基于神经网络的大型无人值守风电场网络安全监控技术研究*

邱情芳[1]，曹学铭[1]，王丹丹[1]，蔡继峰[1]，李新华[1]，周成胜[2]
（1. 北京鉴衡认证中心有限公司，北京 100013；2. 中国信息通信研究院，北京 100083）

摘 要：大型无人值守风电场作为清洁能源的重要组成部分，其网络安全不仅关系到风电场的稳定运行，还直接影响到整个电力系统的安全。研究基于神经网络的大型无人值守风电场网络安全监控技术，以提高风电场的网络安全防护能力。首先分析了大型无人值守风电场的网络安全威胁，包括外部攻击、内部泄露、设备故障等。针对这些威胁，设计了基于神经网络的网络安全监控模型，该模型能够实时监测风电场的网络流量、设备状态等关键信息，并通过深度学习算法对异常行为进行识别和预警。为了验证模型的有效性，在模拟风电场环境中进行了实验，结果表明，该模型能够准确识别出多种网络安全威胁，并提前发出预警，为风电场的网络安全防护提供了有力支持。

关键词：风电场；网络安全；安全监控；神经网络
中图分类号：TP391. 9　　**文献标识码**：A　　**DOI**：10. 19358/j. issn. 2097 - 1788. 2025. 02. 002
引用格式：邱情芳，曹学铭，王丹丹，等. 基于神经网络的大型无人值守风电场网络安全监控技术研究［J］. 网络安全与数据治理，2025，44(2)：10 - 16，31.

Research on network security monitoring technology for large unmanned wind farm based on neural network

Qiu Qingfang[1], Cao Xueming[1], Wang Dandan[1], Cai Jifeng[1], Li Xinhua[1], Zhou Chengsheng[2]
(1. China General Certification Center, Beijing 100013, China;
2. China Academy of Information and Communications Technology, Beijing 100083, China)

Abstract: Large-scale unmanned wind farm is an important component of clean energy, and its network security not only relates to the stable operation of wind farms, but also directly affects the security of the entire power system. Therefore, this study aims to explore the network security monitoring technology for large-scale unmanned wind farms based on neural networks, in order to improve the network security protection capability of wind farms. This study first analyzed the network security threats of large unmanned wind farms, including external attacks, internal leaks, equipment failures etc. In response to these threats, this study designed a neural network-based network security monitoring model that can monitor key information such as network traffic and equipment status of wind farms in real time, and identify and warn of abnormal behavior through deep learning algorithms. In order to verify the effectiveness of the model, experiments were conducted in a simulated wind farm environment. The results showed that the model can accurately identify various network security threats and issue early warnings, providing strong support for the network security protection of wind farms.

Key words: wind farm; network security; security monitoring; neural network

0 引言

随着全球能源结构的转型和可再生能源的快速发展，大型无人值守风电场作为清洁能源的重要组成部分，其建设规模和数量不断增加。然而，由于风电场地理位置偏远、设备众多、通信复杂等特点，其网络安全问题日益凸显。风电场作为电力系统的重要节点，其网络安全不仅关系到风电场的稳定运行，还直接影响到整个电力系统的安全。因此，加强风电场的网络安全监控具有重

*基金项目：国家重点研发计划（2023YFB4203100）

要意义。

传统的网络安全监控方法主要依赖于防火墙、入侵检测系统等技术手段，但这些方法在面对新型网络攻击时往往存在漏报、误报等问题。此外，由于风电场设备众多、通信复杂，传统的监控方法难以实现对所有设备的全面监控和异常行为的及时预警。因此，探索新的网络安全监控技术，提高风电场的网络安全防护能力，是当前亟待解决的问题。

此外，风电场网络安全监控还面临着一些特殊的问题和挑战。例如，风电场设备众多、通信复杂，监控数据量大且异构性强；风电场地理位置偏远，通信延迟和丢包等问题时有发生；风电场网络安全威胁多样且隐蔽性强，难以通过单一技术手段进行全面防护。因此，需要探索新的网络安全监控技术，以适应风电场网络安全监控的特殊需求。

针对以上问题和挑战，本研究旨在探索基于神经网络的大型无人值守风电场网络安全监控技术。具体研究目标包括：设计基于神经网络的网络安全监控模型，实现对风电场网络流量、设备状态等关键信息的实时监测和异常行为的识别预警；通过实验验证模型的有效性，并探讨神经网络在网络安全监控中的应用优势和局限性；提出改进建议和优化措施，进一步提高神经网络在网络安全监控中的应用效果。

1 研究现状

1.1 网络安全监控技术综述

随着网络技术的日新月异与网络威胁的日益复杂多变，网络安全监控技术正步入一个全新的发展阶段，其未来发展趋势不仅深刻影响着企业的信息安全防护体系，更对构建安全、稳定的网络环境具有决定性意义。具体而言，网络安全监控技术将沿着智能化、集成化、协同化及可视化的方向持续演进，为应对复杂多变的网络威胁提供更为坚实的技术支撑。

