Securing IOT Network through Quantum Key Distribution

S.Krithika, T.Kesavmurthy

Abstract— Current cryptographic techniques broadly specified as conventional cryptography is solely based on the solidity of the mathematical concepts. The advancements in quantum computing can use reversible logic to compute the keys and easily break the existing security in conventional computers. From the analysis of the network structure of Internet of Things (IOT) it is very clear that the entire backbone of the system would collapse if it is attacked or hacked. IOT is a wireless technology that connects "ANYTHING" around to the Internet. IOT is a revolution which should be protected from the attackers as it would lead to several losses which could even be fatal. Hence a strong provision for securing users data in IOT is a real challenge. This paper is attempted to review the fundamentals of Quantum Key Distribution, security aspects for IOT and to address how QKD can be used to secure a IOT system. The challenge encountered is to increase the range and increase the transmission rate of data in QKD systems and to check for a possible solution to adhere these systems with existing information security solutions.

Index Terms— Eaves dropping , Internet of Things , Protocols, Quantum Cryptography, Quantum Key Distribution.

I. INTRODUCTION

The interconnection of many devices communicating through the internet where there is data transfer between humans, machines and machines themselves is known as "Internet of Things". IOT aims in improving the quality of day to day life but faces a serious threat to the sensitive and critical data communicated through the Internet [1]. Eaves dropping is a very serious problem that could not be detected using conventional cryptographic techniques.

Applying the principles of Quantum Mechanics to cryptography has paved a route to an exceptional secret communication. Quantum cryptography is blooming area in the history of secure communication. The users produce a shared secret random bit string, which can be used as a key in cryptographic applications. The high security of QKD is based on the fundamental laws of quantum mechanics, Unlike conventional cryptography which depends on unproven computational assumptions [2].Security of QKD relies on the laws of quantum mechanics and not on computational power. This is outraging because it is not possible to measure a photon without affecting its behavior. Quantum cryptography though sounds like something out of futuristic science fiction, there are multiple startups working hard to transform the hypothetical into a scalable, factory-ready product.

Quantum key distribution is based on the principle that anything which is constantly observed will change, which means it is not feasible to intercept traffic between two nodes. Hence, QKD is unbreakable under laws of Quantum Mechanics. By using the elementary particles namely the photons, QKD generates unbreakable secure keys which can be used to protect data[6-8].There are many solutions proposed in the literature based on cryptography to secure IoT networks, but the advancements in Quantum Computing (QC) pave a threat to these existing solutions. So there is an urgent need for Quantum-resistant solutions to secure IoT systems.

II. RELATED WORK

Initially it started with One Time Pad proposed by Vernam which involved a very long key equal to the size of the plain text, which was very difficult from the implementation perspective. This was followed by stream ciphers and many other cryptographic algorithms like RSA till date. All these algorithms are based on the assumption that they are mathematically secure or even can be said computationally secure i.e. if the key length is chosen sufficiently large, then even supercomputers would take hundreds or thousands of years to crack a message

In early 1970s Stephen Weisner recommended the concept of Quantum Cryptography and in 1984 two scientists Bennett and Brassard [3], delivered the first quantum cryptography protocol called the "BB84", which was provably secure. In 1991 Ekart came out with a cryptographic algorithm "E91", which involved the EPR pairs (Einstein–Podolsky–Rosen). In 1992 Bennett introduced a protocol "BB92"which proved that two non-orthogonal states are sufficient for Quantum Cryptography[5]. In 1999 Six State Protocol "SSP" used three orthogonal bases for communication using the same BB84 algorithm. "SARG04" protocol in the year 2004 illustrated the increase in QBER (Quantum Bit Error Rate is defined as the ratio of error rate to key rate, which indicates the presence of a eaves dropper and the amount of information gained.) of BB84 when using attenuated LASER pulse rather than single photon source.[11] Also improvement in security in presence of Photon Number Splitting attack was seen.[10] In the same year Coherent One Way Protocol (COW) demonstrated higher bit rates for weak coherent pulses resulting in high efficiency of distilled secret bits per qubit.[12]

"KMB09" protocol uses two bases for encoding 1 and 0 instead of using two directions from one single base which provided low eaves dropping with ad higher system error rate without compromising privacy of users. [13] Shor's

Revised Manuscript Received on April 12, 2019.

