Quantum Key Distribution for Internet of Things (IoT) - A Review

Kowsalya T, Sukirtha S, Krithika S

Abstract— **Abstract-In recent years the concept of IOT has gained so much attention that it is merely impossible to imagine our lives without it. IOT is the process of connecting, interacting and sharing information between things helping them to communicate. With its growing importance, the privacy and security details of the users is eventually being subjected to risks. It is not difficult for a person with technical knowledge to hack any information online. This demands the need for a furthermore secure platform of communication for the users. This is where the Quantum key distribution (QKD) comes into play. QKD basically deals with photons, the nature of which is hidden within the nature ' itself '. Any sort of eavesdropping during a communication can be detected easily in QKD. So, this review paper emphasizes QKD as a provably secure way of communication in IOT**

Index Terms— **Internet of things (IOT), privacy and security, quantum key distribution (QKD), hack, eavesdropping**

I. INTRODUCTION

Internet of things (IOT) is in a boom. It forms the basis of the digital era. But the basis of IOT lies in Receiving, storing and retrieving information. Information in its raw form called the plain text is being subjected to a lot of security and privacy issues. For this purpose, code Encryptions are used. Encryption codes or keys should be easy to generate but hard to break. Encryption is all about manipulating the information (plain text), with a factor (cipher) and forming the new form of data (ciphertext) to be stored and used for future access. The ciphertext has to be decrypted in order to retrieve the information. This ciphertext can be decrypted only by the concerned parties and not by any unauthorized agent. There are many algorithms such as the RSA algorithm which is currently in practice for this process. This algorithm involves generating a public and a private key, where the public key is distributed and the private key is kept secret. IOT plays a main role in military, government, finance, online transactions and a lot more. All these domains require extreme data protection which is provided the encryption algorithm. The effectiveness of the algorithm lies in the hardness of breaking it. Usually these codes are the products of very large prime numbers that requires more time in breaking it using the modern computers. But once Quantum computers are put in action, this can be done so quickly and easily. All our information is again subjected to risks. This is where Quantum Key Distribution comes into play.

Manuscript received October 31, 2019

Kowsalya T , Student, Department of ECE, Kumaraguru College of Technology, Coimbatore, Tmilnadu, INDIA

Sukirtha S , Student, Department of ECE, Kumaraguru College of Technology, Coimbatore, Tmilnadu, INDIA

Krithika S , Assistant Professor, Department of ECE, Kumaraguru College of Technology, Coimbatore, Tmilnadu, INDIA

II. QUANTUM KEY DISTRIBUTION

Quantum key distribution (QKD) deals with photons. It makes use of the photons to generate the Key. It is based on Quantum rather than classical physics. Quantum mechanics has its unique property of quantum indeterminacy. Any act of measuring the photons will change its state. Hence, breaking a quantum key is not hard but impossible. The advantage of QKD is that any act of eavesdropping can be easily detected and the communication can be aborted if it is greater than a certain threshold and continued if the rate of eavesdropping is below the threshold. The Quantum Superposition and Quantum Entanglement are the properties involved in transmitting the private key. Quantum Superposition involves representing the sum of two waves (superimposed) as one or vice versa. Quantum Entanglement involves representing the quantum state of a particle in a system that cannot be done independently but only as a whole due to their spatial proximity.

In this process the public key is generated in the usual way and only the private key is sent via the photons in optical cables. The key is used only once. Every time a new key is generated for communication. The popular algorithm used is the One-time pad, and the Advanced Encryption Standard Algorithm. This process of encryption has two main protocols namely the BB84(Charles H Bennet and Gilles Brassard) and the E91(Artur Ekert) protocol.BB84 protocol involves Alice at the sending end and Bob at the receiving end. E91 protocol involves using entangled pair of photons from a source separate from both Alice and Bob.

III. QUANTUM KEY GENERATION

The process of quantum key distribution enables to establish a shared key between two parties without a third party learning anything about that key. Fig. 1, following herein is an example of a secured Quantum Key Distribution.

