# Trends in Applied Sciences Research

ISSN 1819-3579

Academic
Journals Inc.

www.academicjournals.com

Trends in Applied Sciences Research 10 (5): 270-277, 2015
ISSN 1819-3579 / DOI: 10.3923/tasr.2015.270.277
© 2015 Academic Journals Inc.

# Quantum Security for University Networks Protection

Mohammed S. Zahrani
College of Computer Science and Information Technology, King Faisal University, Al-Ahsa, 31982, Saudi Arabia

## ABSTRACT

In this era of electronic communication, where computers and other manual devices are sending and receiving messages via wireless networks, security and privacy has always been a fundamental concern. Wireless network is an open medium with air as a transmission media involving radio frequencies which have been easily decode-able since World War II. But, behind every wireless network there is a core network which is normally wired. World has become a global village due to this effective approach of wireless communication. It is an alarming issue now days to secure our core network providing wireless services for home, universities, government and military. Many security protocols have been implemented to secure core networks but there are a great number of security risks associated with the current protocols and encryption methods. Secure information transactions takes place within the limited realms of key encryption and exchange techniques. For secure information transaction, a secret key must be known to both the sender and the receiver hiding it from outside world. This study highlighted the implementation of secure communication of key and successfully addressed the security threats in core network designed for King Faisal University (KFU) accomplished by quantum cryptography. The study also suggested to investigate alternate Quantum Key Distribution (QKD) architectures exploring application of emerging QKD in wireless sensor network and its modeling in a real network.

**Key words:** Quantum cryptography, QKD, wireless communication, network security

## INTRODUCTION

Quantum cryptography is a technique of secure communication which enables the sender and the receiver to produce a shared random secret key known only to them to encrypt and decrypt the message. Basically, quantum cryptography is a form of cryptography that uses quantum mechanical properties of communication channel to enhance the security of shared key distribution to the sender and the receiver. For secure and fast communication, quantum cryptography also runs over optical fiber channel in wired networks and uses light photon properties and the polarization of those photons. The security of quantum cryptography relies on the foundation of quantum mechanics, unlike other public key encryption based on mathematical functions and cannot provide any indication of a hacker or guarantee of key security. It is possible to build a perfectly secure key distribution system based on the principles of the quantum physics known as Quantum Key Distribution (QKD). The keys produced using quantum key distributions are guaranteed to be secret.

A cryptographic system is a combination of cryptographic algorithm and a communication system. Almost any cryptographic system by giving enough time and resources could eventually be solved. The only exception to this is a system which uses absolutely random changing keys with every character encrypted and never repeated which is termed as One Time Pad according to Vernam (1926) and Wang (2011). Previously, many quantum cryptographic schemes were proposed by Liu *et al*. (2011) and Buhrman *et al*. (2011). But the one well reviewed and experimentally

Table 1: Photon polarization (Anghel, 2012)

| Base | Rectilinear | Diagonal | Rectiliniar | Diagonal |
|---|---|---|---|---|
| State | 0° | 45° | 90° | 135° |
| Qbit | → | ↗ | ↑ | ↖ |
| Bit | 0 | 0 | 1 | 1 |

realized was the Quantum Key Distribution protocol (QKD). Generally, the QKD schemes utilize photons to transfer classical bit information. The keys produced using QKD schemes proved to be secret as endorsed by BB84 protocol and explained by Bennett and Brassard (1984) and Khan and Xu (2012). Besides, it can be used in conjunction with any Classical Cryptographic System (CCS). Furthermore, BB84 is the first known quantum key distribution scheme named after the findings of Bennett and Brassard (1984). In order to implement the BB84 algorithm, this study chose for photon polarization the Rectilinear (R) and Diagonal (D) bases as well as the convention from Table 1 to represent the bits from the key.

The various steps of BB84 quantum key distribution algorithm were fully described by Anghel (2012) for the type of photon to use (rectilinearly polarized, R, or diagonally polarized, D) in order to represent each bit in s. In addition to that Anghel (2012) also reported the procedure which allowed the sender and the receiver to detect the eavesdropper's presence and to reschedule their communications.

