Optical and Acoustical Methods in Science and Technology 2013

A Quantum Key as the Fiber Optic Security Sensor

M. Życzkowski and M. Kowalski

Military University of Technology, Institute of Optoelectronics, S. Kaliskiego 2, 00-908 Warsaw, Poland

The paper describes the methodology of identifying an interference in the optical fiber. The paper presents the technology widely known as quantum key distribution. The quantum key distribution is based on the technique of constant comparison of quantum characteristics of the input light source and its characteristics at the end of the fiber optic. Methodology of presented work includes the evaluation of the functional objectives through the constructive assumptions for the laboratory models development. This paper presents the model of a system based on the comparison of polarization states of light quanta using two asymmetric Mach–Zender interferometers as transmitting and receiving systems to enable compensation of polarization state changes at the input and output of the fiber optics sensing cable. Continuous monitoring of the state of the reference signal, the specific changes of natural or ambient effects on the fiber will attempt to identify interference in the optical waveguide as a change of the polarization of the quantum states of the light. The authors indicate the possibility of using such fiber optic sensor as a security sensor to protect the extensive critical infrastructure facilities. In this article the future research conception of using compressed sensing algorithms for data compression in quantum key distribution systems is presented.

DOI: 10.12693/APhysPolA.124.606

PACS: 42.30.Sy, 02.60.−x, 42.30.Tz

1. Introduction

Due to the development of information technology, the amount of data sent over networks is constantly growing. Application of fiber-optic networks significantly improves the throughput of such links and ensure the stability of their work. Networks are frequently used to exchange classified data which requires to ensure the complete safety of transmitted data. However, there are methods that allow eavesdropping of information transmitted using optical fiber, thus the use of optical fiber is not as secure as many thought. Observing the trends and requirements of transmission lines, it appears necessary to consider telecommunication lines used for information transfer as hazardous. The need of maintain constant classified communication forces the need of protection of such lines and consider them as objects of critical infrastructure [1–3]. There are many well known applications of fiber optic sensors in large security objects of critical infrastructure [4–6]. However, the specific of the attacks, precision of performed attacks and the characteristics of the protected object forces a new look at the issue of protecting the telecommunication lines. Therefore, it is necessary to protect the transmission line or encrypt information transmitted via telecommunications lines.

In the process of encrypting the information, it is necessary to manage the problem of certainty and not eavesdropping of encryption key exchanged between sides. At this point, the world of sending classified data introduces the quantum key distribution (QKD) system.

2. Quantum key distribution system

The basics of operation of the quantum key distribution systems are the rules of quantum mechanics. These rules say that at the same moment in time any two polarization states cannot be measured because this measurement introduces disturbances of the polarization state of the photon [6].

Physical principles of QKD are indisputable, but in order to fully use the method advantages it is necessary to use appropriate algorithms that allow the secure key exchange. In 1984, two scientists Bennett and Brassard proposed the use of a key exchange protocol, later named after them, the BB84. Principle of operation [6] is based on the generation of two random bit strings by the sender, and then sending the encoded information about the strings by using polarized photon. The value of the bit in the first string defines the base polarity (straight or diagonal), the value of the bit in the second string specifies one of the two directions of polarization in a given polarization base. In the receiver module, the third sequence of bits is generated. Bit sequence of the sender determines the polarization base used to measure polarization state of received photon. If the base of the sender and receiver are consistent, the measurement of polarization state is correct. If the bases are inconsistent, readout of the correct value occurs with a probability of 50%.

In the next step, polarization bases used to read data between receiver and the sender are transmitted in public channel. Then the information with specific states of polarization bases for which senders and receivers are compatible are sent. Values read in the case of identical bases are a shared encryption key, for validation of the correctness of transmission and readout, a small part of the key is sent and compared between both sides.

A majority of the world's QKD systems work according to the methodology presented above. Systems are built as two separate units connected together with classic telecommunication fiber. Due to the difficulties in the transmission of polarization using optical fibers, in the real systems the phase shift is used instead of polarization. In the classic system [6] the light passes through the optical fiber connector only once and in this case it is necessary to use the system of polarization restoring. However, the systems with auto compensation are also

common. In these systems, light is propagating in two ways inside the transmission fiber. Because of this, the effects of fiber on the propagating radiation are compensated.

In QKD systems, eavesdropping or lack of it is determined by the quantum bit error rate QBER. This parameter allows to specify the normal operating conditions of the system during operation. Disturbance of the system by attempting to eavesdrop leads to growth of QBER, due to the fact that this is a statistical parameter of error during time, the response of the interference of the fiber comes with delay.

Despite the delays, it ensures the threat detection and ability to take appropriate action. However braking the QKD system without the violation of basic principles of quantum mechanics is impossible, imperfection of equipment used for the construction of these systems makes them vulnerable to eavesdropping. This implies the reduction of the safety and security of the data exchanged as confirmed during the research [7–11].

