基于改进长短期记忆网络的新能源场站网络安全评估方法研究

刘珊[1]，李瑞[1]，王尧[2]
（1. 国网山西省电力公司电力科学研究院，山西 太原 030001；
2. 国网山西省电力公司，山西 太原 030021）

摘　要：为了解决新能源大规模并网造成现有新能源场站网络安全防护体系无法满足网络异常监测和告警需求的问题，提出一种基于改进长短期记忆网络的新能源场站网络安全评估方法。首先，根据新能源场站网络系统架构，分析网络安全发生原因；其次，基于随机森林算法求解新能源场站网络流量的基尼系数，进而求出网络流量所有特征的重要系数，选出重要特征；最后，将重要特征输入长短期记忆网络中，利用注意力机制自适应分配数据的时间和特征，加强对网络流量中重要时间和特征的重视，进而提高模型对网络安全评估的准确性。试验结果表明，该方法能够准确评估新能源场站网络安全状态，与支持向量机、卷积神经网络、传统长短期记忆网络相比，评估准确率分别提升了12.65%、9.34%、8.79%，提升了新能源电力系统的网络安全状态感知、评价和告警能力。

关键词：新能源场站；网络安全；长短期记忆网络；随机森林算法；注意力机制
中图分类号：TM73
文献标志码：A
doi: 10.11959/j.issn.1000−0801.2024226

Research on new energy station network security assessment method based on improved LSTM network

LIU Shan[1], LI Rui[1], WANG Yao[2]
1. State Grid Shanxi Electric Power Research Institute, Taiyuan 030001, China
2. State Grid Shanxi Electric Power Company, Taiyuan 030021, China

Abstract: In order to solve the problem of the inability of the existing network security protection system for new energy stations to meet the needs of network anomaly monitoring and alarm caused by the large-scale integration of new energy, a new energy station network security assessment method based on an improved long short-term memory network was proposed. Firstly, based on the architecture of the new energy station network system, the reasons for network security incidents were analyzed. Secondly, based on the random forest algorithm, the Gini coefficient of new energy station network traffic was solved, and then the important coefficients of all network traffic features were cal-

收稿日期：2024−06−07；修回日期：2024−10−13
基金项目：国网山西省电力公司科技项目（No.520530230009）
Foundation Item： State Grid Shanxi Electric Power Company Science and Technology Project (No.520530230009)

culated to select important features. Finally, important features were input into the long short-term memory network, and attention mechanisms were used to adaptively allocate data time and features, strengthening the emphasis on important time and features in network traffic, thereby improving the accuracy of the model for network security assessment. The experimental results show that this method can accurately evaluate the network security status of new energy power stations. Compared with support vector machines, convolutional neural networks, and traditional long short-term memory networks, the evaluation accuracy has been improved by 12.65%, 9.34% and 8.79%, respectively, enhancing the perception, evaluation, and alarm capabilities of network security status in new energy power systems.

Key words: new energy station, network security, long short-term memory network, random forest algorithm, attention mechanism

0　引言

随着“双碳”目标的提出，光伏、风电等新能源的大规模开发与并网利用成为大势所趋。为了实现新能源场站低成本、信息化、区域化以及集约化管理目标，建设新能源控制中心以远程控制和监视分散化的新能源场站显得尤为重要。然而，新能源控制中心普遍面临无人值守的现状，加之光伏电站、风电场等新能源场站多坐落于偏僻地带，户外防护设备布置分散且防护水平不足，这些给电网网络安全带来了巨大挑战。因此，如何在新能源控制中心评估新能源场站网络安全状况并及时预警，以保障电力生产稳定和信息网络安全，成为当前研究的一个热点和难点[1-5]。

目前，国内外学者已经对网络安全开展了一系列研究。文献[6]构建了电力系统安全防护体系，该体系由管理、结构、基因、本体及物理安全组成，依托预警和安全监视作为安全防护行为，能够提前识别和预警影响电力业务的网络安全风险，实现了对攻击行为的溯源。文献[7]提出了网络安全预警系统，该系统将整个网络划分为交换机、主机、服务器的检测域，在各网络段部署网络监控中心，采集并分析信息数据，将分析结果发送至网络预警中心，采用异常检测和误用检测相结合的综合分析方法，实现了网络安全预警、评估和攻击源识别。文献[8]提出了新能源场站网络安全主动预警技术，通过采集主机、安防以及网络设备日志数据，构建网络安全监控体系，并将用户行为纳入考量，识别非法设备接入，从而提升了整个电力系统的安全防御水平。文献[9]从系统、结构、管理以及物理安全4个方面分析了新能源场站网络安全的薄弱环节，并针对性提出了防护措施，从而提高了电力监控网络安全预防能力。文献[10]设计了一个网络安全预警平台，构建了网络安全告警和监测体系，实现了新能源场站网络安全问题的提前感知和快速响应。

