DOI: 10.19666/j.rlfd.202401014

# 基于 CNN-LSTM-Attention 的工业控制系统网络入侵检测方法研究

李　笛，杨　东，王文庆，邓楠轶，刘鹏飞，崔逸群，刘超飞，朱博迪
（西安热工研究院有限公司，陕西　西安　710054）

［摘　　要］随着各类网络攻击事件的增加，能源电力基础设施中工业控制系统安全问题也逐渐成为人们关注的焦点。结合电力系统的特点，提出一种融合卷积神经网络（convolutional neural network，CNN）、长短时记忆（long short-term memory，LSTM）神经网络和注意力（Attention）机制的 CNN-LSTM-Attention 网络入侵检测算法模型，通过在实验室仿真环境中构造和采集 600 MW 燃煤机组制粉系统在 3 种典型工况下受到网络攻击的运行状态数据集，对所提出的检测算法模型进行训练和评估。结果表明：相较于 CNN、LSTM 模型，所提出的入侵检测算法模型性能最优；模型准确率、精确率、召回率等评级指标均为最好，综合评价优于其他的入侵检测方法。该入侵检测算法模型具有较强的创新性和实用性。

［关　键　词］工业控制系统；网络入侵检测；CNN；LSTM 神经网络；注意力机制

［引用本文格式］李笛，杨东，王文庆，等. 基于 CNN-LSTM-Attention 的工业控制系统网络入侵检测方法研究[J]. 热力发电，2024, 53(5): 115-121.　LI Di, YANG Dong, WANG Wenqing, et al. Research on network intrusion detection method for industrial control system based on CNN-LSTM-Attention[J]. Thermal Power Generation, 2024, 53(5): 115-121.

# Research on network intrusion detection method for industrial control system based on CNN-LSTM-Attention

LI Di, YANG Dong, WANG Wenqing, DENG Nanyi, LIU Pengfei, CUI Yiqun, LIU Chaofei, ZHU Bodi
(Xi'an Thermal Power Research Institute Co., Ltd., Xi'an 710054, China)

**Abstract:** With the increase of various types of cyber-attacks, the security of industrial control systems in energy and power infrastructures has gradually become a focus of attention. Combined with the characteristics of power system, the CNN-LSTM-Attention network intrusion detection algorithm model integrating convolutional neural network (CNN), long and short-term memory (LSTM) neural network and Attention mechanism is proposed. By constructing and collecting the operating state data sets of the pulverizing system of a 600 MW coal-fired unit under three typical operating conditions under cyber-attacks in a laboratory simulation environment, the proposed detection algorithm model is trained and evaluated. The results show that, the proposed intrusion detection algorithm model has the best performance compared with the CNN and LSTM models. The model has the best rating indexes such as accuracy, precision, recall, etc., and the comprehensive evaluation is better than other intrusion detection methods. The intrusion detection algorithm model is highly innovative and practical.

**Key words:** industrial control system; network intrusion detection; CNN; LSTM neural network; attention mechanism

工业控制系统（工控系统）是工业生产中各种控制系统的总称[1-2]。随着信息化技术的日益发展，工控系统中应用了越来越多的网络和通信技术，这也打破了工控系统原本相对独立封闭的状态，从德

收 稿 日 期：2024-01-29　网络首发日期：2024-03-29
基 金 项 目：中国华能集团有限公司总部科技项目（HNKJ21-H48）
Supported by：Science and Technology Project of China Huaneng Group Co., Ltd. (HNKJ21-H48)
第一作者简介：李笛(1994)，男，硕士研究生，主要研究方向为网络安全与信息安全，lidi@tpri.com.cn。

国倡导的“工业 4.0”到中国实施的“中国制造 2025”战略，都加速了其对外开放的进程，由此产生的网络威胁逐渐升级。因此，工控系统的网络安全面临着日益严重的挑战[3-7]。近年来，工控系统频繁发生重大网络安全事故：2011 年“震网”病毒攻击伊朗布什尔核电站[8]；2015 年 Black Energy 病毒攻击乌克兰电力部门[9]；2022 年德国风电整机制造商 Enercon 受到网络攻击[10]。这些攻击行为主要针对电力等关键基础设施，给社会造成了严重的危害。网络入侵检测技术通过实时监视和分析系统中网络通信行为，能够探测出潜在的攻击行为，及时进行报警，为进一步拦截和系统恢复工作提供关键支持。网络入侵检测技术具有实时性和主动性等优势，已经逐步成为工控系统网络安全研究的热点之一，具有重要的现实意义和应用价值。

