Opto-Electronics Review 26 (2018) 183–187

Contents lists available at ScienceDirect

Opto-Electronics Review

journal homepage: http://www.journals.elsevier.com/opto-electronics review

Pulsed interferometric optical fibre sensor detecting wiretapping in long transmission lines

M. Życzkowski*, M. Karol

Military University of Technology, Institute of Optoelectronics, 2 Urbanowicza Str., 00-908 Warsaw, Poland

ARTICLE INFO

Article history:
Received 14 November 2017
Received in revised form 4 April 2018
Accepted 16 April 2018
Available online 26 May 2018

Keywords:
Optical fibre sensors
Mach-Zehnder interferometer
Quantum sensors

ABSTRACT

A modified optical fibre based Mach-Zehnder interferometer was applied as a sensor to detect wiretapping in long transmission optical fibre lines. The signal consisting of short pulses (around 1 ns) was launched to the input of the interferometer based on the polarization maintaining fibres and polarization elements. When the sensing line was undisturbed, detectors registered only a single pulse. The additional two side pulses appear, if the wiretapping attempt took place. For robust detection of any alarm situation we proposed two-criteria algorithm to minimize false alarm rate. Moreover, slow environmental fluctuations were continuously monitored and compensated by polarization controllers. We measured frequency characteristics of the sensor and performed a hundred wiretapping attempts, which proved high performance of the sensor.

1. Introduction

Protection of optical fibre lines which transmit sensitive confidential information is a crucial factor for national and civil security. Detection of an illegal wiretapping attempts by means of a clip-on coupler requires continuous monitoring of the transmission line. One or a few fibres from the optical cable can be used as a sensor, which detects not only any movement of the cable but also indicates the position of the attempt point along a multi-kilometre long line.

Commercially available optical fibre sensors [1–3] used to protect transmission lines can be divided into two basic groups: interferometric [4] and scattering [5]. Interferometric sensors are usually based on the Mach-Zehnder setup, which is fed from two sides. Although this configuration is very sensitive, it suffers from high false alarm rate (FAR), because only one criterion can be utilized as an alarm threshold. On the other hand, the Brillouin scattering sensors are less sensitive to considered wiretapping attempts. Both sensors can indicate the attempt point with resolution of about 25 m over the 40-km line [6].

On the other side, the security of transmission is currently being implemented in higher layers of the ISO Open Systems Interconnection Reference Model [7]. This standard includes symmetric or asymmetric encryption of data. In order to enhance data security, it is possible to define a non-standard way of exchanging data in the physical layer of the model. As far as the exchange of optical data in telecommunication optical fibre systems is concerned, it should be underlined that such a process has started with the use of a quantum key distribution (QKD) [8–11].

Briefly, QKD uses a single-photon secure exchange of optical bits, where security of information is hidden in the photon polarization or phase state [12]. Any photon tapping attempt simultaneously changes its state which results in alarm. The main limitation of current QKD systems is connected with imperfections of optoelectronic components, especially single-photon detectors.

In this work, a modified optical fibre based Mach-Zehnder interferometer was merged with the QKD-based configuration in order to enhance detection of the considered attempts and keep the false alarm rate on the low level. The interferometer was in an auto-compensating configuration with short pulses at the input instead of single photons to avoid the mentioned problems with detectors. Any disturbance of the line caused change of the signals at two detectors. Moreover, slow environmental fluctuations were continuously monitored and compensated by the polarization controller to get high interferometric contrast. Relatively fast wiretapping attempts were detected by means of the proposed two-criteria algorithm, which independently used amplitudes of the pulses. The main goal of the presented research was to prove, that the considered sensor can detect any attempt of wiretapping by the clip-on coupler. Best of our knowledge, it is the first time when the proposed arrangement was applied.

