International Journal of Electronic and Electrical Engineering.
ISSN 0974-2174, Volume 7, Number 6 (2014), pp. 623-630
© International Research Publication House
http://www.irphouse.com

Fiber Quantum Key Distribution Technology for SCADA Communication

Shailendra Rathore[1], Sumit Miglani[2], Haresh Joshi[3] and Murli Manohar Sharma[4]

[1]M.E. (Information Security) Thapar University, Patiala, India
[2]Thapar University, Patiala, India
[3]Manager(Technology) Crompton Greaves Ltd. Mumbai, India
[4]M.E. (Information Security) Thapar University, Patiala, India

Abstract

Supervisory Control and Data Acquisition (SCADA) system is widely used in the management of critical infrastructure as well as modern industrial facility such as in manufacturing, Power Systems, Water Treatment and Distribution system. For more usability at lower cost SCADA has increased integration between many networks and the use of IT system. This has increased a higher risk from cyber threats. Recently many researching efforts have been made on SCADA communication network for improving its security. One such effort is the quantum cryptography. This paper shows the comparison between the Classical Cryptography and Quantum Cryptography how the Quantum Cryptography provides strong security assurance with the SCADA communication without introducing excessive delays and latency in data delivery over Classical Cryptography.

IndexTerms: SCADA system, Quantum cryptography, Classical cryptography.

1. Introduction

SCADA stands for Supervisory Control and Data Acquisitions widely deploying over real time infrastructure sectors such as water treatment and distribution, oil and gas pipelines, electrical utility, private and public transportation services for supervisory and controlling infrastructure. In past SCADA system worked as a standalone system which used proprietary protocol and vendor -specific hardware and software.

But in recent years to improve the communication and to augment the degree of automation in the system it is using open protocol and PCs with common operating system, thereby, connecting to the internet to enable sharing of information across the enterprise. This introduces the cyber security problem and higher risk from cyber attack thread. SCADA system uses various methods to solve cyber security problem. Encryption is the most common and powerful approach to securing the SCADA communication. In recent year many cryptographic algorithm has been proposed for encryption.

In this paper we mainly explore the application of Fiber Quantum Key Distribution (QKD) technology for SCADA communication. In second section, the use of classical cryptography in SCADA is analyzed. In third section, an overview of optical fiber communication in SCADA is done. In the fourth section, Principle of fiber QKD is discussed. In fifth, typical use of fiber QKD in SCADA communication is proposed. Finally in the sixth section, Quantum Cryptography comparison with Classical Cryptography is presented.

2. Classical Cryptography

Classical cryptography (CC) algorithm uses several mathematical techniques to restrict eavesdroppers from knowing the content of encrypted message. It is categorized into symmetric and asymmetric encryption algorithm.

2.1 Symmetric Encryption Algorithm

Symmetric encryption is also referred to as shared key or single key encryption. As shown in *Fig.1*, in this type of encryption both sender and receiver share the same key which is used to both encode and decode the message. Sender and receiver have to exchange only key in advance in a secure manner and key must be secret [1]. Thus, in order to implement this in a secure manner, the communication channel must be made secure.

In SCADA, master station may be connected with multiple RTUs and master station has to store a shared key for the communication with every RTU. This creates a problem with managing and ensuring the security of these keys. Thus symmetric encryption is no longer used in SCADA. This problem can be solved by using Asymmetric encryption techniques.

2.2 Asymmetric Encryption Algorithm

Asymmetric Encryption Algorithm is also referred to as Public key encryption. It uses two key for encryption, i.e. a public key and a private key. The public key is publicly available and is used to encrypt message by anyone who wants to send a message to the person that the key belongs to. The private key is kept secret and is used to decrypt receiver message.

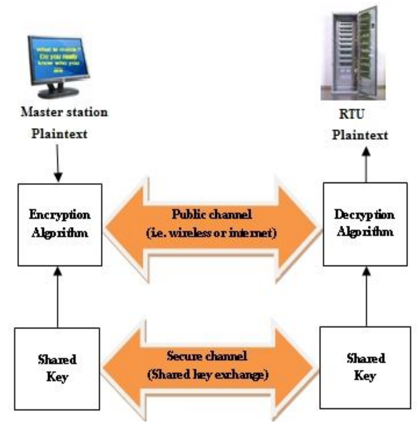


Fig. 1: Symmetric key encryption.

