ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 9, Issue 3, April 2024

SDN ENABLED EMPLOYEE'S NOVEL SECURITY SURVIVAL WITH QUANTUM KEY DISTRIBUTION

[1] Sugavanam M, [2] Balaji S [2]
Master of Engineering In Computer Science And Engineering
[2] Students, Department Of Cse, Kingston Engineering College, Vellore - 632 059, Tamil Nadu, India
[2] Assistant Professor, Department Of Cse, Kingston Engineering College, Vellore - 632 059, Tamil Nadu, India
[1]msugavanam5@Gmail.Com

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. To ensure secured data transmission there are several techniques being followed. One among them is cryptography which is the practice and study of hiding information. The proposed method is Back Track-ASCII algorithm, this is a new cryptographic algorithm which is used for secure the data in cloud. Encryption and decryption require the use of some secret information, usually referred to as a hash key. 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 ECC algorithm is used to generate the key. The data to be encrypted is called as plain text. The plain text is converted into ASCII code, which is added to ASCII code of cover message which is generated by Backtrack algorithm, also the key is added to these. The encrypted data obtained as a result of encryption process is called as cipher text. Depending on the encryption mechanism used, the same key might be used for both encryption and decryption, while for other mechanisms, the keys used for encryption and decryption might be different. Each encryption algorithm can be decrypted within sufficient time and with sufficient resources. The possibility of decryption has increased with the development of computer technology since available computer speeds enable the decryption process based on the exhaustive data search. This has led to the development of steganography, a science which attempts to hide the very existence of confidential information. Hence, a new method which combines the favourable properties of cryptography based on substitution encryption and stenography is analysed in the paper.***

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

I. INTRODUCTION

It is expected that by 2024, 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 2024. 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. Therefore, cryptographic techniques became an inevitable alternative to ensure the safety of communication carried out through the internet. However, one of the most essential cryptographic tasks is to establish secure cryptographic keys across untrusted networks. 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 of mathematical functions, the rapid growth of processor chips and quantum computers has rendered communication security far less reliable. Quantum key distribution (QKD) is one of the most promising alternatives to traditional data encryption methods.

ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 9, Issue 3, April 2024

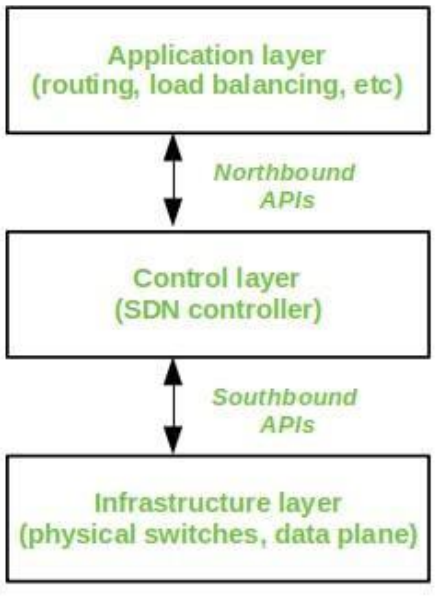

Fig. No 2.1 SDN Architecture

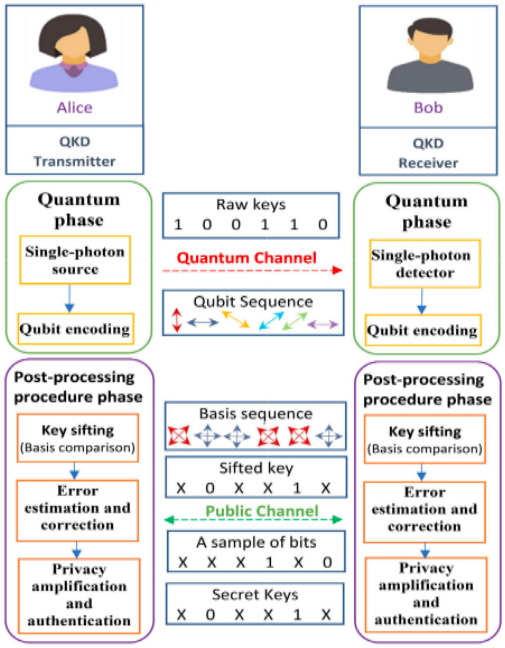

Fig. No 2.2 point-to-point QKD

3. LITERATURE SURVEY

3.1 Key on demand (KoD) for software-defined optical networks secured by quantum key distribution (QKD). Author: Yuan Cao, Yongli Zhao. **Year of Publishing: 2017**

Software-defined optical networking (SDON) will become the next generation optical network architecture. However, the optical layer and control layer of SDON are vulnerable to cyberattacks. While, data encryption is an effective method to minimize the negative effects of cyberattacks, secure key interchange is its major challenge which can be addressed by the quantum key distribution (QKD) technique. Hence, in this paper we discuss the integration of QKD with WDM optical networks to secure the SDON architecture by introducing a novel key on demand (KoD) scheme which is enabled by a novel routing, wavelength and key assignment (RWKA) algorithm.

