

基于 ARMA 建模与 Sigmoid 拟合的光纤周界安防入侵事件识别

黄翔东^{1**}, 王碧瑶^{1***}, 刘琨^{2*}, 刘铁根²

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

摘要 在实际的光纤周界安防系统中,既要求判断入侵事件类别,又要求对各类事件发生的可能性做出全面评估。对此提出一种基于自回归滑动平均(ARMA)建模与 Sigmoid 概率拟合的入侵事件识别方法。在判断入侵事件类别方面,将光纤振动信号的 ARMA 建模系数与信号自身过零率相结合,构造特征向量,并将其馈入支持向量机(SVM),实现对攀爬、敲击、晃动、剪切、脚踢和撞击 6 种常见的入侵动作的识别;在评估各类事件的发生可能性方面,引入 Sigmoid 模型,对训练模式的 SVM 的各输出值作参数拟合,进而将测试样本的 SVM 值代入各自 Sigmoid 模型中完成评估。现场实验表明,该方法对 6 类常见入侵事件的平均识别率达到 87.14%,且可提供各类事件的发生概率参考值,因而具有较高的实用价值。

关键词 光纤光学; 传感器; 光纤周界安防; 入侵事件识别; ARMA 建模; 概率输出

中图分类号 V211

文献标志码 A

doi: 10.3788/CJL202047.1006004

Intrusion Event Identification for Fiber Perimeter Security System Based on ARMA Modeling and Sigmoid Fitting

Huang Xiangdong^{1**}, Wang Biyao^{1***}, Liu Kun^{2*}, Liu Tiegeng²

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

²Department of Precision Instruments and Optoelectronics Engineering, Tianjin University, Tianjin 300072, China

Abstract In a practical optical fiber perimeter security system, not only the discrimination of multiple events but also the comprehensive probability evaluation of these events is required. Therefore, this paper proposes a recognition scheme combining autoregressive moving average (ARMA) modeling with Sigmoid probability fitting. In event discrimination, both the ARMA coefficients and the zero-crossing rate of an optical fiber vibration signal are incorporated into a feature vector, which is then fed into a support vector machine (SVM) to recognize six types of common intrusion events: climbing, knocking, wagging, cutting, kicking, and crashing. In comprehensive probability evaluation, the SVM training pattern outputs are used to fit the parameters of a Sigmoid function. Then, the SVM outputs of the test patterns are substituted into this fitted Sigmoid model to yield the expected result. Field experiments reveal that the average recognition rate of six intrusion events by the proposed scheme reaches 87.14%. Moreover, the occurrence probabilities of all intrusion events can be provided as references, thereby presenting vast potential for future applications.

Key words fiber optics; sensors; optical fiber perimeter security; intrusion events recognition; ARMA modeling; probability output

OCIS codes 060.2370; 060.2330; 060.2310

1 引 言

近年来,分布式光纤技术被广泛应用于周界安

防领域,因其具有对压力及振动敏感的特点,得到了广泛的应用。在光纤周界安防系统^[1-3]中,以采用相位调制型光纤传感技术的双马赫-曾德干涉仪

收稿日期: 2020-05-06; 修回日期: 2020-05-07; 录用日期: 2020-06-19

基金项目: 国家自然科学基金(61671012)、国家重大科学仪器设备开发专项(2013YQ030915)

* E-mail: beiyangkl@tju.edu.cn; ** E-mail: xdhuang@tju.edu.cn; *** E-mail: wby915@tju.edu.cn

(DMZI)分布式光纤传感系统^[4-5]为代表,相比于传统的周界安防系统(如红外线安防系统^[6]、电子围栏安防系统^[7]),具有灵敏度高、响应速度快等优点,已被广泛应用于海底^[8]、机场^[9]、周界安防^[10-11]等周界安全防护领域。然而随着时代的发展,入侵事件趋于多样化。客观上,需要研发出既可实现高精度入侵事件识别,又可全面评估出各类事件发生可能性的方案。

