基于特征组合优化的工业互联网恶意行为实时检测方法

胡向东[1,2],张 琴[2]
(1. 重庆邮电大学现代邮政学院,重庆 400065;2. 重庆邮电大学自动化学院/工业互联网学院,重庆 400065)

摘 要: 工业互联网中节点数据具有高维、冗余和海量等特性,传统的恶意行为检测模型无法对工业互联网恶意攻击行为做出快速且准确的判断,提出基于特征组合优化的工业互联网恶意行为实时检测方法. 采用改进的相关性快速过滤算法和基于奇异值分解的主成分分析算法对工业互联网恶意行为样本数据进行特征组合优化,基于对称不确定性信息度量指标和近似马尔科夫毯准则进行特征相关性计算、冗余特征识别与排除,通过参数特征维度的不同配置得到若干候选特征组合;利用决策树评估器筛选出准确率最高的候选特征组合;通过奇异值分解的主成分分析进一步进行特征降维,得到低维高信息量的最优特征组合;结合极端梯度提升算法和优化的特征组合对工业互联网恶意行为样本进行分类,基于密西西比州立大学多分类电力系统攻击样本数据对本文方法进行了验证;实验结果表明,特征组合优化检测模型训练时间可缩减 57.53%,单个样本的平均检测时间为 0.002 ms,可减少 23.99%,基于特征组合优化的检测模型的准确率、召回率和 $F1$ 值较特征优化前分别提升了 1.11%、1.25% 和 1.01%. 本文方法的突出优势表现为在提升模型检测效果的同时可明显降低模型检测时间,能更好适应工业互联网的实时性要求.

关键词: 工业互联网;改进的相关性快速过滤算法;奇异值分解的主成分分析;特征组合优化;极端梯度提升;恶意行为实时检测

基金项目: 重庆市级人才计划项目(No.cstc204ycjh-bgzxm0088)

中图分类号: TN918.91;TP391.9 **文献标识码:** A **文章编号:** 0372-2112(2024)09-3075-11

电子学报 URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20221394

Real-Time Detection Method of Malicious Behaviors in Industrial Internet Based on Feature Combination Optimization

HU Xiang-dong[1,2], ZHANG Qin[2]
(1. *School of Modern Posts, Chongqing University of Posts and Telecommunications, Chongqing* 400065, *China*;
2. *School of Automation/School of Industrial Internet, Chongqing University of Posts and Telecommunications, Chongqing* 400065, *China*)

Abstract: The data of nodes in industrial Internet have characteristics of high dimensionality, redundancy and mass and traditional malicious behaviors detection model cannot make a fast and accurate judgment on the malicious behaviors of industrial Internet. A real-time detection method of malicious behaviors in industrial Internet based on feature combination optimization is proposed. The feature combination of industrial Internet malicious behaviors sample data are optimized by improved fast correlation filtering algorithm and principal component analysis algorithm based on singular value decomposition. Based on symmetric uncertainty information measurement index and approximate Markov blanket criterion, feature correlation calculation, redundant feature identification and exclusion are performed. Several candidate feature combinations are obtained from different configurations of feature dimensions; Use decision tree evaluator to select the feature combination with the highest accuracy; To acquire the optimal feature combination of lower dimension and higher valuable information, the principal component analysis of singular value decomposition is used for further reduce dimension of feature; To classify malicious behaviors samples in industrial Internet through combing extreme gradient boosting algorithm and the optimized feature combination. The proposed method is verified based on Mississippi State University's multi-class power system attack sample data; The experiment demonstrate that training time of the feature combination optimization detection model can be reduced by 57.53%, and the average detection time of a single sample is 0.002 ms, which can be reduced by

收稿日期:2022-12-15;修回日期:2023-05-04;责任编辑:梅志强

23.99%. The accuracy, recall and $F1$ value of the detection model based on feature combination optimization are improved by 1.11%, 1.25% and 1.01%, respectively compared with those before feature optimization. The outstanding advantage of method in this paper is that it can significantly reduce model detection time while improving model detection effect, and can better adapt to the real-time requirements of industrial Internet.

Key words: industrial Internet; improved fast correlation filtering algorithm; principal component analysis algorithm based on singular value decomposition; feature combination optimization; extreme gradient boosting; real-time detection of malicious behaviors

Foundation Item(s): Chongqing Municipal Talent Program Project (No.cstc204ycjh-bgzxm0088)

1 引言

工业互联网是我国制造业智能化转型的核心支撑,其作为新一代信息技术与工业技术深度融合的产物,推动传统工业制造体系数字化、网络化和智能化变革. 但同时打破了工控系统原有的依靠独立性所建立起的防御屏障,使工业生产遭到各类网络安全威胁,针对工业互联网的恶意行为攻击事件层出不穷[1]. 传统工业环境普遍缺乏完善的信息安全防御体系,无法防御来自网络的各类恶意行为攻击,工业互联网接入设备的多样性和差异性也使其防护变得更加困难. 工业互联网具有高实时性、资源受限和更新困难等特性[2],其场景下的恶意行为检测方法也需要结合这些特性来进行研究,传统的恶意行为检测技术未充分考虑到工业互联网的特性,因此无法直接移植用于工业互联网恶意行为检测,构建工业互联网恶意行为检测模型对维护工业互联网安全具有重大意义.

工业互联网中节点数据具有高维、冗余等特性,使得传统的恶意行为检测模型对各类工业互联网恶意行为的决策性能较差,模型检测的实时性不强. 因此大量研究人员通过特征选择方法约简待检测目标属性集,进而提高模型检测效率[3]. 特征选择方法整体上可划分为过滤式、嵌入式和包裹式[4]. 基于信息论的过滤式特征选择方法具有计算成本低、可直接从数据中获取重要价值信息且通用性强等优点,因此被广泛应用[5]. 如DONG等人[6]提出了基于互信息的工业互联网恶意行为检测模型,采用互信息度量指标进行特征过滤,模型在获取较高检测精度的同时也有效降低了数据维度过高导致的高计算成本. KRITHIVASAN等人[7]使用增强的主成分分析和特征超图修剪对属性集进行降维和冗余特征消除,有效减少了检测模型在训练和测试时间方面的计算开销. 任家东等人[8]采用皮尔逊相关系数度量特征与类别之间的相关性,结合随机森林模型确定了二分类和多分类实验中皮尔逊系数的阈值,筛选出对分类效果影响程度较大的特征,有效提高了模型精度,但该方法不能有效度量特征与特征之间的相关性,忽略了冗余特征对分类效果的影响.

