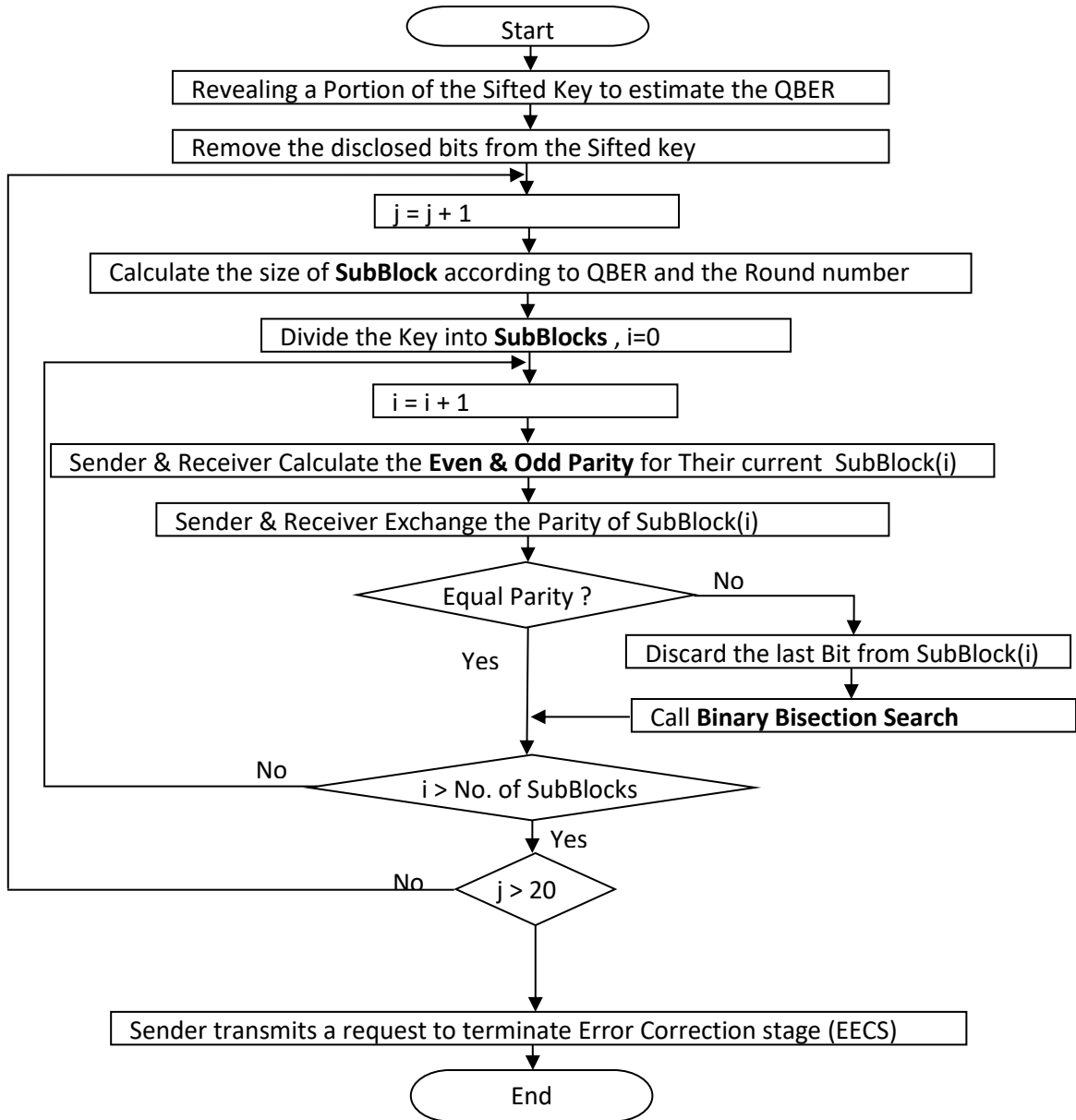
Flowchart 4.9 Depicting raw key sifting stages