3. Conceptions of use of QKD as a sensor in telecommunication fibers

The authors believe that QKD systems are the future of the exchange of classified information with simultaneous detection of potential interference in the transmission channel. Hence, there is an idea to use quantum key distribution systems as sensors to protect and enhance the safety of transmission lines used by the system.

QKD system with some simplifications can be used as a sensor in the telecommunication line. Principles of operation of QKD based on single-photon transmission remain unchanged, but the system itself has a number of simplifications. The first simplification is the ability to override an independent generation of the random parameter, since in this case there is no need to determine and exchange the key.

This can be replaced with random or pre-determined parameter changes of the transmitted photons, and at the same time set the analyzer in accordance with the transmitted parameters. Knowledge of which analyzer to use at the specific time will condition proper detection. This solution would eliminate the errors associated with non-compliance analyzers used during reading, and reduce the value of QBER. However, any attempts to eavesdrop the channel lead to a significant increase of the detection rate of interference. This increases the response time to the attempts of intervention in the lines, and reduce the risk of undisclosed eavesdropping. Although this would not provide to complete elimination of QKD cheating systems.

Another solution to provide greater security is to add the optical fiber sensors to the QKD system, by using wavelength division multiplexing. The optical fiber sensors function is to protect the integrity of the transmission line. An example of a system developed by the article author is presented in Fig. 1.

The optical sensor for monitoring the integrity of the optical fiber developed by authors is based on optical

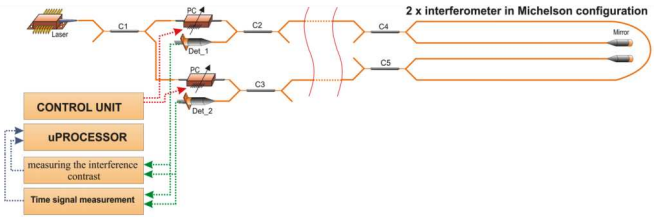

Fig. 1. Mechanical disturbance sensor for protection of telecommunication lines.

fiber Michelson interferometer in double configuration. The system can be divided into two parts: 1. the left side are the optoelectronic transmitting and receiving units with signal processing units, 2. the right side is the optical fiber sensor consisting of two couplers and segments of single-mode fiber.

In detailed description, the sensor consists of insensitive area for couplers C4 and C5 and proper part of the sensor consisting of four double-sided arms of interferometer. By using two-way power supply system we obtain exactly two interferometer systems. Both interferometers are subjected to the same environmental conditions and are affected equally to any inputs. They differ only in the opposite direction of light propagation. In the first case, the light is transmitted in the direction of: laser $\rightarrow$ C1 $\rightarrow$ PC $\rightarrow$ C2 $\rightarrow$ C4 $\rightarrow$ mirror $\rightarrow$ C4 $\rightarrow$ C2 (and laser $\rightarrow$ C1 $\rightarrow$ PC $\rightarrow$ C3 $\rightarrow$ C5 $\rightarrow$ C4 $\rightarrow$ C2) $\rightarrow$ det1. In the second case, the direction of transmission is following: laser $\rightarrow$ C1 $\rightarrow$ PC $\rightarrow$ C3 $\rightarrow$ C5 $\rightarrow$ mirror $\rightarrow$ C5 $\rightarrow$ C3 (and laser $\rightarrow$ C1 $\rightarrow$ PC $\rightarrow$ C2 $\rightarrow$ C4 $\rightarrow$ C5 $\rightarrow$ C3) $\rightarrow$ det2.

According to the well-known relationships describing the result of the interference of light in this type of system, it depends on the intensity of light in the two arms of interferometer and the phase difference between the two arms. The light intensity is dependent on the distribution of light on the couplers C4, C5 and the traveled distance (in our case the distances are different) over a fiber between C3 and C5 (on the assumption it will be several kilometers). The phase difference in the interferometer systems determines whether the beams interfere constructively or destructively. This determines at which point of characteristic the system is operating. Constant phase difference in system is affected by constant phase shift in the fiber couplers and the state of unbalance of fiber lengths belonging to the arms of the interferometer. In both cases (interferometers), the states will be the same. The length difference of the optical paths in arms of interferometer also determines whether there would be interference in the system. In principle, it cannot be greater than the coherence path of the used light source. In the practical arrangements of long distance fiber the difference of length of interferometer arms is at the level of 1 m. This is mainly due to the method of determining the length of the optical fiber. We used the OTDR (fiber length and attenuation meter) which determines

the length of fiber with a resolution of 0.25 m in a 40 km.

