Quantum Key Distribution Mechanism in Optical Networks : A Review

Maninder Kaur
M.Tech (scholar)
Department of electronics and communication, Punjabi University , Patiala, Punjab(India).

Abstract- In this review , we describe several aspects of QKD (Quantum Key Distribution) technology and network design which can theoretically give un-conditional security for communication systems. This technology is believed to be able to given security levels which are needed to with-stand the threats realized by future computing technology adding QCs (Quantum Computers). The power of QKD is independent of maths and calculating power of adversary. In QKD twice legitimate parties say Sender and Receiver can share a protect private key under the nose of listener. The information can be encrypted in the properties of light by its polarization techniques and transmitted as QI (Quantum Information) bits via QC (Quantum Channels). If these bits are eavesdropped then, its state will alter. An existing shared authentication classical channel performs the post-processing and KD to finally create the SK (Secret Key). Analysis of the QKD process explained in detailed and brief explanation in attacks used in QKD like DoS, Trojan, Man-middle atatcks and many more. It analysis to increase network intelligence, which is gradually shifting towards industrization. Moreover, novel threats are emerging example CMT (Control Message Transferred) via the control channels are vulernable to eavesdropping and interception. DE (Data Encryption) is an efficiency path to improve the security of connection as-well-as control message transmitted in software defined ntwork. QKD is being measured as a protect structure to provisional keys for confidential data encoded, which is a potential method to secure communications for security attacks in SD (Software Defiend) Optical Networks.

Keywords- Software Defined optical Network, Quantum Key Distribution, Data Encryption and DoS (Denial of Service).

I. INTRODUCTION

In the last few decades, with the spread of more un-secure CNs(Computer Networks) , a real requirement was handled to utilize cryptography in a huge scale. The SK (Symmetric Key) was searched to be non practical due to challenges , it faced for KM (Key Management) . It gave increase to the PK (Public Key) crypto networks which are world-wide used today. PKC development in maths, while these networks might secure today, future calculating technologies, adding quantum computing, are likely to reduce these networks in-security.

The concept of quantum key was initialized with use of the polarized encoded photons and these are transferred within the free space that covered the distance of 30 cm. After that, the process of quantum keys is utilized in the field of optical fibers gradually it gained a lot of attention from the researchers in the optical communication [1]. The process of quantum key distribution also referred as QKD which gives a method to enhance the process of increasing the secure keys. These keys are generally shared the data. Its first protocol is the BB84 which was initialized in the mid of the 1900's and discovered by Bennett and Brassard [2]. The protocols are increased and the new versions are come under consideretion in several years. A new concept is involved in the quantum key is the cryptography. The quantum cryptography (QC) is released to the new information security needs. It is relied on the principles of the cryptography primitives. QKD is the most usable key protocol which utilized mainly for the creation of the symmetric keys via the features of the quantum and it proceeds in light. Light is the transmission medium which transferred the data from one place to another [2].

In this paper, analyses networks depend on QKD technology which has been notionally established to be un-conditionally secure and will give a much higher-level of protection that can be with-stand threats which can realized by future computing technologies.

a. Quantum Key Distribution

It exploits the main fundamental rules of quantum PHYSICS. The un-conditional security relies on the point that conseration causes perturbation. The power of QKD is independent of maths and calculating power of adversary. In QKD twice legitimate parties say Sender and Receiver can share a protect private key under the nose of listener. The information can be encrypted in the properties of light by its polarization techniques and transmitted as QI (Quantum Information) bits via QC (Quantum Channels). If these bits are eavesdropped then, its state will alter. An existing shared authentication classical channel performs the post-processing and KD to finally create the Sk (Secret Key) [3].

II. QUANTUM KEY DISTRIBUTION PRINCIPLES AND PROCEDURE

In this section, normally used the QKD principles are summarized. In author (1984) [4] published the 1st quantum key distribution depend on polarization ecrypting. Sender and receiver are twice legitimate parties with an existing shared QC and ACC (Authenticated Classical Channel) respectively. Sender sends a series of randomly polarized photons in dissimilar polarization states to receiver over a QC (Quantum Channel). Receiver arbitrarily chooses and measures the state. He keeps a note of the resultant state and basis choosen for measurement. Sender and Reciever signal broadcast their

measurement bases and thereafter reject the consequences for which mis-matched bases were utilized and thereby create a shifted key. They calculate the Quantum Bit Error Rate (QBER), identify the presence of an eavesdropper. Then they generate a protect key after classical post-processing phases which add exception correction and privacy amplification .

