文章编号:1003－6199(2025)02－0172－05 DOI:10.16339/j.cnki.jsjsyzdh.202502030

基于光纤光栅振动传感技术的智慧站场周界入侵行为在线报警技术

张演义†,杨昕谅,李波,郝卓卓,邬建国,王宝宝

(国家管网集团北京管道有限公司,陕西 榆林 719000)

摘 要:为了提高智慧站场周界的安全性,提出了一种智慧站场周界入侵行为在线报警技术。利用光纤光栅振动传感技术,通过控制参数初始化,提取智慧站场周界入侵信号的特征,构建入侵概率矩阵,计算入侵行为的状态转移概率,建立入侵行为与观测攻击指令序列之间的关系。在检测到入侵行为的最佳状态时,系统发出周界入侵行为报警信号,实现智慧站场周界入侵行为的在线报警。实验结果表明,该技术能够有效发出报警信号,并将漏报率和误报率控制在10%以内。

关键词:入侵行为;安全性;特征提取;探测原理;光纤光栅振动传感技术;在线报警

中图分类号:TP277 **文献标识码**:A

On-line Alarm Technology for Perimeter Intrusion Behavior of Smart Station Based on Fiber Bragg Grating Vibration Sensing Technology

ZHANG Yanyi†, YANG Xinliang, LI Bo, HAO Zhuozhuo, WU Jianguo, WANG Baobao

(PipeChina Beijing Pipeline Co., Ltd., Yulin, Shaanxi 719000, China)

Abstract: In order to improve the security of the smart station perimeter, a smart station perimeter intrusion online alarm technology is proposed. By utilizing fiber Bragg grating vibration sensing technology and controlling parameter initialization, the characteristics of the intrusion signal around the smart station are extracted, an intrusion probability matrix is constructed, the state transition probability of the intrusion behavior is calculated, and the relationship between the intrusion behavior and the observation of the attack instruction sequence is established. When the optimal state of intrusion behavior is detected, the system sends a perimeter intrusion behavior alarm signal to achieve online alarm of intelligent station perimeter intrusion behavior. The experimental results show that this technology can effectively send out alarm signals and control the missed and false alarm rates within 10%.

Key words: invasion behavior; security; feature extraction; detection principle; fiber Bragg grating vibration sensing technology; online alarm

智慧站场周界是站场区域与外部空间隔绝的一种安全防护隔离带,一般使用铁栏杆或砖砌筑而成,可以保证站场区域的安全,对维护智慧站场良好秩序具有非常重要的意义[1]。在复杂多变和不确定性因素增强的网络背景下,智慧站场周界与自动化控制相关的入侵问题日益突出,造成了非常严重的后果[2]。现有的周界侵入预警方法受环境、气象和电磁等因素的干扰,辨识效果较低,检测手段以门限判定为主,缺乏有效的追踪手段,虚警率高[3]。随着智慧站场的规模不断扩张,复杂网络中

收稿日期:2023－07－07

作者简介:张演义(1978—),男,山东德州人,本科,工程师,研究方向:天然气输气站场自动控制。

† **通信联系人**,E-mail: hemushi6z@163.com

传统的攻击手段正逐步渗透到智慧站场中，而对周界的保护又是保证智慧站场安全性和高效使用的前提，所以，对智慧站场周界入侵行为的在线预警显得尤为迫切。

许奕杰等[4]为解决现有周界入侵预警技术在复杂天气环境下易出现虚警率高、无法识别入侵类型等问题，构建一种新型的 AE-LSTM 网络结构。首先对输入信号进行隐性编码，通过提取隐性编码的特征，构造与时间序列信息相结合的特征矢量矩阵，以减少网络结构的复杂性。通过仿真实验验证了所建模型在识别过程中的虚警率、识别精度和计算复杂性等方面的优越性。傅荟瑾等[5]为了提升高铁列车周界环境的监控能力，开展高铁列车周界入侵的多传感器信息融合技术研发与应用研究。首先，通过对高铁周界各类典型环境进行深入剖析，将感知技术与毫米波雷达、激光雷达等感知技术的各自特点相结合，实现感知技术与环境相适配，并通过“一景一案”的方式，构建高铁周边环境的监控方法。其次，给出了监控系统的技术框架，实现了监控系统的各个模块设计。探索以视频为基础的雷达-视频-雷达多传感器数据融合方法，并通过实验进行验证，最终形成一套适用于高铁轨道周边环境的多传感器数据融合方法，为高铁轨道周边环境中的人为侵入和外来物体侵入提供可靠的数据支持。