近年来随着计算机网络技术的迅速发展，基于人工智能技术的网络安全评估技术也得到了一定的发展和应用[11]。文献[12]提出了基于遗传算法和人工神经网络的网络攻击行为检测技术，通过特征提取方法处理网络数据，采用引力算法优化网络模型的训练参数，实现了网络数据实时监测和攻击行为溯源。文献[13]构建了网络态势预警模型，首先通过熵关联法获得网络安全态势时间序列，然后采用指数平滑的方法得出初始预测时间序列，并经过马尔可夫链修正误差，输出最终的态势，实现了网络安全状态的感知。文献[14]提出了基于无监督模型的网络安全攻击行为检测方法，使用特征权值初始学习得到攻击行为的初始检测结果，采用Bi-Kmeans聚类算法纠正输出攻击行为，综合二者结果确定最终的攻击行为。

虽然上述研究在网络安全评估方面取得了一定成果，但是存在评估准确率低、评估时间长的

问题。此外，对具有时间序列特征的网络安全数据学习能力不足，未将历史时间点对评估结果的影响纳入考量。长短期记忆网络是一个典型的时间序列预测网络，具有预测时间快、准确率高以及递归能力强的优势[15-20]。鉴于此，本文基于上述研究，提出了一种基于改进长短期记忆网络的新能源场站网络安全评估方法。基于新能源场站网络系统架构，分析网络安全发生原因，基于随机森林算法筛选重要特征，将重要特征输入长短期记忆网络，利用注意力机制自适应分配数据的时间和特征，提高对网络流量中重要时间和特征的重视，同时提高模型对网络安全评估的准确性。试验验证表明，所提方法提升了新能源电力系统网络安全状态感知、评价和告警能力。

1 新能源场站网络

新能源场站网络架构如图1所示。场站I区为控制区，包含监控系统、AGC/AVC和电源管理；场站II区为非控制区，主要包含故障录波、功率预测、电量采集等；信息管理区主要包含办公信息系统、天气预报等。

流量分析是评估新能源场站网络安全的重要手段，它能够有效预警外部攻击，即便在不了解具体攻击行为的情况下也能提高预警准确率，系统能够在网络遭受严重破坏前感知潜在威胁，从而使损失降到最低。流量数据是从网络安全保护装置中获得的，通过对正常时和非正常时的流量数据进行特征分析，可以准确判断系统是否处于异常状态。本文将新能源场站网络安全分为正常状态、预攻击状态、入侵状态以及攻陷状态。其中，正常状态为安全状态，电力网络不会接收到任何警报；预攻击状态、入侵状态和攻陷状态为异常状态，一旦检测到这些状态，电力网络便会立即发出警报。

2 基本理论

2.1 新能源场站网络流量特征重要性分析

本文基于随机森林算法评价新能源场站网络流量特征的重要性，根据结果进行特征评估，删除不重要的特征，减少整个新能源场站网络评估时间，使得出现异常攻击时能够及时处理。

随机森林算法属于继承类的学习算法，该算法利用某一规则组合不同类别的分类回归树，众多分类回归树构成一个森林。每次输入特征数据时，所有树均采用投票的方式对输入数据进行分类，票数最多的类别为最终的输出结果。随机森林算法通过对特征数据进行比较、排序后对其在随机森林中的平均贡献度的大小进行重要性评估，

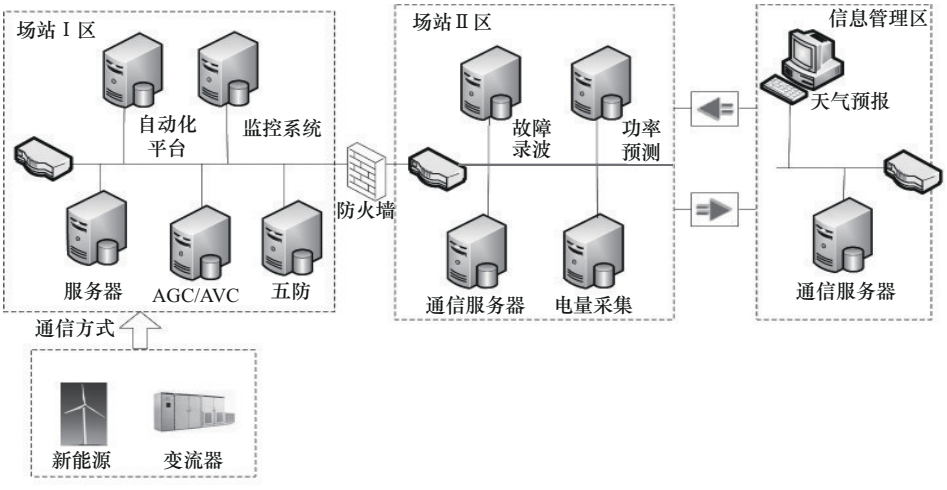

图1 新能源场站网络架构

基尼系数是平均贡献度的衡量参数，计算式为：

$$\mathrm{GI}_n=\sum_{k=1}^{|K|}\sum_{k'\neq k}P_{nk}P_{nk'}=1-\sum_{k=1}^{|K|}P_{nk}^2 \tag{1}$$

