基于改进随机森林的工业互联网安全态势评估方法

胡向东[1,2],万润楠[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: 针对工业互联网安全态势评估存在数据特征提取困难和安全态势评估准确率低等难题,提出一种基于改进随机森林的工业互联网安全态势评估方法. 基于随机采样技术平衡原始数据集以减小不平衡数据集对实验的影响;利用梯度提升决策树确定工业互联网流量数据中不同特征的权重系数,结合递归特征消除法提取其关键特征;构建基于改进随机森林的工业互联网多分类攻击检测模型,识别网络受到的攻击类别,并结合安全态势量化指标确定其风险程度. 实验结果表明,本文算法的检测准确率和$F1$值分别达到89.19%和89.68%,相较于传统随机森林算法、支持向量机和K最近邻算法,其准确率和$F1$值分别至少提高2.91%和1.7%,平均分别提高8.38%和9.33%.

关键词: 工业互联网;态势评估;特征提取;梯度提升决策树;随机森林
基金项目: 重庆市高校创新研究群体(No.CXQT20016)
中图分类号: TN918.91;TP181 **文献标识码:** A **文章编号:** 0372-2112(2024)03-0783-09
电子学报URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20220924

Method of Security Situation Assessment Based on Improved Random Forest for Industrial Internet

HU Xiang-dong[1,2], WAN Run-nan[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: Aiming at the difficulties of data feature extraction and low accuracy of industrial Internet security situation assessment method, a method of security situation assessment based on improved random forest for industrial Internet is proposed. The original data set is balanced based on random sampling technique to reduce the influence of unbalanced data set on the experiment. The gradient boosting decision tree is used to determine the weight coefficients of different features in industrial Internet traffic data, and the key features are extracted by the recursive feature elimination method. Construct a multi-classification attack detection model for the industrial Internet based on improved random forest, identify the types of attacks on the network, and determine the degree of risk in combination with the quantitative indicators of security situation. The experimental results show that the detection accuracy and $F1$ score of this algorithm reach 89.19% and 89.68% respectively. Compared with the traditional random forest algorithm, support vector machine and k-nearest neighbor algorithm, the accuracy and $F1$ score are improved by at least 2.91% and 1.7% respectively, with an average increase of 8.38% and 9.33%.

Key words: industrial internet; situation assessment; feature extraction; gradient boosting decision tree; random forest
Foundation Item(s): Chongqing University Innovation Research Group (No.CXQT20016)

1 引言

基于“互联网+”等战略的实施,工业化与信息化持续深度融合,作为新一代工业基础设施,支撑智能制造等新经济发展的工业互联网得到了快速成长且发展潜力巨大. 值得重视的是,相关机构监测发现,我国工控设备和网络系统存在着大量高危漏洞隐患[1],并且面临着越来越复杂的网络安全威胁和变化多端的攻击手段. 为应对工业互联网安全形势变化,宏观把握工业互联网的安全状况,工业互联网安全态势评估方法成为了当前研究热点之一.

国内外大量学者针对工业互联网安全态势评估展开研究. ALALI等人[2]将模糊推理的思想应用于网络安全态势评估中,从脆弱性、威胁性、可能性和影响程

收稿日期:2022-08-05;修回日期:2022-10-24;责任编辑:梅志强

度四个角度出发对网络进行安全态势评估. ZHAN 等人[3]基于定量警报质量提取攻击步骤,然后利用半马尔可夫随机场和中等粒度的攻击事件,最后将提取的攻击事件作为隐马尔可夫模型的输入进行态势评估,评估结果表明该方法的态势评估更加准确和全面,但该方法只进行警报分析不区分警报来源. WANG 等人[4]针对数据的时空特性,利用卷积神经网络提取其特征,并通过长短时记忆网络进行电力系统的态势评估. 该方法在数据量较少的情况下仍可取得较高的性能. 胡等人[5]针对工业互联网中复杂的攻击行为和非线性的网络流量数据,先使用深度信念网络对非线性特征和长距离依赖信息进行特征提取,再用双向长短时记忆网络进行攻击识别,该方法可以有效识别多数类攻击,但对小样本类攻击的识别效果不佳. HAMMAD 等人[6]通过分析网络流量的特征和数据维度进行数据预处理,并使用采样技术解决数据不平衡问题,最后构建一种利用多项式混合模型改进的随机森林算法,其检测效果较好,可以有效识别网络攻击. HAN 等人[7]针对大型网络安全问题开发了大规模网络安全态势分析系统,通过对安全要素进行高维向量分析,构建多维度、多层次和多粒度的网络安全指数,为大规模网络安全系统的设计提供了理论依据. 杨等人[8]使用编码器组成的并行特征提取网络进行信息融合,再用双向门控循环单元进行攻击类别检测,并利用注意力机制进行优化改进,最终取得了较好的网络安全态势评估效果,不足之处是在态势要素分析中未考虑数据的时序性,不利于细化网络安全态势量化指标. 张等人[9]利用威胁情报和随机博弈的思想建立网络态势评估模型,记录已经发生的安全事件,并对外源威胁进行对比,实现对网络的评估,但该方法对于内部安全事件库的建立还不够完善. XI 等人[10]针对海量网络数据的利用率问题,从威胁、脆弱性和稳定性三个维度出发,对安全态势要素进行量化,最后在决策层合并结果以衡量整个网络的安全状况,该方法能够有效评估网络的安全状况. 吴等人[11]将高斯核函数和支持向量机相结合,利用网格搜索的方式确定模型最优参数,得到的安全态势评估模型能够有效评估网络当前状况,但在检测指标和特征提取方面还需进行完善. DONG 等人[12]面对网络中复杂多样的攻击类型和海量大数据,根据工控网络节点被攻击的前后信息,利用改进文本相似度方法计算文本相似度,最后通过量化文本相似度进行网络安全态势评估,能够有效的评估网络的安全状况,但在评估指标中未考虑工业控制网络节点的安全状况和节点上特定服务的性能指标.

