Implementation of Quantum Key Distribution network simulation in Quantum Channel

Implementation of Quantum Key Distribution network simulation in Quantum Channel

S. Praveen Kumar[1], T. Jaya[2], Prithiviraj Rajalingam[3]
[1,3]Department of ECE, SRM Institute of Science and Technology, Chennai, Tamilnadu, India
[2]Department of ECE, VELS Institute of Science, Technology and Advance Studies, Pallavaram, Chennai, Tamilnadu, India.
[1]praveens1@srmist.edu.in, [2]jaya.se@velsuniv.ac.in,[3]prithivr@srmist.edu.in

Abstract— The aim is to analyze the efficiency of a communication method, Quantum key distribution. This newly popularized method of communication uses the principles of quantum mechanics. The simulation environment allows researchers to create complex network topologies and a high degree of control and repeatable experiments, allowing them to conduct studies and verify their outcomes. It would be costly to implement QKD in reality, which would need optical and Internet connections between network nodes and the verification of a certain network method or protocol. Thus, the performance analysis here is done in open-source software called NS-3 or Network Simulator- 3, which has an in-built module called QKD netsim for creating the quantum channel.

Keywords - Quantum Networks, Quantum Mechanics, Quantum Cryptography, eavesdropper, NS-3 simulation, Quantum channel.

1. INTRODUCTION

Secured communication is a notional term that can cause serious transmission and reception issues. The current solutions to this problem are mostly based on a public key infrastructure (PKI) which depends on suspicions for identifying an eavesdropper and is not very accurate [1]. Thus, the researchers identify other methods of encrypting the data using a quantum channel. Quantum communication uses the laws of quantum physics for encryption and decryption. Quantum stations use photons to communicate information alongside optical links. The known qubits (quantum bits). Qubit is the basic unit of quantum information—the quantum interpretation of the customary twofold piece genuinely recognized with a two-state contraption. When it comes to quantum structures, it's difficult to replace electron turns for demonstrating the unconventionality of quantum mechanics because the two levels can be interpreted as going up and going down. Or take polarisation for example: when two photons have the same polarisation, you can take the up and down levels to represent their polarisation. If a snoop is present, the quantum state subsidies to a value of 1 or 0.

This paper aims to complete QKD graphically and to show the activity of the various topologies. This is done to comprehend the troubles in the extemporizing and running Quantum in a normal channel through the utilization of NS-3 and the QKD NetSim environment incorporated with it.

This paper has divided into the following sections: Section II experiments with intruder identification via QKD, establishing it as a secure data transfer process. Section III explains the system model and methodology used for simulation. In Sections IV, the acquired results have been discussed. Section V deals with present improvements that will form later exploration [2]. We have summed up our contribution to Section VI.

2. SECURE DATA TRANSFER VIA QKD

QKD is a technique of sharing a private key that is shared between two entities i.e., the quantum channel and the public channel. The key encodes just as deciphers messages traded between the two parietes over the public channel. The presence of an eavesdrop can be precisely distinguished on the off chance that it catches the quantum channel; this is because of the delicate idea of quantum particles. For this situation, the age of the key material is ended by the QKD convention. QKD gives a data hypothetically secure solution [3] to the key trade issue, thus making it one of the most secure types of information move

QKD is viewed as the nearly assured type of information move as it depends upon the laws of quantum material science, which can be examined in the following fragment:

- Qubits: It examines the status and eventual disappearance of quantum particles while interacting with the environment, with node-to-node communication between two points is possible. This is considered to be one of the major drawbacks of quantum communication.
- Superposition: Different combinations of 1 and 0 can be represented at the same time by qubit.
- Uncertainty principle: When compared to the classical scale, the physical possession of specific sets of particles is reciprocal dependent on the quantum scale. This statement characterizes Heisenberg's vulnerability Principle. The actual possession used QKD is photon polarization. These polarized particles, if intercepted, change their property, hence helping in intruder identification.
- Entanglement: This describes the correlation of quantum particles in a particular state. It is equipped for encouraging the exploration in significant distance Quantum key distribution [4].

