基于 Bi-RNN 模型的工业控制系统网络入侵检测研究

黎 斌[1]
LI Bin

摘 要 因工业控制系统网络环境复杂且网络流量呈现动态变化，使得时间序列特征难以被精确捕捉，数据包大小分布的离散程度不明显，导致实时特征向量的提取过程受到影响，难以准确区分正常流量与异常流量，降低了入侵检测的准确性和效率。为此，文章提出一种基于 Bi-RNN（bidirectional recurrent neural networks）模型的工业控制系统网络入侵检测研究。采用滑动平均法预处理工业控制系统网络数据，结合时间序列数据构建网络入侵检测 Bi-RNN 模型。通过计算数据包大小的变异系数体现数据包大小分布的离散程度，定向提取异常流量特征，并将其作为实时特征向量，输入至 Bi-RNN 模型中，实现工业控制系统网络入侵检测。实验结果表明，利用 Bi-RNN 模型对工业控制系统网络入侵进行检测后，戴维森堡丁指数可稳定保持在 0.15 以下水平，最小 MAPE 仅为 0.13，检测准确性较高，说明该方法对工业控制系统网络入侵检测准确性较好，可准确地检测出入侵行为。

关键词 Bi-RNN 模型；工业控制系统；网络入侵；检测方法；异常流量特征

doi：10.3969/j.issn.1672-9528.2025.04.010

0 引言

随着信息化技术的不断提高，工业控制系统广泛应用于制造业、能源、交通运输等领域，成为国家基础设施的重要组成部分 [1]。这些系统通常基于工业以太网或现场总线等通信网络进行数据交换，实现了高度的自动化和智能化。但随着工业控制系统的网络化程度不断提高，其面临的网络安全风险也日益严峻。网络入侵、恶意代码感染等安全事件频发，给工业控制系统的安全稳定运行带来了巨大挑战。在短时间内，工业控制系统会产生大量的流量，这些流量既包含工业控制系统的正常业务流量，也可能包含攻击工业控制系统的异常流量。而工业控制系统中正常数据与异常数据分布不均，异常数据较少且具有隐蔽性，增加了工业控制系统网络入侵检测的难度。

白天毅等人 [2] 提出基于 BPMFO 算法的入侵检测方法，提取出代表网络入侵行为的特征，利用 BPMFO 算法进一步增强特征，并结合飞蛾扑火算法将入侵行为特征输入至攻击数据集中进行对比，实现入侵检测。但是两种算法结合后的复杂度较高、计算量大，可能增加特征提取的冗余程度。毛一鸣等人 [3] 提出基于麻雀搜索算法改进 LSSVM 的网络入侵检测方法，对 LSSVM 进行改进，提取异常数据的特征，并通过改进后的 LSSVM 优化控制参数设定，实现网络入侵检测。但该方法在处理大规模动态网络流量数据时不能有效提取入侵流量特征，可能导致入侵检测的性能下降。李楠等人 [4] 提出基于粒子群优化的网络入侵检测方法，利用粒子群算法对支持向量机的惩罚系数和核函数参数进行优化，对不同通信状态下入侵的网络干扰行为进行检测。但是粒子群算法可能导致在优化支持向量机的惩罚系数和核函数参数时，无法找到全局最优解，从而影响入侵检测的准确性。

双向循环神经网络（bidirectional recurrent neural networks, Bi-RNN）是一种特殊的循环神经网络（RNN）结构，结合前向和后向两个 RNN 层，能够同时考虑网络流量的前向和后向信息，从而更准确地识别出异常的网络行为。将 Bi-RNN 应用于工业控制系统网络入侵检测中，可以充分发挥其双向信息捕捉的能力，提高入侵检测的准确性。为此，本文基于 Bi-RNN 模型，对工业控制系统网络入侵检测展开研究。

1 基于 Bi-RNN 模型的工业控制系统网络入侵检测研究

1.1 工业控制系统网络数据预处理

在基于 Bi-RNN 模型的工业控制系统网络入侵检测研究中，预处理网络入侵检测环境是至关重要的环节 。这一过程的首要步骤是对原始网络流量数据进行预处理，剔除因设备故障、网络波动等非正常因素而产生的数据包 [5]。为确保数据的完整性得到准确量化，采用数据包到达率作为评估指标，

