

通信工程学院

毕业设计外文翻译

毕业设计题目：基于多传感器的

UGS 入侵目标识别系统设计

外文题目 The Design of the Instruction
Detection System Based on the UGS

专业：测控技术与仪器（信号处理与仪器）

学号：52160203

学生姓名：孙一诺

指导教师姓名：周求湛

指导教师职称：教授

日期：2020 年 1 月 7 日

基于一种状态网络的光纤 周界安全系统入侵识别方法

(Ningning Wang, Nian Fang, Lutang Wang)

摘要:为了准确有效地识别光纤周界安全系统中不同类型的入侵信号,提出了一种基于回声状态网络(ESN)的入侵信号识别方法。采用基于串联 Sagnac 干涉仪的周界安全系统,在实验室模拟了传感光纤的两种铺设的情况:附在物理围栏上或埋在地下,采集各种事件信号。预处理后的信号被输入到一个训练良好的 ESN 中,以识别不同类型的事件。事件信号段的最终识别结果是根据对应于该信号段的最主要分类标签来确定的。结果表明,两种产卵情况下的平均识别率分别为 98.75%和 100%。该方法不需要提取信号特征和大量样本来训练分类器模型。因此,该方法能够比其他方法更准确、更有效地进行入侵识别。该方法可望满足安全领域实际应用的要求。

关键词: 信号识别、光纤周界安全系统、回声状态网络(ESN)、识别率、在线 Sagnac 干涉仪

一、 介绍

近年来,分布式光纤传感技术因其作用在传感光纤上的振动信号进行检测和定位的能力以及灵敏度高、抗电磁干扰、价格低廉等优点而受到广泛关注。它可以作为安全领域的周界防御^[1-8]。光纤周界安全系统获取的不同类型的信号需要识别为非入侵事件或特定类型的入侵事件,以降低误报率。入侵识别方法越发到人们的重视,在周边安防中发挥着重要作用。方等人^[9]提出了一种基于步态特征的步行入侵信号识别方法。该方法只能区分非入侵事件和行走入侵事件。此外,当有异常步态者闯入时,误报率增加。此外,基于机器学习算法的入侵识别方法也很多。如将有监督人工神经网络与基于时域水平交叉特征的特征提取算法^[10]、 K 最近邻(KNN)分类器^[11]或支持向量机(SVM)分类器^[12-14]结合使用。然而,有时特征提取会由于水平阈值不同而产生偏差,缺乏准确的依据。KNN 算法计算

量大，需要大量内存。对于大型训练集，支持向量机分类器在训练阶段非常耗时。另有基于径向的两种集成方案。

采用基函数（RBF）神经网络分类器对入侵事件进行识别，一种是基于经验模式分解（EMD）和峰度特征的信号预处理^[15]，另一种是基于端点检测和滤波器组的特征提取^[16]。前者可以区分四种常见的入侵事件。后者不仅可以区分两种常见的入侵事件，还可以区分非入侵事件和入侵事件。然而，这两种方案的辨识过程比较复杂，辨识率有待提高。这些方法都难以满足实际应用对高 IRs 和简单识别过程的要求。

本文针对改进 IR、简化识别过程、节省分类器模型训练时间的需要，提出了一种基于回声状态网络（ESN）的识别方法。ESN 在许多领域都取得了很好的效果，包括动态模式识别或时间序列分类^[17-19]。然而，据我们所知，这是 ESN 首次用于识别光纤入侵信号。基于 ESN 的识别方法不需要提取信号特征。由于只需使用少量样本训练一个权值矩阵，因此训练 ESN 分类器模型也快速方便。通过适当的决策规则，该方法可以获得很高的 IR。利用该方法对基于 Sagnac 干涉仪的周界安全实验系统检测到的信号进行了识别。实验结果表明，该方法能够快速识别周界安全系统的信号。