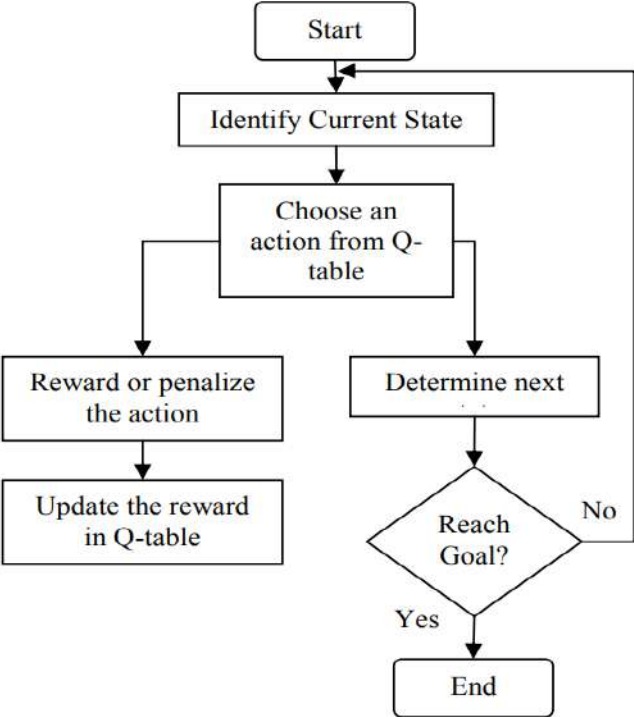
Flowchart 4.10 Process of encoding Qubits



Flowchart 4.11 Steps involved in error correction



Flowchart 4.12 Outlines the Q-Learning algorithm





Title of Paper:

A Novel Security Survival Model for Quantum Key Distribution Networks Enabled by Software-Defined Networking

Published in:

[IEEE Access](#) (Volume: 11)

Date of Publication: 02 March 2023

Electronic ISSN: 2169-3536

INSPEC Accession Number: 22725771

DOI: [10.1109/ACCESS.2023.3251649](https://doi.org/10.1109/ACCESS.2023.3251649)

Publisher: IEEE

IEEE Paper Link: <https://ieeexplore.ieee.org/document/10057401>

Impact Factor: 3.9

 RESEARCH ARTICLE

A Novel Security Survival Model for Quantum Key Distribution Networks Enabled by Software-Defined Networking

OMAR SHIRKO¹, (Graduate Student Member, IEEE),
AND SHAVAN ASKAR², (Senior Member, IEEE)

Department of Information System Engineering, Erbil Polytechnic University, Erbil 44001, Iraq
Corresponding author: Shavan Askar (shavan.askar@epu.edu.iq)

ABSTRACT Quantum key distribution (QKD) is a technique for distributing symmetric encryption keys securely using quantum physics. The rate of key distribution is low and decreases exponentially with increasing distance. A classic trusted relay (CTR) uses additional keys to enhance security distance in QKD networks. In practice, the assurance of security for certain relay nodes is still lacking, despite the fact that CTR requires that all nodes be trusted. Owing to channel unreliability, system faults accumulate during the key relay, thereby increasing the probability of CTR failing to distribute the secret key. The failure of a successful key relay would then result in the subsequent destruction of all the keys involved in the process, which leads to the wasting of the quantum secret key and reduction system encryption. Hence, alleviating the effect of CTR failure for the purpose of obtaining key security distribution of distant quantum network is necessary issue to tackle. Therefore, a new scheme is needed in order to overcome the above-mentioned issues to come up with a better utilization of the generated keys. In this study, a software-defined networking (SDN) technique is introduced to circumvent this drawback by utilising the flexibility provided by the SDN paradigm for better QKD network management. In particular, a novel survivability model called software-defined quantum key relay failure (SDQKRF) is proposed in this paper in which a new function is developed and added to the SDN controller. According to the simulation results, SDN over a QKD network using the SDQKRF model is more reliable and performs better in terms of the key generation ratio, key utilisation rate, recovery after failure, avalanche effect, and service blocking rate than a regular QKD network without the SDQTRF model.

