Simulation of Quantum Channel and Analysis of Its State Under Network Disruption

Chapter · January 2020

DOI: 10.1007/978-981-15-0199-9_51

s. Praveen Kumar
SRM Institute of Science and Technology
49 PUBLICATIONS **530** CITATIONS
SEE PROFILE

Ananya Banerjee
VIT University
1 PUBLICATION **0** CITATIONS
SEE PROFILE

Jaya T J
Vels University
44 PUBLICATIONS **86** CITATIONS
SEE PROFILE

Simulation of Quantum Channel and Analysis of Its State Under Network Disruption

S. Praveen Kumar, Aishwarya Balaje, Ananya Banerjee, Induvalli, T. Jaya and Sonali Sharma

Abstract Presently the work done in the field of quantum cryptography is primarily theoretical, the purpose of this paper is to showcase its implementation in an observable manner. Thus, this paper establishes a more secure network using quantum key distribution (QKD) for data transfer between sender and receiver and also enables the quick identification of an eavesdropper in the said network. An analysis of the quantum channel traffic at the ideal state and also during network disruption (i.e. when the quantum state collapses) has been carried out. Due to the complex nature of quantum networks, a physical implementation of the same is not feasible. Hence, a simulation has been implemented via the use of NS-3 (Network Simulator Version 3).

Keywords Quantum key distribution · Quantum cryptography · Simulation · NS-3 · Quantum channel

S. Praveen Kumar (✉) · T. Jaya
Department of ECE, VELS Institute of Science, Technology and Advanced Studies, Chennai, India
e-mail: praveenkumar.se@ktr.srmuniv.ac.in

T. Jaya
e-mail: jaya.se@velsuniv.ac.in

A. Balaje · A. Banerjee (✉) · Induvalli · S. Sharma
Department of ECE, SRM Institute of Science and Technology, Chennai, India
e-mail: nishupiki@gmail.com

A. Balaje
e-mail: aishwaryabalaje@gmail.com

Induvalli
e-mail: induvalli9@gmail.com

S. Sharma
e-mail: sonali3006sharma@gmail.com

S. S. Dash et al. (eds.), *Artificial Intelligence and Evolutionary Computations in Engineering Systems*, Advances in Intelligent Systems and Computing 1056,
https://doi.org/10.1007/978-981-15-0199-9_51

1 Introduction

In the current age, data security has become one of the foremost priorities of existing organizations; this is majorly due to the value that is attached to information. Hence, the existence of nefarious individuals whose sole purpose is to obtain such data is inevitable. This led researchers to look towards other means of encrypting data, thus quantum particles due to their fragile nature were considered appropriate for this purpose.

Quantum communication takes advantage of the laws of quantum physics to protect data. These laws allow particles to transmit data along optical cables. These particles are known as quantum bits or qubits. Their super-fragile quantum state "collapses" to either 1 or 0, if a hacker tries to observe them in transit. This enables the quick identification of an eavesdropper in the network.

The purpose of this paper is to implement quantum key distribution in an observable manner via the means of a simulation. This is done in order to understand the nuances in the establishment and the working of a quantum as well as a public channel. This is done using NS-3 and QKDNetSim environment that had been built into it.

This paper's contents have been divided into the following sections: Sect. 2 describes the process of intruder identification via QKD. Section 3 describes the system model utilized for simulation. In Sect. 4, the obtained results have been discussed. Section 5, the discussion, addresses the issues faced when simulating the network in the quantum channel versus the public channel. Section 6 deals with the existing developments that can shape future research. We have summarized our contribution in Sect. 7.

2 Intruder Identification via QKD

Quantum key distribution refers to a method in which a private key is shared between two parties using the quantum channel; this is authenticated via the public channel. The key is used to encode and decode messages exchanged by both parties over the public/classical channel. Due to the fragile nature of quantum particles, the presence of an eavesdropper can be accurately identified if it intercepts the quantum channel. In this case, the generation of the key is terminated by the QKD protocol. QKD is one of the most widely known methods of quantum cryptography; it provides information-theoretic security (ITS) solution [1] to the key exchange problem.

As mentioned earlier, QKD process depends on the laws of quantum physics, which have been discussed in the following section:

- Decoherence: This refers to the property that causes qubits to decay and ultimately disappear while interacting with the environment hence making only point to point communication between two nodes feasible.