1.2 神经网络在大型风电场网络安全监控领域的应用挑战

神经网络在监控领域，特别是应用于大型风电场的网络攻击监控时，面临着多重挑战。尽管神经网络如径向基函数网络（RBF）、小波神经网络、Elman 神经网络、卷积神经网络（CNN）、图神经网络（GNN）以及双模态网络入侵检测框架（XG-NID）等在网络攻击监控方面展现出强大的特征提取能力、实时检测能力和自适应学习能力，但在大型风电场的特定环境中，这些优势的实现却面临诸多困难。大型风电场位于偏远地区，网络环境复杂、数据通信量大且类型多。神经网络模型需有强大特征提取能力，处理高并发、大规模数据流，以保监控实时准确，但现有模型处理海量数据时存在计算资源消耗大、速度慢的问题，难以满足实时监控需求。风电场网络结构复杂，设备、传感器和控制系统众多，数据交互频繁复杂。神经网络模型构建攻击监控体系时需处理图结构数据，融合多源信息。风电场网络环境不断变化，新攻击手段频出。神经网络模型需有强大的自适应学习能力以适应变化，但现有模型自适应学习依赖大量历史数据和训练样本，在风电场实际应用中较难实现。

为此多位国内学者探讨了风电场电力监控安全防护，如郭建英关注国内对风电场网络安全基础层面的研究[1]，吴俊杰研究网络攻击下的风电场优化调度及控制策略[2]，宣政探索无人值守风电场的远程监控[3]，王忠超和叶林的研究聚焦于风电场网络系统安全强化[4]，王其乐等也投入关键技术研发[5]。这些研究和实践体现了国内对风电场网络安全监控的重视与深入探索。

1.3 风电场网络安全监控研究现状

风电场监控系统的设计旨在实时收集、处理并分析各类传感器数据，确保风电场高效安全运行。其典型功能包括数据采集与展示（如运行数据、状态参数、电网参数及故障显示），实时控制功能（如根据电网和气象条件远程控制风机启停、复位，调节桨距角度等，以及启动变流器系统并网发电），以及数据统计与查询（包括历史日志查询和各种图表展示）[6-7]。

网络安全监控技术在风电场中的应用迅速发展，其中组态软件如 ForceControl 通过图形化界面实现数据采集与监控，整合数据源进行统一管理；工业物联网（IIoT）与边缘计算技术减少了数据传输延迟，提高了系统响应效率；软件定义网络（SDN）和网络功能虚拟化（NFV）提升了网络的灵活性和安全性；而 5G 网络与混合组网则凭借低时延、高带宽特性，满足了风电场智能运维的需求。然而，风电场也面临着包括数据篡改攻击、中间人攻击、拒绝服务攻击和重放攻击等多种网络安全威胁[8]，这些攻击可能导致数据失真、系统崩溃甚至物理损坏。

2 研究方法与模型构建

2.1 数据采集与预处理

2.1.1 数据采集来源

风电场网络安全监控是一个综合性的系统，它依赖于对风机运行状态数据、控制信号数据、气象数据以及电网连接数据的全面采集与分析。这些数据通过工业以太网、光纤通信等多种通信网络传输至数据采集中心，成为检测异常网络行为、识别潜在网络攻击的重要基础。

风机内部传感器采集的转速、功率、温度等运行状态数据，以及控制系统发出的控制信号数据，能够反映

风机的运行逻辑和健康状况。同时，气象数据如风速、风向、温度等，为关联分析提供了补充信息。而电网连接数据则评估了风电场与电网的交互安全。对这些数据的准确采集和深入分析，有助于及时发现网络攻击的迹象，从而构建更加完善的风电场网络安全监控体系。

2.1.2 数据采集方法

（1）传感器直接采集

对于风机内部的传感器和气象站的传感器，采用直接采集的方法。传感器将物理量转换为电信号（如模拟电压或电流信号），然后通过模数转换（ADC）将模拟信号转换为数字信号。例如，风机电流传感器输出的模拟信号，经过 ADC 芯片转换为数字信号后，按照预定的通信协议（如 Modbus 协议）进行数据封装，以便传输到数据采集中心[9-10]。

（2）系统接口采集

对于风机的控制信号数据和电网连接数据，通过与相应系统的接口进行采集。例如，从风机控制系统的通信接口获取控制信号数据，从电网监测设备的网络接口获取电网连接数据。这些数据以特定的格式（如网络数据包）传输，在采集端需要进行协议解析，将数据转换为可处理的格式[11]。

