基于机器学习的光纤窃听检测方法

陈孝莲[1]，秦奕[1]，张杰[2]，李亚杰[2]，宋浩鲲[2]，张会彬[2]
（1. 国网江苏省电力有限公司无锡供电分公司，江苏 无锡 214000;
2. 北京邮电大学信息光子与光通信研究院，北京 100876）

摘　要：光纤窃听是信息安全的重大隐患之一，但其隐蔽性较高的特点导致筛查困难。针对通信网络中面临的光纤窃听问题，提出了基于机器学习的光纤窃听检测方法。首先基于窃听对传输物理层的影响，设计了 7 个维度的特征向量提取方法；其次通过实验，模拟窃听并收集特征向量，利用两种机器学习算法进行分类检测和模型优化。实验证明，神经网络分类算法的性能优于 K 近邻分类算法，其在 10%分光窃听中可以实现 98.1%的窃听识别率。

关键词：窃听检测；光纤窃听；机器学习；神经网络
中图分类号：TP393
文献标识码：A
doi: 10.11959/j.issn.1000−0801.2020299

Optical fiber eavesdropping detection method based on machine learning

CHEN Xiaolian[1], QIN Yi[1], ZHANG Jie[2], LI Yajie[2], SONG Haokun[2], ZHANG Huibin[2]
1. Wuxi Power Supply Company, State Grid JiangSu Electric Power Co., Ltd., Wuxi 214000, China
2. State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing 100876, China

Abstract: Optical fiber eavesdropping is one of the major hidden dangers of power grid information security, but detection is difficult due to its high concealment. Aiming at the eavesdropping problems faced by communication networks, an optical fiber eavesdropping detection method based on machine learning was proposed. Firstly, seven-dimensions feature vector extraction method was designed based on the influence of eavesdropping on the physical layer of transmission. Then eavesdropping was simulated and experimental feature vectors were collected. Finally, two machine learning algorithms were used for classification detection and model optimization. Experiments show that the performance of the neural network classification is better than the *K*-nearest neighbor classification, and it can achieve 98.1% eavesdropping recognition rate in 10% splitting ratio eavesdropping.

Key words: eavesdropping detection, fiber eavesdropping, machine learning, neural network

收稿日期：2020−04−14；修回日期：2020−09−07
基金项目：江苏省电力有限公司科技项目（No.J2019124）
Foundation Item: Science and Technology Project of Jiangsu Electric Power Co., Ltd. (No.J2019124)

1 引言

随着信息技术的发展，网络安全形势日益严峻。光纤通信作为现代通信的主要支柱之一，在现代通信网络中的作用举足轻重，因此极容易成为不法分子的目标，其数据传输的可靠性是社会无数系统安全、正常运行的重要保障[1]。光纤窃听是一种常用的攻击手段，较其他窃听方法来说，光纤弯曲耦合法的隐蔽性较强，给光纤传输网络带来极大安全隐患[2]。

已有的安全检测研究多数针对设备故障等情况，对于窃听攻击的防护不足。传统的状态参量法是对于单一状态参量的阈值进行分析评价，比如光功率监测法和导频法[3]。当通信设备状态由于绝缘老化等原因发生变化时，其变化过程极为缓慢且难以察觉，导致异常状态的设备数据与原有人为设定的阈值不匹配，检测结果严重滞后。基于机器学习的故障预测法[4-5]针对环境状态提取特征量，并应用可变阈值规则进行故障预测。但其主要针对光缆松动、锈蚀、损伤和其他线路故障问题。利用光时域反射仪（optical time-domain reflectometer，OTDR）也可以实现系统异常的检测和定位[6-7]。通过跟踪反射光信号的时间和强度，OTDR 能够确定光环路的完整路径。但为了检测大多数类型的窃听，信号衰减的限制都必须设置在较高的水平。这就会导致频繁误报，一次例行检查就足以触发告警。不仅如此，OTDR 需要单独作用于链路一端，所以更多用于已知故障链路的定位，而非正常传输链路的检测。实时 OTDR 设备成本过高难以推广，因此存在局限性。因此，探索一种效率更高、成本更低的光纤窃听检测方法具有重要意义。

