PHOTONIC SENSORS / Vol. 5, No. 4, 2015: 365–375

Intelligent Detection and Identification in Fiber-Optical Perimeter Intrusion Monitoring System Based on the FBG Sensor Network

Huijuan WU[1*], Ya QIAN[1], Wei ZHANG[1], Hanyu LI[2], and Xin XIE[1]

[1] *Key Laboratory of Optical Fiber Sensing and Communications, Ministry of Education, University of Electronic Science and Technology of China, Chengdu, 611731, China*

[2] *Chinese People's Liberation Army (CPLA) Urumqi Institute of the Army, Urumqi, 830042, China*

[*]Corresponding author: Huijuan WU E-mail: hjwu@uestc.edu.cn

Abstract: A real-time intelligent fiber-optic perimeter intrusion detection system (PIDS) based on the fiber Bragg grating (FBG) sensor network is presented in this paper. To distinguish the effects of different intrusion events, a novel real-time behavior impact classification method is proposed based on the essential statistical characteristics of signal's profile in the time domain. The features are extracted by the principal component analysis (PCA), which are then used to identify the event with a K-nearest neighbor classifier. Simulation and field tests are both carried out to validate its effectiveness. The average identification rate (IR) for five sample signals in the simulation test is as high as 96.67%, and the recognition rate for eight typical signals in the field test can also be achieved up to 96.52%, which includes both the fence-mounted and the ground-buried sensing signals. Besides, critically high detection rate (DR) and low false alarm rate (FAR) can be simultaneously obtained based on the autocorrelation characteristics analysis and a hierarchical detection and identification flow.

Keywords: Behavior impact classification, fiber-optical fence, PIDS, security, FBG

Citation: Huijuan WU, Ya QIAN, Wei ZHANG, Hanyu LI, and Xin XIE, "Intelligent Detection and Identification in Fiber-Optical Perimeter Intrusion Monitoring System Based on the FBG Sensor Network," *Photonic Sensors*, 2015, 5(4): 365–375.

1. Introduction

With an increase in terrorism in recent years especially after 9·11, it brings most important yet difficult security challenges globally, such as the perimeter protection of airports, railway stations, government buildings, and military bases. The advent of fiber sensors opens up more opportunities to perimeter security and provides a new promising solution for this application [1–4]. Comparing with those conventional perimeter intrusion detection systems (PIDSs) that use ultrasonic, radar, microwave, and infrared or photo-electric sensors to detect intrusions, the optical fiber sensor (OFS) has outstanding advantages of passive operation, high sensitivity, good reliability in harsh conditions, long-distance capability, electro-magnetic interference immunity (EMI), and corrosion resistance, etc. In particular, OFS does not need any power supply along the fiber link, and hence it is an ideal choice for long or medium long distance applications in harsh field environments. Typical OFS technologies in the security area include the phase-sensitive optical time domain reflectometry

Received: 22 August 2015 / Revised: 15 September 2015

DOI: 10.1007/s13320-015-0274-8
Article type: Regular

(Φ-OTDR) [5–7] and many other OTDR technologies [8], Sagnac, Michelson, Mach-Zehnder (M-Z) and their combination structures [9–12], white light interferometers[13], and quasi-distributed FBG sensor networks [14–19].

In comparison with the highly sensitive OTDR and the interferometer-based fiber fences, fiber Bragg grating (FBG) sensors are immune to the environmental interferences and thus with more reliable detection accuracy and much lower nuisance alarm rates (NARs). Besides, they have precise location ability, and they are flexible for assigning effective sensing and non-sensing fiber lengths according to various application requirements. And mature multiplexing and interrogation technologies make the FBG-based sensing network a potentially cost effective and promising monitoring system, especially for perimeter of short or middle range. Moreover, the FBG sensor response changes linearly with the intrusion behavior impacts, so it is more helpful to identify the event features. However, the event identification is still a pending and challenging problem due to the environmental complexity in practical uses [20–22], such as changing climates like wind and rain, and unpredictable wildlife interferences. Even the same person could introduce different effects due to different fence materials or different sensor mount ways, which presents the most difficult problem to extract essentially distinguishable characteristics of the event targets.

Thus in this paper, a smart perimeter intrusion monitoring system based on the FBG strain sensor network is addressed, in which it can not only overcome the difficulties of detecting weak intrusions from large amounts of nonequivalent sensor nodes with high probability of detection (PD) and low false alarm rate (FAR), but also it can distinguish different threatening activities by using the principal component analysis (PCA) feature extraction in the time domain and the K-nearest neighbor classifier.

2. Hierarchical detection and identification flow in a fiber-optical PIDS based on the FBG sensor network

A quasi-distributed fiber-optic PIDS based on the FBG sensor network is constructed as shown in Fig. 1. In this system, a huge number of FBG sensors with a certain central wavelength for each are connected in series or in parallel in the cable to act as the basic sensing segments. The cable can be attached to a physical fence or buried under ground to measure the mechanical deformation of the fence or other disturbances from outside. In the FBG interrogator, a light source with wide frequency band provides original optical signals, and simutaneously demodulates the optical signals reflected from the separate FBG sensors along the fiber and converts them into digital electronic signals. And a processing unit which acts as an alarm system, processes the signal array and decides if any threat happens along the protected perimeter, where it is and even what it is. The basic detection principle of the system is to monitor the shift of the returned "Bragg" wavelength due to the perturbations of the gratings. And the PD, FAR, and identification rate (IR) are the most concerned metrics for the system.