Discussing the system operation, it is justified to present the performance in perfect and stable environmental conditions. We made an assumption that there is no environmental impact on the arms of the interferometer, under both temperature changes and mechanical movements, which have direct impact on the polarization of the light propagating in the fiber. We also have in mind the balance of the optical path of the interferometer. Under ideal conditions, the determined operating point is dependent on: — optical path difference, — introduction of constant phase shift by the couplers, — wavelength of radiation propagating in the system.

Assuming that the laser beam has a constant output power (without own fluctuations), the products of each of the interferometers (from coupler C4/C5) have constant level of power and constant phases dependent on a fixed operating point, so the signal obtained by a detector has a constant level.

However, if we add a mechanical disturbance to an ideal system (we still have no temperature fluctuations and polarization — ideal conditions), then by changing the angle of deflection of the fiber core, the length of the propagation of light in given arm changes. Deposition of the two waves results in constructive or destructive interference at a given operation point of the system. The detectors register signals after a short period of time (the period of interference fringes depends on the impact strength on the fiber, specifically from the optical path difference).

One can notice the deflections in the continuous signal from the detectors which are an evidence of the mechanical impact. According to the results of recent investigations, signals of disorders are strongly connected with the transfer function of the interferometer and are not directly identifiable as "microphone" signals. For a continuous monitoring of the optical fiber cable (i.e. hear mechanical undistorted vibration) one should try to demodulate the signal. Investigation results confirm that: — interferometric sensor is a highly sensitive microphone and can recognize human voice, — bandwidth of such system is practically unlimited in the frequency of the mechanical range (from single Hz to 25–30 kHz), — transmitted changes caused by acoustic/mechanical disorders of fiber have frequencies in the frequency range up to 500 Hz and the duration from several up to hundreds milliseconds, — circulation of light in fiber-optic interferometer takes μs (5 μs per 1 km of fiber).

Taking into account the impact of external conditions on the arms of the interferometer as well as changes in the operation of active devices, the change of the optical path of interferometer arms is caused by: temperature, fibers stress, position, ambient vibrations, and polarization of light. In addition, we talk about the changes in the operation point of the system as a result of tuning of the laser under the influence of e.g. temperature. This automatically translates into changes of the sensor system operating conditions. At the output of the interferometer (detectors) one can notice the interference fringes fluctuating with low frequency. These phenomena can negatively affect the operation of the sensor system and should be minimized or corrected.

The authors propose to use continuous and constant modulation of the laser wavelength to determine the interference contrast. Any change in contrast refers to the changes of polarization in the fiber. Through constant observation of changes in the amplitude of modulated signal we can determine the status, and we can see each detuning from the maximum state.

Frequency range of changes (modulation) cannot coincide with the expected disturbance signals detected by the sensor, and should be contained within the response characteristics of the system. We expect the acousto-mechanical signals with the frequency range of 0–30 kHz. Permanent nature of the changes must be shifted from that range to not to cause a malfunction. There should be introduced technical reactions to these changes in order to tune the system to work at maximum interference contrast polarity, i.e. with two identical beams polarization. Describing it simply, if the contrast falls below unity (maximum) it is necessary to make such changes in polarization interfering beams (via polarization controllers in the feedback loop) to bring the system to work in conditions of maximum interference contrast. With such procedure, changes of polarity sensor system becomes stabilized thermally and dynamically responds to changes in polarization, forced by slow changing of environmental factors. In the case of mechanical problems related to the intentional interference with fiber optic circuit, the contrast changes occur rapidly.

On this basis, it is possible to specify the alarm. Also, for this configuration the sensor can determine the occurrence of disturbances in many kilometers of fiber optic line. Since the occurrence of disorder in one of the arms of the interferometer, the signals of change of the interference products from the two detectors of the two interferometers appear at different times (t_1 and t_2). Due to the nature of light propagation in the fiber (5 μs at 1 km), the two detectors signals will differ naturally over time. Comparing these two times, one can estimate the location of a disturbance. For the optical path of 80 km, the maximum time difference in distributing the information about disturbance to the detectors is 266 μs.

As a result of using this solution, the safety of secure key transmission in a QKD system by providing detection of any interference in the transmission fiber can be achieved. The sensor would provide information about the attempt of breach and the location of such a disorder. It is possible to check whether the eavesdropping of QKD system is installed in the transmission line [8]. However it is essential that all the elements of the transmission line need to be inside the protected area and should be prevented from getting a third party to the transmission and protection system components. The example of QKD system for protection of telecommunication line is presented in Fig. 2.

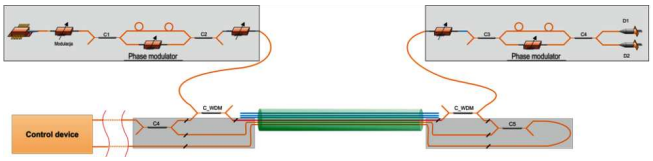

Fig. 2. Integration of the QKD with system of telecommunication lines protection.