为有效提高态势评估模型的特征提取能力和准确率,本文结合工业互联网的安全态势评估需求,提出一种基于改进随机森林的工业互联网的安全态势评估方法. 将梯度提升决策树(Gradient Boosting Decision Tree, GBDT)和递归特征消除相结合(Recursive Feature Elimination, RFE),改进随机森林(Random Forest, RF)作为一种多分类攻击检测模型,识别网络受到的攻击类别,最后根据安全态势量化指标确定其风险程度.

2 相关理论基础

2.1 梯度提升决策树

2.1.1 梯度提升决策树模型

梯度提升决策树[13]是一种以决策树为基学习器的集成算法,其数学模型可以表示为:

$$F(x)=\sum_{m=1}^{M}\alpha_m h_m(x) \tag{1}$$

其中,$F(x)$表示梯度提升决策树模型,x为输入样本,M表示分类回归树的数量,α_m表示对应回归树权重,$h_m(x)$表示分类回归树. 同时,梯度提升决策树也是一种前向分布算法,假设模型初始值为$F_0(x)=0$,则第m步的模型为:

$$F_m(x)=F_{m-1}(x)+\alpha_m h_m(x) \tag{2}$$

其中,$F_{m-1}(x)$表示当前模型,目的是求出下一棵决策树的权重α_m. 新加入一棵树时,根据最小化损失函数求得新加入的分类回归树$h_t(x)$:

$$h_t(x)=\arg\min_{h}\sum_{i=1}^{N}L(y_i,F_{m-1}(x_i)+h(x_i)) \tag{3}$$

其中,N为样本数,L为均方差损失函数,y_i为模型输出. 利用最速下降的近似求解方法得到最优模型:

$$F_m(x)=F_{m-1}(x)-\alpha_m\sum_{i=1}^{N}\frac{\partial L(y_i,F_{m-1}(x_i))}{\partial F_{m-1}(x_i)} \tag{4}$$

针对正则化问题,通过设置步长来控制,防止过拟合:

$$F_m(x)=F_{m-1}(x)+\beta\alpha_m h_m(x) \tag{5}$$

其中,β表示步长. 步长越小,则需要的分类回归树越多,同时,误差会降低,而训练时间会增加. 因此,调整合适的步长和分类回归树的数量,可以得到一个训练速度快并且训练精度较高的模型.

2.1.2 特征重要性评估

在梯度提升决策树模型中,通过基尼指数计算出每个特征的重要性,再累加计算结果得出特征重要性评分,此方法不仅可以缩短计算时间,加快模型训练速度,还可以提高模型的分类精度. 每棵决策树选中某一特征的次数越多,表示此特征的重要性越大,以得到所有特征的重要性排序.

假设原始数据集中每条样本中有k个特征$X_1,X_2,X_3,\cdots,X_k$,在第j棵树中,节点a的基尼指数为:

$$\mathrm{GI}_a = 1 - \sum_{k=1}^{K} p_{ak}^2 \tag{6}$$

其中,K表示类别数,p_{ak}为节点中X_k的比例. 在节点向下分枝时,特征X_i在节点a中的基尼指数变化量为:

$$\Delta\mathrm{GI} = \mathrm{GI}_a - \mathrm{GI}_l - \mathrm{GI}_r \tag{7}$$

其中,GI_l和GI_r分别为左右子节点的基尼指数. 特征X_i的重要性为:

$$\mathrm{VIM}_{ia}^{\mathrm{Gini}} = \chi_a \times \Delta\mathrm{GI} \tag{8}$$

其中,χ_a表示节点a的样本量占总样本量的比例. 假设特征X_i在第j棵树中出现的节点在集合A中,特征X_i在第j棵树的重要性为:

$$\mathrm{VIM}_{ij}^{\mathrm{Gini}} = \sum_{a \in A} \mathrm{VIM}_{ia}^{\mathrm{Gini}} \tag{9}$$

假设模型中有x棵树,则在所有树中特征X_i的重要性分数为:

$$\mathrm{VIM}_{i}^{\mathrm{Gini}} = \sum_{j=1}^{x} \mathrm{VIM}_{ij}^{\mathrm{Gini}} \tag{10}$$

经过所有决策树所得特征重要性分数之和越高,则说明该特征越重要,对预测结果的影响越大.