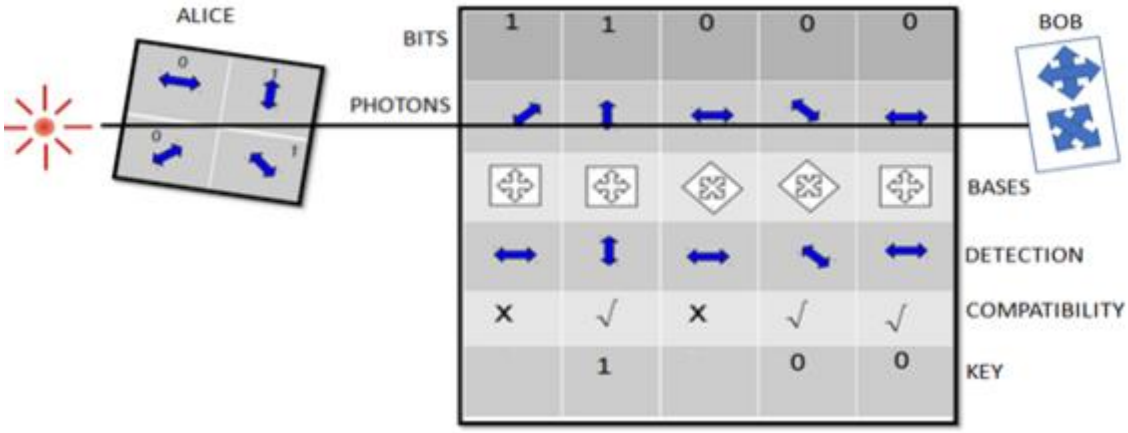

Fig.2: BB84 Principle

Ekert method utilizes entangled couples of photons. These can be generated by either sender and receiver and other source. The photons are divided so that sender and receiver possess single photon form individual couple. The method relies on the fact that entangled states are effortlessly correlated and any attempt at eavesdropping will finish these co-relations in a path that sender and receiver can detect the presence of eve.

Bennet implement another rule called B92 which uses only twice nonorthogonal states. The rule has been given to be un-conditionally protect. Like the BB84, sender transmits to receiver a string of photons encrypted with randomly selected bits, but this interval of time the bits send by sender must utilize. Reciever still randomly selects a basis by which to consider, but if he selectes the wrong basis, he willn't considerThe security of Quantam Key Distribution are ; anything, a situation in QMs (Quantum Mechanics) which is called as an removal.

Coherent single-path protocol is a novel rule for QC (Quantum Cryptography) with time encryption. The experimental set-up is easy and it is tolerant to optimized distortion visibility and the PNS intrudres. It creates a higher secret BR (Bit Rate).

DPS-QKD (Differential Phase Shift) is a novel QKD method that was implemented . Sender randomly step-modulates a pulse train of weak coherent state by 0, pie for each pulse and sends it to receiver. It considers the phase dissimilar between twice series pulses using MZ interferometerand single photon detectors.

QKD Process

There are three steps :-

i) Exchange key :- The photon which are sent by Sender and Receiver via quantum channel constitutes the raw key.

ii) Shifting Key:- Raw key then under-goes the modifying procedure in which photons with similar bases are choosen and set of them are described in a sifted key [5].

iii) Distillation key :- The moved key will be plentiful in exceptions which are created either by an eavedropped or due to im-perfections in the Quantam Key Distribution equipment and transmission line.

iv) Exception Correction :- It is a procedure where sender and receiver with proven shifted key arrive to a normal series. The protocol is most normal for exception correction , but it is highly inter-active , the moved key is separated into blocks, thereafter parties is computed and compared.

i) Mathematical process
ii) No-cloninh theorem
iii) Non-realism
iv) Non-community [6]

III. RELATED WORK

Zhao, Y., et al., (2018) [7] proposed the deep description of resource allocation in the optical networks which was basically secured through QKD (Quantum Key Distribution).These days, the optical network security was being a fascinating concept for the researchers and in the networking field. The loss of private data on the network was easily influenced the majority of users. Therefore, the need was to encrypt the data and it was considered the most usable method to protect the data on networks. Consequently, QKD was predicted to be more secure scenario which was responsible for generating different keys mainly for the encryption of data. In QKD, two other channels were concatenated as namely as QSch and PIch specifically for the synchronization. At the time of network designing, there was need of securing resources also. Hence, the current research was adopting OTDM (Optical Time Division Multiplexing) which had the capability for the allotment of multiple channels

