PROSPECTS OF FIBER QUANTUM KEY DISTRIBUTION TECHNOLOGY FOR POWER SYSTEMS

Ruirui ZHANG
China Electric Power Research Institute – China
zhangrr@epri.sgcc.com.cn

Xi CHEN
China Electric Power Research Institute – China
chenxi@epri.sgcc.com.cn

ABSTRACT

In this paper, we mainly explore the application of fiber Quantum Key Distribution (QKD) technology in Smart Grid. First, the vulnerability of optical fiber communication networks is analyzed. Second, an overview of fiber quantum key distribution technology is given. Third, typical fiber QKD use cases in Smart Grid are proposed. Finally, future research directions of fiber QKD for power systems are discussed. Compared to other classical cryptography technology, the application of fiber QKD in Smart Grid has unique advantages.

INTRODUCTION

With the gradual development and implementation of the Smart Grid, information technology (IT) and communications infrastructures have become more important to ensure the reliability and security of the electric power systems. Due to the increased dependence upon power system communications, the reliability and security of the IT systems and communications infrastructures must also be addressed. In China, during the 11th Five-Year-Plan period (2006-2010), high-speed and large-capacity optical fiber communication plays an important role in power system communication. The total optical fiber length has reached 6.554×10^5 km. At substation level, the fiber coverage rate of 220 kV substations and 110 kV substations has reached 100% and 92%, respectively. Typical utility applications carried over the optical communication network include: protective relay, Supervisory Control And Data Acquisition (SCADA), operations data, distribution automaton, distributed energy management and control, and smart metering, etc.

In recent years, optical fiber tapping technology has made rapid progress. Optical fiber communication exposes new vulnerabilities and its security is facing new challenges:

In 2000, three main trunk lines of Deutsche Telekom were breached at Frankfurt Airport in Germany [1].

In 2003, an illegal eavesdropping device was discovered hooked into Verizon's optical network [1].

In 2005, USS Jimmy Carter, submarine specifically retrofitted to conduct tapping into undersea cables [2].

Nowadays it takes equipment costing under €500, about 10 minutes for the tap installation and some persistence in finding the optical fiber in the right manhole [3].

Although using cryptographic technologies to provide security solutions in Smart Grid is proposed in NISTIR7628 (the foundation document for the architecture of the US Smart Grid) and IEC 62351 standards series, it's far from enough. First, fiber tapping problem is not discussed in these standards. Apparently, it is inadequate to only secure part of the communications performed on the widely deployed fibers, and fiber tapping problem should be considered. Second, it is difficult for the vendors to guarantee perfect implementation and thereby vulnerabilities are inevitable. For example, several vulnerabilities have been disclosed for Transport Layer Security (TLS), the security protocol used by IEC 62351, including Cipher Block Chaining (CBC) vulnerability in TLS 1.0, Man in the Middle (MitM) attack to TLS, and vulnerability in specific implementations. Third, classical cryptography mechanisms are based on mathematical concepts whose robustness is not proven. With the advent of new discoveries in cryptanalysis and new computing technologies (quantum computing, cloud computing, etc.), several of the cryptographic constructs underlying the security model of IPsec and TLS will be broken. For example, the famous signature algorithm SHA-1 has been broken by the team of Xiaoyun Wang in China. Finally, with transport layer encryption, it is difficult to achieve desired security level without compromising performance and cost. Embedded devices such as Protection & Control Intelligent Electronic Devices (IEDs) typically have little computational power, and changing or upgrading hardware is not an easy task. Therefore, it is impractical to adopt computing-intensive encryption technologies on IEDs. IEC 62351-6 suggested that all GOOSE/SMV communication between IEDs on the local area network (LAN) of a substation be digitally signed. Yet computing and verifying a digital signature on commodity hardware takes tens of milliseconds, while GOOSE messages have a latency requirement of at most 4 milliseconds [4].

Quantum Key Distribution (QKD) technology has been proposed as a method of achieving perfectly secure communications. Any eavesdropping attempt by a third party will necessarily introduce an abnormally high quantum bit error rate in a quantum transmission and thus be caught by the users. Compared to other classical cryptography technology, the application of QKD in Smart Grid has the following advantages:

(1) ***Unconditional Security*:** The security of QKD relies on quantum mechanics and can be proven mathematically without imposing any restrictions on the abilities of an eavesdropper, something not possible with classical key distribution. This is usually described as "unconditional security". QKD enables two communicating parties to securely generate and exchange shared random keys for data encryption, which can effectively protect against data interception.

