IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 6, Dec-Jan, 2014
ISSN: 2320 - 8791
www.ijreat.org

QKD Technology For High Performance Computing And Wireless Network

JONISHA S[1], SUREKA V[2]
[1,2]Department of Computer Science and Engineering, Assistant Professors,
S.A ENGINEERING COLLEGE, CHENNAI, Tamil Nadu, INDIA
:

Abstract – Quantum Key Distribution (QKD) is a point to point secure key generation technology which provides unconditional security. To exploit the security of QKD for large scale practical communication, it must be used in a network fashion. BBN DARPA quantum network and SECOQC network of secrets are the examples of such networks. Research is also in progress for the integration of QKD with the protocols in different layers of OSI model. Integration of QKD in point-to-point protocol (PPP) OSI layer 2 and the integration of QKD with IPSEC at OSI layer-3 are the examples of such research efforts. All these steps are moving towards the utilization of QKD technology for enhancing the security of modern computing applications on the internet. This paper presents a model for the exploitation of QKD security networks in high performance distributed computing applications, such as grid computing.

Keywords – Quantum Key Distribution, Grid Computing, Point-to-point protocol, Cryptography, Public Key Encryption, Wireless Networks

1 INTRODUCTION

In the beginning of 21st century two companies of the world one from USA, MagiQ Tech, and another from Switzerland, idQuantique, presented the commercial products of QKD. The practical realization of QKD opened new arena of research in the area of secure QKD networking. At the time of writing this paper QKD is assumed to be more protected than any other known cryptosystem against classical as well as quantum computer attacks. Extensive research has been initiated for sophisticated implementation of QKD in practical communication networks. Built by BBN Technologies with funding from the US Defense Advanced Research Projects Agency (DARPA), the DARPA Quantum Network was jointly developed by researchers at Harvard University, Boston University and BBN Technologies in 2004. The main goal of this point-to-point DARPA Quantum network is to exploit QKD technology for standard internet traffic. The EU funded FP6 project SECOQC – Development of a Global Network for Secure Communication based on Quantum Cryptography, clearly shows the feasibility of constructing highly integrated QKD- networks. The SECOQC network prototype presents a splendid practical example for the development and operation of a point-to-point QKD network architecture with sophisticated protocols. There are number of other approaches and models for the utilization of QKD in network fashion. One step further, research has also been initiated for the integration of QKD protocols into the existing classical protocols which are widely used on the internet for secure communication, like PPP, IP-Sec and SSL-TLS.

The above mentioned progress reveals that the QKD network technology might be an essential part of the modern security schemes for high performance distributed computing applications. In the next section we have explained the potential weaknesses and requirements of the emerging distributed computing applications taking grid computing as an example.

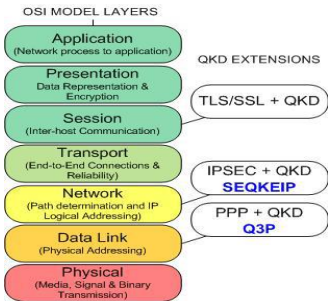

Fig 1: Integration of QKD with different layers of OSI Model

I. MOTIVATION

In computing, grid is a system architecture that coordinates resources which are not subject to centralized control; using standard, open, general purpose protocols and interfaces and delivers nontrivial quality of service. Grid computing is emerging as a modern technology to fulfill the high performance computing requirements of users, institutions and business organizations worldwide.

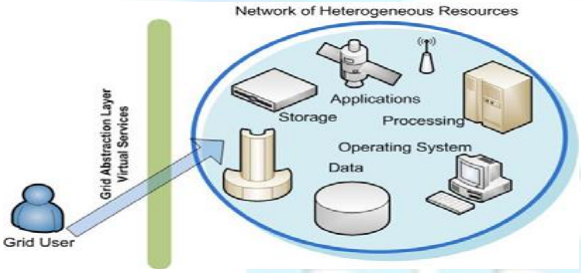

Fig 2: Grid computing (Distributed computing over a network of heterogeneous resources using open standard)

Although there are many important aspects of grid computing but the biggest barrier against the widespread adoption of grid computing is security. There are number of different security issues in grid computing, like data protection, job starvation, denial of service, policy mapping, and information security.