2.2　随机森林

随机森林是由多棵决策树共同参与学习和训练的集成分类器[14],其所有决策树都是基于有放回随机抽样的方法生成. 将生成的多棵决策树组合,利用投票法的思想,统计每棵树的预测结果,将得票数多的类别作为最终分类结果. 如图1所示.

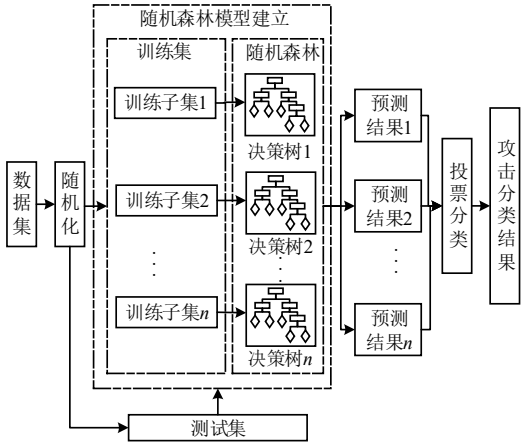

图1　随机森林工作流程

假设在数据集D中,样本数量为n,每个样本有Y个特征,随机森林模型具体构建过程如下:

步骤1　从随机化后的数据集D中有放回地随机选取n个样本并重复n次,生成n个训练子集,每个训练子集生成一棵决策树,共生成n棵决策树. 未被选取的数据构成测试集.

步骤2　在Y个特征中随机抽取y个,组成特征子集($y<Y$),根据节点不纯度最小原则选择最佳分割点进行分裂,将其划分为子节点,同时将训练子集划分到相应节点中,重复地逐层划分,最终得到决策树的全部节点.

步骤3　重复执行步骤2,直到生成n棵决策树,将n棵决策树组合,构成随机森林.

步骤4　将测试集输入随机森林模型进行分类预测,得到n个预测结果. 最后利用投票法原理,根据每棵决策树的预测结果,将票数最多的类别作为最终分类预测结果.

由于工业互联网数据具有海量和高维的特点,使用传统随机森林算法处理工业互联网数据时,主要存在以下问题:(1)在处理海量数据时,由于数据集不平衡,在分类时容易忽略某一部分类别,使分类结果偏向于多数类,导致算法的分类精度降低;(2)在处理高维数据时稍显冗余,容易忽略掉一部分类别的强相关特征,降低模型泛化能力且容易发生过拟合.

3　基于改进随机森林的工业互联网安全态势评估方法

3.1　方法架构

为解决工业互联网数据特征提取困难问题,提高安全态势评估结果的精度,本文提出一种基于改进随机森林的工业互联网安全态势评估方法,其整体方法如图2所示.

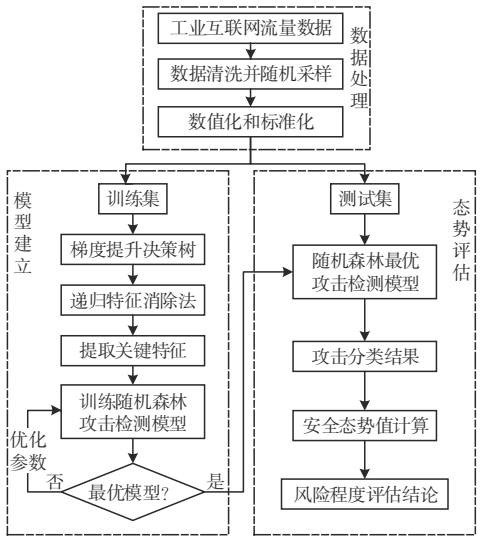

图2　安全态势评估方法

由图2可知,该方法由数据预处理、模型建立和态势评估三个模块组成.

(1)数据预处理:对获取到的工业互联网安全流量相关数据进行预处理,主要包括数据清洗并随机采样、数值化和归一化,并按8:2的比例将其划分训练集和测试集.

(2)模型建立:将数据处理后得到的训练数据输入梯度提升决策树进行训练,确定工业互联网中不同攻击特征的重要性权值;再利用递归特征消除方法提取其关键特征;最后,利用此时处理后的数据对随机森林攻击检测模型进行多分类训练并保存其最优参数.

(3)态势评估:利用已训练好的随机森林攻击检测模型对测试集进行攻击识别,根据识别结果,量化不同攻击对网络的影响严重程度,通过计算安全态势值对网络的安全状况进行有效评估.

针对模型建立中的特征选择部分,将递归特征消除法用于梯度提升决策树中,具体流程如图3所示.

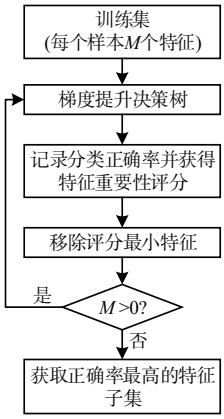

图3 特征选择流程

利用训练集对梯度提升决策树模型进行多轮数的训练,记录每轮训练的准确率的同时记录在该轮训练中所有特征重要性评分;接着移除特征重要评分最低的特征,并将经移除处理的特征集作为新特征集,进行下一轮训练,直到消除所有特征.具体算法步骤如下:

步骤1 将训练集中所有特征作为初始特征集,输入梯度提升决策树训练.

