Quantum Key Distribution using Different Techniques and Algorithms

Sneha Charjan
Department of Computer Engineering
SKNCOE
Pune, India

D. H. Kulkarni
Department of Computer Engineering
SKNCOE
Pune, India

Abstract— **Key Distribution is the main issue in both classical cryptography and Quantum cryptography. In classical cryptography, the security is depend on the computational complexity whereas in quantum cryptography, it is depend on the laws of quantum mechanics that are no-cloning theorem and Heisenberg uncertainty principle. To overcome this issue in quantum cryptography different techniques and algorithms have been proposed. This research paper concentrates on those techniques and algorithms with their comparison and contribution in network security.**

Keywords—Quantum Cryptography, Quantum Key Distribution (QKD), Network Security, Photon Polarization, Three party communications.

I. INTRODUCTION

Key distribution is the function that delivers a key to two parties who wish to communicate. Key distribution is the strength of any cryptographic system as the security of any communication is totally depends on the secret key. Therefore, it is important to have secure key distribution system because if the key get compromised then whole system will get compromised.

Classical cryptography is based on a combination of guess work and mathematics. Security depends on the difficulty of computational complexity which is not enough as the fast growing methods to calculate the secret key will compromise the security. There are two approaches in classical cryptography for key distribution: Symmetric cryptography and asymmetric cryptography.

In symmetric cryptography there is same secret key shared between two parties who want to communicate whereas in asymmetric cryptography communicating parties must have pair of key called public and private key; the private key is kept secret with each party and public key is used for encryption of data is known to everyone who wants to communicate.

Whereas quantum key distribution provides the most secure way to distribute or exchange secrete keys as quantum cryptography uses the laws of quantum mechanics for communication which offers an unconditionally secure solution. Moreover quantum mechanics also provides the ability to detect the presence of eavesdropper who is attempting to learn the key as the quantum state on the transmitted data will collapse to single state and therefore, get disturbed.

II. LITERATURE REVIEW

In quantum key distribution system, two parties who want to communicate are allowed to create secret key based on random function. Many protocols have been introduced to solve a problem of communication using quantum cryptography. The first protocol was introduced by Charles H. Bennett and Gilles Brassard in 1984 named as BB84 [2]. It was based on Heisenberg's Uncertainty principle. All other Heisenberg's Uncertainty principle (HUP) based protocols are essentially variants of the BB84 idea. The basic idea for all these protocols then is that Alice can transmit a random secret key to bob by sending a string of photons where the secret key's bits are encoded in the polarization of the photons. Heisenberg's Uncertainty principle can be used to guarantee that an eavesdropper cannot measure these photons and transmit them on to Bob without disturbing the photon's state in a detectable way thus revealing eavesdropper's presence. Also the non-cloning theorem assures that eavesdropper cannot replicate a particle of unknown state. BB84 uses two phases, in first phase Alice will communicate to Bob over a quantum channel. Alice begins with choosing random strings. Bob will notify over any insecure channel that what bases he used to measure each photon. BB84 uses four polarization states [13]. In 1992 Charles Bennett proposed a simplified version of BB84, in which only two polarization states are necessary, named as B92.

While there are a number of other BB84 variants one of more recent was propose by Scarani, Acin, Ribordy, and Gisin named as SARG04. The protocol shares the exact same phase as BB84. In the second phase when Alice and Bob determine for which bits their bases matched, Alice does not directly announce her bases. Rather she announces a pair of non-orthogonal states, one of which is used to encode her bit. If Bob used the correct basis, he will measure the correct state. If he chose incorrectly, he will not measure either of Alice's states and he will not be able to determine the bit. This protocol has a specific advantage when used in practical equipment [13].

Four state quantum key distributions (QKD) protocol BB84 and two state QKD protocol B92 can let Alice and Bob share the secret key with idealized maximum efficiencies 50 % and 25 % over quantum channel, respectively. In [3], two enhanced QKD protocols are proposed. One is to enhance the idealized maximum efficiency to 28.6 % with the average complexity order 2, and the other has the efficiency 42.9 % and the average complexity order 2.86.

To compensate the loss in the signal the assumption are made while designing BB84 like weak signal source, near perfect transmission line, sensitive and fast quantum detectors, amplifiers, repeaters that are needed. These assumptions might not be practical in many situations. It uses highly attenuated lasers as source of quantum signals which can produce signals that contain more than one photon leads to new attack known as Photon Splitting Attack [4].

