Microprocessors and Microsystems 82 (2021) 103820

Contents lists available at ScienceDirect

Microprocessors and Microsystems

journal homepage: www.elsevier.com/locate/micpro

Simulation of quantum key distribution in a secure star topology optimization in quantum channel

S. Praveenkumar [a], T. Jaya [b], K. Vijayan [c,*], S. Yuvaraj [d]

[a] Department of ECE, VELS Institute of Science, Technology and Advance Studies, Pallavaram, Chennai, Tamilnadu, India
[b] Department of ECE, VELS Institute of Science, Technology and Advance Studies, Pallavaram, Chennai, Tamilnadu, India
[c] Department of Telecommunication Engineering, SRM Institute of Science and Technology, Chennai, Tamilnadu, India
[d] Department of ECE, SRM Institute of Science and Technology, Chennai, Tamilnadu, India

ARTICLE INFO

Keywords:
Quantum key distribution
Quantum cryptography
Simulation
Network simulator-3
Quantum channel
Threshold
Buffer capacity

ABSTRACT

The field of quantum cryptography is mostly theoretical therefore in this paper we represent its implementation by means of virtual scenarios. The central issue in cryptography is the secure transmission of the key between nodes. Thus, in this paper we establish a secure channel using Quantum Key Distribution (QKD) for the transfer of the key material between the nodes and help to identify an eavesdropper in the channel. A graphical representation of the quantum channel traffic at the ideal state and also during network disruption has been established. Due to the complex nature of quantum networks and high cost of establishment, 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) which has QKDNetSim module built into it. Finally, our simulation indicates the presence of an intruder by virtue of various network implementations within the quantum channel.

1. Introduction

Technological advancements in communication have enabled a quicker and more efficient exchange of data and other information. Data is essential to businesses and needs to be accessible inter-departmentally and also be transferable to other companies working with them. Such data may include trade secrets, financial documents or even pharmaceutical formulae. All this information, which in today's age is transferred over an internet connection, is susceptible to unauthorised access. Although once considered one of the most superior methods of keeping data protected are now becoming obsolete as more technologically advanced our world becomes. Thus, this led researchers and scientists to develop a technology that can safely communicate encryption keys that will more efficiently protect the data. A technology which makes this possible is known as Quantum Key Distribution or QKD is probably secure to transfer with minimal or no breach.

As it uses principles of Quantum mechanics [1] for key transfer, we need the encryption key in the form of photons which has a spin. The sender, sends these photons each having a particular, which at the receiver end, is identified by the receiver with the help of a filter which is either diagonal or rectilinear.

If by any chance, there is an eavesdropper on the network, there will be disturbances produced during the key generation [2]. This helps in identification of the presence of a third party.

Although, it has been said that server load in a small inter-network in a star topology is dependent on simulation time and number of nodes [3] the centrally monitored architecture becomes an advantage as it helps us to keep a track of all the information transmissions taking place in any architecture unless there happens to be some glitch in the central node called hub.. Because of this reason star topology is widely used these days in various sectors for setting up their networking structure Fig. 1.

1.1. Vulnerability of public key encryption

The classical method of encryption is known as Public Key Encryption, which uses the same channel for sending the data as well as transferring the encryption key Fig. 2.

First, they transfer a secure packet containing the information and then the sender sends a public key to the receiver. The receiver will have a master key to open the second packet to obtain the encryption key so as to gain access to the enclosed data. However, if there is a third party available on the line, it can make a copy of the secure package, then when the key is exchanged, it can replicate the master key to obtain the encryption key Fig. 3.

* Corresponding author.
E-mail address: vijayank@srmist.edu.in (K. Vijayan).

https://doi.org/10.1016/j.micpro.2020.103820
Received 26 September 2020; Received in revised form 18 December 2020; Accepted 27 December 2020
Available online 4 January 2021

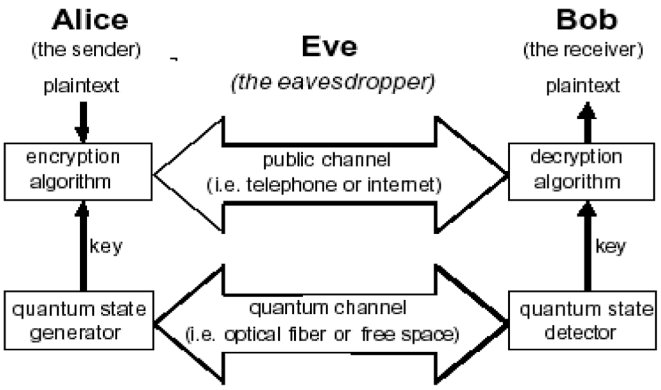

Fig. 1. Quantum Key distribution.

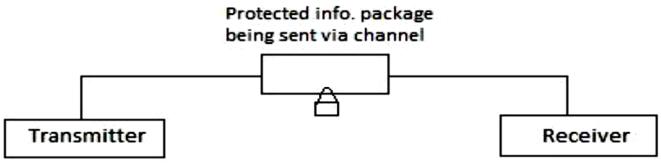

Fig. 2. Stage 1 of Public Key Encryption without an unauthorised third party.

2. QKD using BB84 protocol

In 1984, the BB84 protocol for Quantum Key Distribution [4] was introduced by Bennett and Brassard. The BB84 protocol relies on Heisenberg's uncertainty principle Fig. 4.

The protocol uses two schemes for polarizing the photons i.e. Rectilinear and diagonal. These filters are further divided into two categories which are used to represent binary bits 0 and 1 [5].Several other protocols were introduced SARG04, BBP2, B92, KMB09 [6], etc., but BB84 is the simplest protocol and hence, it is widely used Fig. 5.