In 1984, Charles H. Bennett and Gilles Brassard proposed the first QKD protocol. BB84 is the protocol, and it utilized the state polarizations quantum bits. It has four states of photon polarisation and two bases of measurements.

$$|\varphi\rangle \pm \beta|1\rangle,$$
$$|\emptyset\rangle \pm \beta|1\rangle.$$

The BB84 protocol is considered to be a pioneer in field of QKD for being one of the most used protocols in terms ease of execution. Even though there as a couple of papers have shown that the BB84 show does not secure it is still hypothetically utilized by a few QKD conventions [5]. This protocol is applied in this paper to picture the cycle of information move through a quantum channel. We have chosen this due to the short and recognized evidence that an intruder

exists inside a specific link in the quantum channel and that it is easy to do in a simulation environment in comparison with other protocols [6].

The protocol is based on the Uncertainty Standard and begins with the impartation of four arbitrary quantum states with two frequently linked bases [7]. In the rectilinear there are two polarization premises: 0° (flat) and 90°. (vertical). The bases are diagonal at 45° and 135°. Because such polarisation cannot be predicted as long as it is random, it helps to identify the invader.

3. METHODOLOGY

A. TheoreticalConcept

The Quantum Key Distribution process, as explained in various papers, encompasses three steps [8]:

- Accuracy: The probability of scaling to various topologies increases when modeled circumstances like those seen in real-world testing.
- Extensibility: Usage of new strategies and models in the field of QKD.
- Availability: The objective was to give an idea for the combination and trail of the QKD innovation with various present organization arrangements by limiting the expense.

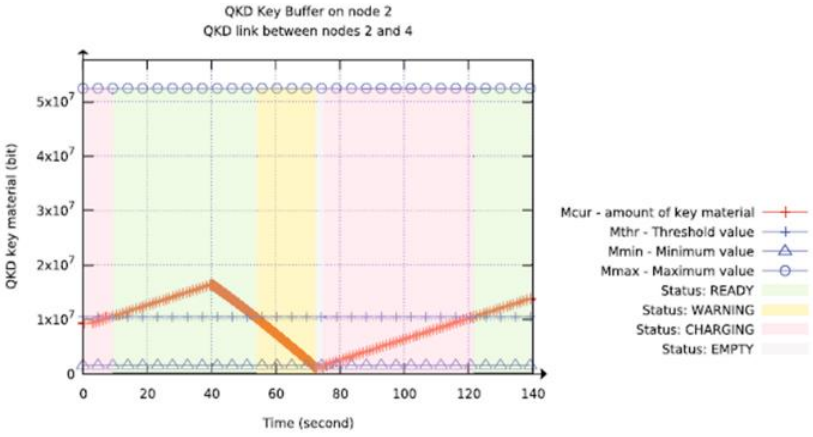

Figure 1: QKD buffer graphical representation

The QKD protocol defines only the first two stages.

B. Simulation Methodology

We chose NS-3 as it was the only available open-source software capable of running complex network simulations and the QKD NetSim module, which enabled us to stimulate and investigate attributes of the quantum channel. This has the following highlights [9]:

- QKD key is an important factor of the QKD NetSim framework. It's used in the QKD procedure to make the key more clear.

- QKD Buffer: To ensure the integrity of the protocol, a buffer is used to store keys.
- QKD Datagram Network Device: Operation of the inlay routing protocol is facilitated by this device.
- QKD Post-processing Application: It removes the confidential key from the fresh key and sends it to the quantum channel.
- QKD Graph: It enables the graphical extractions identified with the QKDbuffer states.

This paper is focused on the QKD buffer. The process of analyzing the quantum channel can be further aided using its variables. New key materials are gradually used to fill the endpoints that contain buffers and indicate the flow rate [10]. The key utilization rate relies upon the encryption calculation utilized and the organization traffic, which in the case of a quantum channel is non-existent; hence it only indicates channel disruption. As long as there is sufficient key material in storage to conduct encryption of data flow [11], the QKD connection will be labeled as "currently unavailable." As long as key storage is really not full, the time to get new keys is optimal. The QKD buffer charts show the variations in key generation rates as they occur.

The factors used to characterize said diagrams are, M_{cur}- present guard, M_{min}– least pre-shared key, M_{max} –storage of maximum depth, M_{cur} – present key fixation in the buffer, M_{thr}– the value of the threshold.

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

- Ready: $M_{cur}(t) \geq M_{thr}$,
- Warning: $M_{thr} > M_{cur}(t) > M_{min}$, the past state was prepared,
- Charging: $M_{thr} > M_{cur}$ (t), the past state was empty,
- Empty: $M_{min} \geq M_{cur}(t)$, the previous state was cautioning or charging.