提高入侵事件识别精度的关键在于,对端点检测^[12]之后的光纤振动信号进行有效的特征描述。现有的光纤扰动信号的特征提取方式有小波分解法^[13]、阈值判断法^[14]和经验模态分解法^[15-16](EMD)等,然而这些方法最多只能识别4类入侵事件,并且难以同时拥有高效率和高识别率,如:文献[13]提出基于小波分解和支持向量机(SVM)相结合的方法,其特征向量是通过将原信号分解为不同频带并计算不同频带的能量^[17]来得到的,然而频带严格划分带来的限制使得该方法往往伴随有巨大的计算量,识别效率较低;文献[14]提出的基于多特征值阈值判断的方法,虽然很好地利用了信号的不同特征,但有限范围的划分使得其仅能识别3类事件(车辆、机器及行人),而这无法满足对于多类人为事件的识别。文献[15]提出基于经验模式分解(EMD)和径向基函数(RBF)神经网络^[18-19]相结合的方法,该方法对信号进行分解,通过计算固有模态函数(IMF)的峭度值,构成特征向量,相比于前两个文献中使用的方法,该方法能够以较高精度识别4类入侵,然而该特征提取方法要经历多次迭代,计算量过大,识别效率不高,并且还会出现模态混叠,影响信息的表述。近年来,随着深度学习和神经网络的兴起,卷积神经网络(CNN)^[20]也开始在光纤周界安防中使用起来,卷积神经网络虽然可以达到较

高的识别率,但需要大量的数据与时间来进行训练,在时效性和应用性上存在不足。

为实现多类入侵事件的高精度和高效率识别,本文提出一种基于自回归滑动平均模型(ARMA)建模^[21-22]的入侵模式识别方法。该方法利用ARMA建模对光纤振动信号进行拟合,提取建模系数,再对信号进行描述,提取整段信号的过零率(ZCR, R_{zc}),最后综合生成最终的特征向量,并将特征向量输入SVM进行训练分类。另外,为克服现有方案无法全面评估各类事件发生概率的缺陷,本文提出基于Sigmoid参数建模的方法。实验表明,本文所使用的方法能够对6类入侵事件进行有效的区分,平均识别率趋近于90%,且可为计算各类事件的发生概率提供参考,更适于实际应用。

2 入侵识别系统体系结构

2.1 DMZI 分布式光纤传感系统

图1为DMZI扰动系统结构示意图。其工作原理可简述如下:激光器发射的激光经可变光衰减器(VOA)和耦合器C1后平均分成两个分支,这两分支的光被传输至DMZI(由耦合器C4、C5和一根电缆组成)中,利用其中的偏振控制器(PC)与保偏器(PM)控制其各自的极化状态^[23]。这两束光分别沿顺时针(CW)和逆时针(CCW)方向传播,并在耦合器C4和C5中发生干涉。最终由光电探测器(PD1和PD2)检测两个信号,由数据采集卡(DAQ1和DAQ2)采集两个信号(为了保持入侵事件检测的高灵敏度,两个数据采集卡均选用量化位数为14 bit的NI系列的采集卡),最后由工业计算机(IPC)进行处理。当D点发生入侵时,相位模拟的干扰信号有两个分支,通过解调和进一步的识别算法可以从这两个分支中提取事件类型信息(位置和类型)。

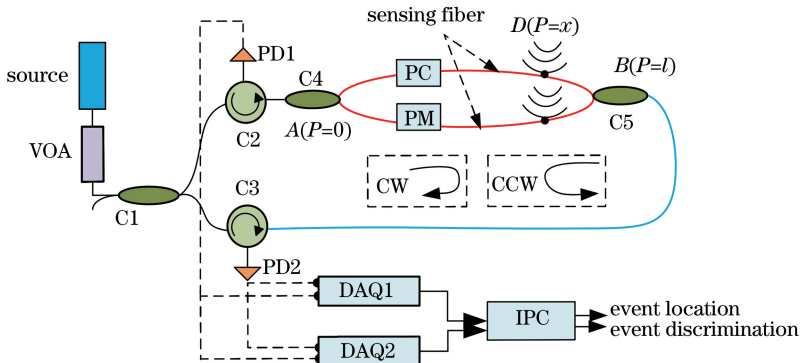


图1 DMZI 分布式光纤传感系统原理图

Fig. 1 Schematic diagram of DMZI disturbed optical fiber sensing system

本文主要针对事件识别方法进行研究,所使用的信号是已经经过端点检测的信号。

2.2 识别流程图

图2给出入侵事件识别流程,主要包含三部分:1)对入侵信号进行端点检测^[24],得到入侵事件发生的端点位置;2)采用合适的特征提取方法,对信号进行贴切的特征描述,从而得到特征向量 F ;3)选择分

类器对特征向量进行训练及识别,判断入侵动作所属类别的同时,给出各类事件的发生概率 p_1, p_2, \dots, p_Q 。在以上步骤中,特征提取算法是影响系统对入侵动作识别表现的最主要因素。其中,对于端点检测部分,可以采用之前在文献[12]中所提的方法对信号进行处理,本文主要研究特征提取和事件识别两个问题,具体流程如图3所示。