The Quantum Bit Error Rate (QBER) method calculates the percentage of errors in the final key according to Treiber (2009) obtained at the end of quantum transmission after bases reconciliation stage. Also, the QBER was defined by Anghel (2012) as follows:

$$\text{QBER} = (\text{Q1-QF})/\text{Q1}\times100$$

where, Q1 represent the number of qbits from primary key and QF represent the number of qbits from final key. The QBER method relies on the fact that the eavesdropper will create an increase in the QBER value.

The Quantum Bit Travel Time (QBTT) method of Anghel (2011a, b) can be implemented in every type of quantum key distribution system and has the advantage that the eavesdropper can be detected by receiver during the quantum transmission after each transmitted qbit. This method uses the fact that the optical components (polarization filters) induce time delays as reported by Zhao and de Raedt (2008). Previous studies contributed towards theoretical security proofs and practical implementations of QKD scheme. Also, efforts were made to blend the security proofs to prove the security of practical implementation prototypes (Wang, 2011). Recently it was proved that QKD protocols can be incorporated with wireless networks to improve their security (Anghel and Coman, 2009; Lopes and Sarwade, 2015).

The QKD systems are emerging in the cryptographic solution space where many claim that they function as unconditionally secure key distribution devices. According to Mailloux *et al.* (2015), the term "Key distribution" is somewhat misleading as QKD systems generate or grow shared secret keys from previously established keys and don't merely distribute them. But the QKD systems can be paired with and configured to increase the security posture of the traditional symmetric encryption algorithms such as Data Encryption Standard (DES), 3DES and advanced encryption standard through frequent rekeying. Other commercial offerings from SeQure net, Quintessence labs, Magi-Q technologies and quantum communication technology showed similar performance limitations (Quantique, 2015; Mailloux *et al.*, 2015). Recent technological advancements in the QKD systems resulted in a diverse trade space of competing design and implementation choices including several encoding schemes and quantum exchange protocols (Mailloux *et al.*, 2015).

For a basic channel model (namely, degraded wiretap channel), the concept of secrecy rate was studied and defined as a maximum achievable transmission rate at which the legitimate receiver can reliably decode the signals whereas an eavesdropper cannot obtain any information (Rostom *et al*., 2014). The protocol "4-way handshake" was modified to integrate the BB84 of the quantum cryptography in order to obtain a new protocol which was defined as the "Quantum handshake" (Rostom *et al*., 2014; Li *et al*., 2014).

As compared to the traditional wireless network, Wireless Mesh Network (WMN) has many advantages such as non-line of sight transmission expands the application field of wireless broadband, high transmission rate makes transmission distance relatively short, high reliability, faster network configuration and maintenance and low cost. However, in Wireless Mesh Networks (WMN) nodes can be divided into three types based on their functions namely Mesh Point (MP) which only supports the mesh interconnection, Mesh Access Point (MAP) which supports the mesh interconnection and access and the Mesh Point with a Portal (MPP) which supports the mesh interconnection and network communication (Li *et al*., 2014). Presently, the use of network is increasing enormously in educational institutions of Saudi Arabia and its security is a burning issue. The objective of this study is the quantum transmission with error estimation, error correction, privacy amplification by implementing the QKD system in a real network at University level.

## MATERIALS AND METHODS

The author has proposed a model for the security of King Faisal University's (KFU) IT Infrastructure which provides internet and data sharing services to 16 different colleges within the campus (Fig. 1).