为此，将光纤光栅振动传感技术应用到了智慧站场周界入侵行为预警中，从而提前给出相应防范措施。

1　智慧站场周界入侵行为在线报警技术设计

1.1　基于光纤光栅振动传感技术探测入侵行为

在探测智慧站场周界的入侵行为时，如果光纤光栅振动传感器受到外力的作用，悬浮在光纤光栅上方的质点在相应的频率和幅度下被强迫振荡，由此改变了布拉格的波长[6]。通过测量布拉格波长的变化幅度，判断智慧站场周界的入侵行为，图 1 给出了光纤光栅振动传感技术的探测原理。

当智慧站场周界发生入侵行为时，光纤光栅传感器会将由入侵行为引起的波长变化波形传输到振动传感器中，由探测软件平台判断是否有真正的入侵行为发生[7]。

当智慧站场周界发生了真正的入侵行为时，对光纤光栅振动传感器的探测参数进行初始化处理[8]，构建入侵概率矩阵，表示为：

$$\boldsymbol{W}=\frac{Z_i+Z_j}{p}-\boldsymbol{G}_s\frac{p_{\mathrm{d}}\times g_{\mathrm{d}}}{\boldsymbol{G}} \tag{1}$$

式中，p 表示入侵行为 Z_i 转换成入侵行为 Z_j 的概率，$\boldsymbol{G}_{\mathrm{s}}$ 表示周界入侵行为的概率矩阵，g_{d} 表示入侵行为的随机观测值，$\boldsymbol{G}$ 表示入侵行为转换的概率矩阵，p_{d} 表示随机观测值的概率。

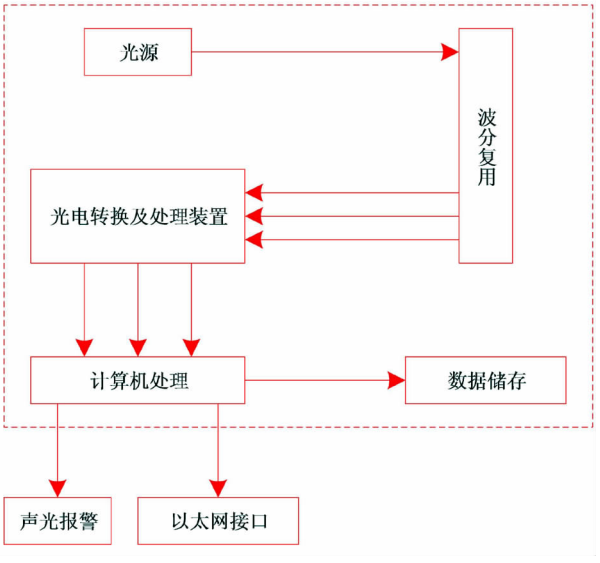

图 1　光纤光栅振动传感技术的探测原理

将智慧站场周界入侵行为的特征向量作为光纤光栅振动传感器的输入[9]，探测周界入侵行为，表示为：

$$C_j=\frac{p_{\mathrm{h}}+Z_{\mathrm{g}}}{S_{\mathrm{d}}\times b_{\mathrm{s}}}\times\frac{p_{\mathrm{x}}}{L_{\mathrm{t}}-W}+Q \tag{2}$$

其中，S_{d} 表示入侵行为的属性，b_{s} 表示缩放因子，L_{t} 表示入侵行为探测的时间长度，p_{h} 表示入侵行为探测结果的后验概率，Z_{g} 表示光纤光栅振动传感器的状态观测值，p_{x} 表示入侵行为探测的校验概率，Q 表示入侵行为探测的最优解。