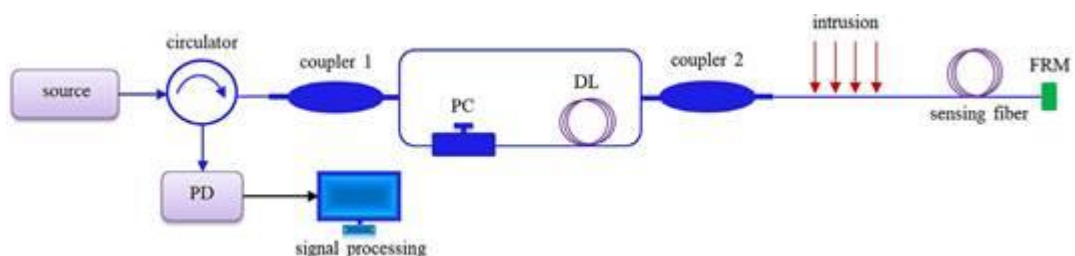


图 1-1 基于在线 Sagnac 干涉仪的光纤周界安全系统的示意图

二、 光纤周界安全系统

图 1-1 是基于在线 Sagnac 干涉仪的光纤周界安全系统的示意图^[4,9]。系统对外界振动信号引起的相位变化敏感，对环境的缓慢变化没有响应。这种直列式结构易于铺设。这些特点使该系统成为最有前途的周边安全系统之一。

在该系统中，来自宽带源的连续波形光通过环行器注入耦合器 1。光被分成两束，其中一束通过两个耦合器的光纤尾纤到达耦合器 2。然后，将光发射到法拉第旋转镜（FRM）的传感光纤中，反射光通过传感光纤、耦合器 2、延迟环

(DL) 和偏振控制器 (PC) 到达耦合器 1。另一束光通过 PC、DL、耦合器 2、传感光纤、FRM 和两个耦合器的光纤尾纤返回耦合器 1。两个光束具有相同的光路，并且可以在耦合器 1 中产生干扰。

当入侵作用于传感光纤时，光纤中光的相位将发生变化，从而导致从光探测器 (PD) 中显示的输出光强度发生变化。最后，信号处理单元对采集到的数据进行处理，得到不同事件的识别结果。

三、 回声状态网络

Herbert Jaeger 于 2001 年提出 ESN 作为递归神经网络 (RNN) 的一种新的设计和训练方法^[20]。它们简化了网络的训练过程，不需要大量的训练样本，而且在结构上比传统的 RNN 更容易确定。

图 2 示出 ESN 的架构^[20]。可见，ESN 由输入层、储层和输出层组成。在输入层，有 K 个输入节点。水库包含 N 个稀疏连接的内部节点。 N 称为 ESN 的大小。在输出层，有 L 个输出节点。 \mathbf{W}_{IN} 、 \mathbf{W} 、 \mathbf{W}_{back} 和 \mathbf{W}_{OUT} 分别是输入权重矩阵、内部权重矩阵、反馈权重矩阵和输出权重矩阵。 \mathbf{W}_{IN} 、 \mathbf{W} 和 \mathbf{W}_{back} 随机生成并保持固定。在训练阶段，通过一个线性回归算法只能得到 \mathbf{W}_{OUT} 。

伺服电机内部节点的状态更新方程可以表示为:

$$x(n+1) = f(Wx(n) + \mathbf{W}_{IN}u(n+1) + \mathbf{W}_{back}y(n)) \quad (3.1)$$

其中 f 是内部节点的激活函数， $x(n)$ 是节点的状态， $u(n)$ 是输入信号， n 是离散时间。网络的输出信号 $y(n)$ 为:

$$y(n+1) = f_{out}(\mathbf{W}_{OUT}x(n+1)) \quad (3.2)$$

其中 f_{out} 表示输出层中的输出函数。

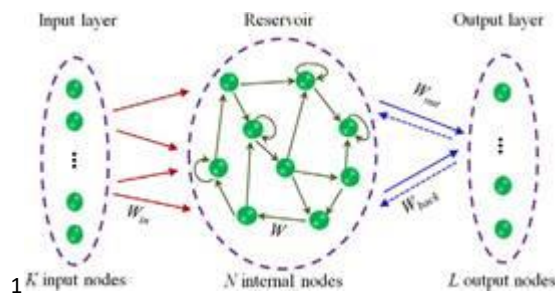


图 3-1 ESN 的体系结构。虚线箭头表示可选的反馈连接。

四、 基于 ESN 的入侵识别方法

我们使用 ESN 模型来识别不同的事件信号。ESNs 属于 RNNs，它能很好地解决光纤周界安全系统中的信号识别等与时间相关的问题。此外，储层的高维特征可以将输入信号扩展到高维空间，使信号识别更加容易，ESNs 的一致性和可分性也有利于信号的分类[21]。因此，ESN 算法适合于光纤入侵信号的识别。由于 ESN 极大地简化了 RNN 的训练过程，因此训练后的 ESN 可以直接对事件信号进行分类，而不是对其特征进行分类。也就是说，基于 ESNs 的识别方法不需要提取信号的特征，输入信号只是事件信号。在信号识别方面，ESN 优于其他 RNN。在后一种情况下，若不能提取出信号的主要特征，将导致训练时间过长，甚至出现维数灾难。