3. Working of QKD to detect the presence of an eavesdropper

A simple QKD model somewhat looks like as follows:-

- The transmitter that sends the polarized photons i.e. qubits also called Alice.
- The receiver which detects the polarized photons is called Bob.
- Classical Channel- for sending the information.
- Quantum channel- for sending the photons or key.

Alice sends a stream of polarized photons [5] which are randomly polarized using any of the 4 filters towards Bob which has a particular binary bit associated with it according to the table. Bob, on the other hand, detects these qubits using its own filter which is also one of the four types used by Alice. Alice tells Bob only the orientation of the filter i.e. rectilinear or diagonal but not the configuration. Bob uses a configuration based on the orientation told to him by Alice Fig. 6.

As Bob keeps on detecting the incoming qubits, a new of binary codes are created which will ultimately be compared with that of Alice's as shown in Table 1. There is a ½ probability that the binary code at Bob's end will be similar to that of Alice's. They cross-check the code with each other and finally, the correct code is kept as the key whereas the rest is discarded as shown in Table 2.

In a different scenario, where we have an eavesdropper i.e. Eve an unauthenticated third user on the line, will also create a set of binary codes according to the orientation told by Alice using its own configuration. However, when the final binary code is decided upon by Alice and Bob there will be less than 50% chance that Eve's code will match theirs. When the keys sent by Alice and Bob to each other are compared after Bob has sent the position of the discarded bits to Alice, there will be disturbances if Eve is present as shown in Table 3. However, if the same base as Alice and Bob is chosen by Eve, then eve's presence would not be detected but the probability of this occurring is almost nil Fig. 7.

4. Summary of QKD

Primarily, the Quantum Key Distribution process is a coalition of three steps (Table 4)

- Key Exchange: Exchange of qubits that occur between two parties which will ultimately lead to the generation of something called raw key.
- Key Sifting: This is he step in which only one or two cases are selected. This step follows the Raw Key Exchange or RKE. After this step is completed, both the parties share a bit sequence, called the sifted key.(Table 4)
- Key Distillation: After sifting, the sender as well as the receiver together process the sift of three steps; error correction, privacy amplification, authentication [7].

Only the first two steps are defined by the QKD protocol.

5. Comparison of various types of topologies

5.1. Mesh topology

This is a type of topology where all the nodes are connected without any proper orientation i.e. randomly, directly and non-hierarchically to all the other nodes in the network and efficiently route data to and fro from clients. The lack of dependency on a single node allows for each node to participate in the transfer of data from one system to another. Such networks self-organize dynamically and self-configure according to need, which reduces node dependency. Self-configuration is essential to facilitate dynamic workload distribution in the event of node failure. Thus, the maintenance costs reduce and the network becomes more robust Fig. 8.

The main advantages includes

- Multiple device usability and high traffic withstanding properties.
- Component independent data transfer.
- Expansion and modification of the network can be done without disruption of the other nodes.

The major drawbacks are

- High Redundancy.
- High Cost.

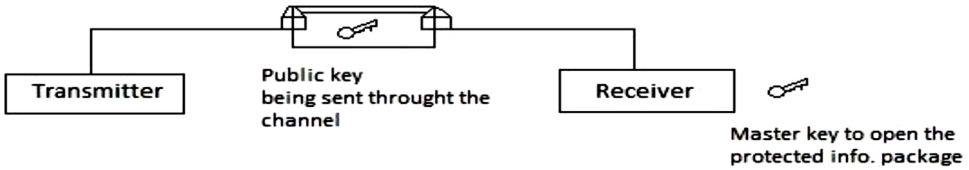

Fig. 3. Stage 2 of Public Key Encryption without an unauthorised third party.

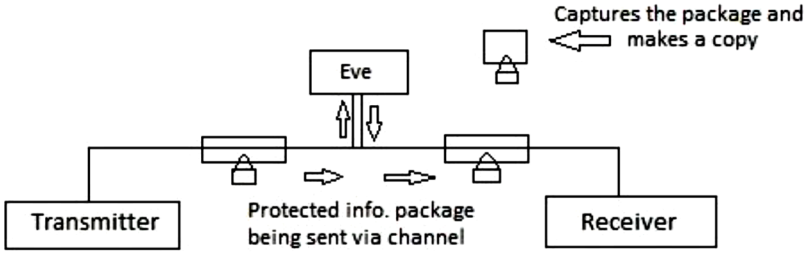

Fig. 4. Stage 1 of Public Key Encryption with an unauthorised third party.

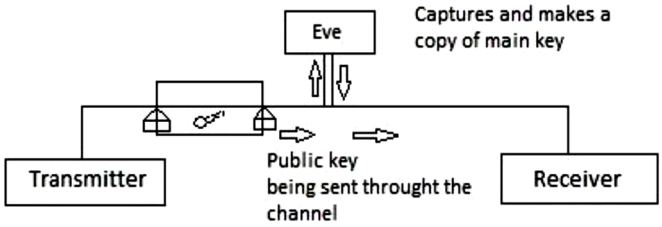

Fig. 5. Stage 2 of Public Key Encryption with an unauthorised third party.

