第53卷第5期 南京航空航天大学学报 Vol. 53 No. 5
2021年10月 Journal of Nanjing University of Aeronautics & Astronautics Oct. 2021

DOI:10.16356/j.1005-2615.2021.05.007

基于改进极限学习机的数据采集与监控系统攻击检测模型

张晓琴[1], 汪云飞[2], 胡春强[3]

(1.重庆市信息通信咨询设计院有限公司,重庆 400041; 2.航天壹进制(南京)数据科技有限公司,南京 210032; 3.重庆大学大数据与软件学院,重庆 400030)

摘要: 提出一种基于改进极限学习机(Online sequence extreme learning machine, OSELM)的新能源电站数据采集与监控(Supervisory control and data acquisition, SCADA)系统攻击检测模型。首先使用ADASYN算法对数据样本中的异常数据和正常数据进行数量平衡,以满足真实电站SCADA系统环境中异常数据量少的特点。接着使用降噪自编码网络对平衡后的数据进行约简,消除无关或冗余特征以降低检测模型的训练时间。最后在AWID数据集上进行了大量对比实验,结果表明,所提的数据约简方法可有效地降低数据维度,降低了检测时间;与其他基于浅层学习算法的检测分类器相比,本文所提方法在检测准确度和误报率方面也体现出了更优性能。

关键词: 新能源电站;SCADA系统;攻击检测;极限学习机;数据约简

中图分类号: TP274 **文献标志码:** A **文章编号:** 1005-2615(2021)05-0708-10

Attack Detection Model of SCADA System Based on Data Preprocessing and Improved ELM

ZHANG Xiaoqin[1], *WANG Yunfei*[2], *HU Chunqiang*[3]

(1. Chongqing Communication Design Institute Co. Ltd., Chongqing 400041, China; 2. Aerospace Unary(Nanjing)Data Technology Co. Ltd., Nanjing 210032, China; 3. School of Big Data & Software Engineering, Chongqing University, Chongqing 400030, China)

Abstract: An attack detection model for supervisory control and data acquisition (SCADA) system of new energy plant based on improved online sequence extreme learning machine (OSELM) is proposed. First of all, ADASYN algorithm is used to balance the number of abnormal data and normal data in the data samples, so as to meet the characteristics of less abnormal data in the real SCADA system environment. Then, the balanced data is reduced by using the de-noising autoencoding network (DAE), and the irrelevant and redundant features are eliminated to reduce the training time of the detection model. Finally, a large number of comparative experiments are carried out on the AWID data set. The results show that the proposed data reduction method can effectively reduce the data dimension and detection time. Compared with other detection classifiers based on shallow learning algorithm, the proposed method also shows better performance in detection accuracy and false alarm rate.

Key words: new energy power plant; supervisory control and data acquisition (SCADA) system; attack detection; extreme learning machine (ELM); data reduction

基金项目: 国家自然科学基金(61702062)资助项目。

收稿日期: 2020-10-11; **修订日期:** 2021-03-10

通信作者: 胡春强,男,教授,博士生导师,E-mail:chu@cqu.edu.cn。

引用格式: 张晓琴,汪云飞,胡春强. 基于改进极限学习机的数据采集与监控系统攻击检测模型[J]. 南京航空航天大学学报,2021,53(5):708-717. ZHANG Xiaoqin, WANG Yunfei, HU Chunqiang. Attack detection model of SCADA System based on data preprocessing and improved ELM[J]. Journal of Nanjing University of Aeronautics & Astronautics, 2021, 53(5):708-717.

随着新能源发电技术在智能电网中的集成，工控系统在电力、石油、天然气和新能源也面临着日益严重的信息安全问题，保障电站工控系统的本地设备和远程运行监控和管理系统的安全成为电力公司所关心的问题[1]。数据采集与监控系统（Supervisory control and data acquisition，SCADA）作为电站发电监督控制的核心，一旦受到网络入侵服导致其停止服务将危及整个发电过程最终导致整个电力系统崩溃。因此，深入研究防范新能源电站网络攻击特征，提出一种高效的SCADA 入侵检测检测模型或系统成为业界研究的重点。

通常SCADA以一种安装在上位机上的应用出现，一个SCADA系统可能连接多个可编程控制逻辑（Programmable logic controller，PLC），它们共同控制一个发电过程。SCADA系统承担了对内和对外数据交换和处理的重要功能，在拓扑系统中，SCADA系统可以对调度指令信息进行全面解析，并且将所得到的数据进行存储和记录。对于下游终端，SCADA系统具有远程硬件预警、网页发布、数据恢复和报表等功能。除了应用在新能源电站中，SCADA系统还广泛用于电网的电力传输、污水净化和交通调度等重要基础设施中[2]。在新能源电站环境中，由于SCADA系统通过有线或无线网络连接控制多种发电终端及数据采集装置，这给攻击者提供了较大的渗透机会。SCADA系统运行时各部分组件相互关联、互相制约和影响[3]，任何一部分遭到网络攻击都可能造成整个新能源电站系统的瘫痪。

考虑到新能源电站的经济效益、可靠性和安全性等因素，通常采用Wi-Fi网络作为系统通信方式[4]。在保障系统稳定安全的前提下，实现了对电站内部资源的高速访问、新能源电站集群的远程监控等功能[5-6]。这意味着它会受到多种的网络攻击。为了评估SCADA系统中的网络安全风险，文献[7]提出了新能源电站安全风险评估模型，从系统建模和风险模拟角度对安全风险进行研究。为了保护新能源电站SCADA系统中的重要资产数据，文献[8]从挖掘系统内部的漏洞出发，深度研究漏洞触发机理，寻找可能导致系统崩溃的违规行为。文献[9]对攻击检测率过高和误报问题进行了细致的分析，提出了一种基于稀疏自编码器的非监督式的模型方法；为了预警在系统中某些特殊的DoS攻击，文献[10]通过数据集中有关Java的序列，进行逻辑回归算法检测溢出攻击，成功获得了数据集并实现了高效的分类。目前，基于机器学习的方法是检测SCADA系统中入侵行为广泛使用的方法，对于算法的准确性要求也必然越来越高，特别是一些有机器学习的先进线性算法模型，诸如决策树、支持向量机（Support vector machine，SVM）、决策树（C4.5）和贝叶斯网络逐渐发展并在工控SCADA系统预警和检测中得到广泛应用。并且有着优异的表现[11-12]。相较于传统基于神经网络的检测方法，上述基于统计理论的机器学习算法具有更好的泛化能力且更适合小样本入侵检测问题。但这些方法对具有大规模样本的入侵检测的效率不高[13-14]。极限学习机（Extreme learning machine，ELM）是一种新型单隐层前馈神经网络（Single-hidden layer feed for ward networks，SLFNs）[9-10]。ELM能克服传统神经网络训练速度慢，具有更好的泛化能力和更快的训练速度。本文采用序列学习策略，获取新的数据并不断更新模型，而非重新训练模型，以实现在线且快速的检测模型训练。