步骤2 记录每一轮训练的准确率并获得所有特征的重要性评分.

步骤3 移除评分最低的特征,形成新的特征子集.设训练集的初始维度为M,则更新后的特征集维度为$M-1$.

步骤4 更新$M=M-1$,如果M大于0,更新初始特征集并重复步骤2和步骤3.

步骤5 当$M=0$时,获取准确率最高的特征子集,将其作为最终特征子集.

3.2 安全态势量化评估

3.2.1 数据集

本文使用澳大利亚网络安全中心建立的UNSW-NB15数据集[15],包括训练数据和测试数据,该数据集大约有254万个样本,每个样本有47个特征和2个标签类属性,并且测试集中含有训练集中没有出现的攻击类型,能够有效模拟出当今复杂异构的工业互联网的真实网络情况,被广泛应用于安全态势评估领域,具有较高的代表性和典型性,同时,对安全态势评估方法研究具有非常重要的意义.其中,UNSW-NB15数据集包含10种网络数据类型,分别为1种正常样本和9种攻击样本,如表1所示(表中DoS代表Denial of Service,即拒绝服务).

表1 10种网络数据类型

攻击类型	描述
Normal	正常交易数据
Fuzzers	发送随机数据使程序或网络暂停运行
Analysis	端口扫描、垃圾邮件和html文件渗透
Backdoors	绕过系统防火墙,访问计算机
DoS	恶意企图使用户无法使用服务器
Exploits	利用操作系统软件中的安全漏洞
Generic	适用于分组密码,但不考虑其结构
Reconnaissance	模拟收集信息的攻击
Shellcode	通过漏洞有效载荷的一小段代码
Worms	复制自身传播到其他计算机

3.2.2 攻击影响值量化

合理的量化攻击影响值有助于网络管理者进一步掌握网络的安全状况,根据网络流量数据所具有的机密性C(Confidentiality)、完整性I(Integrity)和可用性A(Availability)三个指标,同时参考通用漏洞评分系统[16]进行攻击影响等级划分如表2所示.

表2 攻击影响值评定表

指标	影响程度	影响值
机密性(C)	无(N)/低(L)/高(H)	0/0.22/0.56
完整性(I)	无(N)/低(L)/高(H)	0/0.22/0.56
可用性(A)	无(N)/低(L)/高(H)	0/0.22/0.56

攻击影响值计算方法如下:

$$\mathrm{AI}_i=\frac{C_i+I_i+A_i}{3} \tag{11}$$

其中,AI_i表示第i类攻击的影响值,C_i、I_i和A_i分别表示第i类攻击的机密性、完整性和可用性.

3.2.3 攻击严重程度量化

攻击严重程度量化标准依据网络数据丢包率、数据流量变化率和网络数据吞吐量进行量化[17],严重程度因子如表3所示.

攻击严重程度计算方法为:

$$S_i=N_i\times 10^{\tau} \tag{12}$$

其中,S_i表示第i类攻击的严重程度,N_i表示一段时间内第i类攻击的次数,τ表示攻击严重程度因子.

3.2.4 安全态势量化

(1) 安全态势值计算

根据网络攻击严重程度量化和攻击影响值量化,

表3　攻击类型量化评定表

攻击类型	攻击严重程度因子
Analysis	0.275
Backdoors	0.473
DoS	0.560
Exploits	0.473
Fuzzers	1.000
Generic	0.300
Normal	0.250
Reconnaissance	0.500
Shellcode	0.770
Worms	0.450

综合考虑网络受到的攻击对网络造成的影响,安全态势值计算如下:

$$\mathrm{SV}=\frac{\sum_{i=1}^{n}\mathrm{AI}_i\times S_i}{N} \tag{13}$$

其中,SV为安全态势值,n为攻击类型数量,AI_i和S_i分别为第i类攻击的影响值和攻击严重程度,N为样本总数.

(2)　安全态势评估

网络安全态势等级的认定参考《公共互联网网络安全突发事件应急预案》[18],对应工业互联网安全突发事件的影响范围和危害程度,本文将安全态势评估等级划分为特别重大风险、重大风险、较大风险、一般风险和安全5个区间,具体划分如表4所示.

表4　网络安全态势评估等级对照表

态势等级	安全态势值区间
安全	[0.00, 0.40]
一般风险	(0.40, 0.80]
较大风险	(0.80, 1.20]
重大风险	(1.20, 1.60]
特别重大风险	(1.60, 2.00]

4　实验过程与结果分析

4.1　实验环境

实验配置环境:操作系统为Windows 10,处理器为Intel Core i7-10700,内存为16 GB DIMM 2 933 MHz,TensorFlow版本为2.7.0,Python版本为3.8.8.

4.2　数据预处理

实验采用的是UNSW-NB15数据集的子集版本,有大约25万个样本,每个样本包含43个特征,其中39个为连续型特征和4个离散型特征. 数据预处理主要包含数据清洗和采样、离散特征数值化和归一化.

