工业控制系统安全威胁分类模型研究

万佳蓉，王　晔，张　雷，刘　奇，李春阳，周　帅
（华北计算机系统工程研究所，北京　100083）

摘　要：工业控制系统存在面临高强度持续攻击威胁的确定性，同时也存在面临未知威胁的不确定性，在识别威胁时应兼顾通用性和行业特性。基于通用网络数据集和工控专用数据集，将一维卷积神经网络和注意力机制相融合，验证模型在不同场景下的性能情况。实验表明，融合注意力机制后的一维卷积神经网络模型在通用网络数据和工控时序数据中均具有良好的特征捕捉能力，并提升了识别准确率。

关键词：工业控制系统；威胁分类；卷积神经网络；注意力机制

中图分类号：TP399　　**文献标识码：**A　　**DOI：**10. 19358/j. issn. 2097 - 1788. 2025. 09. 002

引用格式：万佳蓉，王晔，张雷，等. 工业控制系统安全威胁分类模型研究［J］. 网络安全与数据治理，2025，44（9）：8 - 14.

Research on the classification model of security threats in industrial control system

Wan Jiarong，Wang Ye，Zhang Lei，Liu Qi，Li Chunyang，Zhou Shuai
（National Computer System Engineering Research Institute of China，Beijing 100083，China）

Abstract：Industrial control systems face the certainty of high-intensity continuous attack threats，as well as the uncertainty of unknown threats. When identifying threats，consideration should be given to both generality and industry characteristics. This research is based on the general network dataset and industrial control dedicated dataset，fuses the one-dimensional convolutional neural network and attention mechanism，and verifies the performance of the model in different scenarios. Experimental results show that the one-dimensional convolutional neural network model fused with the attention mechanism has good feature capture capabilities in both general network data and industrial control time-series data，and improves the recognition accuracy.

Key words：industrial control system；threat classification；convolutional neural network；attention mechanism

0　引言

工业控制系统（Industrial Control System，ICS）关系国计民生和国家安全，广泛应用于社会经济发展的各个领域。ICS 的安全问题一直是人们关注的焦点，关键领域的 ICS 更是国家间网络攻击的重点对象，随着人们认知程度的提升，ICS 将面临更加严峻的网络威胁。

当前 ICS 威胁分类方法主要包括传统方法和深度学习方法。传统方法中，基于签名的方法通过和已知攻击特征库做比对进行威胁识别，具有识别速度快、准确率高的优势，但该方法无法应对未知威胁，且需要不断更新特征库[1]；基于异常行为的方法通过建立系统正常行为准则，识别偏离的异常行为，能够检测出未知威胁[2]，但 ICS 中设备启停、参数波动等正常行为的动态性会导致较高的误报率。

深度学习方法近年来在威胁检测领域取得显著进展，卷积神经网络（Convolutional Neural Network，CNN）广泛用于处理空间特征方面，用以提取网络流量中的局部特征；循环神经网络（Recurrent Neural Network，RNN）及其变体长短期记忆网络（LSTM）擅长处理时序数据，能够捕捉数据中的时间依赖关系[3]。然而，现有深度学习方法在工控场景中仍存在不足，如 CNN 对工控时序数据的动态变化捕捉能力有限，LSTM 在处理高维特征时计算复杂度较高，且缺乏对关键特征的重点关注。

本文针对现有方法的局限性，将注意力（Attention）机制融入神经网络模型，分别用于通用网络威胁和工控时序威胁分类，以提高威胁分类的准确性和适用性。

1　相关工作

近年来，在工控安全威胁检测领域涌现出众多研究成果。Kravchik 等人[4]基于简单轻量级神经网络和主成分分析的方法研究了一种针对 ICS 的攻击检测方法，并通过

实验验证了该方法具有一定的鲁棒性。L(y)u 等人[5]引入一种基于图神经网络（GNN）的方法实现异常检测，在准确性和效率上都有明显的提升。胡智锋等人[6]将生成对抗网络（GAN）和深度神经网络（DNN）结合，提出一种对 ICS 网络入侵威胁检测的模型，提高了检测准确率。