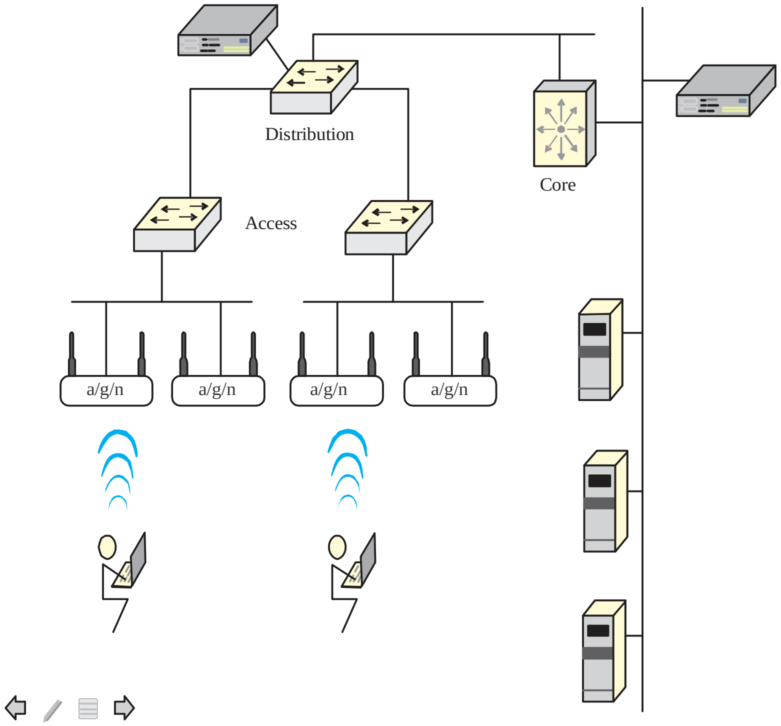

Fig. 1: Proposed KFU IT network

As shown in Fig. 1, the core network of KFU is connected to the servers i.e. proxy server, data sharing server, banner server through optic fiber. The QKD server is attached to the core network before the core switch. The core switch has direct communication with distribution switch through optic fiber and the QKD server is attached to the distribution switch as well. The distribution switch is providing services to 16 colleges via access switches. The network services are distributed with the help of wireless access points to the faculty, students and staff of the college. The wireless access point communicate with each other using proprietary layer 2 routing protocols, forming a self healing wireless infrastructure.

## RESULTS AND DISCUSSION

The author simulated the QKD in the proposed Information Technology (IT) network of King Faisal University (KFU) using QKD simulator built in C and Python. The initial configuration values of simulator are presented in Table 2.

In order to implement the BB84 Quantum transmission, random initial configuration values were selected from Table 2. For example, A prepares a sequence of 590 qubits and send them to B over the quantum channel. B randomly chooses a basis for each qubit, rectilinear polarization (horizontal/0° and vertical/90°) or a diagonal polarization (+45° and -45° shifted). B then maps horizontal and vertical with the qubit states |0> and |1> and +45° and -45° shifted with the states |+> and |->, respectively as summarized below:

- A sent 590 qubits to B with a basis selection bias of 0.6
- Hacker 'H' is eavesdropping on the quantum channel at a rate of 0.2 and with a basis selection bias of 0.6. There is an eavesdropper, 'H', listening in on the channel. H intercepts the qubits, randomly measures them in one of the two mentioned bases and thus destroys the originals and then sends a new batch of qubits corresponding to his measurements and basis choices to B. Since H can choose the right basis only 50% of the time on average, about 1/4 of his bits differ from those of A

**Reconciliation-biased error estimation:** A and B used a biased error estimation scheme. They choose 2 random test subsets, the first consisting of all measurements where A and B both used the rectilinear basis and the second one used the diagonal basis. This scheme offers advantages with respect to a specific attack like the biased eavesdropping strategy. They finally used the estimated error rate to determine whether they should proceed to error correction or whether they should abort the protocol based on a predefined error tolerance threshold, usually around 11%. The detail of the results are summarized below:

Table 2: Initial configuration of QKD implementation

| Parameters | Values |
|---|---|
| Property qubit count | 590 |
| Basis choice bias delta | 0.6 (probability) |
| Eve basis choice bias delta | 0.6 (probability) |
| Eavesdropping | 1 |
| Eavesdropping rate | 0.2 |
| Error estimation sampling rate | 0.3 |
| Biased error estimation | 1 |
| Error tolerance | 0.31 |

- A and B permute their sifted keys in order to flatten the errors across the entire bit string. They then performed the error estimation by comparing a subset of their error-flattened sifted keys
- An error rate of 0.1053 was estimated using a sampling ratio of 0.3

**Reconciliation-error correction, cascade:** A and B performed an interactive error correction scheme called cascade on the public channel in order to locate and correct the erroneous bits in their sifted bit strings. The details of study are given below:

- Cascade was run 6 rounds in order to correct the errors
- 26 erroneous bits were detected and corrected
- 141 bits were leaked in order to correct the errors
- With an error probability of 0.1256, the Shannon bound for the number of leaked bits was 113.0 as compared to the actual number of leaked bits equal to 141

**Error correction confirmation and authentication:** A and B confirmed and authenticated the error correction phase by computing the hash of their error corrected keys using their mutually pre-shared secret key and by comparing their respective digests. The study details are given below:

- 64 bits of key material (pre-shared secret key) were used to authenticate
- The Linear Feedback Shift Register (LFSR) universal hashing scheme was used for authentication

**Privacy amplification:** A and B computed the overall information leakage and run a privacy amplification protocol in order to reduce or minimize H's knowledge gained on the key by having eavesdropped on the channel. They did so by locally applying a universal hashing scheme based on Toeplitz matrices. The hashing function was indexed using yet another chunk of their pre-shared secret keys. They also defined a security parameter to minimize H's knowledge to an arbitrary amount as summarized below:

- 173 bits were leaked up to this point
- The key length before running privacy amplification consists of a total of 207 bits
- The final key length consisted of 14 bits
- The value of chosen security parameter was 20

Based on the simulation, the statistical overview of the QKD implementation in network of King Faisal University (KFU), Al-Ahsa for different colleges and staff is presented in Table 3.

A graph was plotted between the error and the leakage of bits by using QKD simulation tool-kit that reflected some of the asymptotical properties of QKD and certain specific studies found (Fig. 2). A linear relationship was observed between the error and the leakage of bits with QKD simulation. Similar findings were reported by Mailloux *et al*. (2015) who concluded that such technologies have resulted in a diverse trade space of design competition and choice of implementation which included many encoding schemes and quantum exchange protocols.

Table 3: Statistical Overview of QKD implementation

| Parameters | Values |
|---|---|
| Initial number of qubits | 590 |
| Final key length | 14 |
| Estimated error | 0.1053 |
| Eavesdropping enabled | 1 |
| Eavesdropping rate | 0.2 |
| A/B basis selection bias | 0.6 |
| H basis selection bias | 0.6 |
| Information leakage (Total number of disclosed bits) | 173 |
| Overall key cost for authentication | 256 |
| Key length before error correction | 207 |
| Bit error probability | 0.1256 |
| Bits leaked during error correction | 141 |
| Shannon bound for leakage | 113 |
| Security parameter | 20 |

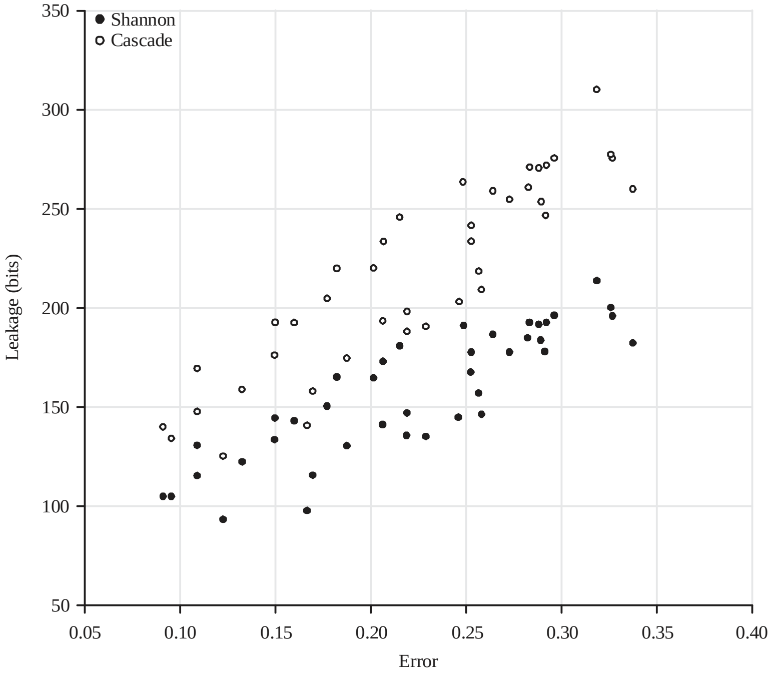

Fig. 2: QKD shannon bound vs. Error correction plot

The study results were also comparable with the findings of Lopes and Sarwade (2015) who suggested that incorporation of QKD protocol with wireless network improved the system security.

