基于自适应VAE的电力物联网异常流量检测

Adaptive VAE Based Anomalous Network Traffic Detection for Power IoT

张 琦,龚笔华,钟 凯,李向明,王 虎,阳跃永,彭娅莉(国能九江发电有限公司,江西 九江 332000)
Zhang Qi, Gong Bihua, Zhong Kai, Li Xiangming, Wang Hu, Yang Yueyong, Peng Yali (Guoneng Jiujiang Power Generation Co., Ltd., Jiujiang 332000, China)

摘 要:
针对电力物联网中传统静态阈值流量异常检测方法误报率和漏报率高的问题,提出一种基于改进自适应变分自动编码器(VAE)的检测方法。该方法利用电力智能融合终端采集的流量构建流特征矩阵,设计了模型迭代与攻击检测双模块架构。网络流量经攻击检测模块的初步筛选后,进入模型迭代模块进行无监督学习。模型迭代模块采用自适应阈值机制动态更新模型。在2个数据集上的实验表明,该方法有效降低了误报率和漏报率,相比传统方法有5%~8%的性能提升。

关键词:
变分自编码器;异常检测;无监督学习;电力物联网
doi:10.12045/j.issn.1007-3043.2026.02.015
文章编号:1007-3043(2026)02-0078-07
中图分类号:TN915
文献标识码:A
开放科学(资源服务)标识码(OSID):

Abstract:
To address the high false positive and false negative rates of traditional static-threshold methods for network traffic anomaly detection in the Power Internet of Things (PIoT), it proposes a detection method based on improved adaptive variational auto-encoder (VAE). The method constructs a flow feature matrix from traffic data collected by smart power fusion terminals. It employs a dual-module architecture comprising a model iteration module and an attack detection module. After the initial screening in the detection module, the flow features enters the iteration module for unsupervised feature learning. The model iteration module dynamically updates the model using an adaptive threshold mechanism. Evaluations on two datasets demonstrate that the proposed method can effectively reduce both false positive and false negative rates by 5%~8% compared to traditional approaches.

Keywords:
Variational auto-encoder (VAE); Anomaly detection; Unsupervised learning; Power IoT

引用格式:张琦,龚笔华,钟凯,等. 基于自适应VAE的电力物联网异常流量检测[J]. 邮电设计技术,2026(2):78-84.

0 引言

近年来,随着信息技术的迅猛发展,电力领域逐渐引入了物联网技术。电力系统作为国家基础设施,承载着重要的能源流量,因而成为网络攻击的重点目标。电力物联网的发展,使得系统中的数据流量更加复杂[1]。攻击者可以通过分析和干扰电力流量,实施针对性的攻击,影响电力供应的稳定性。在这种情况下,电力物联网的异常流量检测尤为关键。

在传统电力物联网的异常流量检测中,大多数方法依赖监督学习来利用标注数据进行训练,可实现较高的检测精度[2]。然而,由于电力物联网的网络流量数据庞大且复杂,专业电力知识的标注成本也很高[3],网络流量数据的结构化和时序性特征也增加了流量识别的难度[4],这使得数据质量要求也变得尤为严

基金项目:国能九江公司(GNJ-24-KJ-01)
收稿日期:2025-12-29

格[5]。此外，由于电力网络环境中缺少充分的有标记数据，有监督学习模型存在泛化性差和过拟合严重的问题，并且该模型对异常值较为敏感[6]。基于以上原因，无监督学习在电力物联网领域的流量识别方面得到了广泛应用，其中作为无监督学习代表的自动编码器（AE）模型更是被广泛应用于异常检测。而变分自编码器（Variational Autoencoder，VAE）相较于AE具有更多优势。VAE能够更好地捕捉数据的潜在分布，生成更具多样性和连续性的样本，在处理复杂数据和不确定性方面表现更为出色，从而能在电力物联网异常流量检测中提供更准确、更可靠的结果。