本文在现有研究基础上，结合 ICS 特点，在神经网络模型中引入 Attention 机制，一是引入通道注意力（Channel Attention，CA），增强关键特征权重，抑制噪声；二是引入空间注意力（Spatial Attention，SA），聚焦关键位置；三是引入时间注意力（Time Attention，TA）机制，提高对工控关键时序特征的关注度。最后通过对比实验，验证了模型在不同场景下的识别准确度。

2 ICS 信息安全与功能安全

信息安全与功能安全是 ICS 的两种安全属性，研究 ICS 安全离不开信息安全和功能安全。随着信息化、数字化和智能化的发展，原有 ICS 的孤岛模式将不断被打破，人们的关注范围由原来的功能安全逐渐引入信息安全，最终朝着“双安融合”的方向发展[7]。

2.1 ICS 信息安全与功能安全的概念

ICS 信息安全是指通过采取安全措施，保护 ICS 网络、资产和数据等免受未经授权的访问、篡改、破坏等威胁，以保证可用性、完整性、保密性为目标[8]，包括对网络设备、通信协议、访问控制、加密算法等方面的安全保护。通过建立可靠的网络架构，降低系统故障和攻击风险；对系统中的用户和设备设立严格的访问权限控制；对网络数据传输进行加密，防止在传输过程中数据被窃取或篡改；采取部署入侵检测系统和其他安全设备的措施，以及时发现和应对潜在的网络攻击。

ICS 功能安全是指通过系列措施保护 ICS 本身的功能免受系统故障、错误操作等威胁，并确保系统在正常和异常情况下都能正常运行。其与工业生产过程联系密切[9]。功能安全以保护系统可靠性和稳定性、降低导致生产事故和财产损失的可能性为目标，包括对硬件、软件、人员、操作流程等方面的安全保护。通过采用冗余设计、故障安全、单一故障、多样性等设计原则，提高系统的故障冗余能力[10]；部署安全仪表系统等实时系统来监控和控制工业过程，以保证过程的安全稳定；同时为操作人员提供明确的操作指南，确保他们在操作过程中遵循安全规程；定期对 ICS 进行维护和审计也是必不可少的工作，这有助于发现并消除潜在的安全隐患。

除信息安全和功能安全外，物理安全也会影响 ICS，它是指通过采取一些保护措施，保护系统免受自然环境和人为破坏。环境因素会间接导致系统功能受损，也应引起足够的重视。通过采取防水、防震、防火等措施降低自然环境带来的影响，在机房等重要场地部署门禁系统、视频监控系统等监控进出人员，机房内的资产及所属环境也应做到充分的保护，并配备专门人员负责和管理。

根据以上所述，可以发现信息安全和物理安全强调的是威胁主体对客体进行侵害导致系统失效，两者的威胁主要来源于系统外部，而功能安全强调系统本身缺乏足够的健壮性导致系统运行受阻，威胁主要来源于系统内部。只有将三种安全综合考量，才能全面保障 ICS 的安全。

2.2 ICS 信息安全与功能安全的联系

尽管 ICS 信息安全和功能安全各有侧重，但它们之间存在着密切的联系。首先，两者都是为了保证 ICS 的正常运行和数据安全，信息安全关注的是系统脆弱性不被外部威胁所利用，功能安全关注的是系统自身能够在正常和预期的运行环境中工作。其次，在 ICS 中，两者相互关联，一方面，若系统中的数据被非法访问或篡改，可能会导致系统运行异常，影响系统的功能安全；另一方面，若系统本身存在故障或缺陷，可能会造成数据泄露或丢失，从而影响到信息安全。再者，两者在对系统完整性要求的理念上是一致的，应相互借鉴，全面保障系统完整性的安全要求[11]。最后，相比功能安全，信息安全起步较晚，存在保护措施不充分的风险，容易造成信息安全得到保障的同时功能安全无法实现的问题，故在进行双安融合的过程中需要解决这种冲突，做到两者互相兼顾。

ICS 信息安全和功能安全侧重点不同但联系密切，无论哪种安全受到威胁，都会影响系统工作，因此在识别威胁时应该综合考虑这两方面的因素。

3 震网事件的跨域攻击机理

2010 年震网事件发生后，ICS 网络安全问题成为全球关注的焦点，也使人们意识到网络战的潜在危险，各国纷纷加强对 ICS 网络安全的投入，以防止类似的网络攻击事件再次发生。