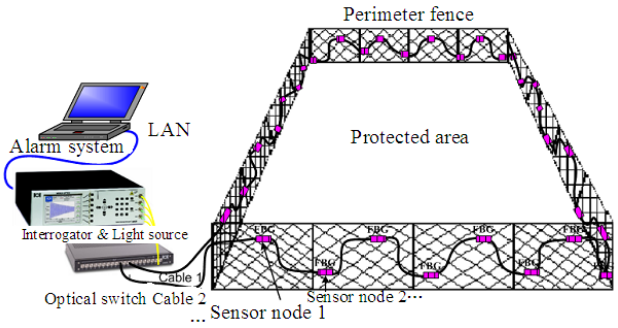


Fig. 1 Configuration of a fiber-optical PIDS based on the FBG sensor network.

Generally, attacks on purpose only occur occasionally in the all day long monitoring, and for most of the monitoring time there is actually no attack or intrusion. To detect the perturbation effectively with high confidence, a hierarchical detection and identification method is introduced in this paper as shown in Fig. 2, which contains three

main stages: abnormity detection with high PD, nuisance alarm exclusion, and real threat identification and classification. At the first two stages we only focus on the detection aim and leave the identification alone. Thus computation of the identification process can be neglected when there isn't any threat, which is quite suitable for the on-line monitoring.

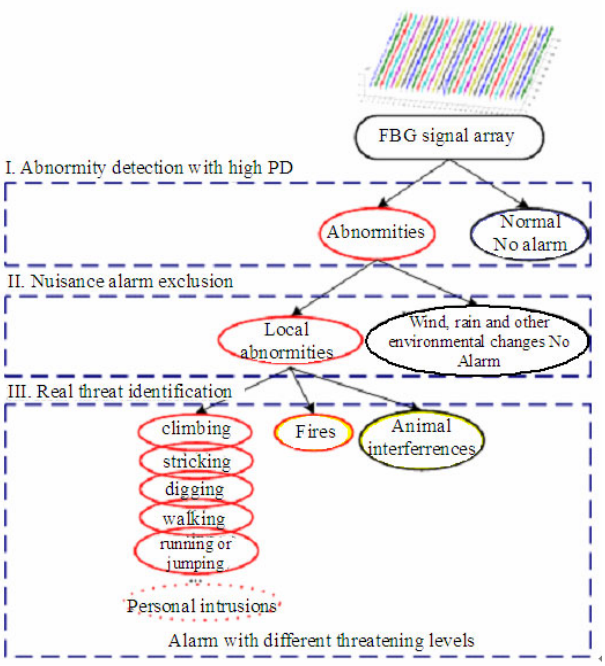


Fig. 2 Hierarchical detection and identification flow for the FBG-based PIDS.

3. Abnormity detection with autocorrelation analysis and nuisance alarm exclusion

In the sensor network as shown in Fig. 1, all the FBG sensors actually have different sensing performances, due to their inherent different sensitivities with slightly different productions and packaging conditions, different attachings or burying ways, and changing environments. The sensing nodes in the network are nonequivalents and the magnitudes of the acquired signal responses differ greatly. Therefore, the traditional energy thresholding method will definitely result in a low PD or a very high FAR in practical applications. And for a perimeter with fences of mixed materials, the case will become even worse, and it cannot play its role any more. Thus the authors introduced a new solution, based on the different autocorrelation characteristics between the attack signals and the non-attack signals [19]. As shown in Fig. 3, the non-intrusion and several typical intrusion signals for the FBG strain sensors have distinguished autocorrelation curves. The line with little square marks represents the autocorrelation function of a certain intrusion signal, such as climbing, striking, swinging, and cutting signals, whose correlation lags are always much longer than those of the lines without square marks, which signify the case of the regular signals without any external perturbation. Here the time lag unit is sample with a sampling rate of 500 Hz. From the autocorrelation curves, it can be seen that the intrusion signal generated from a determined energy source is always highly correlated with itself, while the signals without perturbation are always weakly correlated. Thus it can be taken as a basic intrusion detection criterion in the first step.

And in this paper, this method or criterion is also proved to be suitable for the FBG vibration sensor signals, which can be seen from Fig. 4. In Fig. 4, four typical vibration signals of climbing, temperature rising, animal disturbing, and cutting are examined. The high autocorrelation characteristics of the vibration signals are similar to those of the strain signals but they have more oscillation components for the same event signal.

At the detection stage, to detect the very weak signals from the sensor array, a lower correlation threshold is adopted to maintain a quite high PD. Thus a lot of environmental interferences such as wind, rain, snow, and hailstone, could also be involved, which would be the main nuisance alarm sources. It is thus necessary to exclude these nuisance alarms at the second stage. Fortunately, the environmental changes will influence almost all of the sensors in the network, while real threats always interfere at a local area. And the local and global effects can be directly discriminated from the alarm

sensor number and their locations. By excluding the frequently occurring nuisance sources, the event types to be discerned are significantly decreased, which not only eases the computation load of the identification, but also makes the following identification much more reliable.