深度学习技术能够自主进行特征提取,近年来被广泛应用于恶意行为检测领域. 如SÜZEN等人[9]结合深度信念网络和Softmax分类器构建网络入侵检测系统,对工业控制系统中的响应注入、命令注入和拒绝服务等攻击类别进行判定,其检测精度相比于基于深度信念网络的旧系统提升了5%;尚文利等人[10]结合自编码神经网络和长短期记忆神经网络构建了基于时间序列的异常检测模型,有效提高了工业网络安全防护中工艺数据的异常检测准确率;ZHAO等人[11]提出一种基于分层深度学习的异常检测方法,结合卷积神经网络和长短期记忆网络从工业通信数据中提取状态特征和传输连接特征,模型检测准确率达到99.80%;刘文军等人[12]利用带有门控循环单元、多层感知器和Softmax的循环神经网络来识别网络入侵,在基准数据集KDD99和NSL-KDD上的总检出率分别为96.43%和99.33%. 上述基于深度学习技术所构建的恶意行为检测系统均取得了较高的检测准确率,但工业互联网领域的恶意行为数据具有海量特性,基于深度学习的检测模型的检测效率较低. 机器学习技术具有较高的计算效率,因此越来越多的网络安全领域研究人员开始采用各类机器学习算法构建恶意行为检测模型,用于检测各类恶意行为.

为了降低工业互联网恶意行为样本数据中冗余信息对检测模型的计算资源消耗以及对模型决策的干扰,提升模型对恶意行为判别的实时性,本文提出基于特征组合优化的工业互联网恶意行为实时检测方法. 通过降维算法约简目标属性集,得到一组低维度、低冗余、高信息量的特征组合,结合极端梯度提升算法构建分类模型实现对各类工业互联网恶意行为的快速准确地识别.

2 恶意行为数据特征组合优化

工业互联网恶意行为以工业基础设备、工业控制系统、工业网络为攻击目标,旨在破坏关键生产流程、窃取工业制造关键信息、获得非法访问权限、恶意操控篡改工控数据等. 当系统遭受到恶意行为攻击,网络流量数据、各节点数据将异于正常数据;通过分析网络流量数据特征或节点数据特征可有效识别正常行为和恶意行为. 但由于工业互联网恶意行为具有较高复杂性

和多样性,不同类别的攻击具有不同的特点,且工业数据具有高维、冗余和海量等特性,使得检测模型的时间成本高、检测精度低,如何快速有效识别不同类别的恶意行为关键在于提取出低维有效特征. 鉴于数据特征与不同类别的工业互联网恶意行为之间具有不同程度的关联性,与类别关联程度较高的特征有利于识别出不同类别的恶意行为,本文提出一种基于改进的相关性快速过滤算法和奇异值分解的主成分分析算法的特征组合优化方法,对待检测的工业互联网恶意行为数据进行特征选择与降维. 通过计算特征之间,特征与类别之间的对称不确定性来度量两者的相关性程度,首先通过阈值设定滤除无关特征和与类别相关性极低的特征,但由于特征之间往往存在冗余,与类别具有高相关性的特征组合不一定最佳,进而基于近似马尔科夫毯准则对冗余特征进行识别并排除,改进的相关性快速过滤算法中引入了新的搜索策略,以特征组合维度为停止准则,构建具有不同合适维度的候选特征组合,克服了传统的相关性快速过滤算法快速尖锐的特征消减模式[13];采用决策树模型的准确率作为评价准则筛选得到最佳候选特征组合;为了克服工业互联网恶意行为数据维度过高导致模型决策时间成本过高,利用奇异值分解的主成分分析算法对所筛选出的特征组合进一步进行降维.

2.1　基于对称不确定性的相关性分析

对称不确定性(Symmetric Uncertainty,SU)对互信息量进行了归一化,可应用于评估两个变量之间的相关性. 其值的大小反映了在以其中一个变量作为前提下,另一个变量代表的事件发生的不确定性的降低程度,SU值越大,则表示条件变量对于另一事件变量的不确定性减少程度越大,事件变量发生的概率就越大,该条件变量的重要性程度越高. 对于N维特征集F中的任意特征F_k与类别C而言,若两者之间的对称不确定性越大,代表两者之间的相关性越强,特征F_k对于分类具有关键作用,特征F_k与类别C的对称不确定性$\mathrm{SU}(F_k,C)$定义如式(1)所示[14].

$$\mathrm{SU}(F_k,C)=2\left[\frac{H(C)-H(C|F_k)}{H(F_k)+H(C)}\right] \tag{1}$$

其中,$H(F_k)$,$H(C)$分别为F_k和C的信息熵,定义如式(2)和式(3)所示,$H(C|F_k)$为条件熵,定义如式(4)所示.

$$H(F_k)=-\sum_i f_i \log_2 p(f_i) \tag{2}$$

$$H(C)=-\sum_j c_j \log_2 p(c_j) \tag{3}$$

$$H(C|F_k)=-\sum_i p(f_i)\left(\sum_j p(c_j|f_i)\log_2 p(c_j|f_i)\right) \tag{4}$$

式(2)~(4)中,f_i,c_j分别表示特征F_k,类别C所有可能的取值,$P(f_i)$表示特征F_k的先验概率,$P(c_j)$表示类别C的先验概率,$P(c_j|f_i)$表示F_k发生的前提下C发生的后验概率. 通过以上式子即可计算出每个特征F_k与类别C的对称不确定性$\mathrm{SU}(F_k,C)$,特征F_m与特征F_n的对称不确定性$\mathrm{SU}(F_m,F_n)$.

2.2　基于近似马尔科夫毯的冗余性分析

通过寻求目标特征的马尔科夫毯和非马尔科夫毯可有效进行特征选择,对于给定目标特征$F_k\subset F$,特征子集$M\subset F(F_k\notin M)$,若满足式(5)的条件,即在给定特征子集M的条件下,目标特征F_k与集合$\{F-M-\{F_k\}\}$相互独立,则称M为目标特征F_k的马尔科夫毯,$\{F-M-\{F_k\}\}$则称为目标特征F_k的非马尔科夫毯.

$$F_k\perp\{F-M-\{F_k\}\}|M \tag{5}$$

特征F_k的马尔科夫毯蕴含着其全部的信息,若存在特征子集$M\subset F(F_k\notin M)$为F_k的马尔科夫毯,则特征F_k可判定为冗余特征. 但马尔科夫毯运算量较大,实现条件过于严苛,因此采用近似马尔科夫毯准则对冗余特征进行判别与排除,对于特征F_m和$F_n(m\neq n)$,F_m是特征F_n的近似马尔科夫毯,判定F_n为冗余特征需满足式(6)的条件.

$$\begin{cases}\mathrm{SU}(F_m,C)>\mathrm{SU}(F_n,C)\\ \mathrm{SU}(F_n,C)<\mathrm{SU}(F_m,F_n)\end{cases} \tag{6}$$

2.3　基于奇异值分解的主成分分析算法的特征降维

主成分分析方法基于方差最大化理论,在保留原始数据的大部分信息量的前提下,通过矩阵分解将原始数据映射到低维线性子空间,创造出新的特征向量组合,实现数据降维. 常用的通过特征值分解求解目标协方差矩阵的特征值获取新特征向量的方法计算量较大且存在一定的舍入误差,且特征值分解局限于方阵,因此采用基于奇异值分解矩阵的主成分分析方法对目标特征向量进行降维. 对于任意矩阵$\boldsymbol{A}\in\mathbf{R}^{m\times n}$,其奇异值分解表示为[15]:

$$\boldsymbol{A}=\boldsymbol{U}\boldsymbol{\Sigma}\boldsymbol{V}^{\mathrm{T}} \tag{7}$$

