xIlkogretim Online - Elementary Education Online,2021; Vol 20 (Issue 1): pp.2427-2429
http://ilkogretim-online.org
doi: 10.17051/ilkonline.2021.01.272

Linking Quantum Key Distribution To Space Communication: State Of The Art

Shriya Kapoor, Department of Electronics and Communication Engineering, SRM Institute of Science and Technology, Tamil Nadu, India
Sandeep Kumar, Department of Electronics and Communication Engineering, SRM Institute of Science and Technology, Tamil Nadu, India
Vivek Maik, Department of Electronics and Communication Engineering, SRM Institute of Science and Technology, Tamil Nadu, India
Arvind Lakshmanan, Department of Electronics and Communication Engineering, SRM Institute of Science and Technology, Tamil Nadu, India

Abstract-This paper offers a thorough research about the current whereabouts of quantum encryption in space communication. Due to the difficulties faced in extending transmission distance beyond a few hundred km, satellites are used as middle nodes. Success of Micius Satellite under QUESS supports the feasibility of such operations. However, multiple factors need to be taken into consideration, which have been listed in this work. Global projects have been undertaken for securing the links with the help of quantum key distribution. Hence, this review paper acts as a backbone, offering major factors effecting this approach.

Keywords: Quantum encryption, Space communication, Quantum Key Distribution

I INTRODUCTION

Security of a communication link can prove to be a liability in case of intrusions. Under classical methods of encryption (Symmetric or Asymmetric), this measure of security has remained intact for quite a while. However, their reliance on 'private/public keys' brings them into the danger spot. A comparison between classical and quantum encryption methods in [1], clearly supports the secure results obtained by QKD.

With the advent of Quantum encryption techniques, the classical methods of encryption will become highly vulnerable and obscure. Quantum Key Distribution is such a technique (under Quantum Encryption) that prevents any sort of eavesdropping and hence increasing the security of the link. Nevertheless, QKD has its own limitations and advantages. Its applicability in space-satellite communication has increased its popularity to great extent. Quantum Key Distribution has many variants including: Continuous Variable (CV QKD), Discrete Variable (DV QKD), Detector Device Independent (DDI QKD), Measurement Device Independent (MDI QKD.

Generally, CV QKD requires the transmitter, commonly known as Alice, to send a Local oscillator signal alongside the main quantum signal. This factor weakens the performance of CV QKD. Hence, Shengjun Ren et al [2] proposed a Self-Referenced method which generates the local oscillator signal at the receiver itself (Bob). After conducting the experiment successfully, they were able to achieve secure key rates of 1.69Mbps for 15km and 649kbps for 25 km. These authors also claim an extension of up to 92km distance until the key rate drops to zero. A similar work of establishing an economical QKD link over metropolitan area and submarine has been demonstrated in [3]. It has been made successful with the use of dark fiber and time-bin encoding. However, the methods utilized so far have been employed over wired point to point connections. This setup can be taken to a higher level by the incorporation of drones for Quantum Key Distribution link setup over 10km as discussed by the authors of [4].

II LITERATURE SURVEY

This section discusses about the extensive research work done in Space Communication with the help of Quantum encryption techniques.It has been seen that the transmission distance (over land) of secure QKD link is limited due to the various atmospheric effects. Moreover, as a result of no-cloning theorem, a quantum-based signal cannot be amplified without noise. Hence, limiting the transmission distance. At the present state, there are two possible solutions: Quantum repeaters or Satellites as intermediate nodes. Diverse methods have been suggested for repeaters [5], still the advancements and feasibility of satellites as nodes is more likely. Such losses are bare minimum in vacuum or free space, thus offering an easy establishment of link. [6] The use of low earth orbit satellites (night time) has gained a kHz key rate extending up to 1200km. [7] Downlink offers a less attenuation path compared to uplink and thereby offering a better link efficiency. Few losses experienced in this link were: diffraction loss (22dB), Atmospheric absorption and turbulence (3-8dB), pointing error (<3dB). Some other limiting factors can be due to low coverage area of LEO. [8]

Nevertheless, a single satellite is not sufficient. Donghai Huang et al. proposed a double layer system network including a combination of LEO and GEO satellites. Using this setup, the authors have succeeded in developing a routing and key allocation which provides better outcomes in comparison to single satellite systems, as per simulation results. [9] As a future work, MEO satellites can be incorporated to form a multiple layer network. An unexpected range of 2500km has been achieved by authors of with the use of MDI-QKD and repeater setup. [10] MDI-QKD makes it easier at user end and compatible with repeaters. However, billions of Quantum Memories are required (to achieve mere 1kb/s key rate) and Error Correction schemes have not been taken into account. A lot many countries have taken up satellite projects based on QKD over the period. List of such missions and projects has been depicted in [11]. Implementing Downlink configuration with the use of GEO-satellites, designing of four laser diodes in a single transmitter and Thermal management of space-based device are certain positive outcomes of the work. [12] Added to this are some drawbacks of Random polarization rotation and vibration, Fast-Detectors based on superconducting technology are costly and insufficient speed of the established key. Furthermore, the authors have kept a broad eye over the future outcomes for Efficient working and increase in lifetime of QKD link, Quantum Sensors for gravimetry and mineral exploration. Many such missions have been proposed such as NanoBob, NanoQEY, CQuCoM, while some are funded projects including CAPsat and QEYSSat. [13] A study on Quantum Encryption and Science Satellite (QEYSSat) under the Canadian Space agency has been made by authors of [14]. This microsatellite weighs about 20kg with 30W of power consumption. Based upon numerical analysis, its capability to communicating to the ground station while withstanding various hindrance effects was scrutinized. Moreover, it was concluded that only 100seconds were sufficient for a secure key generation.