1. 广西职业技术学院 广西南宁 530226

并运用滑动平均法对数据进行平滑处理，以有效减少随机波动带来的影响。数据包到达率 $\lambda(t)$ 的计算公式为：

$$\lambda(t)=\frac{1}{\omega}\sum_{i=1}^{t}\delta(p_i) \tag{1}$$

式中：$\lambda(t)$ 表示数据包到达率；p_i 表示第 i 个数据包，当 p_i 处于有效状态时，其取值为 1，若 p_i 无效，则取值为 0；ω 表示滑动窗口的大小 [6]。

随后，为消除不同数据特征间度量单位的差异，进行数据归一化处理。利用 min-max 归一化技术，将所有数据映射到 [0,1] 的区间内。具体的归一化计算公式为：

$$\hat{x}_i=\frac{x_i-x_{\min}}{x_{\max}-x_{\min}} \tag{2}$$

式中：$\hat{x}_i$表示归一化后的数据；$x_{\min}$ 和 $x_{\max}$ 分别表示数据集中的最小值和最大值；x_i 表示原始数据。

然后，由于 Bi-RNN 模型处理的是序列数据，因此需要将清洗和归一化处理后的数据组织成时间序列的形式 [7]。这一步骤包括依据数据包的时间戳进行排序，并根据时间戳将数据切割成一系列连续的、具有固定长度的数据段（即序列）[8]。为了更全面地反映工业控制系统网络的特性，还需构建一系列统计指标体系，这些统计指标旨在捕捉网络流量的整体趋势及异常波动。以数据包传输速率为例，其计算方式为：

$$v(t)=\frac{\sum_{i=1}^{t}\lambda(t)s(p_i)}{\omega\times\Delta t}\hat{x}_i \tag{3}$$

式中：$v(t)$ 表示传输速率；$s(p_i)$ 表示第 i 个数据包的大小；Δt 表示相邻数据包之间的平均时间间隔。为了捕捉数据包大小分布的离散程度，计算数据包大小的方差 σ_s^2，公式为：

$$\sigma_s^2=\frac{1}{N}\sum_{i=1}^{N}(s_i-\mu_s)^2v(t) \tag{4}$$

式中：σ_s^2 表示数据包大小的方差；N 表示数据包的总数；μ_s 表示数据包大小的均值。

通过上述预处理步骤，网络入侵检测环境得到了有效准备 [9]。原始数据经历了清洗、归一化以及序列化处理，同时构建了能够反映工业控制系统网络特性的统计指标，为后续 Bi-RNN 模型的训练提供了高质量的输入数据 [10]。

1.2 网络入侵检测 Bi-RNN 模型构建

网络流量是动态变化的，具有随机性和不确定性。在网络流量发生变化的情况下，直接对预处理后的数据进行检测，不能保持较高的检测准确性 [11]。Bi-RNN 能够同时分析时间序列的前向和反向信息，更全面地理解序列数据中的时间依赖性，能够有效捕捉时序数据中的上下文信息，更准确地识别网络流量数据中的异常模式，有助于全面且准确地捕捉网络流量的动态变化 [12]。因此，本文基于 Bi-RNN，构建网络入侵检测模型。设时间序列数据为：

$$X=[x_{t1},x_{t2},\cdots,x_t] \tag{5}$$

式中：x_t 表示第 t 个时间步的输入特征向量。

利用 Bi-RNN 模型的结构特点，融合了前向和后向两个方向的循环神经网络层，能够有效地捕捉时间序列数据中的上下文信息。具体而言，前向 RNN 层负责从序列起始至末尾顺序传递信息，而后向 RNN 层则从序列末尾向起始传递信息 [13]。这一设计使得模型在每个时间节点上都能兼顾历史与未来数据，从而更准确地判断当前时间点的流量状况。在模型的学习阶段，采用交叉熵损失函数作为优化导向，该函数旨在精确衡量模型预测的概率分布与实际标签之间的差异程度 [14]，交叉熵损失函数的表达式为：

$$L=-\frac{1}{N}\sum_{i=1}^{N}\left[y_i\log(\hat{y}_i)+(1-y_i)\log(1-\hat{y}_i)\right]\sigma_s^2 \tag{6}$$

式中：$\hat{y}_i$表示第 i 个样本的预测概率；y_i 表示真实标签。通过最小化该损失函数，调整模型参数，以期提高其对正常及异常流量的预测精确度 [15]。

