ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

A Survey on Quantum Key Distribution

Kranti V. Nikam[1], Mitali V. Shewale[2], M. R. Dhotre[3]

M.Tech. Student, Dept. of Electronics and Telecommunication, Govt. College of Engineering, Jalgaon, India[1]

M.Tech. Student, Dept. of Electronics and Telecommunication, Govt. College of Engineering, Jalgaon, India[2]

Asst. Professor, Dept. of Electronics and Telecommunication, Govt. College of Engineering, Jalgaon, India[3]

ABSTRACT: Wireless network is one of most important modes of communication. So providing security to the information being communicated through wireless networks is very important issue. Classical cryptography provides conditional security which has many loop holes whereas quantum cryptography promises to be unconditionally secure for wireless networks, recently implementation of quantum cryptography in wireless communication systems using a quantum key distribution (QKD) protocol is done. Cryptography is the technique for secure communication of data in the presence of third parties, called adversary. Quantum cryptography relies on two important elements of quantum mechanics-The Heisenberg uncertainty principle and the principle of photon polarization.The main weakness of classical cryptography is that it does not provide any method to sender and receiver to find out the presence of adversary. Quantum cryptography deals with almost all loopholes found in classical cryptosystem. It provides unconditional security by encrypting the message using standard one time pad encryption scheme. The use of quantum cryptography in optical fibre cables has significant advantages.

KEYWORDS: Quantum cryptography, Quantum key distribution (QKD), Network security.

I. INTRODUCTION

Adversary which is also called as Cryptography is the technique for secure communication of data in the presence of third parties. Classical cryptography is based on the complexity of some mathematical function which is a one way function. The safekeeping is as strong as challenging to degenerate it. It provides uncertain security. The main flaw of classical cryptography is that it does not provide any method to sender and receiver to find out the presence of adversary. Since the most frequently used classical cryptographic method is RSA which is based on difficulty of factorization of a number obtained by product of two large primes. When quantum computer becomes functional all types of classical cryptosystem become breakable keeping forth all these shortcomings in classical cryptosystem in mind, people started to contemplate beyond it for securing future electronic communication. Quantum cryptography deals with almost all ambiguities/loopholes found in classical cryptosystem.

As we all know that light is routinely used to exchange information in telecommunication networks. A pulse is emitted for each bit of information and sent down an optical fibre a thin fibre of glass used to carry light signals to the receiver, where it is registered and transformed back. One can follow the same approach in cryptography, with the only difference that the pulses contain only a single photon. It represents a very tiny amount of light when reading this article your eyes register billions of photons.

The key distribution problem is solved by quantum cryptography by allowing the exchange of a cryptographic key between two remote parties with absolute security, guaranteed by the laws of physics. Along with conventional cryptographic algorithms this key can be used.

II. RELATED WORK

Charles H. Bennett & Gilles Brassard discovered firstly that how photon transmission occurs in quantum channel for making secure communication and they proposed the new protocol as Coin tossing as BB84 by exchange of quantum message which is secure against traditional kind of cheating. [1]

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

Quantum cryptography that has emerged in recent times provides absolute security is described as a point-to-point secure key generation technology. Researchers have started studying new innovative approaches to exploit the security of QKD for a large-scale communication system. A number of approaches and models for secure communication have been developed for utilization of QKD.

A new paradigm for QKD is created by the uncertainty principle in quantum mechanics. For use of QKD one of the approaches involved network fashioned security. Example of such a network is BBN DARPA quantum network. Researchers at Boston, Harvard University, and BBN technologies jointly developed the DARPA Quantum Network in 2004. The main target was point-to-point quantum network that demoralized QKD technology for end-to-end network security via high speed QKD.

Other approaches and models equipped with QKD in network fashion are introduced in the literature as in [5]. A different approach that this paper deals with is using QKD in existing protocols, which are widely used on the Internet to enhance security with main objective of unconditional security. Papers present models and schemes to integrate QKD in classical security protocols like IPsec, PPP and TLS.