(1)　数据清洗和采样

UNSW-NB15数据子集中存在大量的特征值相同但攻击类别不同的冗余样本,在模型训练中称其为噪声数据,过多的噪声数据对模型的训练会产生较大影响,为减少冗余样本对实验的影响,在模型训练之前,删除数据子集中的冗余样本. 由于数据样本量较大且部分攻击类别其样本数较少,由此导致模型的分类效果不佳. 为提高模型分类效率,本文在数据子集的基础上进行采样得到新的训练集和测试集,此时各类别样本的分布情况如表5所示.

表5　实验数据集样本分布及比例

攻击类型	训练集		测试集	
	数量	比例/%	数量	比例/%
Analysis	648	4.03	162	4.03
Backdoors	324	2.01	101	2.51
DoS	725	4.51	169	4.21
Exploits	2 138	13.31	556	13.84
Fuzzers	1 621	10.11	427	10.63
Generic	1 716	10.68	416	10.36
Normal	5 833	36.30	1 449	36.07
Reconnaissance	1 759	10.95	429	10.68
Shellcode	1 170	7.28	279	6.95
Worms	134	0.82	29	0.72
合计	16 068	100	4 017	100

(2)　特征数值化

由于数据集中存在非数值型特征,针对符号型数据的处理通常有One-Hot编码和顺序编码两种方式. 从特征维度考虑,本文所用数据集包含133个不同的协议类型、13个不同的服务类型和11个不同的连接状态,经测试:利用One-Hot编码将样本维度将是原样本维度的4.5倍,特征空间增大,而使用顺序编码的方式不增加特征维度;从运行时间考虑,梯度提升决策树和随机森林都以决策树为基学习器,特征维度的增加,会使决策树的深度增加,从而导致时间复杂度明显增加. 综合上述因素,选择顺序编码技术将协议类型、服务类型、连接状态和标签这4类符号型数据转换为数值型数据,数值化结果如表6所示.

表6　符号型特征转换对照

名称	类型	数据标识
Proto	udp, arp, tcp, …, rtp	0, 1, 2, …, 132
Services	-, http, ftp, …, ssh	0, 1, 2, …, 12
State	INT, FIN, REQ, …, no	0, 1, 2, …, 10
Label	Analysis, …, Worms	0, 1, 2, …, 9

(3)　数据归一化

由于特征之间存在显著的大小差异,为减小特征值差异对实验的影响,对所有特征值进行归一化处理:

$$\bar{x}=\frac{x-x_{\min}}{x_{\max}-x_{\min}} \tag{14}$$

式中，x 表示原特征值，$\bar{x}$ 为归一化后的特征值，x_{max} 和 x_{min} 为特征列的最大值和最小值.

4.3 特征选择

结合梯度提升决策树和递归特征消除算法进行关键特征选择，不同特征数量下模型的训练准确率变化如图4所示.

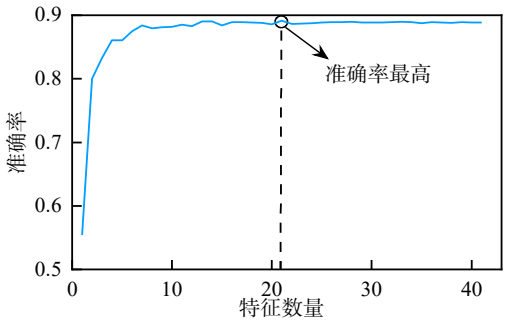

图4 训练准确率变化图

由图4可知，特征数量小于14个时，其准确率变化幅度过大. 图中虚线位置的特征数量为21个，此时模型训练准确率最高，将其作为关键特征子集，具体如表7所示.

表7 关键特征子集

序号	特征名称	序号	特征名称	序号	特征名称
1	dur	8	sload	15	ackdat
2	service	9	dload	16	smean
3	sbytes	10	sinpkt	17	dmean
4	dbytes	11	dinpkt	18	ct_srv_src
5	rate	12	sjit	19	ct_state_ttl
6	sttl	13	tcprtt	20	ct_dst_src_ltm
7	dttl	14	synack	21	is_sm_ips_ports

4.4 评估指标

工业互联网流量数据具有维度高、分布不平衡的特点，通常正常样本在数量上远多于异常样本，如果只用准确率来衡量模型的优劣，不能有效地说明模型的真实效果，仅能表示大样本类的分类精度. 同时，针对安全态势评估问题，遗漏任何一种攻击都可能发生严重的后果，因此，选择合适的评估指标至关重要. 为准确识别出网络所面临的各类攻击，提高网络安全态势评估精度，采用准确率(Accuracy)、精确率(Precision)、召回率(Recall)也称为检测率和 $F1$ 值($F1$-Score)作为评价指标，具体计算公式如下：

$$\text{Accuracy}=\frac{\text{TP}+\text{TN}}{\text{TP}+\text{FP}+\text{FN}+\text{TN}} \tag{15}$$

$$\text{Precision}=\frac{\text{TP}}{\text{TP}+\text{FP}} \tag{16}$$

$$\text{Recall}=\frac{\text{TP}}{\text{TP}+\text{FN}} \tag{17}$$

$$F1=\frac{2\times\text{Precision}\times\text{Recall}}{\text{Precision}+\text{Recall}} \tag{18}$$

其中，TP为将攻击样本预测为攻击样本的数量；FN为将攻击样本预测为正常样本的数量；FP为将正常样本预测为攻击样本的数量；TN为将正常样本预测为正常样本的数量.