与此同时，在异常检测过程中，阈值的计算已成为一个重要问题[7]。然而，传统的阈值方法往往依赖静态的、预设的阈值来判断是否存在异常，在流量异常检测中存在局限性[8]。这种方法难以适应电力系统中的动态变化和复杂的操作环境，在实际应用中可能产生较高的误报率或漏报率[9]。此外，静态阈值无法有效处理数据的多样性和时变特性，限制了其在处理大规模和实时数据中的有效性和准确性。针对上述问题，本文提出了一种基于改进的自适应变分自编码器电力物联网异常流量检测方法。本文的主要贡献如下。

a）本文提出一种基于智能融合终端的特征提取方法，通过对原始网络包的截取、分类计算特征等操作，实现了电力通信网络流量特征提取，为模型迭代提供有效数据输入。

b）本文提出了一种基于VAE的无监督深度学习异常检测方法。VAE模型利用高斯分布表示潜在变量，并使用重新参数化方法，实现了无监督学习下的有效异常检测。

c）本文使用一种自适应动态阈值计算方法计算异常检测所需阈值。该方法实时计算阈值以适应数据的变化，有效解决了固定阈值方法在处理动态环境中的不适应性问题。

1 相关工作

在电力物联网领域，随着网络环境的日益复杂，流量异常检测技术不断发展。统计方法如自适应滤波理论也被引入到流量异常检测中，通过观察网络流量的变化来提前发现异常环境[10]。这种方法简单易行，但需要精确的参数设置和实时的数据更新。然而，随着复杂网络环境的发展，基于统计的方法逐渐面临挑战，特别是在处理高维度和噪声数据时效果不佳。因此，传统机器学习方法应运而生。传统机器学习方法通常将时序问题转换为监督学习任务，并通过特征工程和机器学习模型进行异常检测。文献[11]提出了一种基于K近邻（KNN）方法的新型进化神经模糊推理系统kENFIS，使用最小均方法来减少误差，并使用KNN来选择最佳匹配类，使用模糊逻辑来选择流类标签。文献[12]提出一种支持向量机（OCSVM）模型用于异常检测，但是这种模型并不适合在海量数据集上进行训练。由此可见传统的机器学习方法在处理高维和多变量数据时存在一定的局限性。

近年来，深度学习技术在电力物联网流量异常检测中得到了广泛应用。文献[13]提出并验证了一种基于1D卷积神经网络（CNN）的物联网异常检测模型，显示出在物联网流量检测任务中的有效性。文献[14]提出了一种基于深度特征学习的方法，结合堆叠降噪自编码器（SDA）和softmax，提高了流量特征提取的准确性和鲁棒性。文献[15]通过聚类算法探索样本相关性，提出自信息量挖掘模块和三元组信息量学习策略，进而实现异常检测。

在异常检测阈值计算方面，传统的流量异常检测方法大多采用固定阈值来进行判断，文献[16]提出一种基于Chebyshev阈值和时间序列的快速异常检测算法，通过预设恒定或自适应阈值来判定异常流量。这种方法简单易行，但是无法精确刻画网络异常行为，从而影响检测精度。为了解决这一问题，研究者提出了自适应阈值方法。自适应阈值通过刷新机制叠加前一时刻的行为数据，得出动态的阈值，并将其作为当前时刻检测点是否异常的准则[17]。文献[18]提出一种基于KL距离的自适应阈值方法，该方法也通过滑动窗口控制KL值数量，建立指数加权移动平均模型以获取下一时刻的预测值，并确定自适应阈值范围。

2 基于变分自编码器的电力物联网异常检测

2.1 总体架构

电力物联网的稳定运行与持续发展高度依赖边缘层、接入层和平台层的有机结合。本文提出的基于变分自编码器的电力物联网异常检测方法，通过架构各层协同处理流量数据，完善电力物联网安全防御体系，其总体框架如图1所示。边缘层包含在最前端感知和采集数据的光伏组件、逆变器等电力设备，还包