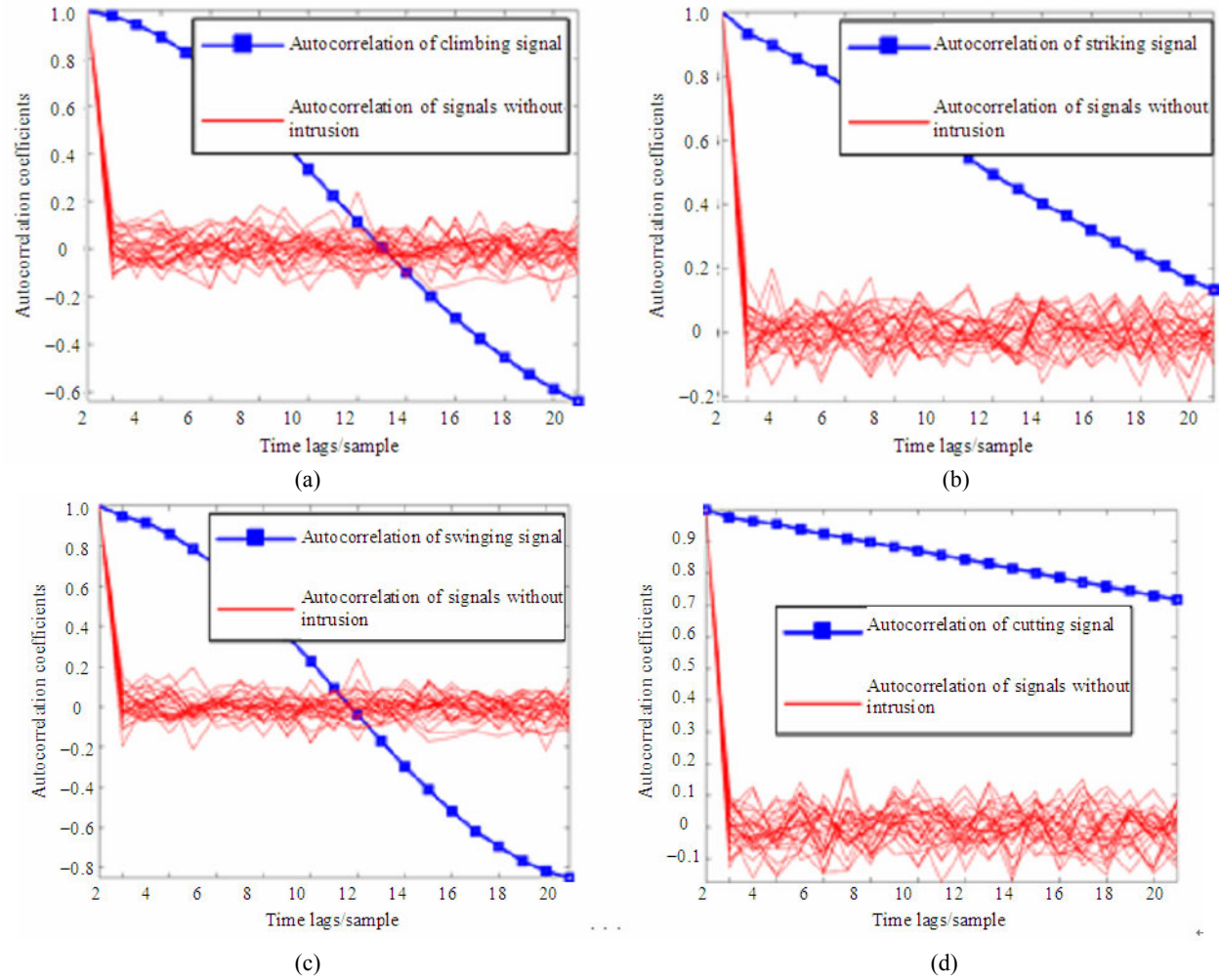


Fig. 3 Correlation characteristics of some typical FBG strain sensing signals: (a) climbing, (b) striking, (c) swinging, and (d) cutting.

4. Abnormity detection with autocorrelation analysis and nuisance alarm exclusion

4.1 Statistical feature extraction based on PCA analysis

As we investigate this problem, the structure or profile of the signals in the time domain reveals more distinguishable information for different types of events, which could be helpful for identifying certain threatening activities in the FBG-based opitcal-fiber fence. But the original temporal signal has a problem of data redundancy, which is definitely not a good vector to be used as the input feature for the identification even though it contains the whole structure information. Here we use the PCA method to convert high dimensional data into a few principal features with much lower dimensions. It uses the temporal data which can tell the signal's profile differences while avoiding its redundancy in the time domain, thus it could be a promising solution for the above problem. As a typical statistical data analysis method, the PCA is successfully employed to find the implicit modality buried in the redundant signals in face recognition [23] and fault diagnosis [24].