其中，GI_n为基尼系数，$|K|$为总的分类数，k为类别序号，k'为不等于k的类别序号，P_{nk}为第n个节点中类别k的占比，即在n个节点中随机选择2个流量数据不同的概率。

假设场站流量特征维度为n，即流量为$\{x_1,x_2,\cdots,x_n\}$，用基尼指数表示某个节点的重要程度，计算式为：

$$\mathrm{VIM}_{in}=\mathrm{GI}_n-\mathrm{GI}_\mathrm{l}-\mathrm{GI}_\mathrm{r} \tag{2}$$

其中，VIM_{in}为第i个输入特征在第n个节点的基尼指数，GI_l、GI_r分别为随机森林左分支、右分支。

归一化处理后，计算式为：

$$\mathrm{VIM}_i^*=\frac{\mathrm{VIM}_i}{\sum_{j=1}^{c}\mathrm{VIM}_j} \tag{3}$$

其中，$\sum_{j=1}^{c}\mathrm{VIM}_j$为所有网络流量特征增益和。

2.2　长短期记忆网络

循环神经网络属于时间序列网络的一种，具有记忆功能和自循环反馈模块[21-23]，循环神经网络内部结构如图2所示。由图2可知，输出事件不仅受此时输入序列的影响，还与之前的输入序列有关。

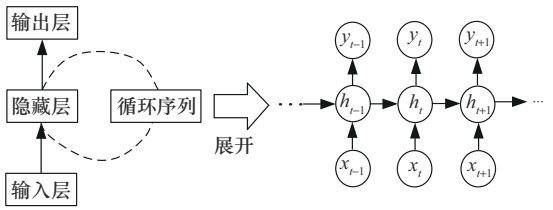

图2　循环神经网络内部结构

循环神经网络训练时先前向传播展开输入序列，然后通过反向传播算法对参数进行更新。若输入序列、输出序列分别为$(x_1,x_2,\cdots,x_{(n-1)},x_n)$、$(y_1,y_2,\cdots,y_{(n-1)},y_n)$，那么前向传播过程为：

$$\begin{cases}h_t=P(W_{xh}x_t+W_{hh}h_{t-1}+b_h)\\o_{t+1}=W_{hy}h_t+b_y\\y_t=P(o_t)\end{cases} \tag{4}$$

其中，h_t为隐藏层值，$P(\cdot)$为激活函数，x_t、y_t分别为输入数据、输出数据，W_{xh}为输入层与隐藏层之间的权值大小，W_{hh}为隐藏层之间的权值大小，W_{hy}为隐藏层与输出层之间的权值大小，b为对应的偏置，O_t为输出门数据。

长短期记忆网络属于一种特殊的循环神经网络，具有预测时间快、准确率高以及递归能力强的优势，能够解决循环神经网络长期依赖的问题[24-26]，加入“门”结构将信息添加或者丢掉，能够起到长期记忆的作用。长短期记忆网络结构如图3所示。

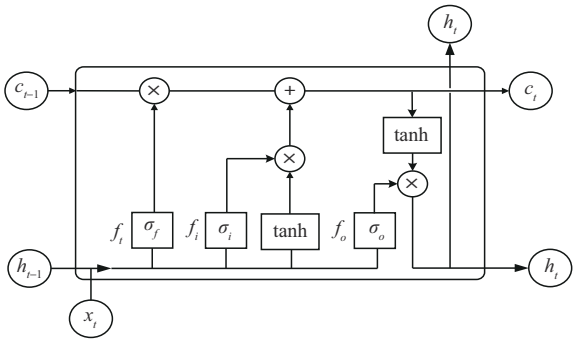

图3　长短期记忆网络结构

长短期记忆网络中的“门”对信息进行选择的计算式为：

$$\begin{cases}g(x)=\sigma(Wx+b)\\\sigma(x)=\dfrac{1}{1+\mathrm{e}^{-x}}\end{cases} \tag{5}$$

其中，$g(x)$为“门”的选择性输出；$\sigma(x)$为激活函数，即Sigmod函数，输出为选择的信息量，大小为0～1。

长短期记忆网络的前向传播计算式为：

$$\begin{cases}i_t=\sigma(W_{xi}x_t+W_{hi}h_{t-1}+b_i)\\f_t=\sigma(W_{xf}x_t+W_{hf}h_{t-1}+b_f)\\o_t=\sigma(W_{xo}x_t+W_{ho}h_{t-1}+b_o)\\c_t=f_t\cdot c_{t-1}+i_t\cdot\tanh(W_{xc}x_t+W_{fc}h_{t-1}+b_c)\\h_t=o_t\cdot\tanh(c_t)\end{cases} \tag{6}$$