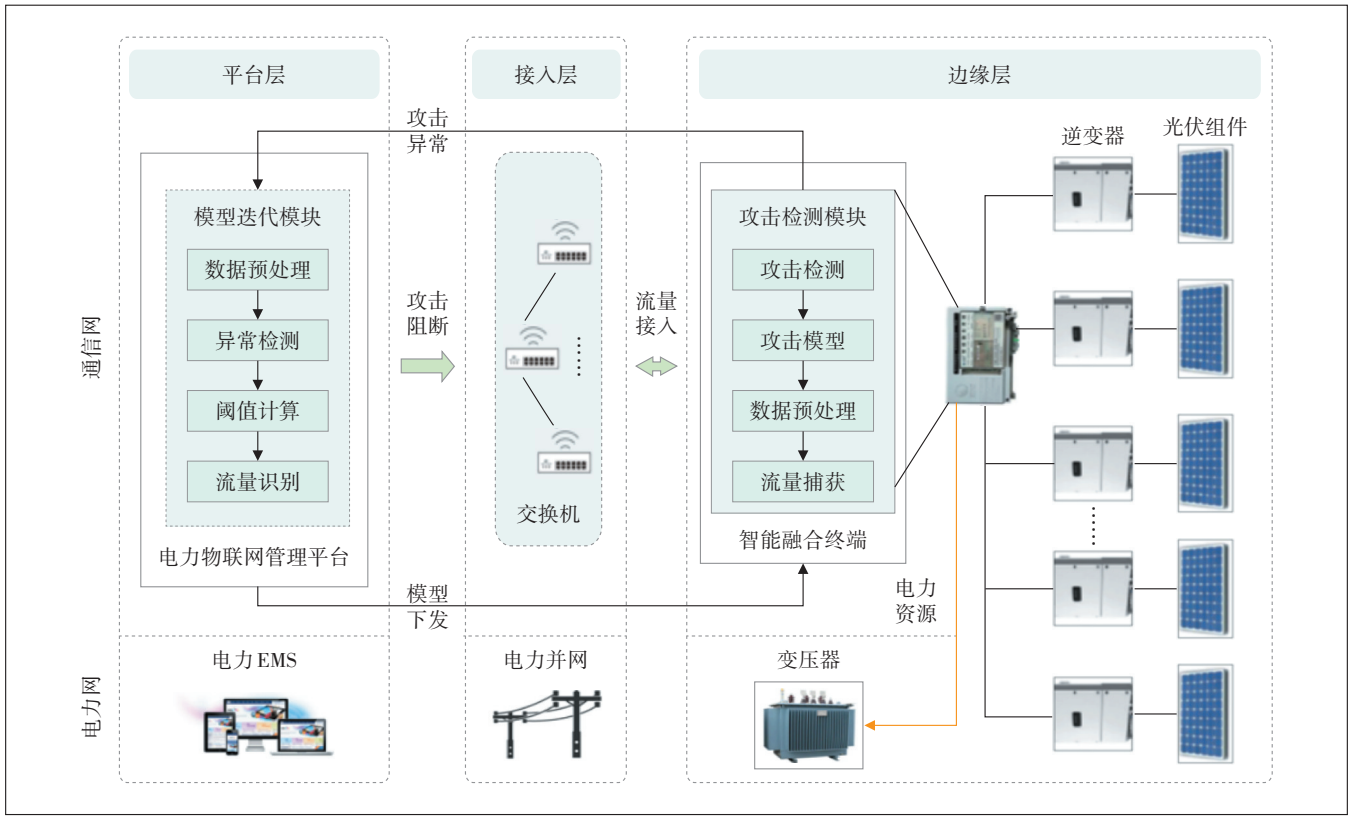

图1 总体框架

含数据采集、状态监测和故障检测的融合终端,并由融合终端进行数据的初步处理和攻击检测;接入层利用交换机实现数据的接入和上层平台的交互;平台层部署的模型迭代模块则接收来自攻击检测模块的数据,利用第2.3.1节提到的阈值计算结果和第2.3.2节提到的异常检测方法对模型进行训练和优化,不断提升对网络安全威胁的适应能力。训练完成后,将更新后的模型下发至攻击检测模块,以提升整个系统的检测和防御能力。同时,生成异常流量识别策略和防御建议,传递给交换机进行异常流量阻断和处理,并将新知识和更新后的策略反馈给攻击检测模块,形成正向反馈循环,以提高检测准确性和效率,共同保障电力物联网的安全。

2.2 模型迭代阶段

2.2.1 基于智能融合终端的特征提取方法

本文基于智能融合终端采集电力通信网原始网络包,设计网络包级流量特征,并根据采样间隔进行操作。在采样的时间间隔内,根据时间戳对原始网络包进行截取,从而形成待提取处理的网络包。根据网络包中的源目IP地址将网络包划分为上行包和下行包,其中上行包是发往智能融合终端的网络包(目的IP为智能融合终端的IP),下行包是由智能融合终端发出的网络包(源IP为智能融合终端的IP)。然后,分别计算上行包和下行包的网络包级特征,最终得到26个网络包级特征。网络流量特征设计如表1所示。