由于光纤传输设备数据体量大、类型繁多的特点，可以将机器学习（machine learning，ML）技术应用到光纤传输窃听检测中，充分挖掘状态数据中的信息。已有部分研究在光通信领域应用了一些算法，其中主要涉及概率图模型[8]、变分贝叶斯方法[9-10]、神经网络[11-13]、*K*-均值聚类算法[14]等。针对上述问题，本文将研究基于 ML 的光纤窃听检测技术，借助其数据处理和分析能力，对光通信系统物理层数据进行智能分析和精细化处理，实现对光纤非法窃听的智能检测，增强信息抗截获能力，最终提升光纤传输网络的安全性。实验收集了 300 km 单模光纤链路中不同分光比的数据，提取反映信道传输质量的特征向量，并应用两种分类算法对比，分别分析其窃听检测成功率。实验表明机器学习算法能快速有效地检测出端到端光纤传输系统的异常运行状态，可为通信设备提供状态评价和决策支持。

2 光纤窃听问题描述

常见的光纤窃听方法有光纤弯曲、V 形槽切割、散射、光分裂和消逝耦合等[15]。其中，最值得注意的是成本极低的光纤弯曲法，可以从漏光中恢复原始信号。光纤窃听难度的降低导致信息泄露现象愈发严重，对信息安全造成极大威胁。针对此问题，本文提出了基于机器学习的光纤窃听检测方法，旨在防止信息泄露，为光纤系统的安全性提供保障。

以相干检测正交频分复用（coherent orthogonal frequency division multiplexing，CO-OFDM）系统为例进行参数说明和实验验证，但是此基于机器学习的窃听检测方法可以扩展到其他更复杂的通信系统。为了感知光纤通道的细微变化，需要了解 CO-OFDM 系统参数和特征值之间的关系。信道状态关系如图 1 所示，关于系统参数如何具体影响光纤信道状态，Nazarathy[15]建立了多跨长距离光纤链路上 CO-OFDM 传播和检测的分析模型，全面分析了四波混频（four-wave mixing，FWM）、色散和放大器自发辐射（amplified spontaneous emission，ASE）噪声的综合影响。此外，Chen[16]导出了密集 CO-OFDM 系统非线性系统性能的闭式解析表达式。这些分析结果清楚地确

定了信道状态对系统参数的依赖性，这些系统参数包括光纤色散、跨度数、色散补偿率和总带宽。

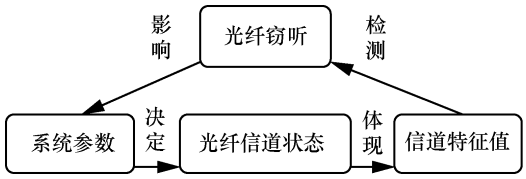


图 1　信道状态关系

另外，参考文献[16]中的数学模型定量描述了光纤通道质量和特征值之间的关系。诸如信道窃听、故障或攻击等负面因素的影响间接导致信道状态产生细微变化，并且在所测量的特征值中表现出某些可区别的特性。这也是本文操作的基础，即可以通过特征值的学习来推断出通道状态的变化，从而判断窃听是否发生。

3　基于机器学习的窃听检测方法

ML 非常适合处理大量数据并识别其中复杂的模式，而无须明确指定模型或参数阈值。窃听引起的复杂影响令光纤安全评估成为 ML 算法的应用新场景。窃听检测流程如图 2 所示，说明了该方案的总体原理。该方案包括两个模块，即窃听训练模块和窃听检测模块。窃听训练模块是调试过程中的准备工作，日常设备运行中的检测是指第二个模块。其中具体包括 6 个步骤。

（1）工作信道的特征值提取

对不同信道情况下多个信号获取信道传输质量的过程。针对光纤信道，采集传输信号的 7 种特征值作为待处理的原始训练数据。由于数据本身对机器学习算法有至关重要的作用，机器学习算法对数据的需求量很大，因此需要设备对数据进行持续的采集和更新，保证模型拥有一定的阶段适应性。