* Corresponding author.
E-mail address: marek.zyczkowski@wat.edu.pl (M. Życzkowski).

https://doi.org/10.1016/j.opelre.2018.04.003

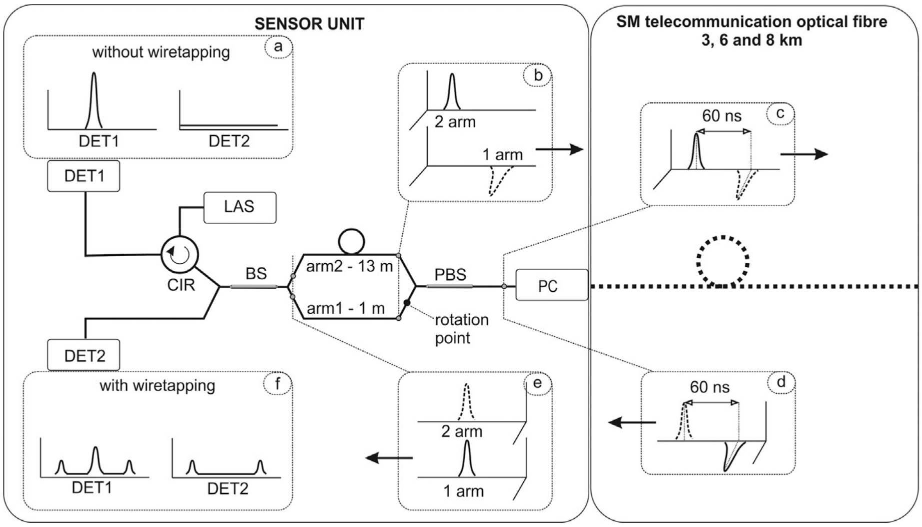

Fig. 1. The scheme of the designed sensor, where DET1 and DET2 are detectors, LAS is the pulsed laser source (1-ns pulse duration time), CIR is the circulator, BS is the beam-splitter, PBS is the polarization beam-splitter, PC denotes the polarisation controller and MIR the silver mirror at the end of the telecommunication optical fibre.

2. Description of the sensor

The proposed setup (Fig. 1) consisted of the sensor unit and a standard single mode optical fibre terminated with a mirror. The sensor unit was a modified version of the classic optical fibre based Mach–Zehnder interferometer (M-ZI) using PANDA polarization maintaining (PM) optical fibre. The setup was fed by the 1.55 μm stabilized pulsed laser (LAS) with the 1-ns pulse duration. Let's assume that the initial polarization of the pulses was vertical and the electric field vector ($\vec{E}$) was parallel to the ordinary axis of the PM fibre. The circulator (CIR) separated the laser from the radiation coming back from the setup, which stabilized laser's operation.

The beam splitter (BS) distributed the pulses generated by the laser into arm1 and arm2 of M-ZI, which had lengths equal to 1 m and 13 m, respectively. The 12-m difference in arm's lengths provided the separation of the pulses equal to 60 ns (Fig. 1c). The PM fibre in arm1 was rotated by 90° and spliced, which caused that $\vec{E}$ became perpendicular to the ordinary axis of PM fibre. As a result, the polarization beam splitter (PBS) combined two separated in time pulses with perpendicular polarizations (Fig. 1b, c), which could not interfere – M-ZI did not work for forward propagating pulses.

The polarization controller (PC) was connected to a multi-kilometre long single-mode (1.55 μm) telecommunication optical fibre (SM). The fibre was terminated with a silver mirror with reflectance 98%@1550 nm (MIR). Two pulses propagating in the SM fibre (Fig. 1c) reflected back and reached the PC. PC changed their polarization state (Fig. 1d) in such a way, that faster pulse had vertical polarization and went through the longer arm2, while the slower horizontal pulse propagated through the shorter arm1, which additionally rotated its polarization to the vertical one. Finally, at BS both pulses had the same arrival time and vertical polarization (Fig. 1e) and thus could interfere.

Therefore, optical fibres denoted as arm1 and arm2 created M-ZI but only for the returning pulses. In case, where the SM fibre used for sensing was not disturbed and the sensor was ideally stable, we obtained a single pulse only at DET1 (Fig. 1a) which was connected with a phase-dependent operation of M-ZI. When a relatively fast wiretapping-like disturbance was applied to the sensing fibre, it introduced a fast random change of polarization of the propagating pulses. Part of the pulses' energy leaked to perpendicular states which disrupted the interference conditions. As a result, the single pulse at DET1 was lower and side pulses at both detectors appeared (Fig. 1f). The wiretapping attempts were next detected by means of a two-criteria algorithm, which independently analysed amplitudes of both pulses.