In [10], Decoy state quantum key distribution (QKD) has been proposed as a novel approach to enhance both the security and the performance of practical QKD setup. In this author report the first experiments on decoy state QKD, thus bridging the gap. Two protocols of decoy state QKD are implemented: one decoy protocol over 15 km of standard telecom fiber, and weak + vacuum protocol over 60 km of standard telecom fiber. The standard security proof give a zero key generation rate at the distance the decoy state QKD is performed. Therefore decoy state QKD is necessary for long distance secure communication which explicitly shows the power and feasibility of decoy method.

A QKD protocol over a two way quantum channel, this protocol does not require any classical channel instead two communicating parties are required to be connected by two way quantum channel. It reduces overhead due to key shifting and key reconciliation over classical channel and also the operational overhead and increase the speed with which keys can be exchanged [5].

Quantum cryptography can provide long term confidentiality for encrypted information without reliance on computational assumptions. Although QKD still requires authentication to prevent man-in-the-middle attacks. In [9], the vulnerability in existing models are reviewed like no authentication of participant, lack of pre process, no estimation of attackers information and the improved QKD protocol is proposed in which they have used both classical and quantum channels and included nine steps that are authentication of participant , initialization, quantum transmission, shifting, error reconciliation, estimating attacker’s information, decision on continuation, privacy amplification, getting error free key which enhance the security.

In an entanglement-based quantum key distribution [7], authors have used a modified version of Cabello’s definition of efficiency of QKD protocols to do comparison between their protocol and BB84. A sequence of qubit pairs is gained by dividing the stream of qubits. The protocol reveals less information about the key bit than BB84 because before the beginning of the protocol the participants get agreed publically on two 2-qubit unitary transformations, U_1 and U_2 and all transmitted qubits are useful unlike BB84 that half of qubits are discarded on average. In this one classical bit is used to acknowledge receiving each qubit and one classical bit is used for determining the basis of each group of qubits. It provides advantage against eavesdropper under an intercept resent attack.

Multiple-Access quantum key distribution networks addresses multi –user QKD networks, there is no need of any other node except the two communicating parties, they can mutually exchange a secret key. In this the idea of switching is used instead of full mesh network in wavelength division multiplexing (WDM) network. Certain wavelength is assigned to two nodes who want to exchange the key and wavelength router links them together. Same network is used for both classical and quantum signals by assigning them two different wavelength bands. The hybrid setup is formed by combining time/code division multiple access (TDMA/CDMA) QKD networks with WDM routing setup, in which each WDM node serves as a hub through multiple TDMA/CDMA users can be supported. In this to get the advantage of both TDMA and CDMA, a listen-before-send (LSB) protocol is proposed which supports multiple users [12].

In [6], the comparison of commercial and next generation quantum key distribution is given. Till date, most of the QKD systems have utilized a discrete variable (DV) binary approach. In this discrete information is encoded onto a quantum state of single photon and binary data are measured using single photon detectors. Recently, continuous variable (CV) QKD system has been developed, in which randomly generated continuous variables are encoded on coherent state of weak pulses of light and continuous data values are measured with homodyne detection methods. CV-QKD offers higher secret key exchange rate for short distances, lower cost, and compatibility with telecommunication technologies. In CV-QKD, unlike DV-QKD, Alice and Bob do not have the same values during key shifting process, they only have correlated data and therefore, key generation, error correction are more tedious in this approach. For short distance CV-QKD system can generate higher secret key rate than DV-QKD system as it uses detector with higher quantum efficiency but at the same time it is very challenging for CV-QKD for long distance as secret key generation rate is strongly dependent on the vacuum noise which increases with distance. On the other hand in DV-QKD system, the QBER is typically not impacted by vacuum noise. For long range distance in fiber and free space, DV-QKD appears to have a competitive edge while CV-QKD systems hold a promise for more economic fiber usage by allowing a higher number of systems to coexist on a single fiber.

In [4], authors have proposed a novel secure quantum key distribution algorithm in which their main objective is to overcome the deficiencies found in BB84 and B92 protocols by eliminating the need for two communicating parties to confirm their used basis over a public channel. Session key is the strength of any cryptography communication. So in this session key is exchanged over the most secure channel that is quantum channel. Before that using public key cryptography the users are authenticated and confidentiality is maintained by exchanging random basis and nonce. It eliminates the inefficiency caused due to requirement of many rounds just to agree on a basis for the quantum communication.

In [1], a new model for QKD is introduced between three parties where there is a trusted center providing the clients the necessary secret information to securely communicate with each other. In this there is no need of physical channel to check qubits sequence. The proposed algorithm consists of two phases: 1. User Authentication and quantum bases distribution. 2. Data Transfer over the quantum channel. When Alice wants to communicate with Bob, Alice sends requests with its ID to QKD, QKD check for authentication and asks to Bob. When both the parties get agreed on communication, QKD starts distributing quantum bases in some sequence to encode the message to Alice and Bob in encrypted message using Alice and Bob's public keys. It improves the efficiency by eliminating the rounds required to check the quantum bases and provide authentication.