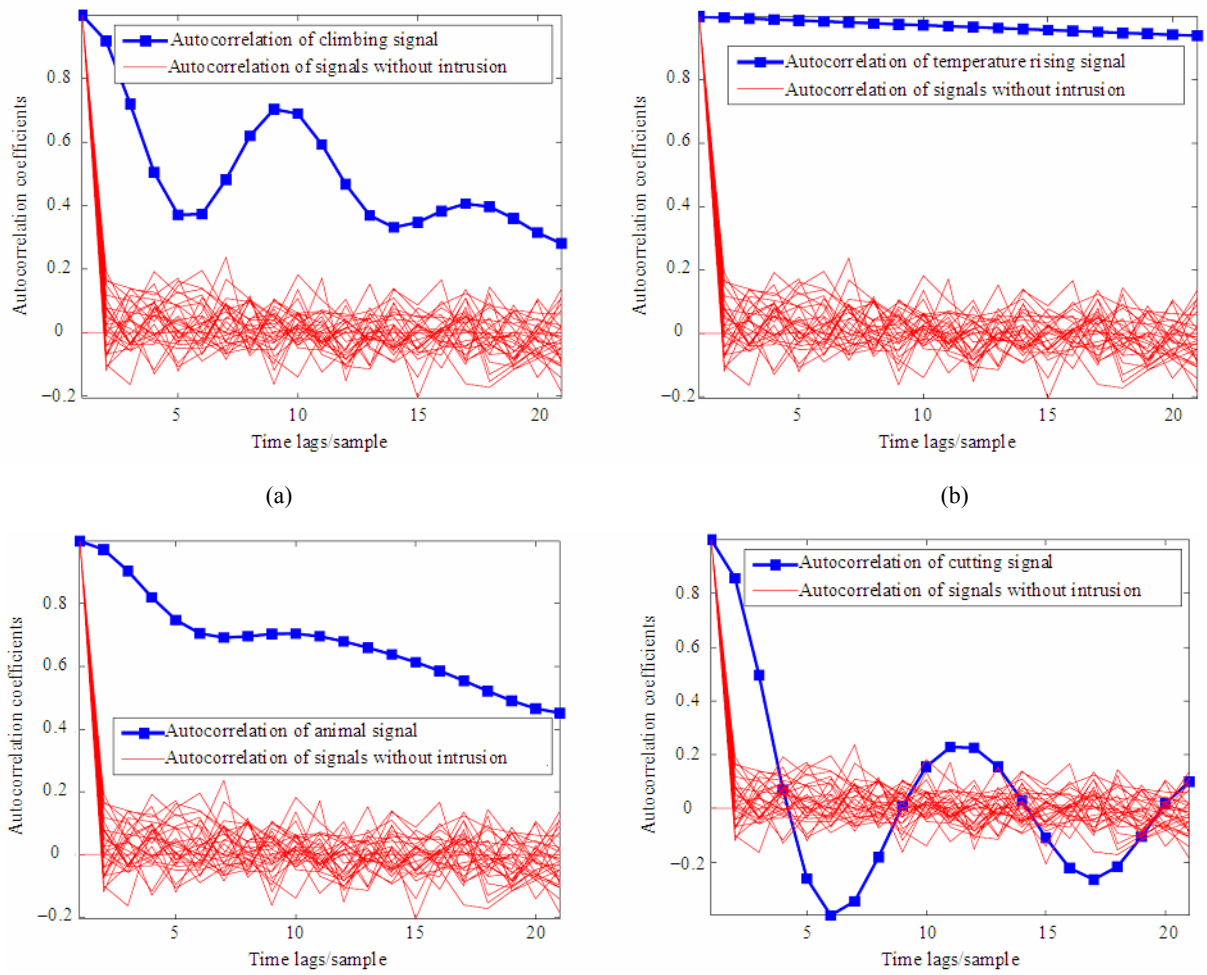


Fig. 4 Correlation characteristics of some typical FBG vibration sensing signals: (a) climbing, (b) temperature rising, (c) animal's disturbing, and (d) cutting.

The principal components analysis process may be regarded as a process of characteristic selection following the feature extraction. First raw temporal intrusion data are transformed into a feature space with a much lower dimension, and its primary statistical feature vectors are selected as its characteristic bases. Each kind of training signal can be approximated or reconstructed by a linear combination of the primary feature bases. The principal features are then selected and used to profile the inputs without any redundancy. Assume m different intrusion events happened, including several typical activity patterns, such as climbing, knocking, digging, and walking. The m detected signals builds up a set of intrusion vectors, regarded as the m dimensions random vector $X=[x_1,x_2,\cdots,x_m]^T$. And its covariance C_X which is denoted as the covariance matrix in this paper is defined as

$$C_X = E[(X-E(X))(X-E(X)^T)] \quad (1)$$

where $E(X)$ is the expected mean value of X. Calculate the eigenvalues $\lambda_1,\lambda_2,\cdots,\lambda_m$ and corresponding normalized eigenvectors $U_1,U_2,\cdots,U_m$ of C_X:

$$C_X U_i = \lambda_i U_i \,(i=1,2,\cdots,m)\,. \quad (2)$$

If we consider the covariance C_X as a vector of m dimensions, and the eigenvectors $U_1,U_2,\cdots,U_m$ decide the direction of the vector. The eigenvalues

$\lambda_1, \lambda_2, \cdots, \lambda_m$ are the contribution factors of each eigenvector, respectively. If the eigenvalue corresponding to the eigenvector is bigger, its contribution radio is larger in reconstruction, and vice versa. A few bigger eigenvalues are kept and the smaller ones are neglected, thus the dimension gets to fall. The fallen dimensions process selects the principal components but discards secondary ones, which is just the key spirit of the PCA method. Supposing $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_m$, the standard deviation contribution radio of primary components is always defined as

$$R(M) = \sum_{i=1}^{M} \lambda_i \Big/ \sum_{i=1}^{m} \lambda_i \ . \tag{3}$$

When the standard deviation contribution radio $R(M)$ is big enough (usually take above 90%), the first M eigenvectors U_i $(i = 1, 2, \cdots, M)$ can be selected to build up a projection space, which is also regarded as the feature space. In this new space, the inputs can be projected as

$$F_i = X^T U_i \quad (i = 1, 2, \cdots, M) \ . \tag{4}$$

The primary features for each intrusion signal are then selected and extracted, which can be represented as a feature vector of M dimensions in the fallen dimension space.