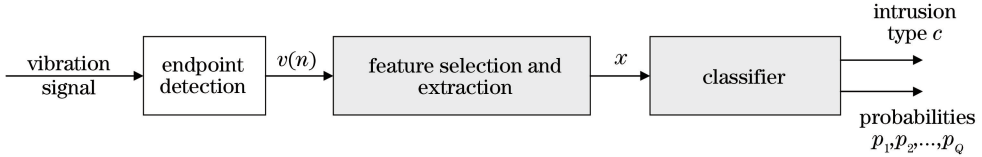


图2 入侵事件识别流程图

Fig. 2 Flowchart of intrusion event discrimination

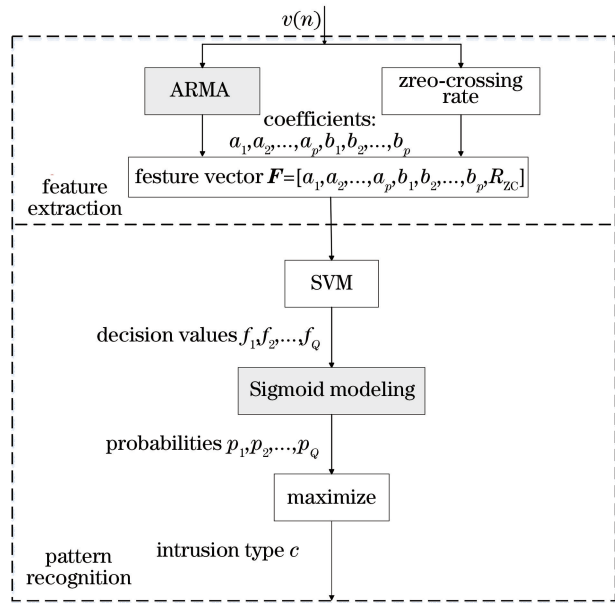


图3 本文所提入侵事件识别方法流程图

Fig. 3 Flowchart of the proposed intrusion event discrimination scheme

图3中主要包括特征提取和模式识别两个部分。

特征提取:对信号 $v(n)$ 进行 $ARMA(p, q)$ 建模,同时计算信号的过零率。将建模得到的系数 $a_1, a_2, \dots, a_p, b_1, b_2, \dots, b_q$ 和整体过零率相结合,得到最终的特征向量 $F = [a_1, a_1, \dots, a_p, b_1, b_1, \dots, b_q, R_{zc}]$ 。

模式识别:将特征提取得到的特征向量以及对应标签馈入 SVM 中进行训练,通过采用 Sigmoid 函数拟合,可以将原本的判决值输出转换为概率输出,从而得到 Q 类事件的发生概率 p_1, p_2, \dots, p_Q ,最终的入侵事件类型可表示为

$$c = \arg \max_{q=1,2,\dots,Q} p_q \quad (1)$$

3 特征提取

3.1 特征向量构造

本文所提方法的特征向量主要由 ARMA 系数和 ZCR 相结合获得,特征向量构造时主要考虑以下几点:

1) 特征向量应该尽量对信号进行全方位的描述,本文方法中系数 a_1, a_2, \dots, a_p 和 b_1, b_2, \dots, b_q 为频域信息,过零率为时域信息,因此,所提取特征包含信号两方面特征;

2) 特征向量长度应该尽可能短,从而降低模式识别的复杂度,也就是说 $p+q$ 的值应尽可能小;

3) 特征向量应该从本质上对扰动信号进行描述,本文方法利用信号建模,能够描述信号的谱特征,可从本质上反映出信号的变化规律。

3.2 基于 ARMA 建模的谱描述

众所周知,谱分析分为经典谱分析和现代谱分析两种。其中,现代谱分析是一种基于数据建模的方法,其本质是通过将观测数据 $v(n)$ 视为白噪声 $w(n)$ 输入一个线性系统 $H(z)$ 来获取,从而对信号进行数据建模。根据统计信号处理理论,观测信号自相关 $r_{VV}(n)$ 和白噪声自相关 $r_{WW}(n)$ 之间的关系可表示为

$$r_{VV}(n) = r_{WW}(n) * h(n) * h(-n), \quad (2)$$

其中, $h(n)$ 是线性系统的冲击响应,“ $*$ ”表示卷积操作。对(2)式进行傅里叶变换可以得到:

$$P_{VV}(\omega) = P_{WW}(\omega) \cdot |H(j\omega)|^2, \quad (3)$$

其中, $P_{VV}(\omega)$ 和 $P_{WW}(\omega)$ 表示观测信号和白噪声的功率谱密度, $H(j\omega)$ 是线性系统的频率响应,可