在预警SCADA系统攻击检测的研究中通常使用KddCUP99[13]和AWID[14]等数据集，这两种方法可以进行高维数据挖掘并且有着很强的数据关联度。同时，为了简化所搭建的分类检测模型，对实验数据集进行线性和非线性约简和优化是必不可少的。文献[15]使用具有降维思想导向的主成分分析（Principal component analysis，PCA）将电网多指标数据集简化为几个综合指标，可以使大数据规模缩小至可管理的程度，不仅减少了数据集的维度，同时保持了数据集中对方差贡献最大的特征，极大地削弱了样本数据的复杂程度和计算量。文献对CT-PAC方法进行了深入的研究，并把它运用到人体活动传感器数据集样本的精简，建立了一系列的粗糙集，这两种线性方法均具有优异的数据约简可靠度。随着信息技术的爆发式发展，不可避免地出现了大量的高维度数据，非线性的约简方法就是一种适用于在更高维度的数据处理和拟合分析方法。非线性的约简方法在处理高维度数据集时较为稳健，可以保护统计上的渐进性质不遭到破坏，目前一般有基于核和基于流形的两种非线性约简方法，一般来说这两种方法不需要创建复杂的假设空间，可以有效地避免传统算法中特征分解和谱峰搜索过程，能够大大简化计算量。自编码器（Auto-encoder，AE）这种数据的压缩算法主要包括编码阶段和解码阶段，拥有着对称的结构，AE能从数据样本中进行无监督学习，并获得良好的性能，AE的应用主要涵盖两个方面：一个是对数据降噪处理，第二是对数据降维并应用可视化[16]。本文对SCADA系统中的攻击检测实验数据集采用基于AE的非线性约简的方法进行数据精简。

1 新能源电站SCADA系统攻击检测方法

对目前的研究进展进行汇总和分析可以发现，二分类过程是SCADA系统入侵检测的核心问题，使用样本特征复用率高的深度学习方法，通过构建含多隐层的多层感知器的学习结构，可以形成更加抽象表示属性类别或特征、挖掘出数据集中的高度隐含关系，并且构筑数据的分布式特征。基于此，本文构建了以改进极限学习机(Online sequence extreme learning machine, OSELM)为算法模型的SCADA系统攻击检测方法。构建AWID数据集进行分类和提高模型收敛速度并减少过拟合，使用拒绝服务攻击、窃取敏感信息攻击、缓冲区溢出攻击、系统漏洞攻击和对操作系统和网络设备的攻击等常见主、被动攻击方式建立数据集，并且对采集的数据集进行预处理，以全面地评价系统的可用性和有效性。对分类器进行训练前，采用降噪自动编码器(Denoising autoencoder, DAE)对数据进行约简以增强模型的抗干扰能力并提升建模的简洁程度。

本文构建的以OSELM为算法模型的SCADA系统预警检测系统运行流程如下：

(1) 对原始数据集进行分类采集，建立测试集和训练集数据样本，并分别采用3:7的样本比例。

(2) 为了改善改善不均衡数据集并获得一个均衡的数据分布，使用自适应综合过采样方法ADASYN在少数类样本之间进行插值，从而使边界区域内少数样本的密度得以增加，进而从数量上平衡数据样本。

(3) 采用DAE的方法对数据进行去除噪声、和对结果影响不大的特征向量，同时保持对结果有明显影响的特征向量和最小子特征集，从而达到对数据进行降维的目的。

(4) 将使用以上方法构建的数据集作为样本输入训练分类器，最终获得OSLEM分类器，并对服务器内的攻击行为进行检测和预警。

针对现信网的网络安全问题，本文以复杂多变的网络入侵领域由于攻击手段和攻击方式为数据集，研究了虚假数据攻击检测方法的原理，最后利用机器学习手段来强化基于统计的检测方法，优化出一种实用和有效的系统攻击检测模型算法，测试改进了入侵检测模型实验平台的性能。

1.1 对数据进行预处理和平衡化处理

所采集的AWID数据一般可以划分为定量数据和定性数据，为了使不同单位或量级的数据具有直接计算并生成复合指标的特征，在开始平衡化处理前应先对数据进行标准化处理使之落入一个小的特定区间，从而减少规模、特征和分布差异等对模型的影响。一般来说这个过程分为数字信号处理和数据计算处理两个步骤：(1)首先将符号值转化成可参与评价与计算的数值，使用函数变换将符号值属性映射至0～1这个数值区间，16进制的数据集属性一般在处理前需要提前转换为整数值。应该指出的是，数据集中的比如“?”的符号在标准化处理中会被替换为“0”。(2)对所有属性值进行同一、统一和合一的归一化变换，使之成为无量纲的表达式，从而有效地提升模型的收敛速度和精度。最后，将原始数据进行线性变换映射到0～1之间，转换函数为

$$y=\frac{x-\min(x)}{\max(x)-\min(x)} \tag{1}$$

式中：$\max(x)$为样本数据的最大值；$\min(x)$为样本数据的最小值。

现实条件下存在的新能源电站SCADA系统往往遭遇到的攻击数据较少，为了最大程度地对真实状态进行预测，有必要进行新能源电站集群数据集的构造。本文采用了ADASYN过采样方法对标准化数据进行平衡处理[15]，从而挖掘并构建出合成的“人造”样本数据集，从而使少数类样本集合和多数类样本集合中的数据数量达到平衡状态。算法步骤如下：