表1 网络流量特征设计

网络流量特征
包到达时间(平均值、最小值、最大值、标准差)
包数量总和
每秒包数
包长度(总计、平均值、最小值、最大值、标准差)
包头部占总长度的比例
包速率

将上述特征按顺序排列形成包特征集合Packet Features(PF):

$$PF = \{pf_1,\ pf_2,\ pf_3,\ \cdots,\ pf_{26}\} \quad (1)$$

其中,pf_i是上述网络流量特征的数值。

对得到的包集合特征进行整合,最终形成一个综合性的特征矩阵,即Fusion Features Matrix(FFM)。这

个特征矩阵将作为模型训练数据的输入，如式(2)所示。

$$FFM=\begin{pmatrix}FF_1\\FF_2\\FF_3\\\cdots\\FF_n\end{pmatrix}=\begin{pmatrix}ff_{1,1},&ff_{1,2},&\cdots,&ff_{1,26}\\ff_{2,1},&ff_{2,2},&\cdots,&ff_{2,26}\\ff_{3,1},&ff_{3,2},&\cdots,&ff_{3,26}\\&&\cdots&\\ff_{n,1},&ff_{n,2},&\cdots,&ff_{n,26}\end{pmatrix}\tag{2}$$

2.2.2　变分自编码器模型

VAE是一种强大的生成模型，它主要由编码器和解码器2个部分组成(见图2)。解码器的目标是通过学习隐藏层特征来获得一个分布，并使该分布尽可能接近真实数据的分布。而编码器则负责从潜在空间中重构出与原始输入尽可能相似的数据。为了获得这样的分布，VAE引入了隐藏层变量Z。具体来说，给定一个真实样本x_k，假设存在一个对x_k特有的分布$q(z|x_k)$，并进一步假设该分布是一个独立的、多变量的正态分布，从这个分布中采样得到的z应该能够还原回x_k。根据隐藏向量z，可以获得一个近似推断过程$P_\theta(z)P_\theta(x'|z)$。

VAE采用KL散度作为量化2个分布之间差异的度量，因此损失函数可定义为式(3)。

$$\text{Loss}=L(X,\ X')+\sum_j \text{KL}\left(q_j(Z|X)\,\|\,p(Z)\right)\tag{3}$$

损失函数由2个分量组成，第1个分量是重建损失，用来衡量模型在重建输入数据时的误差，确保生成的数据尽可能接近原始数据；第2个分量是适当分布和所选择的分布之间的KL散度，使模型的潜在分布尽可能接近先验分布。VAE的目标是最小化损失函数的总和，如式(4)所示。

$$L(x)=E_{zq(z|x)}\log\frac{p(z,x)}{q(z|x)}=\log p(x)-\text{KL}\left(q(z|x)\,\|\,p(z|x)\right)\tag{4}$$

损失函数$L(x)$被称为变分下界。通过优化损失函数$L(x)$使其尽可能接近$\log p(x)$，可以最小化KL散度。这一过程不仅要求生成的数据与输入数据之间的重建损失最小化，还需使隐空间的分布接近预设的先验分布，从而使分布$q_\phi(z|x)$能够更准确地估计真实的后验分布$p_\varphi(z|x)$。

VAE进一步将z的采样分解为2个部分：一部分是由编码器网络输出的，描述了隐变量的分布特征的标准偏差σ和均值μ等固定值，另一部分是随机高斯噪声ε。在应用重新参数化技巧后，$L(x)$可重写为式(5)。

$$L(x)=\frac{1}{2}\sum_{i=1}^{J}\left(1+\log\left(\sigma_j^2\right)-\mu_j^2\right)+\frac{1}{L}\sum_{i=1}^{L}\log p\left(x|z_i\right)\tag{5}$$

$L(x)$的变分下界优化既确保了编码器生成的Z值符合先验高斯分布，又增加了解码器最大化重建原始X的可能性。具体而言，VAE将每个给定输入的潜在特征表示为一个概率分布。在解码过程中，模型从每个潜在状态分布中进行随机采样，生成一个向量作为解码器的输入。