识别过程如下:首先，生成 ESN;然后在输入层将不同类型的原始事件信号作为输入数据进行预处理，进行事件识别。接下来，训练 ESN 并确定。最后，利用 ESN 对预处理后的信号进行分类。

4.1 ESN 的产生

ESN 的生成主要包括确定每一层的节点数、三个权矩阵、激活函数 f 和输出函数、光谱半径 (SR)，这是 ESN 的一个重要参数。输入层和输出层都由一个节点组成，用于输入预处理信号并获得输出信号。在储层中，储层的大小 N 是由经验决定的。如果 N 太小，ESN 的动态特性不够丰富；太大，计算时间过长，影响处理的及时性。 \mathbf{W}_{IN} 和 \mathbf{W} 是两个大小分别为 $N \times 1$ 和 $N \times N$ 的矩阵，根据一定的规则随机生成。为了简单起见，将 α 设为 0，即网络中不存在来自输出层的反馈。常见的激活函数有 sigmoid 和线性函数[22]。sigmoid 函数使内部节点具有非线性能力。线性函数为内部节点提供更短的内存容量。在大多数 ESN 中，选择线性函数作为输出函数，使得网络的训练能够获得全局最优解。当 SR 小于 1 时，在大多数情况下可以保证储层的回波状态特性[22]。

4.2 信号预处理

在光纤周界安全系统的实际应用中，不同类型的事件信号采集时间不同。事

件信号可被视为信号段或样本。由于它们的长度不同，将不同的信号段放入一个矩阵中作为水库的输入是不方便的。因此，将不同类型的事件信号段自由组合，端到端连接起来，形成一个长的一维时间序列作为样本集，即以串行方式将样本送入储层。事件信号类型的选择是基于光纤周界安全系统在现实中大多处于非入侵状态的考虑。因此，无论在训练阶段还是测试阶段，非侵入信号在输入数据中所占的比例都较大。训练样本集涵盖了各种事件信号。然而，测试样本集可以包括部分类型的事件信号。

然后对时间序列进行归一化处理，完成信号的预处理过程。预处理后的信号的第 i 个数据点可以根据以下公式得到：

$$y_i = (x_i - x_{min}) / (x_{max} - x_{min}) \quad (4.1)$$

其中 x_{min} 、 x_i 、 x_{max} 和 x_{min} 是第二个数据点，分别是整个时间序列的最小值和最大值。所有数据点的值都映射到 0 到 1 之间的范围。

4.3 ESN 训练

训练 ESN 是在适当的参数下，寻找最优的输出权矩阵。这里， W_{out} 是大小为 $1 \times N$ 的矩阵，其初始化为 0。对于栅栏安装型，训练样本集由非入侵事件和一种入侵事件组成。对于地理型，训练集的样本数相同，包括非入侵事件和两种入侵事件。两种光纤铺设方式的非入侵事件的含义不同，分别在第 5.1 节中定义。此外，还标记了不同类型的事件，即非入侵事件、入侵事件 1、入侵事件 2 和入侵事件 3 的输出信号分别被指定为“0”、“1”、“2”和“3”的标签。

对训练样本集进行预处理，输入到储层中进行 ESN 训练。内部节点的状态收集在矩阵 B 中。可通过式 (4) 获得。

$$W_{out} = pinv(B)T \quad (4.2)$$

其中 $pinv$ 是伪逆的。 T 是所需的输出信号。

4.4 ESN 测试

测试样本集经过预处理并驱动储层。根据式 (4.2) 得到网络的输出信号 $y(n)$ 。由于测试输出是一个连续信号，并且所需输出由“0”、“1”、“2”和“3”四个