在安全态势评估中，以上指标的值越大，表明攻击检测效果越好，态势评估越准确.

4.5 实验结果分析

4.5.1 攻击类型检测

为验证本文所提方法的有效性，分别将传统的随机森林算法、支持向量机算法(Support Vector Machine，SVM)、K最近邻算法(K-Nearest Neighbor，KNN)和本文方法(Gradient Boosting Decision Tree-Recursive Feature Elimination-Random Forest，GBDT-RFE-RF)作为多分类攻击检测模型，使用UNSW-NB15数据集提供的训练集和测试集进行训练和测试. 选择准确率、精确率、召回率和 $F1$ 值作为评价指标，结果如图5所示.

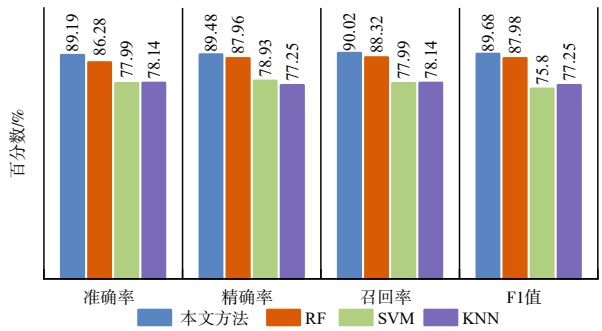

图5 不同算法检测结果对比

由图5分析可知：第一，本文利用GBDT-RFE改进的RF算法各评价指标均高于模型改进之前，主要原因是RF算法在处理高维数据时稍显冗余，容易忽略掉一部分类别的强相关特征，而本文方法利用数据清洗和随机采样对数据进行预处理，该操作去除了冗余样本，且利用GBDT-RFE算法进行特征提取降低了特征维度. 第二，本文所提方法的准确率、精确率、召回率和 $F1$ 分数值分别达到89.19%、89.48%、90.02%和89.68%，为对比模型中最优，相比于传统的RF、SVM和KNN模型，各项指标值分别至少提高2.91%、1.52%、1.7%和1.7%，平均分别提高8.38%、8.1%、8.53%和9.33%. 出现该结果的主要原因是SVM算法在多分类问题中计算复杂度高，性能的好坏过分依赖于核函数和惩罚系数的选择；而KNN算法中邻居的选择至关重要，邻居数过少容易导致过拟合，邻居数过多易发生欠

拟合.

已有网络安全态势评估研究大多从整体分类角度进行网络安全态势评估和量化,忽略了少量攻击类别对整体的影响. 为验证各模型对不同攻击类别的检测率,4种算法对攻击类别的检测情况如表8所示.

表8　4种模型对各类别样本的检测率对比

攻击类型	检测率/%			
	RF	SVM	KNN	本文方法
Analysis	**95.68**	87.04	83.95	90.74
Backdoor	62.38	3.96	10.89	**66.34**
DoS	**32.54**	7.10	18.34	31.36
Exploits	71.58	76.26	70.50	**80.94**
Fuzzers	94.38	84.07	82.90	**95.32**
Generic	87.50	82.45	84.38	**89.42**
Normal	99.93	**100.00**	**100.00**	**100.00**
Reconnaissance	87.88	75.52	68.07	**90.21**
Shellcode	86.02	27.24	43.73	**94.62**
Worms	51.72	3.45	3.45	**79.31**

由表8分析可知,本文方法对十种典型攻击类别都能取得较高的检测率. 虽然“Analysis”和“Shellcode”这两种攻击类型的样本数相较于其他类别的样本数很少,但本文模型对此两类样本的检测率仍达到了90%以上,说明本文模型对少量样本仍具有较强的学习能力;而四种模型对于“DoS”攻击的检测率都偏低,主要原因是DoS流量和正常流量非常相似,由此导致攻击者伪装成正常用户向网络发送数据,以至于系统难以检测出DoS流量.

4.5.2　网络安全态势评估方法对比分析

为验证本文方法较对比方法对网络安全态势评估的有效性,从测试集中随机抽取多组相同条数的测试数据. 首先分别利用RF、SVM、KNN和本文方法进行攻击检测;然后根据机密性、完整性和可用性量化各类攻击对网络的影响值AI_i;接着依据网络数据丢包率、数据流量变化率和网络数据吞吐量计算得到各类攻击的严重程度S_i;最后根据攻击的影响值和严重程度对网络态势进行量化评估,并计算网络安全态势值,图6直观地展示了各态势评估方法的评估值和真实值之间的拟合关系.

由图6分析可知:根据测试集中的实际流量数据,结合态势值计算方法,计算得到网络的实际态势值. 4种态势评估方法确定的网络安全态势值和真实的网络安全态势值在多组测试实验中重合度较高,变化趋势基本相同. 与网络真实态势情况相比,本文所提方法准确性和一致程度更高.