根据光纤光栅振动传感技术的原理，探测智慧站场周界的入侵行为。

1.2　提取智慧站场周界入侵信号特征

光纤光栅振动传感技术在探测入侵行为时，容易受到外部干扰，通过提取入侵信号特征，过滤掉入侵行为的干扰成分。在智慧站场中，通过时频特征分析[10]，建立入侵信号在智慧站场周界传输的结构模型，表示为：

$$A(x)=\varphi\left\{u_{\mathrm{n}}(x)\frac{\mathrm{e}^{-2\pi\mathrm{j}\kappa_n(t)}}{\mathrm{e}^{-2\pi f_c}}[t-\kappa_{\mathrm{n}}(x)]\right\} \tag{3}$$

式中，φ 表示滤波运算，$u_{\mathrm{n}}(x)$ 表示入侵行为信号在站场周界的主频特征，j 表示虚数单位，$\kappa_{\mathrm{n}}(t)$ 表示入侵行为信号在时间维度上的延时量，$\kappa_{\mathrm{n}}(x)$ 表示入侵行为信号在站场周界传输的延时

函数，f_c 表示通信信号在智慧站场的调制频率。

如果入侵信号在智慧站场中的传输路径有 N 条，利用入侵信号在外界干扰下的传递函数，建立入侵信号的特征分布函数，表示为：

$$g(t)=A(x)\sum_{i=1}^{p}s_i p(t-t_i) \tag{4}$$

式中，i 表示求和索引变量，p 表示共有 p 个不同因素，s_i 表示入侵信号在站场周界的损失成分，t 表示智慧站场的传播延时，t_i 表示入侵信号的攻击延时。

根据入侵信号的特征分布函数，对入侵信号的分布空间进行重构[11]，得到入侵信号在站场边界的频谱特征，表示为：

$$\begin{cases} y(t)=\sqrt{f}x(ft) \\ T_y(t,k)=\dfrac{T_x}{g(t)}\left(ft,\dfrac{k}{f}\right) \end{cases} \tag{5}$$

式中，f 表示入侵行为的采样频率，$x(ft)$ 表示经过采样频率调整后的原始入侵信号的表示形式，k 表示智慧站场的网络带宽，$T_x()$ 表示频谱生成的时间窗口函数，$y(t)$ 表示入侵行为的时间序列，$T_y(t,k)$ 表示入侵信号在频域内的伸缩尺度，$g(t)$ 表示调整因子。

入侵信号的频谱特征会受到智慧站场的运行频率影响，导致信号受到干扰[12]，利用滤波器对入侵信号进行抗干扰抑制，得到：

$$s_n=a_i\sum_{i=1}^{M_{\mathrm{AR}}}x_{n-i}+b_j\sum_{j=0}^{M_{\mathrm{MA}}}a_n \tag{6}$$

式中，a_i 表示入侵信号的采样幅值，M_{AR} 表示参与当前时刻信号值计算的过去时刻信号值的数量，b_j 表示入侵信号的振荡幅值，x_{n-i} 表示信号均值相同的时序，M_{MA} 表示参与计算的系数 b_j 的个数以及与之相关的当前时刻信号 a_n 的组合情况，a_n 表示当前时刻的入侵信号幅值相关量。

通过入侵信号的抗干扰抑制，得到入侵信号的时域特征和频域特征，表示为：

$$\begin{cases} T_x(t,k)=x(t+2\tau)x^*(t-2\tau)\mathrm{e}^{-2\pi k\tau}\mathrm{d}\tau \\ T_y(t,k)=y(k+2\lambda)y^*(k-2\lambda)\mathrm{e}^{-2\pi\lambda\tau}\mathrm{d}\lambda \end{cases} \tag{7}$$

式中，λ 和 τ 表示入侵信号的衰减系数，x^* 和 y^* 表示时域共轭函数和频域共轭函数。

根据入侵信号的时域特征和频域特征组成，提取智慧站场周界入侵信号特征，即：

$$\chi=T_x(t,k)+T_y(t,k)+\frac{n(t)}{g(t)} \tag{8}$$

式中，$n(t)$ 表示入侵信号在智慧站场周界的相位变化幅值，$g(t)$ 表示入侵行为的主成分。

根据入侵信号在智慧站场周界传输的结构模型，建立入侵信号的特征分布函数，通过入侵信号的分布空间重构，利用滤波器对入侵信号进行抗干扰抑制，提取智慧站场周界入侵信号特征。