2.1.3 数据预处理流程

数据清洗[12]：即去除异常值。由于传感器误差或环境干扰等因素，采集到的数据可能存在异常值。对于风机运行状态数据，如转速数据，设其序列为：

$$x = \{x_1, x_2, \cdots, x_n\} \tag{1}$$

其均值为：

$$\mu = \frac{1}{n}\sum_{i=1}^{n} x_i \tag{2}$$

标准差为：

$$\sigma = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(x_i - \mu)^2} \tag{3}$$

若 $|x_i - \mu| > 3\sigma$，则将 x_i 判定为异常值并去除。对于气象数据中的风速数据，也可采用类似方法去除异常值[13-14]。

处理缺失值：当某些数据存在缺失时，需要进行处理。例如，对于风机功率数据，如果某一时刻的功率数据缺失，可采用线性插值法处理。设已知时间 t_1、t_2 对应的功率值为 P_1、P_2，中间缺失时刻 t 的功率值 P 可通过下式进行计算：

$$P = P_1 + \frac{(P_2 - P_1)(t - t_1)}{t_2 - t_1} \tag{4}$$

2.1.4 数据特征提取与选择

主成分分析（PCA）：设原始数据矩阵为 $\boldsymbol{A} = (a_{ij})_{p\times q}$，其中 p 为样本数量，q 为特征数量。首先计算协方差矩阵

$$\boldsymbol{C} = \frac{1}{p-1}\boldsymbol{A}^{\mathrm{T}}\boldsymbol{A} \tag{5}$$

然后求解协方差矩阵的特征值 λ_i 和特征向量 $\boldsymbol{v}_i$。按照特征值的大小对特征向量进行排序，选择前 k 个特征向量组成投影矩阵 $\boldsymbol{V} = [\boldsymbol{v}_1, \boldsymbol{v}_2, \cdots, \boldsymbol{v}_k]$，则经过 PCA 变换后的新数据 $\boldsymbol{B} = \boldsymbol{A}\boldsymbol{V}$。通过这种方式可以降低数据的维度，同时保留主要的特征信息。

小波变换：对于具有时间序列特性的风机运行状态数据和气象数据，可采用小波变换进行特征提取。设 $f(t)$ 为原始时间序列数据，小波函数为：

$$\psi_{a,b}(t) = \frac{1}{\sqrt{a}}\psi\left(\frac{t-b}{a}\right) \tag{6}$$

其中，a 为尺度参数，b 为平移参数。通过对 $f(t)$ 进行小波变换

$$Wf(a, b) = \int_{-\infty}^{\infty} f(t)\,\overline{\psi_{a,b}(t)}\,\mathrm{d}t \tag{7}$$

得到不同尺度下的小波系数，这些小波系数可作为数据的特征。

2.2 神经网络模型设计

2.2.1 神经网络结构

（1）多层感知机（MLP）与卷积神经网络（CNN）的融合结构[15-17]

①输入层。根据数据采集的来源，输入层接收经过预处理的风机运行状态数据、气象数据和电网连接数据。输入神经元的数量取决于经过特征选择后的数据特征数量。

②隐藏层。MLP 部分：包含多个全连接层。第一层全连接层的神经元数量设为 n_1，采用 ReLU 激活函数 $f(x) = \max(0, x)$；第二层全连接层的神经元数量设为 n_2，同样采用 ReLU 激活函数。全连接层之间的连接权重矩阵为 $\boldsymbol{W}_{ij}$，偏置项为 $\boldsymbol{b}_i$。

CNN 部分：包含卷积层和池化层。卷积层的卷积核大小设为 3×3，步长为 1，通道数根据输入数据的类型和特征进行设置。卷积层的计算为：

$$y_{ij}^{l} = f\left(\sum_{m=0}^{M-1}\sum_{n=0}^{N-1} w_{mn}^{l} x_{i+m,j+n}^{l-1} + b^{l}\right) \tag{8}$$

其中，y_{ij}^{l} 为第 l 层卷积层的输出，w_{mn}^{l} 为卷积核权重，$x_{i+m,j+n}^{l-1}$ 为第 $l-1$ 层的输入，b^{l} 为偏置项，f 为激活函数。池化层采用最大池化，池化窗口大小为 2×2，步长为 2。

③输出层。输出层的神经元数量根据监控任务进行设置。例如，如果是进行网络攻击分类（正常、攻击类型 1、攻击类型 2 等），则输出层神经元数量等于攻击类型的数量。采用 Softmax 函数进行概率输出：

$$y_i = \frac{e^{z_i}}{\sum_{j=1}^{k} e^{z_j}} \tag{9}$$

其中 z_i 为输出层神经元的输入，y_i 为第 i 个类别的概率。

（2）递归神经网络（RNN）与注意力机制的结合结构

RNN 部分：采用长短期记忆网络（LSTM）单元来处理时间序列数据（如风机运行状态的历史数据和气象数据的时间序列）。LSTM 单元中的遗忘门：

$$f_t = \sigma(\boldsymbol{W}_f \cdot [h_{t-1}, x_t] + \boldsymbol{b}_f) \tag{10}$$