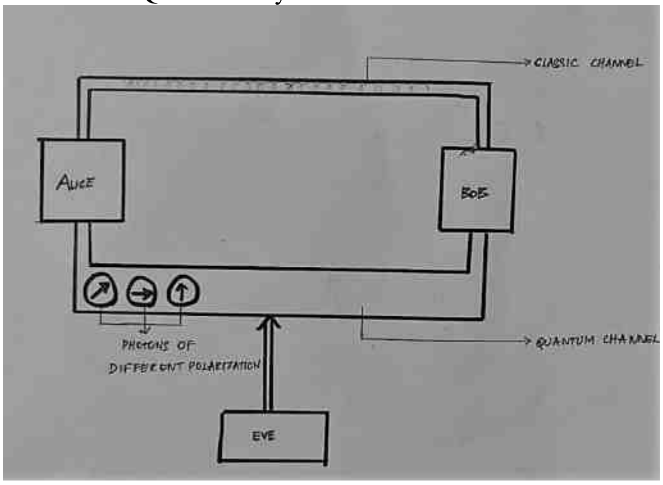

Fig. 1: Transmission of photons in QKD

This illustration includes three parties, a sender, a receiver and an eavesdropper named Alice, Bob and Eve respectively. Alice begins sending the message to Bob using stream of photons randomly chosen in one of for polarizing directions that corresponds to vertical, horizontal or diagonal in opposing directions. For each individual photon Bob will randomly choose a filter either rectilinear (0 or 90 degree) or diagonal (45 or 135 degree) and keep a log of the results to compare with his measurements with that of Alice. Next, using the classic channel Bob will inform Alice about the type of measurement made and which measurements were of the correct type without mentioning the actual results. The photons that were wrongly measured are discarded, while the correctly measured photons are translated into bits based on their polarization. It is important that neither Alice nor Bob will be able to predetermine the key because the key is the product of both their random choices.

Thus, quantum cryptography enables the distribution of a one-time key securely. Now let us suppose that a malicious attacker attempts to infiltrate the system and defeat the quantum key distribution mechanisms. If this attacker named Eve tries to eavesdrop, she too must randomly select either a rectilinear or diagonal filter to measure each of Alice's photons. Hence, Eve will have an equal chance of selecting the right and wrong filter and will not be able to confirm with Alice the type of filter used. Even if Eve successfully eavesdrops while Bob confirms with Alice the protons he received, this information will be of no use to Eve until she knows the correct polarization of each particular photon.

As a result, Eve will not correctly interpret the photons that form the final key, and thus will get failed in her endeavors. Thus, quantum key distribution enables us to share the key in a secured way.

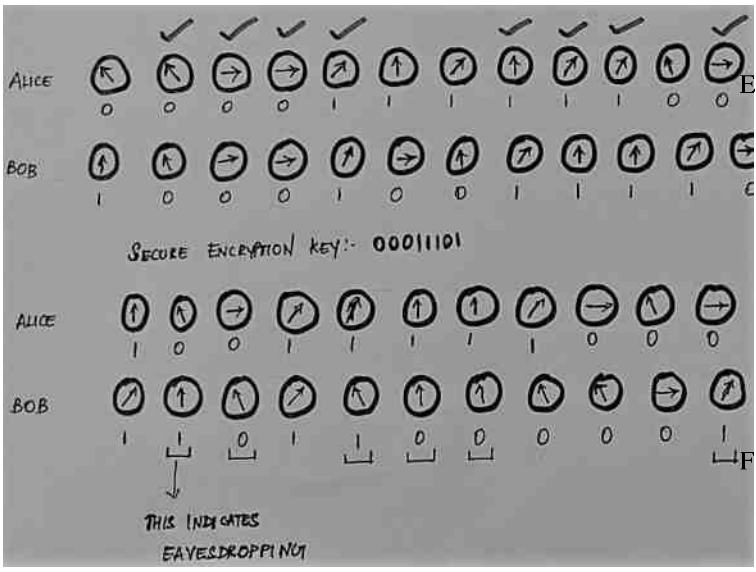
ALICE
BOB
SECURE ENCRYPTION KEY:- 00011101
ALICE
BOB
THIS INDICATES EAVESDROPPING