The measure of key material in the capacity at the estimation time t can be determined utilizing Equation (1), while the normal operational rate can be determined utilizing Equation (2).

$$D_k(t) \leq r_k \cdot t + M_{cur,k}(t) - M_{min,k}(t) \quad (1)$$

$$A_k(t) \frac{Dk(t)}{t} = r_k + \frac{Mcur,k(t) - Mmin,k(t)}{t} \quad (2)$$

The diagram shown below represents the QKD packet encapsulation process of the quantum channel as well as the public channel.

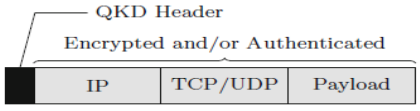

Figure 2: QKD Packet Encapsulation

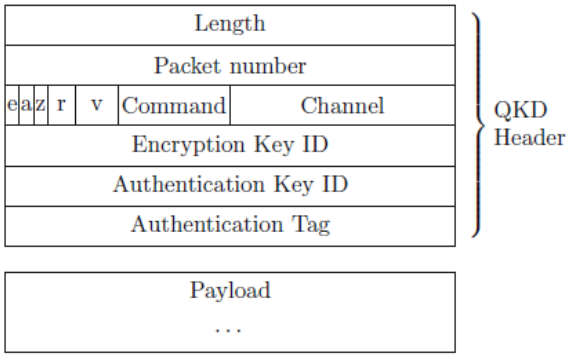

Fig 3: QKD Header

QKD crypto class can perform encryption, decoding, verification, validation check tasks, and reassembly of recently divided packets.

In-network test systems, such tasks are basic since they decrease the execution time and spare computational assets. For instance, instead of producing packets with alternate data, network test systems frequently produce empty packets. Be that as it may, QKD NetSim permits the client to destroy this degree of deliberation to pick the actual key amount and capacity in QKD buffers.

4. RESULTS

This research was divided into two sections: first, a point-to-point network with eight nodes that used a variety of topologies. Second, we use a six-node mesh network to track changes in channel traffic. Quantum key distribution (QKD) cryptosystems and QKD buffers are used by both networks, and they function as an overlay on top of each other.

The ideal values of Mmin, Mmax, and Mcur may be input into the application that was used to create the organisation. Depending on the network topology, the Mthr changes. The use of explicit formulas [12] tends to be dictated. The Mthr threshold is suggested to increase the strength of QKD connections, where Mthr≤Mmax.

- It shows that each node in the network has its own value based on the number of links it shares with its neighbors. We conclude that the value of Mcur the value La is a function of the size of its link to its neighbor j and the length of its connection to its neighbor a. This can be done for each node by comparing its value with the number of links to its neighbors j.

$$N_a = \sum_J^N \frac{M_{cur\,a,j}}{Na}, \forall j \in N_a \quad (3)$$

- After which every node trades the determined worth La with its neighbors. The base estimation of L between the two-node is acknowledged as the edge estimation of the connection.

$$M_{thr,a,b} = Min\{ L_a , L_b\} \quad (4)$$

M_{thr} is used by the node to give information about the network's connections. In the first Equation, M_{cur} is used as the initial key concentration value, representing the maximum buffer capacity. This establishes a definite cutoff point.

The QKD charts have been updated to make it simpler to enter the QKD buffer region and to regulate the usage of essential materials. For each hub having a QKD connection, an accompanying set of QKD buffers may be used for diagramming.

With an eight-node point-to-point network, we could change the Mthr value by changing Mmin, Mmax, and Mcur. We were able to determine the data range between two of the network's eight nodes by modifying the settings.