表示为

$$H(j\omega) = H(z) \Big|_{z=\exp(j\omega)} \quad (4)$$

因为白噪声的功率谱在整个频带均匀分布,因此 $P_{ww}(\omega)$ 可表示为

$$P_{ww}(\omega) = \sigma_w^2, \quad (5)$$

其中, σ_w^2 为噪声方差(因其不是频域特征,故没纳入特征向量 \mathbf{F} 中),从而可将(3)式表示为

$$P_{VV}(\omega) = \sigma_w^2 |H(j\omega)|^2. \quad (6)$$

$H(z)$ 的一般形式为

$$H(z) = \frac{B(z)}{A(z)} = \frac{1 + b_1 z^{-1} + \dots + b_q z^{-q}}{1 + a_1 z^{-1} + \dots + a_p z^{-p}}. \quad (7)$$

对于(7)式,当 $B(z) = 1$, $H(z)$ 被称为 AR (autoregressive) 模型;当 $A(z) = 1$, $H(z)$ 被称为 MA (moving average) 模型;当 $A(z) \neq 1$ 和 $B(z) \neq 1$, $H(z)$ 被称为 ARMA 模型。其中 ARMA 模型是研究随机过程中最经典的一种方法,对比其他两种方法,该方法具有较精准的谱估计及优良的谱分辨率性能。

(7)式的 ARMA 建模要求确定 p 个 AR 系数 $a_i (i=1, 2, \dots, p)$ 和 q 个 MA 系数 $b_j (j=1, 2, \dots, q)$ (p 和 q 分别为 AR 阶数和 MA 阶数)。本文利用经典 Burg 算法^[22] 获得这些参数的精确估计,以确定特征向量 \mathbf{F} 的前 $p+q$ 个分量。

3.3 基于过零率的时间描述

作为常用的时域描述指标,过零率^[25] 反映了信号变化的快慢程度,可表示为

$$R_{ZC} = \frac{\sum_{n=1}^L |\text{sign}[x(n)] - \text{sign}[x(n-1)]|}{2L}, \quad (8)$$

其中,“sign”表示取符号操作,表达式为

$$\text{sign}[x(n)] = \begin{cases} 1, & x(n) \geq 0 \\ -1, & x(n) < 0 \end{cases} \quad (9)$$

通过将过零率与之前求取的 ARMA 系数相结合,可构造出特征向量 $\mathbf{F} = [a_1, a_1, \dots, a_p, b_1, b_1, \dots, b_q, R_{ZC}]$, 该特征向量不仅包括信号的时域特征,同时包含信号的频域特征,从而可进一步提高模式识别的精度。

4 基于 Sigmoid 拟合的 SVM

为了实现多分类和概率输出,本文方法采用了基于 Sigmoid 函数拟合的 SVM^[26] 进行模式分类。通过 Sigmoid 拟合将 SVM 的决策值转换为发生概

率,从而实现最终的概率输出。

假定对于给定的输入特征向量 \mathbf{F} , 在训练阶段,训练得到 Q 个决策函数 $f_q (q=1, 2, \dots, Q)$, 那么对于要决策的样本事件,比较各函数的计算值大小,可得最终的判断类型,即

$$c = \arg \max_{q=1, 2, \dots, Q} f_q. \quad (10)$$

进一步地,将训练样本的对应标签 $y \in \{1, 2, \dots, Q\}$ 改写为长度为 Q 的向量 $\mathbf{v} = [v(1), v(2), \dots, v(q), \dots, v(Q)]^T$, 并且满足以下两个约束条件

$$\sum_{q=1}^Q v(q) = 1 \text{ 和 } v(q) = \begin{cases} -\frac{1}{Q-1}, & q \neq y \\ 1, & q = y \end{cases}. \quad (11)$$

从(10)式和(11)式可以看出, f_y 越大,入侵事件越接近 y 类。

为探索某类事件的 SVM 的输出决策值与该类事件的发生概率之间的关系,不妨收集该类事件的足够量的训练样本,将两者样本分布拟合成某函数曲线。以敲击事件为例,统计该事件的概率值和决策值的变化曲线,如图 4 所示。

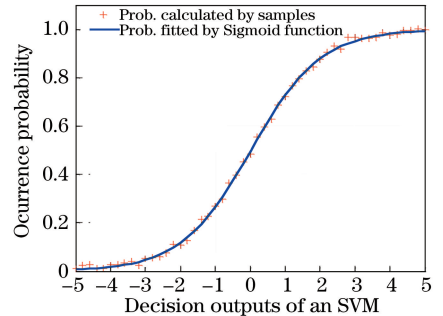


图 4 敲击事件基于 Sigmoid 的概率拟合曲线

Fig. 4 Sigmoid based fitness for occurrence probabilities of the knocking intrusion