离散标签组成，因此需要根据以下规则对输出信号进行量化。当输出信号的振幅大于 2.5、介于 1.5 和 2.5 之间或介于 0.5 和 1.5 之间时，相应的输出标签分别为“3”、“2”或“1”。其余部分对应于输出标签“0”。最后，识别结果是对所有的信号段进行分类，根据与信号段相对应的最主要输出标签是最终分类标签的判定规则。利用红外光谱对识别结果进行评价，结果如下：

$$IR = \frac{N_c}{N_a} \times 100\% \quad (4.3)$$

式中， N_c 是正确识别的段数， N_a 是测试样本集中测试段的总数。

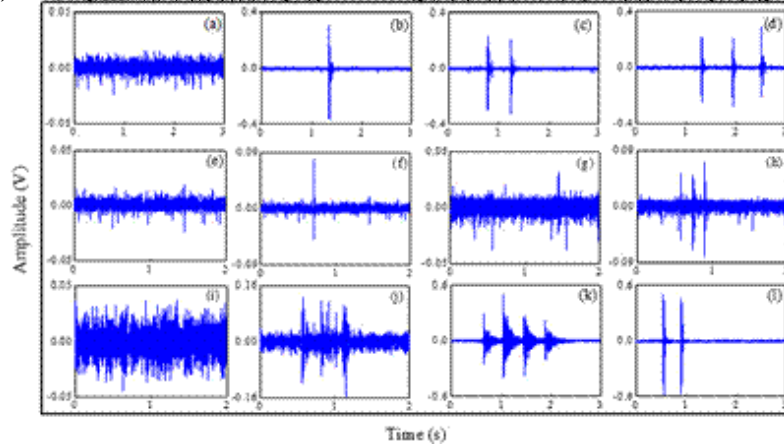


图 4-1 各种类型事件的典型波形

- (a) 晴天没有人为振动，(b) 晴天摇晃一次纤维，(c) 晴天摇晃两次，
 (d) 晴天摇晃三次，(e) 大风天无人工振动，(f) 大风天摇晃纤维一次，
 (g) 小雨和小风时无人工振动，(h) 小雨和小风时摇晃三次，(i) 大雨大风时无人工振动，
 (j) 大雨和大风时摇晃三次，(k) 步行，(l) 敲打纸板两次。

五、 识别结果

5.1 原始事件信号

我们根据图 1 构建了实验系统，以获取传感光纤在两种模拟铺设情况下的原始事件信号：连接到物理围栏并埋在地下。光源为中心波长 1550nm，输出功率 2mw 的宽带光源。DL 和传感光纤为单模光纤，长度分别为 1.01km 和 3.1km。信号采样率为 10ks/s。

由于 Sagnac 光纤干涉系统不受温度波动等环境缓慢变化的影响，可以忽略长距离光纤中的温度不均匀效应。对于基于围栏的系统，需要考虑风和雨引起的振

动。因此，在不同的模拟天气条件下，即晴天、风、小雨和风、大雨和风，我们通过多次摇动悬挂在防震光学台边缘的光纤，获得了攀爬围栏的事件信号。考虑到实际应用情况，将光纤的一次振动或无人为振动视为非侵入事件。对于被埋系统，我们通过穿过传感光纤获取行人入侵的事件信号，通过敲击铺设光纤的纸板多次获取系统的人身伤害事件信号。敲击光纤一次或光纤上无振动被视为非侵入事件。由于地埋系统几乎不受外界环境的影响，因此在恶劣的天气条件下不需要从中收集信号。为了获得足够的实验数据，实验重复了多次。各类事件信号的典型波形如图 3 所示。可见，不同事件的信号具有不同的特征。

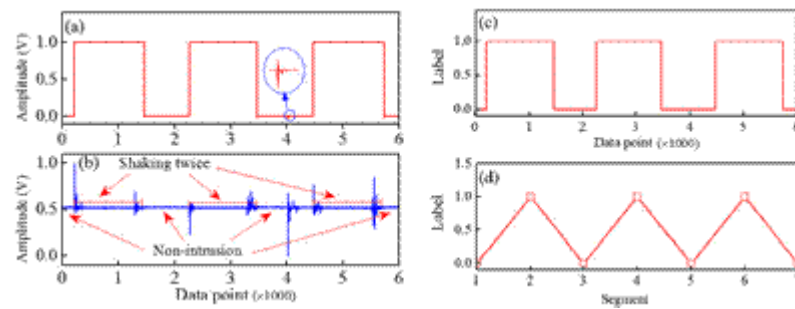


图 5-1 围栏类型量化和确定前后的测试输出
(a) 量化前的测试输出，(b) 测试输入，
(c) 量化后的测试输出，(d) 确定后的测试输出。

5.2 栅栏系统识别结果

伺服电机的大小 N 设为 200。在 -1 和 1 之间以相等的概率生成输入权重矩阵 Win 。内权矩阵是均匀分布的随机稀疏矩阵。激活函数 f 是一个非线性双曲正切函数 \tanh 。为了简化函数，输出函数 f_{out} 是一个线性恒等函数。储层的光谱半径 SR 设定为 0.4。