The sensing fibre was naturally exposed to slow-changing fluctuations connected with environmental conditions. PC continuously corrected the polarization state of the pulses entering M-ZI to ensure maximum power of the single pulse. It must be noted that in the sensing SM fibre polarization state of the pulses changed during propagation in the unknown way, what was inherently connected with its non-polarization maintaining behaviour. Therefore, proper operation of PC was crucial for the effective performance of the sensor.

3. Experimental setup

The sensor unit (Fig. 2) was fed by the 1.55 μm pulsed laser (LAS) PicoQuant LDH-D-C-1550 stabilized with the Peltier cooler.

Pulse duration could be adjusted in the range of 0.1–5 ns; the spectral width was 30 nm. The sensor consisted of two InGaAs detectors (Tektronix P6703B) with a rise time of about 400 ps (denoted as DET1, DET2) which provided proper registering conditions.

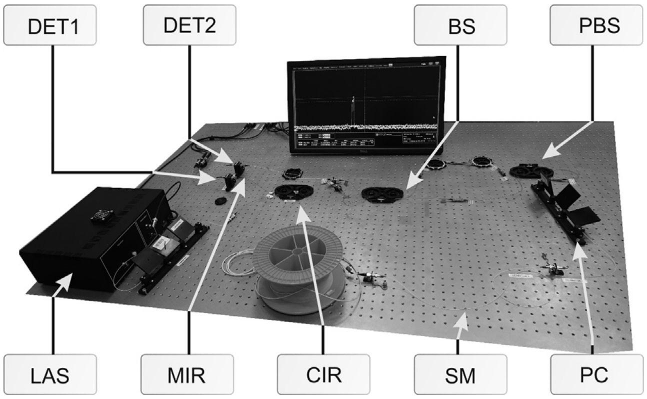

Fig. 2. Laboratory experimental setup, where DET1 and DET2 are detectors, LAS is the 1.55 μm pulsed laser source (1-ns pulse duration time), CIR is the circulator, BS is a beam-splitter, PBS is a polarization beam-splitter, PC denotes a polarisation controller, MIR the silver mirror (reflectance 98% @ 1550 nm) at the end of the telecommunication optical fibre and SM is the single mode sensing fibre.

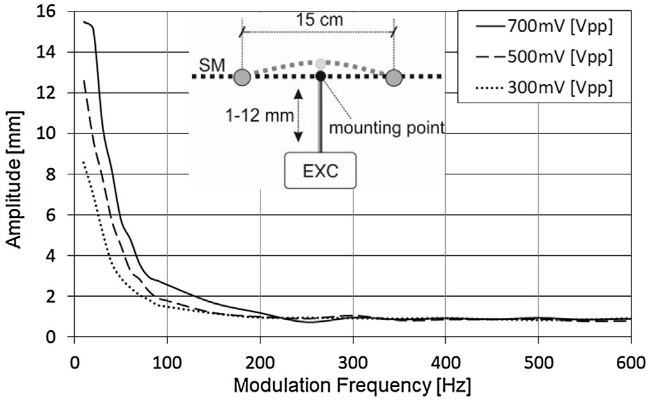

Fig. 3. Frequency characteristics and scheme (inset) of the modulation introduced by the exciter.

All components of the sensor unit were based on the PANDA polarization maintaining (PM) optical fibre (SM15-PS-U25A). The circulator CIR-SM-PIPE-1550, the beam splitter SPL-SM-PIPE-2 × 2 and the polarization beam splitter PBS-1 × 2–1550 were used, all delivered by Cellco. The setup was tested with three lengths of the sensing SM fibre – 3, 6, and 8 km.

Real wire-tapping attempts were performed by means of the Clip-On Coupler FOD 5503, which provided non-invasive bi-directional coupling into 250 μm coated SM fibres. For frequency characteristics measurements, we applied an electro-dynamic exciter (EXC) – Smart Shaker K2007E01 by Modal Shop. It provided movement of the 15-cm section of the sensing fibre with an amplitude in the range of 1–15 mm with the modulation frequency adjustable in the range 5–700 Hz. Figure 3 shows frequency characteristic of the modulation applied by the exciter.