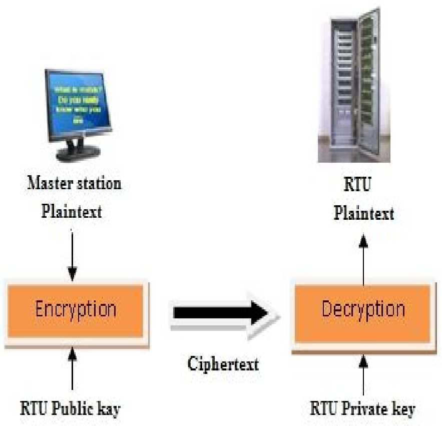


Fig. 2: Asymmetric key encryption.

As shown in *Fig.2* in SCADA if master station wants to send a secret message to RTU. It would encrypt its message with RTU public key and send it via an insecure channel. RTU receive the message and decode it using its private key. These encryption techniques ensure that the master station (sender) can’t decode his message once encrypted. This encryption technique depends on the fact that contain mathematical operation are possible to do in one direction than the other direction. RSA (Rivest-Shamir-Adleman) is an example of first public key cryptosystem [2]. Asymmetric encryption is slow compared to symmetric encryption but SCADA require fast response in real time so it is not feasible for use in decrypting bulk messages. In addition it uses more computer resources which increase the cost of SCADA and maintenance problem of each resource. The disadvantage of classical cryptography is that it does not provide any method for detecting eavesdropping or attacker between RTU and Master station communication. This problem can be solved by using Quantum Cryptography which requires the optical fiber communication between RTU and Master station. Such kind of cryptography can also be implemented in the workflow scheduling in cloud computing [10].

3. Optical Fiber Communication in SCADA

In SCADA Master Station –RTU communication channel can be

1. The internet 2. Satellite 3. Radio
4. Optical fiber 5. Wi-Fi 6. Ethernet

However Fiber optic cable is the most preferred solution for SCADA system due to greater bandwidth, secure transmission, reliability and long distance it covers but in recent year optical fiber tapping technology creates a problem of security for optical fiber communication. This technology provides an opportunity for eavesdroppers to tap the optical fiber network, collect data and use the data for malicious purposes in future. The extraction of information from optical fibers is relatively simple once they are accessed. There are various fiber optic tapping methods including fiber bending, splitting, evanescent coupling, scattering and v-grooves [3]. The most effective method for protecting sensitive data and detect the eavesdropper on optical fiber network against tapping is through encryption using Fiber Quantum Key Distribution.

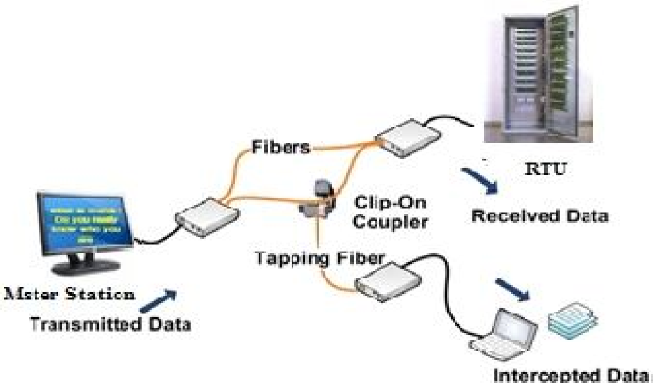


Fig. 3: Fiber optic tapping.

4. Principal of Fiber Quantum Key Distribution Technology

Quantum key distribution invented in 1984 by “Charles Bennett” and Gilles Brassard provide secure key distribution solution based on quantum mechanics [4]. QKD relies on two important principle in quantum mechanics first one is Heisenberg uncertainty principle defines that it is impossible to measure the quantum state of any system without perturbing it.

This principle can be used to detect the attempt of eavesdropper between communications of two valid users in QKD based cryptosystem. Second principle is Polarization of photon defines that how light photon can be polarized in specific direction and a polarized photon can only be detected by a photon filter with the correct polarization otherwise photon will be destroyed [5].In addition the creation of identical copies of unknown quantum state in quantum mechanics is prohibited this is known as the no cloning theorem [6].