There are certain issues pertaining to the PKI authentication mechanism in grid systems. PKI is based upon Asymmetric Key Cryptography which does not provide unconditional security, rather it depends upon the unproven assumption of computing power, i.e. the attackers equipped with sufficient computing power, which may not be possible with the current technology, may crack the key. Key distribution techniques based on public key cryptography only provide computational security.

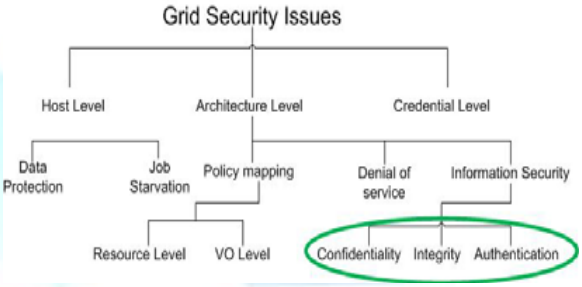

Fig 3: Classification of grid computing security Issues

Finding efficient algorithms to compute the inverse of one-way-functions has not been proven impossible and emerging powerful computers would pose real threats to their security.

II. PROPOSED GRID SECURITY MODEL BASED ON QKD NETWORK

We propose to utilize the QKD technology to enhance the PKI security for distributed computing. A conceptual model of Quantum Infrastructure Framework for Grid Computing is presented, taking the SECOQC QKD network as a model. This framework is based upon the concepts of integrating QKD network and protocol with the classical network and protocols. Authentication is the basis of security in grid. GSI composed of public key encryption, X.509 PKI certificates and SSL/TLS protocol to provide message protection, authentication, delegation and authorization. We propose to create a virtual organization (VO) among the users connected with the QKD network i.e. a grid computing environment secured by QKD technology, see Figure 4.

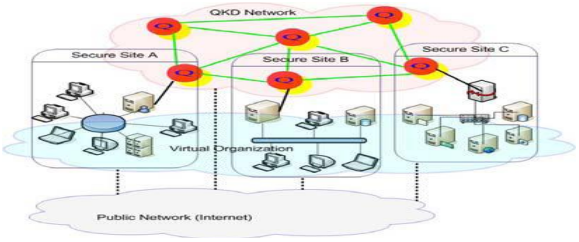

Fig 4: Conceptual model of grid computing based on QKD network

There are following main features in the proposed scheme.

• All the grid communities participating in this scheme are connected with QKD network as well as with the public network i.e. internet.

• It is assumed that all the users connected to the quantum network nodes are present in the secure sites, as shown in the Figure 4.

• The QKD network provides a key management and user authentication system with unconditional security based on QKD technology; hence replacing the vulnerabilities of PKI authentication mechanism against classical as well as quantum computer attack.

• The basic secure communication link between the two parties is possible via the SECOQC QKD network functionality. No upper layer application requires extra modification in order to exploit the unconditionally secure key material.

• In addition to the quantum key distribution capability all the QKD nodes are capable of acting like a Certificate Authority (CA), same as traditional PKI system.

• However the vision of grid is global, the proposed model is designed keeping in view the fact that the grid system secured by QKD network is a subset of the larger global grid which is secured by the classical PKI technology.