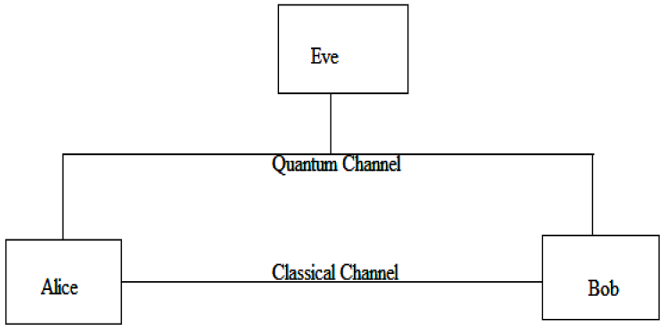

Fig. 6. Simple QKD Model.

Table 1
Quantum Filters used in QKD.

Basis Orientation	Configuration	Binary Bits 0 Polarization	angle	1 Polarization	angle
Recti-Linear		Vertical	90	Horizontal	0
Diagonal		Right	45	Left	135

- Difficult Set-Up and Maintenance.

5.2. Bus topology

This type of a topology has a backbone cable with a terminator at each end. All the nodes are connected to the backbone or the linear cable using a particular device. The terminator absorbs the signal at that particular end preventing signal from bouncing-off. Here, when a system sends out any signal, it traverses the complete length of the cable in both the directions. This may lead to the signal bouncing off the end of the cable which might create problems in the computer network, in the case that collision of the next signal and the bounce-off signal occurs and might cause unnecessary confusion. The collision of signals drastically reduces the performance of the computer network and also its efficiency. Fig. 9

The major advantages are

- Easy to connect a computer or any other peripheral device.
- Least cable length required leading to lower cost.
- Very Reliable and Simple.
- Joining cable can be easily extended
- Single node failure will not affect the whole network.

The major disadvantages include

- The network is highly dependent on the backbone and T-connectors.
- A very high amount of packet collisions in the network
- Slower for a larger network
- Fault isolation is very difficult.

5.3. Star topology

This is a type of topology where every node is individually or separately connected to a central point known as the hub which basically acts as a central point of communication. The hub plays the messenger and passes on the messages to and fro the various nodes connected on the network. The nodes can also be called as hosts and as it is already mentioned there is a central point of communication called the hub. Every host is individually connected to the hub. The hub is acts like the root and peripheral hosts are like leaves. Here, if any of the nodes would like to communicate with the hub, then it has to transmit the message to the hub and then finally the hub forwards its message to the intended node. Thus, this topology closely represents the skeletal structure of a star Fig. 10.

The major advantages include

- The working of the network is independent of node failure.
- Data Collisions are very rare so performance is high.
- Practical usage is seen in offices where sensitive data is stored and monitored.
- Contains individual hub-node peer to peer networks.

The major disadvantages are

- Uses more amount of cable.
- Hub is required as extra hardware.
- Highly dependent on the hub for data transfer.

6. Result and interpretation

The implementation of this paper was done in two parts, firstly we tried to implement a network with 8 nodes, a simple point to point network using various topology. Secondly, we tried to run a complex mesh network with 6 nodes to identify the changes in the channel traffic. Both networks run the public and quantum channels in an overlay Fig. 11.

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 [8]. The threshold value M_{thr} is

Table 2
When Eve is not present.

Alice's Sending bit	0	1	1	0	1	0	0	1
Alice's random sending basis	+	+	×	+	×	×	×	+
Alice's Photon polarization	↑	→	↘	↑	↘	↗	↗	→
Bob's Random measuring basis	+	×	×	×	+	×	+	+
Bob's photon polarization	↑	↗	↘	↗	→	↗	→	→
Bob's receiving bit	0	0	1	0	1	0	1	1
Public discussion of basis								
Shifted key	0		1			0		1

Table 3
Shifted Key after discarding the wrong basis.

Alice's Sending bit	0	1	1	0	1	0	0	1
Alice's random sending basis	+	+	×	+	×	×	×	+
Alice's Photon polarization	↑	→	↘	↑	↘	↗	↗	→
Bob's Random measuring basis	+	×	×	×	+	×	+	+
Bob's photon polarization	↑	↗	↘	↗	→	↗	→	→
Bob's receiving bit	0	0	1	0	1	0	1	1
Public discussion of basis								
Shifted key	0		1			0		1

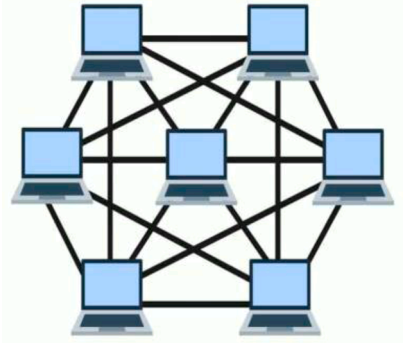

Fig. 7. Network Depicting Mesh Topology.

proposed to increase the stability of QKD links, where it holds that$M_{thr} \leq M_{max}$ Fig. 12.

- With respect to node *a*, calculation of the 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, is done; this can be done for each node.

$$N_a = \sum_{J}^{N} \frac{M_{cur\ a,j}}{Na}, \ \forall j \in N_a \tag{1}$$

- After which each node exchanges the calculated value L_a with its neighbours. The minimum value of *L* between both nodes is accepted as the threshold value of the link.

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

Table 4
When Eavesdropper is present and how it is detected.