震网事件采用了多种先进技术，利用传统网络攻击方式，通过社会工程学、系统漏洞利用、蠕虫、Rootkit 等多个手段将病毒传播到内网，在 PLC 维护期间将载荷植入 PLC 中并进行控制，最终造成大量离心机被毁[12]。在整个过程中，震网病毒跨越了信息域和物理域，巧妙地利用 PLC 控制系统这一纽带实现物理世界的损毁，是

典型的跨域攻击案例。其特点主要体现在以下几方面：

（1）漏洞利用：震网病毒利用了西门子公司 ICS 设备中的多个漏洞，包括 LNK 或 PIF 文件任意代码执行漏洞（CVE-2010-2568）、Windows Server 服务 RPC 请求远程代码执行漏洞（CVE-2008-4250）、打印机后台程序服务漏洞（CVE-2010-2729）、Siemens Simatic Wincc 与 PCS 硬编码口令权限许可和访问控制漏洞（CVE-2010-2772）等[13]，从而能够在系统中执行恶意代码并获取系统权限。

（2）传播方式：震网病毒的传播方式是通过 U 盘等移动存储设备，因此具有很强的隐蔽性和针对性。病毒可通过 U 盘自动启动并在系统中运行，同时还可以通过网络进行传播，跨越多个网络和系统。

（3）控制系统：震网病毒可以获取 ICS 的权限，并控制系统中运行的程序。病毒通过修改系统的配置和参数，从而导致系统运行异常，甚至造成系统崩溃。

（4）破坏性强：震网病毒可对 ICS 中的设备、程序和数据造成严重损坏。病毒能破坏离心机等关键设备，造成伊朗核计划推迟，严重影响了国家安全。

从震网事件可以发现，跨域攻击类事件能跨越不同的网络、系统、领域或行业，攻击者会利用多个漏洞开展攻击，因此在威胁识别和分类时需要考虑通用网络威胁和行业专用网络威胁。

4 ICS 威胁分类模型

4.1 卷积神经网络

卷积神经网络（CNN）是一种特殊的神经网络，它被广泛应用于图像识别、语音识别和自然语言处理等领域。CNN 通过局部感知、权值共享和下采样等操作，有效地提取了数据中的特征，并能够准确地识别出不同的模式。

CNN 的基本构成包括输入层、卷积层、激活层、池化层、全连接层和输出层[14]。输入层是数据进入卷积网络的位置，卷积层通过卷积操作提取特征，激活层将上层的结果做非线性映射，池化层可通过池化操作减少计算量和控制过拟合，全连接层则将特征映射到输出结果，输出层输出 CNN 处理后的最终结果。

CNN 的训练过程是通过反向传播算法来实现的，在训练过程中，CNN 会根据实际输出结果和预期输出结果之间的误差来更新卷积核和全连接层的权重[15]，以达到更好的拟合效果。

4.2 Attention 机制

注意力（Attention）机制是模拟人类关注核心信息的算法，通过给输入数据的各部分分配权重，让模型重点关注与任务相关的内容，提升模型性能和泛化能力[16]。

Attention 机制通常由以下三种方式实现：

（1）通道注意力（CA）：关注重要特征维度的筛选，通过全局池化聚合各通道信息，再经网络学习通道权重，强化关键特征通道，抑制无关通道。

（2）时间注意力（TA）：针对时序数据的动态特性，从时间维度捕捉关键事件时刻，借助神经网络提取时序特征后，对不同时间步赋予不同的注意力权重。

（3）空间注意力（SA）：关注特征图的空间位置重要性，通过分析空间上下文生成位置权重，强化物体所在区域的特征，抑制背景干扰，使模型更精准定位关键空间区域。

4.3 融合 Attention 机制的神经网络威胁分类模型

一维卷积神经网络（1D Convolutional Neural Network，1D-CNN）是 CNN 的变体，用于处理一维数据，如时间序列数据、音频信号等，与 2D-CNN 相比，1D-CNN 只有一维卷积核，用于在一维数据上滑动窗口进行卷积操作，1D-CNN 通常由多个卷积层、激活层和池化层组成。由于本文的数据为一维数据，因此采用 1D-CNN 进行模型训练和分类，并对其融入 Attention 机制以增强关键特征提取能力，聚焦重要位置，识别主要时间点。

