

基于综合特征的光纤周界安防系统高效入侵事件识别

黄翔东 张皓杰 刘琨 马春宇 刘铁根

High-efficiency intrusion recognition by using synthesized features in optical fiber perimeter security system

Huang Xiang-Dong Zhang Hao-Jie Liu Kun Ma Chun-Yu Liu Tie-Gen

引用信息 Citation: *Acta Physica Sinica*, 66, 124206 (2017) DOI: 10.7498/aps.66.124206

在线阅读 View online: <http://dx.doi.org/10.7498/aps.66.124206>

当期内容 View table of contents: <http://wulixb.iphy.ac.cn/CN/Y2017/V66/I12>

---

您可能感兴趣的其他文章

Articles you may be interested in

基于游标效应的增敏型光纤法布里-珀罗干涉仪温度传感器

Sensitivity-enhanced temperature sensor with fiber optic Fabry-Perot interferometer based on vernier effect

物理学报.2017, 66(9): 094205 <http://dx.doi.org/10.7498/aps.66.094205>

面向地壳形变观测的超高分辨率光纤应变传感系统

Ultrahigh resolution fiber optic strain sensing system for crustal deformation observation

物理学报.2017, 66(7): 074208 <http://dx.doi.org/10.7498/aps.66.074208>

基于全相位滤波技术的光纤表面等离子体共振传感解调算法

Optical fiber SPR sensing demodulation algorithm based on all-phase filters

物理学报.2017, 66(7): 074202 <http://dx.doi.org/10.7498/aps.66.074202>

光纤超声传感器及应用研究进展

Fiber-optic ultrasonic sensors and applications

物理学报.2017, 66(7): 074205 <http://dx.doi.org/10.7498/aps.66.074205>

用于气象观测的阵列式温度传感器流体动力学分析与实验研究

Fluid dynamic analysis and experimental study of a temperature sensor array used in meteorological observation

物理学报.2016, 65(9): 094209 <http://dx.doi.org/10.7498/aps.65.094209>

# 基于综合特征的光纤周界安防系统 高效入侵事件识别\*

黄翔东<sup>1)</sup> 张皓杰<sup>1)</sup> 刘琨<sup>2)†</sup> 马春宇<sup>2)</sup> 刘铁根<sup>2)</sup>

1)(天津大学电气自动化与信息工程学院, 天津 300072)

2)(天津大学精密仪器与光电子工程学院, 天津 300072)

(2016年12月24日收到; 2017年3月29日收到修改稿)

在光纤周界安防系统中, 急需对入侵事件实现准确而高效的识别, 对事件特征做简练而恰当的描述是其关键所在. 本文提出一种基于综合特征的入侵事件识别方法, 该方法引入全相位滤波器组将输入信号并行分解为多个频率通道, 以提取这些通道的归一化功率值; 进而与信号过零率相结合, 构成包含时域信息、频域信息的综合特征向量; 最后将该特征向量馈入径向基函数神经网络即可准确识别出攀爬、敲击、晃动、剪切四种常见的入侵动作. 实验证明, 本文方法相比于现有的经验模态分解方法, 不仅提高了精度, 而且显著加快了识别速度.

**关键词:** 光纤周界安防, 入侵事件识别, 综合特征, 滤波器组

**PACS:** 42.81.Pa, 42.79.Ci, 45.70.Qj

**DOI:** 10.7498/aps.66.124206

## 1 引言

光纤周界安防系统<sup>[1-3]</sup>利用光纤传感元件对压力及振动十分敏感的特点, 非常适合于对直接接触及或间接传递给光纤的各类扰动进行检测. 相比于传统的周界安防系统(如红外线安防系统<sup>[4]</sup>、电子围栏安防系统<sup>[5]</sup>), 光纤周界安防系统灵敏度更高, 因而更具有实用价值. 在各类光纤周界安防系统中, 双马赫-曾德尔干涉仪(dual Mach-Zehnder interferometer, DMZI)分布式光纤传感系统<sup>[6,7]</sup>采用相位调制型光纤传感技术, 具有高灵敏度和响应速度快等优点, 已经广泛应用于海底电缆安防<sup>[8]</sup>、机场安防<sup>[9]</sup>、边界安防<sup>[10,11]</sup>等各类安防领域. 在这些安防应用中, 急需解决高效、精确地识别入侵事件的问题, 该问题的解决关键在于信号处理算法的设计. 具体而言, 就是在完成入侵振动信号端点检测<sup>[12]</sup>的基础上, 进一步设计简练、恰当的入侵信号特征描述方法, 并结合相应的模式分类措施, 有效

识别出各类入侵动作.

光纤扰动信号是非稳定信号, 该信号的特征提取方式一般有小波分解法<sup>[13]</sup>、电平检测法<sup>[14]</sup>和经验模态分解(empirical mode decomposition, EMD)法<sup>[15]</sup>等, 然而这些特征提取方法难以兼顾高效率和高精度. 例如, 文献<sup>[13]</sup>提出的小波识别法虽然其特征向量可通过多级分解得到的不同频带的能量来表征<sup>[16]</sup>, 但是其计算量会随小波分解层数的增加而变大, 另外, 该特征向量仅考虑了频域特征, 缺少足够丰富的时域信息, 故识别准确率较低, 仅能识别3类入侵事件; 文献<sup>[14]</sup>提出的电平检测法首先需要确定高于某电平阈值的波形区域, 进一步依据该区域各种时域包络特征(如区域宽度、上升斜率、下降斜率、最高点幅值等)识别各类侵犯动作, 这类方法虽然复杂度降低, 但因仅考虑了信号的时域特征, 缺少足够丰富的频域特征, 故识别精度仍不高; 而文献<sup>[15]</sup>提出的EMD方法需逐个求取分解过程中的固有模态函数(intrinsic

\* 国家自然科学基金(批准号: 61671012, 61475114)资助的课题.

† 通信作者. E-mail: beiyangkl@tju.edu.cn

mode function, IMF) 的峭度值, 对这些峭度值组合得到的特征向量进行分类, 即可高精度地识别 4 类常见动作, 然而这些 IMF 需经历多次复杂的迭代才能获得, 故识别效率不高而影响了其实用性.