Fig. 1 Orthogonal state representation

$$|\varphi\rangle = \alpha|0\rangle \pm \beta|1\rangle,$$

$$|\emptyset\rangle = \alpha|0\rangle \pm \beta|1\rangle.$$

- Superposition: Qubits can represent multiple combinations of 1 and 0 simultaneously.
- Uncertainty principle: Measurement of properties in quantum physics cannot be done in the same way as classical physics. In the quantum scale, some of the physical properties of certain pair of particles are complementary. This statement defines Heisenberg's uncertainty Principle. The primary property utilized QKD is photon polarization.
- Entanglement: This describes a state in which two or more quantum particle's physical properties are strongly correlated. This property can facilitate the research in long-distance quantum key distribution [2] (Fig. 1).

The uncertainty principle-based QKD protocol BB84 developed by Charles H. Bennett and Gilles Brassard is applied in this paper in order to visualize the process of data transfer through a quantum channel. We choose this protocol due to its prompt identification of the presence of an intruder in the quantum channel via this, and because its implementation in a simulation environment when compared to other protocols is easy [3, 4]. It has two bases of measurements (orthogonal states) and four photon polarization states. It begins with the transmission of photons which have four random quantum states, relating to two mutually conjugate bases, rectilinear and diagonal [5]. The rectilinear basis has two polarizations namely 0° represented horizontally and 90° represented vertically. The diagonal basis has 45° and 135°. The measurement of these polarizations cannot be done simultaneously, as if done they randomize each other. Hence, if an intruder attempts to access information from the quantum channel this will change the polarization of the intercepted photon. Thus, alerting the users of the presence of an eavesdropper in the network.

3 System Model

3.1 Theoretical Process

The quantum key distribution process consists of primarily three steps [6]. Although the QKD protocols only define the first two stages:

- Key Exchange: The raw key is generated and is exchanged in the form of Qubits between the two parties.
- Key Sifting: Certain cases from the raw key are selected and checked if they are in perfect correlation between the sender and the receiver. After the sifting step,

both parties share the sequence of correlated bits, called the sifted key. The information revealed ensures that an intruder does not get any access to the secret key.
- Key Distillation: The shifted key is jointly processed by the sender and the receiver jointly to extract the secure sequence of bits called secret key. It consists of three steps: error correction, privacy amplification and authentication.

3.2 Simulation Methodology

The QKDNetSim module that has been built into NS-3 enabled us to simulate and analyse characteristics of the quantum channel. This contains the following features [7]:

- QKD Key: This describes the key being used for encryption.
- QKD Buffer: The keys are stored in the buffer. The analysis of the buffer concentration describes the traffic in the channel. More about this is discussed in a later section.
- QKD Crypto: This class of the module used to perform encryption, decryption, authentication and reassembly of previously fragmented packets.
- QKD Virtual Network Device: It facilitates the operation of the overlay routing protocol.
- QKD Post-processing Application: It deals with the extraction of the secret key from the raw key transmitted over the quantum channel.
- QKD Graph: This class of the module enables the easy extraction of the graphs related to the QKD buffer states.

The element of this module that this paper is primarily focussed on is the QKD Buffer. This has many variables that further facilitate the process of analysing the quantum channel. Endpoints of links which contain the buffer are gradually filled with the new key material and subsequently used for the encryption/decryption of data flow [8]. The key consumption rate depends on the encryption algorithm used and the network traffic, while the key rate of the link determines the key charging rate. If there is not enough key material in the storage, encryption of data flow cannot be performed [9] and QKD link can be characterized as “currently unavailable”. Key material storage has a limited capacity and QKD devices constantly generate keys at their maximum rate until key storages are filled. Hence any disruption in the link can also compromise the key rates, these changes can be observed in the QKD buffer graphs. The variables used to define said graphs are, M_{cur}—current buffer capacity, M_{min}—minimum pre-shared key material, M_{max}—maximum storage depth, M_{cur}—current key concentration in the buffer, M_{thr}—threshold value.

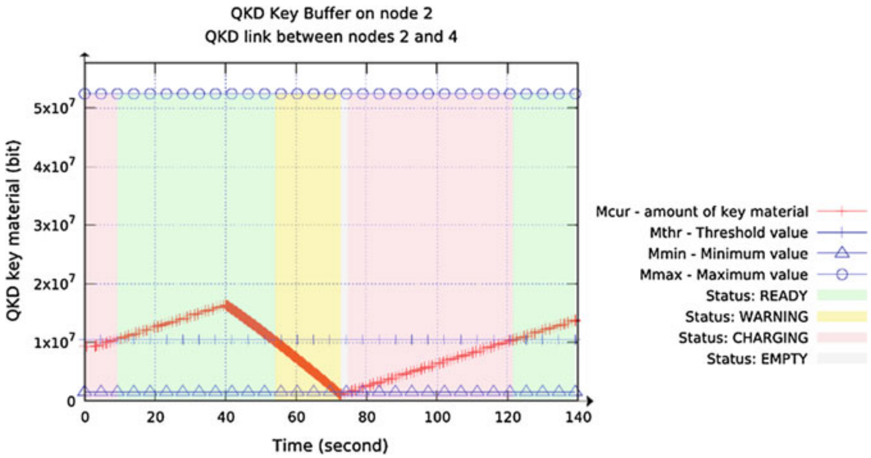

Fig. 2 Graphical representation of QKD buffer

The QKD buffer can be in one of the following states:

- Ready: $M_{\mathrm{cur}}(t) \geq M_{\mathrm{thr}}$,
- Warning: $M_{\mathrm{thr}} > M_{\mathrm{cur}}(t) > M_{\mathrm{min}}$, the previous state was ready,
- Charging: $M_{\mathrm{thr}} > M_{\mathrm{cur}}(t)$, the previous state was empty,
- Emtpy: $M_{\mathrm{min}} \geq M_{\mathrm{cur}}(t)$, the previous state was warning or charging (Fig. 2).

The process used for implementing the simulation of the networks in public as well as quantum channel in NS-3 follows the steps shown in the flowchart. These steps are common for implementation of any network on this platform (Fig. 3).

- Topology Definition: since it is possible to implement these networks in public as well as the quantum channel, it is also possible to integrate the nodes of the network to form various arrangements (like bus, ring, star, mesh) with the help of links.
- Model Development: this speaks of the various protocols (TCP, UDP) that can be implemented in the network in the NS-3 by programming it along with the nodal orientation.

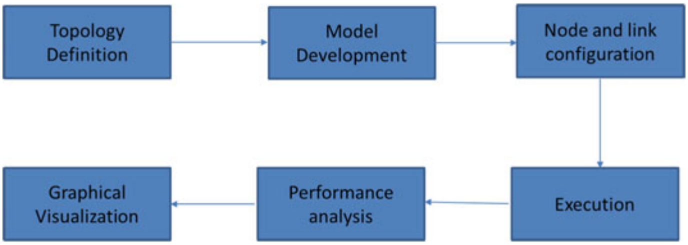

Fig. 3 Network model implementation flowchart

- Node and Link Configuration: these are additional node and link specifications (Baud rate, Bit rate, public channel congestion control, etc.).
- Execution: when the implemented network is simulated in the NS-3, the results are twofold (ASCII and graphical).
- Performance Analysis: this is the ASCII result that tells the client-server relation, the total number of packets sent, the total data transmitted, the client and server address along with the transmitting and receiving ports. In the case of public channel, it also tells the number of packets dropped and at what time.
- Graphical Visualization: by using two software two different graphical visualization of the network is achieved. One is a network animator that simulates the data flow for the total time duration and the other, is a plotting aid that is used to determine the total data transmitted (in bits) and BER.

4 Results

The implementation of this paper has been done in two parts: firstly, we have tried to implement a normal public channel at ideal conditions as well as a public channel network with congestion control. Secondly, we have tried to run a simple quantum channel network at ideal conditions, after which we have tried to implement a more complicated overlay network of the same to identify the changes in the channel traffic.

The ideal values of $M_{\min}$, $M_{\max}$, M_{cur} can be set in the program used to design the network. The M_{thr} depends on the network topology. It can be calculated using specific formulae [10]. The threshold value M_{thr} is proposed to increase the stability of QKD links, where it holds that $M_{\text{thr}} \leq M_{\max}$.

- Each node a calculates value L_a summarizing the M_{cur} values of links to its neighbours j and dividing it with the number of its neighbours N_a, that is:

$$L_a = \frac{\sum_j^N M_{\text{cur},a,j}}{N_a}, \quad \forall j \in N_a \tag{1}$$

- Then, each node exchanges calculated value L_a with its neighbours. The minimum value is accepted as the threshold value of the link, that is:

$$M_{\text{thr},a,b} = \min\{L_a, L_b\} \tag{2}$$

By using M_{thr}, the node gains information about the statuses of network links. The higher the value, the better the state of links that are more than one hop away. Since the protocol used by the networks in both channels is Open Shortest Path First (OSPF), the node of higher threshold value can be chosen. Depending on this, paths can be rerouted or terminated. Hence, the QKD buffer capacity graph enables