S.Krithika, Assistant Professor, Kumaraguru College of Technology, Coimbatore, T.N, India. (E-mail: Krithika.s.ece@kct.ac.in)

Dr.T.Kesavmurthy, Professor, PSG College of Technology, Coimbatore, T.N, India.. (E-mail: tkm@ece.psgtech.ac.in)

algorithm which performs factorization of prime numbers has a potential to break the RSA algorithm, created an interest among scientists because of its impact on computational complexity, proving strongly that the quantum computers may be more powerful than their classical peers. [15]

III. SECURITY CHALLENGES IN IOT

The growth of Industrial IOT is increasing every second as are the vulnerabilities too. As per survey (Techsynt solutions Nov 2017), massive cyberattacks on IOT devices and protocols happened without compromising users personal data or credentials but could happen again with a bigger damage. [14] Hence there arises a need for detailed security analysis with the top priority and building up of algorithms to safeguard the network. The challenges the security experts to take into concern are i) Protecting user data with privacy and compliance rules ii) Updating all IOT devices as often as possible iii) ensuring the following of embedded technology security protocols by integrating all IOT services iv) Increase of level of perception form the customer side towards usage of IOT devices v) Device management.

Among all these challenges the main point to be concentrated upon is maintaining the integrity and secrecy of the data communicated over IoT. High security can be achieved by combining every piece of an IOT chain for protection purposes—state-of-art encryption, passwords, the latest versions of software and hardware on the device. But with evolution of Quantum computers all these classical algorithms like DES, AES, ECC will not be able to support. All these algorithms involves exchange of keys between the end users, which becomes the main loophole for security. There arises the concept of Quantum Key Distribution which relies on Quantum Mechanics and provides unconditional security between communicating entities that cannot be compromised by eaves dropping technique [4].

IV. QUANTUM CRYPTOGRAPHY PRELIMINARIES

Quantum Cryptography is a point-to-point light wave transmission using photons through a fiber optic cable link or open air. By means of Quantum Key Distribution random keys are transmitted using any of quantum cryptography mechanism and then after conventional cryptography is used for secure communication. The quantum system processes the information by making use of quantum bits or qubits which can represent 0 and 1 simultaneously in a state known as superposition. The ability of a photon to be polarized makes it act as a secret key. The information attached to the photon spin can be used to create binary data. Photons can be polarized to one of four angular states: 0º, 45º, 90º, and 135º. The zero and 90º polarizations are called the rectilinear basis, the 45º and 135º polarizations are referred to as the diagonal basis.

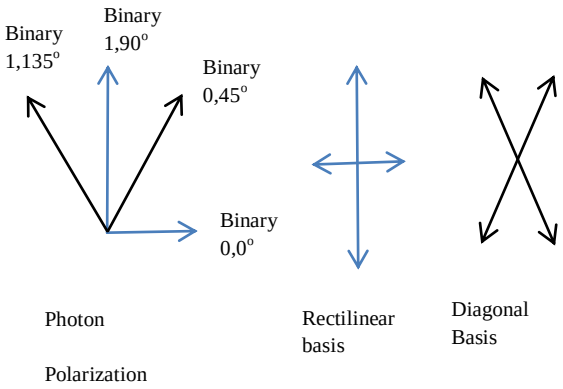

Fig1. Photon Polarization and Basis

There are two concepts of Quantum Mechanics that provides this unconditional security.

(i) Superposition principle: A system can exist in all possible states at the same time. Qubits can be in two states simultaneously rather than being restricted to a single state, thereby storing much more information at a less energy than classical bits. The size of the superposition grows exponentially with the number of particles.

(ii) "No-Cloning Theorem": It is impossible to copy an unknown quantum state. Quantum mechanics places hard limits on precise measurements. The No-Cloning Theorem also paves the way for secure communications.

For example consider two persons, Alice and Bob, sending quantum states of light (photons) between them, then an eavesdropper, Eve, cannot measure these photons without disturbing them. Finally they end up with a cryptographic key of shared random bits resulting in perfect encryption.

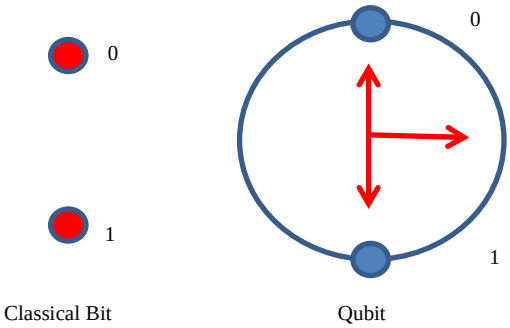

Fig2 . Principle of Superposition

Other Concepts of Quantum Mechanics like Uncertainty Principle, Entanglement also offers a solution to security issues. Heisenberg's uncertainty principle states that two properties of an object cannot be measured at the same time, since measuring one makes other quantity measurement inaccurate. The concept of Entanglement implies that two entangled photons separated from each other still get their properties linked and changes to one are instantaneously

transferred to the other despite no visible contact between them. It uses particles, such as photons, to enable two remote parties to produce a shared random secret key known only to them, which can then be used to encrypt and decrypt confidential messages in a classical way. [18-19]