(1) 记少数类样本为m_s，多数类为m_b，使用公式$d=m_s/m_b, d\in(0,1]$计算类不平衡度；

(2) 对于每一个少数类样本，使用$G=(m_b-m_s)\times\delta$计算需要合成的样本数量，$\delta\in[0,1]$，它表示加入合成样本后所期望的不平衡度，当其值为1时表示G等于少数类和多数类的差值，这种情况下合成数据后的多数类个数和少数类数据达到平衡。

(3) 针对少数类样本x_i使用欧式距离计算出K个邻居，记Δ为K个邻居中属于多数类的样本数目，使用式$r_i=\Delta_i/K, i=1,2,\cdots,m$来计算邻居样本数据的占比。

(4) 使用$r_i'=r_i\Big/\sum_{i=1}^{m_s}r_i$对$r_i$正则化，计算少数类样本周围多数类的情况。

(5) 使用式$g_i=r_i'\times G$对少类样本x_i需要合成的样本数量进行确定，其中G表示合成样本数据的总数量。

(6) 在每个少数类样本周围K个邻居中确定1个少数类样本，对x_i少数样本进行合成，所得到的样本数量记为g_i，所使用的等式为

$$s_j=x_i+(s_{mi}-x_i)\times\lambda \tag{2}$$

对 j 从 1 到 g_i 操作：x_{si} 定义为从 x_i 的 K 个邻居中随机选择的一个少类样本；合成样本 s_j，其中 $\lambda\in[0,1]$。

以上步骤中，$m_s\leqslant m_b$。

1.2　基于降噪自编码器的数据精简

如图 1 所示，AE 共有 3 个组成部分：编码器、解码器和隐含层，编码器的作用将输入压缩成潜在空间表征，又叫输入层，可以用编码函数 $y=f_\theta(x)$ 表示，解码器的作用是重构来自潜在空间表征的输入，又叫输出层，可以用解码函数 $z=g_{\theta'}(y)$ 表示，编码器和解码器这两个部分构成了编码网格。由于隐含层内的神经元素数量较少，AE 在处理与训练集相类似的数据时会适当地压缩输入层数据。在运行时，通过缩小隐含层的维度、改变元素个数和加入惩罚项等施加约束条件，以达到在某个给定的数据集上训练自编码器，所设置的输入层和输出层数量的相对大小决定了是否对数据进行降维[17]。

在解码网格部分，输入层向量和隐含层向量之间的映射关系由非线性编码函数表示。将这两层向量之间的重构误差用 $L(x,z)$ 表示，并将反向回馈神经网路算法应用到对 AE 网络参数交叉熵的微调中，使交叉熵获得最小值。重新组织后的 AE 网络解码和编码逻辑框架如图 1 所示。

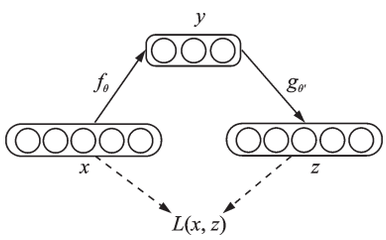

图 1　AE 网络编码和解码过程

Fig.1　Encoding and decoding processes of AE

AE 的原理可用下面两个等式表示，即

$$y=f_\theta(x)=s(W_x+b) \tag{3}$$

$$z=g_{\theta'}(y)=s'(W_y'+b') \tag{4}$$

式中：$\theta=\{w,b\}$ 表示一个表示编码器和隐含层数据函数的参数，而 $\theta'=\{w',b'\}$ 则代表了隐含层和解码器两者之间的参数，m 维和 n 维偏置分别用 b 和 b' 符号表示，在编码过程中，维度为 $m\times n$ 的权重矩阵使用 $\boldsymbol{W}$ 符号表示，在解码过程中，对应的权重矩阵用 $\boldsymbol{W}'$ 表示，隐含层和编码器和隐含层与解码器之间的激活函数使用 s 和 s' 符号表示，应用以上步骤，输入层 x 经过编码器过程被精简为 y，随后解码器发挥作用使其重构成为输出向量 z，这样设计的编码器和解码器之间的函数关系能够保证得到误差最小的重构数据，从而使得使用 AE 网络编码和解码能够获得输入数据集最大程度地保留特征，即对数据进行了降维。

为了让隐藏层的特征性得到更好的表达，获得捕获输入信号的稳定性结构，采用鲁棒性更强的数据降维方法，即 DAE 方法。DAE 可以在不改变 AE 网络结构的前提下，通过人为的增加噪声使模型获得鲁棒性更强的特征表达，并且避免使隐含层学习一个传统自编码器中没有意义的恒等函数。图 2 是本文所构建的对数据进行降噪处理的流程。图 2 中 X 表示输入编码器的原始数据，q_D 表示人为的加噪，$\overline{X}$ 为对输入中的噪声扰动重建以后的数据，将此数据作为 DAE 自编码器的输入数据，并将其所在层视为隐含层，最后通过激活函数 f_θ 求解该层神经元的激活值得到 H，最后通过激活函数求解该层神经元的激活值。本文中实验设计 DAE 算法的噪声系数为 0.1。

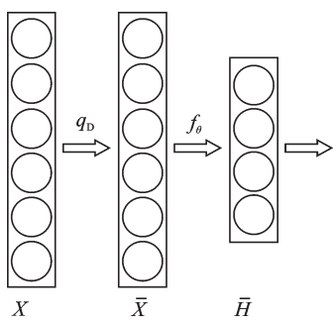

图 2　DAE 原理图

Fig.2　Schematic diagram of DAE

1.3　基于 ELM 的权重矩阵建立

极限学习机（Extreme learning machine，ELM）是一种 SLFNs 学习算法[18]。ELM 的优势是可以随机设定输入层和隐含层的连接权值、隐含层的阈值，并且设定完后无需反复调整；其次，隐含层和输出层之间的连接权值 $\boldsymbol{\beta}$ 不需要迭代调整和更新隐含层节点个数，只需设置隐含层神经元的阈值，便可通过求解方程组方式一次性确定最优解。研究表明，ELM 模型的泛化性能很好，这使得 ELM 方法具有较快的收敛速度，达到局部最优特点时所需要的时间相对较短。除了检测速度较快，ELM 在预警攻击时的误报率也非常低，相对于传统的神经网络，尤其是 SLFNs，ELM 具有更快的检测速度和更准确的检测结果。随机初始化参数是 ELM 网络的核心，随后将输入权重和偏置随机初始化并得到相应的输出权重，典型的 ELM 网络如图 3 所示。