Alice's Sending bit	0	1	1	0	1	0	0	1
Alice's random sending basis	+	+	×	+	×	×	×	+
Alice's Photon polarization	↑	→	↘	↑	↘	↗	↗	→
Eave's Receiving basis	+	+	+	×	+	×	+	×
Eave's Photon polarization	↑	→	→	↘	↑	↗	→	↗
Bob's Random measuring basis	+	×	×	×	+	×	+	+
Bob's photon polarization	↑	↗	↗	↘	↑	↗	→	→
Bob's receiving bit	0		0			0		1
Check eavesdropping			x					0

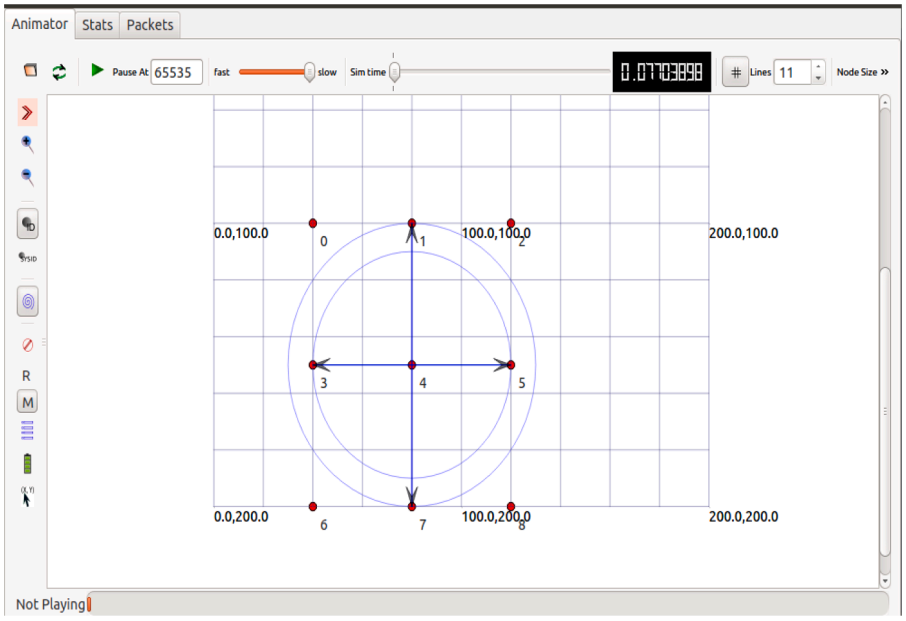

Fig. 8. NS3 Animation for Mesh Topology.

The node gains information about the statuses of network links by usingM_{thr}. The higher the value, the better the state of links that are more than one hop away.TheM_{cur}in the first equation is assumed as the initial key concentration value, which is equivalent to the maximum buffer capacity. Hence establishing a stable threshold value. Fig. 13

QKD graphs are implemented to allow easier access to the state of QKD buffers and easier monitoring of key material consumption. QKD graph is associated with QKD buffer which allows plotting of graphs on each node with associated QKD link and QKD buffer Fig. 14.

By implementing a point-to-point network of 8 nodes, we were able to manipulate the M_{min},M_{max},M_{cur}values to get various M_{thr}values. By changing the values, we determined the range for the ideal transmission of data between two of the nodes in the 8 nodes network Fig. 15.

7. Simulations results

This results shows the implementation of a network with more nodes and an overlay between the public and quantum channel. The graphs show the amount of data sent and received as well as the QKD buffer concentration Fig. 16.

This results shows the implementation of a complex network that relays information in the quantum channel. The QKD buffer graph are

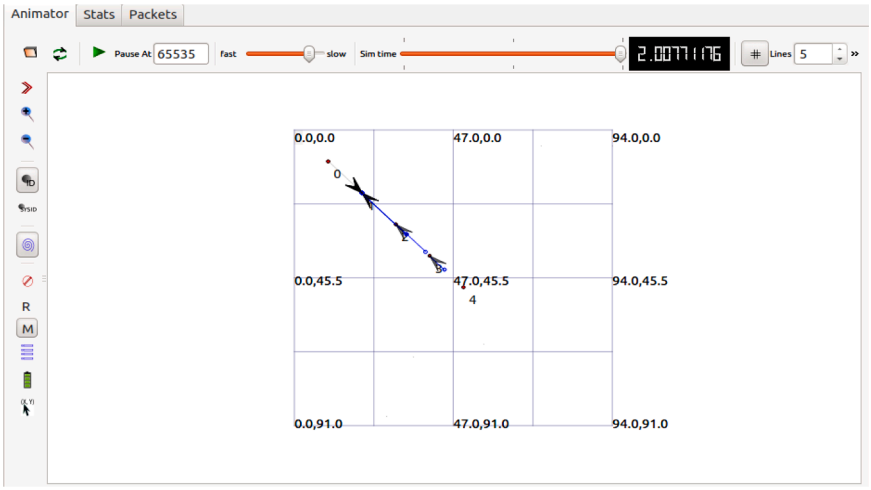

Fig. 9. NS3 Animation for Bus Topology.

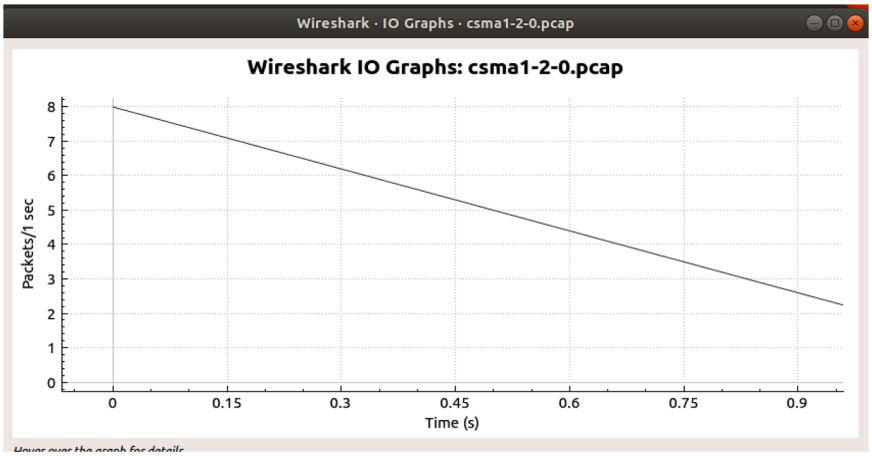

Fig. 10. Efficiency Graph(Packets/*sec*) for Bus Topology.