本文建立的 Attention-1D-CNN 模型主要流程如图 1 所示，将数据集预处理成符合输入层特征的格式，经过卷积层、激活层、池化层、Attention 机制、全连接层的处理后，最终由输出层输出威胁类别。

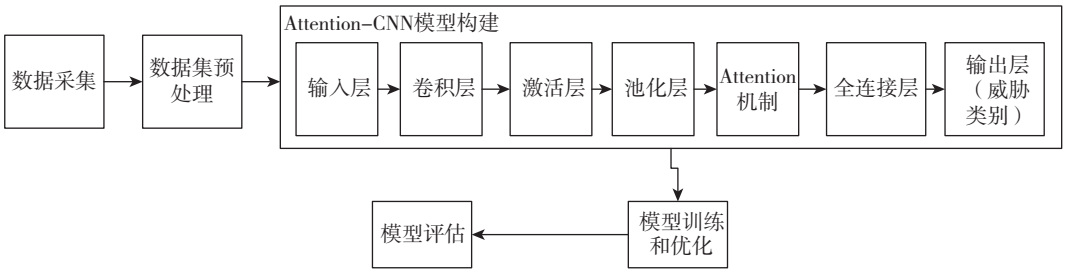

图 1 Attention-1D-CNN 模型流程图

4.3.1 数据预处理

数据预处理的目的是将数据集处理成符合模型输入结构的数据。数据集中会有一些无关特征，因此首先需要进行特征提取，提取数据中的有用信息，减少数据维度，提高模型的可解释性；其次，由于数据的格式不统一，故应将字符型特征进行数字化表示；再者，为提高模型性能和算力，将数据做归一化处理；最后，因为输入层要求为定长向量，所以应该统一每条数据的长度，同时，模型采用的是 1D-CNN，故在数据进入模型之前，应将数据平铺成符合输入层格式的一维数据，表示为 $[M, n, 1]$，其中 M 为样本数，n 为特征维度数，1 为通道数。

4.3.2 Attention-1D-CNN 模型构建

在构建的 Attention-1D-CNN 模型中，经过预处理后的一维数据向量进入输入层，经过卷积层的一维卷积操作得到局部特征值，然后在激活层中加入 ReLU 函数以缓解模型的过拟合情况，再经池化层做最大池化，经过多次卷积层、激活层、池化层处理后，融入 Attention 机制进行关键特征筛选，后进入全连接层，该层规定分类的类别数，最终由输出层输出分类结果。输出向量中对应概率最大的即为该条数据的威胁类别。

模型采用两次卷积操作，以增强对网络特征的多层次提取。模型构建如算法 1 所示。

算法 1　Attention-1D-CNN 模型构建算法

输入：预处理后一维数据向量 a
输出：威胁分类结果 s

```
//定义参数
n = 特征维度数
p = 威胁类别数
M = 样本数
//输入层
input_layer = Input（shape = （M, n, 1））
//第一次卷积
x = Conv1D（filters = 64, kernel_size = 3, padding = 'same', activation = 'relu'）（input_layer）
x = MaxPooling1D（pool_size = 2）（x）
//CA 机制
x = channel_attention（x）
//第二次卷积
x = Conv1D（filters = 128, kernel_size = 3, padding = 'same', activation = 'relu'）（input_layer）
x = MaxPooling1D（pool_size = 2）（x）
//SA 机制
x = spatial_attention（x）
//TA 机制
x_tem = temporal_attention（x）
//全连接层
x = Dense（128, activation = 'relu'）（x）
//分类输出层
output = Dense（p, activation = 'softmax'）（x）
return output
```

4.3.3 模型评估

对模型进行训练，然后采用测试集和验证集来评估模型，并通过评估结果对模型继续优化，包括调整参数、选择更合适的特征提取方法、使用更多的训练数据等，以提高模型整体的性能和识别准确率。