根据检测数据的来源和性质，网络入侵检测技术可分为基于网络流量的入侵检测方法和基于设备状态的入侵检测方法 2 类[11]。基于网络流量的入侵检测方法主要用于实时监测网络流量包，以识别潜在网络攻击[12-15]。而基于设备状态的入侵检测方法则专注于分析设备的当前状态和属性，包括登录状态、操作变量、输出变量及设备的运行状态[16-19]。本文提出了一种基于设备状态的入侵检测模型，该模型融合了卷积神经网络（convolutional neural network，CNN）、长短时记忆（long short-term memory，LSTM）神经网络和注意力机制[20]等方法的优点，旨在提高入侵检测的性能，进而提升工控系统的网络安全防护能力。

# 1 模型构建

## 1.1 卷积神经网络

CNN 是一种广泛应用的深度学习模型，主要用于图像识别、计算机视觉等领域。CNN 模型由卷积层、池化层以及全连接层组成。其中卷积层进行特征提取；池化层进行特征信息约简，防止过拟合；全连接层进行权重加总，用来输出结果。这些层次化的结构使得 CNN 模型在空间特征提取上表现出色，进而可以使用其空间特征信息进行识别分类。

## 1.2 长短时记忆神经网络

LSTM 神经网络是一种特殊的循环神经网络（recurrent neural network，RNN），其独特之处在于它能够长时间地保持短期记忆[21]。LSTM 神经网络通过调整信息传递方式，能够保持需要长期记忆的信息，同时抑制无关紧要的信息，因此擅长处理时间序列中间隔较长的重要事件。相较于传统 RNN，LSTM 模型引入了遗忘门、输入门和输出门等机制，这些结构使得 LSTM 神经网络可以更好地捕捉和建模时序数据中的长期依赖关系，提取出多维时序数据中的时间特征信息。图 1 为 LSTM 神经网络的内部结构。

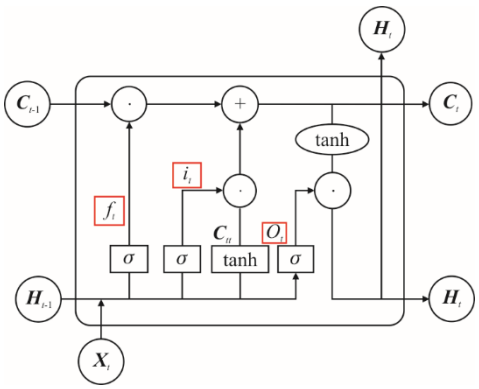


**图 1 LSTM 神经网络内部结构**

**Fig.1 Internal structure of the LSTM neural network**

图 1 中，遗忘门的输出 $f_t$ 是一个位于 0~1 的数值，用于表示对 $t$–1 时刻临时单元记忆状态 $\boldsymbol{C}_{t\text{-}1}$ 中信息的保留或丢弃。

$$f_t=\sigma(\boldsymbol{W}_{\mathrm{f}}\cdot[\boldsymbol{H}_{t\text{-}1},\boldsymbol{X}_t]+\boldsymbol{b}_{\mathrm{f}}) \tag{1}$$

式中：$f_t$ 为遗忘门；$\sigma$ 为 Sigmoid 函数；$\boldsymbol{W}_{\mathrm{f}}$ 为遗忘门权重；$\boldsymbol{b}_{\mathrm{f}}$ 为偏置系数；$\boldsymbol{H}_{t\text{-}1}$ 为 $t$-1 时刻的输出；$\boldsymbol{X}_t$ 为 $t$ 时刻的输入。

输入门决定输入 $\boldsymbol{X}_t$ 有多少进入当前的 $\boldsymbol{C}_t$ 中。

$$i_t=\sigma(\boldsymbol{W}_{\mathrm{i}}\cdot[\boldsymbol{H}_{t\text{-}1},\boldsymbol{X}_t]+\boldsymbol{b}_{\mathrm{i}}) \tag{2}$$

$$\boldsymbol{C}_{\mathrm{tt}}=\tanh(\boldsymbol{W}_{\mathrm{c}}\cdot[\boldsymbol{H}_{t\text{-}1},\boldsymbol{X}_t]+\boldsymbol{b}_{\mathrm{c}}) \tag{3}$$

$$\boldsymbol{C}_t=f_t\cdot\boldsymbol{C}_{t\text{-}1}+i_t\cdot\boldsymbol{C}_{\mathrm{tt}} \tag{4}$$

式中：$i_t$ 为输入门；$\boldsymbol{W}_{\mathrm{i}}$ 为输入门权重；$\boldsymbol{b}_{\mathrm{i}}$ 为偏置系数；$\boldsymbol{C}_{\mathrm{tt}}$ 为 $t$ 时刻更新的信息；tanh 为双曲正切激活函数；$\boldsymbol{W}_{\mathrm{c}}$ 为临时单元权重；$\boldsymbol{b}_{\mathrm{c}}$ 为偏置系数；$\boldsymbol{C}_t$ 为 $t$ 时刻临时单元记忆状态。