2.3　攻击检测阶段

2.3.1　自适应动态阈值计算方法

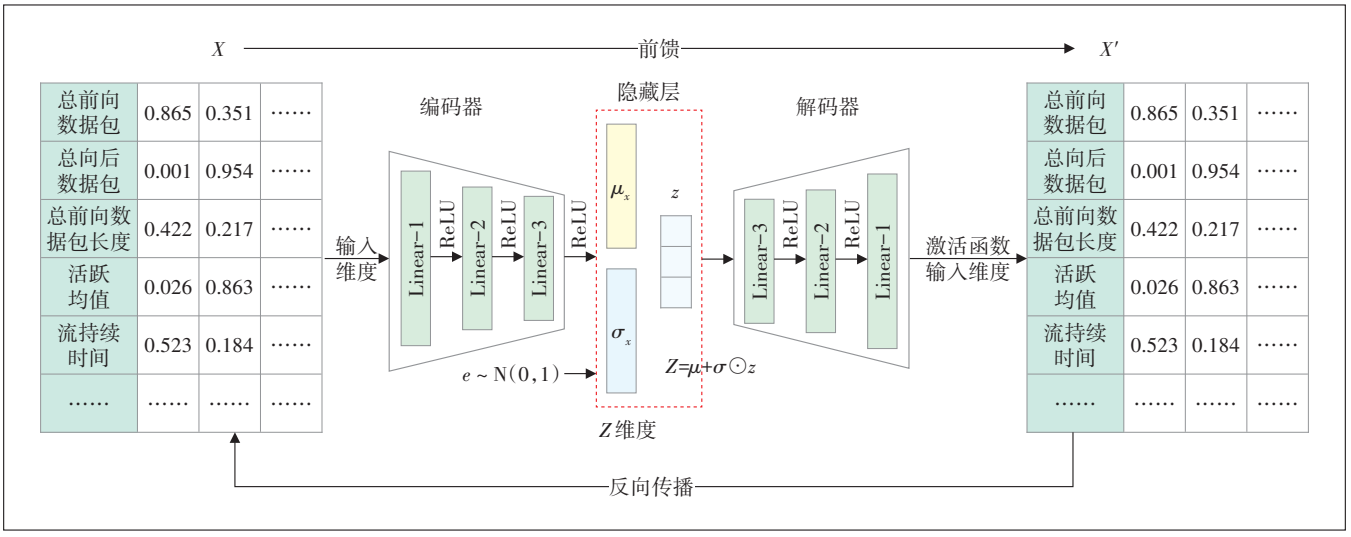

图2　VAE结构

传统的阈值通常依赖静态设定或经验性调整,可能无法适应数据分布的变化和模型的性能波动,导致异常检测的准确性和鲁棒性受到限制。异常检测模型通过获取正常流量分布来重建正常流量数据。该实验将流量值输入到模型的测试集中,然后计算重建数据与原始数据之间的距离。通常,异常流量的重建距离远大于正常流量的重建距离。因此,如何选择一个合适的阈值以区分正常流量和异常流量成为识别流量的关键。在使用均方误差(MSE)计算2个分布之间的距离时,通常选择损失收敛后的值作为模型的阈值。然而,如果模型的收敛性不好,可能会导致阈值设定无效或不准确。此外,收敛后的均方误差值往往较为杂乱,不利于精确寻找阈值。因此,本文提出了一种自适应动态阈值计算方法,通过动态调整阈值来适应数据分布的变化,能够更有效地应对这些挑战,提高异常检测的准确性和鲁棒性。具体计算流程包括以下4个步骤。

a)设定数据集的流量分布。将数据集设置为不同比例的正常流量和恶意流量,评估模型在该流量比例下的表现。

b)计算重建误差。使用模型对数据进行重建,并计算i个样本的重建误差。重建误差的公式为:

$$e_i = (x_i - \hat{x}_i)^2 \tag{6}$$

其中,x_i是真实值,$\hat{x}_i$是重建值。e_i衡量了模型在重建数据时的误差大小。

c)计算误差的方差。计算样本数据与式(4)得到的VAE损失函数之间的平均误差,评估VAE在处理数据时的性能表现,其计算公式为:

$$\sigma = \frac{1}{n}\sum_{i=1}^{n}\left[e_i - L(x)\right]^2 \tag{7}$$

d)计算阈值。根据损失函数$L(x)$和方差(σ),使用阈值计算公式来确定一个合适的阈值:

$$\theta_\alpha = L(x)_\alpha + Z_\alpha \times \sigma_\alpha \tag{8}$$

其中,Z_α是标准正态分布上对应α%的临界值。阈值θ_α用于区分正常数据和异常数据。

2.3.2 异常检测

在检测阶段,首先依据训练所得的结果,运用第2.3.1节提到的自适应动态阈值计算方法计算阈值。将经过预处理后的数据输入到已经训练好的模型中,从而获得相应的预测值。随后,计算预测值与输入值之间的损失。在此之后,对该损失与阈值ω进行比较判断。当测试样本的异常得分高于设定的阈值ω时,即可明确判断该样本为恶意流量;而当测试样本的异常得分低于设定的阈值ω时,则可以判断该样本为正常流量。

3 实验设置

3.1 实验环境设置

实验硬件环境为Windows 10操作系统,AMD Ryzen 7 3750H处理器,AMD Radeon(TM) RX Vega 10 Graphics,NVIDIA GeForce GTX 1650等,软件环境为Anaconda3以及python3.11。