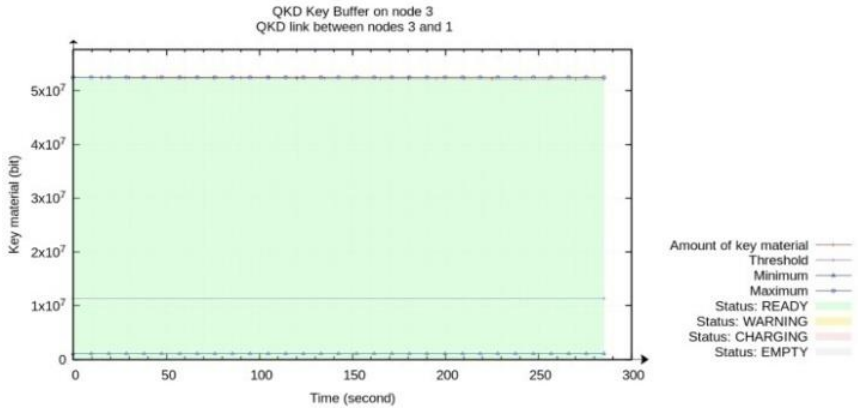

Figure 4: Ideal quantum channel graph for the 8-node network

To simulate a link failure the values of M_{thr} can be altered to generate a buffer graph where the connection has been terminated due to the buffer/container not being in a ready state. It's not in READY, WARNING, or CHARGING its EMPTY which means the connection has been terminated. This happens only when either the channel is severed or the $M_{thr} >> M_{cur}$.

To depict the loss of key material, the M_{thr} values can be manipulated. This is due to setting it to a high value. Even though the state is ready and transmitting, there is a considerable amount of data loss in the individual container and the total graph due to this configuration.

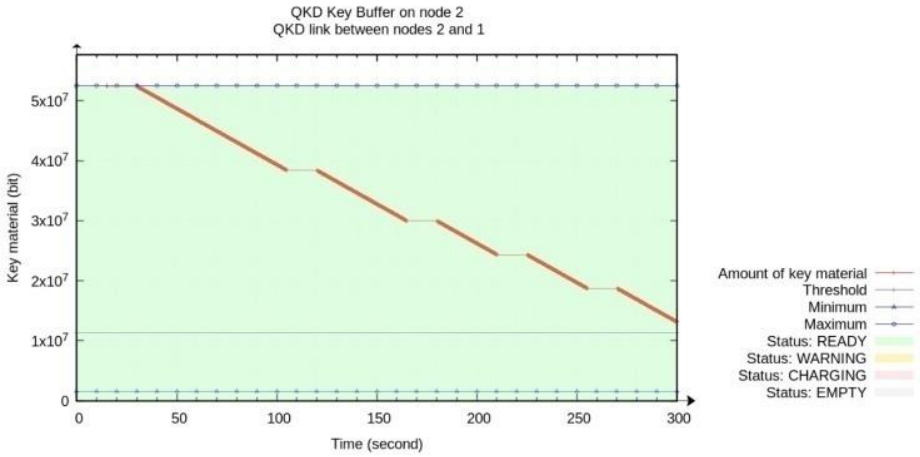

Figure 5: Loss of key material

The total graph shows the overall data loss amongst all the network nodes, including the missed transmissions, the terminated ones, and the dropped ones. Although, this is primarily due to the presence of an eavesdropper/intruder.

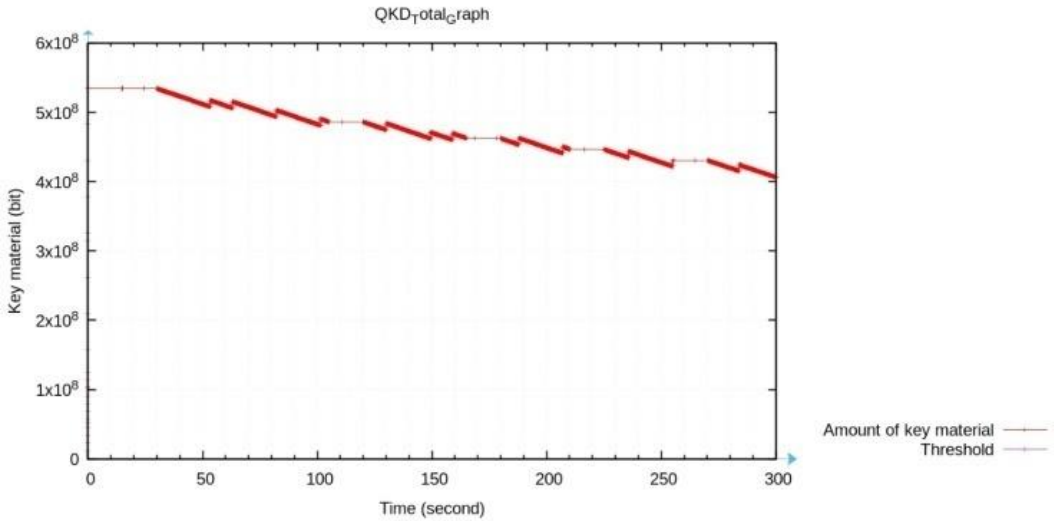

Figure 6: Total buffer graph indicating network state

With the help of the text editor, we were able to generate the routing tables for each node, which provide all the necessary details such as the Gateway, Interface, Hop Count, Seq Num, Life Time, Settling Time etc. at different time intervals. The network animation can be obtained by using the NetAnim Tool.