其中，i_t、f_t、o_t分别为输入门、遗忘门以及输出门，c_t、h_t分别为t时刻的短时记忆、长时记忆。

前向传播过程中，输入门影响输入数据被记忆在短时记忆中的信息；遗忘门影响长期记忆需要保存的信息，即前一时刻忘记的短时记忆信息；输出门影响短时记忆信息，即下一时刻的信息。

经过反向传播算法和交叉损失函数更新参数，损失函数计算式为：

$$\begin{cases} L_t(y_t,\hat{y}_t)=-y_t\log\hat{y}_t \\ L(y,\hat{y})=\sum_t L_t(y_t,\hat{y}_t)=-\sum_t y_t\log\hat{y}_t \end{cases} \tag{7}$$

其中，y_t、$\hat{y}_t$分别为实际输出、预测输出。

2.3 softmax函数

softmax函数是一种多分类函数，如果输入x的输出标签为y，那么x属于第j类的概率为$P(y=j|x)$。假设softmax函数输出向量维度为m，所有元素大小在0～1，且相加为1，得出的计算式为：

$$\boldsymbol{y}'_{(i)}=\begin{bmatrix} P(y_{(i)}=1|x_{(i)}) \\ P(y_{(i)}=2|x_{(i)}) \\ \cdots \\ P(y_{(i)}=n|x_{(i)}) \end{bmatrix}^{\mathrm{T}}=\mathrm{softmax}(y_{(i)})= \frac{1}{\sum_{l=1}^{m}\mathrm{e}^{x(T_i)wl}}\begin{bmatrix} \mathrm{e}^{x(T_i)w1} \\ \mathrm{e}^{x(T_i)w2} \\ \cdots \\ \mathrm{e}^{x(T_i)wm} \end{bmatrix}^{\mathrm{T}} \tag{8}$$

其中，$P(y_{(i)}=k|x_{(i)})$为样本i属于第k个类别的概率。

2.4 注意力机制

本文提出的注意力机制重点关注流量数据内部联系，减少对外部数据的依赖，提高网络安全评估准确性。权值则通过将流量序列不同位置数据联系起来进行计算，对于权值大的位置给予重要信息，加强结果影响。

对输入序列进行打分，计算式为：

$$s_i=\sigma\left(W^{\mathrm{T}}x_i+b\right) \tag{9}$$

其中，s_i为第i个序列的打分结果，W、b分别为权重和偏置大小。

所有序列打分值得出后，进行归一化处理，计算式为：

$$\alpha_i=\frac{\exp(s_i)}{\sum_i\exp(s_i)} \tag{10}$$

其中，α_i为第i个输入序列的注意力权值。

经过注意力机制处理后，得到的输出计算式为：

$$O=\{\alpha_1\cdot x_1,\alpha_2\cdot x_2,\cdots,\alpha_n\cdot x_n\}^{\mathrm{T}} \tag{11}$$

3 网络安全评估方案

3.1 评估模型

基于改进长短期记忆网络的新能源场站网络安全评估模型如图4所示，将重要特征输入长短期记忆网络中，利用注意力机制自适应分配数据的时间和特征，加强对网络流量中重要时间和特征的重视，提高模型对网络安全评估的准确性。模型具体结构说明如下。