（2）训练数据收集及预处理

主要完成窃听情况和性能信息的采集、采集数据的预处理以及上传等操作。具体来说，实验中

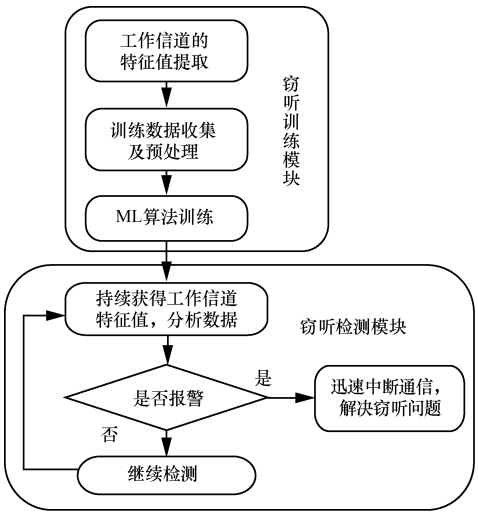


图 2　窃听检测流程

进行了 3 种不同分光比的窃听实验，分别为 10%、30%和 50%。分别采集正常传输和各分光情况下传输线路的特征向量，进行学习。其中涉及的性能参数有如下 7 个。

- 品质因子（quality，Q 因子）：接收机在最佳判决门限下信号功率和噪声功率的比值。Q 因子综合反映眼图的质量问题。眼图是反映信号整体传输效果的关键特征，Q 因子越高，眼图的质量就越好，信噪比就越高。Q 因子一般受噪声、光功率、电信号阻抗匹配等因素影响。
- 光信噪比（optical signal to noise ratio，OSNR）：光信号功率和噪声功率的比值。光信号的功率一般取峰值，而噪声的功率一般取相临两路的中间点的功率电平。
- 误码率（bit error ratio，BER）：是衡量数据在规定时间内数据传输精确性的指标，误码率为传输中的误码/所传输的总码数。
- 误差向量幅度（error vector magnitude，EVM）：信号平均功率的均方根值与理想信号平均功率的均方根值之比，并以百分比的形式表示。EVM 越小，信号质量越好。
- 眼高（eye height，EH）：反映了传输线上信号的噪声容限，是空白的区域在纵轴上

的距离。噪声瞬时值超过眼高的一半就可能发生错误判决。

- 眼宽（eye width，EW）：反映信号的总抖动，是眼图在水平轴所开的大小，其定义为一个 UI 中左右交叉点的时间差。交叉范围内的时间点是基于信号中的两个零交叉点处的直方图平均数计算而来。
- 平均功率：平均功率通过眼图反映的平均功率，即整个数据流的平均值。平均功率则是直方图的平均值，应为总眼图振幅的 50%。

由于窃听需要利用各种手段窃取信号光，所以光纤窃听会导致信号光相对正常传输过程的减弱。除此之外，由于窃听原理不同，各种方法还会对信道造成各种不同的影响。信号光功率降低的共性及各方法的特性共同导致其对上述特征值的影响。上述 7 个特征值可以分为两类：直接体现光纤信道状态的 Q 因子、OSNR、BER 和 EVM 以及通过描述眼图特征间接体现光纤信道状态的眼高、眼宽和平均功率。参考文献[16]中给出了考虑四波混频（FWM）、色散以及放大器自发辐射（ASE）噪声影响的 OFDM 系统解析模型，直接特征值有如下表示形式：

$$Q=\pi/(m\sqrt{\kappa_m(\sigma^2_{\angle\mathrm{FWM}}+\sigma^2_{\angle\mathrm{LN}})}) \tag{1}$$

其中，m 是相态数（M-ary PSK），κ_m 是模型的准确性校正因子（$\kappa_4=1.11$），$\sigma^2_{\angle\mathrm{FWM}}$ 是由 FWM 引起的相位噪声方差，$\sigma^2_{\angle\mathrm{LN}}$ 是是线性相位噪声的方差：

$$\sigma^2_{\angle\mathrm{LN}}=\frac{\frac{1}{2}N_0(N_{\mathrm{span}}+1)W}{P_T} \tag{2}$$

$$\mathrm{OSNR}_{\mathrm{OFDM}}=\frac{P_T}{2(N_{\mathrm{span}}+1)N_0W_{\mathrm{ref}}} \tag{3}$$