训练集由 240 个事件信号段组成。在晴天、风、小雨和风、大雨和风四种不同天气条件下的震动事件片段（两次和三次）占训练数据的 1/8。其它为四种天气条件下的非侵入信号（一次震动，无人为振动）。震动事件被视为入侵事件 1。在普通个人计算机上的训练集和 Matlab 软件编程平台下，训练时间为 10.23s。

在四种天气条件下，分别构建了四个测试集。每个测试集由 60 个片段组成，包括 20 个震动事件和 40 个非入侵事件。以晴天条件下的试验台为例，给出了试验结果。在对测试输出进行量化和决策后，得到最终的分类结果。量化和确定前后的测试输出如图 4 所示。在对测试输出进行量化之前，它们的振幅稍有紊

乱，如图 4（a）所示。特别是在 4000 左右的数据点，振幅的波动比较明显，如图 4（a）的局部放大入口所示。即使如此，如图 4（a）所示，测试输出与对应于测试输入的所需标签一致，即，“1”表示震动事件，“0”表示非入侵事件如图 4

（b）所示；量化测试输出后，无序现象消失，如图 4（c）所示。图 4（d）示出了根据第 4.4 节中的判定规则判定后的基于段的测试输出。可见，在晴天条件下，震动事件与非侵入事件的识别是完全正确的。4 种不同天气条件下的 IRs 分别为 100%、100%、98.33%和 96.67%。因此，基于栅栏的系统的平均红外光谱为 98.75%。在当前条件下，ESN 分类器模型识别每一段的平均时间仅为 0.081s。

5.3 地理系统识别结果

储液罐的尺寸 N 、输入重量矩阵 W_{inn} 、内部重量矩阵 W 、激活函数 f 、输出函数 f_{out} 和储液罐的 SR 与第 5.2 节相同。

这套训练仪还有 100 个信号段，包括 30 次人工敲击（两次和三次）、30 次步行和 40 次非侵入事件（敲击一次和无振动）。敲门和行走事件分别是入侵事件 2 和入侵事件 3。在训练集、软硬件条件下，ESN 的训练时间仅为 7.58s。

我们做了三组测试。第一个和第二个测试集都由 60 个片段组成。第一组包括 1/3 行人（步行）入侵段。其余的都是非入侵事件。第二组包括 20 个敲门事件和 40 个非侵入事件。第三组包括 20 个行人入侵信号、20 个敲门和 46 个非侵入事件。对于三个测试集中的非入侵事件和两种入侵事件，所有 IRs 都能达到 100%。此外，在当前条件下，分类器识别三个测试集的每个片段所用的平均时间分别为 0.157s、0.121s 和 0.131s。因此，对于埋藏系统，每段的平均识别时间为 0.136s。每个测试集在较短的时间内达到 100%的 IR。

为了直观地呈现识别结果，图 5-2 示出了确定后的测试输出和期望输出。我们可以看到，无论基于图 5-2（a）中的段和图 5-2（b）中的数据点的结果如何，这两个输出都是完全相同的。

为了研究训练集大小对识别率和训练时间的影响，我们构建了另外两个较小的训练集。第一个包含 90 个信号段，包括 27 个行走事件、27 个敲击事件和 36 个非侵入事件。第二个训练集包含 30 个片段，其中步行事件、敲击事件和非侵入事件各占训练集的 1/3。上面的第三个测试集包含 86 个信号段，用于测试不同

训练集上的 esn。两种训练集下的 IRs 分别为 97.76%和 32.56%，训练时间分别为 7.02s 和 2.42s。当训练集较小时，训练速度提高，但识别率降低。为了保持较高的识别性能，训练样本不应太少，至少要满足 ESN 分类器所需的训练次数。