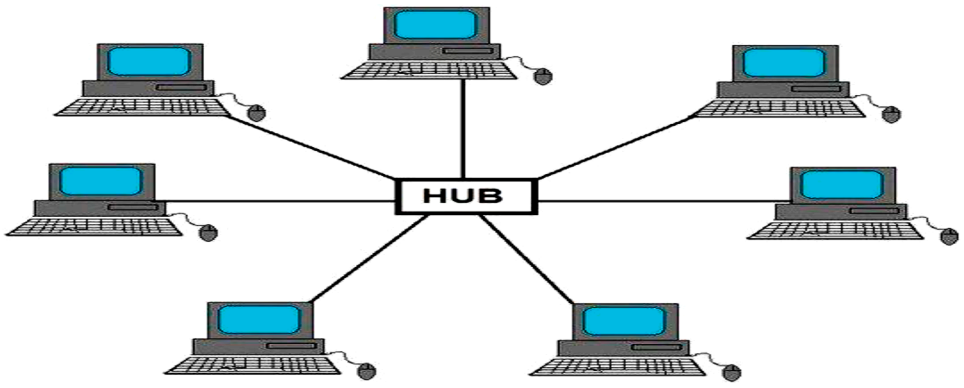

Fig. 11. A Simple Network depicting Star Topology.

not ideal due to channel disruption Fig. 17.

This simulation results of QKD in Star Topology in GNU Plot showed that the given topology has almost constant efficiency as compared to other topologies which keep decreasing with increased traffic Fig. 18.

8. Conclusion

Thus, we can conclude that Quantum Key Distribution or simply, Quantum Cryptography provides us with one of the most secure methods of Communication with high accuracy and reliability with the advantage of detection of an unauthorised party. On the other hand, simulation results of QKD in Star Topology in GNU Plot showed that the given topology has almost constant efficiency as compared to other topologies which keep decreasing with increased traffic Fig. 19.

In the new age, security of data is one of the gravest concerns today. Quantum Key Distribution provides a promising solution to the security,

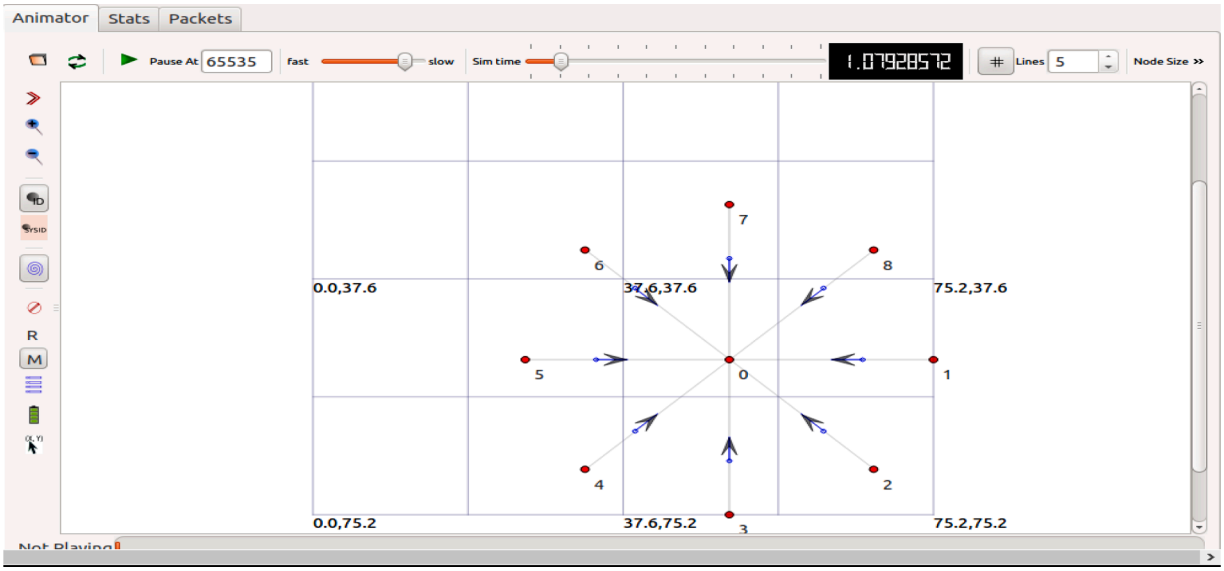

Fig. 12. NS3 Simulation for Star Topology.