对模型的评估指标通常包括：准确率（Accuracy）、精确率（Precision）、召回率（Recall）、$F1$ 分数（$F1$_Score）、损失函数（Loss Function）、混淆矩阵（Confusion Matrix）。各指标的具体定义为：

（1）准确率：表示所有预测中预测正确的概率，即模型正确分类的比例，是分类任务中衡量模型性能的直观指标；

（2）精确率：衡量模型预测正例的准确程度，即被模型预测为正类的样本中实际为正类的比例；

（3）召回率：衡量模型找出所有正例的能力，即所有实际为正类的样本中被模型正确识别为正类的比例；

（4）$F1$ 分数：精确率和召回率的调和平均数，综合考虑了模型的预测精度和覆盖率，在类别分布不平衡时更加有效；

（5）损失函数：也称为代价函数，用于计算模型对单个样本的预测值与真实值之间的差异或误差；

（6）混淆矩阵：是一个 $N \times N$ 的表格（N 代表类别数），在分类任务中，展示模型预测结果与真实标签的对比。

4.4 模型验证

4.4.1 实验环境和数据集

实验运行环境：Windows 11 专业版，Intel（R）Core（TM）i5-10210U CPU@1.60 GHz 2.11 GHz，24 GB RAM，使用 Python 编程语言。

Attention-1D-CNN 模型验证采用的数据集为 KDD CUP99。KDD CUP99 数据集是一个通用网络入侵检测数据集，包含正常流量和攻击流量，其中攻击流量共分为 4 大类 39 小类（22 类在训练集中，17 类未知攻击类型在测试集中），包含 41 维特征。

4.4.2 实验过程

（1）预处理

由于 KDD CUP99 数据集包含了正常流量和异常流

量，而本文的威胁模型需要异常流量，因此首先进行初步筛选，将异常流量组成新的数据集；其次，数据集中含有一些字符型数据，故要将其数值化和标准化处理，对类别进行独热编码。

（2）模型构建和训练

将数据集的 70% 作为训练集，30% 作为测试集，并选用测试集中的 20% 作为验证集。预处理后进入 Attention-1D-CNN 模型训练，进行两次卷积，其中特征维度数 n 取 41，本文中模型采用的是 Adam 梯度下降算法，并通过设置早停机制来降低训练轮数。实验参数设置如表 1 所示。参数选择说明如下：

①第一层卷积选择中等数量的 64 个卷积核，能够捕获基础特征模式，避免过度拟合，第二层卷积选择 128 个卷积核，可学习更复杂的组合特征。

②卷积核大小选择 3，是为了捕捉更局部的特征，减少参数量。

③池化窗口选择 2，是为了在减少数据维度的同时尽可能保留有用信息，用于降低特征维度。

④通道注意力压缩比为 8，能平衡信息保留与计算效率，也符合 KDD CUP99 数据集的特点；空间注意力卷积核为 7，能确保对称填充，并且覆盖典型的关联范围；时间注意力选择 64 个单元，可避免过多单元的过拟合、过少单元的捕获不全问题。

⑤全连接层作为分类层之前的特征压缩层，神经元个数选择 128 可保留足够的信息量，同时避免维度灾难。

⑥训练批次选择 128，是为了平衡梯度稳定性和训练速度。

表 1　Attention-1D-CNN 实验参数表

模型架构参数名称	参数值
卷积核个数	64，128
卷积核大小	3
池化窗口	2
通道注意力	压缩比为 8
空间注意力	7×1 个卷积核
时间注意力	64 个单元
全连接层神经元个数	128
训练参数名称	参数值
批次大小	128
初始学习率	0. 001
训练轮次	20
早停机制	5
Dropout 率	0. 5