输入门：

$$i_t = \sigma(\boldsymbol{W}_i \cdot [h_{t-1}, x_t] + \boldsymbol{b}_i) \tag{11}$$

输出门：

$$o_t = \sigma(\boldsymbol{W}_o \cdot [h_{t-1}, x_t] + \boldsymbol{b}_0) \tag{12}$$

细胞状态：

$$C_t = f_t * C_{t-1} + i_t * \tanh(\boldsymbol{W}_C \cdot [h_{t-1}, x_t] + \boldsymbol{b}_C) \tag{13}$$

隐藏状态：

$$h_t = o_t * \tanh(C_t) \tag{14}$$

其中，$\boldsymbol{W}_f$、$\boldsymbol{W}_i$、$\boldsymbol{W}_o$、$\boldsymbol{W}_C$ 为权重矩阵，$\boldsymbol{b}_f$、$\boldsymbol{b}_i$、$\boldsymbol{b}_o$、$\boldsymbol{b}_C$ 为偏置项，$\sigma(x) = \frac{1}{1+e^{-x}}$。

注意力机制部分：设输入序列为

$$X = \{x_1, x_2, \cdots, x_T\} \tag{15}$$

计算注意力权重

$$\alpha_t = \frac{\exp(e_t)}{\sum_{i=1}^{T} \exp(e_i)} \tag{16}$$

其中：

$$e_t = \boldsymbol{v}^{\mathrm{T}} \tanh(W_h h_t + W_x x_t + b) \tag{17}$$

（$\boldsymbol{v}$，W_h，W_x，b）为可学习的参数。然后通过加权求和得到带有注意力的输出：

$$y = \sum_{t=1}^{T} \alpha_t x_t \tag{18}$$

这种注意力机制可以使神经网络更加关注数据中的关键部分，提高对风电场复杂数据的处理能力。

2.2.2 参数设置

（1）权重初始化[18]

对于全连接层的权重初始化，采用 Xavier 初始化方法。设全连接层的输入神经元数量为 n_{in}，输出神经元数量为 n_{out}，则权重 $\boldsymbol{W}$ 的初始化为：

$$\boldsymbol{W}_{ij} \sim U\left(-\frac{\sqrt{6}}{\sqrt{n_{\text{in}}+n_{\text{out}}}}, \frac{\sqrt{6}}{\sqrt{n_{\text{in}}+n_{\text{out}}}}\right) \tag{19}$$

其中，U（）表示均匀分布。

对于卷积层的权重初始化，根据卷积核的输入和输出通道数以及卷积核的大小来确定权重的初始化范围。例如，对于输入通道数为 C_{in}，输出通道数为 C_{out}，卷积核大小为 $k \times k$ 的卷积层，权重 $\boldsymbol{w}$ 的初始化可参考类似的均匀分布范围确定方法。

（2）学习率设置

初始学习率设为 $\alpha = 0.01$。采用学习率衰减策略，如 Adagrad 衰减方法。设 g_t 为第 t 步的梯度，则学习率为：

$$\alpha_t = \frac{\alpha}{\sqrt{\sum_{i=1}^{t} g_i^2}} \tag{20}$$

这种衰减策略可以根据梯度的变化动态调整学习率，使模型在训练过程中更快地收敛。

（3）批处理大小（Batch Size）

根据风电场监控数据的规模和计算资源，初始设置批处理大小为 64。如果在训练过程中发现内存占用过高或者收敛速度过慢，可以适当调整批处理大小。例如，当出现内存不足时，可以减小批处理大小为 32；当收敛速度过慢时，可以尝试增大批处理大小为 128。

2.3 监控算法与实现

2.3.1 基于神经网络的网络安全监控算法

（1）数据输入与特征编码

将经过预处理的风电场监控数据输入到设计好的神经网络模型中。对于不同类型的数据（风机运行状态数据、气象数据、电网连接数据），按照模型输入层的要求进行编码。例如，对于分类特征（如风机的运行状态类别），可以采用独热编码（One-Hot Encoding）的方式。设风机运行状态有 n 种类型，某一时刻的运行状态为第 i 种类型，则对应的独热编码向量为：$\boldsymbol{v} = [0, \cdots, 1, \cdots, 0]$，其中第 i 个元素为 1，其余为 0。

对于数值型数据（如风机转速、功率等），直接将标准化后的数据输入到模型中。在神经网络内部，通过卷积层、全连接层等操作逐步提取数据的特征。对于融合结构中的 CNN 部分，卷积层通过卷积核与输入数据进行卷积操作，提取局部特征，如对于风机功率数据的时间序列，卷积层可以提取不同时间段内功率变化的特征模式。