结合表4安全态势评估等级可知:通过本文方法得出的安全态势值与网络真实值始终保持一致变化,和

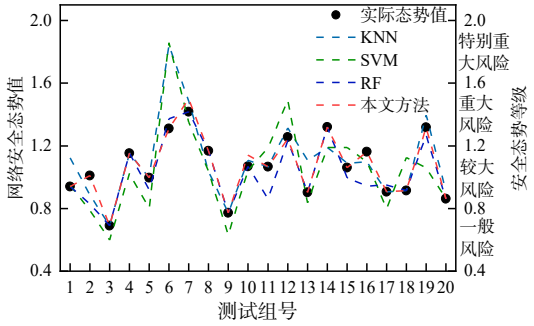

图6　安全态势值对比

其它3种方法相比,本文方法误差最小;在20组测试实验中,各方法对第3组、第10组和第20组真实态势值的拟合度均较高,但本文方法的优势更为明显;而在第6组和第12组实验中各方法得到的态势值与真实值相比误差较大,其中对于第6组测试实验,SVM和KNN模型得出的态势评估结果为特别重大风险,而本文方法得到的态势值与实际态势值更加接近,其态势评估结果和真实的态势情况都是重大风险.

图7所示为4种模型在测试集上的均方根误差计算结果. 其中SVM作为传统机器学习模型,其均方根误差值最大,KNN和RF模型误差值相比SVM较小,而本文模型的误差值小于另外三种模型.

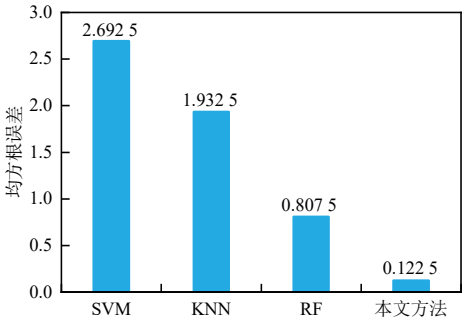

图7　均方根误差计算结果

为进一步说明本文方法的有效性,从测试集中任意选取一组数据进行实验,其网络流量类别分布如表9所示.

利用RF、SVM、KNN和本文方法对选取的这组流量数据进行攻击检测,其分类情况如图8所示.

表9　网络流量分布

标签编号	攻击类型	数量
1	Backdoors	1
4	Fuzzers	4
5	Generic	2
6	Normal	8
7	Reconnaissance	3
8	Shellcode	2

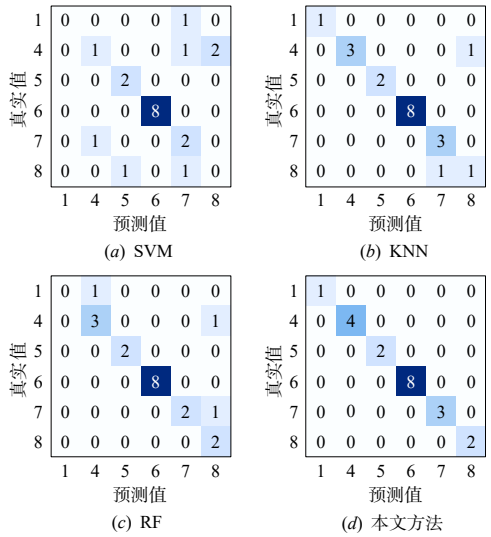

图 8 测试数据分类情况

由图 8 可知：SVM 模型相较于其他方法对 Backdoors、Shellcode、Reconnaissance 和 Fuzzers 这 4 类攻击的检测率均偏低，主要原因在于其参数选取困难；KNN 模型较 SVM 模型对 Backdoors 和 Shellcode 两类样本的检测效果有所提升，但仍不能较好地识别 Fuzzers 和 Reconnaissance 这两类攻击．RF 模型较上述两种模型对 Shellcode 类攻击的检测率更高，但对 Fuzzers 类的检测率仍待提高．对于 Fuzzers 和 Reconnaissance 类攻击不能有效检测．相比于 RF、SVM 和 KNN 模型，利用本文方法对选取的这组流量数据进行攻击检测均能正确识别出其攻击类型，由此表明本文模型在分类稳定性和整体准确率上更具优势．

根据以上 4 种方法的分类情况并结合态势值计算公式得到该组数据的态势结果如表 10 所示．由表可见，尽管这里四种方法得到的态势等级与实际一致，但本文方法得到的安全态势值与实际值最接近．

表 10 安全态势对比

	实际值	RF	SVM	KNN	本文方法
态势值	1.284 3	1.240 7	1.450 9	1.309 6	1.284 3
态势等级	重大风险	重大风险	重大风险	重大风险	重大风险

由上述分析可知，本文态势评估方法的稳定性更高，得到的态势评估结果能够更准确反映网络当前的安全状况．

5 结论

本文提出一种基于改进随机森林的工业互联网安全态势评估方法．首先使用梯度提升决策树对训练集的所有特征进行特征重要性排序，然后利用递归特征消除法提取不同网络威胁的关键信息；最后使用随机森林算法对网络攻击类型进行检测并计算其网络态势值，从而有效对网络安全态势进行评估．实验结果表明，相比于传统的网络安全态势评估算法，本文提出的工业互联网安全态势评估模型有较高的准确率、精确率、召回率和 $F1$ 分数值，能够更加准确地评估网络安全态势．后续将进一步完善工业互联网安全态势评估的量化指标，从而使模型评估的细粒度更高，能够从多角度评估网络的安全状况，提高其稳定性和可靠性．

参考文献

[1] 董悦, 王志勤, 田慧蓉, 等. 工业互联网安全技术发展研究[J]. 中国工程科学, 2021, 23(2): 65-73.
DONG Y, WANG Z Q, TIAN H R, et al. Development of industrial Internet security technology in China[J]. Strategic Study of CAE, 2021, 23(2): 65-73. (in Chinese)

[2] ALALI M, ALMOGREN A, HASSAN M M, et al. Improving risk assessment model of cyber security using fuzzy logic inference system[J]. Computers & Security, 2018, 74: 323-339.