为解决以上方法难以兼顾识别效率和识别精度的矛盾, 本文提出一种基于综合特征的入侵模式识别方法. 该方法首先对输入的扰动信号进行端点检测, 判断扰动起始点; 然后将确定扰动起始点的信号馈入全相位滤波器组<sup>[17-19]</sup>的各个通道进行频域分离处理, 并计算各通道输出信号的归一化功率值, 再综合整段扰动信号的时域过零率 (zero-crossing rate, ZCR) 便可生成特征向量; 最后, 将综合特征向量馈入径向基函数 (radial basis function, RBF) 神经网络<sup>[20,21]</sup>即可实现侵犯动作识别. 由于基于全相位滤波器的特征提取以并行流水线的方式进行, 避开了小波多级分解和 EMD 多次迭代的方式, 故其工作效率高; 由于其特征向量蕴含了频域信息 (各频带功率值) 和时域信息 (ZCR), 对侵犯动作描述得更全面, 故可实现高精度识别. 实验表明, 本文方法能够快速有效区分 4 类入侵事件, 平均识别准确率接近 90%, 特征提取效率相比于 EMD 方法提高了 4 倍.

## 2 DMZI 光纤传感系统及入侵事件识别总体流程

### 2.1 DMZI 光纤传感系统

DMZI 分布式光纤传感系统的结构如图 1 所示. 图 1 中,  $P$  点为扰动点, 传感光缆总长度为  $L$ . 激光源发出的光线通过隔离器后, 经由耦合器  $C1$  被平均分为两束光线, 随后进入由耦合器  $C2$  和  $C3$  组成的 DMZI 中. 两束光分别按照顺时针和逆时针方向沿着传感光缆传播, 之后进入相应的对端耦合器 ( $C3, C2$ ) 中, 并在其中发生干涉, 干涉结果输出到探测器  $PD1$  和  $PD2$  中. 探测器将所探测到的光信号转换为电信号, 经过隔直流处理后由对应的高速采集卡 (data acquisition, DAQ) 采集. 根据不同要求, 可以对 DAQ 设定不同的采样率. 其中, DAQ1 用于端点检测和入侵事件分类<sup>[19]</sup>, DAQ2 用于入侵事件定位. 为提高入侵事件的检测敏感度, 两个 DAQ 选用的是量化位数为 14 bit 的 NI 系列的采集卡. 最后, 通过在工业计算机 (industrial personal computer, IPC) 中执行特定算法, 实现所

需要的功能.

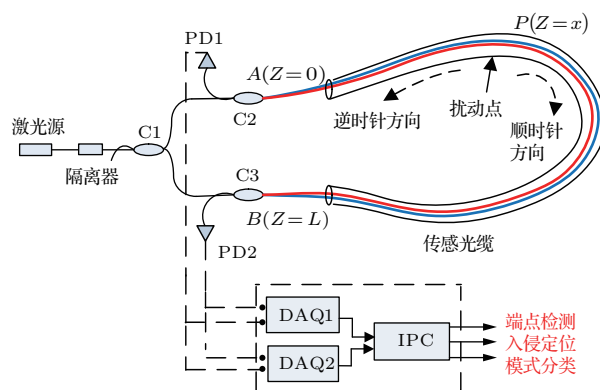


图 1 (网刊彩色) DMZI 分布式光纤传感系统原理图

Fig. 1. (color online) Schematic diagram of DMZI disturbed optical fiber sensing system.

### 2.2 入侵事件识别总体流程

DMZI 分布式光纤传感系统的入侵事件识别通常需经历如图 2 所示的流程: 首先, 通过降噪、高通滤波等数据预处理措施来增强光纤振动信号的质量并提取事件发生的时间端点位置<sup>[12,22]</sup>; 其次, 运行特征提取算法, 将庞大的预处理后的样本恰当地描述成简短精炼的特征向量; 最后, 选择合适的分类器对特征向量做训练及测试, 输出入侵动作的识别结果. 在以上步骤中, 特征提取算法是影响入侵动作识别性能的最主要因素.

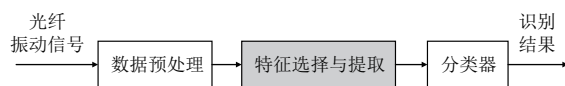


图 2 入侵事件识别流程图

Fig. 2. Dataflow of intrusion event discrimination.

好的特征提取算法不仅需要具备高的准确表达性, 而且其处理过程应尽量简单. 基于这两方面的考虑, 本文提出如图 3 所示的事件识别流程 (其特征提取流程如虚框所示), 具体流程描述如下.

1) 初始化及预处理: 对多组非入侵动作样本进行快速傅里叶分析 (fast Fourier transform, FFT) 得到空闲环境的下限截止频率  $f_e$ , 进一步用截止频率为  $f_e$  的高通滤波器 (high pass filter, HPF) 检测出光纤振动信号中与入侵事件对应的端点位置 (其具体操做详见文献<sup>[12, 22]</sup>, 本文不再做具体介绍); 另外, 用  $f_e$  和动作上限截止频率  $f_u$  (可事先对常见的入侵振动信号做统计谱分析得到) 对  $Q$  个子滤波器  $g_0, \dots, g_{Q-1}$  的系数进行配置.

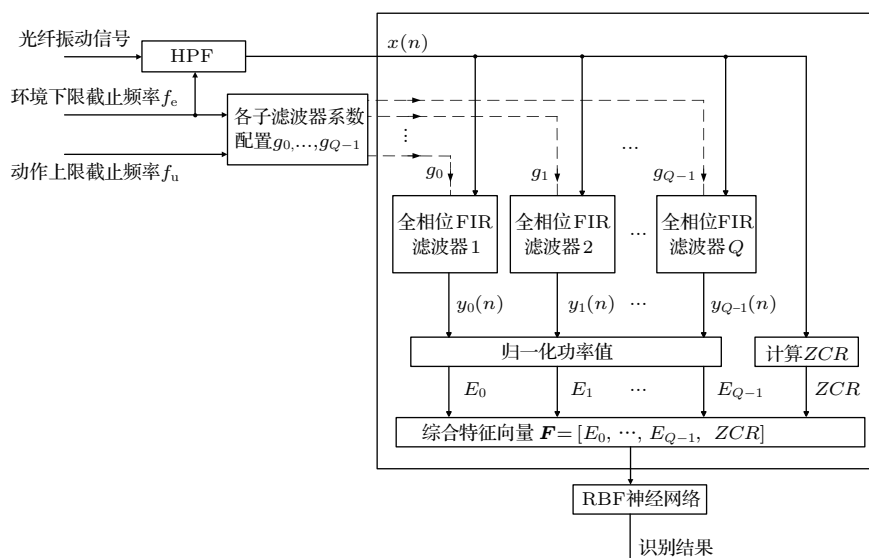


图3 本文所提入侵事件识别方法流程图

Fig. 3. Dataflow of the proposed intrusion discrimination scheme.