(2) ***Versatility*:** A fiber QKD system can be used for multiple purposes. A smart self-healing grid depends on large amounts of health-monitoring sensors, which are required to have the following attributes:

passive, anti-electromagnetic, low attenuation, high sensitivity and long detect distance, etc. A fiber optic sensor is an ideal choice, since it inherently has the aforementioned attributes. Apart from cryptography function, a fiber QKD system can also function as a single-photon interferometer, creating a passive fiber sensor for various harsh environments.

(3) ***Cost-effectiveness*****:** Nowadays, one fiber QKD system is capable of supporting 10-Gb Ethernet traffic, which is important for low-cost implementation, reliability, and straightforward installation and maintenance [5]. QKD will be able to seamlessly integrate into Smart Grid information and communications infrastructures in the future.

In this paper, first, we analyze the vulnerability of optical fiber communication network and give a brief introduction to fiber tapping methods. Second, we give a brief overview of fiber QKD technology. Third, we propose several typical QKD use cases in Smart Grid. Finally, we present future research directions and conclude the paper.

VULNERABILITY OF OPTICAL FIBER COMMUNICATION NETWORKS

For years it has been public knowledge that optical fiber networks are inherently secure as the light transporting the data remains within the cable. This is a false belief. In fact, optical fibers can be intercepted with relative ease once they are accessed, and there is no inherent security for data travelling inside a fiber.

WDM networks can also be tapped as nothing prevents an eavesdropper from having the same equipment to demultiplex the signal as the intended recipient of the information. The vulnerability of optical fiber networks provides an opportunity for eavesdroppers to "sniff" the data, collect the data, and use the data at a later time for malicious purposes.

There are several ways to tap into an optical fiber including fiber bending, splitting, evanescent coupling, scattering, and V-grooves [6]. Fiber tapping can be intrusive and non-intrusive. The former requires the fiber to be cut and reconnected into the tapping mechanism while the later achieves tapping without cutting the fiber or causing any service disruption. Furthermore, mainstream network analyzers have the capability to capture and process traffic up to maximum bandwidth. Intercepted traffic can also be stored in bulk for offline analysis. An example of fiber bend tapping is as shown in Fig.1.

The most effective method for protecting sensitive data on the network against interception is through encryption. Employing the right encryption technology will ensure that performance is not sacrificed for security.

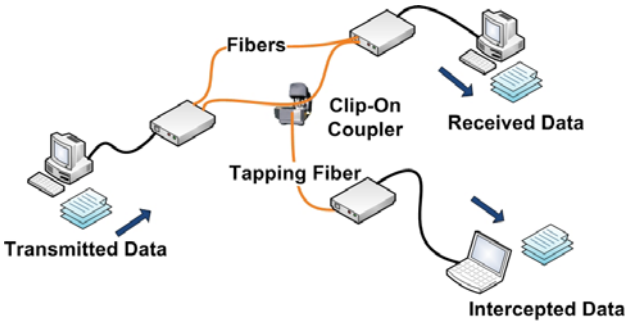

Fig.1 Fiber bend tapping

OVERVIEW OF FIBER QUANTUM KEY DISTRIBUTION TECHNOLOGY

Quantum Key Distribution, invented in 1984 by Charles Bennett and Gilles Brassard, is an unconditionally secure key distribution solution based on quantum mechanics [7]. QKD is secure against any attack, even in the future, irrespective of the computing power that may be used. The security of QKD relies on the fact that it is impossible to gain information about non-orthogonal quantum states without perturbing these states. This unique property can be used to establish a random key between two users, commonly called Alice and Bob, and guarantee that the key is perfectly secret to any third party eavesdropping on the line, commonly called Eve.

The fundamental component of a practical QKD system is QKD link. A QKD link is a point-to-point connection between two users, and consists of a quantum channel and a classical channel. The quantum channel allows quantum states to be transmitted, and in the case of photons it is generally either an optical fiber or free space. To establish a key, Alice generates a random stream of bits and encodes them into a sequence of non-orthogonal quantum states of light, sent over the quantum channel. Upon reception of those quantum states, Bob performs appropriate measurements leading him to share some bits correlated with Alice's bit stream. Alice and Bob then communicate over the classical channel to test these correlations. If the correlations are high enough, it implies that no significant eavesdropping has taken place on the quantum channel and thus a perfectly secure symmetric key can be distilled from the correlated bits shared by Alice and Bob. Otherwise, the key generation process has to be aborted and started again.

Since 1990's, multi-user fiber QKD networks have been extensively investigated in field environments. Examples include: DARPA Quantum Network, SECOQC QKD network, SwissQuantum QKD network, and Tokyo QKD Network. Most experiments and field tests have been performed on dark fibers. In the absence of data signals on the same fiber, secure key rates exceeding 1 Mb/s and a transmission distance of over 250 km have been achieved. As dark fiber is a scarce and expensive resource, there is a pressing need to enable QKD's coexistence with data signals on the same fiber.