Any attempt to intercept the key during creation and distribution will disturb the correlation, alerting users not to use the key thus preempting eavesdropping. The superposition state of a quantum system gets destroyed when exposed to external environment making the state unpredictable, and detects eaves dropper during key distribution process. The biggest challenge at present is to extend the range and increase the data rate of QKD systems. Also to integrate these systems with existing information security solutions for securing all connected devices.[17]

V. QUANTUM KEY DISTRIBUTION – EXAMPLE: BB84

Alice, the sender selects a random binary number which are then subjected to a polarizer whose basis are also randomly selected. The polarized photons which are the secret keys are sent over a quantum channel to the receiver Bob. Bob reconverts the photons into binary numbers. If a diagonally polarized photo is passed through a rectilinear polarizer it choses either Horizontal or Vertical polarization with a 50% of probability each and vice-versa. Therefore some of the bits are changed , missed or are changed due to other disturbances during transmission.

Alice and Bob communicate over a public channel about the bases used in order to retrieve the correct keys and also to find out the presence of eaves dropper. Based on the discussion some bits are discarded and the remaining bits constitute the shared key. QKD ensures distribution of one time key exchange securely. [21]

TABLE 1 QKD – Key Sharing and Extraction

ALICE - SENDER									
Random Bits	1	0	0	1	1	0	1	1	0
Bases	D	R	R	R	R	R	D	R	D
Photons	↘	↔	↔	↕	↕	↔	↘	↕	↙
BOB - RECEIVER									
Bases	D	R	D	D	R	R	D	D	R
Bits	1	0	-	-	1	0	1	-	-
Shared Key - 10101									

Assume on transit in quantum channel suppose a malicious attacker named Eve tries to infiltrate into the photons. Eve randomly selects any of the bases to measure Alice's photons. There is an equal chance of selecting the right and the wrong bases. According to Heisenberg's Uncertainty principle once a photon is measured or disturbed , the information carried by it gets destroyed, therefore photons measured by Eve don not reach Bob. Therefore by analyzing the traffic of the transmitted photons Bob can understand that the network is being sniffed. Even if Eve tried to measure and create a photon and send to Bob, 50% of the time it will be incorrect on an average. Hence the error rate will also reveal the presence of Eve to Bob. Therefore QKD ensures its unconditional security in key distribution between end users. [16]

VI. QKD FOR IOT & RESULTS

IoT will have a wide spread deployment in all the sectors which involves general as well as some critical applications like smart transport systems, , biometric data transfer, e-government, e-commerce , e-health smart grids, smart cities and many others services. The Integrity of stired data, long term privacy and higher levels of confidentiality plays vital role in these systems. Quantum Key Distribution under the backbone of Quantum Mechanics has proven to maintain an end to end security in the long term.

IoT infrastructure will involve connection of heterogeneous networks with an integration of various technology and multivendor interoperability.[20] Henceforth there arises a need for integration of classical as well as quantum networks which form a platform for implementation of QKD.

There are some limitations in QKD implementation of a dedicated hardware which involves a huge cost, transmission distance which is limited to few hundreds of Kilometers, comparatively lower data (Key) transmission rate. There are some key areas to be concentrated on QKD specifically for IoT infrastructure implementation like:

i) Integration of QKD with classical cryptography
ii) A wide area network with more intermediate trusted nodes to be created due to the current distance limitations in QKD.
iii) Carrying out key distribution along with data transmission over optical channel to improve the data rate.
iv) Broadcasting in a QKD network as currently it supports only point – point communication.
v) Overall cost reduction.

But comparing to the huge amount of data involved in IoT with the necessity of meeting a strong security conditions QKD seems to be a viable solution for IoT.

VII. CONCLUSION

IoT is going to be a major utility with a vision to facilitate sensing, actuation, communications, control of vast amounts of data from varied applications and sources. Quantum communication forms the core idea for a universal secured IOT.[9] This idea of a highly secure network opens doors to many future possibilities. QKD is a viable solution to counter the threats that may appear in future from quantum computers thereby securing all IOT related applications. Also QKD is an essential element for building a quantum safe infrastructure including quantum-resistant classical algorithms and quantum cryptographic solutions.