2) 特征提取: 将预处理后的信号  $x(n)$  并行馈入到全相位滤波器组 (包含  $Q$  个子有限冲击响应 (FIR) 滤波器  $g_0, \dots, g_{Q-1}$ ), 计算出其滤波输出  $y_q(n) (q = 0, \dots, Q-1)$  的  $Q$  个归一化功率值  $E_q$ ; 另外, 直接计算信号  $x(n)$  的整体 ZCR, 将该值与  $E_q$  做综合得到长度为  $Q+1$  的综合特征向量  $\mathbf{F} = [E_0, E_1, \dots, E_{Q-1}, ZCR]$ .

3) RBF 神经网络模式识别: 将特征提取得到的综合特征向量以及对应标签馈入 RBF 神经网络进行训练, 再将未知种类入侵信号的特征向量馈入该网络做测试, 并输出入侵动作的模式识别结果.

### 3 综合特征向量构造原理

#### 3.1 构造特征向量的考虑

如前所述, 特征的提取及描述对于后续的模式识别工作具有深远的影响. 为提高模式的精度与效率, 本文方法在构造特征向量时做了以下考虑:

- 1) 为保证模式的准确度, 特征向量应尽可能完整地描述信号特征;
- 2) 为消除主要位于低频的环境噪声的影响, 特征提取应在较高频段进行;
- 3) 为提高模式的速度, 特征提取的复杂度尽量低, 其提取过程应简单高效;
- 4) 为体现各子通道信号特征的独立性, 其各部分之间的耦合性应尽可能小, 特征向量长度应尽可能短.

从图 3 可看出, 本文构造的特征向量  $\mathbf{F} = [E_0, E_1, \dots, E_{Q-1}, ZCR]$ , 其中,  $E_0, E_1, \dots, E_{Q-1}$  反映了信号各频段的能量分布, 而 ZCR 则反映了整段信号的时域统计特性, 故特征向量  $\mathbf{F}$  综合凝练了信号的时、频域两方面特征, 符合第 1 个要求; 而在特征提取之前, 对光纤振动信号做了高通滤波处理, 因而消除了环境干扰, 符合第 2 个要求; 从图 3 可看出, 借助全相位 FIR 滤波器组,  $E_0, E_1, \dots, E_{Q-1}$  是对  $x(n)$  做并行流水线滤波获得的, 绕开了文献 [15] 的 EMD 处理的反复迭代求 IMF 的过程, 故计算复杂度更低, 效率更高, 符合第 3 个要求; 而第 4 个要求, 由各全相位子滤波器的性能决定, 下节做详细分析.

#### 3.2 全相位滤波器组的系数配置及性能分析

##### 3.2.1 全相位滤波器组的系数配置

如图 3 所示, 借助全相位滤波器组, 可将输入信号  $x(n)$  并行分解成不同频率通道的  $Q$  个子信号  $y_0(n), \dots, y_{Q-1}(n)$ , 进而方便于从中提取具体特征, 作为后续动作模式识别的依据. 全相位滤波器组应具备灵活配置的特性, 以满足 DMZI 系统适应于不同环境的需求.

我们在文献 [18] 中指出: 全相位设计法是直接在频率域进行滤波器设计的方法. 文献 [17] 指出: 全相位 FIR 滤波器系数可由下列 3 个简单步骤得到.



**步骤1** 对某个长度为 $N$ 满足 $H(k) = H(N - k)$ 的频率向量 $\mathbf{H}$ 做广义离散傅里叶逆变换(inverse discrete Fourier transform, IDFT), 从而得到向量 $\mathbf{h} = [h(-N + 1), \dots, h(-1), h(0), h(1), \dots, h(N - 1)]$ , 即

$$h(n) = \frac{1}{N} \sum_{k=0}^{N-1} H(k) e^{j2\pi nk/N}, \quad n \in [-N + 1, N - 1]. \quad (1)$$

**步骤2** 将某个长度为 $N$ 的窗 $f(n)$ , 与自身的翻转窗 $f(-n)$ 进行卷积, 生成长度为 $2N - 1$ 的双

窗卷积窗 $w_c(n)$ <sup>[18]</sup>, 即

$$w_c(n) = f(n) * f(-n), \quad -N + 1 \leq n \leq N - 1, \quad (2)$$

**步骤3** 将 $h(n)$ 与 $w_c(n)$ 对应元素相乘, 即得最终的长度为 $2N - 1$ 的滤波器系数 $g(n)$ .

以上步骤中, 滤波器的通带范围是在步骤1中通过改变频率向量 $\mathbf{H}$ 来实现. 为获得 $Q$ 个通带位于不同范围的子滤波器, 不妨将其频率向量 $\mathbf{H}_q (q = 0, \dots, Q - 1)$ 的期望通带的元素值设置为1, 其他元素值设置为0. 频率向量 $\mathbf{H}_q$ 的格式如下:

$$\mathbf{H}_q = [\underbrace{0, \dots, 0}_e, \underbrace{0, \dots, 0}_{mq}, \underbrace{1, \dots, 1}_m, \underbrace{0, \dots, 0}_{N-(2mq+2m+2e-1)}, \underbrace{1, \dots, 1}_m, \underbrace{0, \dots, 0}_{mq}, \underbrace{0, \dots, 0}_{e-1}], \quad q = 0, \dots, Q - 1. \quad (3)$$

(3)式中,  $e$ 为环境干扰参数,  $m$ 为通带参数. 文献[12]指出, 无入侵时DMZI系统的周边环境干扰以低频成分为主(该干扰的截止频率 $f_e$ 可通过对多组入侵样本做FFT统计分析得到). 显然,  $f \in (0, f_e)$ 内的环境干扰不应作为动作特征, 故(3)式的 $\mathbf{H}_q$ 在低频段设置了 $e$ 个0对其进行抑制. 令DAQ1的采样速率为 $f_s$ , 则频率向量 $\mathbf{H}_q$ 的每个元素占据的模拟带宽为 $\Delta f = f_s/N$ , 故整数参数 $e$ 应配置如下:

$$e = [f_e/\Delta f] = [Nf_e/f_s], \quad (4)$$

其中“ $[\cdot]$ ”表示四舍五入操作. 从而(3)式所对应的子滤波器 $\mathbf{g}_q$ 的理想通带范围为

$$f \in [(qm + e)\Delta f, (qm + e + m)\Delta f], \quad q = 0, \dots, Q - 1. \quad (5)$$