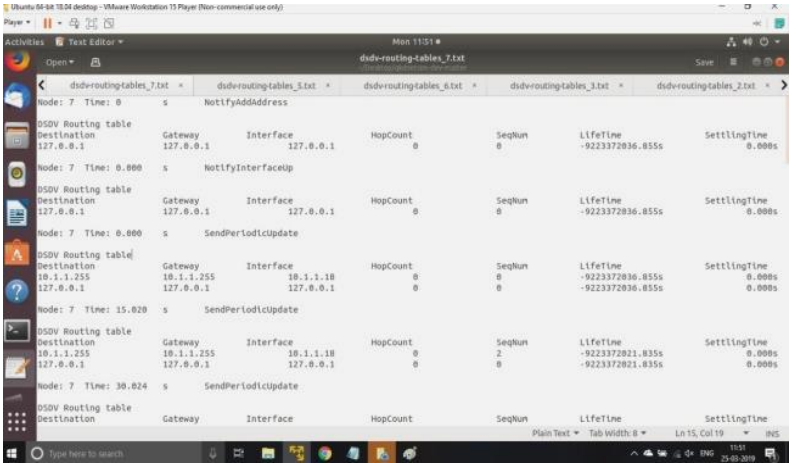

Figure 7: Routing table

The buffer capacity graphs for the point-to-point networks indicate the state of each link. For an efficient quantum channel, every node should be connected to the other for a point connection. Hence if there is a drop in the buffer graph, the key material gets dropped, which either indicates congestion or the presence of an intruder but being a point to connection, there is no possibility of congestion, so it represents the presence of an intruder.

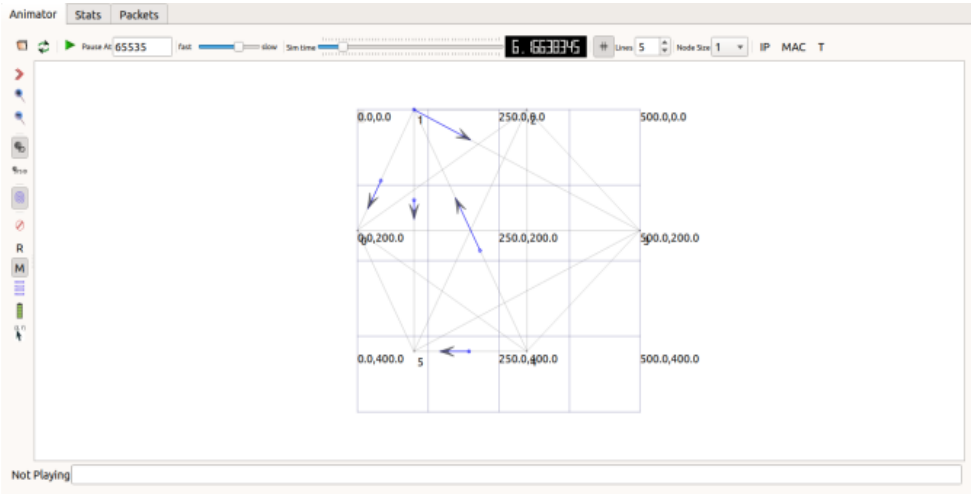

Figure 8: 6-node mesh network topology Network animation

For the pair of nodes shown below, due to a marginal difference between the M_{min} and M_{thr} values the link enters the CHARGING state and ultimately stops the transmission as buffer concentration falls below the M_{min}.