输出门决定输出隐藏信息内容。

$$o_t=\sigma(\boldsymbol{W}_{\mathrm{o}}\cdot[\boldsymbol{H}_{t\text{-}1},\boldsymbol{X}_t]+\boldsymbol{b}_{\mathrm{o}}) \tag{5}$$

$$\boldsymbol{H}_t=o_t\cdot\tanh(\boldsymbol{C}_t) \tag{6}$$

式中：$o_t$ 为输出门；$\boldsymbol{W}_{\mathrm{o}}$ 为输出门权重；$\boldsymbol{b}_{\mathrm{o}}$ 为偏置系数；$\boldsymbol{H}_t$ 为 $t$ 时刻的输出。

RNN 结构中的“全连接乘法”操作被 LSTM 模型中的“乘加结合”所替代，从而成功地解决了长序列训练中出现的梯度消失和梯度爆炸问题[22]。

## 1.3 注意力机制

注意力机制（attention mechanism）是深度学习

领域广泛运用的技术，适用于自然语言处理和序列数据处理等。该技术的主要目标是模拟人类的关注机制，以便在处理输入数据时使模型更集中于与任务相关的部分，从而提高性能和泛化能力。注意力机制先对查询向量与键向量进行相似性度量，再进行缩放标准化，最后将权重与值向量进行加权，其计算过程如式(7)所示。

$$\text{Attention}(\boldsymbol{Q},\boldsymbol{K},\boldsymbol{V})=\text{softmax}\left(\frac{\boldsymbol{Q}\boldsymbol{K}^{\mathrm{T}}}{\sqrt{d_{\mathrm{k}}}}\right)\boldsymbol{V} \tag{7}$$

式中：$\boldsymbol{Q}$ 为查询向量；$\boldsymbol{K}$ 为键向量；$\boldsymbol{V}$ 为值向量；$d_{\mathrm{k}}$ 为 $\boldsymbol{K}$ 向量的维度；softmax 为归一化函数。

### 1.4 CNN-LSTM-Attention 神经网络模型的构建

本文模型首先将 CNN 和 LSTM 结合，兼顾了空间信息和时间信息的提取能力，从而更全面地捕捉多维时序数据的多样性特征。在实现相近的预测性能下，采用 CNN-LSTM 连接方式的模型相对于采用 LSTM-CNN 连接方式的模型，能够显著缩短训练时间[23]。因此，本文模型采用 CNN-LSTM 结构。进一步地，在 CNN-LSTM 基础上引入了注意力机制，该机制能够赋予 CNN-LSTM 输出结果不同的权重，以更加精准地聚焦于关键信息，从而提升入侵检测性能。算法模型结构如图 2 所示。

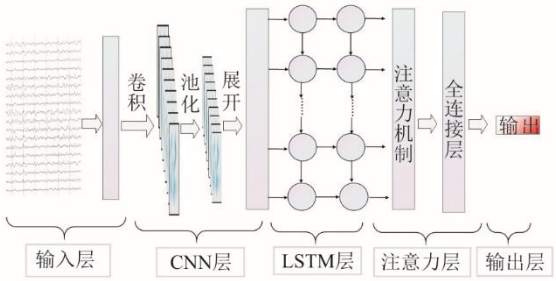


图 2 CNN-LSTM-Attention 神经网络模型
**Fig.2 The CNN-LSTM-Attention neural network model**

### 1.5 工控系统入侵检测模型流程

工控系统入侵检测模型根据多维时序数据进行预测，深入挖掘时序数据的非线性关系，并用其预测下一时刻的时序数据。所构建的入侵检测模型以工控系统历史运行数据为输入，对多维时序数据进行预处理和训练。然后，利用经过训练的模型对测试数据进行预测，以获得入侵检测模型的阈值。在线状态下，对实时获取的数据进行预处理，然后利用训练完成的模型进行预测，计算误差是否超出阈值，若超出则系统存在攻击行为；若未超出，则系统状态正常[24]。入侵检测模型流程如图 3 所示。

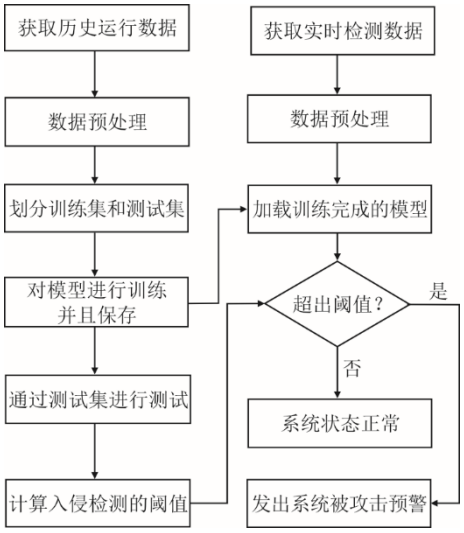


图 3 工控系统入侵检测模型流程
**Fig.3 Flow chart of the intrusion detection model for industrial control system**