从(3)和(5)式可看出, 每个子滤波器的通带宽度为 $m\Delta f$ , 假定常见入侵事件的上限频率为 $f_u$ (可提前对多组动作进行FFT统计分析得到), 则整个滤波器组的通带带宽为 $B = f_u - f_e$ , 每个子滤波器通带宽度则为 $B/Q$ , 故参数 $m$ 配置如下:

$$m = \left\lceil \frac{B}{Q \cdot \Delta f} \right\rceil = \left\lceil \frac{(f_u - f_e)N}{Q \cdot f_s} \right\rceil. \quad (6)$$

进一步地, 把(1)式中的 $H(k)$ 替换为(3)式的 $\mathbf{H}_q(k)$ , 可得到其广义IDFT的计算结果 $h_q(n)$ ,

$$h_q(n) = \begin{cases} \frac{2\cos[\pi n(2mq + 2e + m - 1)/N] \sin(m\pi n/N)}{N \sin(\pi n/N)}, & n \in [-N + 1, 1] \cup [1, N - 1], \\ 2m/N, & n = 0. \end{cases} \quad (7)$$

最后, 根据步骤3, 可得所有 $Q$ 个全相位子FIR滤波器的系数为

$$g_q(n) = w_c(n)h_q(n), \quad q = 0, \dots, Q - 1. \quad (8)$$

从以上推导可以看出, 只需分别用(4)和(6)式确定环境干扰参数 $e$ 和通带参数 $m$ , 将之代入(7)和(8)式即可直接得到全相位FIR滤波器组的所有系数 $g_0(n), \dots, g_{Q-1}(n)$ , 即将三步全相位滤波器设计法简化为代入解析公式一步实现, 故本文提出的针对DMZI系统的全相位滤波器的参数配置方法兼顾了高灵活性和高效性.

众所周知, FIR滤波是前馈的连续卷积过程,

图3的 $Q$ 个子滤波器实际上是以并行流水线方式工作, 故本文提出的基于全相位滤波器组的特征提取无需任何迭代处理, 相比于EMD分解方法, 大大提高了工作效率.

### 3.2.2 全相位滤波器组的性能分析

如前所述, 事件识别的准确度由全相位滤波器的传输性能决定. 具体而言, 对某个子滤波器, 在相邻子滤波器频带内衰减应尽量大, 才能降低特征向量各元素之间的耦合; 反过来, 在事件识别精度一定的情况下, 滤波器的带外衰减越大, 所要求的子滤波器数目就越少, 对应的特征向量长度就越

短. 文献[17]指出, 全相位滤波器频率响应的内插函数用卷积窗傅里叶谱替代了传统的矩形窗傅里叶谱, 故可以保证很大的带外衰减, 以下用一具体实例说明该问题.

令频率向量长度  $N = 256$ , 数据采集卡 DAQ1 的采样率  $f_s = 10$  kHz, 滤波器组的子滤波器个数  $Q = 5$ . 借助现场统计分析, 推算出环境干扰的截止频率  $f_e = 250$  Hz, 一般入侵事件上限频率  $f_u = 3500$  Hz, 根据 (4) 和 (6) 式可确定滤波器参数  $e = 6$ ,  $m = 17$ , 窗函数  $f(n)$  选用 Hamming 窗. 根据 (7) 和 (8) 式得到 5 个子滤波器  $g_0(n), \dots, g_4(n)$ , 相应的衰减曲线为  $20 \lg |G_q(j2\pi f)|$ ,  $q = 0, \dots, 4$ , 如图 4(a) 所示; 为进行比较, 给出采用经典频率采样法得到的衰减曲线  $20 \lg |H_q(j2\pi f)|$ ,  $q = 0, \dots, 4$ ,

如图 4(b) 所示.

从图 4 可看出, 采用经典频率采样法得到的滤波器组传输曲线图在通带内有明显的波纹, 每个子滤波器的第 1 旁瓣衰减只有  $-22$  dB (对应通带幅值的 7.94%); 相比之下, 本文采用的全相位滤波器组几乎不存在通带波纹, 每个子滤波器的第 1 旁瓣衰减接近  $-70$  dB (对应通带幅值的 0.0316%), 这意味着相比于频率采样法, 全相位滤波器组的各子滤波器之间的耦合程度大幅度降低; 另外, 在频率低于  $f \in (0, 250)$  Hz 的区域, 全相位滤波器组的衰减曲线仍接近  $-70$  dB, 这意味着环境干扰可较彻底地得以消除. 全相位滤波器组的这些良好性能保证了后续动作识别的高准确性.

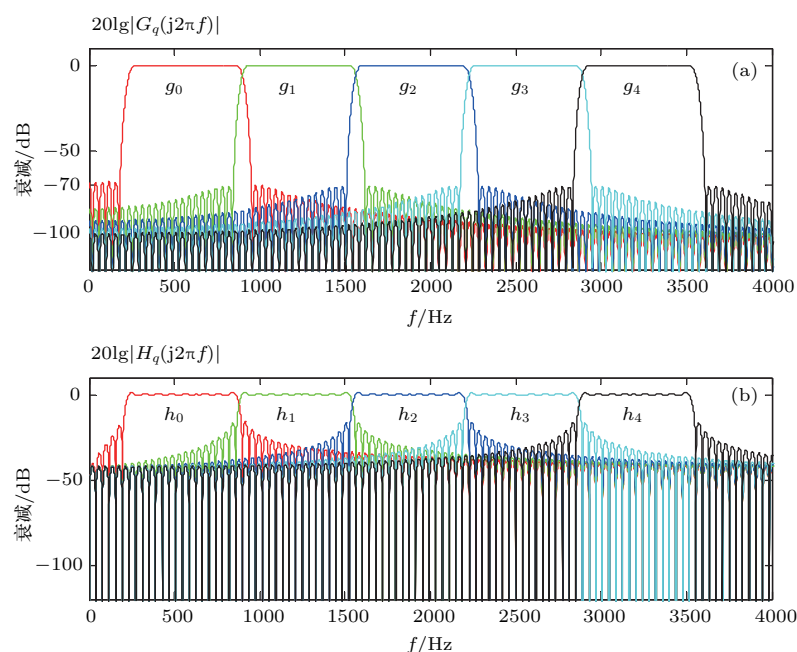


图 4 (网刊彩色) (a) 本文滤波器组的衰减曲线; (b) 经典频率采样法所得滤波器组的衰减曲线

Fig. 4. (color online) (a) Attenuation curves of the proposed filter bank; (b) attenuation curves of classical frequency sampling method based filter bank.