⑦初始学习率 0. 001 是深度学习领域的标准初始学习率。

⑧训练轮次依据多次实验以及早停机制（设为 5，即验证损失 5 轮后不再下降即停止训练）设为 20。

⑨Dropout 用在分类之前，0. 5 是常用数值，可有效防止过拟合。

4. 4. 3　结果分析

模型的性能采用准确率 A、精确率 P、召回率 R、$F1\_Score$、损失函数、混淆矩阵来评价，其中前四个评价指标的公式见式（1）~式(4)。

$$A = \frac{TP + TN}{TP + TN + FN + FP} \tag{1}$$

$$P = \frac{TP}{TP + FP} \tag{2}$$

$$R = \frac{TP}{TP + FN} \tag{3}$$

$$F1\_Score = 2 \times \frac{P \times R}{P + R} \tag{4}$$

其中，TP 表示识别为正的正样本数量，FP 表示识别为正的负样本数量，FN 表示识别为负的正样本数量，TN 表示识别为负的负样本数量。

图 2 展示的是模型准确率趋势，图 3 展示的是损失趋势，图 4 展示了混淆矩阵。

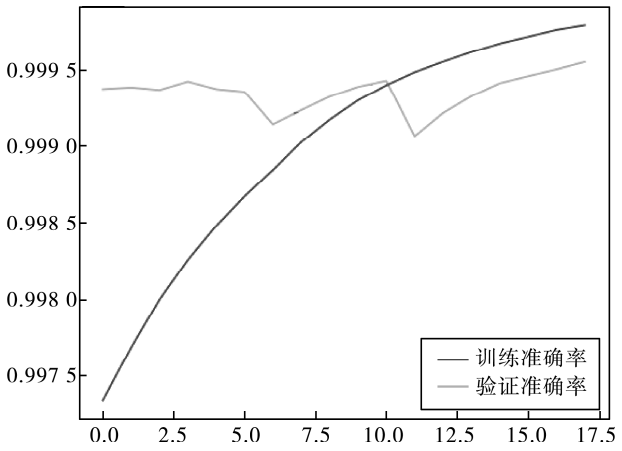

图 2　模型训练和验证准确率（平滑后）

由图 2 和图 3 可以看出，随着迭代次数的增加，准确率逐渐逼近 100%，损失值逐渐逼近 0。从图 4 的混淆矩阵也可以看出本文模型的分类具有良好的效果。

将该模型与 1D-CNN、随机森林、支持向量机、多层感知机算法进行实验对比，准确率、精确率、召回率和 $F1\_Score$ 具体数据见表 2。可以看出，相较而言，融入 Attention 机制的 1D-CNN 算法识别率最高。