## 2 数据预处理

### 2.1 数据集构造和采集

本文使用的训练数据来自 600 MW 燃煤机组的制粉系统的仿真运行系统，该机组配有 6 台磨煤机。根据工艺流程特点，选取与机组运行关联性高的 192 个典型测点，其中包含 114 个模拟量、78 个开关量。每个磨煤机组选取的测点一致，包括 19 个模拟量和 13 个开关量，A 磨煤机组部分测点信息见表 1。

表 1 测点信息
**Tab.1 Measurement point information**

| 测点 | 测点描述 | 测点类型 |
|---|---|---|
| FA01 | A 原煤仓煤位 | 模拟量 |
| FA02 | 给煤机 A 给煤量反馈 | 模拟量 |
| FA03 | 给煤机 A 电流 | 模拟量 |
| FA04 | 给煤机 A 转速 | 模拟量 |
| FA05 | 给煤机 A 进煤管电动煤闸门开状态 | 开关量 |
| FA06 | 磨煤机 A 出口气动插板门开状态 | 开关量 |
| FA07 | 磨煤机 A 出口 CO 浓度 | 模拟量 |
| FA08 | 磨煤机 A 电流 | 模拟量 |
| FA09 | 磨煤机 A 分离器电机启动 | 开关量 |
| FA10 | A 密封风管道电动挡板门开状态 | 开关量 |
| FA11 | 磨煤机 A 出入口风压差 | 模拟量 |
| FA12 | 磨煤机 A 石子煤一级阀开状态 | 开关量 |
| FA13 | 磨煤机 A 风管道气缸气动插板门开状态 | 开关量 |
| FA14 | 磨煤机 A 分离器润滑油泵电机启动 | 开关量 |

网络入侵攻击行为的模拟是通过篡改测点的状态来实现。选取的攻击测点包括进煤管电动闸门、给煤机、分离器以及气动插板门等测点如图 4 所示。

本文选取机组并网、50%负荷、100%负荷 3 种典型运行工况，用不同工况的数据集来验证本文提出的入侵检测模型的可行性、有效性、准确性。训练数据收集时间共 1 天，首先制粉系统在各个工况下运行 8 h，期间进行篡改攻击，1 次攻击持续时间为 15 min，中间间隔 15 min，攻击时间共 2 h。最终获取 86 400 组运行数据，其中攻击数据为 21 600 组，时间间隔为 1 s。