为有效捕获时间序列数据中的长期相关性，RNN 层在模型中常采用长短期记忆单元或门控循环单元等增强形式 [16]。这些增强形式引入了额外的门控机制来调控信息的流通，有效解决了传统 RNN 在处理长序列数据时面临的梯度消失或梯度爆炸难题。LSTM 单元的前向传递流程可以描述为一系列复杂的非线性操作，具体涉及输入门、遗忘门和输出门的复杂计算流程 [17]。以输入门 i_t 为例，其计算公式为：

$$i_t=\sigma\left(W_{x_i}x_t+W_{h_i}h_{t-1}+b_i\right)L \tag{7}$$

式中：W_{x_i}和W_{h_i}分别表示输入特征和上一时间步隐藏状态到输入门的权重矩阵；b_i 表示输入门的偏置项；σ 表示激活函数。类似遗忘门和输出门的计算也涉及非线性变换。

最终，在构建的网络入侵检测 Bi-RNN 模型中，输出层配置为全连接层，并通过 softmax 激活函数转换输出为概率分布形式，经 softmax 激活函数处理后的预测概率表示为：

$$\hat{y}_t=\text{softmax}(W_oh_t+b_o)i_t \tag{8}$$

式中：b_o 表示输出层的偏置项；W_o 表示隐藏状态到输出层的权重矩阵 [18]。

1.3 异常流量特征定向提取

虽然 Bi-RNN 模型可以通过比较预测概率与真实标签，准确捕捉网络流量的时间序列特征。但正常与异常流量的区分往往涉及多个方面的特征，如数据包大小、源 IP 地址分布、时间戳等 [19]。数据包离散程度可以反映网络流量的波动情况，

因此，可通过计算数据包大小的变异系数，来体现数据包大小分布的离散程度，实现异常流量特征定向提取。

为了捕捉网络流量的时间相关性，计算相邻数据包之间的时间间隔，并基于这些时间间隔构建时间序列特征[20]。通过计算时间间隔的均值 μ_t 和标准差 σ_t，量化流量变化的稳定性和波动性，从而对异常流量特征进行定向提取。均值和标准差的计算公式为：

$$\mu_t = \frac{1}{N}\sum_{i=1}^{N} t_i h_t$$
$$\sigma_t = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(t_i - \mu_t)^2} \tag{9}$$

式中：t_i 表示第 i 个数据包与前一个数据包之间的时间间隔。为了实现对异常流量关键特征的判定，可以通过计算数据包大小的变异系数 CV_t，来体现数据包大小分布的离散程度，根据离散程度判定异常流量的关键特征。变异系数的计算公式为：

$$CV_t = \frac{\sigma_t}{\mu_t} \tag{10}$$

式中：CV_t 表示数据包大小的变异系数。通过计算数据包大小的变异系数，可以得出数据包大小相对于其均值的离散程度，在外围分离的数据包，即为包含异常流量关键特征的数据包[21]。数据包大小的离散程度表示如图 1 所示。

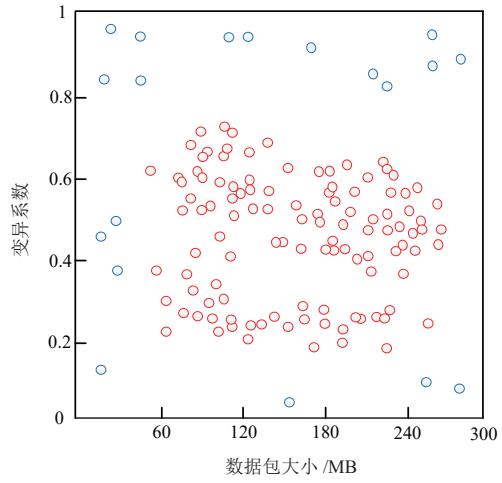

图 1 数据包大小离散程度

1.4 工业控制系统网络入侵检测

训练模型的过程实际上是让 Bi-RNN 学习正常和异常网络流量的特征模式。通过大量的训练数据，模型能够识别出正常流量的典型特征以及异常流量的独特模式。这使得模型能够在后续对实时网络流量进行检测时，准确地将流量分类为正常或异常。因此在完成异常流量特征定向提取后，将其作为实时特征向量，输入至 Bi-RNN 模型中，实现工业控制系统网络入侵检测。

在模型应用阶段，即工业控制系统网络入侵检测的实际操作中，利用训练好的 Bi-RNN 模型对实时网络流量数据进行检测。设时间序列数据为 $X=[x_{t1},x_{t2},\cdots,x_t]$，其中，$x_t$ 表示第 t 个时间步的输入特征向量这些特征向量经过与训练阶段相同的预处理和特征提取步骤后，被输入到 Bi-RNN 模型中。模型在接收到每一个时间步的实时特征向量后，会即时生成一个预测概率，该概率反映了当前网络流量属于正常或异常状态的分布情况。