（1）第一层自注意力层：自适应分配权值，

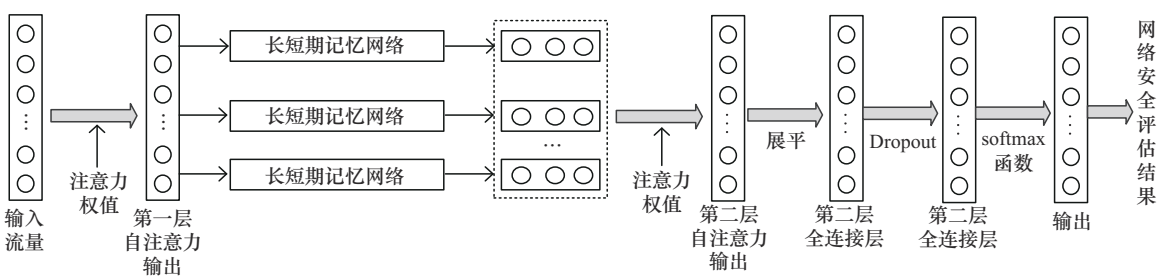

图4 基于改进长短期记忆网络的新能源场站网络安全评估模型

提高对输入流量数据重要特征的学习。

（2）长短期记忆网络层：提取时间序列深层特征。

（3）第二层自注意力层：自适应不同时间和隐藏单元权值。

（4）全连接层：展平数据，利用 Dropout 函数防止过拟合。

（5）输出层：利用 softmax 函数输出网络安全评估结果，即正常状态、预攻击状态、入侵状态以及攻陷状态。

3.2　评估过程

基于改进长短期记忆网络的新能源场站网络安全评估流程如图 5 所示，具体步骤如下。

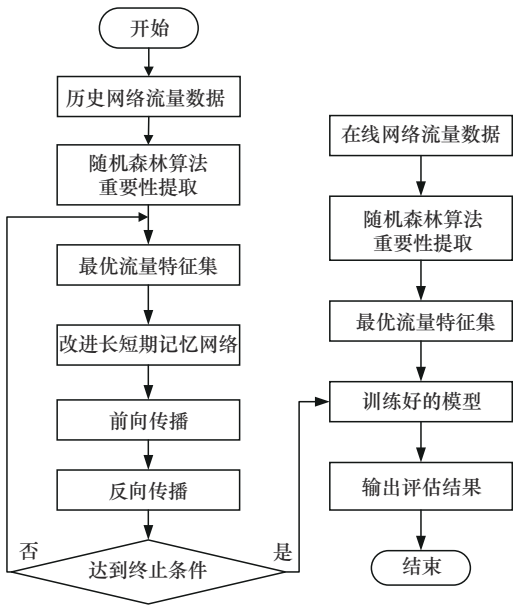

图 5　基于改进长短期记忆网络的新能源场站网络安全评估流程

步骤 1　提取网络流量数据，将数据划分成训练集和测试集。

步骤 2　设置训练集为历史流量数据，基于随机森林算法求出基尼指数，提取出重要程度高的数据，构成最优流量特征集。

步骤 3　将输入数据输入改进长短期记忆网络中，前向传播网络，得出输入门、遗忘门以及输出门，反向传播网络更新参数。

步骤 4　判断是否满足终止条件。若不满足，返回步骤 2；若满足，继续下一步。

步骤 5　设置测试集为在线流量数据，将输入数据输入已经训练好的模型中。

步骤 6　设置 softmax 函数输出维度为 4，分别对应正常状态、预攻击状态、入侵状态以及攻陷状态 4 种状态，输出评估结果。根据实际网络安全状态验证本文所提评估模型的有效性。

4　试验与分析

4.1　试验环境

为了验证本文所提方法的应用效果，搭建的实验仿真环境见表 1。

表 1　实验仿真环境

性能属性	参数
适配器	Intel Centrtino Advanced-N 6205 / atheros AR9485
硬盘参数	机械硬盘：2 TB
内存	16 GB
CPU	Intel Core i7-7400
系统	Windows 10

4.2　网络安全评估指标

当网络被攻击时，需要及时发出告警信号给工作人员，本文采用评估准确率、误报率、漏报率以及误警率作为衡量指标，计算式如下。

$$\begin{cases} R_{\mathrm{A}}=\dfrac{n_{\mathrm{TP}}+n_{\mathrm{TN}}}{n_{\mathrm{TP}}+n_{\mathrm{TN}}+n_{\mathrm{FP}}+n_{\mathrm{FN}}} \\ R_{\mathrm{FP}}=\dfrac{n_{\mathrm{FP}}}{n_{\mathrm{TN}}+n_{\mathrm{FP}}} \\ R_{\mathrm{FN}}=\dfrac{n_{\mathrm{FN}}}{n_{\mathrm{TP}}+n_{\mathrm{FN}}} \\ R_{\mathrm{FA}}=\dfrac{R_{\mathrm{FN}}+R_{\mathrm{FP}}}{2} \end{cases} \tag{12}$$

其中，R_{A}、R_{FP}、R_{FN}、R_{FA} 分别为准确率、误报率、漏报率、误警率，n_{TP}、n_{TN} 分别为正样本、反样本被正确识别的数量，n_{FN}、n_{FP} 分别为正样本、反样本被错误识别的数量。

4.3 模型参数

首先，确定长短期记忆网络隐藏层神经元个数。将隐藏层神经元个数从50开始逐步增加，准确率和隐藏层神经元数量的关系如图6所示。由图6可知，当隐藏层神经元达到200时，评估准确率最高，如果继续增加隐藏层神经元数量，评估准确率反而下降，出现过拟合。因此，设置后续的长短期记忆网络隐藏层神经元个数为200。

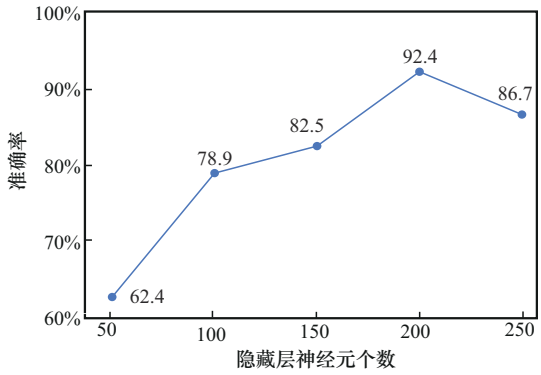

图6 准确率和隐藏层神经元数量的关系

其次，确定长短期记忆网络迭代次数。网络损失函数和评估准确率随迭代次数的变化分别如图7、图8所示。由图7、图8可知，当迭代次数达到100时，损失函数达到最低、评估准确率达到最高。因此，后续模型训练中，设置迭代次数为100。