以图 3 中的典型 SLFNs 为例，假设 N 个任意的样本 $(\boldsymbol{X}_i,\boldsymbol{t}_i)$，其中 $\boldsymbol{X}_i=[x_{i1},x_{i2},\cdots,x_{im}]^{\mathrm{T}}\in\mathbf{R}^n$，$\boldsymbol{t}_i=$

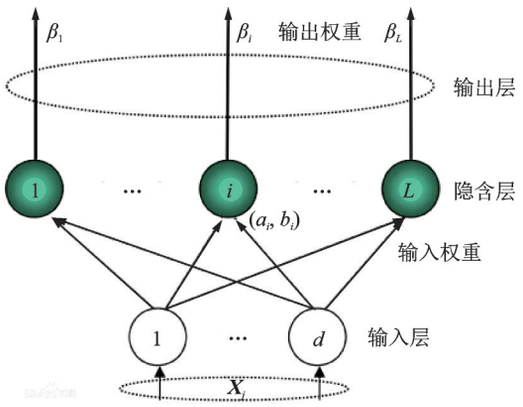

图3 ELM示意图

Fig.3 Schematic diagram of ELM

$[t_{i1}, ti_{i2}, \cdots, t_{im}]^{\mathrm{T}} \in \mathbf{R}^m$，将含有$N$个隐含节点的SLFNs表示为

$$\sum_{i=1}^{N} \beta_i g(\boldsymbol{W}_i \boldsymbol{X}_j + b_j) = o_j \quad j = 1, 2, \cdots, N \tag{5}$$

$$\boldsymbol{W}_i = [w_{i1}, w_{i2}, \cdots, w_{\mathrm{in}}]^{\mathrm{T}} \tag{6}$$

式中：激活函数表示为$g(x)$；输入权重表示为$\boldsymbol{W}_i = [w_{i1}, wi_{i2}, \cdots, w_{\mathrm{im}}]^{\mathrm{T}}$；输出权重表示为$\beta_i$；第$i$个隐层单元的偏置表示为$b_i$$\boldsymbol{W}_i$和$\boldsymbol{X}_j$的内积用$\boldsymbol{W}_i\boldsymbol{X}_i$表示，进一步地，存在$\boldsymbol{W}_i$，$\beta_i$和$b_i$，满足以下等式

$$\sum_{i=1}^{N} \beta_i g(\boldsymbol{W}_i \boldsymbol{X}_j + b_j) = t_j \quad j = 1, 2, \cdots, N \tag{7}$$

用$\boldsymbol{H}$表示隐含层节点的输出矩阵，用β表示β_i构成的输出权重矩阵，用T表示期望的输出值，则矩阵可简化为

$$\boldsymbol{H}\beta = T \tag{8}$$

权重和偏执是在ELM训练前随机生成的，所以对ELM隐含层节点个数及使用的激活函数进行分析和计算，便可得到输出权重β隐含层的输出矩阵$\boldsymbol{H}$与随机确定的输入权重$\boldsymbol{W}_i$和隐层的偏置b_i具有一一对应的关系，对以上线性公式进行计算可以得到输出权重为

$$\hat{\beta} = H^{+} T \tag{9}$$

式中H^{+}为矩阵$\boldsymbol{H}$的Moore-Penrose伪逆。通过数学推演可发现所得解$\hat{\beta}$的范数最小且唯一。为了进行实时的SCADA系统Wi-Fi入侵检测，并且应用ELM在预警入侵方面检测速度快、误报率低的特点，对SCADA系统应用了在OSELM的检测方法。相比于传统ELM的检测方法，OSELM在ELM的基础上进一步发展，采用序列学习策略，可以获取新的数据并不断更新模型，而非重新训练模型，如此便实现了在线且快速的训练。随后使用最小二乘法对式(8)中的输出权重求解，当隐含层节点数为m时，输出矩阵$\boldsymbol{H}$的秩为m，此时$\boldsymbol{H}$的广义逆可表示为

$$H^{+} = (H^{\mathrm{T}} H)^{-1} H^{\mathrm{T}} \tag{10}$$

当$H^{\mathrm{T}}H$为奇异矩阵时，有$\hat{\beta} = (H^{\mathrm{T}} H)^{-1} H^{\mathrm{T}} T$。在ELM中，求解输出权重可视为

$$\min_{\beta} \left\| H\beta - T \right\| \tag{11}$$

求解得$\beta = (H^{\mathrm{T}} H)^{-1} H^{\mathrm{T}} T$，当含$N_1$个样本的新数据集$(X_i^1, t_i^1)$输入到ELM后，上述优化问题变为

$$\min_{\beta} \left\| \begin{bmatrix} H \\ H_1 \end{bmatrix} \beta - \begin{bmatrix} T \\ T_1 \end{bmatrix} \right\| \tag{12}$$

式中：$\boldsymbol{H}_1$，T_1为新样本的输出矩阵和期望输出值，此时的输出权重$\beta_1 = (\begin{bmatrix} H \\ H_1 \end{bmatrix}^{\mathrm{T}} \begin{bmatrix} H \\ H_1 \end{bmatrix})^{-1} \begin{bmatrix} H \\ H_1 \end{bmatrix}^{\mathrm{T}} \begin{bmatrix} T \\ T_1 \end{bmatrix}$，即$\beta_1 = \beta + \left(\begin{bmatrix} H \\ H_1 \end{bmatrix}^{\mathrm{T}} \begin{bmatrix} H \\ H_1 \end{bmatrix} \right)^{-1} H_1^{\mathrm{T}} (T_1 - H_1\beta)$。当含$N_k$个样本的数据集$(X_i^k, t_i^k)$输入时，可得到

$$\beta_k = \beta_{k-1} + \boldsymbol{K}_k^{-1} H_k^{-1} (T_k - H_k \beta^{k-1}) \tag{13}$$

$$\boldsymbol{K}_k = \boldsymbol{K}_{k-1} + H_k^{\mathrm{T}} H_k \tag{14}$$

式中：$\boldsymbol{K}_0 = H^{\mathrm{T}} H$；$\boldsymbol{K}_1 = \boldsymbol{K}_0 + H_1^{\mathrm{T}} H_1$。