从图 4 可以看出,其样点分布与 Sigmoid 函数非常近似,故对于任意第 y 类入侵事件,可以将其训练样本的发生概率和其对应的 SVM 决策输出 f_y 利用 Sigmoid 函数进行拟合,即

$$P(c = y | f_y) = \frac{1}{1 + \exp(A_y f_y + B_y)}, \quad y \in \{1, 2, \dots, Q\}. \quad (12)$$

也就是说,一旦确定了 Q 组拟合参数对 $\{(A_y, B_y), y=1, 2, \dots, Q\}$, 对任意测试样本而言,将其 SVM 输出的 Q 个输出值 $f_q (q=1, 2, \dots, Q)$ 代入(12)式的 Q 个函数中,即可获得所有的 Q 个事件发生概率的评估值。

5 实验结果与分析

5.1 特征提取

实验装置如图 1 所示。光源为波长为 1550 nm, 功率为 5 mW 的分布式反馈激光器。DAQ1 和 DAQ2 的数据采样率分别设置为 10 MSa/s 和 1 MSa/s, 采样时间分别为 0.3 s 和 3 s。DAQ1 和 DAQ2 获取的数据在 IPC (CPU: i7-4790K, RAM: 8 Gb) 上进行处理。为了提高检测灵敏度, 将长度为 2.25 km 的线缆以正弦方式系在围栏上。对 6 类入侵事件: 攀爬、敲击、晃动、剪切、脚踢和撞击进行数据采集, 每类入侵事件重复次数为 120 次, 其中 50 组用于训练, 70 组用于测试。

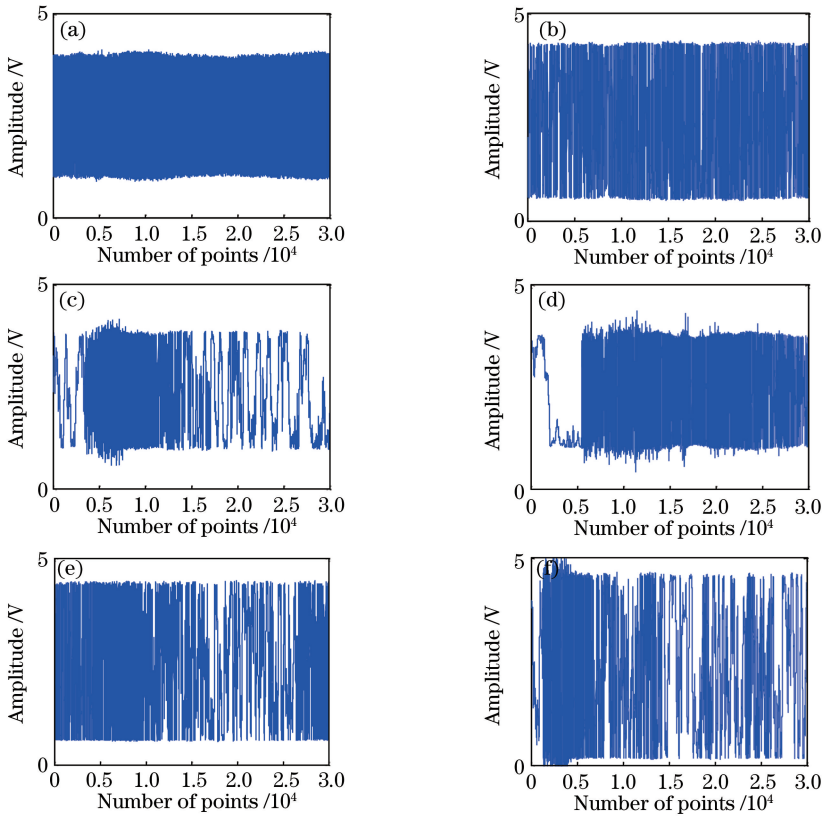


图 5 6 类入侵事件波形。(a) 攀爬; (b) 敲击; (c) 晃动; (d) 剪切; (e) 脚踢; (f) 撞击
Fig. 5 Waveforms of 6 intrusion events. (a) Climbing; (b) knocking; (c) wagging; (d) cutting; (e) kicking; (f) crashing

除此之外, 从表 1 中可以看出, 在同一系统环境下, 本文所使用的方法相对于 EMD 来说在效率方面有大幅度提升, 这也使得本文方法相较于 EMD 更适用于实际的现场操作。