其中，N_0 代表每个 I 和 Q 正交分量的单侧功率谱密度（PSD），N_{span} 是系统跨度数，W 是信道总带宽，$W_{\mathrm{ref}}\equiv12.5\ \mathrm{GHz}$ 是 0.1 nm 的噪声分辨率带宽，P_{T} 是发送端信号功率。不难看出 Q 因子和 OSNR 相互联系且均与发送端功率相关。BER 以及 EVM 为最常见的信道性能参数，与 Q 因子与 OSNR 同样相关，受到发送端功率影响。眼图作为衡量信号质量的工具，可以比较全面地反映信道状态。其同样与发送端功率相关，且一定程度上可以反映窃听方法带来的其他干扰。考虑检测效率，选取其 3 个常见参数加入数据集，也就是眼宽、眼高和平均功率。综上，7 种特征值都与窃听密切相关，组合成为本方案数据集。

以上特征值全部由接收端的 DSP 模块直接导出，其中，N 为总数据量。本文的训练集，即特征向量 X 由 7 种特征值加一种窃听状态标签 S（安全状态、10%、30%和 50%窃光状态，一共 4 种标签）组成，其中，N 为数据点个数。

$$X=\left\{\begin{pmatrix}Q_n & \mathrm{OSNR}_n & \mathrm{BER}_n & \mathrm{EVM}_n\\ \mathrm{EH}_n & \mathrm{EW}_n & P_n & S_n\end{pmatrix}\middle|\, n=1,\cdots,N\right\} \tag{4}$$

预处理部分，主要包括数据清洗、不同窃听情况下的数据集平衡以及不同维度数据的归一化和标准化。特征向量 X 经过处理后得到数据集 D：

$$D=\left\{\begin{pmatrix}X_{1n} & X_{2n} & X_{3n} & X_{4n}\\ X_{5n} & X_{6n} & X_{7n} & S_n\end{pmatrix}\middle|\, n=1,\cdots,N\right\} \tag{5}$$

因为数据的质量，直接决定了模型的预测和泛化能力的好坏。它涉及很多因素，包括准确性、完整性、可信性等。而在真实数据中，拿到的数据可能包含了大量的缺失值，可能包含大量的噪声，非常不利于算法模型的训练。所以数据清理、数据集成和数据规约的目的是得到标准的、干净的、连续的数据，提供给下一步中的 ML 模型训练步骤。

（3）ML 算法训练

步骤完全取决于所采用的算法。本文主要涉及两种分类算法，而 K 近邻算法本身没有训练过程，所以算法训练这部分主要针对神经网络算法，其训练方法在之后的部分会具体介绍。

（4）此步骤中需要对光纤信道进行实时检测，得出上述特征。在后续处理中作为测试集数据。

（5）窃听模块判决报警

若输出层结果为 1/0，则判定为存在窃听行为。反之判断为安全。根据此判决方法，可以实时对工作信道进行分析，判断其是否存在窃听，并在发现窃听行为后进行报警。

（6）窃听情况处理

首先中断通信，避免让窃听者获得更多有有效信息。然后对窃听情况进行排查处理， 根据每次事故处理情况、总结事故处理经验和技巧，提高通信光缆事故处理效率，及时恢复通信光缆的正常运行。