根据以上步骤，更新多批次实时数据的输出权重，训练OSELM单隐含前馈神经网络完毕。

2 实验和性能分析

2.1 实验数据

基于新能源电站SCADA系统所处的现实环境，本文中应用攻击类型非常全面的AWID数据集去测试和评估所提出的OSELM方法的性能和稳定性。在训练和测试过程中，训练数据集AWID-CLSR-Trn包括中1 633 190正常实例和162 385条攻击流量。AWID-CLSR-tst作为测试数据集，其中正常的数据流量为530 785条，攻击的流量为44 858条。表1给出了训练和测试集中不同种类攻击的分布情况。

表1 攻击分布

Table 1 Distribution of attacks

攻击类型	训练集	测试集
虚假攻击	30 522	20 079
泛洪攻击	48 484	8 097
注入攻击	83 379	16 682
总计	162 385	44 858

经上述分析可知，训练数据集中的正常和攻击数据量分布不均衡，即SCADA系统在实际运行状态下遭遇的正常流量数量远远高于攻击流量，其比值约为10∶1，这不利于训练和更新OSELM模型。为了克服数据不平衡问题，首先对数据进行归一化

处理，然后应用合成少数类过采样技术，即ADASYN方法对数据集进行平衡处理，使正常流量数据集和攻击流量数据集的比值维持在1∶1附近。经过随机处理后的正常流量数量缩减为170 000条。本文将经过处理后得到的均衡数据集作为样本数据，对OSELM分类器进行训练获得不均衡数据集，最后对模型进行验证。

经对新能源电站的实际运行条件进行考察和调研，本文所使用的AWID数据集具有以下特点：

（1）最大程度模拟真实的网络和流量。在理想条件下，数据集意外往往很少出现，这往往是基于更清晰的反应攻击的真实影响以及工作站的应答。基于此，本文所采用的原始数据尽可能地逼真、不掺杂任何人为的捕获和跟踪插入。

（2）对数据集进行标记。标记数据集能够有效地将异常流量与正常流量区分，能够降低人工标签的不准确性，从而对评估监测机制的稳定性具有重要意义。

（3）捕获总交互信息。搭建LAN内部和之间的数据集交换机制，获得提供检测异常行为的信息，从而能够对结果进行正确的解释和评估。

（4）数据集的完整性。本文使用的数据集的有效载荷不需要任何的清理，也不会被匿名化，能够比较完全地追踪到所有信息，从而提升了结果数据集的完整性。

目前，在新能源SCADA电站中发生的攻击在攻击频率、大小、类别和复杂性都逐渐攀升，需要广泛考量多种入侵场景来帮助研究人员进行分析和判断。

2.2　DAE约简可行性及性能分析

使用均方误差（Mean squared error，MSE）来评价预估量和被预估量的差异程度，以此来验证DAE用于数据降维的可行性，MSE的值越小，说明模型的效果越好。经过约简后的数据能否完整的反映出原数据集的信息是考察DAE重构的重要方面。本文所使用的MSE定义为

$$\mathrm{MSE}=\frac{1}{N}\sum_{i=1}^{N}(y_{\mathrm{data}}-y_{\mathrm{recon}})^2 \tag{15}$$

式中：y_{data}表示训练样本数据和测试样本数据集；y_{recon}表示重构的样本数据集；N代表在DAE过程中测试或者训练的样本数量。在本文所制造的攻击中，主要有Smurf病毒攻击，Ping-sweep扫射攻击，Syn flood链接攻击和Ping-of-death拒绝服务攻击4种类别，基于内容和链接的特征分别有96和41个，将这两种特征方式进行归一化合并处理，共得到137个实验样品数据特征。将这137个数据特征输入降噪自动编码器，输出方式选择为5维编码，以137-100-50-20-5神经元数量分布的方式设定4层DAE的网络结构，并将其分别命名为 DAE1137-100、DAE2100-50、DAE350-20 和DAE420-5。本文中降噪自动编码器模型的训练次数为10次。

从图4的各层DAE重构误差的变化曲线可以非常明显看出，经过5次训练以后，多数层的MSE已经达到1个较小值（低于0.09）并且趋于稳定。所以认为DAE的训练次数大于5时，可以得到经过降噪处理的各项初始数据。

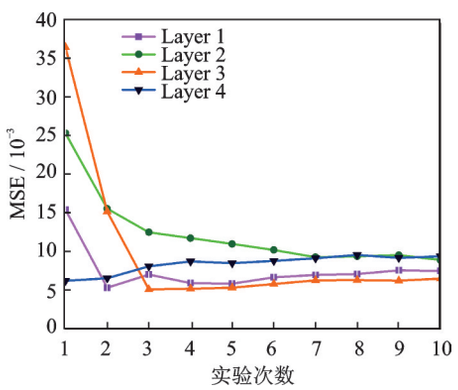

图4　各层DAE的重构误差变化曲线

Fig.4　Reconstruction error curves of DAEs

另一方面，对经过10次DAE训练以上的MSE重构误差进行研究，进一步地评估DAE降噪处理前后数据的差异。如图5所示，满足训练次数大于等于10的条件，MSE误差取值曲线已经小于0.003，并且曲线趋于稳定值，在MATLAB中的数据表明，本模型的样本数据最小MSE为0.002 25。所以输出方式选择为5维可以维持原始137维的数据集特征，从而说明了降噪自动编码在本文降维处理中的适用性。

使用较为常见的正确率（Accuracy）为评价指标，将本文多个堆叠的降噪自动编码器（Stacked denoising autoencodes，SDAE）分类模型得到的数据与对比实验中其他模型的处理效果进行比对和评