III. METHODOLOGY

Quantum cryptography is an evolving technology that provides safety and security for network communication by performing cryptographic tasks using quantum mechanical effects. Quantum Key Distribution (QKD) is a technique that is an application of quantum cryptography that has gained popularity recently since it overcomes the flaws of conventional cryptography. QKD makes the secure distribution of the key among different parties possible by using properties of physics.

The quantum states of photons are used and the security key information is transmitted via polarized photons that contain the message denoted by bits (0 or 1) and each photon contains one bit of quantum information called as Qubit. The sender sends the polarized photon to the receiver. At the receiver end, the user determines the photon polarization by passing it through a filter and checks for any modifications in the received bits of photons when compared to the bits measured by the receiver. Any modifications found would show that there has been an intrusion from a third party because the intrusion would irreversibly change the encoded data in the photon of either the sender or the receiver. This method is based on the Heisenberg's uncertainty principle that states that the quantum state can't be measured without disturbing the state of either the sender or the receiver and hence introducing an anomaly in the quantum system that can be noticed by users as an intrusion.

Thus, quantum cryptography applies the principles of physics governed by the laws of quantum mechanics for distributing the secret cryptographic key among the parties involved in the cryptosystem in a manner that makes it next to impossible for a third party to eavesdrop.

1 .QUANTUM KEY DISTRIBUTION BB84 QKD PROTOCOL

BB84 protocol was proposed Bennett and Brassard in 1984. The protocol consists of two main channels used for transmission:

1. Quantum channel: One-way communication.
2. Classical channel: Two-way communication

With the help of BB84 two parties such as a Sender and a Receiver conventionally establishes communication by a common key sequence using polarized photons.

Key exchange and key sifting are done as follows.

• The information is encoded in random bits of 0 & 1 by the sender and uses randomly selected bases such as rectilinear or diagonal, to transmit bits in it as shown in Fig. 3.1 the bases for each photon is chosen randomly and is repeated by the sender again so that the photos should be send to the receiver in the same order.

• The receiver at the other end selects the bases such as rectilinear or diagonal at random to measure the received photons that may not be aware of the bases used to encode the photons by the sender.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

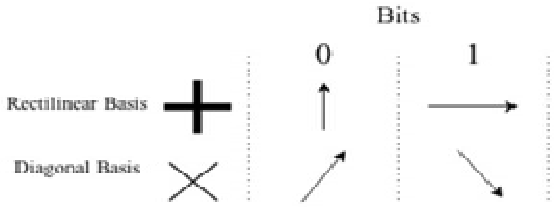

Fig.1 Photon Polarization Using Bases

As all the photons get received by the receiver, the receiver starts communicating with the sender using the public channel for key sifting.

Using Classical channel (Key Sifting):

• The sender is informed by the receiver what bases he used to measure the photons and sender further responds by saying whether it matched the bases used.

• When correct matching of the bases is there both agree on it without announcing the actual value of information. All the data on the polarizer bases that did not match is discarded, and both are left out with two key strings of shorter sequences, known as the raw keys.In this way the protocol works.

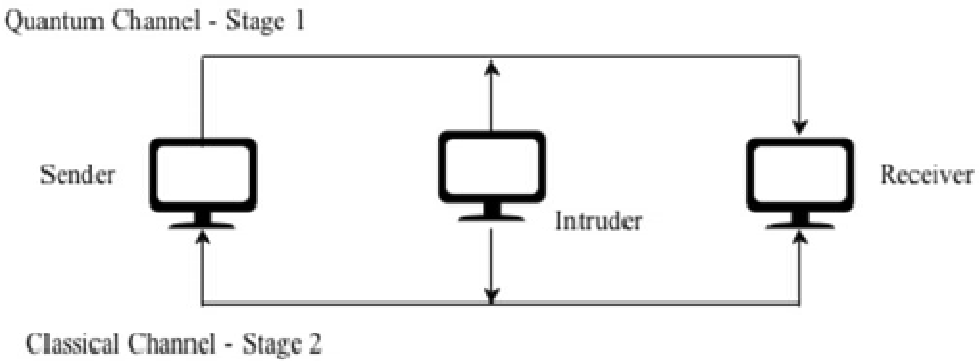

Fig.2 QKD channel

A secrete raw key is made up when the bits are matched which is not complete key and the communication still continues between the two comprising of the following steps:

1. Error estimation: The raw keys are compared in order to check if any eavesdropping has occurred, if interruption takes place, error would be introduced in one of the raw key and the two keys on comparison won't match. Hence, the errors are to be estimated and the key is aborted and they try sending data again. If the error rate exceeds the threshold QBER (Quantum Bit Error Rate) for quantum transmission.

2. Error correction (Resolution): In order to remove the errors in the raw key and to get the common key by using a protocol from the many available protocols such error resolution is performed. Cascade (based on optimal linear codes, uses and releases less data, end by performing parity based error correction), Winnow (based on exchange of parity and helps correcting single errors using hamming hash function) are the most widely used protocol.

3. Privacy Amplification: Both sender and receiver will hold in the end, not completely private but identical strings of bits the information of which can be partially obtained one eavesdropping by a third party .The partially

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

obtained information by the third party is removed with the help of privacy amplification and hence make a correct secured secret key.

IV. CONCLUSION AND FUTURE WORK

The main goal of this technique is to show a method to improve the security aspect of WLANs. It has been shown that the integration of Quantum Cryptography in Wireless Networks has great prospective in terms of better network security.Key management and distribution is difficult using classical cryptographic algorithms but the proposed approach provides a better solution for this problem. Research has shown that use of QKD to distribute network key raises the security and makes it harder for an eavesdropper to interrupt communication. With the proposed modification, this paper has achieved the main objective of improving security of WLANs.
Future applications are in the most secure communication lines for bank-to-ATM transactions, financial information protection over the internet, and military and government communications including the use for ship-to-ship, ground-to-satellite, and satellite-to-satellite communication.

REFERENCES

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and poi tossing," in Proc. IEEE Int. Conf. Computers, Systems and Signal Processing, New York, Bangalore, India, 1984, pp. 175–179.
[2] Changhua He John Mitchell "IEEE 802.11i Wireless Networking Standard" IEEE Int conf.pp.176.
[3] Eleni Diamanti,1 Hoi-Kwong Lo2, Bing Qi,3, 4 and Zhiliang Yuan5,"Practical challenges in quantum key distribution'' Quantum Information Science Group, Computational Sciences and Engineering Division, IEEE 6 June 21, 2016 .
[4] Floriano De Rango, Dionogi Lentini, Salvatore Marano, Static and Dynamic 4-Way Handshake Solutions to Avoid Denial of Service Attack in Wi-Fi Protected Access and IEEE 802.11i,EURASIP Journal on Wireless Communications and Networking archive, Volume 2006 Issue 2,April 2006.
[5] H. K. Kalita and A. Kar, "Wireless sensor network security analysis," International Journal of Next-Generation Networks (IJNGN), vol. 4, no. 6, June 2009.
[6] U. K. D. R.Lalu Naik, Dr.P.Chenna Reddy, "Provely Secure Quantum Key Distribution
Protocol in 802.11 Wireless Networks," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, no. 7, July 2013.
[7] W. Stalling, "Cryptography and Network Security (principles and practices)" International Journal of Computational Engineering Research (ijceronline.com), vol. 3, no.1, January 2012.
[8] Thi Mai Trang Nguyen, Mohamed Ali Sfaxi and Solange Ghernaouti-Hélie "802.11i Encryption Key Distribution Using Quantum Cryptography'', journal of networks, vol.1, no. 5, September/October 2006.
[9] J. Watson, "Data Security Hits Home," IJAITI, vol. 1, no. 2, Mar/Apr 2012.