5.2 模式识别

本实验将本文方法与现有的 EMD 方法进行比较, 其中 EMD 方法所用的特征向量长度为 6, 并且

考虑到特征向量的长度对于特征提取的计算复杂度有影响, 并且依据实际实验结果可以看出, 低阶的 ARMA 足以反映信号特征, 最终的 AR 阶数 p 设置为 2, MA 阶数 q 设置为 1, 也就是说最终的特征向量为 $\mathbf{F}=[a_1, a_2, b_1, R_{zc}]$, 总长度为 4。

图 5 给出了 6 类入侵事件的波形特征图, 相应的每类入侵事件的平均特征向量如图 6 所示。根据图 6 可以看出, 不同入侵事件的特征向量之间具有较大差异: 攀爬动作具有最大的过零率; 晃动动作 AR 系数全为负, MA 系数为正; 脚踢和撞击动作的第一个 AR 系数均为负, 其他为正, 但脚踢动作的 MA 系数明显高于撞击动作; 敲击动作和剪切动作特征向量较为相似, 但剪切动作的系数 a_2 和过零率稍高于敲击动作。

表 1 两种方法对入侵事件识别的时间花费对比
Table 1 Time consumption of two methods for intrusion event discrimination unit: s

Method	EMD	Proposed
Time consumption	13.274	1.057

对 IMF 求取峭度值, 计算量巨大。表 2 给出了两种方法分别对于 4 类入侵事件 (攀爬、敲击、晃动、剪

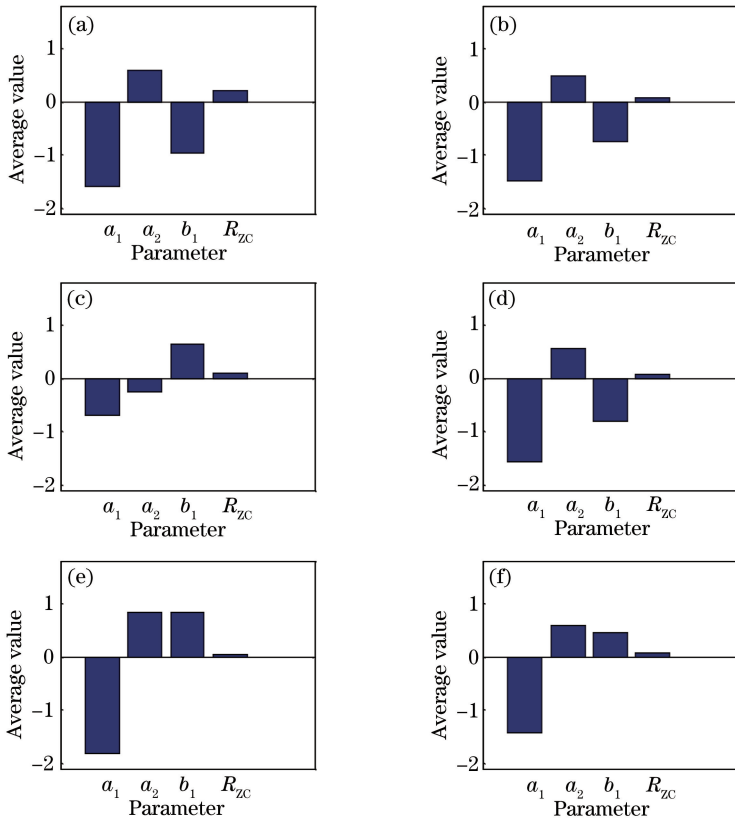


图 6 6 种入侵事件的平均特征向量。(a)攀爬;(b)敲击;(c)晃动;(d)剪切;(e)脚踢;(f)撞击

Fig. 6 Averaged feature vectors of 6 intrusion events. (a) Climbing; (b) knocking; (c) waggling; (d) cutting; (e) kicking; (f) crashing

切)的识别率。从表 2 可看出,本文方法对于 4 类入侵事件的平均识别率为 90.36%,EMD 方法的平均识别率为 85.75%,本文方法的总体识别精度明显高于 EMD 方法。

为进一步比较本文方法与 EMD 方法的性能,添加了两个新动作脚踢和撞击,并分别用两种方法对这 6 类动作进行识别,得到的结果如表 3 所示。

表 2 两种方法对于 4 类入侵事件的模式识别率

Table 2 Pattern recognition rates of two methods for 4 intrusion events unit: %

Method	Climbing	Knocking	Wagglng	Cutting
EMD	87.3	70.9	99.7	85.1
Proposed	100	70	100	91.43