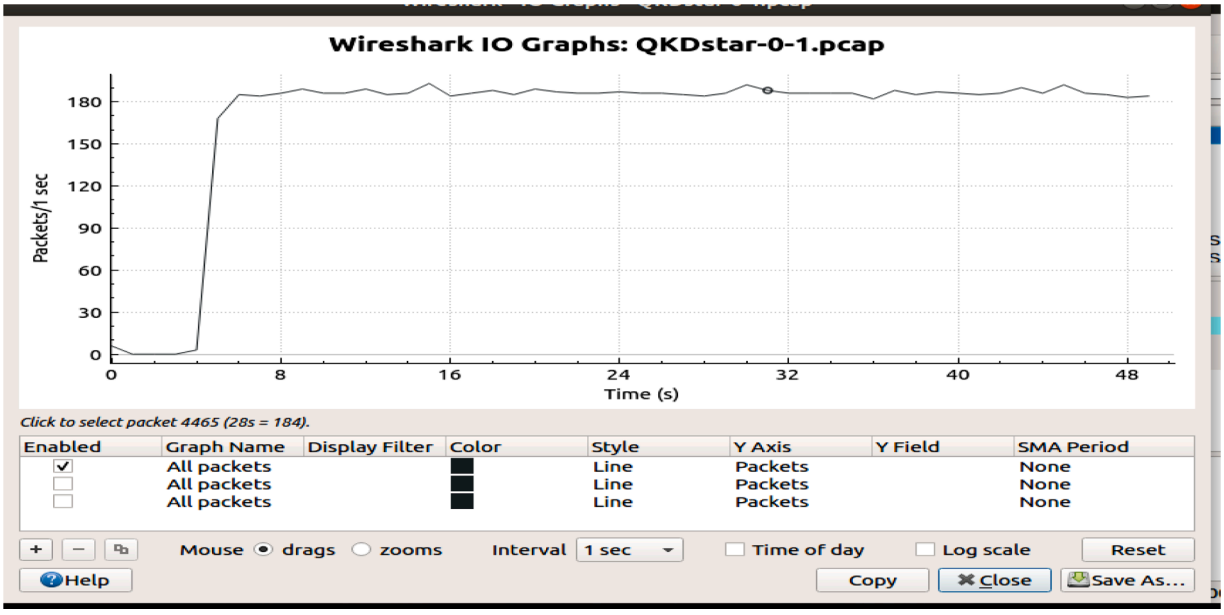

Fig. 13. Efficiency Graph (Packets/*sec*) for Star Topology.

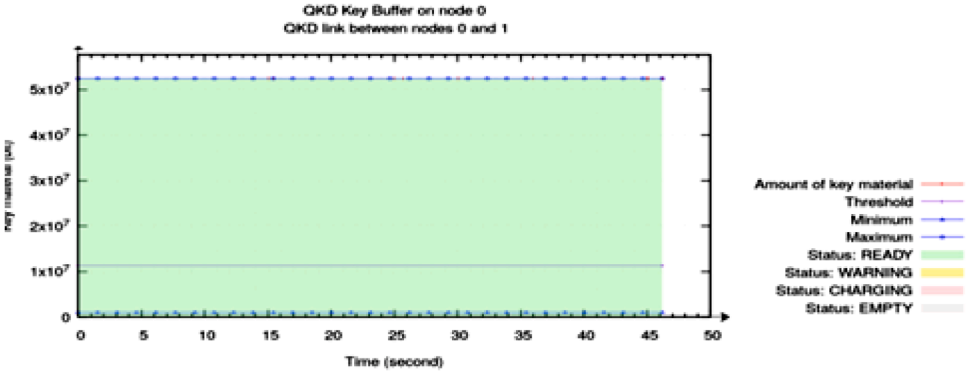

Fig. 14. Quantum Channel between Node 0 and Node 1.

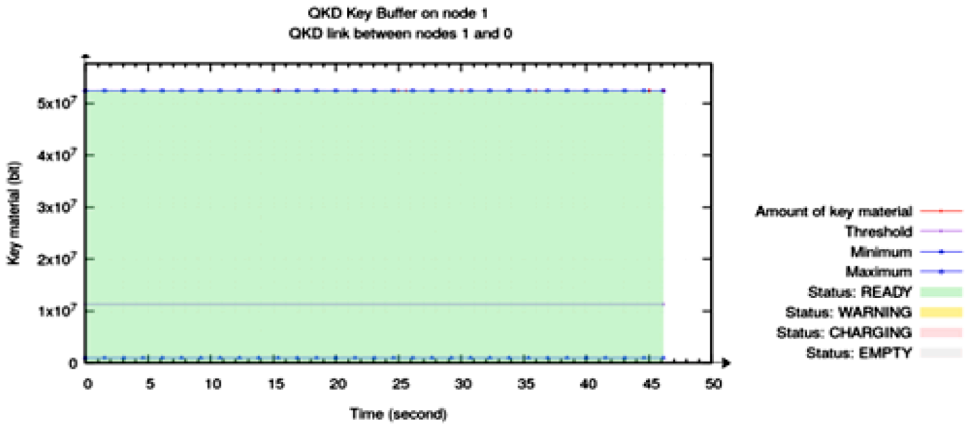

Fig. 15. Quantum Channel between Node 1 and Node 0.

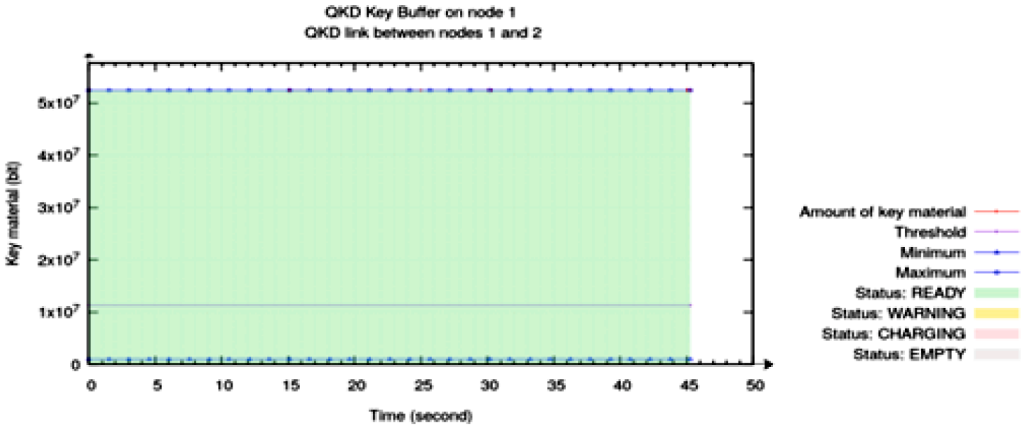

Fig. 16. Quantum Channel between Node 1 and Node 2.