In 2012, K. A. Patel *et al*. proposed such a cheap QKD solution [5]. They exploit a novel temporal-filtering effect for noise photon rejection. This allows high-bit-rate QKD over fibers up to 90 km in length and populated with error-free bidirectional Gb/s data communications. With a high-bit rate and range sufficient for important information infrastructures, such as smart cities and 10-Gbit Ethernet, QKD is a significant step closer toward wide-scale deployment in fiber networks.

TYPICAL QKD USE CASES IN SMART GRID

Substation communications

Since substations consist of critical entities of the utility infrastructure, they are a high priority target for malicious cyber attacks. Substations communicate with external networks such as remote monitoring systems, control centers, other substations and third party data networks. When the substation network opens up to the public network, a range of security concerns arises and therefore a dedicated security system is mandatory.

In this case QKD can be used: the control center and substations are inter-connected with QKD links which could be ADSS/OPGW installed along electrical transmission lines or other buried fibers. The cryptographic keys which are continuously generated and exchanged by the QKD links are fed into QKD link encryptors using a symmetrical block cipher (for example the Advanced Encryption Standard AES) or steam cipher (One Time Pad for highest security) for transparent traffic encryption on an Ethernet of fiber channel link.

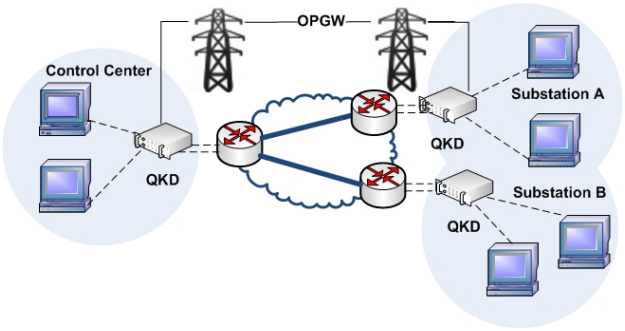

Fig.2 QKD use case: communications between a control center and its substations

It is also important to secure the communications between the master station and IEDs, as well as communications between IEDs. For example, information like open/close breaker orders or electrical measures for the grid global balance can be highly sensitive, and must be protected.

In this case QKD can be used similar to above use case. IEDs in the substations are grouped into sub-networks or LANs which are then connected to the mater station with QKD links. QKD link encryptors can ensure the master station-IED and IED-IED communications are secured.

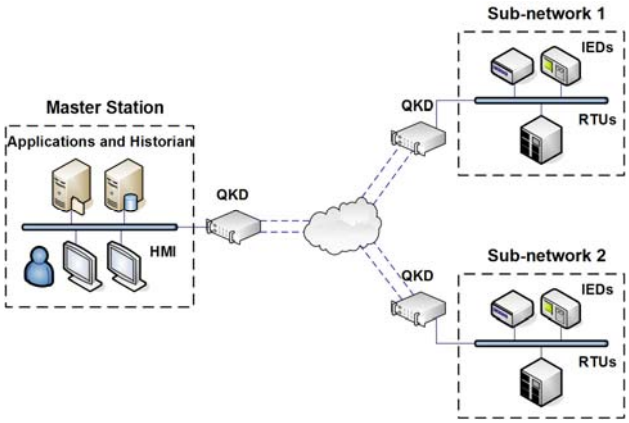

Fig.3 QKD use case: master station-IED and IED-IED communications

Smart metering optical network

Passive Optical Network (PON) is viewed as the next wave local access network technology for smart metering network. It can not only provide high band width, but also meet the low cost requirement of access networks. In the future, the fiber will get to IP meters or concentrators in the building. All communications in a PON are performed between an Optical Line Terminal (OLT) and Optical Network Units (ONUs). The OLT resides in the utility's master station while the ONUs are installed at the end users' locations. Passive optical couplers will be inserted at substations mainly and in street cabinets where needed. A PON uses only passive components and each ONU sees the entire downstream broadcasted from the OLT. Therefore, encryption must to be used to prevent eavesdropping of ONUs.

In this case, the same path which is used to relay the classical information from the OLT to the ONUs can be used to exchange quantum information. Through a system of synchronized clocks, the ONU and the OLT can identify corresponding measurements when distilling a mutual secret key. Continuous keys generation in a QKD enabled PON can mitigate the key revocation problem.