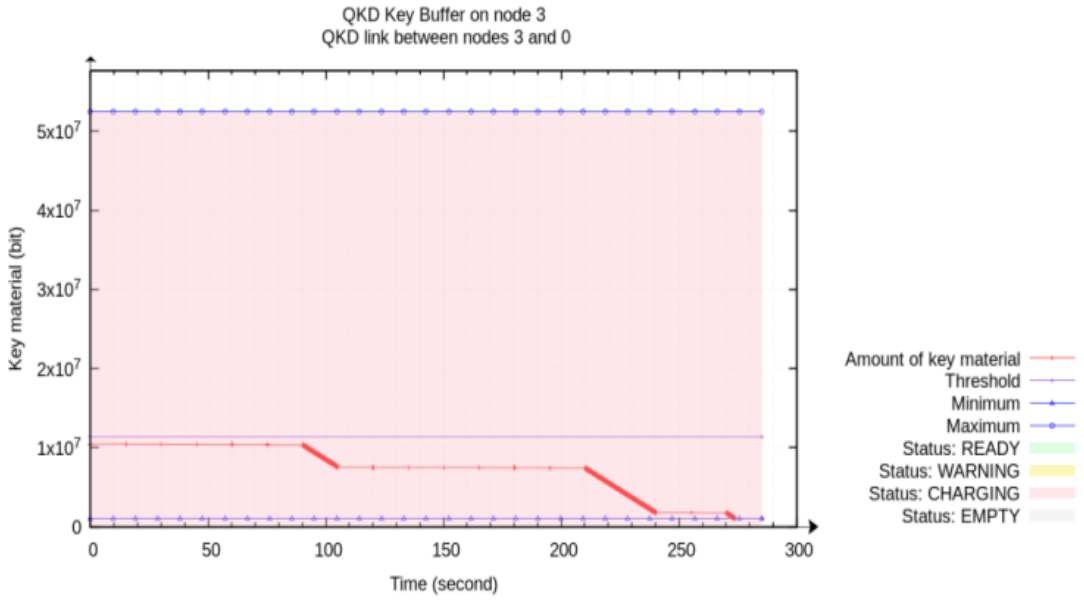

Figure 9: Buffer capacity below the threshold

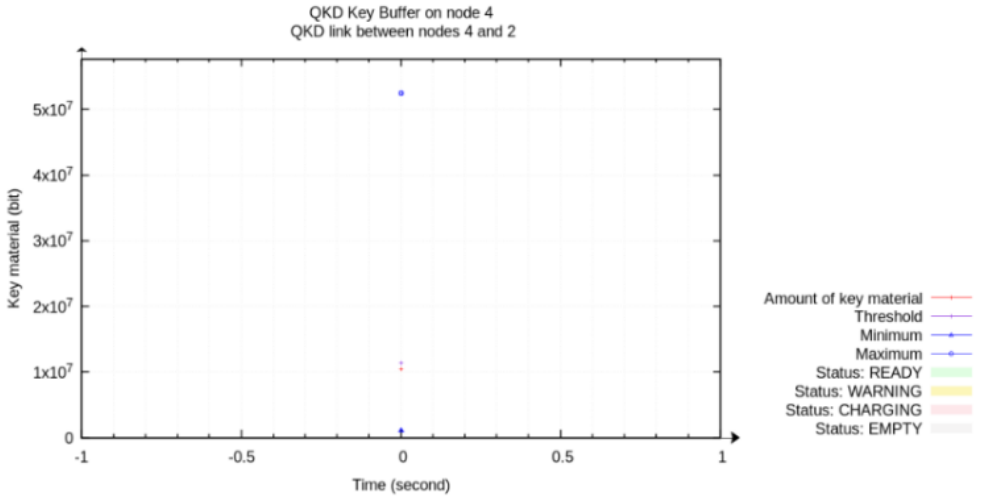

Figure 10: Buffer graph after termination of connection

5. FUTURE RESEARCH

Up until now, the QKD encryption plot appears to be robust, however, it's as yet trial and its clients outside the exploration network are those for whom security is unmistakably more significant than the expense or accommodation. Albeit different movements turned out to be made in the area of qubits, they are absolutely speculation based, they do they portray the way where this exploration is going.

Since the transmission of data in the quantum channel is done primarily through fiber optics, it's affected by the problems in this form of data transmission. Research has been carried out to

counter such problems by referencing frame independent QKD protocol for the polarization of qubits and consequently indicating that it defeats the negative impacts drifting fiber birefringence in a polarization-maintaining fiber [13].

The execution of quantum repeaters through all-graphene solid-state components is also being looked into [14]. In terms of increasing the transmission area, there is a possibility of implementing Quantum key distribution from satellite to ground-based on the characteristics of complication[15]. Its implementation via wireless networks by integrating it with IoT[16].

Also, the level of complexity of the networks can be increased, more than one constraint may be delivered to the simulated networks so that it could more intently emulate an actual-life scenario. The most distance of transmission may be accelerated for the reason that modem executed in this area is purely theoretical, the simulation constraints may be further enhanced to put into effect the one's studies pointers. Some guidelines could be QKD using quantum gates, QKD over multiple terrains, QKD transmission over wireless networks, encrypting cellular transmission using QKD.