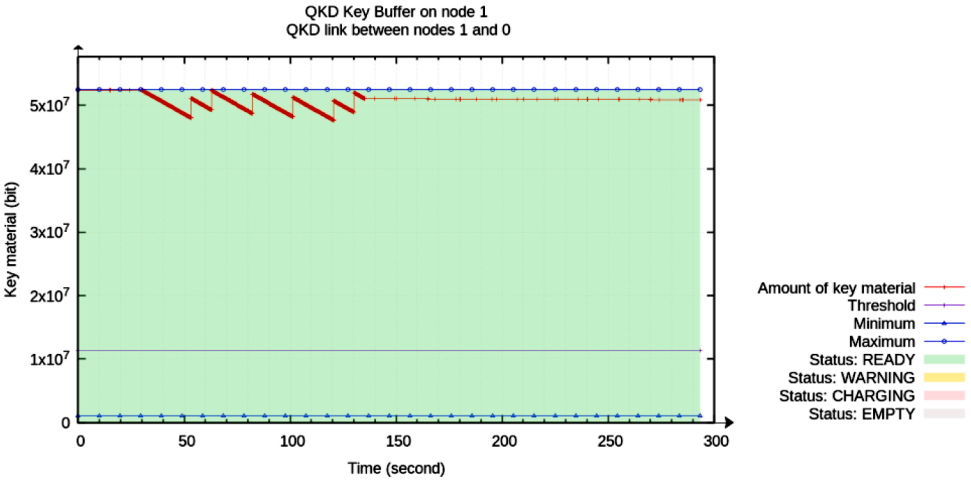

Fig. 17. QKD buffer capacity between nodes 0&1.

reliability and accuracy issues in communication. QKD provides an efficient method for identification of eavesdropper and make the communication more secure. The presence of any eavesdropper can be continuously monitored using the Bell's constant and its detect ability can also be increased by implementing Ekert Quantum cryptography using entangled photon pairs [9]. Additionally, it is hypothesized that a 3 two-party QKDP has combined advantages of classical channel and quantum channel i.e. it can reduce attacks in reputation in p-2-p systems [10]. Moreover, a generally called the distillation process or accurately known as the two way entanglement distillation process which can quiet easily disentangle the eavesdropper from an ensemble of imperfect EPR pairs between Alice (or the sender) and Bob (or the receiver) even in the presence of noise as the pairs can only be purified up to a certain limit of maximum fidelity i.e. Fmax<1 [1]

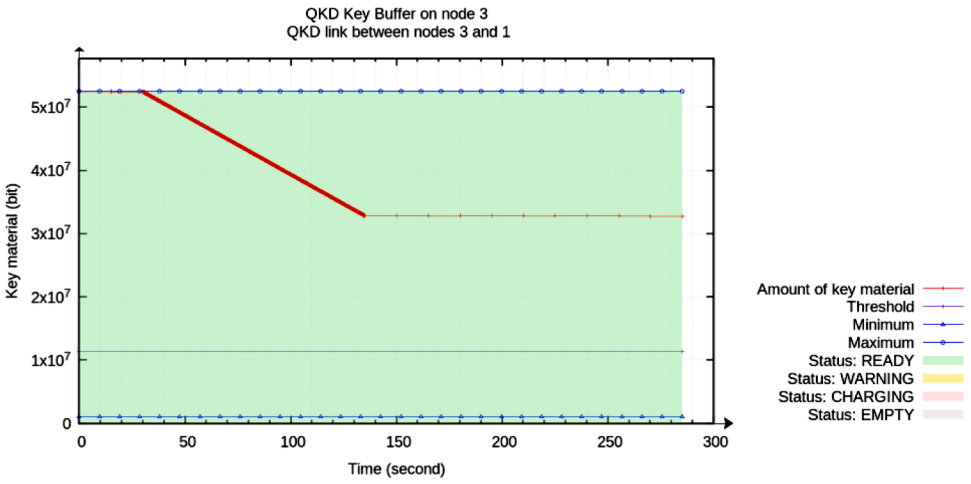

Fig. 18. QKD buffer capacity between nodes 3&1.

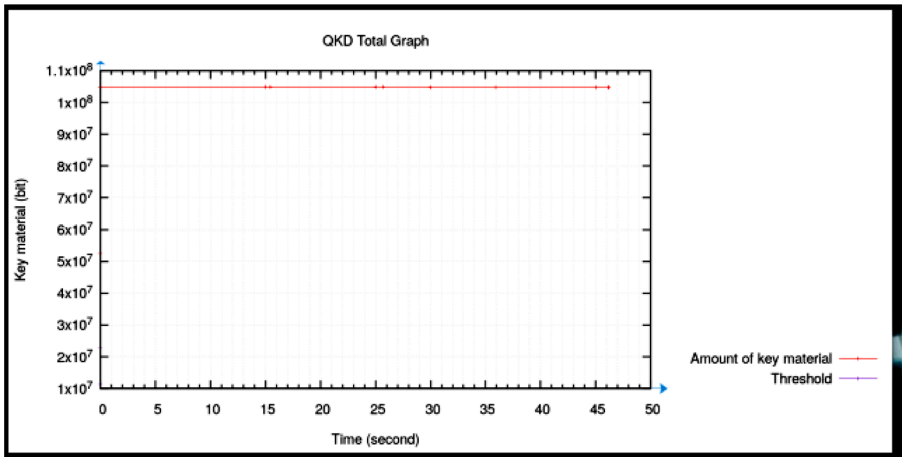

Fig. 19. Total Efficiency of Quantum Cryptography in Star Topology.

