Applications of QKD Network for High Performance Distributed Computing

Muhammad Mubashir Khan, Jie Xu
School of Computing, University of Leeds, LS2 9JT, UK
{mmkhan, jxu} @comp.leeds.ac.uk

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.

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 [1]. 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 [2-4], 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, see [5-8]. 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 [9-13].

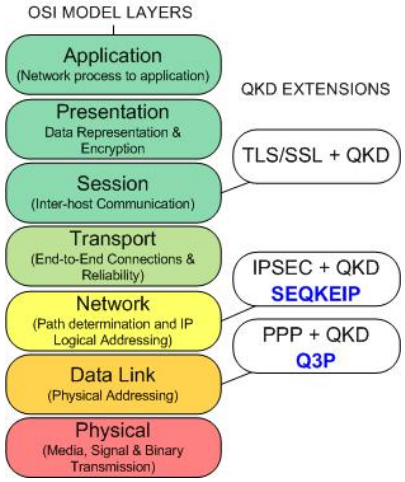

Figure 1: Integration of QKD with different layers of OSI Model

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.

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 non-trivial 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.

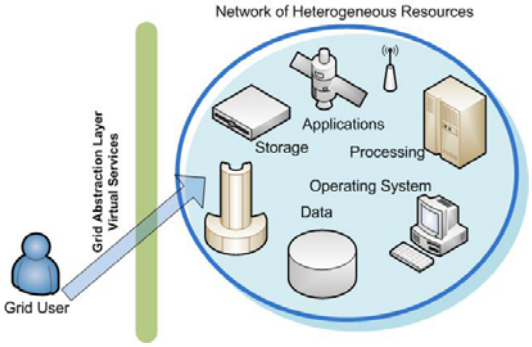

Figure 2: Grid computing (Distributed computing over a network of heterogeneous resources using open standard)

Although there are many important aspects of grid computing but the biggest barrier against the widespread adoption of grid computing is security. According to [14], there are number of different security issues in grid computing, like data protection, job starvation, denial of service, policy mapping, and information security. Confidentiality, integrity and authentication are the key issues in information security. These issues are normally handled by the PKI (Public Key Infrastructure).

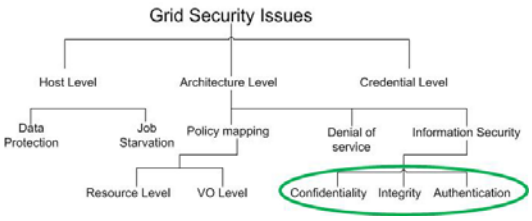

Figure 3: Classification of grid computing security issues

There are certain issues pertaining to the PKI authentication mechanism in grid systems [15]. 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. According to [16], key distribution techniques based on public key cryptography only provide computational security. 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.

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.

Globus Alliance introduced the grid security foundation built on top of Grid Security Infrastructure (GSI). 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.

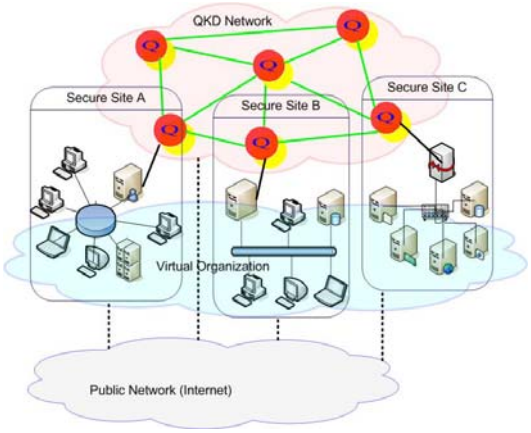

Figure 4: Conceptual model of grid computing based on QKD network

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. As explained in detail in [2], no upper layer application require 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.

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.

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**(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 quant-ph/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, *PKI-Based 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.