经过多次实验验证，确定的网络安全评估模型参数见表2。

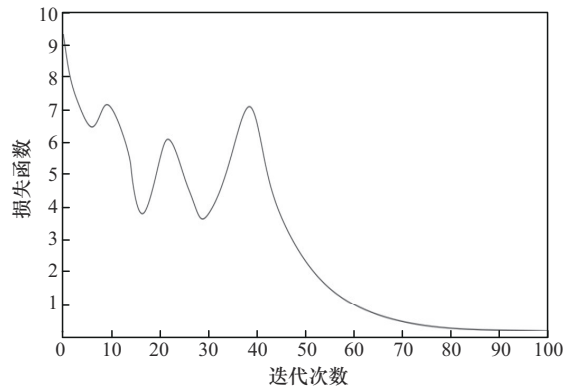

图7 网络损失函数随迭代次数的变化

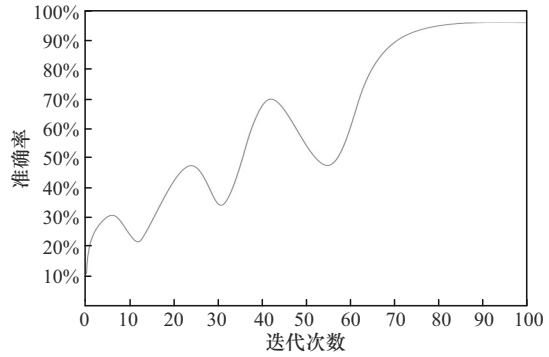

图8 评估准确率随迭代次数的变化

表2 网络安全评估模型参数

参数	大小
随机森林决策树个数	400
批量	256
迭代次数	100
第一层全连接层单元个数	200
第二层全连接层单元个数	20
长短期记忆网络隐藏层神经元个数	200

4.4 结果分析

网络安全评估性能测试的各项指标结果如图9所示。由图9可知，评估准确率高达96.82%，误报率、漏报率、误警率分别只有4%、10%、7%，这说明本文方法对于网络安全评估效果较好，当网络遭受攻击时，能够及时发现异常状况并上报告警信号。

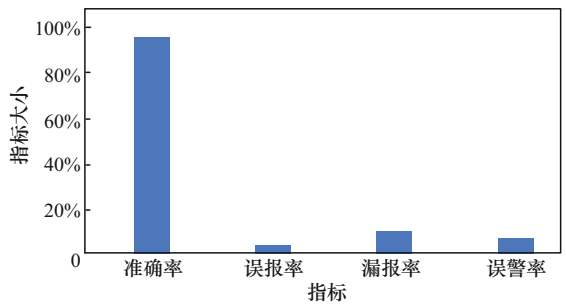

图9 网络安全评估性能测试的各项指标结果

不同状态的评估准确率如图10所示。由图10可知，本文方法对正常状态、预攻击状态、入侵状态及攻陷状态均具有较高的评估准确率，这说明所提方法能够精准预测网络攻击过程，当

出现异常状态时，可以早期干预，防止网络被攻陷。

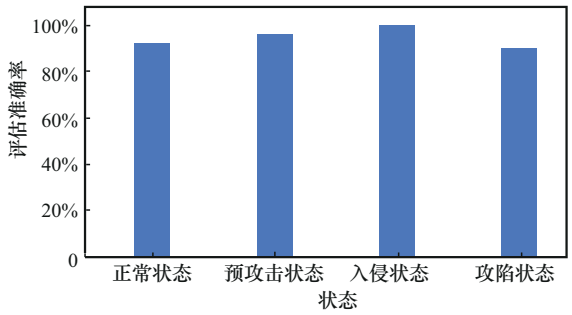

图10　不同状态的评估准确率

当出现预攻击状态、入侵状态、攻陷状态这些异常状态时，说明网络安全遭受攻击，需要及时发出告警信号，异常告警准确率变化如图11所示。由图11可知，受到攻击的80 min内告警准确率始终保持在93%以上，这说明本文方法能够准确预测各种状态变化，能够直观感受某一时刻的实际状态。

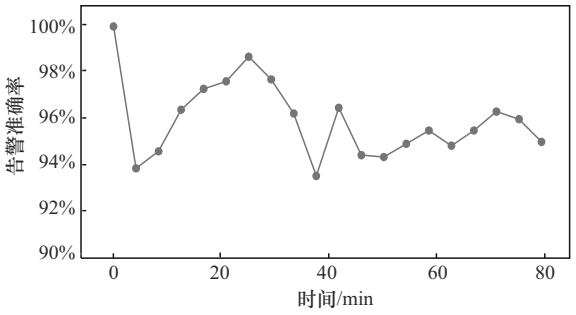

图11　异常告警准确率变化

为了验证本文方法的先进性，将本文方法与支持向量机、卷积神经网络、传统长短期记忆网络进行对比，不同方法的指标对比见表3。由表3可知，本文方法相比于支持向量机、卷积神经网络、传统长短期记忆网络，评估准确率分别提升了12.65%、9.34%、8.79%，误报率分别降低了13.79%、8.46%、3.42%，漏报率分别降低了15.57%、9.27%、4.85%。这是因为支持向量机属于浅层式机器学习，无法深层次提取高纬度新能源场站网络流量数据；卷积神经网络虽然具有深度学习的能力，但是在面对时序的场站网络流量数据时，无法充分学习流量不同时刻的特征；传统长短期记忆网络虽然能够提取流量时序特征，但是缺少对流量数据内部联系的重点关注，且未加强对网络流量中重要时间和特征的重视。本文所提方法引入注意力机制，将权值大的位置给予重要信息，加强结果影响，进而提高了模型对网络安全评估的准确性，验证了本文方法的优越性。