4. Future research

The technology of quantum key distribution is in its early stage of development, thus the world of science need to face large number of issues. One of the most urgent problem of quantum key distribution technology is low transmission rate. This problem needs to be solved to increase the popularity of this technology. The data compression can be a possible solution of the issue. We propose a novel solution of compressing and encoding the quantum key by implementing the compressed sensing [12] algorithms to compress and encrypt the transmitted quantum key.

Compressed sensing is a signal processing method based on the fact that an undersampled sparse signal can be reconstructed from a small number of measurements. Quantum keys can be considered as bit sequences thus they fully satisfy all the conditions needed to use compressed sensing. The compressed sensing (CS) method shows that a signal can be compressed and still contains all useful information [13, 14]. The compression means that the quantum key includes much less information than the traditional one. The CS method is also an encryption method of data, thus the transmission is even more secure.

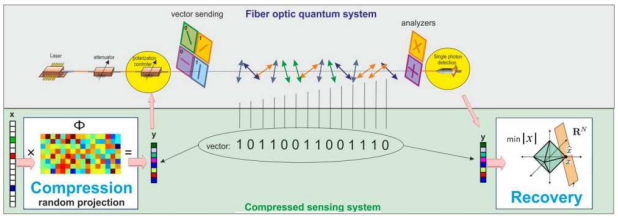

Fig. 3. A conception of CS based fiber optic quantum system.

The theory of compressed sensing was basically described in [12]. Suppose we have available undersampled data about x of the following form (1):

$$y = \Phi x. \tag{1}$$

One would recover x by finding — among all coefficient sequences consistent with the data — the decomposition with minimum ℓ_1-norm [1] (2):

$$\min \|\tilde{x}\|_{\ell_1} \quad \text{such that} \quad \Phi' \tilde{x} = y. \tag{2}$$

From an application point of view, the ℓ_1-norm minimization can be achieved using e.g. a conjugate gradient algorithm or gradient projection method [14].

The conception of the fiber optic quantum system with implemented compressed sensing compression algorithm is presented in Fig. 3. The conception assumes that before transmission, a quantum key is compressed using CS algorithm. The compressed and encrypted key is transmitted to the receiver and then recovered and decrypted with pre-defined parameters. It is expected to achieve compression factor up to 50%.

5. Conclusions

We believe that using the appropriate security methods and using the QKD systems will soon become the standard for the transmission of classified information. The entire system still requires improvements in the level of components technology, which are critical points of transmission security. However, using additional security elements and putting constant efforts on manufacturers to ensure the safety of the system, gives this technology great potential for development in the future. The authors claim that in a few years perspective, it is possible to manufacture the alarm components based on a certain data exchange using QKD technology in optical fiber signal transmission lines based on TCP/IP protocol. Because of low transmission rates in QKD systems, authors proposed a solution based on the compressed sensing method. This solution uses compressed sensing algorithms for data compression and additional encryption.

Acknowledgments

The project is co-financed by the National Centre for Research and Development within the project realized for national security and defence (contract no. DOBR/0070/R/ID1/202/03).

References

[1] M. Kondrat, M. Szustakowski, N. Pałka, W. Ciurapiński, M. Życzkowski, *Opto-Electron. Rev.* **15**, 127 (2007).

[2] T. Pustelny, K. Barczak, K. Gut, J. Wojcik, *Opt. Appl.* **34**, 531 (2004).

[3] M. Życzkowski, M. Kondrat, W. Ciurapinski, *J. Phys. IV (France)* **129**, 189 (2005).

[4] M. Szustakowski, M. Chojnacki, M. Życzkowski, N. Pałka, *Opto-Electron. Rev.* **9**, 413 (2001).

[5] K. Barczak, *Bull. Pol. Acad. Sci., Techn. Sci.* **59**, 4009 (2011).

[6] L. Lydersen, J. Skaar, *Quant. Inform. Comput.* **10**, 1 (2010).

[7] K. Gut, *Acta Phys. Pol. A* **114**, A121 (2008).

[8] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, V. Makarov, *Nature Photon.* **4**, 10 (2010).

[9] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, V. Makarov, *Nature Photon.* **4**, 801 (2010).

[10] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, V. Makarov, *Opt. Expr.* **18**, 26 (2010).

[11] Ø. Marøy, L. Lydersen, J. Skaar, *Phys. Rev. A* **82**, 3 (2010).

[12] D. Donoho, *IEEE Trans. Inform. Theory* **52**, 1289 (2006).

[13] E. Candés, M. Wakin, S. Boyd, *J. Fourier Anal. Appl.* **14**, 877 (2008).

[14] J. Romberg, *J. Imaging Sci.* **2**, 1098 (2009).