4.2 Identification using a K-Nearest neighbor classifier

Through the above transformation, the test samples are individually projected in an *M*-multi-dimensional feature space constructed by the training samples. Because similar signals with similar feature values could be located at a closer location in the new space, then a K-nearest neighbor classifier is used to discriminate them. However, the identification rate (IR) of this method is mainly dependent on whether the extracted PCA features as above are distinguishable. It assigns a test sample to the *j*th class if a majority of its nearest neighbors belong to the *j*th class. The neighborhood is defined using the Euclidean distance, in which the distance between a test sample, *xtest*, and any training sample *x* is given by

$$\mathrm{dist}(xtest, x) = \sqrt{\sum_{i=1}^{M} (xtest_i - x_i)^2} \ . \tag{5}$$

The Euclidean distances describes the dissimilarity of the test sample and the train samples, thus is always chosen as the dissimilarity representation (DR).

5. Experimental results and discussion

5.1 Hierarchical detection with autocorrelation analysis

In this section, the hierarchical detection with the autocorrelation analysis is first investigated for the fence-mounted sensing nodes. The experimental setup is constructed as in Fig. 1. Thirty FBG strain sensors are used, and the sensors are installed every 2 meters for monitoring a perimeter of about 65 meters length. The interrogator for demodulating the FBG sensing signals is MOI si130 (MICRON OPTICS, USA) with a sampling frequency of 500Hz. In the test, five typical signals are included to be detected, such as climbing, striking, swinging, pushing, and non-threat signals. The test fences include two kinds of wire mesh with different iron materials and a kind of window bar of aluminum alloy, which are remarked as Fence Type I, II, and III, respectively. The test can be classified into two groups: (1) The first group is for a single point intrusion test, where a total of 564 weak personal intrusions are exerted onto the three kinds of fences, of which 178 are tested on the harder Al alloy bars while the others are tested on the other two soft wire meshes, with 198 intrusions each; (2) The second one is for multiple-event detection where 350 tests are run, and two events are simultaneously exerted on two different fences at each time, thus there are 700 events in total for this group. The detection results are concluded in Table 1. The PD can be improved up to 99.65% and 99.57% for the single- and multiple-event detection, respectively, and the missing report rate mainly lies in the harder aluminum alloy fence test group.

Table 1 Test results for single- and multiple-event detection based on the autocorrelation analysis.

	Total test number	Total events	Detected events	PD
Single event	564 (I: 150; II: 150; III: 264)	564	562	99.65%
Dual events	350 (I: 100; II: 100; III: 150)	700	697	99.57%

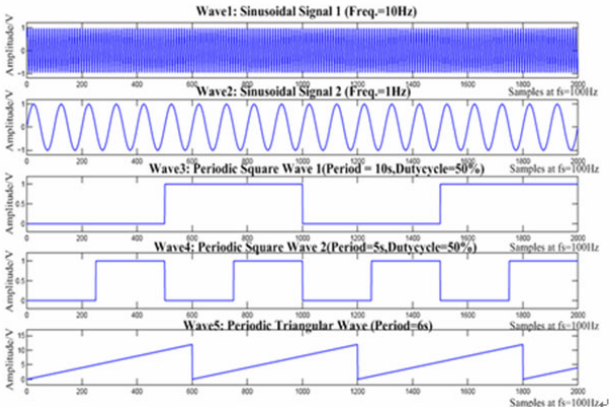
5.2 Identification with PCA analysis

5.2.1 Simulation results and discussion

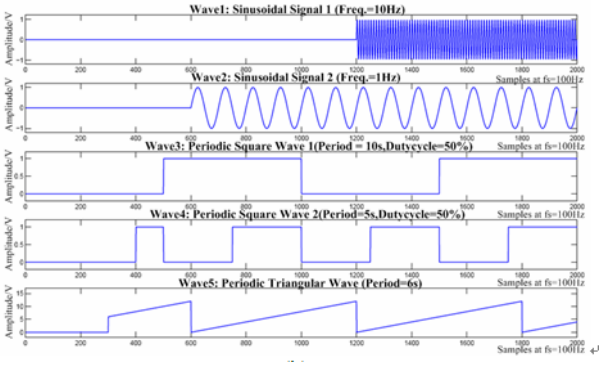
To evaluate the effectiveness of the proposed feature extraction and identification method, different simulated signals are first trained and tested. As shown in Fig. 5(a), five different types of signals are generated and taken as the training samples, which include two sinusoidal signals of 10 Hz and 1 Hz, respectively, two periodic square waves with different periods (Period1=10 s, Period2=5 s, both with duty cycle of 50%) and a periodic triangular wave with a period of 6 seconds. For the testing samples, we add different delays to each kind of signal and modify the amplitude for each delayed version as shown in Fig. 5(b), for being close to real cases. A total of 30 testing samples are generated corresponding to the five training samples above, with 6 testing samples for each type. As we can see from the identification results in Fig. 6, an IR is acquired as high as 96.67% in the simulation test, which proves that different signals' profile or structure can be extracted by PCA, and it could make a good classification result.