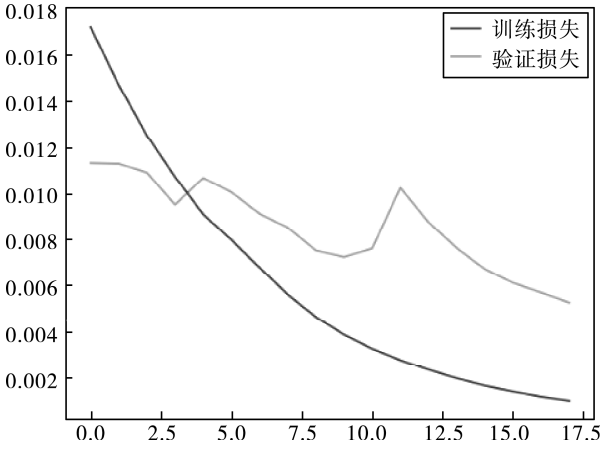

图 3　模型训练和验证损失（平滑后）

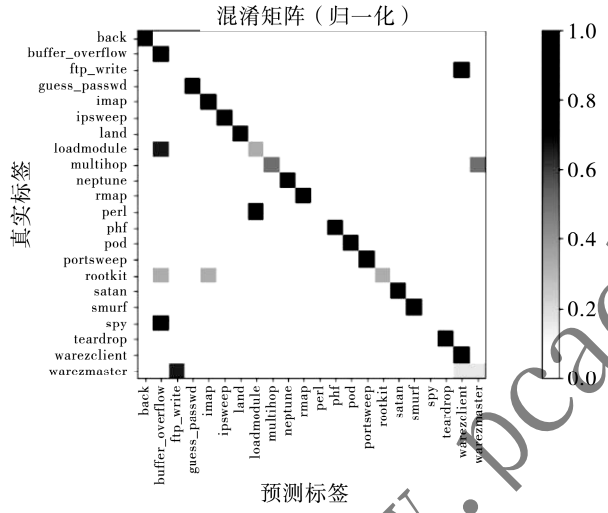

图 4　混淆矩阵

表 2　实验评价指标结果

模型	*A*/%	*P*/%	*R*/%	*F*1_Score/%
Attention-1D-CNN 模型	99.98	99.94	99.98	99.97
1D-CNN	99.94	99.94	99.94	99.94
随机森林	99.95	99.95	99.95	99.95
支持向量机	99.93	99.97	99.89	99.93
多层感知机	99.96	99.97	99.91	99.94

4.4.4　ICS 场景模型验证

为验证模型在 ICS 中的准确度，需要使用工控专用数据集进行模型训练，此数据集应集合信息安全数据和功能安全数据，故选取密西西比州立大学工控入侵检测数据集 Gas pipeline 进行训练。Gas pipeline 数据集是工控专用数据集，数据来自于串口数据记录仪捕获的气体管道装置的 ICS 网络流量，包含网络流量特征（提取自 Modbus 协议字段，如命令/响应设备地址、内存地址）和有效载荷内容特征（如测量值、电磁阀状态等），共 26 维特征，包括正常数据和 7 类攻击数据[17]。

在工控场景中，设备运行参数的时序波动是威胁识别的重要特征，模型中融入了 TA 机制，使用双向长短期记忆网络（Bi-directional Long Short-Term Memory，BiLSTM），因此适用于分析 Gas pipeline 数据中的时序信息。

对数据集进行标签和文本字符编码，并标准处理，将预处理完毕的数据输入到模型中进行训练和评估。为符合该数据集的维度特点，将 CA 中的压缩比设为 5，训练轮次设为 50。图 5 和图 6 给出了准确率和损失趋势图，表 3 给出了实验指标结果。

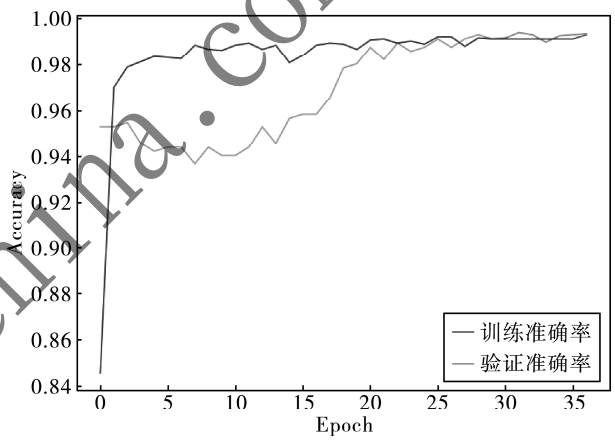

图 5　工控数据集训练和验证准确率

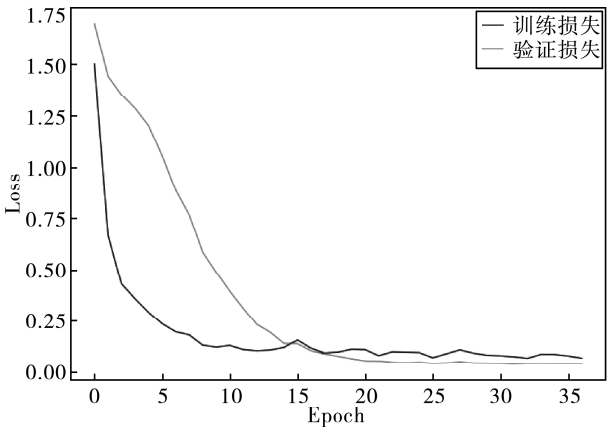

图 6　工控数据集训练和验证损失

表 3　实验结果

模型	*A*/%	*P*/%	*R*/%	*F*1_Score/%
Attention-1D-CNN	99.99	99.99	99.99	99.99

通过上述结果发现，Attention-1D-CNN 模型在通用网络数据集（如 KDD CUP99）中和工控数据集（如 Gas pipeline）中均具备高识别率。