3.2 数据集

本文数据集利用SCT230A智能融合终端来采集电力通信网边缘层12 h的流量数据,该数据将作为后续分析用的正常流量样本。同时,为了使检测模型学习恶意流量特征以提高攻击检测的准确性与可靠性,全面评估模型在电力通信网络环境下的性能,恶意流量数据选用了Bot-IoT数据集。通过提供详尽的标注数据,Bot-IoT为研究人员提供了一个可靠的基础,以便深入分析IoT设备的安全性,并优化入侵检测机制。

表2 Bot-IoT数据集攻击类型

流量类型	百分比/%
DoS	44.43
DDoS	47.68
Reconnaissance	7.82
Theft	0.07

Bot-IoT数据集攻击类型如表2所示。

3.3 性能评价指标

本文的性能评价指标包括精确度(Precision)、准确度(Accuracy)、召回率(Recall)、F1分数(F1-score)和AUC。精确度(Precision)用于衡量模型在所有被标记为异常的数据中,实际为异常的数据所占的比例。准确度(Accuracy)反映了模型在所有样本中正确分类的比例。召回率(Recall)强调模型对异常数据的检测能力。F1分数(F1-score)是精确度和召回率的调和平均值,用于综合考虑模型的精确性和全面性。AUC代表ROC曲线下的面积,用于衡量模型的总体分类性能,尤其是在不同分类阈值下的表现,能够提供模型在各种判别条件下的稳定性和有效性。

3.4 实验结果与分析

本文对LOF、PCA和本文提出的基于变分自编码器的电力流量识别优化算法这3种无监督学习算法进

行了网络入侵检测算法的比较实验。为了评估这些算法在异常检测任务中的性能，本文对每种算法进行了系统的实验分析。

本文利用变分自编码器（VAE）模型对异常流量进行了检测。实验涵盖了3种数据集模式，分别为：99%正常流量与1%恶意流量、95%正常流量与5%恶意流量以及90%正常流量与10%恶意流量。在每种模式下，本文比较了基于损失函数的阈值计算方法和自适应动态阈值计算方法这2种阈值计算方法的效果，具体数据如表3所示。在3种数据集模式下，自适应动态阈值计算方法均优于基于损失函数的阈值计算方法，在准确率、召回率和F1-score等指标上均表现出更高的性能，这验证了该方法在异常流量检测中的有效性和优越性。

表3　不同阈值计算方法数值对比

VAE模型		Precision	Accuracy	Recall	F1-score
99%正常流量、1%恶意流量	基于损失函数的阈值计算方法	0.990 2	0.707 8	0.707 8	0.819 9
	自适应动态的阈值计算方法	0.970 2	0.876 6	0.765 8	0.855 9
95%正常流量、5%恶意流量	基于损失函数的阈值计算方法	0.951 5	0.703 1	0.719 3	0.788 7
	自适应动态的阈值计算方法	0.944 2	0.846 8	0.789 5	0.859 9
90%正常流量、10%恶意流量	基于损失函数的阈值计算方法	0.903 2	0.750 0	0.733 6	0.750 1
	自适应动态的阈值计算方法	0.921 8	0.862 6	0.779 3	0.844 6

VAE模型异常检测性能的ROC分析如图3所示。根据图3可知，本文提出的基于变分自编码器的电力流量识别优化算法模型在Bot-IoT数据集上表现出色。AUC值较高表明VAE模型在区分正常流量和恶意流量方面具有优异的能力，能够有效地检测出异常流量。

在99%正常流量、1%恶意流量的模式下，3种无监督学习实验结果如表4所示。受正常流量数量远多于恶意流量的影响，尽管VAE的总体准确率较低，但其在恶意流量的召回率和AUC值上均优于其他模型。VAE对恶意流量的召回率高达0.956 0，展示了其强大