5.4 该方法与基于 RFB 神经网络的辨识性能比较

为了更客观地评价该方法的识别性能，以埋藏式为例，比较了该方法与 EMD、峭度特性和 RBF 神经网络相结合的方法的识别性能^[15]。在后一种情况下，首先基于 EMD 将事件信号分解为 13 层固有模态函数（IMF）分量。然后利用前 11 个 IMF 构造峰度特征向量，输入 RBF 网络进行信号类别识别。识别率和识别时间如图 6 所示。I、 II 和 III 分别代表第 5.3 节中三个试验装置的识别性能。IV 是三个测试集的平均识别率。V 表示三个测试集的每个段的平均识别时间。

如图 5-2（a）所示，对于三种不同的测试集，基于 RBF 神经网络的方法识别率分别为 96.67%、 68.33%和 76.74%。平均红外光谱为 80.57%，明显低于 100%。从图 6（b）可以看出，基于 RBF 网络的三种不同测试集的每段识别时间分别为 0.097s、 0.114s 和 0.1s，每段识别时间略短于所提出方法的相应时间。在相同的测试集和计算平台下，该方法的平均识别时间为 0.104s，仅比提出的方法少 0.032s。但在相同的训练集和计算平台下，该方法的训练时间比提出的方法长 5.05s

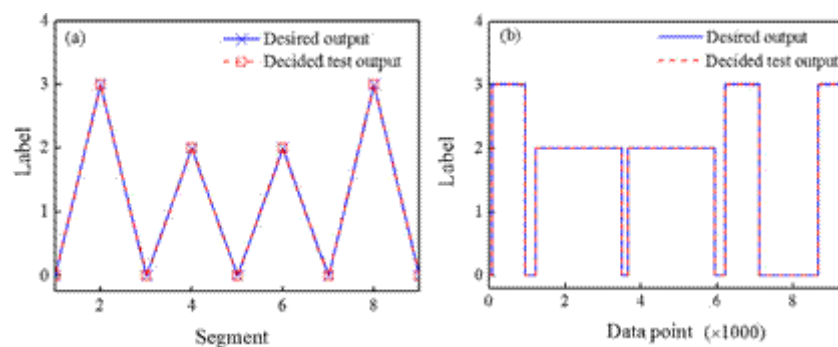


图 5-2 确定后的试验输出与地理式理想输出的比较

（a）基于段，（b）基于数据点。

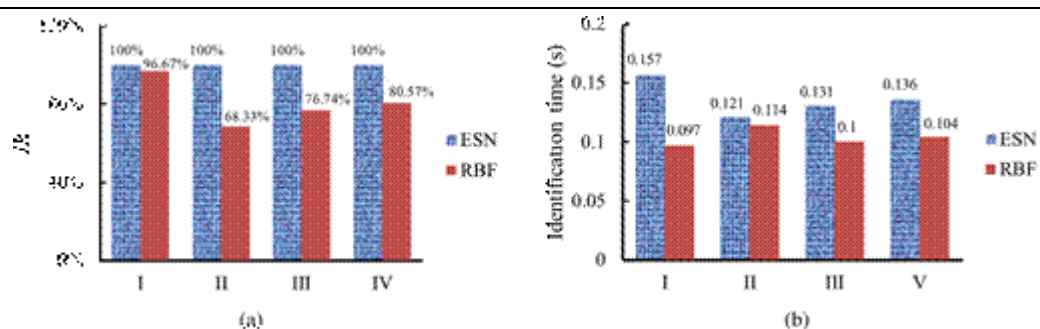


图 5-3 该方法与基于 RBF 神经网络的辨识性能比较

(a) 识别率。(b) 识别时间

六、 结论

本文提出了一种基于 ESN 的入侵信号识别方法。利用该方法对基于串联 Sagnac 干涉仪的光纤周界安全系统检测到的信号进行识别。通过选择合适的网络参数和最终分类标签的判定方法，模拟围栏式和埋地式光纤周边安全系统的平均识别率分别达到 98.75% 和 100%。该方法不需要提取信号特征，识别过程简单。另外，由于不需要大量的信号段来训练分类器模型，因此训练时间比其他方法要短。虽然鉴定时间稍长，但在实际应用中是可以接受的。综上所述，利用该方法可以准确、快速地识别入侵信号，降低光纤周边安全系统的虚警率。该方法有望满足安全领域实际应用的需要。