3.2 A Quantum Cryptography Communication Network Based on Software Defined Network .
Author: Hongliang Zhang, Dongxiao Quan. **Year of Publishing: 2018**

Development of the Internet, information security has attracted great attention in today's society, and quantum cryptography communication network based on quantum key distribution (QKD) is a very important part of this field, since the quantum key distribution combined with one-time-pad encryption scheme can guarantee the unconditional security of the information. The secret key generated by quantum key distribution protocols is a very valuable resource, so making full use of key resources is particularly important.

3.3 Quantum-Key-Distribution (QKD) Networks Enabled by Software-Defined Networks (SDN).
Author: Hua Wang , Yongli Zhao. **Year of Publishing: 2018**

As an important support for quantum communication, quantum key distribution (QKD) networks have achieved a relatively mature level of development, and they face higher requirements for multi-user end-to-end networking capabilities. Thus, QKD networks need an effective management plane to control and coordinate with the QKD resources. As a promising technology, software defined networking (SDN) can separate the control and management of QKD networks from the actual forwarding of the quantum keys.

3.4 A security model for preserving the privacy of medical big data in a healthcare cloud using a fog computing facility with pairing based cryptography. Author: H. A. A. Hamid. **Year of Publishing: 2020**

Nowadays, telemedicine is an emerging healthcare service where the healthcare professionals can diagnose, evaluate, and treat a patient using telecommunication technology. To diagnose and evaluate a patient, the healthcare professionals need to access the electronic medical record (EMR) of the patient, which might contain huge multimedia big data including x-rays, ultrasounds, CT scans, MRI reports, etc. For efficient access and supporting mobility for both the

healthcare professionals as well as the patients, the EMR needs to be kept in big data storage in the healthcare cloud. In spite of the popularity of the healthcare cloud, it faces different security issues; for instance, data theft attacks are considered to be one of the most serious security breaches of healthcare data in the cloud. In this paper, the main focus has been given to secure healthcare private data in the cloud using a fog computing facility.

3.5 Quantum Key Distribution Over a Channel with Scattering. Author: Qi-Hang Lu, Fang-Xiang Wang. Year of Publishing: 2021

Scattering of light by cloud, haze, and fog decreases the transmission efficiency of communication channels in quantum key distribution (QKD), reduces the system's practical security, and thus constrains the deployment of free-space QKD. Here, we employ wave-front shaping technology to compensate distorted optical signals in high-loss scattering quantum channels and fulfill a polarization-encoded BB84 QKD experiment. With this quantum-channel compensation technology, we achieve a typical enhancement of about 250 in transmission efficiency and build a secure communication link even considering finite key length effect, while the link is impossible to share secure keys before optimization. The method applied in the QKD system shows the potential to expand the application range of QKD systems from lossless channels to highly scattered ones and therefore enhances the deployment ability of a global quantum communication network.

4. RESEARCH AND METHODOLOGIES

4.1 Proposed System

The proposed method is BackTrack-ASCII algorithm, which consists of the following process,

1. Cover Message Generation - **Backtracking Algorithm**
2. Secret Key Generation (Sk) - **ECC Hashing Algorithm**
3. Mixing Operation - **ASCII Steganography**
    a) ASCII code generation for Secret Message (As)
    b) ASCII code generation for Cover Message (Ac)
    c) Stego-message generation (Sm) = As + Ac + Sk
4. Secret Message Extraction - **ASCII Steganography**
    a) Secret Key Verification
    b) Separating Secret Key (Ss) = Sm - Sk
    c) Original Message (m) = Ss - Ac

Advantages

- The security of quantum communication is guaranteed by the quantum no-cloning theorem and the quantum uncertainty principle to prevent eavesdroppers from unconditional attacks.
- Authentication is considered necessary as a defense against active attacks.