INDEX TERMS Quantum key distribution (QKD), software-defined network (SDN), survivability, classical trusted relay (CTR).

I. INTRODUCTION

It is expected that by 2023, approximately two-thirds of the world population will have Internet access, this suggests that the amount of Internet users is estimated to will increase from 3.9 billion (51% of the world population) in 2018 to 5.3 billion (66% of the world population) in 2023 [1]. The increase in internet access will lead to an increase in the number of security breaches such as eavesdropping and data

interception, which consequently can result in the loss of personal information, financial losses, and significant disruptions to services [2], [3]. Therefore, cryptographic techniques became an inevitable alternative to ensure the safety of communication carried out through the internet [4]. However, one of the most essential cryptographic tasks is to establish secure cryptographic keys across untrusted networks [5]. Traditionally, encryption methods based on public-key cryptography have been used, enabling cryptographic keys to be distributed over unreliable networks. Although public-key cryptography security relies on the computational complexity

The associate editor coordinating the review of this manuscript and approving it for publication was Abderrahmane Lakas³.

پوخته

دابه‌شکردنی کللی کوانتتم (QKD) نوین‌رایتی به‌کارهینانیکي پیش‌کوتووی فیزیای کوانتتم دهکات بو دابه‌شکردنی کللی کؤدکردنی هوسهنگی پاریزراو. نهم شیوازه تاییه‌تمه‌ندییه ناوازه‌کانی میکانیکي کوانتتم وهک تیورمی بی کلونکردن و بنه‌مای نادلنایی هاین‌نییرگ دهقوزیتتهوه بو دروستکردنی کللی پاریزراو له بنه‌رندا که بهرگریان له گوینگرتن له گوینگرتن هه‌یه. به‌لام ته‌هدای سهرمی که‌مبوونه‌وی ریژه‌بی ریژه‌ی دابه‌شکردنی سهرمکیه له‌گه‌ل زیادبوونی مه‌وداکان. بو دریزکردنه‌وی مه‌ودای په‌یوه‌ندی پاریزراوی توره‌کانی QKD، پلانیکي کلاسیک متمانه‌پیکراوی ریله‌ی (CTR) پیشنیار کراوه، که گری نیوان متمانه‌پیکراو بو بهرزکردنه‌وی ناسایش له دوریدا دناسینیت. سهر‌رای ئه‌وش، نیگهرانییه‌کان سه‌بارت به‌پیداویستییه‌کانی متمانه له گریکانی ریله‌ی و متمانه‌پیکراوی که‌نالی په‌یوه‌ندیکردن مه‌ترسییه‌کی به‌رچاو دروست ده‌کن، که نه‌گهری هه‌یه بیته هوی شکستی CTR و سازشکردنی گشتی ناسایشی سیستهم.