QKD uses two main relevant protocols BB84 and B92.BB84 protocol simply states that a photon may be polarized in one of the two bases. One basis can consist of horizontal (|H|) and vertical (|V|) polarization state of photon, let us call this basis Rectilinear. The other basis, diagonal, can consist of states of linear polarization at 45` (anti-diagonal) |A|, and 135` (diagonal) | D|.

As shown in *Fig.4*, at the beginning the two parties say Alice and Bob wish to communicate agree that |H| and |D| represent the bit value ‘0’ and |V| and |A| represent the bit value

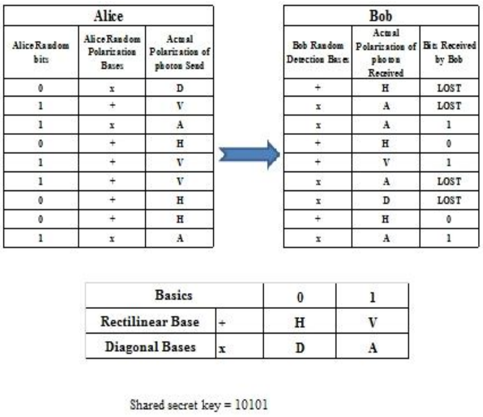
‘1’. Now Alice (the sender) generate a sequence of random bits that she wants to transmit and converts each bit into polarized photons on the basis of randomly choose polarization state among four polarization states |H|, |V|, |A|, |D| and send it through a communication channel to the receiver Bob. At the receiver end Bob reconverts the photon back into the bit on the basis of randomly chooses polarization state by him. Alice and Bob need an auxiliary public channel to tell each other what polarization state they had used for each transmitted and detected photon whenever their state coincide “Alice” and “Bob” keep the bit. On the other hand the bit is discarded when they choose different state or due to the imperfect efficiency of detector. The sequence of keeping bits work as Quantum key for encryption and decryption.

To check the presence of eavesdropping let us assume that the final key comprises ‘n’ binary bits. Alice and Bob randomly select subset of these bits say ‘k’ bits and compare these bits if they differ by certain bits say ‘p’ bits then they would know someone was listening in and then would not use the key. They would need to start the key exchange again over a secure channel inaccessible to someone. On the other hand if they match then they have concluded that the key is secure. Since they have communicated k bits over un-secure channel, these k bits should be discarded and final key will be n-k bits. Thus QKD is easy and convenient.

5. FIBER QKD in SCADA Communication

In SCADA it is important to secure the communication between the master station and RTUs as well as communication between RTUs for example information like open/close breaker orders or electrical measure (input voltage, output voltage, current) can be highly sensitive and must be protected. In this situation fiber QKD can be used.

As shown in *Fig.5*, The master station and RTU are connected with QKD link which could be optical fibers.QKD link continuously generate and exchange the cryptographic keys. Data between master station and RTUs is encrypted by using cryptographic keys generated by QKD link and suitable encryption algorithm (for example Advance Encryption Standard AES or One Time Pad for higher security) and transmit this data on an Ethernet of fiber channel link. Thus QKD link can ensure the master station–RTU communication and RTU–RTU communication is secured.



Alice		
AliceRandom bits	AliceRandom Polarization Bases	Actual Polarization of photon Send
0	x	D
1	+	V
1	x	A
0	+	H
1	+	V
1	+	V
0	+	H
0	+	H
1	x	A

Bob		
Bob Random Detection Bases	Actual Polarization of photon Received	Bits Received by Bob
+	H	LOST
x	A	LOST
x	A	1
+	H	0
+	V	1
x	A	LOST
x	D	LOST
+	H	0
x	A	1