5. MODULES DESCRIPTION

1. HIDING SENDER
2. HIDING MESSAGE
3. MESSAGES TRANSMISSION
4. DECRYPT THE MESSAGE
5. DECRYPT THE RECEIVER

The detailed description of the modules are ,

1. Hiding Sender

In the present world scenario it is difficult to transmit data from one place to another with security. This is because hackers are becoming more powerful nowadays. To ensure secured data transmission there are several techniques being followed. One among them is cryptography which is the practice and study of hiding information.

2. Hiding Message

In this technique the first step is to assign a unique color for each receiver. Each color is represented with a set of three values. For example violet red color is represented in RGB format as (238, 58,140). The next step is to assign a set of three key values to each receiver.

At the receiver's side, thereceiver is aware of his own color and other key values.

3. Message Transmission

There are many types of encryptions and not all of it is reliable. The same computer power that yields strong encryption can be used to break weak encryption schemes. Initially, 64-bit encryption was thought to be quite strong, but today 128-bit encryption is the standard, and this will undoubtedly change again in the future.

4. Decrypt the Message

ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 9, Issue 3, April 2024

Encrypt provides symmetric encryption functionality via the CryptoKey object. CryptoKey's core methods, EncryptFile, DecryptFile, EncryptText and DecryptText, allow you to implement file and text encryption in your application in just a few lines of code.

An instance of the CryptoKey object is created using CryptoContext's methods GenerateKey and GenerateKeyFromPassword.

5. Decrypt the Receiver

Decryption involves the process of getting back the original data using decryption key. The data given by the receiver (the color) is matched with the data stored at the sender's end. For this process the receiver must be aware of his own color being assigned and the key values.

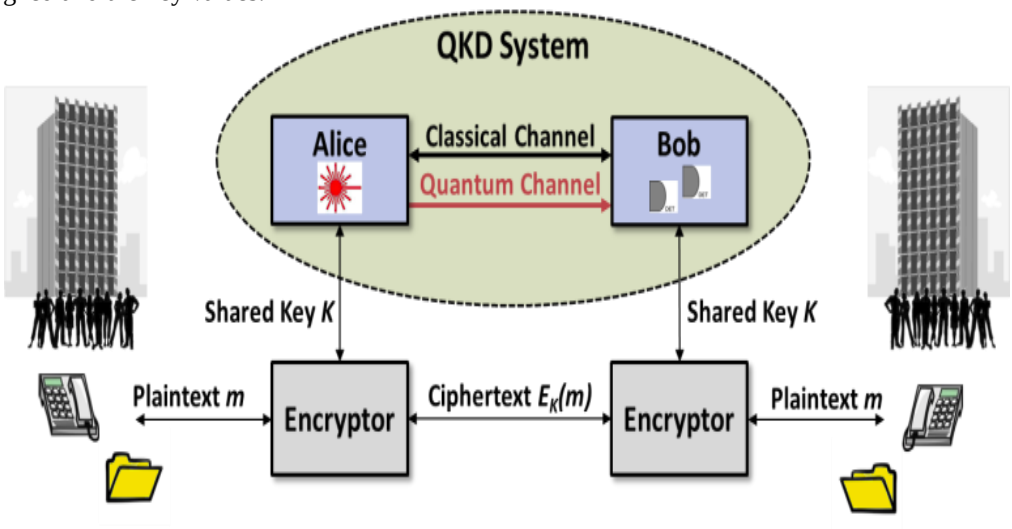

Fig. No 5.1 QKD Transition

6. RESULT

6.1 INPUT/OUTPUT WORKING MODEL:

Steps:

1. Sender Send the Message Word to Text Paragraph Message.
2. SDN Controller Provide the Processing Algorithm In Network.
3. Cover Message Generation **-Backtracking Algorithm**
4. Secret Key Generation **ECC Hashing Algorithm**
5. **Secret Message and Cover Message** Combine in **ASCII Steganography** Mixing Point.
6. Transfer in **QKD Network Using CTR**