REFERENCES

1. Ashvini Kamble, Sonali Bhutad, " Survey on IOT Security Issues and Solutions" IEEE Xplore compliant , ICISC2018,ISBN : 97-1-5386-0807-4.

2. Z. L. Yuan, A.W. Sharpe, A. J. Shields, "Unconditionally secure quantum key distribution using decoy pulses," Appl. Phys. Lett. 90, 011118, 2007.
3. C.H. Bennett, G. Brassard, Quantum cryptography: public key distribution and coin tossing, in: Proc. of International Conference on Computers, Sys-tems, and Signal Processing, Bangalore, India, 1984, pp.175–179.
4. Aysajan Abidin , Jan-˚ake Larsson "Vulnerability Of "A Novel Protocol-Authentication Algorithm Ruling Out A Man-In-The-Middle Attack In Quantum Cryptography" Int.Journal of Quantum Information , 2009, pp 1401-1407.
5. Bennett, Ch., and Brassard, G.: Quantum Cryptography Using Any Two Non-Orthogonal States. Physical Review Letters, Vol. 68, Issue 21, pp. 3121—3124 (1992).
6. D. Mayers, Unconditionalsecurity in quantum cryptography, J. ACM 48 (2001) 351; eprint arXiv:quant-ph/9802025.
7. E. Biham, M. Boyer, P.O. Boykin, T. Mor, V. Roychowdhury, A proof of the security of quantum key distribution, in: Proceedings of the Thirty Second Annual ACM Symposium on Theory of Computation, 2000, pp.715–724; arXiv:quant-ph/9912053.
8. P.W. Shor, J. Preskill, Simple proof of security of the BB84 quantum key distribution protocol, Phys. Rev. Lett. 85 (2000) 441–444; eprint arXiv:quant-ph/0003004.
9. John A. Stankovic "Research Directions for Internet of Things", IEEE Internet Of Things Journal, Vol. 1, No. 1, February 2014
10. V. Scarani, A. Acin, G. Ribordy, N. Gisin, "Quantum cryptography protocols robust against photon number splitting attacks for weaklaser pulse implementations", *Physical review letters*, vol. 92, pp. 057901, 2004. [Online]. Available: http://dx.doi.org/10.1103/PhysRevLett.92.057901
11. Chi-Hang Fred Fung, Kiyoshi Tamaki, and Hoi-Kwong Lo, "On the performance of two protocols: SARG04 and BB84", arXiv:quant-ph/0510025v2 12 Oct 2005.
12. Mhlambululi Mafu, Adriana Marais, Francesco Petruccione "Towards the unconditional security proof for the Coherent-One-Way protocol"
13. Syed.S.Hussain, Muhammed M.Khan, Mirza M.Baij, G.Wang, " Numerical Modelling of Quanutum Key Distribution Ssytem for KMB09 Protocols", International Journal of Computer science and Information Security, Vol.14, No Aug 2016.
14. Ashvini Kamble, Sonali Bhutad, "Survey On Internet Of Things (Iot) Security Issues & Solutions ",Proceedings of the Second International Conference on Inventive Systems and Control (ICISC 2018) IEEE Xplore Compliant - Part Number:CFP18J06-ART, ISBN:978-1-5386-0807-4
15. Eleanor Rieffel , Wolfgang Polak, "An Introduction to Quantum Computing for Non-Physicists", arXiv:quant-ph/9809016v2 19 Jan 2000.
16. Anindita'Banerjee, Anil'Prabhakar, Mark'R'Mathias, " Quantum Key Distribution – A Technology Review" , Journal on Defence Information and Communication Technology Vol 3 No 1 2017
17. Valerio Scarani, Helle Bechmann, Nicolas J. Cerf, Miloslav Dušek, Norbert Lütkenhaus, " The Security of Practical Quantum Key Distribution", Reviews Of Modern Physics, Volume 81, July–September 2009.
18. Mhlambululi Mafu and Makhamisa Senekane , " Security of Quantum Key Distribution Protocols", http://dx.doi.org/10.5772/intechopen.74234
19. Akshata Shenoy, Anirban Pathak, Srikanth Radhakrishna, " Quantum Cryptography: Key Distribution and Beyond", arXiV:102:05517v1 [quant-ph] 15 Feb 2018.
20. Sayanta Gupta, Chayan Dutta, " Internet of Things Security Analysis of Networks Using Quantum Key Distribution" , Indian Journal of Science and Technology, Vol 9 (48), Dec 2016.
21. Krithika.S, "Quantum Key Distribution (QKD): A Review on Technology, Recent Developments and Future Prospects", Research J. Engineering and Tech. 8(3): July-September 2017.