为判断当前流量是否属于入侵行为，设定一个阈值 θ。当预测概率 $\hat{y}_t$ 中异常流量的概率超过阈值 θ 时，即认为当前流量存在入侵行为，触发报警机制。阈值 θ 的设定需要根据实际应用场景和模型性能进行权衡和调整。

为进一步提高检测的准确性和鲁棒性，引入滑动窗口机制。即在每个时间步上，不仅考虑当前时间步的预测概率，还考虑过去一段时间内预测概率的滑动平均值。设滑动窗口大小为 ω，则滑动平均预测概率 $\bar{\hat{y}}_t$ 表示为：

$$\bar{\hat{y}}_t = \frac{1}{\omega}\sum_{i=1}^{t} \hat{y}_i XCV_t \tag{11}$$

式中：$\bar{\hat{y}}_t$ 表示滑动平均预测概率。当滑动平均预测概率中异常流量的概率超过阈值 θ 时，同样认为当前流量存在入侵行为。

综上所述，通过利用训练好的 Bi-RNN 模型对实时网络流量数据进行预测，并设定合适的阈值和引入滑动窗口机制，最终实现对工业控制系统网络入侵的有效检测。

2 实验

2.1 实验设置

在进行基于 Bi-RNN 模型的工业控制系统网络入侵检测实验之前，准备实验所需的硬件。实验的硬件参数如表 1 所示。

表 1 实验硬件配置

序号	参数	数值
1	CPU	Core i9-12900H
2	最高主频 /GHz	2.5
3	ROM/TB	2
4	RAM/GB	16
5	操作系统	Linux

此外，对实验环境进行了必要的优化和配置，包括安装必要的软件工具、配置网络参数、设置防火墙规则等，以确保实验能够顺利进行并达到预期的效果。

网络流量模拟可以通过网络抓包工具捕获实际网络流量，并利用流量回放工具 Tcpreplay 设置具体的参数来模拟动态流量变化。设置每秒发送的数据包数量分别为 100、1 000、10 000、50 000 个，用以模拟不同时间段内

的网络繁忙程度；数据包的大小随机分布，以反映实际网络传输中不同类型数据的比例；数据包发送的时间间隔分别为 1、10、30、60、120 ms，以模拟流量的突发性和周期性变化。

KDD CUP99 数据集作为验证入侵检测方法的基准。在本文中，从 KDD CUP99 数据集中筛选出占总量 10% 的防火墙日志记录，作为实验样本集。此样本集全面覆盖了四大类入侵活动的防火墙日志，同时包含了一类表示正常无入侵状态的日志。具体而言，这四类入侵日志的记录数分别为 2 100、1 950、1 300 和 1 280 条，而正常状态的日志记录则达到了 1 400 条。这样的样本构成设计，有助于全面而准确地评估入侵检测系统的性能表现。实验环境如图 2 所示。

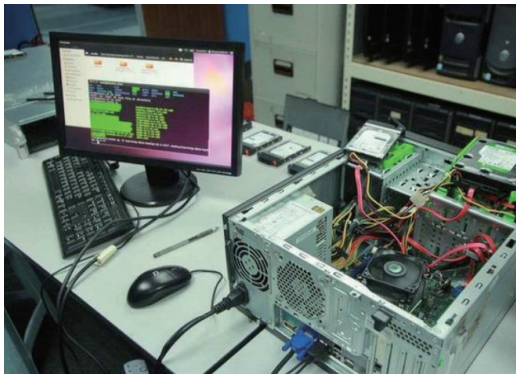

图 2 实验环境

2.2 实验结果与分析

为验证本文所提出基于 Bi-RNN 模型的工业控制系统网络入侵检测方法的应用性能，以基于 BPMFO 算法的入侵检测方法、基于改进 LSSVM 的网络入侵检测方法、基于粒子群优化的网络入侵检测方法为对比的测试方法，选择戴维森堡丁指数和平均绝对百分比误差为实验指标，与本文方法共同进行测试。