5.2.2 Field test results and discussion

To test its actual effectiveness, the field test for the FBG-based fiber optical PIDS is also carried out around a school building, in which both the fence-mounted and the ground-buried sensors are tested. The sensor array and the signal demodulating configuration used is the same as above in the detection test in Section 5.1. Most of the sensors are attached onto the perimeter fence, and only two of them are buried under the ground. For the ground-buried type, to enhance its sensitivity in a larger area, we bond the sensing cable onto a soft wire mesh of 80 cm width, and bury them into the ground together with a burial depth of 15 cm in the clay soils. Four seconds of data are taken as a processing unit and analyzed for the event decision,



(a)



(b)

Fig. 5 Training and testing sample signals for PCA analysis and identification: (a) five kinds of training sample signals and (b) testing signals corresponding to the training samples.

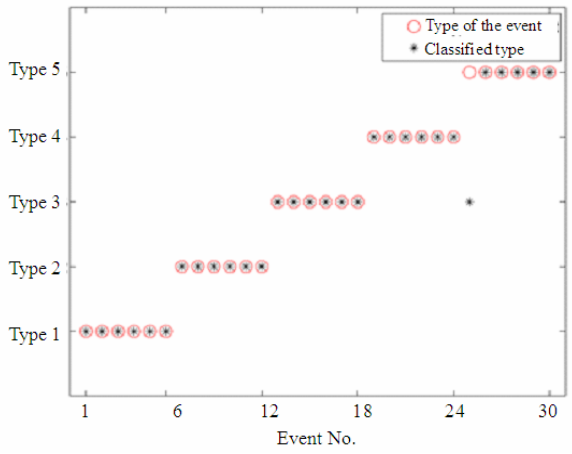


Fig. 6 Identification results for the simulation test (IR=96.67%).

which is updated at each second. A field database is constructed for eight typical events as shown in Fig. 7, which includes 1322 intrusion signals in total. Four types are for the fence-mounted sensing cable,

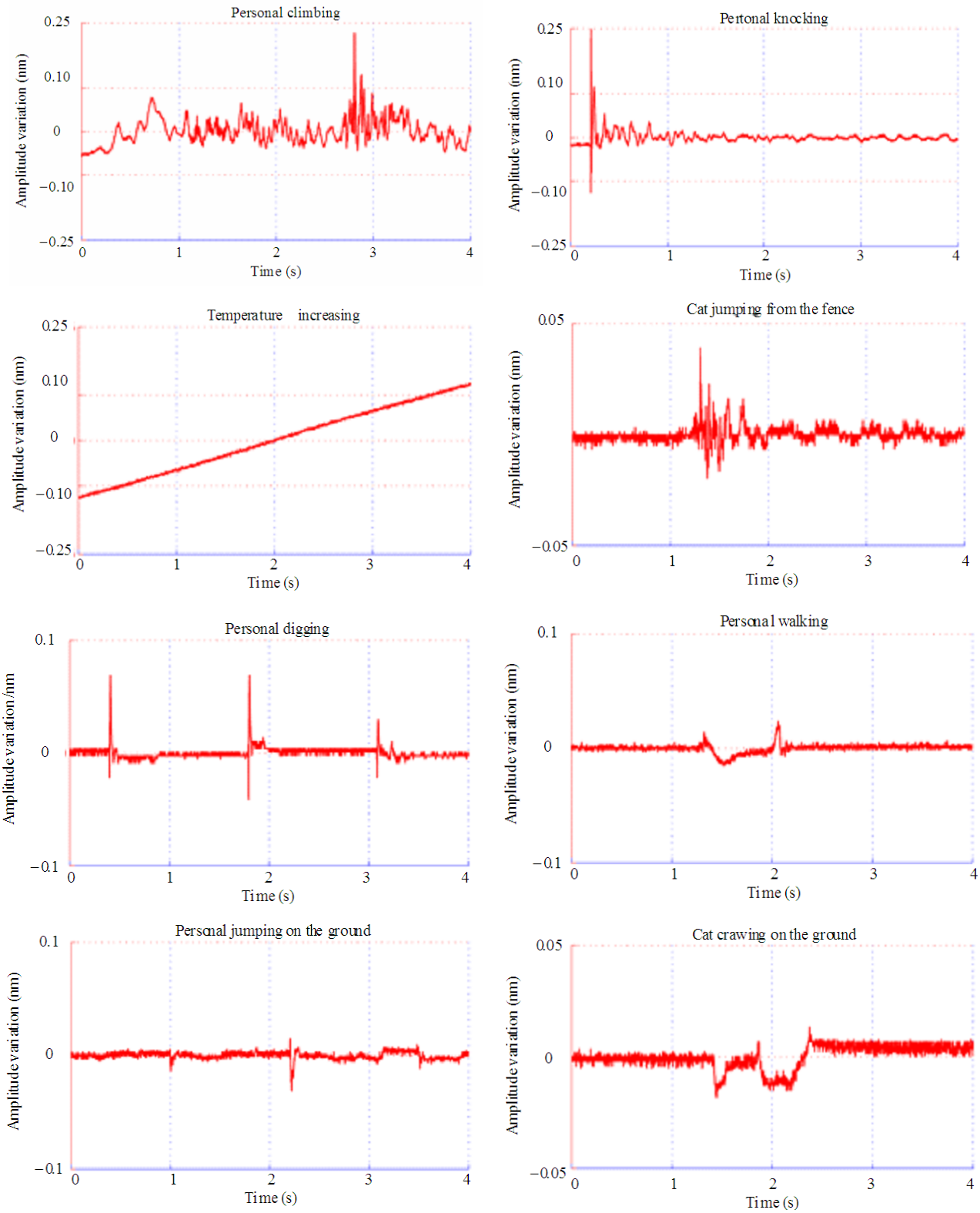


Fig. 7 Typical event signals in the field test.

e.g. personal climbing on the fence, personal striking on the fence, heating on the fence, cat jumping on the fence, and the other four are for the ground-buried cable, such as personal digging on the ground, personal walking on the ground (across the cable), personal running on the ground (across the cable), and cat crawling on the ground. Half of the signals in each type are taken as training samples (661 signals in total), and the other half are testing samples (661 signals in total).