其中,$\boldsymbol{U}$,$\boldsymbol{V}$为正交阵,$\boldsymbol{U}=(\boldsymbol{u}_1,\boldsymbol{u}_2,\cdots,\boldsymbol{u}_m)\in\mathbf{R}^{m\times n}$,$\boldsymbol{V}^{\mathrm{T}}=(\boldsymbol{v}_1,\boldsymbol{v}_2,\cdots,\boldsymbol{v}_n)\in\mathbf{R}^{m\times n}$,分别称为左奇异矩阵和右奇异矩阵,$\boldsymbol{u}_i$和$\boldsymbol{v}_i$分别为左奇异向量和右奇异向量,$\boldsymbol{\Sigma}$为对角阵且$\boldsymbol{\Sigma}=\mathrm{diag}(\sigma_1,\sigma_2,\cdots,\sigma_r)\in\mathbf{R}^{m\times n}$,$\sigma_i$为奇异值且降序排列,$r=\min(m,n)$为奇异值的个数.

由式(7)可得,矩阵$\boldsymbol{A}^{\mathrm{T}}\boldsymbol{A}$可表示为:

$$\boldsymbol{A}^{\mathrm{T}}\boldsymbol{A}=\boldsymbol{V}\boldsymbol{\Sigma}^{\mathrm{T}}\boldsymbol{U}^{\mathrm{T}}\boldsymbol{U}\boldsymbol{\Sigma}\boldsymbol{V}^{\mathrm{T}} \tag{8}$$

对于正交矩阵$\boldsymbol{U}$、$\boldsymbol{V}$,$\boldsymbol{U}^{\mathrm{T}}\boldsymbol{U}=\boldsymbol{E}$,$\boldsymbol{E}$为单位矩阵,$\boldsymbol{V}^{\mathrm{T}}=\boldsymbol{V}^{-1}$,$\boldsymbol{\Sigma}^{\mathrm{T}}\boldsymbol{\Sigma}=\mathrm{diag}(\sigma_1{}^2,\sigma_2{}^2,\cdots,\sigma_n{}^2)$,则式(8)可转化为:

$$\boldsymbol{A}^{\mathrm{T}}\boldsymbol{A}=\boldsymbol{V}\boldsymbol{\Sigma}^{\mathrm{T}}\boldsymbol{\Sigma}\boldsymbol{V}^{-1} \tag{9}$$

式(9)可看做矩阵$\boldsymbol{A}^{\mathrm{T}}\boldsymbol{A}$的特征值分解,可以得出,

矩阵$\boldsymbol{A}^{\mathrm{T}}\boldsymbol{A}$的特征向量组成的矩阵为右奇异矩阵$\boldsymbol{V}^{\mathrm{T}}$,矩阵$\boldsymbol{A}^{\mathrm{T}}\boldsymbol{A}$的特征值为矩阵$\boldsymbol{A}^{\mathrm{T}}$的奇异值的平方.同理,左奇异矩阵$\boldsymbol{U}$为矩阵$\boldsymbol{A}\boldsymbol{A}^{\mathrm{T}}$的特征向量,矩阵$\boldsymbol{A}\boldsymbol{A}^{\mathrm{T}}$的特征值为矩阵$\boldsymbol{A}$的奇异值的平方,因此利用奇异值分解可避免计算协方差矩阵等结构复杂的矩阵,直接求解出新特征空间$\boldsymbol{V}^{\mathrm{T}}$和降维后的新特征矩阵.在利用主成分分析算法实现降维过程中,可先利用奇异值分解获得原始数据$\boldsymbol{X}_{m\times n}$的新特征空间$\boldsymbol{V}^{\mathrm{T}}{}_{n\times n}$,即奇异值分解的右奇异矩阵,选取信息量最大的前$k$个特征向量,构成降维后的新特征空间$\boldsymbol{V}^{\mathrm{T}}{}_{k\times n}$,然后对原始数据$\boldsymbol{X}_{m\times n}$进行映射求解新特征矩阵$\boldsymbol{X}_{\mathrm{dr}}$,可表示为:

$$\boldsymbol{X}_{\mathrm{dr}}=\boldsymbol{X}_{m\times n}\times\boldsymbol{V}_{n\times k} \tag{10}$$

式(10)中,$\boldsymbol{X}_{\mathrm{dr}}\in\mathbf{R}^{m\times k}$,成功实现了对数据列的压缩,即对数据特征向量进行了降维.

2.4 特征组合优化流程描述

特征组合优化流程描述如算法1所示,主要包含3个阶段,第一阶段为构建候选特征组合,根据式(1)计算特征与特征,特征与类别之间的对称不确性以评估两者之间的相关性,通过设定对称不确定性阈值删除与类别不相关和相关性极低的特征,利用式(6)所定义的近似马尔科夫毯准则删除相关性较高的特征组合中的冗余特征,设置特征维度参数L构建合适维度的候选特征组合;第二阶段为选取最佳候选特征组合,采用决策树作为评估器,整体准确率作为评价准则,从候选特征组合中选出准确率最高的特征组合;第三阶段为特征组合降维,利用基于奇异值分解的主成分分析算法对所获取的最佳候选特征组合进行进一步降维.

3 基于特征组合优化的工业互联网恶意行为实时检测模型

基于特征组合优化的工业互联网恶意行为实时检测模型整体架构如图1所示.其整体思路是通过改进的相关性快速过滤算法和奇异值分解的主成分分析算法对工业互联网恶意行为样本数据进行特征组合优化,对原始数据集进行特征选择与降维,进而提升检测模型的决策效率,使之能够在较短时间内对恶意行为攻击做出响应,同时结合具有较高计算效率的极端梯度提升(eXtreme Gradient Boosting,XGBoost)算法构建分类模型实现对各类工业互联网恶意行为样本的实时性判别.