表3　不同方法的指标对比

参数	本文方法	支持向量机	卷积神经网络	传统长短期记忆网络
准确率	96.82%	84.17%	87.48%	88.03%
误报率	0.16%	13.95%	8.62%	3.58%
漏报率	0.10%	15.67%	9.37%	4.95%
误警率	0.13%	14.81%	9.00%	4.27%

5　结束语

本文提出一种基于改进长短期记忆网络的新能源场站网络安全评估方法，采用随机森林算法求出流量基尼系数，将重要特征输入改进长短期记忆网络方法中。试验结果表明，本文方法评估准确率高达96.82%，误报率、漏报率、误警率分别只有0.16%、0.10%、0.13%，说明本文方法对于网络安全评估效果较好，当网络遭受攻击时，能够及时发现异常状况并上报告警信号。与支持向量机、卷积神经网络、传统长短期记忆网络相比，本文方法的评估准确率分别提升了12.65%、9.34%、8.79%，误报率分别降低了13.79%、8.46%、3.42%，漏报率分别降低了15.57%、9.27%、4.85%，验证了本文方法的先进性。

参考文献：

[1]　金志刚, 刘凯, 武晓栋. 智能电网AMI领域IDS研究综述[J]. 信息网络安全, 2023, 23(1): 1-8.
JIN Z G, LIU K, WU X D. A review of IDS research in smart

grid AMI field[J]. Netinfo Security, 2023, 23(1): 1-8.

[2] 周劼英, 张晓, 邵立嵩, 等. 新型电力系统网络安全防护挑战与展望[J]. 电力系统自动化, 2023, 47(8): 15-24.
ZHOU J Y, ZHANG X, SHAO L S, et al. Challenges and prospects of cyber security protection for new power system[J]. Automation of Electric Power Systems, 2023, 47(8): 15-24.

[3] 陈伟雄, 杨晓晨, 春增军, 等. 电力企业网络安全威胁情报管理体系的研究与实践[J]. 电信科学, 2022, 38(7): 184-189.
CHEN W X, YANG X C, CHUN Z J, et al. Research and practice of network security threat intelligence management system for power enterprise[J]. Telecommunications Science, 2022, 38 (7): 184-189.

[4] WANG S X, CHEN H W, ZHAO Q Y, et al. Preserving scheme for user's confidential information in smart grid based on digital watermark and asymmetric encryption[J]. Journal of Central South University, 2022, 29(2): 726-740.

[5] 王增平, 林一峰, 王彤, 等. 电力系统继电保护与安全控制面临的挑战与应对措施[J]. 电力系统保护与控制, 2023, 51(6): 10-20.
WANG Z P, LIN Y F, WANG T, et al. Challenges and countermeasures to power system relay protection and safety control[J]. Power System Protection and Control, 2023, 51(6): 10-20.

[6] 辛耀中, 石俊杰, 周京阳, 等. 智能电网调度控制系统现状与技术展望[J]. 电力系统自动化, 2015, 39(1): 2-8.
XIN Y Z, SHI J J, ZHOU J Y, et al. Technology development trends of smart grid dispatching and control systems[J]. Automation of Electric Power Systems, 2015, 39(1): 2-8.

[7] 王超. 计算机网络安全中入侵检测系统的研究与设计[D]. 成都: 电子科技大学, 2007.
WANG C. Research and design of intrusion detection system in computer network security[D]. Chengdu: University of Electronic Science and Technology of China, 2007.

[8] 金学奇, 苏达, 毛南平, 等. 面向新能源场站的主动监视与预警技术研究[J]. 浙江电力, 2019, 38(6): 106-112.
JIN X Q, SU D, MAO N P, et al. Research on active monitoring and early warning technology for new energy station[J]. Zhejiang Electric Power, 2019, 38(6): 106-112.

[9] 刘博, 李梁, 刘军娜, 等. 新能源场站电力监控系统网络安全薄弱环节分析[J]. 电工技术, 2021(18): 78-80.
LIU B, LI L, LIU J N, et al. Analysis of weak links in network security of power monitoring system in new energy fields[J]. Electric Engineering, 2021(18): 78-80.