4. Experimental results

First, we carried out research on frequency characteristic of the sensor with use of the exciter, which provided useful information on the frequency sensitivity. Next, we tested sensor's performance with real wiretapping attempts by means of the clip-on coupler.

4.1. *Frequency characteristics of the sensor*

Figure 4 presents signals at the detectors both for the undisturbed and "exciter on" case. In the first case we observe a single main pulse with power of about 76 μW (P_1) only at DET1. The noise level for both detectors was equal to about 2 μW. Introducing the exciter decreased the main pulse power at DET1 to 60 μW. Moreover, two symmetrical side pulses with power of about 4 μW appeared at both sides of the main pulse. Time difference between the main and side pulses was 60 ns and was connected with time separation in M-ZI. DET2 registered two side pulses with amplitude of about 10 μW (P_2). Time difference between these pulses was 120 ns.

Since the visibility depended on the amplitude of the exciter, we defined the relative sensitivity (*RS*) as the visibility divided by the amplitude of the exciter. Figure 5 shows, that RS decreased with the increase of the modulation frequency, which was connected with the drooping exciter's characteristics (Fig. 3). Some minima (e.g. at 60 Hz) were probably connected with mechanical resonances of the exciter. RS reached the highest values in the 10–30 Hz range while in the range 60–600 Hz it oscillated near 0.4.

Figure 6 presents the power P_1 as a function of time without modulation and for modulation with frequency of 8 Hz and amplitude of 15 mm. The length of the sensing fibre was 3 km. One can notice that P_1 oscillated according to the modulation of the exciter.

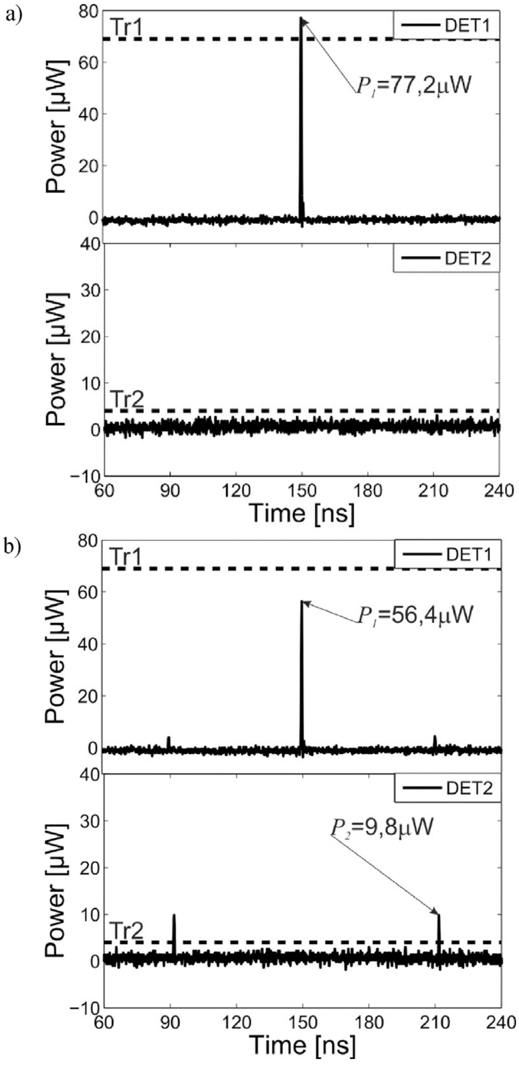

Fig. 4. Signals at detectors for: undisturbed setup (a) and "exciter-on" (b). Tr1 and Tr2 denotes threshold levels indicating if the wiretapping occurred or not.

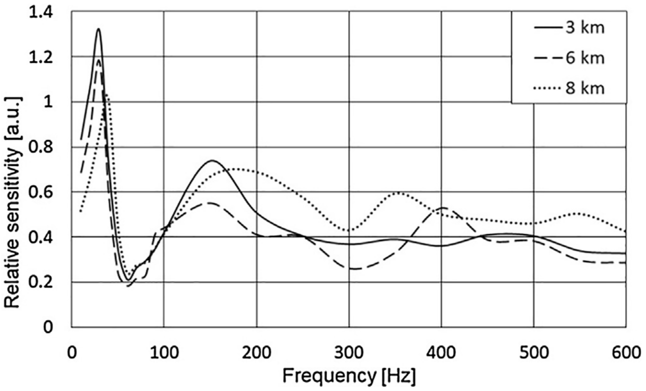

Fig. 5. Relative sensitivity (defined as the visibility divided by the amplitude of exciter) of the sensor for three different lengths of the sensing fibre.