[3] ZHAN M G, LI Y, YANG X H, et al. NSAPs: A novel scheme for network security state assessment and attack prediction[J]. Computers & Security, 2020, 99: 102031.

[4] WANG Q, BU S Q, HE Z Y, et al. Toward the prediction level of situation awareness for electric power systems using CNN-LSTM network[J]. IEEE Transactions on Industrial Informatics, 2021, 17(10): 6951-6961.

[5] 胡向东, 盛顺利. 融合 DBN 和 BiLSTM 的工业互联网入侵检测方法[J]. 重庆邮电大学学报(自然科学版), 2022, 34(01): 134-146.
HU X D, SHENG S L. Industrial internet intrusion detection method integrating DBN and BiLSTM[J]. Journal of Chongqing University of Posts and Telecommunications (Natural Science Edition), 2022, 34(1): 134-146. (in Chinese)

[6] HAMMAD M, HEWAHI N, ELMEDANY W. MMM-RF: A novel high accuracy multinomial mixture model for network intrusion detection systems[J]. Computers & Security, 2022, 120: 102777.

[7] HAN W, TIAN Z, HUANG Z, et al. System architecture and key technologies of network security situation awareness system YHSAS[J]. Computers, Materials and Continua, 2019, 59(1): 167-180.

[8] 杨宏宇, 张梓锌, 张良. 基于并行特征提取和改进 BiGRU 的网络安全态势评估[J]. 清华大学学报(自然科学版),

2022, 62(5): 842-848.
YANG H Y, ZHANG Z X, ZHANG L. Network security situation assessments with parallel feature extraction and an improved BiGRU[J]. Journal of Tsinghua University (Science and Technology), 2022, 62(5): 842-848. (in Chinese)

[9] 张红斌, 尹彦, 赵冬梅, 等. 基于威胁情报的网络安全态势感知模型[J]. 通信学报, 2021, 42(6): 182-194.
ZHANG H B, YIN Y, ZHAO D M, et al. Network security situational awareness model based on threat intelligence [J]. Journal on Communications, 2021, 42(6): 182-194. (in Chinese)

[10] XI R R, YUN X C, HAO Z Y. Framework for risk assessment in cyber situational awareness[J]. IET Information Security, 2019, 13(2): 149-156.

[11] 吴海涛, 代尚林, 乔中伟, 等. 基于RBF-SVM智能配变终端的网络安全态势评估[J]. 电力科学与技术学报, 2021, 36(5): 35-40.
WU H T, DAI S L, QIAO Z W, et al. Research on network security situation awareness of intelligent distribution transformer terminal unit based on RBF-SVM[J]. Journal of Electric Power Science and Technology, 2021, 36(5): 35-40. (in Chinese)

[12] DONG R H, SHU C, ZHANG Q Y. Security situation assessment algorithm for industrial control network nodes based on improved text SimHash[J]. International Journal of Network Security, 2021, 23(6): 973-984.

[13] FRIEDMAN J H. Greedy function approximation: A gradient boosting machine[J]. the annals of statistics, 2001, 29(5): 1189-1232.

[14] FARNAAZ N, JABBAR M A. Random forest modeling for network intrusion detection system[J]. Procedia Computer Science, 2016, 89: 213-217.

[15] MOUSTAFA N, SLAY J. The evaluation of network anomaly detection systems: Statistical analysis of the unsw-NB15 data set and the comparison with the KDD99 data set[J]. Information Security Journal: A Global Perspective, 2016, 25(1-3): 18-31.

[16] FIRST. Org, Inc. Common vulnerability scoring system v3.1: Specification document[EB/OL]. (2019-06-10) [2022-08-05]. https://www.first. org.

[17] ZHANG H F, KANG C Y, XIAO Y. Research on network security situation awareness based on the LSTM-DT model[J]. Sensors, 2021, 21(14): 4788.

[18] 工业和信息化部.工业和信息化部印发《公共互联网网络安全突发事件应急预案》[J]. 中国应急管理, 2017 (11): 22-25.
Ministry of Industry and Information Technology. The ministry of industry and information technology issued the public internet network security emergency response plan[J]. China Emergency Management, 2017(11): 22-25. (in Chinese)

作者简介

胡向东　男, 1971年生, 四川武胜人. 博士, 重庆邮电大学教授, 博士生导师. 荣获“重庆英才, 名家名师”称号, 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

万润楠　男, 1997年生, 重庆万州人, 硕士研究生, 主要研究方向为工业互联网安全.
E-mail: 364172781@qq.com