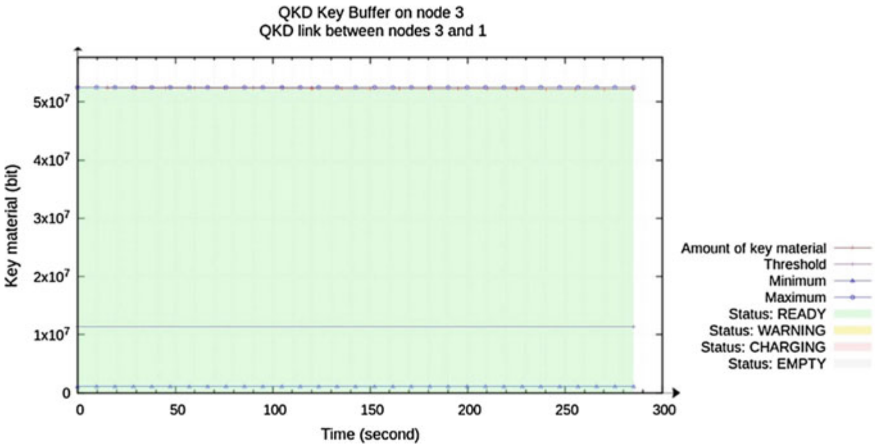

Fig. 4 Ideal quantum channel buffer graph

us to analyse the traffic in the current path, and choose a more efficient path for data exchange. A dip in the QKD buffer capacity indicates that parts of the key have been dropped. This can be due to congestion or the presence on an intruder in the path. Path congestion in the quantum channel is unlikely since the connection between the nodes is point to point. This is because the key material is primarily in the form of qubits, and it follows quantum properties. The addition of constraints due to the environment need not be implemented in the simulation, as data transfer via the quantum channel is done using fibre optic cables. The images shown below are the results that we have obtained via simulating data transfer through a six-node mesh network in both channels (Figs. 4, 5 and 6).

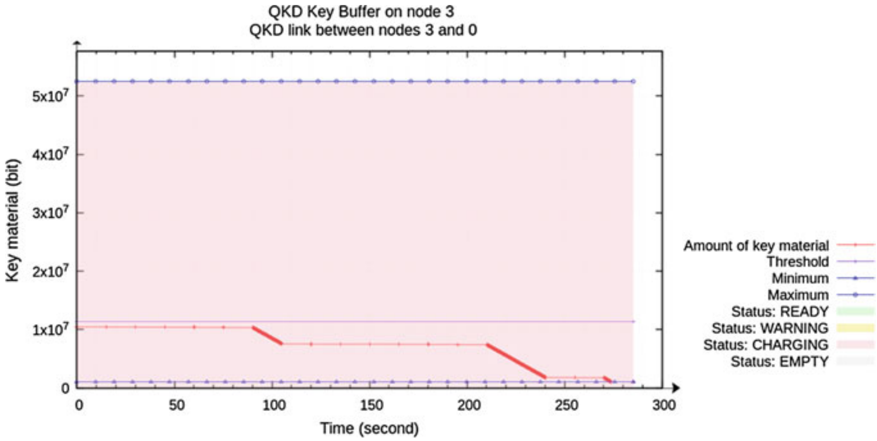

Fig. 5 Buffer graph due to disruption in quantum channel

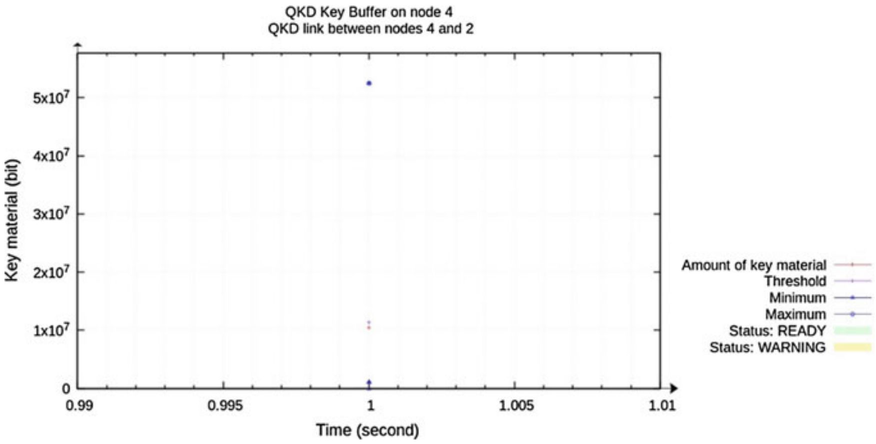

Fig. 6 Buffer graph when connection has been terminated

5 Discussion

In the process of implementing the simulation of the QKD network, we had encountered certain hurdles on the basis of which we made the following observations:

- Even though there is no limit to the number of nodes that can be added to an executable network in the public channel, in the quantum channel of our network this number was limited to 6.
- Also, unlike the public channel networks, the quantum channel ones are not so complicated as they do not exhibit any congestion control features. Hence increasing its ability to detect intruders more efficiently in simpler networks.