6. CONCLUSION

The primary aspect of this paper distributes the QKD NetSim reenactment environment which is to test the current arrangements and the execution of the new arrangements in the area of QKD organizations. The work sums up the impediments and the essential attributes of the QKD organization and depicts the methods of execution of QKD organizations

Due to the acquired diagrams, a comparison of the QKD Buffer types in the presence of organizational disturbances as an interloper has been set up for the examination. It will help people understand how the QKD innovation can be used practically, allowing them to take advantage of a wider range of applications inside the company. As a result, QKDNetSim may be used to recreate a variety of different organizations. To simplify the reproductions that involve the use of an even encrypted key, virtual-TCP/IP stacks like QKD Cryptos and QKD Buffers are often used.

REFERENCES:

[1] Jasim, Omer K., Safia Abbas, El-Sayed M. El-Horbaty, and Abdel-Badeeh M. Salem 2015 Quantum key distribution: simulation and characterizations *Procedia Computer Science 65* pp 701-710
[2] S.Praveen Kumar, T.Jaya, A.Banerjee, Sonali, and A.balaje 2020 Simulation of Quantum channel and analysis if its states under network disruption *Artificial Intelligence and Evolutionary computations in engineering systems, Advance in Intelligent systems, Springer Nature* pp 593-602
[3] Mehic, Miralem, Peppino Fazio, Miroslav Vozňák, and Erik Chromý 2016 Toward designing a quantum key distribution network simulation model *Information And Communication Technologies And Services*
[4] Houshmand, Monireh, and Saied Hosseini-Khayat 2011 An entanglement-based quantum key distribution protocol."*International ISC Conference on Information Security and Cryptology,* pp 45-48
[5] S.Praveen Kumar,T.Jaya, K.Vijayan, and S.Yuvaraj 2021 Simulation of Quantum Key Distribution in a secure star topology optimization in quantum channel *Journal of Microprocessors and Microsystems,* Volume 82
[6] Trizna, Anastasija, and Andris Ozols 2018 An Overview of Quantum Key Distribution Protocols *Information Technology & Management Science* 21
[7] Padmavati, V., B. Vishnu Vardhan, and A. V. N. Krishna 2016 Quantum Cryptography and Quantum Key Distribution Protocols: A Survey *International Conference on Advanced Computing (IACC)* pp 556-562
[8] Jasim, Omer K., Safia Abbas, El-Sayed M. El-Horbaty, and Abdel- Badeeh M. Salem 2015 Quantum key distribution: simulation and characterizations *Procedia Computer Science 65* pp 701-710
[9] Mehic, Miralem, Oliver Maurhart, Stefan Rass, and Miroslav Voznak 2010 Implementation of quantum key distribution network simulation module in the network simulator NS-3 *Quantum Information Processing 16, no. 10* pp.253
[10] Kollmitzer, Christian, and Mario Pick, eds 2010 *Applied quantum cryptography* Vol. 797
[11] Elliott and Chip 2002 Building the quantum network *New Journal of Physics 4*, no. 1 46
[12] Mehic, Miralem, Marcin Niemiec, and Miroslav Voznak 2015 Calculation of the key length for quantum key distribution *Elektronika ir Elektrotechnika 21*, no. 6 pp 81-85
[13] Lobino, Mirko, Pei Zhang, Enrique Martín-López, Richard W. Nock, Damien Bonneau, Hong Wei Li and Antti O. Niskanen 2014 Quantum key distribution with integrated optics *19th Asia and South Pacific Design Automation Conference (ASP-DAC)* pp 795-799
[14] Wu, G. Y., and N-Y. Lue 2012 Graphene-based qubits in quantum communications *Physical Review B* 86 no. 4
[15] Yin, Juan, Yuan Cao, Yu-Huai Li, Ji-Gang Ren, Sheng-Kai Liao, Liang Zhang and Wen-Qi Cai et al 2017 Satellite-to-ground entanglement-based quantum key distribution *Physical review letters 119* no. 20: 200501
[16] Routray, Sudhir K., Mahesh K. Jha, Laxmi Sharma, Rahul Nyamangoudar, Abhishek Javali, and Sutapa Sarkar 2017 Quantum cryptography for IoT: APerspective In *International Conference on IoT and Application (ICIOT)* pp 1-4