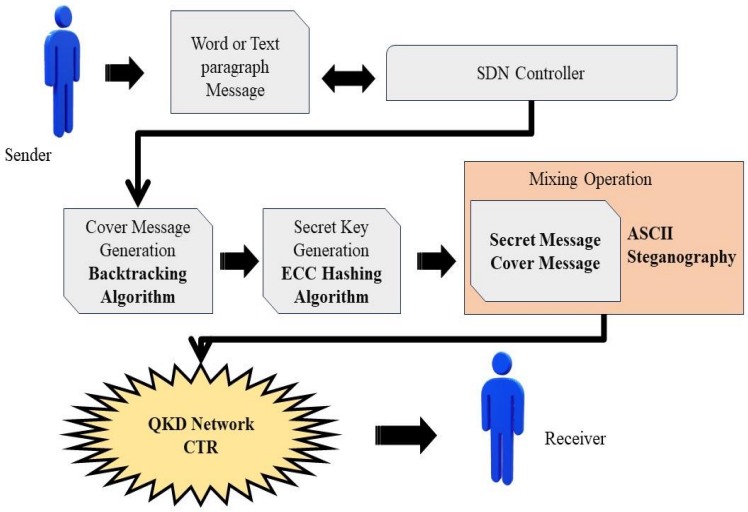

Fig. No 6.1 Input/Output Working Model

ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 9, Issue 3, April 2024

6.2 PERFOMANCE EVALUATION:

1. Encoding Time

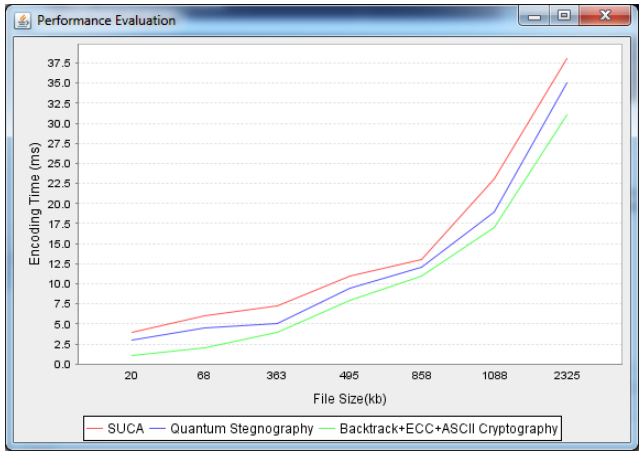

Fig. No 6.2.1

2. Memory Usage

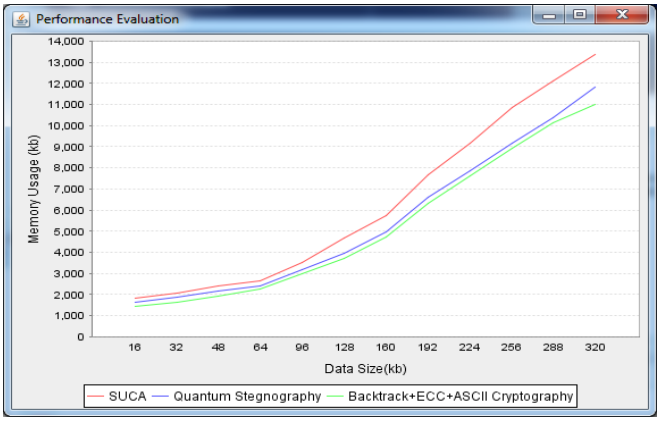

Fig. No 6.2.2

3. Security Probability

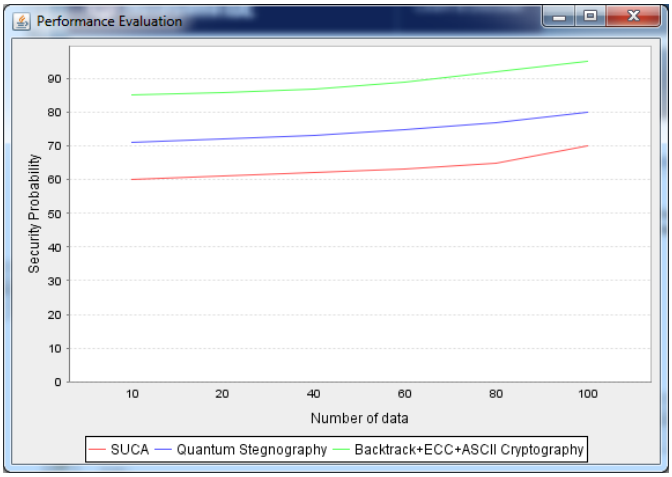

Fig. No 6.2.3

7. CONCLUSION

Currently, the CTR technology is the preferred practical solution for sending quantum information over long distances. However, if the security of certain CTR nodes unable to be guaranteed in practical systems, the CTR technique can be regarded as unreliable for the remote distribution of quantum keys. However, to minimise the impact of CTR on the QKD