6 Future Research

Multiple advancements that have been made in the field of quantum cryptography even though they are purely hypothesis based, they depict the path in which this research is headed. The primary purpose of this is to create systems that can closely emulate and counter the real-life constraints of execution; some of which are, the effect of fibre birefringence on data transmission in the quantum channel, the use of the implementation of quantum repeaters by use of all-graphene solid-state components [11, 12]. Also, the implementation of satellite to ground quantum key distribution on the basis of entanglement, as well as the implementation of QKD in IoT to increase the security of wireless sensor-based networks as well as cellular networks is being researched [13, 14].

7 Conclusion

In this paper, we have presented a practical realization of QKD networks. We have also analysed the factors that affect traffic in the quantum channel. Hence, a relation between the variation of the QKD Buffer with the presence of network disruptions in the form of an intruder has been established. This simulation has been done by utilizing the BB84 protocol due to its ease of implementation, although other protocols can also be implemented within the developed simulation environment. The simulations carried out in this paper have been done using NS-3 with QKDNetSim built into it. Hence, the main purpose of this project was to prove theoretical concepts in the form of a simulation which closely emulates the real-life constraints of data transmission. Thus, proving that QKD is the most secure means of data encryption.

Acknowledgements We would like to express our gratitude to our University SRM Institute of Science and Technology, for giving us access to the resources required to undertake this project. We would also like to thank our guide Mr. S. Praveen Kumar, who is a faculty in this institution, for his valuable guidance, constant encouragement, timely help and for providing us an opportunity to do research in this field.

References

1. Mehic, M., Fazio, P., Voznak, M., Chromy, E.: Toward designing a quantum key distribution network. Adv. Electr Electron. Eng. **14**(4), 413–420 (2016)
2. Houshmand, M., Hosseini-Khayat, S.: An entanglement-based quantum key distribution protocol." In: IEEE 8th International ISC Conference on Information Security and Cryptology, pp. 45–48. IEEE (2011)
3. Abdulbast, A., Elleithy, K.: QKDP's comparison based upon quantum cryptography rules. In: IEEE Long Island Systems, Applications and Technology Conference (LISAT), pp. 1–5. IEEE (2016)
4. Trizna, A., Ozols, A.: An overview of quantum key distribution protocols. Inf. Technol. Manage. Sci. **21** (2018)
5. Padamvathi, V., Vishnu Vardhan, B., Krishna, A.V.N..: Quantum cryptography and quantum key distribution protocols: a survey. In: IEEE 6th International Conference on Advanced Computing (IACC), pp. 556–562 (2016)
6. Jasim, O.K., Abbas, S., El-Horbaty, E.-S.M., Salem, A.-B.M.: Quantum key distribution: simulation and characterizations. Procedia Comput. Sci. **65**, 701–710 (2015)
7. Mehic, M., Maurhart, O., Rass, S., Voznak, M.: Implementation of quantum key distribution network simulation module in the network simulator NS-3. Quantum Inf. Process. **16**(10), 253 (2017)
8. Kollmitzer, C., Pivk, M. (eds.): Applied quantum cryptography, vol. 797. Springer (2010)
9. Elliott, C.: Building the quantum network. New J. Phys. **4**(1), 46 (2002)
10. Mehic, M., Niemiec, M., Voznak, M.: Calculation of the key length for quantum key distribution. Elektron. Elektrotechnika **21**(6), 81–85 (2015)
11. Lobino, M., Zhang, P., Martín-López, E., Nock, R.W., Bonneau, D., Li, H.W., Niskanen. A. O.: Quantum key distribution with integrated optics. In: IEEE 19th Asia and South Pacific Design Automation Conference (ASP-DAC), pp. 795–799 (2014)

12. Wu, G.Y., Lue, N.-Y.: Graphene-based qubits in quantum communications. Phys. Rev. B **86** (4) (2012)
13. Yin, J., Cao, Y., Li, Y.-H., Ren, J.-G., Liao, S.-K., Zhang, L., Cai, W.-Q., et al.: Satellite-to-ground entanglement-based quantum key distribution. Phys. Rev. Lett. **119**(20) (2017)
14. Routray, S.K., Jha, M.K., Sharma, L., Nyamangoudar, R., Javali, A., Sarkar, S.: Quantum cryptography for IoT: A perspective. In: IEEE International Conference on IoT and Application (ICIOT), pp. 1–4 (2017)