Attacks in satellite communication can have three targets: ground station, satellite or the communication link. A detailed survey [15] shows that attacks on ground station are the most common, followed by RF links. Some of the open challenges in this field have also been mentioned. Key rate, cost and robustness, distance pose some hindrances to the implementation [16]. Eleni Diamanti et al. also discusses about some recent advancements in the QKD protocols. Apart from the hardware and developmental limitations, atmospheric impacts also play a major role. Fog, Haze, unstable eddies severely affect in the first 10-20km from ground [17]. Simulations based on MODTRAN5, have shown that these phenomena are larger for uplink than downlink. Furthermore, night time is more suitable than daytime due to the temperature variations and unstable eddies (during day). Such factors have been in direct support with the Micius Satellite. Error Analysis plays a crucial role in understanding the data or information received. A novel method including removal of errors in QKD have been proposed in [18].

III CONCLUSION

The detailed literature survey provides a clarity about the present status of quantum encryption in space communication. With many possible options, MDI QKD is widely chosen especially BB-84 protocol. Distance remains to be a hindrance factor mainly in terrestrial communication. Cost and Hardware also act as obstacles. Added to these are the hurdles provided by atmospheric factors. Taking them into consideration, it can be concluded that downlink is more preferable due to comparatively less losses than uplink. Furthermore, night operations are most suitable for communication links using QKD due to multiple factors listed above. Constellation and multiple layers of satellites can provide an unobstructed pathway. Especially, the use of MEO-GEO satellites instead of LEO. Although it may get redundant and add to the cost.

Most of the research done so far has not mentioned or included error mitigation and detection techniques which can play a major role. A lot of future projects are possible incorporating quantum key distribution technique as encryption including quantum fingerprinting, quantum digital signatures, quantum sensors for gravimetry and mineral exploration.

REFERENCES

1. H. R. Pawar and D. G. Harkut, "Classical and Quantum Cryptography for Image Encryption & Decryption," 2018 International Conference on Research in Intelligent and Computing in Engineering (RICE), San Salvador, 2018, pp. 1-4
2. S. Ren, S. Yang, A. Wonfor, R. Penty and I. White, "Demonstration of Robust Self-Referenced Continuous Variable Quantum Key Distribution over 25km Fiber Link," 2020 Conference on Lasers and Electro-Optics (CLEO), San Jose, CA, USA, 2020, pp. 1-2.
3. Vagniluca, D. Bacco and A. Zavatta, "Fiber-Based Stations for Quantum Key Distribution Field Trials over Installed Fiber Links," 2020 22nd International Conference on Transparent Optical Networks (ICTON), Bari, Italy, 2020, pp. 1-4.
4. S. Isaac et al., "Drone-Based Quantum Key Distribution," 2020 Conference on Lasers and Electro-Optics (CLEO), San Jose, CA, USA, 2020, pp. 1-2.
5. W. J. Munro and K. Nemoto, "Routing on Quantum Repeater Networks," 2020 Conference on Lasers and Electro-Optics (CLEO), San Jose, CA, USA, 2020, pp. 1-2.
6. Z. Li et al., "Experimental demonstration of all-photonic quantum repeater," 2019 Conference on Lasers and Electro-Optics (CLEO), San Jose, CA, USA, 2019, pp. 1-2.
7. P. K. Lam et al., "Building a quantum repeater with quantum memories and noiseless amplifiers," 2013 Conference on Lasers and Electro-Optics Pacific Rim (CLEOPR), Kyoto, 2013, pp. 1-2.
8. N. C. Jones, K. De Greve and Y. Yamamoto, "Fault-tolerant quantum repeaters for long-distance quantum communication based on quantum dots," 2012 Conference on Lasers and Electro-Optics (CLEO), San Jose, CA, 2012, pp. 1-2.
9. Y. Liu, L. Zhang and X. Zhang, "A quantum repeater in infrared quantum communication system," 2010 3rd International Conference on Biomedical Engineering and Informatics, Yantai, 2010, pp. 2824-2827.
10. Liao, S., Cai, W., Liu, W. et al. Satellite-to-ground quantum key distribution. Nature 549, 43–47 (2017)
11. D. Huang et al., "Quantum Key Distribution Over Double-Layer Quantum Satellite Networks," in IEEE Access, vol. 8, pp. 16087-16098, 2020
12. Nicoló Lo Piparo, Mohsen Razavi, “Long-Distance Trust-Free Quantum Key Distribution,” arXiv:1407.8025, 2013
13. Bedington, R., Arrazola, J.M. & Ling, A. Progress in satellite quantum key distribution. npj Quantum Inf 3, 30 (2017)
14. T. Jennewein, "Towards Quantum Communications with Satellites," 2018 IEEE Photonics Society Summer Topical Meeting Series (SUM), Waikoloa Village, HI, 2018, pp. 217-218
15. Manulis, M., Bridges, C.P., Harrison, R. et al. Cyber security in New Space. Int. J. Inf. Secur. (2020)
16. Diamanti, E., Lo, H., Qi, B. et al. Practical challenges in quantum key distribution. npj Quantum Inf 2, 16025 (2016).
17. Carlo Liorniet al. Satellite-based links for quantum key distribution: beam effects and weather dependence2019 New J. Phys. 21 093055
18. S. Baili, H. Shangfu, Z. Xiao and W. Zhihui, "An Improved Method of Quantum Key Distribution Protocol," 2009 International Forum on Computer Science-Technology and Applications, Chongqing, 2009, pp. 115-117