4　两种 ML 分类器

4.1　*K* 近邻分类器

K 近邻（*K*-nearest neighbor，*K*NN）分类器是一种用于分类和回归的算法，其原理如图 3（a）所示。具体来说，就是寻找目标分类点 t（其对应数据点为 D_t）在特征空间中的 k 个最接近的训练样本（其对应数据点为 $D_1 \cdots D_t$），即其“邻居”。目标点的分类结果是由其“邻居”的“多数表决”确定的，为使较近点的权重比较远点的权重大，一种常见的加权方案是给每个邻点的权重赋值为 $1/d_k$，其中，d_k 是目标点到该邻居点的距离，p_k 是目标点归类为该邻居点标签的概率：

$$d_k = \sqrt{\sum_{m=1}^{7}(X_{mk} - X_{mt})^2} \tag{6}$$

$$p_k = \frac{S_k}{d_k}\left(\sum_{l=1}^{k}\frac{S_l}{d_l}\right)^{-1} \tag{7}$$

得出 k 个概率值后，对相同标签的概率求和，对应概率最大的标签值为目标点分类结果。*K*NN 没有训练过程，但是分类过程需要计算每个训练样本和测试样本的 K 个近邻距离，因此当训练集和测试集较大时，分类效率较低。

4.2　神经网络分类器

神经网络（neural network，NN）从信息处理角度对人脑神经元网络进行抽象，建立某种简单模型，按不同的连接方式组成不同的网络。多层的神经网络具有出色的特征学习能力，并且所学习的特征具有更多的数据特征，有利于可视化或分类。Lippmann[17]表明，单层网络足以满足线性分离功能，两层网络足以满足二次分离曲线或形成凸区域的曲线，而三层网络则可以形成任何所需的决策区域。因此本文采用三层网络，其原理如图 3（b）所示。激活函数 φ 采用常用的 Sigmoid 函数。网络具体训练过程分为以下 3 步。

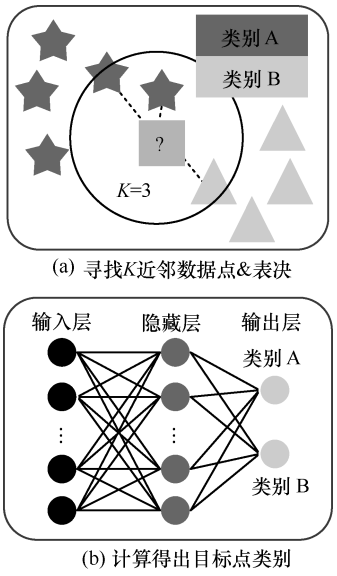


图 3　ML 分类器原理示意图

（1）随机初始化网络权值和神经元的阈值。

（2）向前传播：按照式（2）和激活函数分层计算隐层神经元和输出层神经元的输入和输出。其中，m 指此层中神经节点的个数，i 只做计数功能。w 为神经节点的权重。

$$y = \varphi\left(\sum_{i=0}^{m} w_i x_i\right) = \varphi\left(w^{\mathrm{T}} x\right) \tag{8}$$

（3）向后传播：根据式（3）修正权值和阈值。其中，误差函数 ε 根据算法不同有不同的定义，本文中采用交叉熵损失函数，η 为权重调整步长。

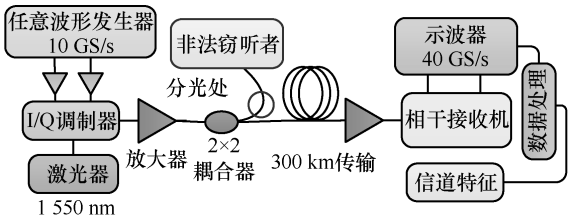
$$w = w + \eta\nabla\varepsilon(w) \tag{9}$$

反复重复（2）（3）步骤，直到满足终止条件（误差函数趋于收敛）。然后根据最终的输出

层神经元值判断窃听位置。

5 实验验证与结果分析

将光纤通信系统和包括发射机、接收机和信道的传输链视为完整的端到端传输过程。以CO-OFDM 系统为例，此检测方法可以轻松地应用于其他更复杂的通信系统。图 4 显示了用于演示所建议的窃听检测的实验装置。建立了一个具有 300 km 标准单模光纤的数字相干光传输系统的实验平台，以模拟实际的传输过程。



(a)

(b)