III. QUANTUM KEY DISTRIBUTION

A. Quantum cryptography

Quantum cryptography aims at exploiting the laws of quantum physics in order to carry out a cryptographic task. For the moment, the use of quantum physics at cryptographic ends is limited mainly to the distribution of secret keys. That's why we very often use the more precise term of quantum key distribution. The quantum key distribution rests on a common function of the whole protocols, namely the combined use of a traditional channel and a quantum channel. The sensitivity of the quantum channel to espionage is based on various points. First, it is impossible to duplicate an arbitrary quantum state. Second, the encoding of the quantum bits can be made sensitive to espionage since information is coded on at least two non-orthogonal states. Indeed, any measurement of a quantum object carried out in a basis other than the basis of which the quantum state is created will have an effect on the measured object. For that reason, the sender and receiver could obtain a real secret key, providing the use of some protocols including key distribution, key reconciliation and privacy amplification protocols. The quantum key distribution (QKD) is said "unconditionally secure", i.e. independent of the computation power of the spy, and more generally of the technology that he has.

B. BB84 and other QKD protocols

Up to now, several QKD protocols have been proposed since the birth of the first one BB84. BB84 was introduced by Bennet and Brassard in 1984, thus it was named BB84. In 1994, this protocol was proved to be secure against eavesdropping by Dominic Mayers, EliBiham, and Michael Ben-Or. BB84 is a nondeterministic protocol, which means that it is useful only for the distribution of a random sequence. BB84 is a four state protocol. Other protocols can be a two-state protocol (e.g. the B92), a three-state protocol or a six-state protocol. The BB84 and B92 protocols are nowadays widely used. These protocols are securely proven and largely experimented. Multiple techniques have been developed enabling quantum cryptography. We will in particular mention three techniques:

- Auto compensating weak laser pulse systems: This technique has been extensively studied and is used in commercially available products. Its particularity is that it is invariant to the

polarization rotation of the photon induced by the use of fiber optic.
- Entangled photons: Two photons are generated in a manner that their states are conjointly defined. One is sent to Alice, the other to Bob. Each person then measures the photons' polarization. - Continuous Variable: In this technique the information is not based on the photons' polarization but coded on the phase or amplitude of the light pulses.

As we use the BB84 for the integration of quantum cryptography in 802.11 networks, the remainder of his section is dedicated to the description of this protocol. The operating mode of BB84 consists on two main steps: Quantum transmission as presented in Fig. 5, and public discussion.

In the phase of quantum transmission, the information is encoded in non-orthogonal quantum states. The sender and the receiver must agree first on the meaning of the photon polarizations for instance 0 or □/4 for a binary 0, and □/2 or 3□/4 for a binary 1. The sender (Alice) generates a random bit string and a random sequence of polarization bases then sends the receiver (Bob) photon by photon. Each photon represents a bit of the generated bit string polarized by the random basis for this bit position. When receiving photons, Bob selects the polarization filters (rectilinear or diagonal) to measure the polarization of the received photon. In the phase of public discussion, after finishing the quantum transmission Bob reports the bases that he picked for each received photon. Alice checks Bob bases and says which ones were correct as described in Fig. 6

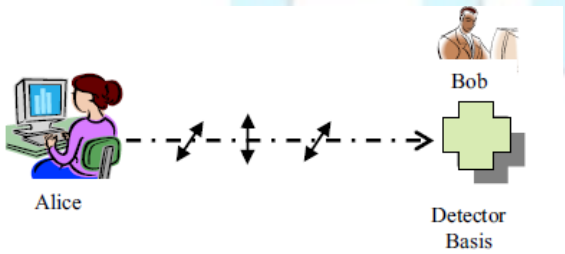

Fig 5: Photon Exchange

Bob and Alice take the bits resulting from these correct bases, these bits are only known by Alice and Bob. At this moment Alice and Bob share a secret bit string. This exchange is unconditionally secure providing that there is no eavesdrop or active attack and that the quantum channel is perfect. However, as an attack is always possible and the quantum channel is usually imperfect, an additional step is used to estimate the error rate.