2.2.1 戴维森堡丁指数对比

戴维森堡丁指数能够直观地反映出入侵检测方法在异常流量数据分类上的准确性，其值越小，意味着簇内数据点越为紧凑，从而表明对异常流量的聚类效果越佳，能够更准确的检测出工业控制系统网络入侵。戴维森堡丁指数 ξ 的计算公式为：

$$\xi=\frac{\sum_{k=1}^{n_k}\max_{k\neq j}\left(\frac{\bar{d}_k+\bar{d}_j}{\sqrt{O_k-O_j}}\right)}{n_k} \tag{12}$$

式中：n_k 表示第 k 簇中的网络入侵实例数；O_k 和 O_j 分别表示第 k 个簇中心、第 j 个簇中心；$\bar{d}_k$和$\bar{d}_j$分别表示第 k 个簇中和第 j 个簇中样本到聚类中心的平均距离。戴维森堡丁指数对比如图 3 所示。

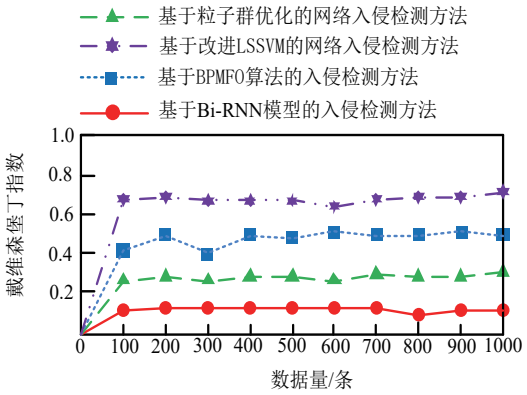

图 3 戴维森堡丁指数对比图

从图 3 可以看出，基于 BPMFO 算法的入侵检测方法获取的戴维森堡丁指数最高为 0.52；基于改进 LSSVM 的网络入侵检测方法获取的戴维森堡丁指数最高为 0.72；基于粒子群优化的网络入侵检测方法获取的戴维森堡丁指数最高为 0.32；而本文所提的入侵检测方法获取的戴维森堡丁指数最高仅为 0.11，相比之下，本文方法的戴维森堡丁指数最低，可稳定保持在 0.15 以下水平，说明该方法可有效聚类异常流量，可有效检测出工业控制系统网络入侵行为。

2.2.2 MAPE 对比

平均绝对百分比误差（mean absolute percentage error, MAPE）是评估预测准确性的一种指标。其衡量的是预测值与实际值之间差异的百分比平均值。MAPE 越小，表示该方法对工业控制系统网络入侵检测准确性越高。计算公式为：

$$\mathrm{MAPE}=\frac{100\%}{n}\sum_{t=1}^{n}\left|\frac{N_t}{M_s}\right| \tag{13}$$

式中：N_t 表示准确识别的入侵检测数据量；M_s 表示总的入侵数据测试输入量。

入侵检测 MAPE 的对比情况如图 4 所示。

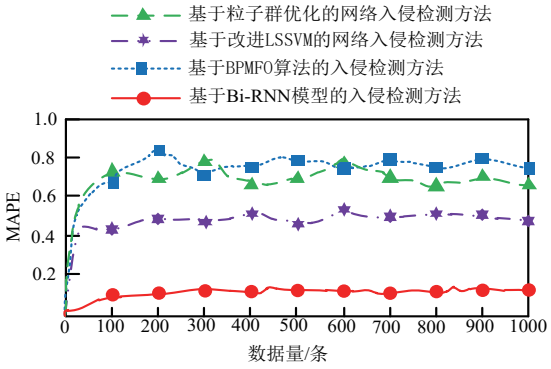

图 4 入侵检测 MAPE 对比图

从图 4 可以看出，基于 BPMFO 算法的入侵检测方法获取的最小 MAPE 为 0.68；基于改进 LSSVM 的网络入侵检测

方法获取的最小 MAPE 为 0.43；基于粒子群优化的网络入侵检测方法获取的最小 MAPE 为 0.62；而本文所提出的入侵检测方法获取的最小 MAPE 仅为 0.13，远低于对比过的其他方法，检测的平均绝对百分比误差较小，说明该方法对工业控制系统网络入侵检测准确性较高，可准确的检测出入侵行为，具有一定的实际应用价值。

3 结语

本文所研究的基于 Bi-RNN 模型的工业控制系统网络入侵检测方法，在提升工业控制系统的安全防护能力方面发挥了重要作用。不仅为工业控制系统的稳定运行提供了有力保障，也为网络安全防护技术的进一步发展提供了新的思路。然而，本文仍存在一些局限性。例如，在特征提取阶段，虽然已经提取了一系列关键特征，但可能仍有其他重要特征未被充分考虑。针对这些局限性，未来的研究可以从以下几个方向进行改进。首先，可以进一步深入研究网络流量数据的特征，挖掘更多对入侵检测有重要价值的特征。其次，可以尝试采用不同的模型参数和优化算法，以提升模型的检测性能和稳定性。最后，可以将本文方法与其他先进技术相结合，形成更加全面、高效的工业控制系统网络入侵防护体系。