由于工业互联网的各类恶意攻击行为复杂多变,浅层的机器学习算法无法深入学习到各类恶意攻击行为的特性,进而做出精准的判断.因此,本文采用XGBoost算法对特征组合优化后的恶意行为样本进行分类.XGBoost算法是CHEN等人[14]在梯度提升树的基础上进行优化得到的一种集成学习模型,通过在目标函数中引入模型复杂度实现了模型表现和运算速度的平衡,具有较高的计算效率和良好的防拟合特性.其目标函数定义如下:

$$\mathrm{obj}=\sum_{i=1}^{m}l(y_i,\hat{y}_i)+\sum_{k=1}^{K}\Omega(f_k) \tag{11}$$

其中,i表示第i个数据样本,m表示数据样本总量,$l(y_i,\hat{y}_i)$表示误差函数,y_i为数据样本x_i的真实值,$\hat{y}_i$分别为数据样本x_i的预测值,$\hat{y}_i$计算如式(12)所示,K表示模型中所建立的树的总量,$\Omega(f_k)$表示模型复杂度,f_k

算法1 基于改进的相关性快速过滤算法和奇异值分解的主成分分析算法的特征组合优化方法

输入:初始数据集$S(F_1,F_2,\cdots,F_N,C)$,SU值阈值th,候选特征组合维度L,目标特征组合维度K

过程:

1.FOR $i=1$to N

2.计算各特征F_i与类别C的对称不确定性$\mathrm{SU}(F_i,C)$

3.IF $\mathrm{SU}(F_i,C)>\mathrm{th}$

4.将F_i添加到特征组合D^*中

5.选择$\mathrm{SU}(F_i,C)$值最大的特征F_j加入目标特征组合D,并从D^*中删除F_j

6.在特征组合D^*查找F_j的近似马尔科夫毯子集,删除特征组合D^*中满足$\mathrm{SU}(F_i,F_j)>\mathrm{SU}(F_i,C)$的特征$F_i$

7.重复步骤5和6,直到满足目标特征组合D的维度为L

8.设置L值,构建具有不同合适维度的候选特征组合,重复步骤5~7

9.采用决策树作为评估器,整体准确率为评价准则,从候选特征组合中筛选出准确率最高的特征组合

10.基于改进的相关性快速过滤算法提取出的特征数据,利用奇异值分解求解出右奇异矩阵

11.通过累计可解释方差贡献率学习曲线设定目标维度K,得到新特征向量空间

12.将原始数据映射到新特征空间,得到K维新特征向量,构成目标特征组合D

输出:目标特征组合D

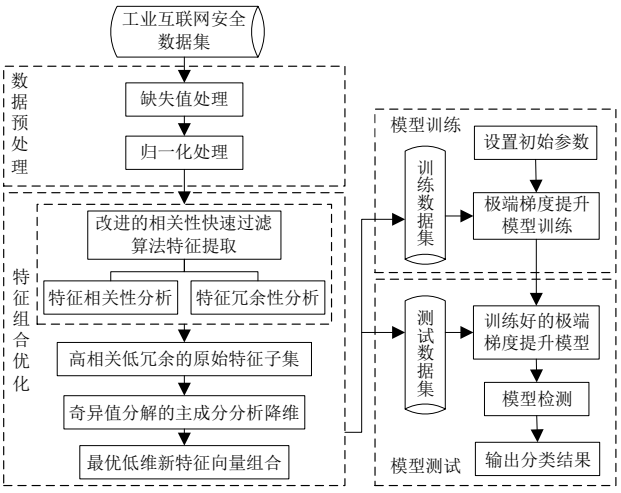

图1 基于特征组合优化的工业互联网恶意行为实时检测模型

代表所建立的第k棵树模型.

$$\hat{y}_i=\sum_{k}^{K}f_k(x_i) \tag{12}$$

其中,$f_k(x_i)$为样本x_i在第k树上的预测分数,又称叶子权重,$\hat{y}_i$则为K棵树的叶子权重之和,则样本x_i第t次迭代的预测值可表示为第$t-1$次迭代的预测值与$f_t(x_i)$之和,如式(13)所示.

$$\hat{y}_i^{(t)}=\hat{y}_i^{(t-1)}+f_t(x_i) \tag{13}$$

为了寻求目标函数与树结构f_k的直接联系,最小化目标函数,构建最优树模型,引入泰勒二阶展开式对目标函数进行展开并舍去常数项,可得:

$$\text{obj}^{(t)}=\sum_{i=1}^{m}\left[f_t(x_i)g_i+\frac{1}{2}(f_t(x_i))^2h_i\right]+\Omega(f_t) \tag{14}$$

其中,g_i和h_i为每个样本的梯度统计量,分别表示损失函数l的一阶导数和二阶导数.

对于树模型而言,每棵树都具有独特的结构,而叶子节点的模式影响了树的结构本身,并且同一叶子节点上的样本具有一致的叶子权重. 因此,在XGBoost树模型构建中,通过叶子节点的数目来表征树结构和模型复杂度,并在模型复杂度中引入了正则项来修正树模型容易过拟合的缺陷,则可通过叶子节点的数目来定义树结构和模型的复杂度,如式(15)和式(16)所示:

$$f_t(x_i)=w_q(x_i) \tag{15}$$

$$\Omega(f_t)=\gamma T+\frac{1}{2}\lambda\sum_{j=1}^{T}{w_j}^2 \tag{16}$$

其中,$w_q(x_i)$表示样本x_i落到第k棵树上的第$q(x_i)$个叶子节点上的预测分数,T为叶子节点数目,w_j为索引为j的叶子节点的叶子权重,参数γ表示复杂度惩罚项,λ表示正则化参数.

将式(15)和式(16)代入简化后的目标函数,可得:

$$\text{obj}^{(t)}=\sum_{j=1}^{T}\left[w_j\sum_{i\in I_j}g_i+\frac{1}{2}{w_j}^2\left(\sum_{i\in I_j}h_i+\lambda\right)\right]+\gamma T \tag{17}$$

其中,I_j为叶子权重为w_j所在叶子节点上的所有样本的集合,将目标函数转化为关于w_j的二次函数,通过一阶求导获取极值,当树结构确定时,叶子节点j对应的权重最优值为:

$${w_j}^*=-\frac{\sum_{i\in I_j}g_i}{\sum_{i\in I_j}h_i+\lambda} \tag{18}$$

则目标函数的最优值为:

$$\text{obj}^*=-\frac{1}{2}\sum_{j=1}^{T}\frac{\left(\sum_{i\in I_j}g_i\right)^2}{\sum_{i\in I_j}h_i+\lambda}+\gamma T \tag{19}$$

目标函数又可称为结构分数,其值越小,则代表所构建的树的结构越佳,模型训练的效果就越好. XGBoost模型构建过程中,采用贪婪算法求解最优树,选取结构分数之差最大的特征进行分枝,从而构建最优树模型.

因此,利用上述XGBoost树模型形成原理构建工业互联网恶意行为分类器,能够使本文提出的基于特征组合优化的工业互联网恶意行为实时检测模型对数据样本进行充分学习,进而更好识别出待检测的各类恶意行为,同时XGBoost算法较高的计算效率一定程度上能够有效应对工业互联网节点数据具有海量特性所带来的挑战.

4　实验结果与分析

4.1　实验数据与预处理

工业互联网广泛应用于石油、天然气、智能电网等领域,鉴于数据来源的权威性、典型性和研究对象的适用性,本文采用密西西比州立大学公开的电力系统攻击数据集[17]进行实验验证. 产生该数据集的电力系统架构如图2所示,这是一个复杂的智能电力监控系统组合,与各种智能电子设备交互,并辅以Snort和Syslog系统等网络监控设备. 该输电系统由两个发电机G1、G2和4个断路器BR1~BR4构成,BR1~BR4由智能电子继电器保护装置R1~R4控制,可以开关断路器. 这些智能电子设备通过变电站开关和路由器将信息传回数据采集和监控系统.