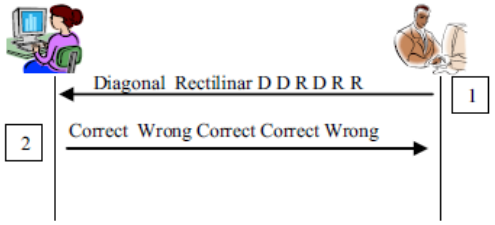

Fig 6: Validation of BOB bases

In this step, Bob chooses a random sequence of testing bits and sends it back to Alice. Alice checks whether these bits are in conformity with those sent by Alice originally. If there is an attack on the quantum channel the error rate will be about 25% or higher. In this case, Alice and Bob detect the eavesdropper. Otherwise, i.e. the error rate is less than 25%, the two parties discard the revealed bits and take the resulting stream as the secret key. The secrecy of this final stream is unconditional. Other steps could be applied to enhance the secrecy and generalize the unconditional security of key exchange. These steps are done mainly by error correction and privacy amplification.

C. Related works using quantum cryptography in mobile wireless networks

Free space QKD uses the air as the medium for the transmission of photons between the quantum sender and receiver. The feasibility of QKD over the air is considered problematic because of a medium with varying properties and a high error rate. However, the study and experiments of QKD systems showed that these problems are tractable. In contrast to the optical fibers, free space has a high transmission window where photons can be easily detected and a non-birefringent characteristic which does

not alter the polarization state of the photon. Although preliminary research and experiments on free space QKD start from a short distance and indoor environment, the final objective of these research and recent experimental systems is towards long distance and outdoor systems such as satellites or laser communication systems. The two approaches the most used in free space QKD studies are single qubit scheme based on faint-laser pulses and entanglement based quantum cryptography. Some recent results of the research on free-space QKD systems that can be cited as examples are the practical free-space QKD system over 10km on mountains using laser pulses and the BB84 protocol , the practical free space QKD system over 500m between two buildings in a city using weak coherent pulse and the BB84 protocol, the proposed free-space QKD system between satellites using entangled photons, and the experimental free space QKD system over 7.8 km between buildings using entangled photons. Different from above mentioned studies, our proposal aims at a short distance and an indoor environment, the wireless local area network 802.11. In comparison to the presented related work, our work has some advantages of the shorter distance and a better environment against bad weather conditions. The apparatus in our system may have a smaller size and 802.11 access points can be found almost everywhere indoor.

For a QKD system used together with a satellite or laser based data communication system, the outdoor environment can be much noisy. The large distance may need a bigger size apparatus, and the final mobile users who are inside a building cannot directly have a line-of sight optical path with the satellite or with the communicating point of a laser data transmission path, which is usually installed at the top of a high building. In fact, our proposal is final mobile user centric while previous related works are communication system centric. Hence, our work is not contradictory to the previous works but very complementary. The final mobile user can use our approach to establish a quantum key with the access point and secure the wireless link. The remainder part of the end-to-end communication can be secured also by quantum cryptography but realized by satellite-based or laser-based communication system.The disadvantage that we can encounter in comparison with the other related work is the problem of maintaining a line-of-sight path between the apparatus of the mobile user and the apparatus of the access point.

IV. INTEGRATING QKD IN 802.11I

A. How to integrate QKD in 802.11i?

. Our main objective is using quantum cryptography to establish the key used for the encryption of user data in 802.11i, which is the TK. As the TK is part of the PTK which is established during the 4-way handshake, we modify the 4-way handshake to integrate the BB84 protocol and call it the Quantum handshake

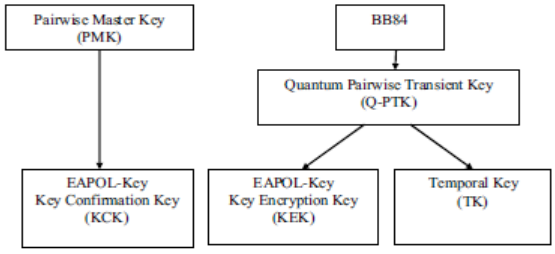

Fig 7: Keys establishment schema in the Quantum Handshake

Fig.7 summarizes how different keys are generated during the Quantum handshake. The KCK is generated from the PMK to serve the mutual authentication of the supplicant and the authenticator and protect the BB84 protocol from the man-in-the-middle attack. Once the mutual authentication finished, the supplicant and the authenticator starts the BB84 protocol for the establishment of the Q-PTK of 256 bits (for CCMP) or 384 bits (for TKIP). The Q-PTK is then splits into the KEK of 128 bits and the TK of 128 bits (for CCMP) or 256 bits (for TKIP). The integration of quantum cryptography into 802.11i should be step in step and changes should be minimized at the beginning. A step in step and modular integration will facilitate the experiment and testing process. For this reason,