（2）攻击检测与分类

在神经网络的输出层，根据输出的概率值来判断是否存在网络攻击以及攻击的类型。设输出层的概率向量为：

$$\boldsymbol{y} = [y_1, y_2, \cdots, y_k] \tag{21}$$

其中，k 为攻击类型的数量（包括正常状态，即 y_1 可能表示正常状态的概率）。如果 y_i（$i \neq 1$）大于某个设定的阈值 θ，例如 $\theta = 0.5$，则判定为存在第 i 种类型的网络攻击。

对于攻击程度的评估，可以进一步根据输出概率的大小进行量化。例如，概率值越高，表示攻击的可能性越大或者攻击的严重程度越高。同时，可以结合多轮次的检测结果进行综合判断，以提高检测的准确性。

（3）异常行为分析与预警

除了直接的攻击检测与分类，神经网络还可以对风电场数据中的异常行为进行分析。通过分析数据在神经网络中的隐藏层表示，可以发现数据中的异常模式。设某一隐藏层的输出为 $\boldsymbol{h} = [h_1, h_2, \cdots, h_m]$，计算样本与正常样本在隐藏层表示上的距离（如欧几里得距离）。设正常样本的隐藏层表示均值为 μ_h，标准差为 σ_h，对于待检测样本的隐藏层表示为 h，计算距离：

$$d = \sqrt{\sum_{i=1}^{m} (h_i - \mu_h)^2} \tag{22}$$

如果 d 大于某个阈值 δ（δ 根据正常样本的统计信息确定），则判定为存在异常行为，并发出预警信号。

2.3.2 实现过程

（1）训练阶段

数据划分：将标注好的风电场监控数据划分为训练集、验证集和测试集[19]。一般按照 7 ∶ 2 ∶ 1 的比例进行划分。

模型初始化：按照前面设计的神经网络结构进行模型初始化，包括确定网络的层数、神经元数量、权重初始化等操作。

训练循环：将训练集数据按照设定的批处理大小分批输入到神经网络中。对于每一批数据，计算模型的输出和损失函数。设预测输出为 $\hat{y}$，真实标签为 y，采用交叉熵损失函数：

$$L = -\sum_{i=1}^{n} y_i \log(\hat{y}_i) \tag{23}$$

根据损失函数，计算梯度并使用 Adam 优化算法更新模型的权重。在每个训练轮次（epoch）结束后，计算验证集上的损失函数和准确率等评估指标。准确率表示为：

$$P = \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FP}} \tag{24}$$

其中，TP 为真阳性（预测为正例且实际为正例的数量），FP 为假阳性（预测为正例但实际为负例的数量）。

模型调整：根据验证集的性能指标，如当验证集上的损失函数不再下降或者准确率不再提高时，采用早停法停止训练。同时，根据验证集的结果调整模型的超参数，如学习率、正则化系数等。如果验证集上出现过拟合现象（例如验证集损失函数开始上升而训练集损失函数继续下降），可以增加正则化强度或者调整 Dropout 概率。

（2）测试阶段

将测试集数据输入到训练好的模型中，计算模型在测试集上的性能指标[20]，如准确率、召回率、$F1$-score 等。召回率表示为：

$$R = \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FN}} \tag{25}$$

其中，FN 为假阴性（预测为负例但实际为正例的数量）。

$$F1\text{-score} = \frac{2PR}{P + R} \tag{26}$$

根据测试结果评估模型的有效性。如果模型性能不理想，可分析数据预处理是否充分、模型结构是否合适等。如果是数据预处理问题，可以重新调整数据清洗、标准化、特征提取等步骤；如果是模型结构问题，可以尝试调整神经网络的层数、神经元数量、激活函数等，然后重新进行训练和测试。

（3）监控阶段

在风电场的实际运行中，将实时采集和预处理后的监控数据输入到训练好的神经网络模型中。模型输出网络攻击检测结果、异常行为分析结果等。根据这些结果采取相应的措施。例如，如果检测到网络攻击，根据攻击类型采取相应的防御策略，如切断受攻击设备的网络连接、启动防火墙的特定规则等；如果发现异常行为但未确定为攻击，则进一步进行分析或者加强对相关设备的监控。同时，记录监控结果，用于后续的数据分析和模型优化。

3 实验设计与结果分析

3.1 实验设计

3.1.1 数据集准备

（1）数据来源与采集

从某大型风电场采集了为期一年（2023 年 1 月 ~ 2023 年 12 月）的监控数据。其中，风机运行状态数据每 10 min 采集一次，包括转速、功率、温度等数据；气象数据每 30 min 采集一次，包括风速、风向、温度等数据；电网连接数据每 15 min 采集一次，包括输出功率、电压、电流等数据，数据进行实时同步。总共同步到的样本数量约为 300 000 个。