It was observed, that when a short section of the sensing fibre was disturbed, the resultant change of the polarization was small and reversible – mean value of P_1 was constant.

Basing on Fig. 6, we defined the visibility $V = (P_{1\max} - P_{1\min})/(P_{1\max} + P_{1\min})$. For the undisturbed sensor V was around 0.04. For modulation frequency 10 Hz, the visibility linearly

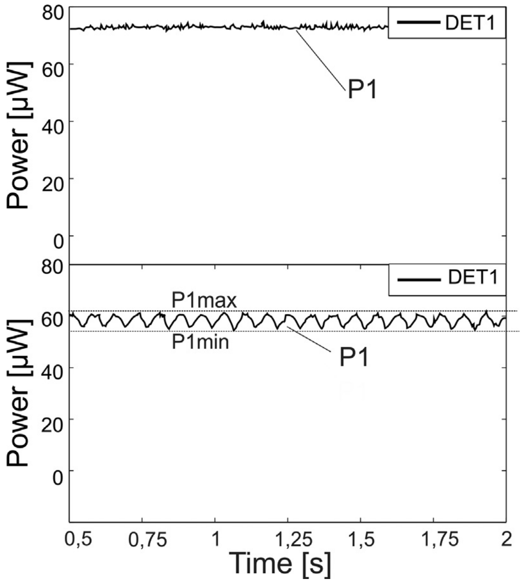

Fig. 6. Power P_1 as a function of time: without modulation (a) and with 8 Hz modulation with 15-mm amplitude (b).

Table 1
Average setup sensitivity vs. length of the sensing fibre.

Sensing fibre length	Average sensitivity [a.u.]	
	10 Hz–30 Hz	60 Hz–600 Hz
3 km	1.08 ± 0.03	0.39 ± 0.19
6 km	0.92 ± 0.08	0.36 ± 0.17
8 km	0.68 ± 0.03	0.46 ± 0.16

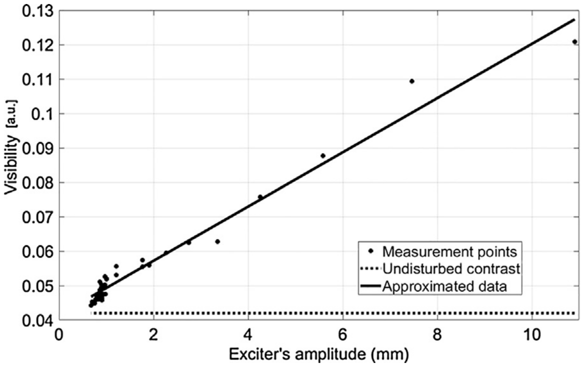

Fig. 7. Visibility of fringe pattern corresponding to the power modulation at DET1 caused by the introduced exciter as a function of the exciter's amplitude.

increased with the increase of the exciter amplitude up to $V = 0.12$ (Fig. 6).

Table 1 summarizes RS values for both frequency ranges vs. lengths of the sensing fibre. It can be concluded that the developed sensor will be sensitive for the real attempt of the wiretapping, because the majority of the tapping-related movement of the fibre lies in the low-frequency range (Fig. 7).

4.2. Detection of wiretapping attempts

The second part of the sensor's tests was based on the wiretapping attempts by use of the clip-on coupler. In comparison to the exciter's measurements, the application of the coupler caused larger disturbances of the fibre which resulted in bigger change of the polarization of the propagating pulses (Fig. 8). More power leaked to the side pulses and the main pulse dropped to about half of its undisturbed state (Fig. 4a).