the principle of generating the KCK remains unchanged. That means that the KCK is generated from the PMK within the mutual authentication process between the mobile terminal and the access point. Once the KCK is generated and both the supplicant and the access point are authenticated, the BB84 protocol is used to establish the encryption key TK. As the GTK, the key used for the encryption of group traffic, is distributed from the access point to the mobile terminal via the encryption using the KEK, we decide to establish also the KEK by quantum cryptography to secure more the GTK distribution process.

B. Quantum handshake

In the first design of the Quantum handshake presented in Fig. 8, the BB84 protocol is started when the Supplicant is authenticated by the authenticator but the Authenticator has not been authenticated yet. The authenticator is only authenticated after the fifth message of the Quantum handshake. This design presents a problem of potential waste of resources. If the access point is a fake one, the photons are exchanged before the fake access point is detected.

Fig. 8 presents the enhanced version of the Quantum handshake. The three first messages of the Quantum handshake allow the Supplicant and the Authenticator to derive a fresh KCK and authenticate each other before starting the BB84 protocol.In the second message, the Supplicant sends to the Authenticator the SNonce value and a MIC calculated based on the message content and the KCK just derived.

When this message arrives at the Authenticator, the access point has all materials to build the KCK and use it to authenticate the Supplicant via the verification of the MIC received. If the Supplicant is authenticated, the Authenticator sends the third message of the Quantum handshake appending a MIC allowing the Supplicant to authenticate the authenticator.

This message can also be used as a control message for the QKD process. For example, this message can send a QKD-start signal to inform the Supplicant that the access point is ready to receive photons from the mobile terminal. If the Authenticator is authenticated, the Supplicant starts the photon transmission step of the BB84 protocol.

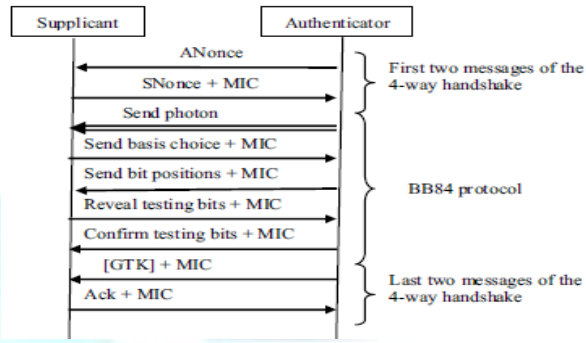

Fig 8: The first design of the Quantum Handshake

V. CONCLUSION

As a result of our proposed solution we conclude that QKD Networks have strong applications in the high performance distributed computing. Issues of confidentiality, integrity and authentication, in grid computing, can be solved using QKD technology. Although the vision of Grid computing is global, but QKD networks are very few and still in the testing phase, which is the biggest barrier against the wide spread exploitation of QKD technology on large scale distributed computing networks. Also the high cost of implementation of QKD Networks is also an issue for its exploitation on large scale networks. Interoperability of QKD with other widely used security schemes like PKI and Kerberos is also possible, as a result of the proposed solution. Modern security applications should be designed keeping in view the requirements and limitations of QKD technology, so that as the QKD technology will become more mature, it would be easier to exploit its unconditional security power in those applications.