in the network with similar wavelength. Next to it, RWTA (Routing, Wavelength, Time-Slot and Assignment) method was utilized for the allocation of time and wavelength mainly on three categories of channels. There were different security phases that were generally used in RWTA via updation in the secure keys. The experiment demonstrated that, the effect of the security levels were also influenced the allocation of resources in the network. **Rajpoot, S., et al., (2017) [8]** represented the upcoming trends in the fiber optic communication ways. The most of the useful impetus was the great usage of fiber optics which was generally high and increased the number of users as well as for the business. The interest of business was seen more in the media transmission and the web related purposes. Basically, the fiber optical systems were the most crucial form of media transmission mainly used in every broadband service. In the current applications, the most important requirement was the capability of data transmission under the low delay. It was giving a vast variety of transmission methods and the high speed. The present research was related to the detailed description of the fiber optics. It generally composed of the advancement of keys, mechanical issues and the updation in the next generation of networks.**Essaiambre, R.J., et al., (2012) [9]** described the capacity related trends in the optical networking with its restrictions. From the first development of the optical communication, the capacity by the single optical fiber was raised via 10000 times. The growth was reached at the peak in the first few decades and therefore, the traffic of data was also flourished by a factor of 100. The next 100 factors were noticed in one decade. Therefore, the difference in the growing rate and the delivery capability of fibers were assumed to the shorter approximately in 10 years. The first section of current research was related to the background of the data traffic and the increase of the capacity for the upcoming time periods. The second section of research was described the technological related issues which were obtained due to the raise of capacity of single fibers. The third section was utilized to represent the elementary capacity specifically for the data transmission in the multi modes and to make a comparison with the single mode transmission. At the end, the main discussion was about the fiber and its supportive spatial modes. These modes were combination of multimode and the multicore and also these were playing out a major role in the field of digital processing methods. It was assumed that, the spatial modes were enabled the systems to increase the growth and to complete the requirements of traffic raise in few years.**Idachaba, F., et al., (2014) [10]** proposed the future concepts related to the fiber optical communication. The raising driving forces were associated to the large demand of fiber optic communication and it was growing sharply as well as the demand of consumers and the commercial needs were also flourished due to the use of telecommunication capacity and the usage of internet. The fiber optics was essential in the field of telecommunication for the broadband networks. The large bandwidth signals for the data transmission with reduced delay was the crucial need in the current applications of networking, it was capable to give access for the un-surpassed transmission bandwidth with reduced latency. In the current research, the overview of fiber optic systems was described and the new technical trends were given for the next generation of telecommunication.**Liga, G., et al., (2017) [11]** recommended the information rates of the long haul fiber schemas with its coded modulation. A detailed description was given on the performance of long haul efficient WDM (Wavelength Division Multiplexing) fiber model with different decoding structures. The desired information rates were obtained mainly for the different QAM (Quadrature-Amplitude Modulation) format. The optimal format was considered as the function of distance and the decoder implementations. The four case analyses were utilized to concatenate the hard decision and the soft decision together with a de-mapper. The de-mapper was a bit wise or a symbol wise. The information rates were evaluated on the basis of the unmatched decoder concepts. With the combination of decoder, two different approaches were analyzed as EDC (Electronic Dispersion Compensation) and DBP (Digital Back-Propagation). It was clear that, some of the methods which were relied on the hard decisions were acquire more rates of data rather than soft decisions.**Jabbar, M.A., et al., (2017) [12]** utilized various methods for the data transmission by optical systems. In this technical world, the signal communication was being an interesting topic for researchers and an essential need to fulfil the needs of new advancements. It was happened because of the processing of large amount of data and the data was mainly in the form of text, voice, images, videos, audio and so on. Therefore, to process the large amount of data, the need of transmission capacity also increased. The medium utilized for the transmission of data must be a copper wire but it had reduced capacity. Hence, the issues were raised and required to be managed. A new method was considered which had the tendency for processing large data, higher signals and the long communication. The research work focused on the structure and the modeling procedure of the channels in the optical communication. Basically, it utilized the light waves as the carrier for the transmission of data. The present work was described the different characteristics and determined the performance as well as design a framework communication system via using different transmission and reception approaches. The optisystem results were considered as a novel simulation approach for the deployment of optical modules. It implies on the transmitter which changed the signals into light, fiber optic channels and it reverts the process to change the light into original signal.

IV. ATTACKS IN QUANTUM KEY DSTRIBUTION (QKD)

It is given to be un-conditionally protect, but it is implement is vulnerable to various attacks. The need considers are adopted accordingly for illustration, inserting trick photons etc and altered protocols are overviewed to counted these attacks. [13]

i)Beam-Splitting Attack :- it can replace the quantum channel with a loss less one and place a bean splitter in its way.

ii) Entaglemeny and Consider Attack :- it can entangle her qubit with the photon and will extract the data by evaluating the consideration on her qubit.

iii) Timing Attack :- if the light source and destinations aren't synchronized then eve can attain the data about the detector which had clicked by hearing the interval of time signature announced by receiver.

iv)DoS Attack :- It can disrupt the photons in the channel by either applying few unitary blocking the line.