同时该数据在传统监测机制中监测准确率为 43.51%，其中对于数据篡改攻击，准确率为 41.7%；对于拒绝服务攻击，准确率为 50.41%；对于恶意指令注入攻击，准确率为 33.84%；

（2）数据标注

邀请了风电场的专家对数据进行标注。将数据分为正常和网络攻击两类，其中网络攻击又细分为数据篡改

攻击（15 000 个样本）、拒绝服务攻击（10 000 个样本）和恶意指令注入攻击（5 000 个样本）。标注后的数据集按照 7 ∶ 2 ∶ 1 的比例划分为训练集、验证集和测试集。

（3）数据预处理

按照前面提到的数据预处理流程进行操作。在数据清洗中，通过统计分析发现，风机转速数据中约有 0.5% 的异常值，采用 3σ 原则进行去除；对于缺失的气象温度数据（约占 0.3%），使用线性插值法进行填补。数据标准化采用 $z-score$ 标准化方法，特征提取使用主成分分析（PCA），保留了 90% 的主成分。

3.1.2 模型参数设置与训练

（1）模型参数设置

对于多层感知机（MLP）与卷积神经网络（CNN）的融合结构模型：输入层神经元数量根据经过特征选择后的特征数量确定为 200 个。MLP 部分的第一层全连接层神经元数量 $n_1=128$，第二层全连接层神经元数量 $n_2=64$。CNN 部分的卷积层卷积核大小为 3×3，步长为 1，通道数为 16，池化层池化窗口大小为 2×2，步长为 2。输出层神经元数量为 4（正常、数据篡改攻击、拒绝服务攻击、恶意指令注入攻击）。权重初始化采用 Xavier 初始化方法，初始学习率 $\alpha=0.01$，批处理大小为 64，采用 Adagrad 学习率衰减策略。

对于递归神经网络（RNN）与注意力机制的结合结构模型：LSTM 单元的隐藏状态维度为 64。注意力机制的参数按照默认设置进行初始化。权重初始化采用 Xavier 初始化方法，初始学习率 $\alpha=0.01$，批处理大小为 64，采用 Adam 优化算法，$\beta_1=0.9$，$\beta_2=0.999$，$\varepsilon=10^{-8}$。

（2）模型训练

对于两种模型结构分别进行训练。每个模型训练 30 个轮次，在每个轮次结束后，计算验证集上的损失函数和准确率。采用早停法，如果验证集上的准确率连续 5 个轮次没有提高，则停止训练。训练数据的准确率如图 1 所示。

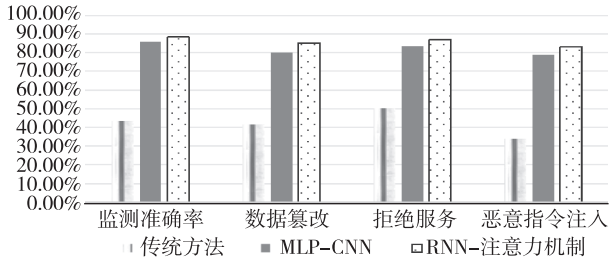

图 1 训练准确率对比图

3.2 评估结果

模型性能评估指标采取混淆矩阵进行评估。

（1）MLP-CNN 融合结构模型结果

在测试集上，模型的准确率为 85.6%。

对于数据篡改攻击，召回率为 80.2%，$F1$-score 为 82.1%；对于拒绝服务攻击，召回率为 83.5%，$F1$-score 为 84.7%；对于恶意指令注入攻击，召回率为 78.9%，$F1-score$ 为 80.3%；对于正常状态，召回率为 90.1%，$F1$-score 为 92.0%。

损失函数曲线如图 2 所示，可以看出，在训练初期，损失函数值迅速下降，在大约 15 个轮次后，损失函数值下降趋势变缓，验证集上的准确率在 20 个轮次左右达到最高，之后由于过拟合现象，准确率略有下降，触发早停法停止训练。

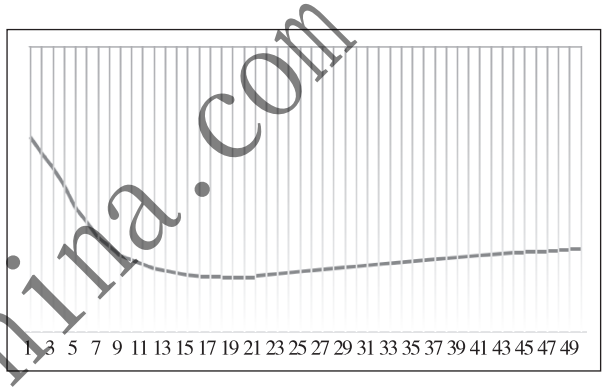

图 2 MLP-CNN 损失函数曲线

（2）RNN-注意力机制结合结构模型结果

在测试集上，模型的准确率为 88.3%。

对于数据篡改攻击，召回率为 85.1%，$F1$-score 为 86.5%；对于拒绝服务攻击，召回率为 86.8%，$F1$-score 为 87.9%；对于恶意指令注入攻击，召回率为 83.2%，$F1$-score 为 84.7%；对于正常状态，召回率为 92.5%，$F1$-score 为 93.8%。