1.3 构建智慧站场周界入侵行为在线报警模型

以入侵信号特征为依据，得到入侵行为的隐含状态，在光纤光栅振动传感技术下[13]，将 α 时刻下的入侵行为 X_α 转移到 β 时刻下的入侵行为 X_β，利用式(9)给出转移概率：

$$P_{\alpha\beta}=P(X_\beta \mid X_\alpha) \tag{9}$$

利用输出概率矩阵描述入侵行为 X_β 与攻击指令 X_γ 之间的关系，根据式(9)的转移概率，计算入侵行为 X_β 观测到攻击指令 X_γ 的概率，公式为：

$$P_{\beta\gamma}=\frac{1}{P_{\alpha\beta}}P(X_\gamma \mid X_\beta) \tag{10}$$

为了预测智慧站场周界入侵行为在接下来的状态，定义一个预测模型 $R=\{r_1,r_2,\cdots,r_K\}$，t 时刻监测到的攻击指令为 $V_K=v_1,v_2,\cdots,v_T$，此时，根据入侵行为 X_β 观测到攻击指令 X_γ 的概率[14]，计算入侵行为在接下来出现的概率，具体步骤为：

Step1：当 $t=1$ 时，计算智慧站场周界入侵行为 r_1 与可观测攻击指令序列 v_1 之间的转移概率，公式为：

$$p_1(\sigma)=\pi_\sigma(r_1)b_\sigma(v_1) \tag{11}$$

式中，$\pi_\sigma(r_1)$ 表示入侵行为 r_1 的初始概率分布，$b_\sigma(v_1)$ 表示攻击指令序列 v_1 的初始概率分布。

Step2：当 $t\geqslant 1$ 时，在可观测攻击指令序列 v_T 下，计算第 σ 个入侵行为的最大概率，公式为：

$$p_t(\sigma)=\max\left[p_t(\beta)a_{\beta\sigma}\right]b_\sigma(v_T) \tag{12}$$

式中，$a_{\beta\sigma}$ 表示入侵行为 β 转移到 σ 的概率，$b_\sigma(v_T)$ 表示周界入侵行为 σ 被观测成 v_T 的概率。

Step3：确定入侵行为在 t 时刻的最佳状态[15]，发出周界入侵行为报警信号，即：

$$\psi_1(\sigma)=\arg\max\left[p_{t-1}(\beta)a_{\beta\sigma}\right]U_t^* \tag{13}$$

式中，$p_{t-1}(\beta)$ 表示 $t-1$ 时刻入侵行为的状态，U_t^* 表示入侵行为的最佳状态序列。

综上所述，通过预测入侵行为接下来的状态，实现智慧站场周界入侵行为的在线报警。

2 实验对比分析

2.1 实验环境

为了验证文中技术在智慧站场周界入侵行为报警中的有效性，设置了如下实验环境：

实验平台：Pentiunm4 3.6 GHz
操作系统：Red Hat Linux 8.07
内存：32 GB
RAM：256 MB
链路带宽：4 Mbps
传输半径：200 m
仿真时间：1000 s

实验过程中，将智慧站场周界节点的活动范围设置为 1000 m×500 m，一共包含 50 个节点，运动速度在 0～20 m/s 之间，仿真时，智慧站场内部节点的运动是在运动模型下，从一个节点向另一个节点运动，达到目标节点之后需要暂停一段时间，接着再选取一个新的目标点和速度，直到仿真结束。

2.2　实验数据

本文选择 4 类入侵行为攻击智慧站场周界，各种入侵行为的具体内容如表 1 所示。

表 1　入侵行为的内容

编号	入侵行为	内容
A	修改攻击	修改、删除与非法插入数据
B	抛弃攻击	攻击者只接收数据，不转发数据
C	假冒攻击	冒充其他周界节点发送数据
D	编造攻击	编制假数据进行发送

表 1 中，四种入侵行为的攻击方式不同，预警的效果也存在相应差异。

2.3　入侵行为报警

在对智慧站场周界的入侵行为进行报警之前，将入侵行为的报警阈值设定为 0.5，利用 1.2 节的方法提取入侵行为的特征，当入侵行为的特征值超过 0.5 时，需要发出报警信号进行报警，否则说明智慧站场周界能够抵御该入侵行为的攻击，保证智慧站场的安全，不需要报警。在表 1 的入侵行为中随机选取 100 份样本数据，利用光纤光栅振动传感技术探测智慧站场周界的入侵行为，结果如图 2 所示。