Basics		0	1
Rectilinear Base	+	H	V
Diagonal Bases	x	D	A

Shared secret key = 10101

Fig. 4: Quantum Transmission

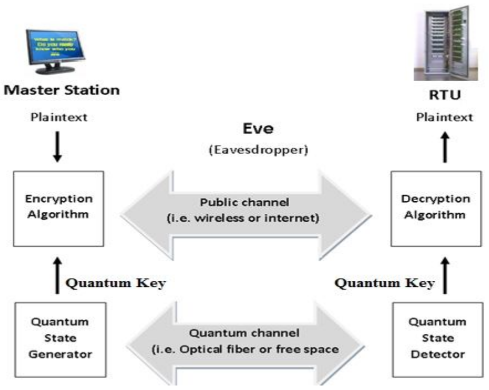


Fig. 5: Fiber QKD in SCADA Communication

6. Comparisoin of Classical and Quantum Cryptography (Cc V/S Qc)

Both Quantum and Classical cryptography can be compared on the basis of following points:

A. Passive eavesdropping- Classical Cryptography based on classical physics so there is open possibility of passive eavesdropping means private channel can be easily monitored inertly without the knowledge of sender or receiver but QC is based on quantum theory and follow the Heisenberg principle so sender or receiver can easily detect the eavesdropper.

B. Transmission Medium- Security of QC depends on transmission medium it requires quantum channel like optical fiber but in CC security depends on the computational complexity so communication medium is not an issue in CC.

C. Digital Signature- QC lacks digital signature feature which is very vital problem when information or key exchange is done through the shared network [7]. However this problem can be solved by Quantum digital signature is presented by author in [8].In case of CC digital signature is present.

D. Transmission distance- QC does not work over the long distance .it has not exceed

150 Km [7].However this problem can be solved using laser pulses instead of a single photon source[9].On the other hand CC can work over the long distance.

E. Life Expectancy- CC require a longer keys because computational power double in every 18 months and cost of computation is reducing rapidly with time [Moore law].Thus an algorithm using k bit key which is may not be secure in future i.e. it needs regular updating but in QC security depends on the basic principle of quantum mechanics so possibility of major changes requirement for future are almost negligible.

F. Implementation requirement- CC can be implemented on software and small hardware component like smartcard and it cost for consumer is almost negligible but in the case of QC it requires hardware is very expensive.

7. Conclusion

This paper shows that quantum cryptography is compatible with the SCADA communication (master station–RTU- RTU communication) providing strong security assurances rooted in the laws of physics without introducing excessive delays and latency in data delivery. A key advantage of the QKD is that it works quickly and eliminates the possibilities of somebody eavesdropping to hack the key which is required for SCADA system. From the comparison of CC and QC, it is clear that quantum cryptography is having more advantage over classical cryptography. Although some issue with quantum cryptography remains to be solved. This is mainly due to the implementation problem but in future one can expect most of the implementation problem to be solved.

References

[1] Dacfey Dzung, Mario Crevatin, “Security for Industrial Communication System,” IEEE Proceedings, 2005.

[2] R. L. Rivest, Dr. Ron “Rivest on the Difficulty of Fatoring,” Ciphertext:The RSA Newsletter, v.1, n.1, pp.6-8, fall 1993.

[3] K. Shaneman and S. Gray, “Optical Network Security:Technical Analysis of Fiber Tapping Mechanisms and Methods for detection and Prevention,” IEEE Military Communications Conference, 2004.

[4] C. H. Bennett and G. Brassard, “Quantum Cryptography: Public key distribution and coin tossing,” Proceedings of the IEEE International Conference on Computers, System and Signal processing, 175-179, 1984.

[5] A. Sharma, V. Ojha. and V. Goar, “Security Aspect of Quantum Key Distribution,” International Journal of Computer Application(IJCA), No.2, 2010.

[6] Wooters, W.K. and Zurek,W.H., “A Single Quantum Cannot be Cloned,” Nature, Nature Publishing Group, Vol.299, pp.802-803, 1982.

[7] Vignesh, R.S, Sudharssun, S., Kumar, K.J.J., “Limitations of Quantum and the Versatility of Classical Cryptography: A Comparative Study,” Second International Conference on Environmental and Computer Science (ICES), pp.333-337,2009.

[8] Lu, X., and Feng, D.-G., “Quantum Digital Signature Based on Quantum One-Way Function,” 7th International Conference on Advanced Communication Technology (ICACT’05), pp.514-517, 2005.

[9] Los Alamos National Laboratory, http://www.physorg.com/news86020679.html, 2006.

[10] Sharma, Murli Manohar, and Anju Bala. "Survey Paper on Workflow Scheduling Algorithms Used in Cloud Computing."