9. Future work

As Quantum Cryptography is still in its rudimentary stages of development, there is still a lot of work that has to be done even still. Future work, includes research and development of QKD over wireless networks as well as security of IoT based systems [11]. Furthermore, using quantum cryptography in computers has potential advantage to the era of scientific and technological development. Inclusion of quantum physics to computing is expected to bring about essential development by making use of quantum principles [8].

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] H.ans Aschauer, H.an J. Briegel, Security Proof of Quantum Cryptography based entirely on entanglement purification, Phys. Rev. A 66 (2002), 032302.
[2] M.onireh Houshmand, S.aied Hosseini-Khayat, An entanglement based Quantum Key Distribution Protocol, in: 8th International ISC Conference on Information Security and Cryptology (ISCISC), 2011.
[3] A.bsar Mohammad Jahangir Alam, T.asnuva Ahmed, Performance study of star topology in small inter-networks, Int J Comput Appl (2014).
[4] V.V. Murali Babu Polukonda, A. Harish, Improving security by quantum cryptography in P2P reputation management in distributed identities and decentralized recommendation chains, Int. J. Comput. Sci. Inf. Technol. 3 (4) (2012) 4738–4742.
[5] V. Padmavathi, B. Vishnu Vardhan, A.V.N. Krishna, Quantum cryptography and quantum key distribution protocols: a survey, in: IEEE 6th International Conference On Advanced Computing, 2016.
[6] A. Abushgra, K. Elleithy. QKDP's Comparison Based Upon Quantum Cryptography Rules. IEEE Long Island Systems, Applications and Technology Conference (LISAT), Farmingdale, NY, 2016, pp. 1-5.
[7] S. Praveen Kumar, A.nanya Banerjee, I.nduvali Aishwarya Balaje, S.onali Sharma, Simulation of quantum channel and analysis of its states under network disruption. artificial intelligence and evolutionary computations in engineering systems, Adv. Intell. Syst. Comput. 1056 (2016) 593–602.
[8] J.eremy Goldman, Quantum Cryptography – Current Methods and Technology, cs.tufts.edu, 2014.
[9] D.S. Naik, C.G. Peterson, A.G. White, A.J. Berglund, P.G. Kwiat, Entangled State Quantum Cryptography Eavesdropping on the Ekert Protocol 84, Phys. Rev.Lett., 1999, p. 4733.
[10] M.iralem Mehic, M.arcin Niemiec, M.iroslav Voznak, Calculation of the key length for quantum key distribution, Elektronika ir Elektrotechnika 21 (6) (2015) 81–85.
[11] S.K. Routray, M.K. Jha, L. Sharma, R. Nyamangoudar, A. Javali. Quantum cryptography for IoT: a perspective. 2017 International Conference on IoT and Application (ICIOT).

Mr.S.Praveen Kumar completed his Masters in engineering in Embedded Systems from Shanmugha Arts, Science, Technology & Research Academy, popularly known as ***SASTRA*** University, in 2009, Currently doing Phd from Vels Institute of science, technology and advanced studies (VISTAS) formerly known as VELS university. His-research interest includes Wireless sensor networks, Quantum cryprography,routing and networking in wireless sensor networks. He has 11 years of teaching experience and currently working as Assistant professor in Department of Telecommunication Engineering SRM Institute of science and Technology formerly SRM university. He has supervised 8 post graduate students and 20 undergraduate students for their academic projects. He has published 7 papers in international journals and 7 papers in international conferences. He is also a life member of ISTE,OSI.

Dr.T.Jaya completed his Phd from College of engineering Guindy - Anna university. His-research interest includes Wireless Networking and underwater Communications. He has 11 years of teaching experience and 7 years of Industry Experience and currently working Vels Institute of science, technology and advanced studies (VISTAS) formerly known as VELS university.

Dr.K.Vijayan completed his Phd from Vels Institute of science, technology and advanced studies (VISTAS) formerly known as VELS university. His-research interest includes Wireless sensor networks,VLSI circuits and systems, routing and networking in wireless sensor networks. He has completed his Masters in engineering in VLSI design from College of engineering Guindy - Anna university in 2003. He has 17 years of teaching experience and currently working as Assistant professor in Department of Telecommunication Engineering SRM Institute of science and Technology formerly SRM university. He has supervised 15 post graduate students and 20 undergraduate students for their academic projects. He has published 10 papers in international journals and 7 papers in international conferences. He is also a life member of ISTE,IETE,IAENG and IACSIT.

Dr. S. Yuvaraj, has completed his BE in Electronics and communication engineering in 2008 from Anna university, M. Tech -VLSI Design from SRMIST in 2010 and received his phd degree in the year 2019 in the field of cyber physical security. He has 11 years of teaching experience and currently working as Assistant professor in Department of Telecommunication Engineering SRM Institute of science and Technology formerly SRM university with 20 indexed publication and three patents.