Figure 7 shows that the differences of the eight event signals mainly lie in their varying profiles of time sequences. Their averaged PCA feature values are extracted and concluded in Table 2. From the first four dimensions of the feature space, it can be seen that each kind of event has distinguishable PCA feature values especially in the 1st dimension. Choosing the feature dimension as M =4, most of the identification results can be achieved up to a hundred percent as shown in Table 3, except two events occurring in the ground-buried fences, walking and running, due to the essential similarity between these two activities. In general, the average IR can be achieved up to 96.52% for the eight typical event targets.

Table 2 PCA feature values for eight typical event signals in the field test.

	1st dimension	2nd dimension	3rd dimension	4th dimension
Personal climbing	~68575.61	~ –27.83	~0.39	~ 0.44
Striking	~68710.36	~ –26.97	~ –0.12	~ 0.27
Fire	~ 67576.74	~ –26.69	~ 0.02	~ 0.26
Cat jumping on the fence	~ 68562.35	~ –27.05	~ 0.22	~ 0.23
Digging	~ 69000.15	~ –27.32	~ 0.12	~ 0.22
Walking	~ 69261.58	~ –27.29	~ 0.08	~ 0.32
Running	~ 69128.55	~ –27.34	~ 0.04	~ 0.27
Cat crawling on the ground	~ 68991.10	~ –27.04	~ 0.42	~ 0.67

The average IR and its elapsed time varying with the dimension of the PCA features are also investigated in Fig. 8 for the proposed feature extraction and event identification method in this field test. As we can see that the IR is always kept above 90%, even though it slightly changes with the PCA feature dimension M and performs best when M is equal to 4, which gives a good proof for the proposed method based on the PCA feature extraction. The elapsed time for the 661 test samples takes more or less 1.2 seconds, and each processing unit's computation time takes less than 2 miliseconds. The processing time can be nearly negligible thus the algorithm is very suitable for the on-line identification and classification.

Table 3 Identification results for eight typical events in the field test.

		IR(%) when M=4 is chosen	
Fence-mounted	Personal Climbing (74 events)	100%	Average IR of 96.52%
	Knocking (25 events)	100%	
	Firing (109 events)	100%	
	Cat jumping on fence (23 events)	100%	
Ground-buried	Digging (121 events)	100%	
	Walking (98 events)	89.8%	
	Running (191 events)	93.2%	
	Cat crawling on the ground (20 events)	100%	

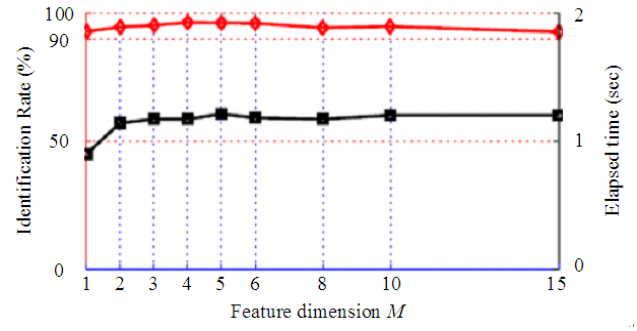


Fig. 8 Average IR and its elapsed time varying with the feature dimension M.

6. Conclusions

In this paper, it is first presented that the PCA method can be used to extract different intrusion signal's profiles or structures in the time domain and give good features for the following behavior identification of the FBG-based fiber-optical PIDS. Based on the autocorrelation characteristics analysis and by using a hierarchical detection and identification model, the PD for multiple-event detection can even be improved up to 99.57%, and

an average recognition rate for eight typical events in real field test can be achieved as high as 96.52%, which is suitable for both the fence-mounted and the ground-buried applications. Moreover, the proposed detection and identification method can be carried out on line in real time. The good performance or intelligence improvement of the proposed method can promote its application in many important areas in perimeter security, safety monitoring of oil/gas pipe lines, electrical power lines, large-scale civil structures, etc.

Acknowledgement

The authors gratefully acknowledge the previous supports provided by National High Technology Research and Development Program of China (863 Program, Grant No. 2007AA01Z245), the supports provided for this research by the Major Program (Grant No. 61290312) and Youth Foundation (Grant No. 61301275) of the National Natural Science Foundation of China (NSFC), and the Fundamental Research Funds for the Central Universities (Grant No. ZYGX2011J010). This work is also supported by Program for Changjiang Scholars and Innovative Research Team in University (PCSIRT, IRT1218), and the 111 Project (B14039).

References

[1] J. Geng, Y. Zou, S. Staines, M. Blake, and S. Jiang, "A real-time distributed fiber strain sensor for long-distance perimeter intruder detection," in *Optical Solutions for Homeland and National Security (Optical Society of America)*, U. S. A., pp. P3, 2005.