## CONCLUSION

This study presented quantum transmission, error estimation, error correction and privacy amplification by implementing QKD in a real network. Basically, the QKD simulation programs are meant to give an alternative to physical implementation of the quantum devices used in the quantum transmission. It provides a safe key exchange i.e. robust against attacks from hackers. Implementation of QKD ensures long-term data protection and forward secrecy. One quantum key server can distribute keys to several encryptors for up to 100 Gbps of data. It works on dark fibre and WDM networks. The devices for implementing quantum key distribution exist and the performance of the demonstration system is being continuously improved.

By implementing the QKD of quantum cryptography, it was found a reliable and applicable technique integrating with larger networks and especially the E-Learning systems of universities. It also made the KFU's IT network more secure and reliable to avoid any network security events. Thus the long-term goals of quantum security systems are realistic implementations that can be achieved through fibers and wireless networks.

It suggests and recommends to study alternate QKD architectures exploring emerging applications such as QKD in Wireless Sensor Networks (WSN) and its modeling capabilities in a real network. The proposed strategy can be tested and experimented for evaluating the accuracy of approach. Depending on the results, possibilities of further improvements are high.

## REFERENCES

Anghel, C. and G. Coman, 2009. Base selection and transmission synchronization algorithm in quantum cryptography. Proceedings of the 17th International Conference on Control Systems and Computer Science, Volume 1, September 2009, Bucharest, Romania, pp: 281-284.

Anghel, C., 2011a. New eavesdropper detection method in quantum cryptography. Annals Dunarea de Jos University Galati, 34: 1-8.

Anghel, C., 2011b. New quantum cryptographic protocol. Annals Dunarea de Jos University Galati, 34: 7-13.

Anghel, C., 2012. Research, development and simulation of quantum cryptographic protocols. Elektronika ir Elektrotechnika, 19: 65-70.

Bennett, C.H. and G. Brassard, 1984. Quantum cryptography: Public key distribution and coin tossing. Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Volume 175, December 10-12, 1984, Bangalore, India, pp: 175-179.

Buhrman, H., N. Chandran, S. Fehr, R. Gelles, V. Goyal, R. Ostrovsky and C. Schaffner, 2011. Position-based quantum cryptography: Impossibility and constructions. Lecture Notes Comput. Sci., 6841: 429-446.

Khan, M.M. and J. Xu, 2012. Generalization of quantum key distribution protocol. Int. J. Comput. Sci. Network Secur., 12: 98-101.

Li, M., X. Lv, W. Song, W. Zhou, R. Qi and H. Su, 2014. A novel identity authentication scheme of wireless mesh network based on improved kerberos protocol. Proceedings of the 13th International Symposium on Distributed Computing and Applications to Business, Engineering and Science, November 24-27, 2014, Xian Ning, pp: 190-194.

Liu, B., F. Gao and Q.Y. Wen, 2011. Single-photon multiparty quantum cryptographic protocols with collective detection. IEEE J. Quantum Electron., 47: 1383-1390.

Lopes, M. and N. Sarwade, 2015. On the performance of quantum cryptographic protocols SARG04 and KMB09. Proceedings of the International Conference on Communication, Information and Computing Technology, January 16-17, 2015, Mumbai, India, pp: 1-6.

Mailloux, L.O., M.R. Grimaila, D.D. Hodson, G. Baumgartner and C. McLaughlin, 2015. Performance evaluations of quantum key distribution system architectures. IEEE Security Privacy, 13: 30-40.

Quantique, I.D., 2015. Quantum-safe cryptography. What is it and why should you care? March 2015. http://www.idquantique.com/quantum-safe-cryptography/.

Rostom, R., B. Bakhache, H. Salami and A. Awad, 2014. Quantum cryptography and chaos for the transmission of security keys in 802.11 networks. Proceedings of the 17th IEEE Mediterranean Electrotechnical Conference, April 13-16, 2014, Beirut, Lebanon, pp: 350-356.

Treiber, A., 2009. A fully automated quantum cryptography system based on entanglement for optical fibre networks. New J. Phys., 11: 1-19.

Vernam, G.S., 1926. Cipher printing telegraph systems for secret wire and radio telegraphic communications. Am. Instit. Elect. Eng. Trans., 55: 295-301.

Wang, Y., 2011. Unconditional security of cryptosystem: A review and outlook. Trends Applied Sci. Res., 6: 554-562.

Zhao, S. and H. de Raedt, 2008. Event-by-event simulation of quantum cryptography protocols. J. Comput. Theor. Nanosci., 5: 490-504.