V. OPEN CHALLENGES AND PROBLEMS

Recent work, main focus on how to enhance the BR (Bit Rate) and TD (Transmission Distance) of quantam signals using prior OF (Optical Fibre). Moreover, there are various research problems and challenges on the networking aspect of a Quantum Key-distributio enabled to be identified , which are stated below:-

i) Resource Allocation [14]
ii) Security Level
iii) Trusted Repeater Node Placement
iv) Resiliency in Quantum key Distribution enabled [15]

VI. CONCLUSION AND FUTURE SCOPE

In this conclusion, the performance of every network depend on its fundamental operation rules, designs and process in QKD (Quantum Key Distribution) . While the security of QKD is depend on rules of quantum structure the design method determine the strength of security that given. In survey paper , concluded the various protocols and process detailed explained in QKD. The protocols are increased and the new versions are come under considered in several years. A new concept is involved in the quantum key is the cryptography. The quantum cryptography (QC) is released to the new information security needs. It is relied on the principals of the cryptography primitives. QKD is the most usable key protocol which utilized mainly for the creation of the symmetric keys via the features of the quantum and it proceeds in light. Light is the transmission medium which transferred the data from one place to another.

Further , free memory QKD (quantum key distribution) designs will improve the rangle pf applications, adding secure satellite to ground station communication.

VII. REFERENCES

[1]. Xavier, G. B., Walenta, N., De Faria, G. V., Temporão, G. P., Gisin, N., Zbinden, H., & Von der Weid, J. P. (2009). Experimental polarization encoded quantum key distribution over optical fibres with real-time continuous birefringence compensation. New Journal of Physics, 11(4), 045015.

[2]. Singh, H., Gupta, D., & Singh, A. (2014). Quantum key distribution protocols: a review. IOSR Journal of Computer Engineering (IOSR-JCE), 16.

[3]. Bennett, C. H. (1984). Quantum crytography. In *Proc. IEEE Int. Conf. Computers, Systems, and Signal Processing, Bangalore, India, 1984* (pp. 175-179).

[4]. Pathak, Anirban. *Elements of quantum computation and quantum communication*. CRC Press, 2013.

[5]. Scarani, Valerio, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev. "The security of practical quantum key distribution." *Reviews of modern physics* 81, no. 3 (2009): 1301.

[6]. Inoue, Kyo, Edo Waks, and Yoshihisa Yamamoto. "Differential phase shift quantum key distribution." *Physical Review Letters*89, no. 3 (2002): 037902.

[7]. Zhao, Y., Cao, Y., Wang, W., Wang, H., Yu, X., Zhang, J., and Mukherjee, B. (2018). Resource allocation in optical networks secured by quantum key distribution. IEEE Communications Magazine, 56(8), 130-137.

[8]. Rajpoot, S., Singh, P., Solanki, S., and Yasin, S. J. (2017). Future Trends in Fiber Optics Communication. International Journal on Cybernetics & Informatics, 6, 23-28.

[9]. Essiambre, R. J., and Tkach, R. W. (2012). Capacity trends and limits of optical communication networks. Proceedings of the IEEE, 100(5), 1035-1055.

[10]. Idachaba, F., Ike, D. U., and Hope, O. (2014, July). Future trends in fiber optics communication. In Proceedings of the World Congress on Engineering (Vol. 1, pp. 2-4).

[11]. Liga, G., Alvarado, A., Agrell, E., and Bayvel, P. (2017). Information rates of next-generation long-haul optical fiber systems using coded modulation. Journal of Lightwave Technology, 35(1), 113-123.

[12]. Jabbar, M. A., Albaker, B. M., and Iqbal, S. Z. (2017). Using Different Techniques in Data Transferring by Optisystem Program. American Journal of Optics and Photonics, 5(6), 59.

[13]. Takesue, H., E. Diamanti, T. Honjo, C. Langrock, M. M. Fejer, K. Inoue, and Y. Yamamoto. "Differential phase shift quantum key distribution experiment over 105 km fibre." *New Journal of Physics* 7, no. 1 (2005): 232.

[14]. Lo, Hoi-Kwong, Marcos Curty, and Bing Qi. "Measurement-device-independent quantum key distribution." *Physical review letters* 108, no. 13 (2012): 130503.

[15]. Liu, Yang, Teng-Yun Chen, Liu-Jun Wang, Hao Liang, Guo-Liang Shentu, Jian Wang, Ke Cui et al. "Experimental measurement-device-independent quantum key distribution." *Physical review letters* 111, no. 13 (2013): 130502.