表 3 两种方法对于 6 类入侵事件的模式识别率

Table 3 Pattern recognition rates of two methods for 6 intrusion events unit: %

Method	Climbing	Knocking	Wagglng	Cutting	Kicking	Crashing
EMD	71.43	65.71	98.57	77.14	42.86	24.29
Proposed	100	75.71	97.14	91.43	85.71	72.86

从表 3 可看出:1)当识别种类增加为 6 时,EMD 方法的平均识别精度从 85.75%降低到 63.33%,也就是说 EMD 方法不能有效地描述新增的两类动作;2)本文方法在增加入侵种类之后,所受的影响不大,从 90.36%降低到 87.14%,仅降低了 3.22%;3)本文方法对于新增的两类入侵动作的识别准确率均在 72%以上,说明能够有效识别新增动作,相反,EMD 方法对于两类新动作的识别率均在 50%以下,无法满足实际应用需求。

另外,表 4 给出除攀爬事件之外的 5 类事件错分的例子,同时给出出现错分时,判断为其他类型的概率值。从表 4 可以看出,对于错分的样本,通常正确类型的概率值仅次于最大值,且接近错分类型的概率值,远大于其他类型的概率值。从表 4 最后一列可看出,在错分事件中,当考虑最大两个概率值时,除晃动事件外,识别错误率均降到了 5%以下,而晃动事件的识别率也增加到了 90%以上。因此,在进行入侵识别时,应考虑两个具有较大概率值的识别结果。

表 4 6 类入侵事件的发生概率估计

Table 4 Estimation of occurrence probabilities for 6 intrusion events

unit: %

Real event	Recognition result	Climbing	Knocking	Wagging	Cutting	Kicking	Crashing	Error rate (when two events with maximum probability values are taken into account)
Knocking	Cutting	0.79	44.23	0.61	52.80	0.38	0.19	1.97
Cutting	Knocking	0.73	62.76	0.75	35.18	0.39	0.19	2.05
Wagging	Crashing	1.35	3.10	33.56	2.98	2.50	56.52	9.93
Kicking	Crashing	0.68	1.22	1.27	0.73	36.22	59.88	3.90
Crashing	Kicking	0.56	1.07	1.22	0.6	53.36	43.19	3.45

6 结 论

本文提出的基于 ARMA 建模的 DMZI 入侵事件识别方法,有机融合了 ARMA 建模理论、支持向量机分类及概率输出技术,能够高效地识别更多类型的入侵事件,同时输出各类事件的发生概率。现场实验证明了本文方法比现有的 EMD 方法可识别更多类别并拥有高精度的优点,具有广泛的应用前景。

参 考 文 献

[1] Liu X, Jin B Q, Bai Q, et al. Distributed fiber-optic sensors for vibration detection[J]. *Sensors*, 2016, 16(8): 1164.

[2] Girao P M B S, Postolache O A, Faria J A B, et al. An overview and a contribution to the optical measurement of linear displacement [J]. *IEEE Sensors Journal*, 2001, 1(4): 322-331.

[3] Gong H P, Song H F, Zhang S L, et al. Curvature sensor based on hollow-core photonic crystal fiber Sagnac interferometer [J]. *IEEE Sensors Journal*, 2014, 14(3): 777-780.

[4] Sun Q Z, Liu D M, Liu H R, et al. Distributed disturbance sensor based on a novel Mach-Zehnder interferometer with a fiber-loop [J]. *Proceedings of SPIE*, 2005, 6344: 63440K.

[5] Liu D, Shum P. Distributed fiber-optic sensor with a ring Mach-Zehnder interferometer [J]. *Proceedings of SPIE*, 2007, 6781: 67814D.

[6] Yu S Y, Sun S L. The design of multi-wireless infrared detectors and intelligent burglary-resisting system [J]. *Laser & Infrared*, 2008, 38(4): 345-347.

于胜云, 孙胜利. 多路无线红外探测智能安防系统设计 [J]. *激光与红外*, 2008, 38(4): 345-347.

[7] Fan Z M. Design principle and application status of tension electronic fence perimeter protection alarm system [J]. *China Security & Protection*, 2008(3):

42-45.

樊治敏. 张力式电子围栏周界防范报警系统设计原理及应用现状 [J]. *中国安防*, 2008(3): 42-45.

[8] Xie S R, Zhang M, Lai S R, et al. Positioning method for dual Mach-Zehnder interferometric submarine cable security system [J]. *Proceedings of SPIE*, 2010, 7677: 76770A.

[9] Jiang L H, Yang R Y. Identification technique for the intrusion of airport enclosure based on double Mach-Zehnder interferometer [J]. *Journal of Computers*, 2012, 7(6): 1453-1459.