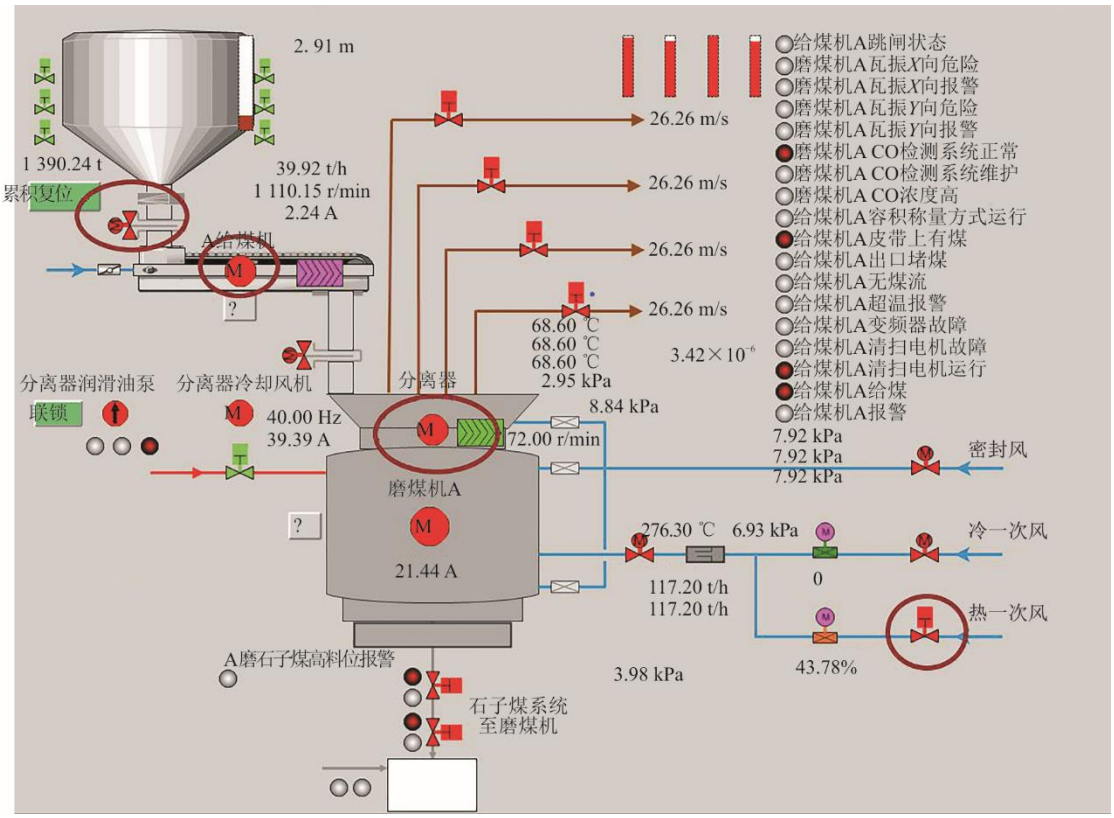


**图 4 攻击测点位置**
**Fig.4 Attack point locations**

### 2.2 特征选择及标准化处理

在数据集的预处理过程中，首要任务是进行特征选择，以提高模型性能和泛化能力。首先排除方差为 0 的特征，如 FA14（磨煤机 A 分离器润滑油泵电机启动），这些特征数值保持不变，不能为检测结果提供信息贡献；其次，进行数据相关性分析，以处理高度相关的特征对。在高度相关的特征对中，仅保留 1 个特征，以降低信息冗余。部分特征相关性如图 5 所示，图 5 展示了每个特征与其他特征之间的相关性大小，颜色越深表示相关性越高，例如 FA02（给煤机 A 给煤量反馈）和 FA04（给煤机 A 转速）相关性较高，即可保留其中一个特征。

在机组正常运行时，特征数据呈现规律的变化。然而，一旦受到篡改攻击，特征数据就会发生突变。通过具体示例说明，模拟机组 100%负荷正常运行时，A 原煤仓煤位循环缓慢减少，而磨煤机 A 出入口风压差则保持基本稳定的数值。在进煤管电动闸门测点受到篡改攻击时，A 原煤仓煤位保持不变，磨煤机 A 出入口风压差则出现剧烈波动。具体的特征数值变化如图 6 和图 7 所示，红色框表示异常的数值波动。

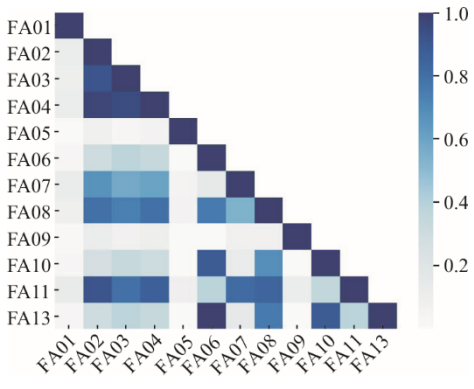


**图 5 部分特征相关性**
**Fig.5 Partial feature correlation**

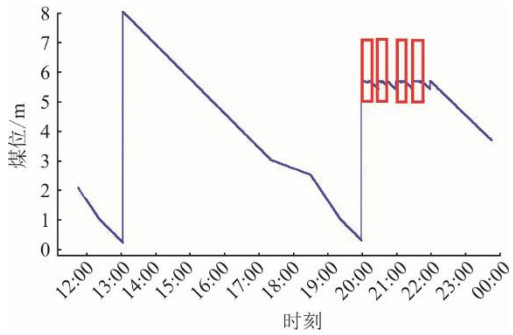


图 6　煤位数值波动
**Fig.6 Numerical fluctuations of coal level**

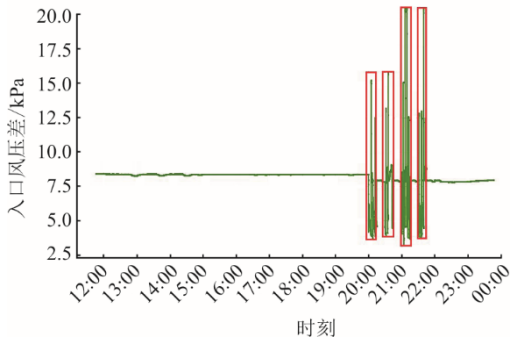


图 7　出入口风压差特征数值波动
**Fig.7 Numerical fluctuations of differential air pressure at the entrance and outlet**