[2] M. Szustakowski, W. Ciurapinski, N. Palka, and M. Zyczkowski, "Recent development of fibre optic sensors for perimeter security," in *Proceedings of the International Conference: Modern Problems of Radio Engineering, Telecommunications and Computer Science*, Chile, pp. 158–162, 2002.

[3] S. V. Shatalin, V. N. Treschikov, and A. J. Rogers, "Interferometric optical time-domain reflectometry for distributed optical-fiber sensing," *Applied Optics*, 1998, 37(24): 5600–5604.

[4] J. Bush, C. A. Davis, P. G. Davis, A. Cekorich, and F. P. McNair, "Buried fiber intrusion detection sensor with minimal false alarm rates," in *Proc. SPIE*, vol. 3489, pp. 285–295, 1998.

[5] J. C. Juarez, E. W. Maier, K. N. Choi, and H. F. Taylor, "Distributed fiber-optic Intrusion sensor system," *Journal of Lightwave Techology*, 2005, 23(6): 2081–2087.

[6] J. C. Juarez and H. F. Taylor, "Field test of a distributed fiber-optic intrusion sensor system for long perimeters," *Applied Optics*, 2007, 46(11): 1968–1971.

[7] Y. J. Rao, J. Luo, Z. Ran, J. Yue, X. Luo, and Z. Zhou, "Long-distance fiber-optic Φ-OTDR intrusion sensing system," in *Proc. SPIE*, vol. 7503, pp. 75031O-1–75031O-4, 2009.

[8] F. Peng, Z. Wang, Y. Rao, and X. Jia, "106 km fully-distributed fiber-optic fence based on P-OTDR with 2nd-order Raman amplification," in *Optical Fiber Communication Conference and Exposition and the National Fiber Optic Engineers Conference (OFC/NFOEC)*, Anaheim, CA, pp. 1–3, 2013.

[9] A. D. Kersey, "Recent progress in Interferometric fibre sensor technology," in *Proc. SPIE*, vol. 1367, pp. 2–12, 1990.

[10] A. A. Chtcherbakov and P. L. Swart, "Polarization effects in the Sagnac-Michelson distributed disturbance location sensor," *Journal of Lightwave Technology*, 1998, 16(6): 1404–1412.

[11] B. Kizlik, "Fibre optic distributed sensor in Mach-Zehnder interferometer configuration," in *Proceedings of the International Conference: Modern Problems of Radio Engineering, Telecommunications and Computer Science*, Chile, pp. 128–130, 2002.

[12] M. Szustakowski, W. M. Ciurapinski, and M. Zyczkowski, "Trends in optoelectronic perimeter security sensors," in *Proc. SPIE*, vol. 6736, pp. 67360Q-1–67360Q- 12, 2007.

[13] L. Yuan and Y. Dong, "Loop topology based white light interferometric fiber optic sensor network for application of perimeter security," *Photonic Sensors*, 2011, 1(3): 260–267.

[14] A. D. Kersey, M. A. Davis, H. J. Partrick, M. Leblance, K. P. Koo, C. G. Askins, *et al.*, "Fiber grating sensors," *Journal of Lightwave Technology*, 1997, 15(8): 1442–1463.

[15] Y. Rao, "In-fibre Bragg grating sensors," *Measurement Science and Technology*, 1997, 8(4): 355–375.

[16] Y. Rao, "Recent progress in application of in-fiber

Bragg grating sensors," *Optics and Lasers in Engineering*, 1999, 31(4): 297–324.

[17] Z. Ran, Y. Rao, N. Nie, and R. Chen, "Long-distance fiber Bragg grating sensor system based on hybrid Raman/erbium-doped fiber amplifier," in *Proc. SPIE*, vol. 5855, pp. 583–586, 2005.

[18] Q. Jiang, Y. Rao, and D. Zeng, "A fiber-optical intrusion alarm system based on quasi-distributed fiber Bragg grating sensors," in *APOS'08. 1st Asia-Pacific Optical Fiber Sensors Conference*, Chengdu, China, pp. 1–4, 2008.

[19] H. Wu, Y. Rao, C. Tang, Y. Wu, and Y. Gong, "A novel FBG-based security fence enabling to detect extremely weak intrusion signals from nonequivalent sensor nodes," *Sensors and Actuators A: Physical*, 2011, 167(2): 548–555.

[20] F. Blackmon and J. Pollock, "Blue Rose perimeter defense and security system," in *Proc. SPIE*, vol. 6201, pp. 620123, 2006.

[21] D. Anderson, "Smart perimeter security," Fiber-SenSys.,http://www.fibersensys.com/index.php?option=com_docman&task=doc_details&gid=55&Itemid=54 (2009).

[22] H. Yan, G. Shi, Q. Wang, and S. Hao, "Identification of damaging activities for perimeter security," in *2009 International Conference on Signal Processing Systems*, Singapore, pp. 162–166, 2009.

[23] Y. Zhao, X. Shen, N. Georganas, and E. M. Petriu, "Part-based PCA for facial feature extraction and classification," in *IEEE International Workshop on Haptic Audio visual Environments and Games*, Lecco, pp. 99–104, 2009.

[24] X. Han, D. Xu, and Y. Liu, "Application of principal components analysis in condenser fault diagnosis," in *The Sixth World Congress on Intelligent Control and Automation*, Dalian, pp. 5666–5669, 2006.