如图 3 所示，该模型的损失函数曲线在训练过程中相对较为平滑，在 25 个轮次左右达到最优性能，验证集上的准确率和损失函数趋于稳定，训练过程中没有明显的过拟合现象。

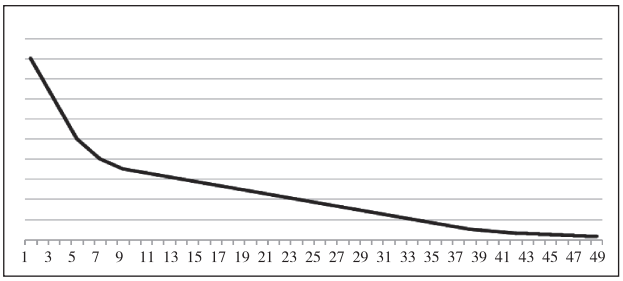

图 3 RNN-注意力机制损失函数曲线

3.3 结果分析与讨论

（1）模型比较

从准确率来看，RNN-注意力机制结合结构模型（88.3%）优于 MLP-CNN 融合结构模型（85.6%）。这是因为 RNN-注意力机制能够更好地处理风电场监控数据中的时间序列特性，尤其是风机运行状态和气象数据的时间相关性。通过图 4 能够清晰地看到 RNN-注意力机制结合结构模型优于 MLP-CNN 融合结构模型。

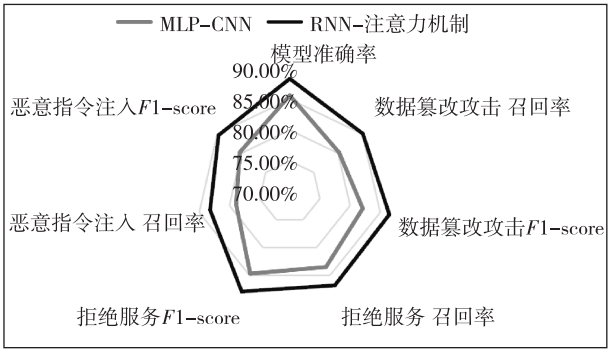

图 4 模型比较图

在召回率和 *F*1-score 方面，RNN-注意力机制结合结构模型对于各种攻击类型和正常状态的表现也普遍优于 MLP-CNN 融合结构模型。这表明 RNN-注意力机制在准确识别网络攻击和正常状态方面具有更好的性能。

（2）误差分析

对于两种模型，在恶意指令注入攻击的检测上召回率相对较低。这可能是因为恶意指令注入攻击在数据中的特征相对较为隐蔽，与正常数据的差异较小。在 MLP-CNN 融合结构模型中，出现过拟合现象，导致在后期训练轮次中准确率下降。可以考虑增加数据量、增强正则化手段（如增大正则化系数或者调整 Dropout 概率）来缓解过拟合问题。

4 结论

本研究围绕大型风电场网络攻击监控中的神经网络应用展开，构建方法与模型并进行实验分析，以应对风电场网络安全监控挑战。从数据采集到算法实现全面探索神经网络保障风电场安全运行的方式。

实验中，RNN-注意力机制结合模型在准确率、召回率和 *F*1-score 等指标上优于 MLP-CNN 融合模型，前者能更好捕捉数据时序特征与关键信息，RNN 处理时序数据有优势，注意力机制聚焦重要部分提升性能，而 MLP-CNN 融合模型在处理复杂时序和特征关系时稍弱。两种模型在恶意指令注入攻击检测上召回率低，可能因其特征隐蔽。未来可探索更深入的特征工程，如高级特征提取算法或人工构造特征；也可改进模型结构，如增加层数或调整连接方式。MLP-CNN 融合模型存在过拟合，模型训练应注重正则化，可尝试新方法，增加数据量也可缓解，如采集更多数据或采用数据增强技术。

风电场规模和智能化程度的不断提高使其网络安全问题凸显，传统网络安全监控方式越来越不能满足要求，本研究的神经网络模型和算法为其网络安全监控提供技术手段，可检测攻击和异常，保障风机等关键设备正常运行，提高发电效率和可靠性，防止电力供应被破坏，保障电力系统稳定运行，满足电力需求和能源安全要求。

参考文献

[1] 郭建英. 风电场电力监控系统安全防护的探讨 [J]. 电气技术与经济，2023（7）：300－302.

[2] 吴俊杰. 考虑网络攻击下的风电场优化调度及控制策略 [D]. 南京：南京邮电大学，2023.