基于上述规律进行特征选择，保留只与系统入侵有关而与设备本身正常运行状态无关的特征，删除那些对网络攻击不敏感的特征。特征选择后的部分特征见表 2。

表 2　关键测点信息
**Tab.2 Information of key measurement points**

| 测点 | 测点描述 | 测点类型 |
|---|---|---|
| FA01 | A 原煤仓煤位 | 模拟量 |
| FA02 | 给煤机 A 给煤量反馈 | 模拟量 |
| FA05 | 给煤机 A 进煤管电动煤闸门开状态 | 开关量 |
| FA06 | 磨煤机 A 出口气动插板门开状态 | 开关量 |
| FA08 | 磨煤机 A 电流 | 模拟量 |
| FA09 | 磨煤机 A 分离器电机启动 | 开关量 |
| FA10 | A 密封风管道电动挡板门开状态 | 开关量 |
| FA11 | 磨煤机 A 出入口风压差 | 模拟量 |
| FA13 | 磨煤机 A 风管道气缸气动插板门开状态 | 开关量 |

数据集通过特征选择后，数据维度从 192 个约简到 61 个，然后进一步进行数据标准化以便消除特征之间的尺度差异，统一量纲[25]。采用的 z-score 标准化，计算公式为：

$$y_i=\frac{x_i-\mu}{s},\qquad \mu=\frac{1}{n}\sum_{i=1}^{n}x_i,$$
$$s=\sqrt{\frac{i}{n-1}\sum_{i-1}^{n}(x_i-\mu)^2} \tag{8}$$

式中：$y_i$ 为标准化后的数据点；$x_i$ 为原始数据点；$\mu$ 为均值；$s$ 为标准差。

## 3 模型训练及评估

本文模型以滑动窗口输入多维时序数据，使用 PyTorch 深度学习框架进行模型训练，具体训练参数见表 3。在实验评估阶段，混淆矩阵是深度学习领域通用的评价标准，混淆矩阵见表 4。

为了评估算法模型，需借助一些定量评价指标，入侵检测研究常用评价指标包含准确率、精确率、召回率和 $F_1$ 等，利用混淆矩阵，这些指标具体计算如式(9)—式(12)所示。

表 3　模型参数
**Tab.3 Parameters of the model**

| 项目 | 内容 |
|---|---|
| 迭代次数 | 10 |
| 批次大小 | 32 |
| 窗口大小 | 5 |
| 优化器 | Adam |
| 学习率 | 0.001 |
| 阈值 | 5.19 |

表 4　混淆矩阵
**Tab.4 Confusion matrix**

| 真实值 | 预测值 | |
|---|---|---|
| | 攻击类 | 正常类 |
| 攻击类 | TP | FN |
| 正常类 | FP | TN |

1）准确率（Accuracy）：正常和攻击行为被正确检测出来的概率。

$$\delta_{\mathrm{ACC}}=\frac{\mathrm{TP}+\mathrm{TN}}{\mathrm{TP+FP+FN+TN}} \tag{9}$$

2）精确率（Precision）：在预测为异常攻击类型中，被正确检测的异常攻击所占比率。

$$\sigma_{\mathrm{PRE}}=\frac{\mathrm{TP}}{\mathrm{TP+FP}} \tag{10}$$

3）召回率（Recall）：攻击行为被正确检测出来的概率。

$$\sigma_{\mathrm{Recall}}=\frac{\mathrm{TP}}{\mathrm{TP+FN}} \tag{11}$$

4）$F_1$：综合召回率和精准率的综合指标。

$$F_1=\frac{2\times\sigma_{\mathrm{Recall}}\times\sigma_{\mathrm{PRE}}}{\sigma_{\mathrm{Recall}}+\sigma_{\mathrm{PRE}}} \tag{12}$$

对多层感知机（multi-layer perceptron，MLP）、CNN、LSTM 和 CNN-LSTM-Attention 等模型进行训练，获取最终训练结果。各个模型的评价指标如图 8 所示。由图 8 可见，通过对各模型的评价指标

对比分析，结果显示 MLP 模型表现明显较差，各个评价指标都是最低，其中召回率仅为 75.5%；CNN 模型和 LSTM 模型分别在不同的评价指标上取得较高的数值，如 CNN 模型的精确率为 96.9%，LSTM 模型的召回率为 98.0%；相较于其他模型，本文提出的 CNN-LSTM-Attention 模型在各项指标上均表现出色，这些指标中准确率为 99.7%，精确率为 97.5%，召回率为 99.2%，$F_1$ 为 97.7%。