参考文献：

[1] 陈虹，由雨竹，金海波，等 . 改进特征选择和 CNN-BiLSTM 的网络入侵检测方法 [J/OL]. 微电子学与计算机 :1-12[2024-10-13].http://kns.cnki.net/kcms/detail/61.1123.TN.20241104.1053.008.html.

[2] 白天毅，王建国 . 基于 BPMFO 算法的网络入侵检测研究 [J]. 信息技术 , 2024(10):188-194.

[3] 毛一鸣，程艳艳 . 麻雀搜索算法改进 LSSVM 的网络入侵检测 [J]. 太原学院学报 (自然科学版), 2024, 42(4): 64-69.

[4] 李楠，叶锦川，刘锋 . 基于粒子群优化的通信网络入侵干扰检测技术 [J]. 粘接 ,2024,51(10):189-192.

[5] 周倩如 . 基于形式化可解释人工智能的网络入侵检测方法 [J]. 智能安全 , 2024,3(3):34-44.

[6] 吴忠强，李孟亭 . 基于 CBAMTL-MobileNet V3 的车载网络入侵检测 [J]. 计量学报 ,2024,45(9):1407-1415.

[7] 李井龙，刘胜全，马宇航，等 . 融合 Transformer 和 MSCNN 双分支架构的工控网络入侵检测研究 [J]. 东北师大学报 (自然科学版), 2024, 56(3):70-78.

[8] 王心怡，行鸿彦，史怡，等 . 基于复杂网络演化博弈的无线传感器网络入侵检测方法 [J]. 电子测量与仪器学报 , 2024, 38(9): 85-94.

[9] 胡智锋，孙峙华 . 基于 Open-DNN 和 SEGAN 混合模型的工业控制系统入侵威胁检测算法研究 [J/OL]. 控制工程 :1-8[2024-09-17].https://doi.org/10.14107/j.cnki.kzgc.20240380.

[10] 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.

[11] 刘联海，黎汇业，毛冬晖 . 基于 CNN 和仿射变换技术的网络入侵检测方法 [J]. 网络安全技术与应用 ,2025(4):35-38.

[12] 史长鑫，宗学军，何戡，等 .Transformer 融合 CNN-SRU 的工业控制网络入侵检测方法 [J]. 重庆理工大学学报 (自然科学), 2025,39(3):85-92.

[13] 郭海智，贾志诚，李金库 . 基于马尔可夫判定过程的光纤网络入侵检测方法 [J]. 激光杂志 , 2025,46(3):193-198.

[14] 王继伟，张海建，霍巍 . 基于 ResNet-Att 的网络入侵检测模型研究 [J]. 铁路计算机应用 , 2025,34(3):7-11.

[15] 张跃，郭子昕，黄益彬，等 . 基于 convLSTM 的卷积神经网络的网络入侵检测方法 [J]. 计算机与现代化 , 2025(3): 119-126.

[16] 王斌 . 人工智能在网络入侵检测系统中的应用与优化策略 [J]. 中国宽带 , 2025,21(3):61-63.

[17] 秦丽娜 . 基于对抗性机器学习的网络入侵检测方法分析 [J]. 电子技术 , 2025, 54(2):192-193.

[18] 郭军 . 基于异常流量多级特征提取的网络入侵检测方法 [J]. 电脑编程技巧与维护 ,2025(1):174-176.

[19] 郭盈盈，张冬梅，李成龙 . 基于深度聚类与对比学习的网络入侵检测 [J]. 软件导刊 ,2025,24(3):119-126.

[20] 李聪聪，袁子龙，滕桂法 . 基于深度学习的时空特征融合网络入侵检测模型研究 [J]. 信息安全研究 , 2025, 11(2): 122-129.

[21] 朱悦云 . 基于深度学习的工业控制网络入侵检测系统设计 [J]. 电子技术 , 2025, 54(1):118-120.

【作者简介】

黎斌（1981—），男，广西梧州人，硕士研究生，副教授，研究方向：信息安全、网络安全、数据安全。

（收稿日期：2025-04-15）