### 3.3 综合特征提取

不难理解, 全相位滤波器组并行输出子信号  $y_0(n), \dots, y_{Q-1}(n)$  的  $Q$  个功率值反映了输入信号  $x(n)$  在各频段的能量分布, 若这些功率值与原整段输入  $x(n)$  的 ZCR 结合, 即可构造出蕴含时、频域两方面信息的综合特征向量.

1) 功率: 假定输出样本长度为  $L$ , 则全相位滤波器组的第  $q$  个输出信号  $y_q(n)$  的平均功率  $\tilde{E}_q$  可由下式算出

$$\tilde{E}_q = \frac{1}{L} \sum_{n=0}^{L-1} y_q^2(n), \quad q = 0, \dots, Q-1. \quad (9)$$

然而, 由于 ZCR 总是处于  $(0, 1)$  区间内, 而平均功率  $\tilde{E}_q$  可能远远超出该区间, 因而为保证特征向量内部各元素取值范围的均衡性, 需对平均功率  $\tilde{E}_q$  做归一化处理, 即算出如下功率值  $E_q$ ,

$$E_q = \frac{\tilde{E}_q}{\sum_{q=0}^{Q-1} \tilde{E}_q}, \quad q = 0, \dots, Q-1. \quad (10)$$

2) ZCR: ZCR 是在时域内整体统计的性能指

标, 反映的是信号变化快慢程度.  $ZCR$  可由下式算出:

$$ZCR = \frac{\sum_{n=1}^L |\text{sign}[x(n)] - \text{sign}[x(n-1)]|}{2L}, \quad (11)$$

其中, “sign” 表示取符号操作, 由下式算出:

$$\text{sign}[x(n)] = \begin{cases} 1, x(n) \geq 0, \\ -1, x(n) < 0. \end{cases} \quad (12)$$

将以上两种特征进行组合, 即可构造出综合特征向量  $\mathbf{F} = [E_0, E_1, \dots, E_{Q-1}, ZCR]$ , 用于馈入 RBF 神经网络进行动作模式识别.

## 4 RBF 神经网络

近年来, 人工神经网络因具有强大的自学习能力以及易于硬件实现等优点受到广泛关注. RBF 神经网络作为一种前馈神经网络, 具有学习算法收敛速度快的优点. 本文方法采用 RBF 神经网络进行入侵动作模式识别.

最基本的 RBF 神经网络主要由输入层、单隐层和输出层三部分组成. 输入层作为特征向量的输入端, 其神经元数目应与训练样本的维数相同; 隐层采用 RBF 作为神经元激活函数, 并与输出层之间以一定的权值实行全连接; 输出层则是对隐层神经元输出的线性组合, 输出神经元数目由所需要区分的模式数目决定. 对于 DMZI 系统的动作识别情况而言, 如图 5 所示, 需馈入  $(Q+1)$  维向量  $\mathbf{F} = [E_0, E_1, \dots, E_{Q-1}, ZCR]$ , 输出为  $P$  个动作的判决值  $Z_1, \dots, Z_P$ , 这些判决值由下式算出

$$Z_p = \sum_{i=1}^h \omega_{i,p} \cdot \rho(\mathbf{F}, \mathbf{c}_i), \quad p = 1, \dots, P, \quad (13)$$

其中,  $h$  为隐层神经元数目,  $\mathbf{c}_i$  和  $\omega_{i,p}$  分别是第  $i$  个隐层神经元所对应的中心和权重,  $\rho(\mathbf{F}, \mathbf{c}_i)$  为 RBF, 通常定义为样本数据  $\mathbf{F}$  到数据中心  $\mathbf{c}_i$  之间欧氏距离的单调减函数, 本文选用高斯函数作为 RBF. 按照 (13) 式算出  $Z_1, \dots, Z_P$  后, 取其最大值来判断入侵动作的类别 (一共可识别  $P$  种入侵动作).

图 5 的 RBF 网络的训练过程如下: 对于已知入侵事件类别 (假设为第  $p$  种,  $p = 1, \dots, P$ ) 的特征向量, 将对应输出  $Z_p$  标记为 1, 其余标记为 0, 以训练过程中实际  $Z_p$  值和标记值的均方误差 (mean square error, MSE) 为向导, 对多个用于训练的特

征向量做处理, 不断地优化隐层的 RBF 的各参数 (包括平均值  $c_1, \dots, c_h$ 、方差  $\sigma_1, \dots, \sigma_h$ ) 以及隐层和输出层之间的权值  $\omega_{i,p}$  ( $i \in [1, h], p \in [1, P]$ ).

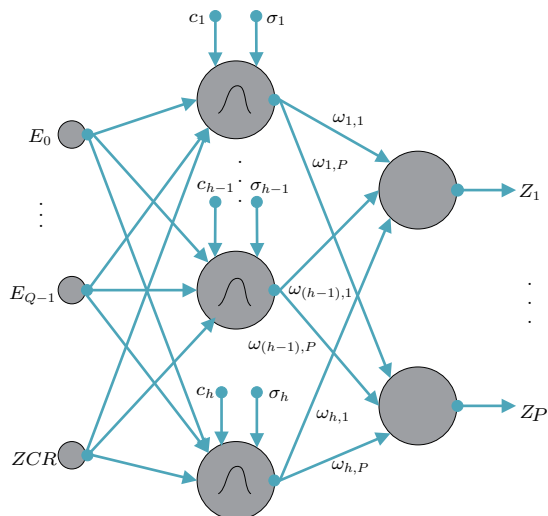


图 5 RBF 神经网络结构图

Fig. 5. RBF neural network architecture.