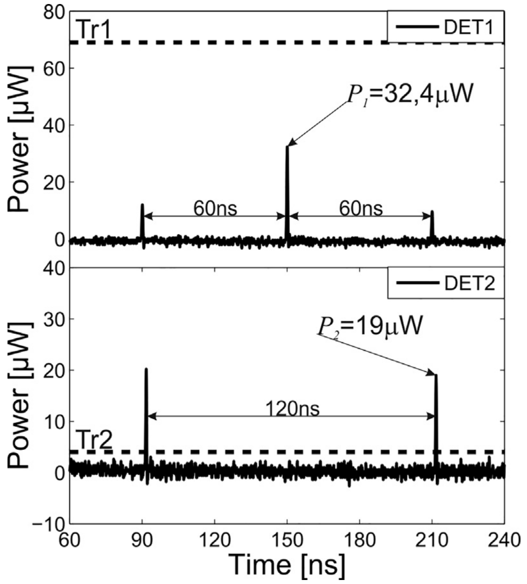

Fig. 8. Signal registered at detectors for the wiretapping attempt. Tr1 and Tr2 denotes threshold levels indicating if the wiretapping occurred or not.

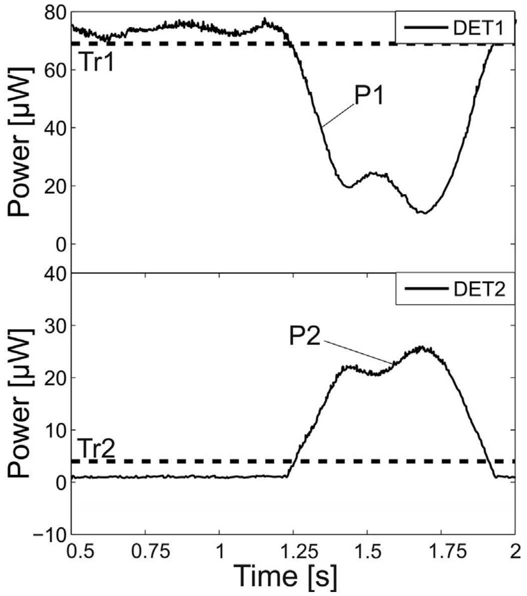

Fig. 9. P_1 and P_2 during insertion of the clip-on coupler. Tr1 and Tr2 denotes threshold levels equal to 90% and 5% of maximal value of signal P_1, respectively.

Figure 9 presents power P_1 and P_2 registered at DET1 and DET2, respectively, during insertion of the coupler. Small changes of the signal power P_1 related to the final part of inserting the fibre inside clip-on coupler are visible up to the time of 1.25 s. Next half of a second corresponds to the real insertion of the coupler into the fibre, which means bending the optical fibre and setting to the prism, which can be seen as significant decrease of the power P_1 and increase of the power P_2. The time between 1.7 and 1.9 s corresponds to switching off the coupler. It can be seen that both power values tend to be similar to the initial ones and only sometimes they must be optimized by the use of PC. It should be underlined that the fact that after introducing the coupler the system is coming back to its initial state is the biggest disadvantage and obstacle in detecting the wiretapping of the fibre. After inserting into fibre, this device in such short time is still not noticeable for all known methods of monitoring. Therefore, introducing two-criterion method of determining the alarm level assures more reliable detection of the wiretapping attempt.

It was experimentally proven, that in the undisturbed case, the main pulse power P_1 was stable and its slow environmental fluctuations oscillated in the range of a few percent and were easily compensated by PC. To increase the probability of detecting wiretapping attempt and to lower the false alarm rate, we developed the two-criteria algorithm, which considered two experimentally determined thresholds Tr1 and Tr2 applied to DET1 and DET2, respectively. Tr1 was equal to 90% of P_1, while Tr2 was equal to 5% of P_1. In the presented case $P_1 = 77\,\mu W$, Tr1 = 69 μW and Tr2 = 4 μW. Depending on the requirements, the system generates the alarm either when only one of the thresholds was exceeded (logic "or") or when both of them were surpassed (logic "and").