network, an efficient survivability model called SDQTRF was proposed in this study. With the help of the proposed new relay protocol, a new function has been proposed called the ‘‘Contingency Function’’ inside the SDN controller to improve key management in the case of an unsuccessful relay key. The quantity of recycling is determined using Q-learning for security improvements of the recycling process. To increase the survivability of the QKD network, a novel concept for finding a new secure path based on the Q-learning method was developed. In terms of KGR, KUR, RAF, AETF, and SBR, the performance of the proposed model was compared with and without utilisation of the SDQTRF model. To examine the effectiveness of the proposed SDQTRF, simulations were performed on two networks, NSFNET and USNET. Regardless of the values of KGR, KUR, RAF, AETF, and SBR, the simulation results indicate that the proposed SDQTRF model is superior to the system without the SDQTRF model. The SDQTRF model could be improved in the future by considering certain aspects that should be taken into account. Instead of excluding some CTR nodes when searching for a new secure path, the SDQTRF model can be used to overcome or assess the major reasons for CTR technology failure. In addition, owing to the high resource requirements of the Q-table, Q-learning cannot be utilised directly to enhance network routing. Therefore, the deep Q-learning approach can be used to enhance the SDQTRF model instead of the Q-learning method. The reason for this is that deep Q-learning employs neural networks to calculate Q-values instead of regular Q-tables, leading to more precise results.

8. REFERENCES

[1] Cisco. (Mar. 9, 2020). *Cisco Annual Internet Report—Cisco Annual Internet Report (2018–2023) White Paper*. [Online]. Available: https:// www.cisco.com/c/en/us/solutions/collateral/executive- perspectives/annual-internet-report/white-paper-c11-741490.html

[2] N. Skorin-Kapov, M. Furdek, S. Zsigmond, and L. Wosinska, ‘‘Physical- layer security in evolving optical networks,’’ *IEEE Commun. Mag.*, vol. 54, no. 8, pp. 110–117, Aug. 2016, doi: 10.1109/MCOM.2016.7537185.

[3] M. Furdek, N. Skorin-Kapov, S. Zsigmond, and L. Wosinska, ‘‘Vulnerabilities and security issues in optical networks,’’ in *Proc. 16th Int. Conf. Transparent Opt. Netw. (ICTON)*, Jul. 2014, pp. 1–4, doi: 10.1109/ICTON.2014.6876451.

[4] H. Dong, Y. Song, and L. Yang, ‘‘Wide area key distribution network based on a quantum key distribution system,’’ *Appl. Sci.*, vol. 9, no. 6, p. 1073, Mar. 2019, doi: 10.3390/app9061073.

[5] M. Mehic, M. Niemiec, S. Rass, J. Ma, M. Peev, A. Aguado, V. Martin,
S. Schauer, A. Poppe, C. Pacher, and M. Voznak, ‘‘Quantum key distribu- tion: A networking perspective,’’ *ACM Comput. Surv.*, vol. 53, pp. 1–41, Sep. 2020.

[6] P. Sharma, A. Agrawal, V. Bhatia, S. Prakash, and A. K. Mishra, ‘‘Quantum key distribution secured optical networks: A survey,’’ *IEEE Open J. Commun. Soc.*, vol. 2, pp. 2049–2083, 2021, doi: 10.1109/OJCOMS.2021.3106659.

[7] H.-K. Lo, M. Curty, and K. Tamaki, ‘‘Secure quantum key distribution,’’
Nature Photon., vol. 8, no. 8, pp. 595–604, Aug. 2014.

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

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

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

[11] H.-K. Lo, M. Curty, and B. Qi, ‘‘Measurement-device-independent quan- tum key distribution,’’ *Phys. Rev. Lett.*, vol. 108, no. 13, Mar. 2012, Art. no. 130503.

[12] Y.-L. Tang, H.-L. Yin, Q. Zhao, H. Liu, X.-X. Sun, M.-Q. Huang,
W.-J. Zhang, S.-J. Chen, L. Zhang, L.-X. You, Z. Wang, Y. Liu, C.-Y. Lu,

[13] Jiang, X. Ma, Q. Zhang, T.-Y. Chen, and J.-W. Pan, ‘‘Measurement- device-independent quantum key distribution over untrustful metropolitan network,’’ *Phys. Rev. X*, vol. 6, no. 1, Mar. 2016, Art. no. 011024.