数据来源于对37个不同电力系统事件场景下的关键节点数据的采集,包含了28个攻击事件、8个自然事件和1个无事件场景;开源数据集经过前期的数据处理,具有工业互联网数据的一般特性. 初始数据集根据事件类别划分的不同形成了二分类、三分类和多分类3种类型的数据集,每种类型数据集包含15组数据. 其中,每个样本都包含128个特征,前116列特征来源于4个相量测量单元测量的关键电气量,包括电压和电流的相角和幅值,正序、负序、零序电压电流的相角和幅值等,在不同类别的恶意行为攻击下,相关的电气量值的变化具有特定的规律性,详细的特征描述如表1所示,其余12列特征为控制面板日志、Snort警报和继电器日志.

本文所提方法主要目的是对工业互联网领域的恶意行为进行快速精确识别分类,因此,采用多分类数据集进行实验,用于验证所构建的工业互联网恶意行为攻击检测模型对多种不同类型攻击的检测性能. 15组数据命名为数组1~15,每组数据约5 000个样本,按照数据类别将数据集划分为五个大类,数据的具体类别如表2所示.

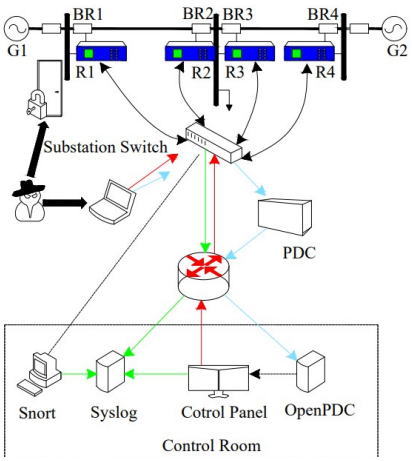

图2 电力系统架构图

表1 数据集特征描述

特征	描述
PA1: VH - PA3: VH	A-C相电压相角
PM1: V - PM3: V	A-C相电压幅值
PA4: IH - PA6: IH	A-C相电流相角
PM4: I - PM6: I	A-C相电流幅值
PA7: VH - PA9: VH	正序、负序、零序电压相角
PM7: V - PM9: V	正序、负序、零序电压幅值
PA10: VH - PA12-VH	正序、负序、零序电流相角
PM10: V - PM12: V	正序、负序、零序电流幅值
F	继电器频率
DF	单位时间继电器频率变化
PA: Z	继电器对外阻抗
PA: ZH	继电器对外阻抗角
S	继电器状态标记

表2 数据集类别描述

样本类别	标签值	标签描述
Normal Operation	0	正常样本数据
Natural Events	1	自然事件
Data Injection	2	数据注入攻击
Remote Tripping Command Injection	3	远程跳闸命令注入攻击
Relay Setting Change	4	继电器设置改变攻击

针对所采集的电力系统关键节点攻击数据，首先采用平均值法填补缺失值，同时为了降低数据之间数量级的差异对模型检测结果的干扰，对所有数据进行归一化，将所有样本特征值都归至区间[0, 1].

4.2 实验环境设置

为了确保实验结果的准确性、一致性和可对比性，本文实验均在相同的软硬件环境下进行，实验过程不使用GPU加速，实验环境配置如表3所示. 值得指出的是，该实验环境与实际应用场景的节点配置会存在一定的差异.

表3 实验环境配置

类别	参数
操作系统	Windows 10,64位
处理器	Intel(R) Core(TM) i5-1035G4
内存	8 GB
Anaconda	3
Python	3.7

4.3 性能评价指标

采用模型整体准确率(Accuracy)、召回率(Recall)、$F1$值和维度缩减率(Dimension Reduction, DR)[18]作为性能评价指标. 准确率评估了所有样本中被正确分类的占比，召回率可评估所有攻击样本中被正确预测为攻击的占比，$F1$值由精准率(Precision)和召回率共同定义，相比准确率可以更好地评估模型检测效果，DR由优化前特征数(Number of All Features, NAF)和优化后特征数(Number of Selected Features, NSF)共同决定，用于度量特征组合优化前后特征数目的减少程度，进一步说明特征选择算法的性能. 定义TP为将攻击样本预测为攻击的样本数，FN为将攻击样本识别为正常的样本数，TN为将正常样本归类为正常的样本数，FP为将正常样本判别为攻击的样本数. 准确率、召回率、精确率、$F1$值和维度缩减率DR可分别由以下公式定义：

$$\text{Accuracy}=\frac{\text{TP}+\text{TN}}{\text{TP}+\text{FN}+\text{TN}+\text{FP}} \tag{20}$$

$$\text{Recall}=\frac{\text{TP}}{\text{TP}+\text{FN}} \tag{21}$$

$$\text{Precision}=\frac{\text{TP}}{\text{TP}+\text{FP}} \tag{22}$$

$$F1=\frac{2\text{Precision}\times\text{Recall}}{\text{Precision}+\text{Recall}} \tag{23}$$

$$\text{DR}=1-\frac{\text{NSF}}{\text{NAF}} \tag{24}$$

4.4 特征组合优化结果分析

4.4.1 特征组合优化方法有效性分析

为了对样本数据进行有效的特征组合优化，首先结合改进的相关性快速过滤算法和决策树算法探索样本数据特征维度如何影响模型分类效果，同时为了避免单个数组的数据结果存在随机性，在数组1~6上进行了实验验证. 设定对称不确定性的阈值为0.01，决策树作为评估器，整体准确率作为评价准则. 图3为数组1~6经过特征组合优化后所得到的不同特征维度的数组数据的评估结果.

从图3可以看出数据特征维度与模型分类准确率整体上呈现先增后减的趋势. 由于较少的特征无法充分描述各类恶意行为的特性，较多的特征容易造成特征冗余，这两种情况下模型分类准确率均较低，随着特

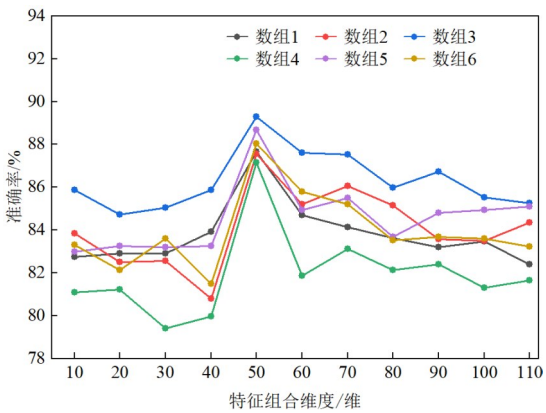

图3　特征组合维度对模型分类的影响

征维度逐渐增加,特征中所包含的样本信息更多,模型对各类样本特性的学习更加充分,因此分类准确率整体呈现上升趋势. 上述结果也充分证明特征组合优化方法的潜在有效性.