图 5 的 RBF 网络的测试过程如下: 将未标记分类的特征向量馈入训练好的网络, 借助已优化后的网络参数, 算出输出值  $Z_1, \dots, Z_P$ , 取其最大值来确定当前输入特征向量的所属分类.

## 5 实验结果与分析

### 5.1 综合特征提取

实验在激光源为 1550 nm 的分布式反馈激光、光强为 3.5 mV 的 DMZI 分布式光纤传感系统上进行. 为提高识别精度, 将总长度为 2.25 km 的传感光缆上下环绕固定于围栏上. DAQ1 采样率  $f_s = 10$  kHz, 记录时间为 3 s. 对 4 类常见入侵事件: 攀爬围栏、敲击光缆、晃动和盗剪进行 480 次数据采集, 每类入侵事件重复次数为 120 次.

特征向量长度的选取主要出于以下两方面的考虑: 一方面, 考虑到要识别  $P = 4$  类入侵事件, 为保证模式识别分类的准确度, 特征向量长度  $Q + 1$  应大于或等于所要识别的事件数目 4; 另一方面, 因为采用过长的特征向量会使得特征提取的计算复杂度增加, 所以  $Q$  值又不宜过大. 基于以上考虑, 本实验将全相位子滤波器数目设置为  $Q = 3$ , 从而特征向量  $\mathbf{F}$  长度为 4 (文献 [15] 的特征向量长度为 6).

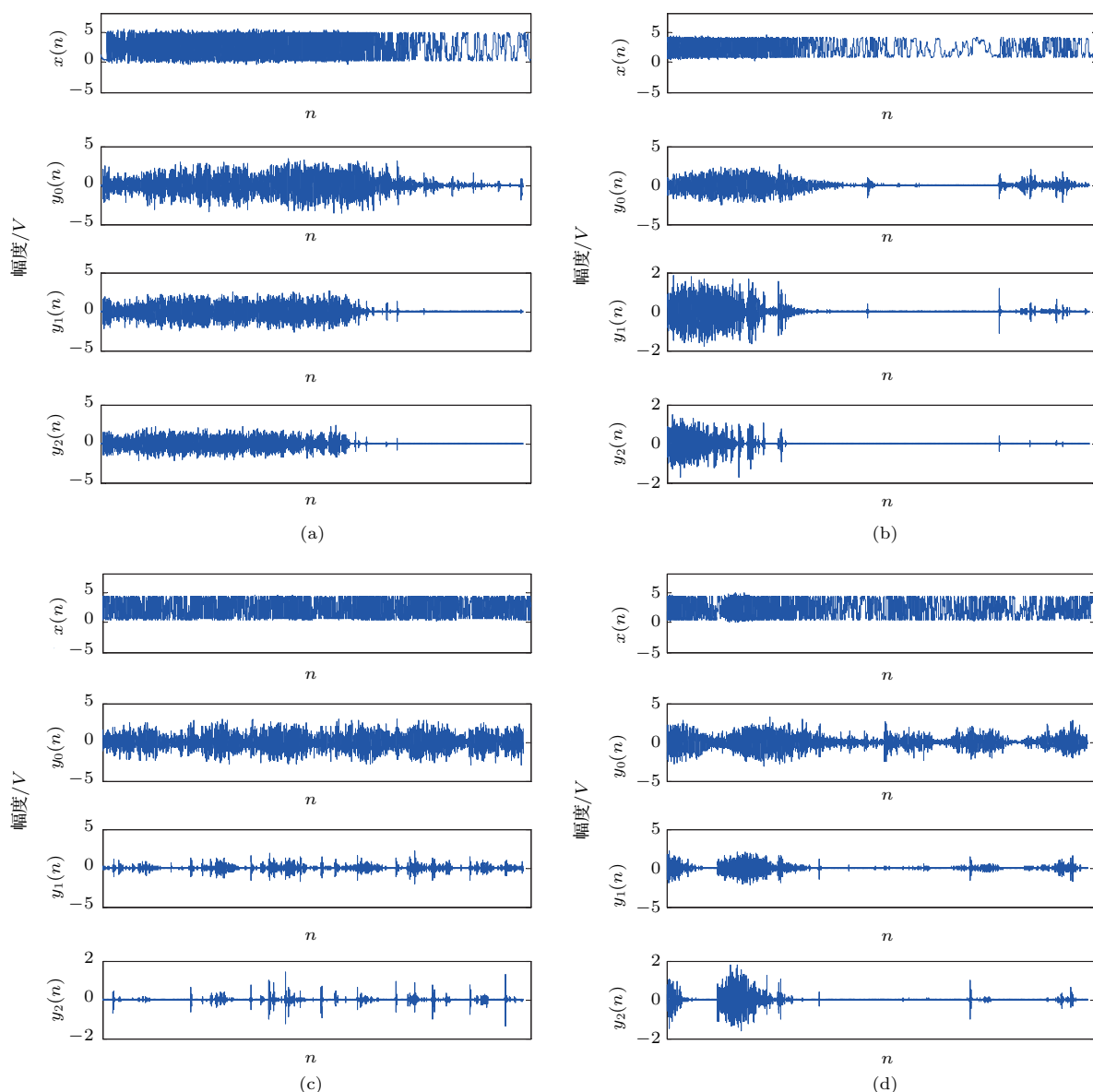


图6 滤波器组处理结果 (a) 攀爬; (b) 敲击; (c) 晃动; (d) 剪切

Fig. 6. The results of filter bank based processing: (a) Climbing; (b) knocking; (c) waggling; (d) cutting.

设定滤波器频率向量长度  $N = 256$ , 则频率分辨率  $\Delta f = f_s/N = 39.0625$  Hz. 分别对非入侵样本以及入侵样本做FFT统计分析, 得到滤波器的截止频率  $f_e = 220$  Hz,  $f_u = 4000$  Hz. 因此, 全相位滤波器组的通带宽度为  $B = f_u - f_e = 3780$  Hz, 由(4)和(6)式可确定参数  $e = 6$ ,  $m = 32$ , 由(5)式可估算出子滤波器的通带范围分别为  $f \in [234.375, 1484.375]$  Hz,  $f \in [1484.375, 2734.375]$  Hz,  $f \in [2734.375, 3984.375]$  Hz. 4类入侵信号以及经过全相位滤波器组处理后的各路子信号波形如图6所示.