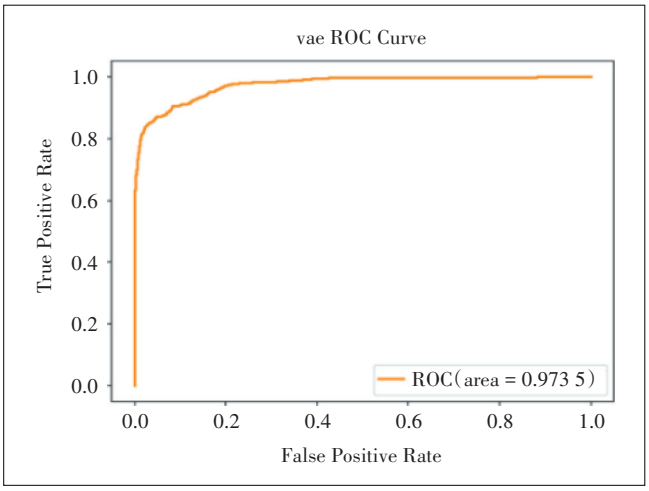

图3　VAE模型异常检测性能的ROC分析

表4　99%正常流量、1%恶意流量下3种无监督学习实验结果

模型		Precision	Accuracy	Recall	F1-score	AUC
LOF	正常	0.998 6	0.881 6	0.881 7	0.936 5	0.915 8
	恶意	0.068 6		0.872 0	0.127 2	
PCA	正常	0.999 1	0.901 5	0.901 3	0.947 7	0.958 7
	恶意	0.085 2		0.920 0	0.156 0	
VAE	正常	0.999 5	0.821 6	0.820 3	0.901 1	0.973 5
	恶意	0.050 5		0.956 0	0.096 0	

的异常检测能力；其AUC值为0.973 5，表明模型在区分正常流量与恶意流量方面表现卓越。

由于本实验旨在模拟实际网络环境，因此测试中正常流量与恶意流量的比例设置为99∶1。恶意流量的检测准确性受到正常流量被误判为恶意流量和恶意流量被误判为正常流量的影响。然而，这一低准确率并不意味着模型存在缺陷。相反，由图4可知，模型

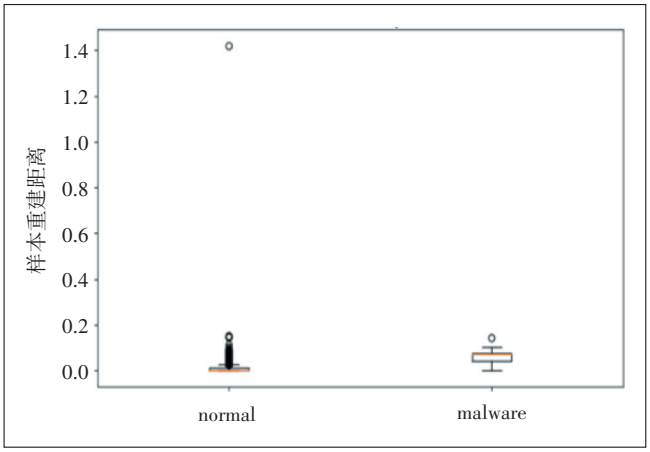

图4　恶意流量与正常流量区分

依然能够有效地区分恶意流量与正常流量。恶意流量样本的重建距离如图5所示,其中第41 000个测试集样本的重建距离显著增大。这一现象表明,该样本可能代表恶意流量的精确位置。这种明显的重建距离差异有助于模型准确识别和定位恶意流量样本,提

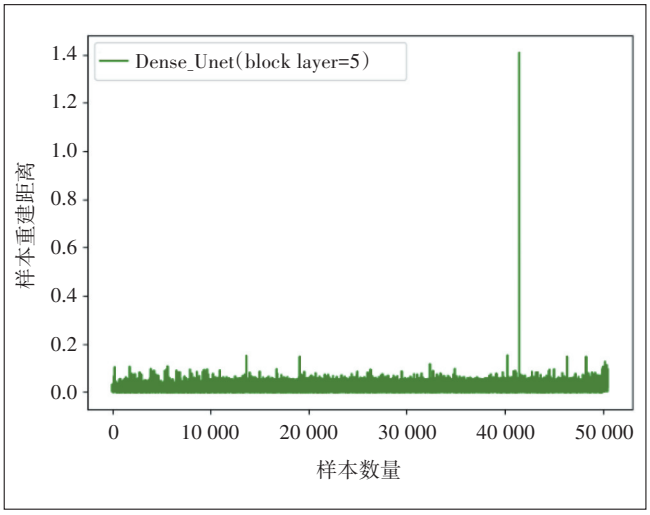

图5 恶意流量样本的重建距离

高了异常检测的精确性和可靠性。

4 结束语

为了提升电力物联网中的异常流量检测能力,本文提出了一种基于改进自适应VAE的检测方法。首先,通过智能终端采集网络包,并计算上下行包的特征矩阵,为模型提供训练数据。模型设计了两大模块:第一是攻击检测模块,负责初步筛查异常流量;第二是模型迭代模块,负责对检测到的未知异常流量进行进一步分析,并通过无监督学习捕捉数据特征。为了进一步提升检测精度,本文采用了一种自适应动态阈值计算方法,该方法能够根据数据分布的变化实时计算并调整检测阈值,有效打破了固定阈值方法在动态网络环境中适应性差的局限。实验结果表明,在真实和Bot-IoT数据集上,该方法优于传统检测方法,显著提高了电力物联网的安全性和稳定性。