[3] 宣政. 无人值守风电场区域远程监控系统设计与实现 [D]. 乌鲁木齐：新疆大学，2020.

[4] 王忠超，叶林. 风电场网络系统安全强化研究 [J]. 中国设备工程，2019（1）：172－173.

[5] 王其东，孟凯锋，朱志成，等. 风电场网络安全防护策略关键技术研究 [Z]. 北京：中能电力科技开发有限公司，2020－06－19.

[6] 史可鉴，代子阔，徐妍，等. 基于改进半不变量法的概率潮流特性分析 [J]. 控制工程，2024，31（11）：1937－1946.

[7] 杜锡力，刘友波，孙飒爽，等. 面向两个细则多考核指标的风电场配建储能联合运行策略 [J/OL]. 电网技术，1－13 [2024－11－24]. https：//doi. org/10. 13335/j. 1000－3673. pst. 2024. 1522.

[8] 黄晟，凌吉莉，魏娟，等. 大规模风电机群服役质量调控方法研究综述 [J/OL]. 电工技术学报，1－22 [2024－11－24]. https：//doi. org/10. 19595/j. cnki. 1000－6753. tces. 240793.

[9] 李晓东. 深度学习的网络安全入侵检测系统设计与实现 [J]. 信息系统工程，2024（11）：28－31.

[10] 刘珊，李瑞，王尧. 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 [J]. 电信科学，2024，40（10）：124－133.

[11] 张生成. 基于卷积神经网络的无线网络安全风险评估及控制 [J]. 中国新通信，2024，26（21）：25－27.

[12] 徐国政. 基于时间因子和复合 CNN 结构的网络安全态势评估 [J]. 网络安全技术与应用，2024（11）：36－38.

[13] 王小戈，李凯，王潇. 基于行为画像数据挖掘的异常流量监测技术 [J/OL]. 自动化技术与应用，1－6 [2024－11－24]. http：//kns. cnki. net/kcms/detail/23. 1474. TP. 20241023. 1632. 036. html.

（下转第 31 页）

配研究［J］. 中国铁路，2023（8）：106－111.
［13］董哲一，王超. 以 CPU、操作系统为核心的国内外信息技术产品生态体系现状对比分析［J］. 网络空间安全，2018，9（12）：56－62.
［14］王硕，胡现刚，杨欢，等. 多通道 10G 网络安全设备的设计与实现［J］. 网络安全与数据治理，2024，43（10）：7－13，35.
［15］朱琳，马晓妹. 等保 2.0 标准在地震信息系统的应用［J］. 网络安全技术与应用，2024（6）：133－135.

（收稿日期：2024－11－14）

作者简介：

董思秀（1996－），女，硕士，工程师，主要研究方向：地震信息网络建设、网络安全、核心系统监测。

马晓妹（1989－），女，硕士，工程师，主要研究方向：地震信息网络建设、网络运维、地震监测。

朱琳（1993－），女，硕士，工程师，主要研究方向：地震信息网络建设、信息服务、核心系统监测。

（上接第 16 页）

［14］范海菊，马锦程，李名. 基于深度神经网络的遗传算法对抗攻击［J/OL］. 河南师范大学学报（自然科学版），1－10［2024－11－24］. https：//doi. org/10. 16366/j. cnki. 1000－2367. 2023. 09. 21. 0003.
［15］杨秀璋，彭国军，刘思德，等. 面向 APT 攻击的溯源和推理研究综述［J/OL］. 软件学报，1－50［2024－11－24］. https：//doi. org/10. 13328/j. cnki. jos. 007162.
［16］刘立亮，文涛，叶磊. 基于卷积神经网络模型的电力信息系统安全状态监测［J］. 电气自动化，2024，46（5）：11－14.
［17］马鹏，傅剑锋，俞文超，等. 深度学习算法在网络安全态势感知模型中的研究与实现［J］. 信息与电脑（理论版），2024，36（16）：135－138.
［18］王刚，彭倩，段宏军，等. 基于人工智能技术的计算机网络安全防御系统的设计与实现［J］. 黑龙江科学，2024，15（18）：70－73.
［19］王勇亮，谭远波，郑学通. 基于深度学习的网络安全主动防御策略研究［J］. 工业信息安全，2024（4）：59－66.
［20］向蓉. 基于机器学习算法的电力系统故障预测与安全评估［J］. 现代工业经济和信息化，2024，14（7）：93－94.

（收稿日期：2024－12－25）

作者简介：

邱情芳（1982－），女，硕士，高级工程师，主要研究方向：风电领域安全性、新能源信息化等。

曹学铭（1988－），男，硕士，工程师，主要研究方向：风电机组控制系统、大数据分析等。

周成胜（1982－），通信作者，男，硕士，高级工程师，主要研究方向：网络安全、大数据、人工智能等。E-mail：zhouchengsheng@ caict. ac. cn。

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部