4.4.2　目标特征组合生成

实验所采用的数据类别包含正常样本数据、自然事件、虚假数据注入攻击、远程跳闸命令注入攻击、继电器设置改变攻击. 其中,虚假数据注入攻击是通过篡改电压、电流等参数值造成电路故障的假象,使操作人员出现错误判断,造成停电,远程跳闸命令注入攻击是攻击者在突破外部防御后向继电器保护装置发送命令导致断路器不能正常工作,继电器设置改变攻击是通过篡改设置来禁用其功能,使其无法在电力系统发生故障时发挥作用. 针对系统不同节点的攻击会导致不同节点的工作状态发生异常,其所对应的电气量值也会发生改变. 数据采集系统同时收集了不同事件场景下的关键节点数据,用于检测各类恶意行为. 由于数据特征维度过高且存在冗余,因此利用本文所提出的特征组合优化方法对所有样本数据进行特征选择与降维,以数组1为基准阐述数据特征组合优化的实现过程. 首先,通过计算各特征与类别之间的对称不确定性值评估各特征与类别之间的相关性程度,值越大表明两者的相关性越强,该特征更有利于模型的分类. 定义特征数字标签值依次为1~128,图4展示了数组1中各特征与类别之间的对称不确定性值.

从图4可以观察出各列特征与类别之间具有不同程度的相关性. 位于116~128列特征与类别的相关性很低或与类别完全不相关,其数据来源于控制面板日志、Snort警报和继电器日志信息. 表明针对该电力系统的攻击行为具有一定的欺骗性,成功绕过了相关的监测设备. 而前116列特征来自相量测量单元,其建立在网络层之上,为能源管理系统提供实时数据,能够实时反映当前系统的工作状态,其所测量得到的关键电气量特征值能够为识别各类恶意行为提供信息. 但同时也能发现位于15~18,44~47,73~76,102~105等列的特征与类别的相关性较低,因此有必要对数组特征做进一步筛选.

设定对称不确定性阈值为0.01,保留与类别相关性较高的特征,为了进一步降低特征与特征之间的冗余性,同样通过计算特征与特征之间的对称不确定性值评估两者之间的相关性,并基于近似马尔科夫毯准则识别出冗余特征并删除,以目标特征组合维度为停止准则. 根据图3所示的特征维度对模型分类的影响,可以发现当特征组合维度取值为50左右时,所得到的评估模型的总体准确率较高. 因此为了寻求较低维度的优化特征组合,将特征维度取值为40~50得到多组候选特征组合,以决策树模型的准确率作为评价指标筛选出准确率最高的特征组合,约简得到43维的候选特征组合:[1,3,5,7,9,11,13,19,27,28,30,32,34,36,38,39,40,42,48,56,57,59,61,63,65,67,69,71,77,85,86,88,90,92,94,97,98,100,106,107,114,115],对应的特征名称与相应的对称不确定性值如图5所示.

从图5可以看出,数组1经过特征筛选后维度由原始128维下降至43维,保留的特征与类别之间均具有较高的相关性,但也有部分相关性较高的冗余特征被滤除. 对分类影响较大的特征类别有PA:*Z*、PA:ZH、PA1:VH-PA3:VH、PA4:IH-PA6:IH和PA7:VH-PA9:VH,对分类影响较低的特征类别有*S*、DF、*F*、控制面板日志、Snort警报和继电器日志.

为了进一步降低数据维度对模型资源的消耗,提炼出关键信息用于模型训练,采用奇异值分解的主成分分析算法对提取出的特征组合进行进一步降维,利用累计可解释方差贡献率学习曲线确定降维后的特征组合维度. 数组1的累计可解释方差贡献率学习曲线如图6所示,横坐标为目标特征组合维度,纵坐标为降维后新的特征组合所包含的信息量占原始特征集信息量的多少.

从图6可以看出,当目标特征维度到达10以后,新特征组合包含的信息量达到原始数据集的95%左右,较大程度保留了原始特征信息. 为了尽可能保证降维过程中信息损失量的最小化,同时为了保证模型的检测准确率,选取了方差贡献率较高时模型识别效果最佳时的特征维度作为降维之后的新特征组合维度. 对于数组1,降维之后的特征维度为40.

利用上述特征组合优化过程对数组1~15进行了实验,各数组特征组合优化结果如表4所示. 从表4可以得出,数组1~15的特征维度缩减率最低到达62.50%,最高达到93.75%,整体维度缩减率均达到60%以上,本文所提的特征组合优化方法较大程度降低了原始数据特征维度.

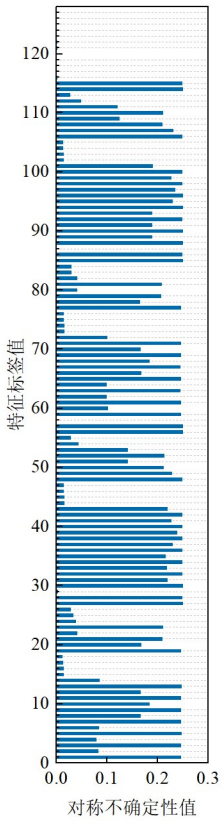

图4 数组1特征与类别的对称不确定性值

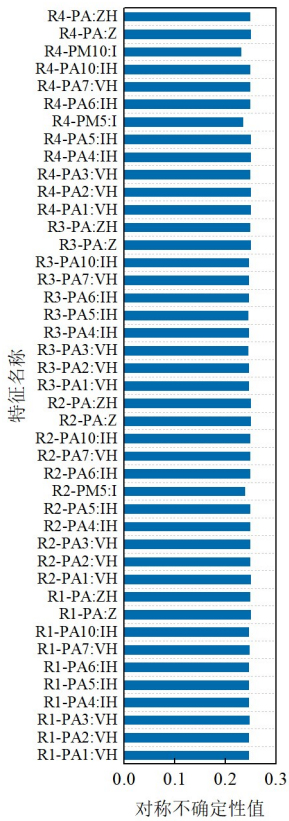

图5 数组1特征选择结果

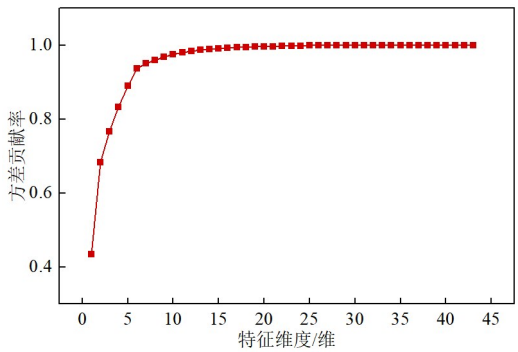

图6 数组1累计可解释方差贡献率学习曲线图

4.5 特征组合优化前后模型检测效果对比

本文提出一种基于改进的相关性快速过滤算法和奇异值分解的主成分分析算法的特征组合优化方法，为了进一步说明该方法的有效性，将特征组合优化前后的数据作为XGBoost分类模型的输入，验证所提出的特征组合优化方法对模型的影响．将特征组合优化前后的数据按照7:3划分训练集和测试集，采用XGBoost算法默认参数，迭代次数为100进行训练．分别从模型的运行时间、准确率、召回率和$F1$值4个方面进行效果对比．各组数据优化前后模型运行时间对比如图7所示，其中横坐标为数据集所包含的15组数据．