Fig. 2: Detection of Eavesdropping

IV. QUANTUM KEY DISTRIBUTION IN PRACTICE

Generally, the main security goals for the IoT are confidentiality, integrity and authentication. There are currently four companies offering quantum key distribution systems commercially, these include ID Quantique (Geneva), Magiq Technologies Inc (NewYork), sequrenet (Paris) and Quintessencel labs (Australia). Practical implications of QKD also include several forms of networks. These include:

A. SECOQC - The SECOQC (Secure Communication based on Quantum Cryptography) network is the world's first computer network protected by quantum key distribution. This was implemented in October 2008, at a scientific conference held in Vienna. This network used 200km of standard fiber optic cable to interconnect six locations across Vienna and the town of St Poelten located in the west of Vienna.

B. DARPA - The DARPA (Defense Advanced Project Research Agency) quantum network was developed by Harvard university, Boston university BBN technologies and Qnietiq. This is a 10- node quantum key distribution network, which has been running since 2004 in Massachusetts, USA.

C. Swiss quantum - The main goal of the swiss quantum network project installed in the Geneva metropolitan was to validate the reliability and robustness of QKD in continuous operation over a long time period in a field environment. This has successfully completed the longest running project for testing QKD in field environment. This quantum layer operated for nearly two years before it was shut down in January 2011.

D. Chinese networks - In May 2009, a hierarchical quantum was demonstrated in Wuhu China. This network had a backbone network of four nodes connecting a number of number of subnets. These backbone nodes were connected through an optical switching quantum router. Nodes within watch subnet were also connected through an optical switch, which were connected to the backbone network through a trusted relay.

E. Tokyo QKD network - The Tokyo QKD network was inaugurated on the first day of the UQCC2010 conference. The network involves an international collaboration between 7 partners; Id Quantique (Switzerland), all Vienna (Austria), NEC, Mitsubishi Electric, NTT, NICT from Japan and Toshiba research Europe Ltd. Among them all Vienna is represented by researchers from the Austrian Institute of Technology for Quantum Optics and Quantum Information (IQOQI) and the University of Vienna.

F. Hub and spoke network - This network is being operated by the Los Almos National laboratory since 2011. Here all the messages are routed through the hub. Only the hub receives he quantum messages. To communicate, each node sends a one- time pad to the hub, which it then uses to communicate securely over a classical link. The hub can route this message to another node using another onetime pad from the second node. The entire network is secure only if the central hub is secure. Individual nodes are around the size of a box of matches.

CONCLUSION

Quantum key distribution is the future security to data online. Covering a larger distance is the area that has to be worked on. Since optical fibers are used to transmit and receive private key, laying the pathway without any damage should be given special care. Currently, QKD networks are available for a distance over 60 miles or 200 kilometers. This range has to be improvised to facilitate easy communication. Our work is basically explaining the concepts of QKD and in emphasizing its security level as the best with the available proofs.

Further, we are planning to develop working models using simulation software and verify its prominently secure connection to gain more exposure to the applications of Quantum Key Distribution in the field of Internet of Things to ensure more data privacy and security. This would help the general public by providing even more safer platform to communicate.

REFERENCES

[1] Abudhahir Buhari, Zuriati Ahmad Zukarnain, “An Efficient modelling and simulation of QKD protocol”, IEEE, Malaysia, 2012

[2] Akash Shrivastava, Manvendra Singh, “A Security enhancement approach in Quantum cryptography”, IEEE, Lucknow, 2012

[3] Archana B, Krithika S, “Passive optical networks – Implementation of noise immune QKD”, IJRITCC, Coimbatore, April 2015

[4] Sanwar Ali, Waleed Farag, “How is Quantum Cryptography used for secure financial transactions?” SDIWC, Indiana, 2013

[5] Vijayalakshmi, Ramya, Palaniammal, “Applications of Quantum Cryptography”, IJCR, Chennai, 2012

ACKNOWLEDGMENTS

The authors whole heartedly acknowledge and thank all the authors and publishers whose content has been referred and cited in this research paper.