5 结论

当今 ICS 存在的威胁不止包括功能安全方面的威胁，还有信息安全方面的威胁，并且存在跨域攻击的风险，因此做好威胁识别和分类是一项必不可少的工作。本文通过将模型应用于不同数据集中进行实验，发现融入 Attention 机制后，分类模型在通用网络威胁识别和有时序特征的工控网络威胁识别上均具有良好的识别准确率。未来工作中，可针对模型进行进一步的算法优化；继续增加威胁类别，细分威胁类型，扩大威胁信息库；还可结合威胁情报、多模态融合等方式，对模型做更深层次的改进，以服务于真实生产环境，提高 ISC 的安全性。

参考文献

[1] 曹举阳，王思山，司华超，等. 基于 Transformer 编码器的 CAN/CAN-FD 协议入侵检测研究［J/OL］. 计算机工程与应用，1－12［2025－06－06］. http：//kns. cnki. net/kcms/detail/11. 2127. TP. 20240913. 1550. 006. html.

[2] 李佳文，胡光俊，王锐，等. 一种基于主客体敏感行为学习的入侵检测方法［J］. 网络安全技术与应用，2025（6）：41－43.

[3] 崔文旭. 基于深度学习的网络安全威胁检测方法研究［D］. 北京：北京邮电大学，2023.

[4] KRAVCHIK M，SHABTAI A. Efficient cyber attack detection in industrial control systems using lightweight neural networks and PCA［J］. IEEE Transactions on Dependable and Secure Computing，2022，19（4）：2179－2197.

[5] L(Y)U S Y，WANG K，WEI Y L，et al. GNN-based advanced feature integration for ICS anomaly detection［J］. ACM Trans. Intell. Syst. Technol.，2023，14（6）：1－32.

[6] 胡智锋，孙峙华. 基于 SEGAN 和 Open-DNN 的工业控制系统入侵威胁检测研究［J］. 控制工程，2025，32（3）：400－408.

[7] 王晓鹏. 工业控制系统功能安全与信息安全融合初探［J］. 新型工业化，2021，11（10）：126－129.

[8] 卢家越. 面向工业控制系统的两安融合评估模型研究［D］. 广州：广州大学，2024.

[9] 马霄. “双安融合”下的工业互联网安全协同防护解决方案［C］//中国网络安全产业联盟. 2022 年网络安全优秀创新成果大赛论文集，2022：137－140.

[10] 邸丽清，谢丰. 工业控制系统信息安全与功能安全结合之探讨［J］. 中国信息安全，2016（4）：62－65.

[11] 郭怡安，曹德舜，李娜. 基于信息安全与功能安全融合的安全控制系统设计方案研究［J］. 安全、健康和环境，2023，23（5）：22－27.

[12] 谢耀滨. 工控现场系统安全分析与防护技术研究［D］. 郑州：战略支援部队信息工程大学，2022.

[13] 李东. 震网病毒事件浅析及工控安全防护能力提升启示［J］. 网络安全技术与应用，2019（1）：9－10，24.

[14] 章霞. 基于卷积神经网络特征重构的网络威胁检测技术［D］. 杭州：杭州电子科技大学，2022.

[15] GAYATHRI R G，SAJJANHAR A，XIANG Y. Image-based feature representation for insider threat classification［J］. Applied Sciences，2020，10（14）：4945.

[16] 邢温豪，郑梦策. 基于 DBN-BiLSTM-Attention 的工控网络入侵检测算法［J/OL］. 软件导刊，1－17［2025－06－06］. http：//kns. cnki. net/kcms/detail/42. 1671. TP. 20250520. 0929. 014. html.

[17] MORRIS T，Gao Wei. Industrial control system traffic data sets for intrusion detection research［C］//IFIP WG 11. 10 International Conference on Critical Infrastructure Protection. Springer，2014：65－78.

（收稿日期：2025－06－06）

作者简介：

万佳蓉（1996－），女，硕士，工程师，主要研究方向：工控信息安全、数据安全。

王晔（1986－），女，硕士，高级工程师，主要研究方向：工控信息安全、网络安全。

张雷（1985－），男，硕士，高级工程师，主要研究方向：工控信息安全、数据安全。

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