参考文献:

[1] 童博,施俊,赵纯熙. 复杂网络环境下加密流量识别方法研究[J]. 邮电设计技术,2022(8):70-74.
[2] 樊琳娜,李城龙,吴毅超,等. 物联网设备识别及异常检测研究综述[J]. 软件学报,2024,35(1):288-308.
[3] 苏盛,汪干,刘亮,等. 电力物联网终端安全防护研究综述[J]. 高电压技术,2022,48(2):513-525.
[4] HE K,KIM D D,ASGHAR M R. Adversarial machine learning for network intrusion detection systems: a comprehensive survey [J]. IEEE Communications Surveys & Tutorials,2023,25(1):538-566.
[5] GUO B,ZHANG D Q,YU Z W,et al. From the Internet of things to embedded intelligence[J]. World Wide Web,2013,16(4):399-420.
[6] 柴浩轩,金曦,许驰,等. 面向工业物联网的5G机器学习研究综述[J]. 信息与控制,2023,52(3):257-276.
[7] 李泽一,王攀. 基于代价敏感度的改进型K近邻异常流量检测算法[J]. 南京邮电大学学报(自然科学版),2022,42(2):85-92.
[8] 陆旦宏,范文尧,杨婷,等. 基于生成对抗Transformer的电力负荷数据异常检测[J]. 电力工程技术,2024,43(1):157-164.
[9] 黄林,常健,杨帆,等. 基于改进k-means的电力信息系统异常检测方法[J]. 深圳大学学报(理工版),2020,37(2):214-220.
[10] 崔伟兰,尹逊伟,程永强. 一种基于统计的网络流量异常检测方法[J]. 网络安全技术与应用,2008(1):31-32.
[11] SHUBAIR A,RAMADASS S,ALTYEB A A. kENFIS: kNN-based evolving neuro-fuzzy inference system for computer worms detection [J]. Journal of Intelligent & Fuzzy Systems: Applications in Engineering and Technology,2014,26(4):1893-1908.
[12] ZENG Z Q,YU H B,XU H R,et al. Fast training support vector machines using parallel sequential minimal optimization[C]//2008 3rd International Conference on Intelligent System and Knowledge Engineering. Xiamen:IEEE,2008:997-1001.
[13] ALTANGEREL G,TEJFEL M,TSOGBAATAR E. A 1D CNN-based model for IoT anomaly detection using INT data[C]//2022 IEEE 16th International Scientific Conference on Informatics (Informatics). Poprad:IEEE,2022:106-113.
[14] 董书琴,张斌. 基于深度特征学习的网络流量异常检测方法[J]. 电子与信息学报,2020,42(3):695-703.
[15] 刘洋,翟锐,巩坤. 异常检测在网络安全防护中的应用研究[J]. 邮电设计技术,2024(8):24-28.
[16] 胡平,叶坤,刘瑞琴. 一种基于Chebyshev的网络流量异常检测方法[J]. 计算机应用与软件,2016,33(5):127-131.
[17] 曹敏,程东年,张建辉,等. 基于自适应阈值的网络流量异常检测算法[J]. 计算机工程,2009,35(19):164-166,177.
[18] 蒋华,张红福,罗一迪,等. 基于KL距离的自适应阈值网络流量异常检测[J]. 计算机工程,2019,45(4):108-113,118.

作者简介:
张琦,毕业于武汉水利大学,高级工程师,学士,主要研究方向为电力系统及其自动化;龚笔华,毕业于南昌大学,高级工程师,学士,主要从事电力系统继电保护工作;钟凯,毕业于山东科技大学,工程师,硕士,主要从事电力系统继电保护工作;李向明,毕业于南昌大学,高级工程师,学士,主要研究方向为电力系统及其自动化;王虎,毕业于华北电力大学,高级工程师,学士,主要从事电力系统继电保护工作;阳跃永,毕业于上海电力学院,学士,主要研究方向为电力系统自动化;彭娅莉,毕业于上海电力学院,学士,主要研究方向为热能与动力工程。