[10] Juarez J C, Maier E W, Choi K N, et al. Distributed fiber-optic intrusion sensor system [J]. *Journal of Lightwave Technology*, 2005, 23(6): 2081-2087.

[11] Xie S R, Zou Q L, Wang L W, et al. Positioning error prediction theory for dual Mach-Zehnder interferometric vibration sensor [J]. *Journal of Lightwave Technology*, 2011, 29(3): 362-368.

[12] Huang X D, Yu J, Liu K, et al. Configurable filter-based endpoint detection in DMZI vibration system [J]. *IEEE Photonics Technology Letters*, 2014, 26(19): 1956-1959.

[13] Liu L, Sun W, Zhou Y, et al. Security event classification method for fiber-optic perimeter security system based on optimized incremental support vector machine [C] // Li S, Liu C, Wang Y. *Pattern Recognition, CCPR 2014. Communications in Computer and Information Science*. Berlin, Heidelberg: Springer, 2014, 484: 595-603.

[14] Qu H Q, Zheng T, Pang L P, et al. A new detection and recognition method for optical fiber pre-warning system [J]. *Optik*, 2017, 137: 209-219.

[15] Liu K, Tian M, Liu T G, et al. A high-efficiency multiple events discrimination method in optical fiber perimeter security system [J]. *Journal of Lightwave Technology*, 2015, 33(23): 4885-4890.

[16] Chen Y, An W Y, Liu H L, et al. Application of improved empirical mode decomposition algorithm in fiber Bragg grating perimeter intrusion behaviors classification [J]. *Chinese Journal of Lasers*, 2019,

- 46(3): 0304003.
 陈勇, 安汪悦, 刘焕淋, 等. 改进经验模态分解算法在光纤布拉格光栅周界入侵行为分类中的应用[J]. 中国激光, 2019, 46(3): 0304003.
- [17] Li K Y, Zhao X Q, Sun X H, et al. A regular composite feature extraction method for vibration signal pattern recognition in optical fiber link system [J]. *Acta Physica Sinica*, 2015, 64(5): 054304.
 李凯彦, 赵兴群, 孙小茜, 等. 一种用于光纤链路振动信号模式识别的规整化复合特征提取方法[J]. 物理学报, 2015, 64(5): 054304.
- [18] Huan H X, Hien D T T, Tue H H. Efficient algorithm for training interpolation RBF networks with equally spaced nodes[J]. *IEEE Transactions on Neural Networks*, 2011, 22(6): 982-988.
- [19] Lyons W B, Ewald H, Lewis E. An optical fibre distributed sensor based on pattern recognition [J]. *Journal of Materials Processing Technology*, 2002, 127(1): 23-30.
- [20] Chen P C, You C T, Ding P F. Pattern recognition of intrusion events in perimeter defense areas of optical fiber[J]. *Chinese Journal of Lasers*, 2019, 46(10): 1006001.
 陈沛超, 游赐天, 丁攀峰. 光纤周界防区入侵事件的模式识别研究 [J]. 中国激光, 2019, 46(10): 1006001.
- [21] Huang S J, Shih K R. Short-term load forecasting via ARMA model identification including non-Gaussian process considerations [J]. *IEEE Transactions on Power Systems*, 2003, 18(2): 673-679.
- [22] Erdem E, Shi J. ARMA based approaches for forecasting the tuple of wind speed and direction[J]. *Applied Energy*, 2011, 88(4): 1405-1414.
- [23] Chen Q N, Liu T G, Liu K, et al. An elimination method of polarization-induced phase shift and fading in dual Mach-Zehnder interferometry disturbance sensing system [J]. *Journal of Lightwave Technology*, 2013, 31(19): 3135-3141.
- [24] Huang X D, Wang Y D, Liu K, et al. Event discrimination of fiber disturbance based on filter bank in DMZI sensing system [J]. *IEEE Photonics Journal*, 2016, 8(3): 1-14.
- [25] Liu K, Weng L F, Jiang J F, et al. Zero-crossing rate based efficient identification of intrusion events in fiber perimeter security systems [J]. *Acta Optica Sinica*, 2019, 39(11): 1106002.
 刘琨, 翁凌峰, 江俊峰, 等. 基于过零率的光纤周界安防系统入侵事件高效识别 [J]. 光学学报, 2019, 39(11): 1106002.
- [26] Smola A J, Bartlett P, Schölkopf B, et al. *Probabilities for SV machines*[M]. Cambridge, MA: MIT Press, 2000: 61-74.
- [21] Huang S J, Shih K R. Short-term load forecasting