[10] 韩硕, 戚红建, 李宏亮. 新能源场站网络安全态势感知和监测预警平台设计[J]. 工业信息安全, 2023(3): 69-75.
HAN S, QI H J, LI H L. Design of a new energy station network security situation awareness and monitoring & warning platform[J]. Industry Information Security, 2023(3): 69-75.

[11] 熊中浩, 张伟, 杨国玉. 基于DBN的网络安全态势评估和态势预测建模研究[J]. 电子技术应用, 2021, 47(5): 35-39, 44.
XIONG Z H, ZHANG W, YANG G Y. Research on network security situation assessment and situation prediction modeling based on DBN[J]. Application of Electronic Technique, 2021, 47(5): 35-39, 44.

[12] 罗予东, 陆璐. 基于人工神经网络和遗传算法的网络攻击检测[J]. 计算机工程与设计, 2021, 42(9): 2446-2454.
LUO Y D, LU L. Network attack detection based on artificial neural networks and genetic algorithm[J]. Computer Engineering and Design, 2021, 42(9): 2446-2454.

[13] 杨宏宇, 张旭高. 一种网络安全态势自适应预测模型[J]. 西安电子科技大学学报, 2020, 47(3): 14-22.
YANG H Y, ZHANG X G. Network security situation adaptive prediction model[J]. Journal of Xidian University, 2020, 47(3): 14-22.

[14] 王婷, 王娜, 崔运鹏, 等. 基于半监督学习的无线网络攻击行为检测优化方法[J]. 计算机研究与发展, 2020, 57(4): 791-802.
WANG T, WANG N, CUI Y P, et al. The optimization method of wireless network attacks detection based on semi-supervised learning[J]. Journal of Computer Research and Development, 2020, 57(4): 791-802.

[15] ZHANG J J, WANG P, YAN R Q, et al. Long short-term memory for machine remaining life prediction[J]. Journal of Manufacturing Systems, 2018(48): 78-86.

[16] SU C, LI L, WEN Z J. Remaining useful life prediction via a variational autoencoder and a time-window-based sequence neural network[J]. Quality and Reliability Engineering International, 2020, 36(5): 1639-1656.

[17] 李京峰, 陈云翔, 项华春, 等. 基于LSTM-DBN的航空发动机剩余寿命预测[J]. 系统工程与电子技术, 2020, 42(7): 1637-1644.
LI J F, CHEN Y X, XIANG H C, et al. Remaining useful life prediction for aircraft engine based on LSTM-DBN[J]. Systems Engineering and Electronics, 2020, 42(7): 1637-1644.

[18] CHEN Z H, WU M, ZHAO R, et al. Machine remaining useful life prediction via an attention-based deep learning approach[J]. IEEE Transactions on Industrial Electronics, 2021, 68(3): 2521-2531.

[19] ZHANG Y, XIN Y Q, LIU Z W, et al. Health status assessment and remaining useful life prediction of aero-engine based on Bi-GRU and MMoE[J]. Reliability Engineering & System Safety,

2022(220): 108263.

[20] 闫啸家, 梁伟阁, 张钢, 等. 基于RCNN-ABiLSTM的机械设备剩余寿命预测方法[J]. 系统工程与电子技术, 2023, 45(3): 931-940.
YAN X J, LIANG W G, ZHANG G, et al. Prediction method for mechanical equipment based on RCNN-ABiLSTM[J]. Systems Engineering and Electronics, 2023, 45(3): 931-940.

[21] ZHANG X Y, YIN F, ZHANG Y M, et al. Drawing and recognizing Chinese characters with recurrent neural network[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2018, 40(4): 849-862.

[22] GUO L, LI N P, JIA F, et al. A recurrent neural network based health indicator for remaining useful life prediction of bearings[J]. Neurocomputing, 2017(240): 98-109.

[23] WANG H, PENG M J, MIAO Z, et al. Remaining useful life prediction techniques for electric valves based on convolution auto encoder and long short term memory[J]. ISA Transactions, 2021(108): 333-342.

[24] ZHAO H T, SUN S Y, JIN B. Sequential fault diagnosis based on LSTM neural network[J]. IEEE Access, 2018(6): 12929-12939.

[25] SONG H, DAI J J, LUO L G, et al. Power transformer operating state prediction method based on an LSTM network[J]. Energies, 2018, 11(4): 914.

[26] NANDURI A, SHERRY L. Anomaly detection in aircraft data using Recurrent Neural Networks (RNN) [C]//Proceedings of the 2016 Integrated Communications Navigation and Surveillance (ICNS). Piscataway: IEEE Press, 2016: 5C2-1-5C2-8.

[作者简介]

刘珊（1987– ），女，国网山西省电力公司电力科学研究院高级工程师，主要研究方向为电网数字化及网络攻防技术。

李瑞（1981– ），男，博士，国网山西省电力公司电力科学研究院正高级工程师，主要研究方向为电力系统自动化及其智能数字化技术。

王尧（1991– ），男，国网山西省电力公司工程师，主要研究方向为电网网络安全攻击防御技术。