根据图 2 的结果可知，采用文中技术对智慧站场周界的入侵行为进行报警之前，光纤光栅振动传感技术能够探测到站场周界的入侵行为，并发出报警信号，提高智慧站场的安全性。

2.4　对比分析

为了突出文中技术在入侵行为报警中的优势，引入基于 AE-LSTM 网络模型的报警技术和基于多传感技术融合的报警技术作为对比，以漏报率和误报率为评价指标，计算式为：

$$\zeta = \frac{N_l}{N_{all}} \times 100\% \tag{14}$$

$$\varepsilon = \frac{N_f}{N_{ture}} \times 100\% \tag{15}$$

式中，N_l 表示遗漏掉的样本数量，N_{all} 表示入侵行为样本总数，N_f 表示错误报警的入侵行为，N_{ture} 表示发出报警信号的样本数量。

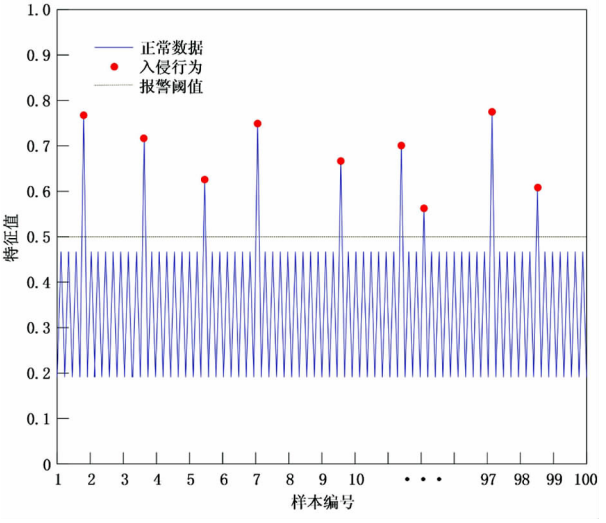

图 2　入侵行为探测结果

测试了入侵行为报警的漏报率和误报率，结果如图 3、图 4 所示。

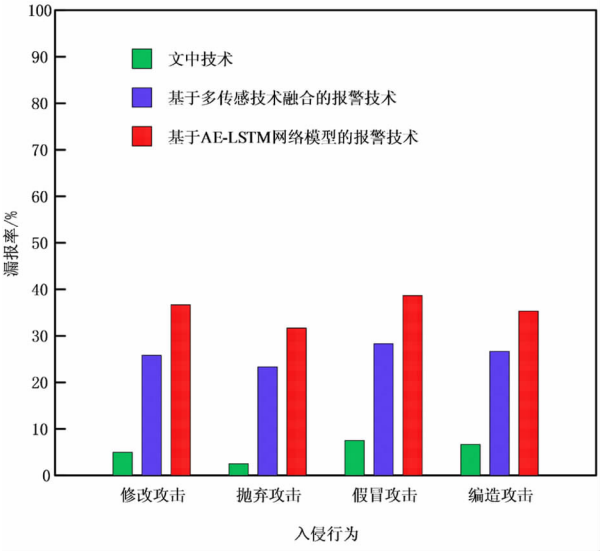

图 3　入侵行为报警的漏报率

从图 3 的结果可以看出，采用基于 AE-LSTM 网络模型的报警技术时，由于 AE-LSTM 网络模型在入侵行为隐性编码特征提取中比较单一，导致漏报率偏高。采用基于多传感技术融合的报警技术时，由于多个传感器共同探测时会互相干扰，出现了对入侵行为漏报的现象。而采用文中技术时，