图 4 实验原理

实验采集了 3 种不同分光比下的传输特征值（10%、30%和 50%），并针对此 3 种情况进行了窃听检测训练。对于每种考虑到的情况，将分类器训练为两类：窃听和安全。对于两种算法，实验数据分类结果如图 5 所示，随着分光比的增加，信道损伤加剧，窃听检测则更加容易，所以两种算法的准确率都有所升高。神经网络分类器的效果明显好于 *K* 近邻分类器，10%分光比处的神经网络分类器已经达到了 98.1%的准确率，而 50%分光比处的 *K*近邻分类器准确率也只能达到 96.6%。实验中分类算法采用 MATLAB 自带库函数中的Fitcknn 分类器和 nntool 分类器。在此之前，针对窃听检测的研究多为方案设计而缺少实验结果，其中参考文献[18]设计了一种基于 LabVIEW 的光纤安全监视预警系统，其利用干涉型光纤传感系统检测人为扰动，并判断持续性一般人为扰动为窃听。其在总长 4.75 km 的线路上进行了实验，共实验人为扰动 30 次，漏报率约为 3.3%。虽然对窃听的判断方法不同，但机器学习方法有其灵活性，数据的更新可以让其适应系统参数的缓变，算法的改变可以满足不同检测效率和精确度的需求，更多数据集的训练有希望区分不同的窃听方法，所以机器学习的应用在窃听检测方面很有潜力。

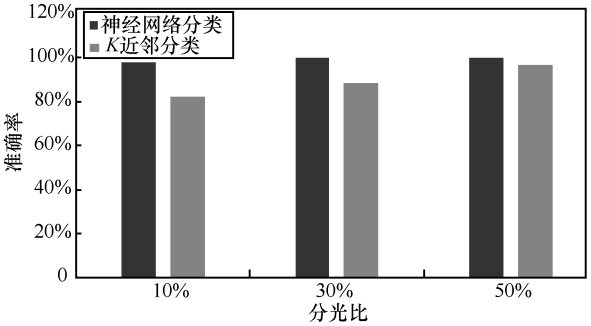


图 5 实验数据分类结果

6 结束语

针对目前通信网中窃听攻击频发和检测困难的问题，本文提出基于 ML 算法的光纤窃听检测方法。利用 ML 的精确处理能力，该方法可以察觉受窃听影响的光信道的细微变化。通过基于 OFDM 端到端系统的实验，评估了所提出方法的可行性和性能。实验中考虑了不同的窃听强度，实验结果表明，此特征值组合的输入训练成功实现了窃听检测。此外，通过对比实验证明神经网络分类器具有更好的性能。尽管该方法在端到端实验中验证成功，但是将其部署到实际基础结构中仍然是一项挑战。本文初步探索了光纤窃听检测的新方法，为基于 ML 的通信网络中的窃听检测技术奠定了基础，可以有效增强通信网络的安全性。

参考文献：

[1] 黄伟庆. 国家秘密不能曝“光”[J]. 保密工作, 2015(5): 50.

HUANG W Q. State secrets cannot be exposed[J]. Confidential Work, 2015(5): 50.

[2] 张睿汭. 光纤通信网络窃听方法及防御措施[J]. 电信科学, 2012, 28(11): 112-115.
ZHANG R R. Fiber optic communication network eavesdropping methods and defensive measures[J]. Telecommunications Science, 2012, 28(11): 112-115.

[3] IQBAL M Z, FATHALLAH H, BELHADJ N. Optical fiber tapping: methods and precautions[C]//Proceedings of 8th International Conference on High-capacity Optical Networks and Emerging Technologies. Piscataway: IEEE Press, 2011: 164-168.

[4] 邹钟璐. 基于否定选择算法的现场运维故障预测方法研究[J]. 电力信息与通信技术, 2019, 17(9): 55-61.
ZOU Z L. Research on fault prediction method for on-site operation and maintenance based on negative selection algorithms[J]. Electric Power ICT, 2019, 17(9): 55-61.

[5] 侯晓凯, 李师谦, 王杰琼, 等. 一种基于神经网络的网络设备故障预测系统[J]. 山东理工大学学报(自然科学版), 2014, 28(6): 29-34.
HOU X K, LI S Q, WANG J Q, et al. Neural network fault prediction system in network equipment[J]. Journal of Shandong University of Technology (Natural Science Edition), 2014, 28(6): 29-34.