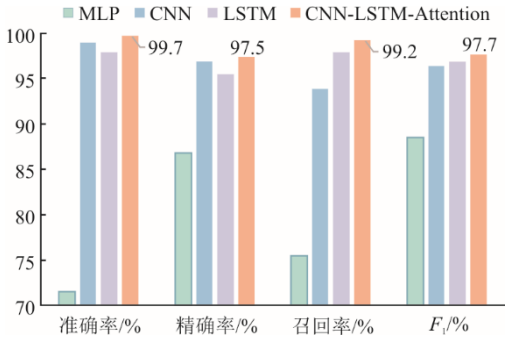


图 8 各类入侵检测模型评价指标

**Fig.8 Evaluation indexes of various intrusion detection models**

由于实际的数据集经常会出现不平衡的现象，不同阈值的选取会导致评价指标的波动，而在不同阈值下精确率-召回率曲线（precision recall curve，PRC）能够保持不变。因此 PRC 曲线更能直观体现各类入侵检测模型的优劣，其中精确率-召回率曲线下的面积（area under the precision recall curve，AUPRC）越大表明模型具备更优异的性能。图 9 为各类入侵检测模型 PRC 曲线。由图 9 可见，本文模型的 AUPRC 达到 0.997 6，表现优于 MLP、CNN 和 LSTM 模型，具有更出色的识别效果。

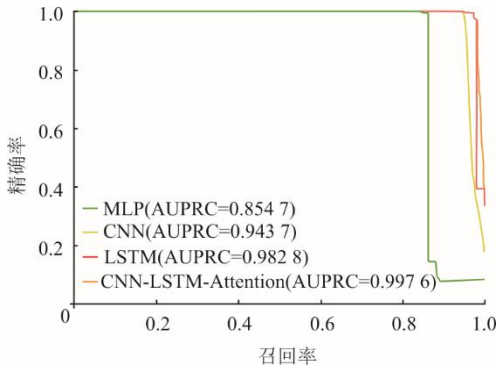


图 9 各类入侵检测模型 PRC 曲线

**Fig.9 PRC curves for various intrusion detection models**

## 4 结 论

1）通过构建 CNN-LSTM-Attention 入侵检测模型，可挖掘多维时序数据的非线性关系，并能够根据预测值和实际值的误差是否超过阈值完成对网络入侵行为的检测。

2）利用混淆矩阵，计算包含准确率、精确率、召回率和 $F_1$ 等的评价指标，更加全面和综合地评价各入侵检测模型。与 MLP、CNN、LSTM 等模型进行比较，CNN-LSTM-Attention 入侵检测模型在综合检测效果方面表现更佳。

3）CNN-LSTM-Attention 入侵检测模型具有创新性和实用性，可提升入侵检测的效率，具备及时发现潜在安全风险的能力，有助于提升工控系统的在线防护能力。

［参 考 文 献］

［1］ 张晔. 信息安全新焦点——工业控制系统安全[J]. 信息安全与通信保密, 2012(4): 46-48.
ZHANG Ye. New focus of information security-industrial control system security[J]. Information Security and Communications Privacy, 2012(4): 46-48.

［2］ 杨安, 孙利民, 王小山, 等. 工业控制系统入侵检测技术综述[J]. 计算机研究与发展, 2016, 53(9): 2039-2054.
YANG An, SUN Limin, WANG Xiaoshan, et al. Intrusion detection techniques for industrial control systems[J]. Journal of Computer Research and Development, 2016, 53(9): 2039-2054.

［3］ PENG Y, JIANG C, XIE F, et al. Industrial control system cybersecurity research[J]. Journal of Tsinghua University Science and Technology, 2012, 52(10): 1396-1408.

［4］ 傅扬. 国内外工业互联网安全态势和风险分析[J]. 信息安全研究, 2019, 5(8): 728-733.
FU Yang. Security situation and threats analysis of industrial internet in China and abroad[J]. Journal of Information Security Research, 2019, 5(8): 728-733.

［5］ 冯凯. 工业控制网络入侵检测系统的设计与实现[D]. 郑州: 郑州大学, 2018: 1-10.
FENG Kai. Design and implementation of industrial control network intrusion detection system[D]. Zhengzhou: Zhengzhou University, 2018: 1-10.

［6］ KRIAA S, PIETRE-CAMBACEDES L, BOUISSOU M, et al. A survey of approaches combining safety and security for industrial control systems[J]. Reliability Engineering & System Safety, 2015, 139: 156-178.

［7］ 赖英旭, 刘增辉, 蔡晓田, 等. 工业控制系统入侵检测研究综述[J]. 通信学报, 2017, 38(2): 143-156.
LAI Yingxu, LIU Zenghui, CAI Xiaotian, et al. Research on intrusion detection of industrial control system[J]. Journal on Communications, 2017, 38(2): 143-156.

［8］ KUSHNER D. The real story of stuxnet[J]. IEEE Spectrum, 2013, 50(3): 48-53.

［9］ 张林鹏. 电力系统恶意攻击检测关键技术研究[D]. 上海: 上海电力学院, 2018: 1-10.
ZHANG Linpeng. Research on the key technology of power system malicious attack detection[D]. Shanghai: Shanghai University of Electric Power, 2018: 1-10.