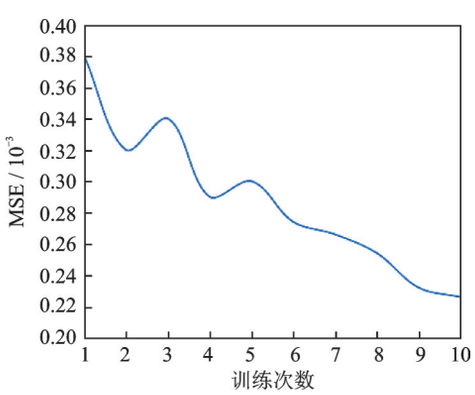

图5　DAE的重构误差变化曲线

Fig.5　Reconstruction error curves of DAE

估，进一步验证DAE在新能源电站SCADA系统攻击侵检测中特征数据约简的高效性。正确率的计算方法是被正确的划分为正类的样本测试个数除以所有样本数，其计算公式为

$$\text{Accuracy}=(\text{TN}+\text{TP})/C \tag{16}$$

式中：被正确地划分为负例的个数和被正确地划分为正例的个数分别用TN和TP表示；测试样本的综述记为C，C为N和P之和。使用这个描述符，本文对DAE、PCA、EMD三种降维方法的SVM分类器检测效果进行综合评估，通常来说，正确率越高越好，其代表DAE方法具有更高的高效性和一致性。如图6所示，10次实验中DAE+SVM的约简方法准确率数据较其他两种方法都要高，具有较大优势。

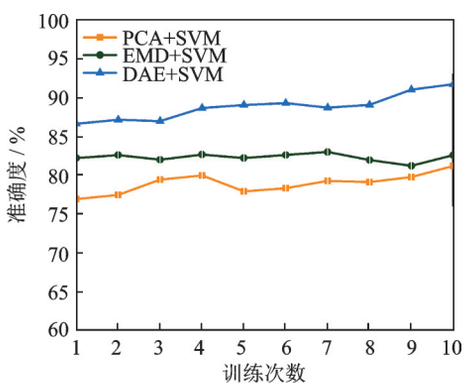

图6 不同约简方法对分类结果的影响

Fig.6 Influence of different methods on classification

为说明所提降维方法的有效性，本文分别对PCA、EMD、DAE三种降维方法的OSELM分类器检测效果进行综合评估。如图7所示，10次实验中DAE+OSELM方法的准确率较其他两种方法都要高，验证所提方法的正确性。

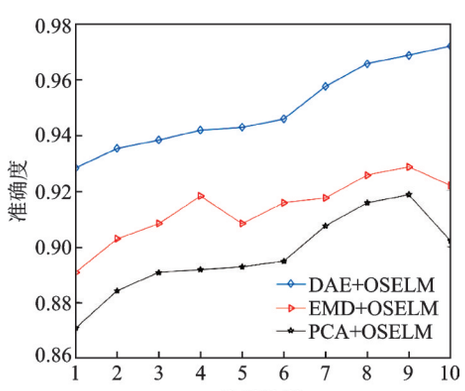

图7 不同约简方法对OSELM检测效果影响

Fig.7 Influence of different methods on OSELM detection

2.3 预处理对检测结果的影响

为了使模型获得良好的学习精度和性能，本文对包含缺失值和重复值的原始检测结果进行预处理，主要用到ADASYN算法和DAE算法两种算法对数据进行预处理。为了评价这两种方法与OSELM同时使用时对分类结果的影响，先后搭建了OSELM，ADASYN+OSELM，DAE+OSELM，ADASYN+DAE+OSELM，DAE+ADASYN+OSELM五种分类方法，算法执行顺序为命名中的先后顺序。

在OS-ELM的网络结构和参数相同的情况下，将ADASYN的采样率设置为N，并且将N的变化范围规定为1～30。将DAE的噪声系数设置为0.10。为了使模型达到更加优异的稳定性和精确度，经过预实验，采用ADASYN+OSELM算法来确定最优采样率。采样率N的值与分类结果之间的关系如图8所示。图中Pre代表精度，Rec代表召回率，AUC代表ROC曲线下面积，可以看到在0～18范围内ADASYN+OSELM的性能与N值具有一定的正相关的关系，当N值取18左右时，OSELM达到最优的求解性能，当N值在18～30区间内时，OSELM模型分类性能逐渐下降。综上，可以看出预处理操作对本节中5种分类方法具有不同的影响。

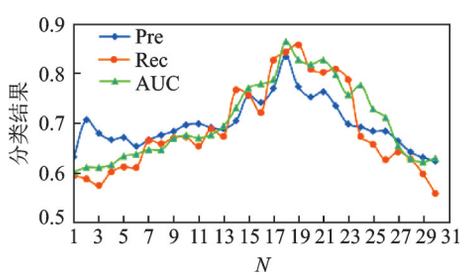

图8 N与分类结果之间的关系

Fig.8 Relation between N and classification result

2.4 OSELM与其他分类器比较

为了证明本文所提出的OSELM分类器的准确性和稳定性，并且保证结果的可靠度，以DAE和ADASYN算法处理后的数据为实验数据集，使用平均分类时间，将OSELM方法与传统ELM模型和SVM方法进行相同状态下的对比，以10次十折交叉验证对应的平均值为描述符。获得ROC曲线如图9所示，可以看到OSELM单分器对应的数据具有最高的真正类率。

激活函数是影响ELM分类器性能的重要因素。为了达到选择最佳激活函数的目标，本文在相同实验条件下对“Sigmoid”“Sin”“Hardlim”“Tribas”和“Radbas”5种不同类别的激活函数进行测试，对使用不同激活函数所获得的训练时间/检测时间/检测精度和训练精度进行评估和分析。