In this paper, we present an enhanced version of the Quantum handshake, a scheme integrating quantum key distribution in 802.11 networks proposed by our previous works. The

Quantum handshake, a modified version of the 4-way handshake, is defined to integrate the BB84 protocol for the distribution of the cryptographic keys used by 802.11i. In the enhanced version, the mutual authentication between communicating parties must be done before the photon exchange to avoid potential waste of resources. The quantum handshake is our first step in the integration of quantum cryptography in mobile wireless networks.

REFERENCES

[1] Elliott, C., *The DARPA Quantum Network.* Quantum Communications and Cryptography, 2006.

[2] Mehrdad Dianati, R.A., Maurice Gagnaire, Xuemin (Sherman) Shen, *Architecture and protocols of the future European quantum key distribution network.* Security and Communication Networks, 2008. (1): p. 57 - 74.

[3] Poppe, A., M. Peev, and O. Maurhart, *Outline of the SECOQC quantum-key distribution network in Vienna.* International Journal of Quantum Information, 2008. **6**(2): p. 209-218.

[4] Alleaume, R., et al., *SECOQC White Paper on Quantum Key Distribution and Cryptography.* Arxiv preprint quantph/ 0701168, 2007.

[5] Khan, M.M., et al., *A Quantum Key Distribution Network through Single Mode Optical Fiber.* Proceedings of the International Symposium on Collaborative Technologies and Systems, 2006: p. 386-391.

[6] Le, Q.C. and P. Bellot, *Enhancement of AGT Telecommunication Security using Quantum Cryptography.* Research, Innovation and Vision for the Future, 2006 International Conference on, 2006: p. 7-16.

[7] Kimble, H.J., *The quantum internet* Nature, 2008. **453**(7198): p. 1023.

[8] Gisin, N. and R. Thew, *Quantum communication.* NATURE PHOTONICS, 2007. **1**(3): p. 165.

[9] Nguyen, T.M.T., M.A. Sfaxi, and S. Ghernaouti-Hélie, *802.11 i Encryption Key Distribution Using Quantum Cryptography.* JOURNAL OF NETWORKS, 2006. **1**(5): p. 9.

[10] Ghernaouti-Helie, S. and M. Sfaxi, *Upgrading PPP security by quantum key distribution.* NetCon 2005 conference, 2005.

[11] Ghernaouti-Helie, S., et al., *Using quantum key distribution within IPSEC to secure MAN communications.* MAN 2005 conference, 2005.

[12] Ghernaout-Helie, S. and M.A. Sfaxi, *Applying QKD to reach unconditional security in communications.*

[13] Rass, S., et al., *Secure Message Relay over Networks with QKD-Links.* Quantum, Nano and Micro Technologies, 2008 Second International Conference on, 2008: p. 10-15.

[14] Chakrabarti, A., A. Damodaran, and S. Sengupta, *Grid computing security: A taxonomy.* IEEE Security & Privacy, 2008.**6**(1): p. 44-51.

[15] Zhao, S.A., Akshai Kent, Robert D, *PKIBased Authentication Mechanisms in Grid Systems.* Networking, Architecture, and Storage, 2007. NAS 2007, 2007: p. 83-90.

[16] Dianati, M. and R. Alleaume, *Architecture of the Secoqc Quantum Key Distribution network.* Arxiv preprint quant-ph/0610202,2006.

[17] Integration of Quantum Cryptography in 802.11 Networks The Mai Trang Nguyen, Mohamed Ali Sfaxi, and Solange Ghernaouti-Hélie .

[18] Bennett, C. H., and Shor, P. W. Quantum information theory. IEEE Transaction on Information Theory 44, 6 (1998), 2724–42.

[19] Shannon, C. E., 1949, ‘‘Communication theory of secrecy systems, ’’ Bell Syst. Tech. J**2**8, 656–715.

[20] B. Schneier, *Applied Cryptography*, John Wiley & Son,1996.

[21] K. G. Paterson, F. Piper, and R. Schack, “Why quantum cryptography?”, *Quantum physics*, quant-ph/0406147, June 2004.