从图6可看出, 4类动作的原始信号  $x(n)$  波形差别不明显; 经过全相位滤波器组处理后, 其输出

信号  $y_0(n) \sim y_2(n)$  呈现出很明显的差异, 这保证了后续模式识别的准确度.

依据(9)–(12)式, 可算出综合特征向量  $\mathbf{F} = [E_0, E_1, E_2, ZCR]$ . 为更突出地表达各类入侵事件特征向量的特征, 对每类事件包含的所有样本的综合特征向量取平均, 得到如图7所示的平均综合特征向量.

从图7可看出, 各类事件的综合特征向量具有明显区别: 攀爬信号变化最快, 具有最大的ZCR; 晃动信号的功率值  $E_0$  最大,  $E_1, E_2$  则远小得多, 即  $E_0 \sim E_2$  变化最为剧烈; 剪切信号  $E_0$  值高于敲击信号的  $E_0$  值,  $E_0 \sim E_2$  的变化更剧烈些, 且ZCR最小.



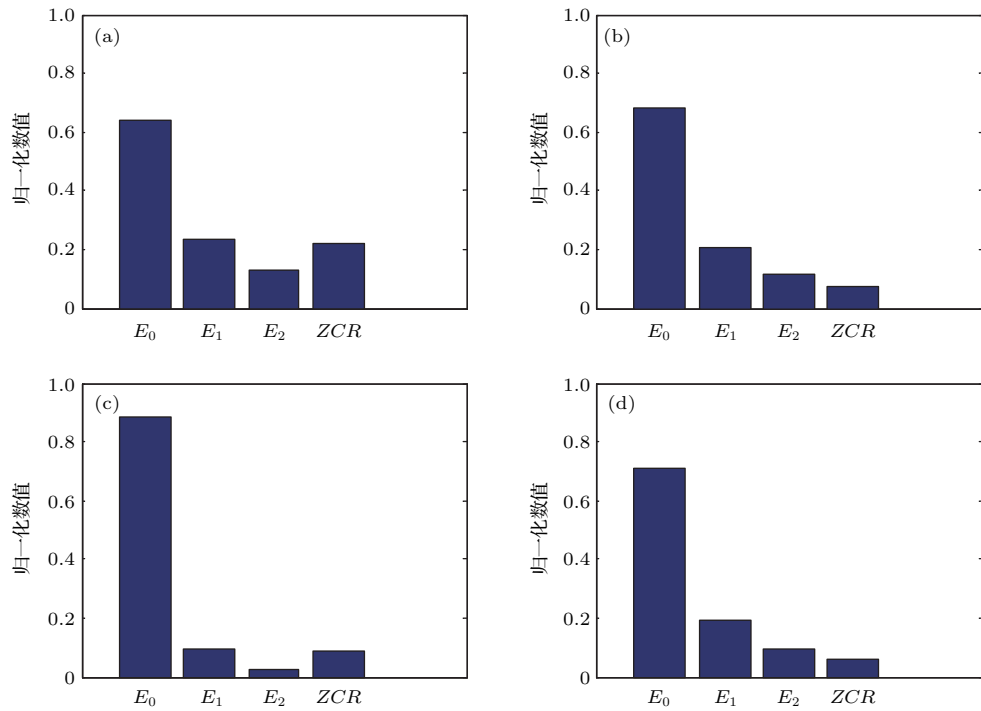


图7 四种入侵事件的平均特征向量 (a) 攀爬; (b) 敲击; (c) 晃动; (d) 剪切

Fig. 7. Averaged feature vectors of four intrusions: (a) Climbing; (b) knocking; (c) wagging; (d) cutting.

## 5.2 模式识别结果

本实验采用图5的RBF神经网络进行模式识别, 具体参数设置如下: 最小MSE值预设设为0.0442289; 最大神经元数目 $h$ 为30. 神经元数目将会逐渐增加, 直到MSE满足预设要求. 将神经网络的4个输出 $\mathbf{Z} = [Z_1, Z_2, Z_3, Z_4]$ 分别表示攀爬、敲击、晃动、剪切入侵事件. 尽管采用较多的训练样本会提高识别的精度, 但这会增加处理时间, 为权衡以上两点, 本实验共采集480组数据, 其中, 每种入侵信号的训练样本数设为50, 测试样本数设为70. 表1列出了最终的识别成功率, 并与EMD方法进行了比较.

表1 两种方法的模式识别率

Table 1. Pattern recognition rates of two methods.

方法	模式识别率/%			
	攀爬围栏	敲击光缆	晃动光缆	剪切光缆
EMD方法	87.30	70.9	99.7	85.10
本文方法	96.86	70.86	100	86.57

从表1可以看出, 本文方法平均识别率为88.5725%, EMD方法的平均识别率为85.75%, 故本文方法总体识别精度高于EMD方法. 具体而言,

本文方法的识别精度最高可达100%(晃动事件), 攀爬事件和剪切事件的识别率均高于EMD方法, 敲击事件的识别率接近于EMD方法. 其主要原因在于: 1) 本文方法采用了综合特征向量(EMD方法只用了单一的峭度特征向量)对入侵事件做了更全面的描述; 2) 本文引入了各子通道的耦合程度非常小的全相位滤波器组(EMD方法各次迭代得到的IMF之间耦合仍较大).

从表2可以看出: 在特征提取阶段, 本文方法的提取速度明显快于EMD方法, 处理时间仅约为EMD方法的1/4. 其主要原因在于: 1) 本文方法采用的全相位滤波器组以流水线方式工作, 避开了EMD方法的复杂迭代过程; 2) 本文方法的特征向量长度仅为4, 比EMD方法更短(其长度为6). 在模式识别阶段, 虽然两种方法都采用RBF神经网络进行识别, 但同样因为输入更短的特征向量的缘故, 本文方法的识别时间仍低于EMD方法.

表2 两种方法的处理时间

Table 2. Time cost of two methods.

方法	处理时间/s	
	特征提取	模式识别
EMD方法	6.1719	1.08027
本文方法	1.5622	0.65240

## 6 结 论

本文提出的基于综合特征向量的DMZI入侵事件识别方法, 由于有机地融合了全相位滤波理论、神经网络分类技术、时频域联合特征表达技术, 因而兼顾了高识别精度和高效率. 实验结果验证了本文方法相比于现有的EMD方法的这两大优势. 因所采用的传感光缆长达2.25 km, 可识别范围达到近2 km. 鉴于光纤周界安防系统对识别精度和效率的突出需求, 本文方法具有广泛的应用前景.