نهم دیزمه‌تیشنه ریپازیکی نوئ ده‌خاته روو که باس له ته‌هددیاتی شکستی CTR و باشکردنی به‌کارهینانی کللی دروستکراو دهکات. چاره‌سهرمه‌که توری پیناسه‌کراوی نهرمه‌کالا (SDN) له‌گه‌ل QKD تیکه‌ل دهکات، که سوود له نهرمی و کؤنترؤلکردنی SDN وهرده‌گریت بو باشترکردنی به‌ریوه‌بردنی تور SDN. که تورمه‌که دابه‌ش دهکات به‌سهر فرؤکه‌ی کؤنترؤل و داتا، به‌ریوه‌بردن و به‌رنامه‌سازی به‌گرتوو پیشکمش دهکات. بو بهرزکردنه‌وی خورگری و متمانه‌پیکراوی توری QKD، مؤدیلی شکستی ریله‌ی متمانه‌پیکراوی کوانتته‌می پیناسه‌کراوی نهرمه‌کالا (SDQTRF) پیشنیار کراوه. نهم مؤدیله فه‌نکشنیکی نویی کؤنترؤلکهری SDN به‌کارده‌هینیت بو ری‌کخستنی کاریگهرانه‌ی کاره‌کانی توری QKD. به‌یکخستنی تواناکانی SDN، مؤدیلی SDQTRF لیپورده‌یی هه‌له و توانای سیستهمه‌که بو چاکبوونه‌وه له شکستی ریله‌ی بهرز دهکاته‌وه. کؤنترؤلکهری SDN چالاکانه چاودیری توری QKD دهکات، له‌وانه‌ش دؤخی گری ریله‌ی و پرؤسه‌کانی دابه‌شکردنی کللی. له‌گه‌ل دیاریکردنی شکستی ریله‌ی، کؤنترؤلکهری SDN به‌شیوه‌یه‌کی چالاکانه وه‌لام ده‌داته‌وه به ری‌کخستنه‌وی تورمه‌که له ریگه‌ی ریسیاکلکردنی کلله‌کانه‌وه به به‌کارهینانی Q-learning. نهم ریسیاکلکردن شکستی هینا، کؤنترؤلکهرمه‌که پرؤسه‌ی دابه‌شکردنی کلله‌کان له ریگه‌ی ریروه‌ی به‌دیله‌وه که به شیوازی فیروبونی Q دیاریکراون، ریروه ده‌گوریت. نهم ریپازه چالاکه کاریگهری شکستی ریله‌ی کهم دهکاته‌وه، دابه‌شکردنی به‌رده‌وامی کلله‌کان مسوگهر دهکات، و ناسایشی سیستهم ده‌پاریزیت.

بۆ ھەئسەنگاندنی کاریگەری مۆدیلی SDQTRF، ھاوشیوھکردنی بەرفراوان لەسەر دوو توپۆلۆژیای تۆری جیاواز ئەنجامدرا: تۆری بنەمای زانستی نیشتمانی (NSFNET) و تۆری ئەمریکا (USNET). ھاوشیوھکردنەکان GPU ی NVIDIA GeForce RTX 3060Ti ی کارایی بەرزیان بەکارھێنا و لەسەر سیستمی کاریگەری ویندۆز ۱۱ کاردەکرد، کە سەقامگیری دابین دەکرد. بۆ ھاوشیوھکردنی مۆدیلی پیشنیارکراوی SDQTRF، زمانەکانی بەرنامەسازی جاڤاسکرپت، PHP و پایتۆن بە بەکارھێنانی کتیبخانەیی NetworkX بەکارھێنران بەھۆی نەرمی و کتیبخانە بەرفراوانەکانیان بۆ کۆمپیوتەری زانستی و ھاوشیوھکردنی تۆر. ئەنجامەکانی ھاوشیوھکردن ناماژە بە باشتربوونی بەرچاو دەکەن، لەوانەش زیادبوونی بەرچاو لە ریزەیی نەوێ کلێل، بەرزبوونەوێ ریزەیی بەکارھێنانی کلێلەکانی سەرنجراکێش، چاکبوونەوێ سەرنجراکێش دوای ریزەیی شکست، کەمبوونەوێ بەرچاو لە کاریگەری بەفربارین، و ریزەیی کەمتری بلۆککردنی خزمەتگوزاری بەھۆی جێبەجێکردنی مۆدیلی SDQTRF.



حکومەتی هەریمی کوردستان – عێراق
سەرۆکایەتی ئەنجومەنی وەزیران
وەزارەتی خویندنی باڵا و تووژینهووی زانستی
زانکۆی پۆلیتەکنیکی هەولێر
کۆلیژی تەکنیکی ئەندازیاری
بەشی ئەندازیاری سیستەمی زانیاری

تێزیکە

پیشکەشی ئەنجومەنی کۆلیژی تەکنیکی ئەندازیاری کراوە لە زانکۆی پۆلیتەکنیکی هەولێر وەکو بەشێک لە
پیداویستیهکانی بەدەست هێنانی پلەي دکتورا ئەندازیاری سیستەمی زانیاری

لەلایەن

عمر شیرکو مصطفی

ماستەر لە تەکنەلۆژیای زانیاری

بەسەرپەرشتیاری

پروفیسۆری دکتۆر شیفان کمال اسکار

هەولێر - کوردستان

رێبەندان ٢٠٢٣