During tests, we inserted the coupler in various points of the three sensing fibres. For 100 attempts we obtained 100% of effectiveness in detecting the wiretapping. The average power drop of the main pulse (P_1) was equal to $27 \pm 9\,\mu W$, while the average power of the side pulses (P_2) increased up to $21 \pm 5\,\mu W$. After each attempt, the proper polarization state of the pulses was restored by means of PC. Similar research was carried out during cutting the optical fibre resulting in uncovering the single fibre. It was very arduous task and therefore in our experimental verification only few such attempts were carried out. Nevertheless, it should be underlined that just first seconds of such operation resulted in exceeding both criteria (threshold values) and setting the alarm.

5. Conclusions

The conducted studies show that the setup can be used as an element of optical fibre transmission line protection. In comparison to conventional optical transmission systems, the protection against wiretapping of the transmission line by the present sensor setup requires less complicated algorithms. Also, compared to currently used optical fibre sensors, the presented solution combines a sensing signal with transmitted data in a single signal, significantly increasing its safety. As demonstrated by the tests, it is one of the few systems able to indicate attempts of clip-on coupler insertion. In addition, with the use of two threshold values for the development of an alarm signal at two independent optical channels in one sensing unit, we achieved a significant improvement in the FAR of the detection system. It should be highlighted that power drop of interfering pulses can occur due to environmental factors as in conventional interferometric sensors, the polarization controller can monitor and restore the proper polarization of the pulses.

Future works will focus on the use of the laser pulses also for the transmission of information, while maintaining the unique sensor properties of the setup. Application of a mirrored system will allow for full duplex transmission which will additionally allow for disturbance localization. Due to the need to use a doubled setup, it is necessary to perform additional tests. However, theoretical calculations shows that resolution of localization depends on the pulse repetition rate and for 100 MHz the resolution of about 4 m can be reached.

References

[1] G. Allwood, G. Wild, S. Hinckley, Optical fibre sensors in physical intrusion detection systems: a review, IEEE Sens. J. 16 (2016) 5497–5509.
[2] M.P. Fok, Z. Wang, Y. Deng, P.R. Prucnal, Optical layer security in fibre-optic networks, IEEE Trans. Inf. Forensics Secur. 6 (2011) 725–736.
[3] B. Javidi, et al., Roadmap on optical security, J. Opt. 18 (2016) 083001.
[4] G. Wild, S. Hinckley, Acousto-ultrasonic optical fibre sensors: overview and state-of-the-art, IEEE Sens. J. 8 (2008) 1184–1193.
[5] X. Bao, L. Chen, Recent progress in distributed fibre optic sensors, Sensors 12 (2012) 8601–8639.
[6] H.F. Taylor, Ch.E. Lee Apparatus and method for fibre optic intrusion sensing, U.S. Patent 5194847 A (1993).
[7] B. Wu, B.J. Shastri, P.R. Prucnal, Secure communication in fibreoptic networks, in: B. Akhgar, H. Arabnia (Eds.), Waltham, Emerging Trends in ICT Security, Elsevier, MA, USA, 2014, 173–183.
[8] D. Rosenberg, J.W. Harrington, P.R. Rice, P.A. Hiskett, C.G. Peterson, R.J. Hughes, et al., Long-distance decoy-state quantum key distribution in optical fibre, Phys. Rev. Lett. 98 (2007), 010503-1-010503-4.
[9] R.H. Hadfield, J.L. Habif, J. Schlafer, R.E. Schwall, S.W. Nam, Quantum key distribution at 1550 nm with twin superconducting single-photon detectors, Appl. Phys. Lett. 89 (2006), 241129-1-241129-3.
[10] J. Scheuer, A. Yariv, Giant fibre lasers: a new paradigm for secure key distribution, Phys. Rev. Lett. 97 (2006), 140502-1-140502-4.
[11] M. Ben-Or, M. Horodecki, D.W. Leung, D. Mayers, J. Oppenheim, The universal composable security of quantum key distribution, in: J. Kilian (Ed.), Theory of Cryptography: Second Theory of Cryptography Conference, Lecture Notesin Computer Science, vol. 3378, Springer Verlag, 2005, 386–406.
[12] N. Jain, B. Stiller, I. Khan, D. Elser, C. Marquardt, G. Leuchs, Attacks on practical quantum key distribution systems (and how to prevent them), Contemp. Phys. 57 (2016) 366–368.