［10］ 伊娜, 徐建军, 陈月, 等. 电力CPS多阶段低代价虚假数据注入攻击方法[J]. 浙江电力, 2023, 42(11): 39-47.

YI Na, XU Jianjun, CHEN Yue, et al. A multi-stage low-cost false data injection attack method for power CPS[J]. Zhejiang Electric Power, 2023, 42(11): 39-47.

[11] 刘夏扬. 基于深度学习的工业控制系统入侵检测研究[D]. 北京: 北京石油化工学院, 2022: 1-10.
LIU Xiayang. Research on intelligent intrusion detection based on deep learning[D]. Beijing Institute of Petrochemical Technology, 2022: 1-10.

[12] 高春梅. 基于工业控制网络的流量异常检测[D]. 北京: 北京工业大学, 2014: 1-10.
GAO Chunmei. Network traffic anomaly detection based on industrial control network[D]. Beijing: Beijing University of Technology, 2014: 1-10.

[13] 王楠. 木马和僵尸网络监测平台设计与实现[D]. 天津: 天津大学, 2016: 1-10.
WANG Nan. Design and realization of Trojan and botnet monitoring platform[D]. Tianjin: Tianjin University, 2016: 1-10.

[14] SOODEH H, MEHRDAD A. The hybrid technique for DDoS detection with supervised learning algorithms[J]. Computer Networks, 2019, 158: 35-45.

[15] ADEPU S, MATHUR A. Distributed detection of single-stage multipoint cyber attacks in a water treatment Plant[C]//The 11th ACM Asia Conference on Computer and Communications Security (ASIACCS 2016). ACM, 2016. DOI:10.1145/2897845.2897855, 2016.

[16] 张文安, 洪榛, 朱俊威, 等. 工业控制系统网络入侵检测方法综述[J]. 控制与决策, 2019, 34(11): 2277-2288.
ZHANG Wenan, HONG Zhen, ZHU Junwei, et al. A survey of network intrusion detection methods for industrial control systems[J]. Control and Decision, 2019, 34(11): 2277-2288.

[17] 张金. 基于信息融合的挤压机状态监控系统研究[D]. 西安: 西安石油大学, 2018: 1-10.
ZHANG Jin. Research on state monitoring system for extruder based on information fusion[D]. Xi'an: Xi'an Shiyou University, 2018: 1-10.

[18] 赵华. 工业控制系统异常检测算法研究[D]. 北京: 冶金自动化研究设计院, 2013: 1-10.
ZHAO Hua. Research on anomaly detection algorithm for industrial control systems[D]. Beijing: Automation Research and Design Institute of Metallurgical Industry, 2013: 1-10.

[19] ADEPU S, MATHUR A. Distributed attack detection in a water treatment plant: method and case study[J]. IEEE Transactions on Dependable and Secure Computing, 2018, 18(1): 86-99.

[20] VASWANI A, SHAZEER N, PARMAR N, et al. Attention is all you need[C]//31st Conference on Neural Information Processing Systems(NIPS 2017), Long Beach, CA, USA, 2017.

[21] 王洪亮, 穆龙新, 时付更, 等. 基于循环神经网络的油田特高含水期产量预测方法[J]. 石油勘探与开发, 2020, 47(5): 1009-1015.
WANG Hongliang, MU Longxin, SHI Fugeng, et al. Production prediction at ultra-high water cut stage via recurrent neural network[J]. Petroleum Exploration and Development, 2020, 47(5): 1009-1015.

[22] 李依尘. 面向自动问答的中学历史知识库构建[D]. 哈尔滨: 哈尔滨工业大学, 2018: 1-10.
LI Yichen. Construction of high school history knowledge base for automatic question answering[D]. Harbin: Harbin Institute of Technology, 2018: 1-10.

[23] AKSAN F, LI Y, SURESH V, et al. CNN-LSTM vs. LSTM-CNN to predict power flow direction: a case study of the high-voltage subnet of Northeast Germany[J]. Sensors, 2023, 23(2): 901.

[24] 赵征, 丁建平. 基于深度双向门控循环神经网络的制粉系统故障预警[J]. 动力工程学报, 2023, 43(5): 598-605.
ZHAO Zheng, DING Jianping. Fault warning of pulverizing system based on deep bidirectional gated recurrent neural network[J]. Journal of Chinese Society of Power Engineering, 2023, 43(5): 598-605.

[25] 刘竞妍, 张可, 王桂华. 综合评价中数据标准化方法比较研究[J]. 数字技术与应用, 2018, 36(6): 84-85.
LIU Jingyan, ZHANG Ke, WANG Guihua. Comparative study on data standardization methods in comprehensive evaluation[J]. Digital Technology & Application, 2018, 36(6): 84-85.

（责任编辑　杜亚勤）