## 参考文献

- [1] Rangaswamy S, van Doorn E 2012 *US Patent* 8 232 878
- [2] Girao P M B S, Postolache O A, Faria J A B, Pereira J M C D 2001 *IEEE Sens. J.* **1** 322
- [3] Gong H, Song H, Zhang S 2014 *IEEE Sens. J.* **14** 777
- [4] Yu S Y, Sun S L 2008 *Laser & Infrared* **34** 345 (in Chinese) [于胜云, 孙胜利 2008 激光与红外 **34** 345]
- [5] Fan Z M 2008 *China Security & Protection* **3** 42 (in Chinese) [樊治敏 2008 中国安防 **3** 42]
- [6] Sun Q Z, Liu D M, Liu H R, He Y, Yuan J G 2006 *Proc. SPIE* **6344** 63440K
- [7] Sun Q Z, Liu D M, Liu H R, Shum P 2007 *Proc. SPIE* **6781** 67814D
- [8] Xie S R, Zhang M, Lai S R, Liao Y B 2010 *Proc. SPIE* **7677** 76770A
- [9] Jiang L H, Yang R Y 2012 *J. Comput.* **7** 1453
- [10] Juarez J C, Maier E W, Choi K N, Taylor H F 2005 *IEEE J. Lightw. Technol.* **23** 2081
- [11] Xie S R, Zou Q L, Wang L W, Zhang M, Li Y H, Liao Y B 2011 *IEEE J. Lightw. Technol.* **29** 362
- [12] Huang X D, Yu J, Liu K, Liu T G, Chen Q N 2014 *IEEE Photon. Technol. Lett.* **26** 1956
- [13] Liu L, Sun W, Zhou Y, Li Y, Zheng J, Ren B T 2014 *Pattern Recognition* (Berlin Heidelberg: Springer) pp595–603
- [14] Mahmoud S S, Visagathilagar Y, Katsifolis 2012 *Photon. Sens.* **2** 225
- [15] Liu K, Tian M, Liu T G, Jiang J F, Ding Z Y, Chen Q N, Ma C Y, He C, Hu H F, Zhang X Z 2015 *IEEE J. Lightw. Technol.* **33** 4885
- [16] Li K Y, Zhao X Q, Sun X H, Wan S R 2015 *Acta Phys. Sin.* **64** 054304 (in Chinese) [李凯彦, 赵兴群, 孙小蕊, 万遂人 2015 物理学报 **64** 054304]
- [17] Huang X D, Jing S X, Wang Z H, Xu Y, Zheng Y Q 2015 *IEEE Trans. Signal Process.* **64** 1173
- [18] Wang Z H, Huang X D 2009 *All Phase Spectrum Analysis and Filtering Technology of Digital Signal* (Beijing: Publishing House of Electronics Industry) pp14–31 (in Chinese) [王兆华, 黄翔东 2009 数字信号全相位谱分析与滤波技术 (北京: 电子工业出版社) 第14—31页]
- [19] Huang X D, Wang Y D, Liu K, Liu T G, Ma C Y, Chen Q N 2016 *IEEE Photon. J.* **8** 1
- [20] Huan H X, Hien T T H, Tue H H 2011 *IEEE Trans. Neural Netw.* **22** 982
- [21] Lyons W B, Ewald H, Lewis E 2002 *J. Mater. Process. Technol.* **127** 23
- [22] Huang X D, Wang Y D, Liu K, Liu T G, Ma C Y, Tian M 2016 *IEEE J. Lightw. Technol.* **34** 5049

# High-efficiency intrusion recognition by using synthesized features in optical fiber perimeter security system<sup>\*</sup>

Huang Xiang-Dong<sup>1)</sup> Zhang Hao-Jie<sup>1)</sup> Liu Kun<sup>2)</sup><sup>†</sup>  
Ma Chun-Yu<sup>2)</sup> Liu Tie-Gen<sup>2)</sup>

1) (School of Electrical and Information Engineering, Tianjin University, Tianjin 300072, China)

2) (College of Precision Instrument and Opto-electronics Engineering, Tianjin University, Tianjin 300072, China)

( Received 24 December 2016; revised manuscript received 29 March 2017 )

## Abstract

In an optical fiber perimeter security system, due to the fact that a large quantity of samples are collected in the process of data acquisition, this heavy data burden inevitably degrades the efficiency and accuracy of intrusion recognition. Hence, it is urgent to remove the redundancy of the collected data records, which essentially requires to describe event features in a concise and proper way. In this paper, we propose a synthesized feature based intrusion recognition method, which is especially suitable to describing the fiber intrusion vibration signals with both wide bandwidth and high nonstationarity. Firstly, the all-phase filter bank characterized by large sidelobe attenuation and high flexibility of coefficient configuration, is employed to parallelly divide the input signal into multiple frequency channels, from which the power values can be accurately calculated. Secondly, the crossing rate of the input signal is combined with these power values to construct a synthetic feature vector, in which both the time-domain information and frequency-domain information are incorporated together. Finally, these synthetic feature vectors are fed into a radial-basis-function network based classifier to recognize 4 common intrusions (climbing, knocking, wagging and cutting). Essentially, the high efficiency of our proposed scheme lies in the parallel pipeline mode of the configurable filter bank and simple calculation of features, which facilitates speeding up the intrusion recognition. The high accuracy of our proposed scheme lies in two aspects: 1) the all-phase filter bank possesses small inter-channel interference, which helps to reduce the inter-coupling between output power values; 2) the synthesis of both frequency-domain information and time-domain information ensures the completeness of feature description. Experiments show that the sensing range of the proposed scheme can reach 2.25 km. Moreover, compared with the empirical mode decomposition based method, the proposed method not only improves the precision, but also significantly speeds up the recognition.

**Keywords:** optical fiber perimeter security, intrusion recognition, synthesized features, filter bank

**PACS:** 42.81.Pa, 42.79.Ci, 45.70.Qj

**DOI:** 10.7498/aps.66.124206

<sup>\*</sup> Project supported by the National Natural Science Foundation of China (Grant Nos. 61671012, 61475114).

<sup>†</sup> Corresponding author. E-mail: [beiyangkl@tju.edu.cn](mailto:beiyangkl@tju.edu.cn)