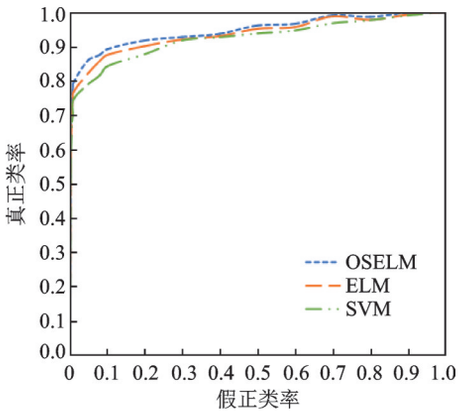

图 9　单分类器比较

Fig.9　Comparison of single classifier

基于深度学习的ELM分类器性能受其自身的激活函数的制约。本文通过使用MATLAB对6种常见的激活函数进行试验（“Sigmoid”“Sin”“Tanh”“Hardlim”“Tribas”和“Radbas”），最终筛选出最适合OSELM的激活函数。具体来说，首先收集降至5维的数据集，然后使用上述激活函数进行运算，每个激活方式进行100次重复试验。从平均检测时间、平均训练时间、平均检测精度和训练精度4个方面进行数据统计。所得数据如表2所示，可以发现“Sigmoid”这种“S”型的饱和激活函数有着最短的平均训练时间，并且平均精度都要比其他的激活函数高，适合应用于OSELM，故选择其为激活函数。

表 2　5种激活函数性能比较

Table 2　Performance comparison between five activation functions

激活函数	平均训练时间/s	平均检测时间/10^{-2} s	平均检测精度/10^{-2}	调练精度
Sigmoid	59.4	10.12	97.8	1
Sin	63.2	12.58	92.1	1
Hardlim	65.5	14.54	89.8	1
Tribas	68.7	16.84	92.1	1
Radbas	69.3	17.91	91.1	1

在现实SCADA能源电站的攻击检测过程中，实时性检测出攻击是系统具有优异准确性和稳定性的重要标志。为了对本文中提出的OSELM方法对Wi-Fi检测的实时性进行评估，分别使用SADE方法将1 800个样本的训练数据集进行5～50维的模型降维训练，然后使用3种分类器对600个降维训练的样品数据集进行检测时间的统计，所得统计结果如图10所示。可以看出，OSELM经过5维模型降维训练后所对应的检测时间最低，约为28 ms，低于传统ELM模型和支持向量机方法，具有最快的相应速度。另一方面，OSELM表现出了较为稳定的检测时间，而非如其他两种方法那样随着维度增加使检测时间显著升高。综上所述，OSELM模型能够节约大量的检测时间，并且不随检测维度的变化产生大的波动，具有优良的检测实时性。

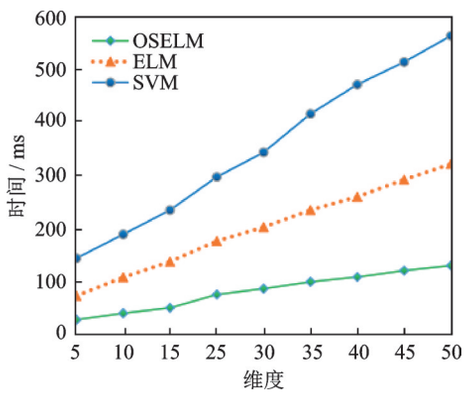

图 10　不同分类器的检测时间

Fig.10　Detection time of classifiers

为验证所提方法较现存方法ELM及SVM的优势，本文首先将实验数据约简至5维再进行实验，从表3中可以看出，所提方法较ELM和SVM更有优势，基于ELM的检测方法较SVM有了较大提升。结合图10可知，虽然OSELM较ELM提升幅度不大，但时间有了明显提升。

表 3　5种激活函数性能比较

Table 3　Detection performance comparison of OSELM, ELM and SVM

分类器	OSELM	ELM	SVM
准确度/%	93.24	91.15	86.23

本文选用机器学习算法集成平台Weka进行实验。选取J48算法，随机森林算法（Random forest，RF）和朴素贝叶斯方法（Naïve Bayes，NB）作为分类器与所提方法进行比较，且实验中所使用的数据集经过ADASYN和DAE处理。图11显示了由RF分类器完成的分类的相应裕度曲线。同样，图12和图13分别展示了基于NB算法和J48算法对应的裕度曲线。由图11～13可以看出，基于RF和NB算法的分类器性能接近，基于J48算法的分类器性能最差。如表4所示，所提出的OSELM方法与其他3个模型（J48、RF和NB）相比，OSELM具有最高的检测精度，达到97.8%，故基于OS-ELM的分类起检测性能最优。实验结果数据与表4中显示的数值一致。

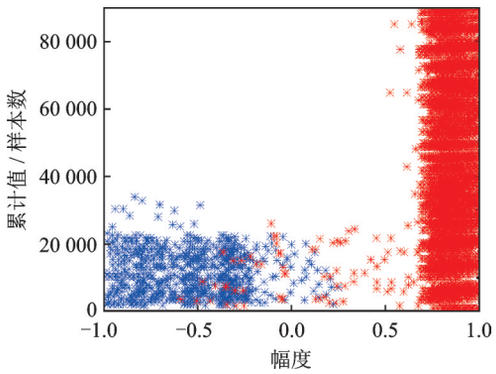

图 11 RF 可视化裕度曲线

Fig.11 Margin curve of RF

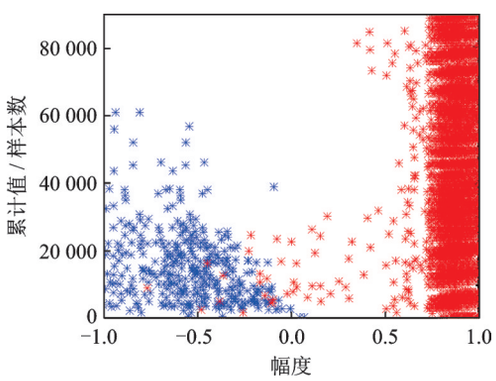

图 12 NB 可视化裕度曲线

Fig.12 Margin curve of NB

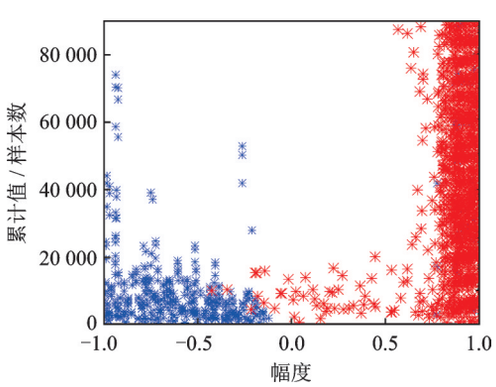

图 13 J48 可视化裕度曲线

Fig.13 Margin curve of J48

表 4 J48, NB 和 RF 算法之间的比较

Table 4 Performances of J48, NB, RF and OSELM

分类器	J48	NB	RF	OSELM
正确分类实例	540 932	545 767	557 222	565 167
错误分类实例	34 711	29 876	18 421	10 476
正确分类实例的准确性/%	93.97	94.95	96.80	98.180
分类实例的不正确准确度/%	6.03	5.05	3.20	1.82
Kappa	0.929 8	0.948 1	0.954 2	0.972 6
实例总数	575 643	575 643	575 643	575 643