A new algorithm for three party quantum key distribution [8] provides new mechanism to establish trust between different parties. The trusted third party forms an agreement on the secret key and establishes a trust between them. The specific aim is to allow the parties to agree on the basis and not the final secret key. This protocol requires three quantum channels between parties along with classical channel. QKD selects random classical bits and orthogonal bases to generate qubits. Qubits are transmitted to Alice and Bob through quantum channel. Then Alice and Bob must select random bases to measure received qubits and transfer them to classical bits. They send these classical bits to QKD. After receiving qubits from Alice and Bob, QKD measures it using original bases and transfer result to classical bits and compare bits with received bits and maintain record to indicate correct and incorrect positions of the received bits. All steps are repeated several times depending on key size then determine correct position to get final key. It is also useful to determine the presence of eve.

III. CONCLUSION

All the techniques and algorithms discussed above are having advantage over other and at the same time having some drawbacks. Quantum cryptography is the most secure system of communication but suffers from the problem of user's authentication and also inefficiency caused due to number of rounds required to measure the correct bases and final key which can be overcome using classical cryptography that is public key cryptography. Combination of both removes drawback and provides the most secure communication.

ACKNOWLEDGMENT

I thank my guide Prof. D. H. Kulkarni and staff members for their generous help and also to my colleagues and parents for their invaluable support.

REFERENCES

[1] Ammar Odeh, Khaled Elleithy, Muneer Alshowkan, Eman Abdelfattah, "Quantum Key Distribution by Using Public Key Algorithm (RSA)", London, United Kingdom: third International Conference on Innovative Computing Technology (INTECH),IEEE, August 2013.

[2] Charles H. Bennett, Gilles Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing", International Conference on Computers, Systems and Signal Processing Bangalore, India, December 10-12, 1984.

[3] Ching-Nung Yang and Chen-Chin Kuo "Enhanced Quantum Key Distribution Protocols Using BB84 and B92".

[4] Abdulrahman Aldhaheri, Khaled Elleithy, Majid Alshammari, Hussam "A Novel Secure Quantum Key Distribution Algorithm", University of Bridgeport.

[5] Farnaz Zamani, P. K. Verma, "A QKD Protocol with a Two-way Quantum Channel", in Advanced Networks and Telecommunication systems (ANTS), 5th International Conference IEEE, pp 1-6, 2011.

[6] L. Osterling, D. Hayford, G. Friend, "Comparison of Commercial and Next Generation Quantum Kay Distribution: Technologies for secure communication of information", in Homeland Security (HST), IEEE Conference on Technologies for, pp. 156-161, 2012.

[7] M. Houshmand and S. Hosseini-Khayat, "An Entanglement-base Quantum Key Distribution Protocol', in Information Security and cryptology (ISCISC), 8th International ISC Conference on. IEEE, pp. 45-48, 2011.

[8] M. Alshowkan, K. Elleithy, A. Odeh, e. Abdelfattag, "A New Algorithm for Three –Party Quantum Key Distribution", 3rd International Conference on Innovative Computing Technology (INTECH), London, United Kingdom, August 2013.

[9] R. D. Sharma, A, De, "A New Secure Model for Quantum Key Distribution Protocol", Industrial and Information system (ICIIS), 6th IEEE International Conference, pp 462-466, 2011.

[10] Y. Zhao, B. Qi, X. Ma, H. Lo. L. Qian, "Simulation and Implementation of Decoy State Quantum Key Distribution over 60km Telecom Fiber", ISIT, Seattle, USA, July 2006.

[11] M. Niemiec, A. Pach, "Management of Security in Quantum Cryptography", IEEE Communication Magazine, pp.36-41, August 2013.

[12] M. Razavi, "Multiple-Access Quantum Key Distribution Networks", IEEE Transactions on Communication, vol. 60, no. 10, October 2012.

[13] M. Haitjema, "A Survey of the Prominent Quantum Key Distribution Protocols", December 2007

[14] M. Sharbaf, "Quantum Cryptography: An Emerging Technology in Network Security", IEEE, 2011.

[15] Mahboobeh Houshmand, Monireh Houshmand, H. Mashhadi, "Game Theory base View to the Quantum Key Distribution BB84 Protocol', 3rd International Symposium on Intelligent Information Technology and Security Informatics (IITSI), IEEE, 2010.