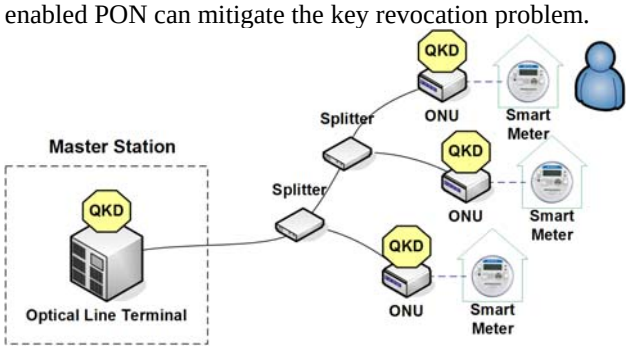

Fig.4 QKD use case: smart metering optical network

Fiber sensing

A quantum key distribution system can function as a single-photon interferometer creating a passive fiber sensor for harsh environments. The interferometer at the

receiver side of the system is able to actively track and reject vibrations to keep the phase match between the interferometers extremely precise. This technology can apply directly to seismic sensing in seismically active region, which help to provide better emergency preparedness for utilities and make power grids more resilient to natural disasters.

Disaster recovery center

Disaster recovery plays a critical role in ensuring the business continuity of the Smart Grid in case of disasters. As strict confidentiality of data is required, an encryption system is mandatory to secure the communications between the control center and disaster recovery center. In this case a QKD module can be used: the cryptographic keys shall be established and exchanged between the control center and disaster recovery center with a QKD link and fed into a link encryptor which uses a symmetrical block or steam cipher to encrypt traffic on an Ethernet of fiber channel link.

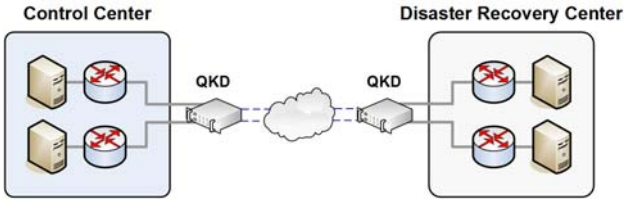

Fig.5 QKD use case: disaster recovery center

FUTURE RESEARCH DIRECTIONS

Practical QKD in power systems

Our future work will implement a fiber-based QKD system using decoy method for BB84 into power system communication. First, we will test the performance of the QKD system on different types of optical fibers (ADSS/OPGW used in overhead transmission lines and other buried fibers etc.) Secure key rate and transmission distance are two major performance indicators. Second, we will also test the performance of the aerial-fiber-based QKD system under various weather conditions, e.g., wind-induced cable motion, such as aeolian vibration, galloping, and wind sway. Third, we will realize the aforementioned QKD use cases. The final goal is to achieve an efficient and practical QKD system that can be easily integrated with the power systems.

Integration of QKD into IPsec/TLS

QKD can be integrated into existing security algorithms and protocols to secure communication networks. The Point-to-Point Protocol (PPP), IP Security protocol (IPsec) and Transport Layer Security (TLS) can support the use of QKD. These protocols are widely used. Integrating QKD into these protocols will highly affect the security level of the communications.

Fiber sensing network

Sensors will be critical for the construction of a Smart Grid. Currently available sensors are electronics-based and cannot operate due to blackouts. Apart from cryptography, the QKD technology can apply to sensing many physical parameters. Further improvements should allow future seamless expansion and integration with other power devices. In the future, QKD network will also function as a fiber sensing network.

Standardization

Although ETSI has started a universal QKD standardization initiative, there are no specialized design and performance specifications for the power industry. Moreover, some companies already offer off-the-shelf market products, which have proven their reliability in several demonstration projects and field tests. However, not all of these products are suitable for the power industry. Standardization of QKD for the power industry will be essential because system interoperability with existing infrastructures and applications as well as conformance with utilities' requirements have to be assured.

Acknowledgments

The work described in this paper has been jointly funded by State Grid Corporation of China and China Electric Power Research Institute.

REFERENCES

[1] S. K. Miller, 2006, "Hacking at the Speed of Light", *Security Solutions Magazine*

[2] S. K. Miller, 2006, "Optical Illusion", *Information security Issue*

[3] ID Quantique white paper, 2011, "Fiber optic networks: your weakest link?"

[4] S Fuloria, R Anderson, K McGrath, K Hansen, and F Alvarez, 2010, "The Protection of Substation Communications", *Proceedings of SCADA Security Scientific Symposium*

[5] K. A. Patel, J. F. Dynes, I. Choi, A.W. Sharpe, A. R. Dixon, Z. L. Yuan, R.V. Penty, and A. J. Shields, 2012, "Coexistence of High-Bit-Rate Quantum Key Distribution and Data on Optical Fiber", *Phys. Rev. X* 2, 041010

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

[7] C. H. Bennett and G. Brassard, 1984, "Quantum Cryptography: Public key distribution and coin tossing", *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, 175–179.