表4 数组1~15的特征组合优化结果

数据集	初始特征维度/维	优化后特征维度/维	维度缩减率/%
数组1	128	40	68.75
数组2	128	44	65.63
数组3	128	43	66.41
数组4	128	41	67.97
数组5	128	18	85.94
数组6	128	29	77.34
数组7	128	14	89.06
数组8	128	39	69.53
数组9	128	41	67.97
数组10	128	48	62.50
数组11	128	8	93.75
数组12	128	14	89.06
数组13	128	45	64.84
数组14	128	18	85.94
数组15	128	41	67.97

从图7可以看出，本文所提出的特征组合优化方法有效提高了模型的检测效率．模型的训练时间大幅度减少，特征组合优化前模型的平均训练时间为5 317.120 ms，特征组合优化后模型的平均训练时间为2 258.325 ms，训练时间整体可缩减57.53%，由于测试样本数量相对较少，测试时间整体上有小幅度减少．为了更好说明本文方法的实时性，进一步分析了特征组合优化前后单个样本的测试时间，其结果如图8所示．

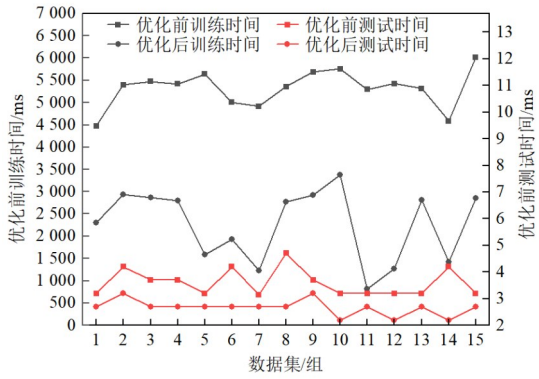

图7 特征组合优化前后模型时间对比

从图8可以看出，特征组合优化后单个样本所需的测试时间更少．经统计分析，单个样本的平均检测时间为0.002 ms，较特征优化前时间可减少23.99%．因此，结合特征组合优化和XGBoost模型的检测方法具有更强的实时性．同时，为了说明特征组合优化对模型检测效果的影响，图9展示了特征组合优化前后模型的各个评价指标值．

从图9可以看出，数组1~15的数据经过特征组合

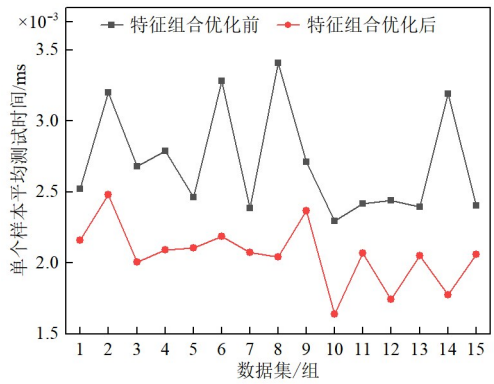

图8　特征组合优化前后单个样本平均测试时间对比

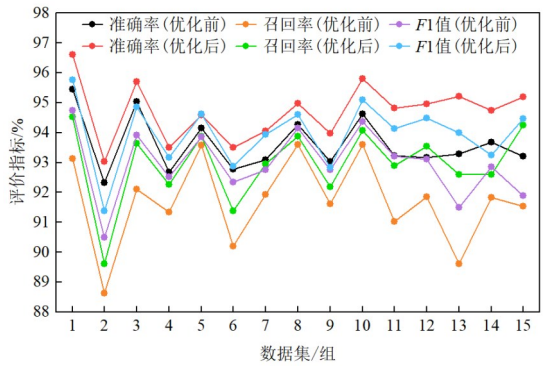

图9　特征组合优化前后模型各评价指标对比

优化后,模型的准确率、召回率和$F1$值均有所提高. 可见本文所提出的特征组合优化方法有效提取出了原始数据集中的价值信息,在降维过程中也充分保留了原始数据的关键信息,克服了传统的特征选择与降维过程中由于信息量的损失导致模型检测效果的下降. 综合分析可得,本文方法在提升模型检测效果的同时能够大幅度降低模型的检测时间. 对于工业互联网高维、海量数据而言,本文方法的时间优势会更加突出,更能适应工业互联网的实时性要求.

4.6　对比实验

为了进一步验证本文所提方法的优势,与其他特征组合优化模型的分类检测结果进行了对比,包括直接将原始数据作为分类模型输入的情形,得出15组数据的检测准确率、召回率和$F1$值的平均值如表5所示.

表5　不同特征组合优化模型的检测结果

特征组合优化模型	准确率均值/%	召回率均值/%	$F1$值均值/%
无(原始数据输入)	93.60	91.70	92.96
主成分分析算法	89.90	86.99	88.24
改进的相关性快速过滤算法	93.10	91.21	92.42
本文方法	94.71	92.95	93.97

从表5可见,利用主成分分析算法对原始数据直接进行降维,由于原始数据存在大量冗余信息,数据映射所创造的新特征同样包含了冗余信息,且降维之后信息损失较大,使得其检测过程无法精准识别出各类恶意行为,故检测效果相对最差;改进的相关性快速过滤算法因特征选择过程中损失了少量的特征信息,其检测准确率、召回率和$F1$值均有一定程度的下降;本文方法首先通过改进的相关性快速过滤算法删除冗余信息和选择出相关性较高的特征,然后利用奇异值分解的主成分分析算法对数据进行降维,不仅进一步降低了数据维度,所创造出的新特征更有利于算法对各类工业互联网恶意行为的识别,算法的准确率、召回率和$F1$值相对于未采用特征组合优化算法的原始数据输入平均分别提升了1.11%、1.25%和1.01%.

为了进一步检验本文所提方法的实时性,测试了不同特征组合优化方法的极端梯度提升分类模型的运行时间,包含模型的平均训练时间、平均测试时间和单个样本平均测试时间,实验结果如表6所示.

从表6可以推算出,相比其他3种对比特征组合优化方法,本文所提出的特征组合优化方法的训练时间和检测时间都更短,单个样本平均检测时间至少下降了7.14%,相对于无特征组合优化算法的单个样本平均检测时间下降23.99%、平均训练时间下降57.53%. 综合分析,主成分分析算法直接进行特征降维而快速做出决策,所产生的新特征向量无法有效区分各类工业互联网恶意行为,模型的检测效果有明显的降低;改进的相关性快速过滤算法有效删减了冗余特征,一定程度上降低了特征维度,模型的运行时间相比特征优化前有一定的缩减,但该方法检测效率的提升是以损失部分模型检测效果为代价的;本文方法不仅有效降低了模型的运行时间,而且提升了检测效果,具有一定优势.