能够根据光纤光栅振动传感技术的探测结果，提取入侵行为特征，降低了入侵行为的漏报率。

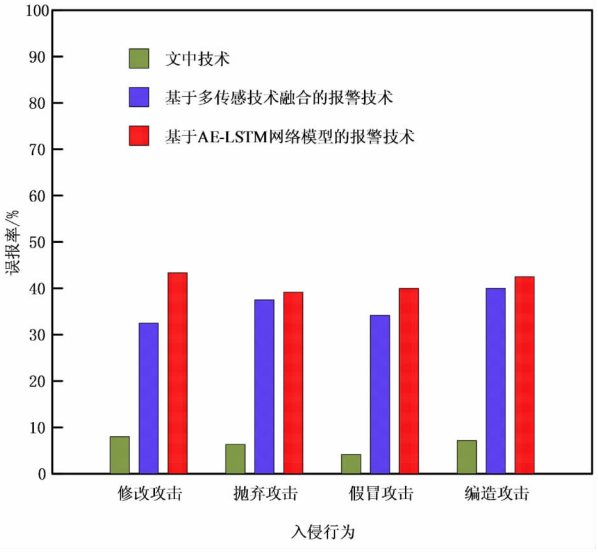

图 4 入侵行为报警的误报率

从图 4 的结果可以看出，与基于 AE-LSTM 网络模型的报警技术和基于多传感技术融合的报警技术相比，文中在光纤光栅振动传感技术下能够探测到入侵行为，将误报率控制在 10%以内，提高了入侵行为的报警精度。

3 结 论

提出了一种基于光纤光栅振动传感技术的智慧站场周界入侵行为在线报警技术，经过测试发现，该技术可以降低入侵行为报警的漏报率和误报率。本文研究虽然取得一定成果，但是还存在很多不足，在今后的研究中，希望可以考虑到光纤光栅振动传感技术的使用场景，避免噪声、滤波等因素影响入侵行为探测精度。

参考文献

[1] 王瑞，史天运，包云. 一种基于视频的铁路周界入侵检测智能综合识别技术研究[J]. 仪器仪表学报，2020，41(9)：188－195.

[2] 喻后聃，米秋实，赵栋，等. 基于一维卷积神经网络的光纤周界入侵模式识别[J]. 光子学报，2021，50(9)：95－105.

[3] 李创，孙子文. IWSN 中基于属性变化率的全局信任入侵检测[J]. 传感技术学报，2023，36(2)：294－300.

[4] 许奕杰，王嵘，万永菁，等. 基于 AE-LSTM 网络模型的机场周界入侵报警及分类算法[J]. 华东理工大学学报(自然科学版)，2021，47(3)：323－330.

[5] 傅荟瑾，郭鹏跃，徐成伟，等. 基于多传感技术融合的高速铁路周界入侵监测技术方案研究[J]. 铁道运输与经济，2022，44(9)：122－129.

[6] 李盛，邱阳，南秋明，等. 基于超弱光栅传感阵列的钻机违法入侵地铁线路识别定位方法[J]. 振动与冲击，2022，41(20)：202－207.

[7] 王瑞，李霄峰，史天运，等. 基于视频深度学习的铁路周界入侵检测算法研究[J]. 交通运输系统工程与信息，2020，20(2)：61－68.

[8] 程小辉，牛童，汪彦君. 基于序列模型的无线传感网入侵检测系统[J]. 计算机应用，2020，40(6)：1680－1684.

[9] 张侠. 深度学习网络的光通信系统入侵行为识别[J]. 微电子学与计算机，2020，37(4)：76－79.

[10] 吴虎，孔勇，王振伟，等. 基于 EMD 分解与 1-D CNN 算法的光纤振动信号的识别[J]. 激光与红外，2021，51(8)：1043－1049.

[11] 苏新，张桂福，行鸿彦，等. 基于平衡生成对抗网络的海洋气象传感网入侵检测研究[J]. 通信学报，2023，44(4)：124－136.

[12] 肖衡，龙草芳. 基于机器学习的无线传感网络通信异常入侵检测技术[J]. 传感技术学报，2022，35(5)：692－697.

[13] 刘拥民，杨钰津，罗皓懿，等. 基于双向循环生成对抗网络的无线传感网入侵检测方法[J]. 计算机应用，2023，43(1)：160－168.

[14] 刘洲洲，尹文晓，张倩昀，等. 基于离散优化算法和机器学习的传感云入侵检测[J]. 吉林大学学报(工学版)，2020，50(2)：692－702.

[15] 黄翔东，王碧瑶，刘琨，等. 基于 ARMA 建模与 Sigmoid 拟合的光纤周界安防入侵事件识别[J]. 中国激光，2020，47(10)：203－210.