[6] 彭昌东. 光纤通信网络窃听方法与防御对策[J]. 计算机产品与流通, 2019(12): 36.
PENG C D. Fiber optic communication network eavesdropping methods and defensive countermeasures[J]. Computer Products and Distribution, 2019(12): 36.

[7] 范雨辰, 郭才福, 林毅俊, 等. 一种电力光纤实时检测系统设计[J]. 计算机时代, 2014(8): 14-16.
FAN Y C, GUO C F, LIN Y J, et al. Design of real-time monitoring system for electric power optical fiber[J]. Computer Era, 2014(8): 14-16.

[8] IRUKULAPATI N V, MARSELLA, DOMENICO, et al. Stochastic digital backpropagation with residual memory compensation[J]. Lightwave Technology, 2016, 34(2): 566-572.

[9] BORKOWSKI R, ZIBAR D, CABALLERO A, et al. Stokes space-based optical modulation format recognition for digital coherent receivers[J]. IEEE Photonics Technology Letters, 2013, 25(21): 2129-2132.

[10] ISAUTIER P, PAN J, DESALVO R, et al. Stokes space-based modulation format recognition for autonomous optical receivers[J]. Lightwave Technology, 2015, 33(24): 5157-5163.

[11] WU X, JARGON J, SKOOG R, et al. Applications of artificial neural networks in optical performance monitoring[J]. Lightwave Technology, 2009, 27(16): 3580-3589.

[12] WU X, JARGON J, PARASCHIS L, et al. ANN-based optical performance monitoring of QPSK signals using parameters derived from balanced-detected asynchronous diagrams[J]. IEEE Photonics Technology Letters, 2011, 23(4): 248-250.

[13] DONG Z, KHAN F, SUI Q, et al. Optical performance monitoring: a review of current and future technologies[J]. Lightwave Technology, 2016, 34(2): 525-543.

[14] GONZALEZ N G, ZIBAR D, MONROY I T. Cognitive digital receiver for burst mode phase modulated radio over fiber links[C]//Proceedings of 6th European Conference and Exhibition on Optical Communication. [S.n:s.l], 2010(1): 23-25.

[15] NAZARATHY M, KHURGIN J, WEIDENFELD R, et al. Phased-array cancellation of nonlinear FWM in coherent OFDM dispersive multi-span links[J]. Optics Express, 2008, 16(20): 15777-15810.

[16] CHEN X, SHIEH W. Closed-form expressions for nonlinear transmission performance of densely spaced coherent optical OFDM systems[J]. Optics Express, 2010, 18(18): 19039-19054.

[17] LIPPMANN R. An introduction to computing with neural nets[J]. ASSP Magazine, 1987, 4(2): 4-22.

[18] 邓大鹏, 盛兴, 廖晓闽, 等. 基于 LabVIEW 的光纤安全监视预警系统的设计[J]. 光通信技术, 2011, 35(10): 57-59.
DENG D P, SHENG X, LIAO X M, et al. Design of supervising and early-warning system for the safety of optical fiber based on LabVIEW platform[J]. Optical Communication Technology, 2011, 35(10): 57-59.

[作者简介]

陈孝莲（1977− ），女，国网江苏省电力有限公司无锡供电分公司高级工程师，主要研究方向为电力通信。

秦奕（1979− ），男，国网江苏省电力有限公司无锡供电分公司高级工程师，主要研究方向为电力通信运维。

张杰（1972− ），男，博士，北京邮电大学信息光子与光通信研究院院长、博士生导师，主要研究方向为安全光通信技术。

李亚杰（1990− ），男，博士，北京邮电大学信息光子与光通信研究院在站博士后，主要研究方向为安全光通信技术。

宋浩鲲（1996− ），女，北京邮电大学信息光子与光通信研究院博士生，主要研究方向为安全光通信技术。

张会彬（1980− ），男，博士，北京邮电大学信息光子与光通信研究院讲师，主要研究方向为安全光通信技术。