3 结 论

本文提出了一种基于改进极限学习机 OS-ELM 的新能源电站 SCADA 系统攻击检测方法。首先，为了平衡真实世界中新能源电站 SCADA 系统中的正常和攻击数据集，使用合成少数类过采样技术对数据进行归一化和平衡化处理，获得样本数量均一的多种数据集。随后，使用鲁棒性更强的 DAE 算法对获得的数据集进行降维降噪处理，对攻击检测模型的复杂度进行了精简。最后，在 Weka 平台中对所提出的 OSELM 检测模型进行评估和分析，发现本文所提出的 OSELM 检测模型比 J48 算法、随机森林算法和朴素贝叶斯方法性能都要优异和准确。OSELM 除实现了快速的检测执行时间，还具有更高的检测精确度和更低的报错率，可以承担新能源 SCADA 电站风险攻击检测和预警的系统工程。应当说明的是，本文所提出的 OSELM 不具备在线检测功能，仍需要对模型进一步优化和增强。

参 考 文 献：

[1] ARAD-VOSK N, BEACH R, RON A, et al. Infrared photoconductivity and photovoltaic response from nanoscale domains of PbS alloyed with thorium and oxygen[J]. Nanotechnology, 2018, 29(11): 115202.

[2] BARBOUR K, MCCLUNE DW, DELAHAY R J, et al. No energetic cost of tuberculosis infection in European badgers (Meles meles)[J].J Anim Ecol, 2019, 88(12): 96-110.

[3] 陈敏康. 浅析智能配电网技术在配电网规划中的应用. 电力系统装备[J]. 2019, 28(17): 40-42.
CHEN Minkang. Application of intelligent distribution network technology in distribution network planning. Power system equipment[J].2019, 28(17): 40-42.

[4] 齐星，李光磊，周华春，等. 多数据中心基于流量感知的 DDoS 攻击消除策略[J]. 计算机工程与应用，2018, 54(24): 87-96.
QI Xing, LI Guanglei, ZHOU Huachun, et al. DDoS attack elimination policy based on traffic awareness for multidata center[J]. Computer Engineering and Applications, 2018, 54(24): 87-96.

[5] BONOMI S, MARONGIU D, SESTU N, et al. Novel physical vapor deposition approach to hybrid perovskites: Growth of MAPbI3 thin films by RF-magnetron sputtering[J]. Sci Rep, 2018, 8(1): 15388.

[6] EHAMPARAM R, OQUENDO L E, LIAO M W, et al. Axially bound ruthenium phthalocyanine monolayers on indium tin oxide: Structure, energetics, and charge transfer properties[J]. ACS Appl Mater Interfaces, 2017, 9(34): 29213-29223.

[7] JAMES D V, MULLEN P E, MELOY J R, et al. Stalkers and harassers of British royalty: An exploration of proxy behaviours for violence[J]. Behav Sci Law, 2011, 29(1): 64-80.

[8] 齐林，王伟，吴忱. 长输管道SCADA保护报警信息与现场处置[J]. 中国石油和化工标准与质量，2019，39(15)：134-135.
LIN Qi, WEI Wang, CHEN Wu. Alarm information and field disposal of long distance pipeline SCADA protection[J]. Chinese Petroleum and Chemical Standards and Quality, 2019, 39(15): 134-135.

[9] PARK S, SEO S, KIM J. Network intrusion detection using stacked denoising autoencoder[J]. Advanced Science Letters, 2017, 23(10): 9907-9911.

[10] SHONE N, NGOC T N, PHAI V D, et al. A deep learning approach to network intrusion detection[J]. IEEE Transactions on Emerging Topics in Computational Intelligence, 2018, 2(1): 41-50.

[11] SAXENA H, RICHARIYA V. Intrusion detection in KDD99 dataset using SVM-PSO and feature reduction with information gain[J]. International Journal of Computer Applications, 2014, 98(6): 25-29.

[12] YANG Y, CHEN W G. Taiga: Performance optimization of the C4.5 decision tree construction algorithm[J]. TUP Journals & Magazines, 2016, 21(4): 415-425.

[13] SAXENA H, RICHARIYA V. Intrusion detection in KDD99 dataset using SVM-PSO and feature reduction with information gain[J]. International Journal of Computer Applications, 2014, 98(6): 25-29.

[14] KOLIAS C, KAMBOURAKIS G, STAVROU A, et al. Intrusion detection in 802.11 networks: Empirical evaluation of threats and a public dataset[J]. IEEE Communications Surveys & Tutorials, 2015, 18(1): 184-208.

[15] YU Z H, CHIN W L. Blind false data injection attack using PCA approximation method in smart grid[J]. IEEE Transactions on Smart Grid, 2015, 6(3): 1219-1226.

[16] CHEN Z, ZHU Q, CHAI S Y, et al. Robust human activity recognition using smartphone sensors via CT-PCA and online SVM[J]. IEEE Transactions on Industrial Informatics, 2017, 11(99): 1-1.

[17] HE H, BAI Y, GARCIA E A. et al. ADASYN: Adaptive synthetic sampling approach for imbalanced learning[C]//Proceedings of International Joint Conference on Neural Networks. Shenzhen, China: IEEE, 2008: 1322-1328.

[18] TANG J X, DENG C W, HUANG G B. Extreme learning machine for multilayer perceptron[J]. IEEE Transactions on Neural Networks and Learning Systems. 2016, 27(4): 809-821.

（编辑：刘彦东）