表6　不同特征组合优化模型的运行时间

特征组合优化模型	平均训练时间/ms	平均检测时间/ms	单个样本平均检测时间/ms	本文方法单个样本平均检测时间相对占比/%
无(原始数据输入)	5 317.120	3.895	2.705×10^{-3}	76.01
主成分分析算法	2 402.036	3.193	2.214×10^{-3}	92.86
改进的相关性快速过滤算法	3 222.538	3.497	2.424×10^{-3}	84.82
本文方法	2 258.325	2.962	2.056×10^{-3}	100

5 结论

本文提出了基于特征组合优化的工业互联网恶意行为实时检测方法. 利用改进的相关性快速过滤算法和奇异值分解的主成分分析算法对工业互联网恶意行为样本数据进行了特征组合优化,能有效删减无关特征和冗余特征,提取出更低维度更高质量的新特征,提高模型的检测效果和检测效率,模型训练时间可缩减57.53%,单个样本的平均测试时间为0.002 ms,可缩减23.99%,模型的准确率、召回率和$F1$值较特征优化前分别平均提升了1.11%、1.25%和1.01%;本文所提的方法兼顾了工业互联网恶意行为检测实时性要求,在提升模型的检测效果的同时,能大幅度缩减模型的检测时间,相比传统的恶意行为检测方法更适用工业互联网领域. 但该方法对于区分度不高的各类攻击的辨别能力有待提升,后续工作将进一步改进模型,提升其检测能力.

参考文献

[1] ALLADI T, CHAMOLA V, ZEADALLY S. Industrial control systems: Cyberattack trends and countermeasures [J]. Computer Communications, 2020, 155: 1-8.

[2] 胡向东, 李之涵. 基于胶囊网络的工业互联网入侵检测方法[J]. 电子学报, 2022, 50(6): 1457-1465.
HU X D, LI Z H. Intrusion detection method based on capsule network for industrial Internet[J]. Acta Electronica Sinica, 2022, 50(6): 1457-1465. (in Chinese)

[3] 崔鸿雁, 徐帅, 张利锋, 等. 机器学习中的特征选择方法研究及展望[J]. 北京邮电大学学报, 2018, 41(1): 1-12.
CUI H Y, XU S, ZHANG L F, et al. The key techniques and future vision of feature selection in machine learning [J]. Journal of Beijing University of Posts and Telecommunications, 2018, 41(1): 1-12. (in Chinese)

[4] 王进, 孙万彤. 基于相关性分析的多标签特征选择方法[J]. 重庆邮电大学学报(自然科学版), 2021, 33(6): 1024-1037.
WANG J, SUN W T. Multi-label feature selection method based on correlation analysis[J]. Journal of Chongqing University of Posts and Telecommunications (Natural Science Edition), 2021, 33(6): 1024-1037. (in Chinese)

[5] GAO W F, HU L, ZHANG P, et al. Feature selection by integra-ting two groups of feature evaluation criteria[J]. Expert Systems with Application, 2018, 110: 11-19.

[6] DONG R H, WU D F, ZHANG Q Y, et al. Mutual information-based intrusion detection model for industrial internet [J]. International Journal of Network Security, 2018, 20(1): 131-140.

[7] PRIYANGA S, KRITHIVASAN K, PRAVINRAJ S, et al. Detection of cyberattacks in industrial control systems using enhanced principal component analysis and hypergraph-based convolution neural network (EPCA-HG-CNN) [J]. IEEE Transactions on Industry Applications, 2020, 56 (4): 4394-4404.

[8] 任家东, 张亚飞, 张炳, 等. 基于特征选择的工业互联网入侵检测分类方法[J]. 计算机研究与发展, 2022, 59(5): 1148-1159.
REN J D, ZHANG Y F, ZHANG B, et al. Classification method of industrial Internet intrusion detection based on feature selection[J]. Journal of Computer Research and Development, 2022, 59(5): 1148-1159. (in Chinese)

[9] SÜZEN A ALI. Developing a multi-level intrusion detection system using hybrid-DBN[J]. Journal of Ambient Intelligence and Humanized Computing, 2021, 12(2): 1913-1923.

[10] 尚文利, 石贺, 赵剑明, 等. 基于SAE-LSTM的工艺数据异常检测方法 [J]. 电子学报, 2021, 49 (8): 1561-1568.
SHANG W L, SHI H, ZHAO J M, et al. An anomaly detection method of process data based on SAE-LSTM[J]. Acta Electronica Sinica, 2021, 49 (8): 1561-1568. (in Chinese)

[11] ZHAO J M, ZENG P, CHEN C Y, et al. Deep learning anomaly detection based on hierarchical status-connection features in networked control systems[J]. Intelligent Automation & Soft Computing, 2021, 29(3): 337-350.

[12] 刘文军, 郭志民, 吴春明, 等. 基于深度学习的配电网无线通信入侵检测系统[J]. 电子学报,2020,48(8): 1538-1544.
LIU W J, GUO Z M, WU C M, et al. A deep learning based intrusion detection system for electric distribution grids[J]. Acta Electronica Sinca, 2020, 48(8): 1538-1544. (in Chinese)

[13] SENLIOL B, GULGEZEN G, YU L, et al. Fast correlation based filter (FCBF) with a different search strategy [C]//2008 23rd International Symposium on Computer and Information Sciences. Piscataway: IEEE, 2008: 1-4.

[14] 唐宏, 刘丹, 姚立霜, 等. 面向类不平衡网络流量的特征选择算法[J]. 电子与信息学报, 2021, 43(4): 923-930.
TANG H, LIU D, YAO L S, et al. Feature selection algorithm for class imbalanced Internet traffic[J]. Journal of Electronics & Information Technology, 2021, 43(4): 923-930. (in Chinese)

[15] LIU H, DONG H B, GE J, et al. High-precision sensor tuning of proton precession magnetometer by combining

principal component analysis and singular value decomposition[J]. IEEE Sensors Journal, 2019, 19(21): 9688-9696.

[16] CHEN T Q, GUESTRIN C. XGBoost: A scalable tree boosting system[C]//Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. New York: ACM, 2016: 785-794.

[17] Mississippi State University Critical Infrastructure Protection Center. Industrial control system cyber attack data set [EB/OL]. (2014-04-15) [2022-05-26]. https://sites.google.com/a/uah.edu/tommy-morris-uah/ics-data-sets.

[18] 李占山, 刘兆赓. 基于XGBoost的特征选择算法[J]. 通信学报, 2019, 40(10): 101-108.
LI Z S, LIU Z G. Feature selection algorithm based on XGBoost[J]. Journal on Communications, 2019, 40(10): 101-108. (in Chinese)

作者简介

胡向东　男,1971年生,四川广安人,博士,重庆邮电大学教授,博士生导师. 主要研究方向为智能感知、网络化测量及工业互联网安全等.
E-mail: huxd@cqupt.edu.com

张　琴　女,1997年生,重庆开州人,硕士研究生,主要研究方向为工业互联网安全.
E-mail: 1181937109@qq.com