基于 1D CNN 的工业物联网入侵检测模型

张学欢[1] 黄迎春[1*]
ZHANG Xuehuan HUANG Yingchun

摘 要 随着工业物联网（industrial internet of things, IIoT）的快速发展，越来越多的关键基础设施和工业系统接入了网络，随之网络安全问题日益突出，入侵检测技术成为保障其安全的重要手段。因此文章设计了一种面向工业物联网环境的多路径结构的一维卷积神经网络（1D CNN）模型，多路径结构采用不同大小的卷积核来确保能够进行全面覆盖各类特征的信息提取。在特征整合方面，采用权重分配方式充分融合各个路径特征，使模型能够自动地选择最有利的特征。为进一步增强特征传递与信息提取能力，在模型中引入残差连接（Residual Connection）、软池化机制（SoftPool）。残差连接有助于缓解深度网络中的梯度消失问题，确保信息能够有效地在模型中传递。软池化则在特征压缩的过程中保留更多的关键信息，提升了模型的特征表达能力。并在工业物联网数据集上进行验证，结果表明，该模型在召回率、精确率、F_1 值上都具有出色的表现，适用于复杂的工业物联网环境。

关键词 工业物联网；入侵检测；1D CNN；多路径特征提取；特征融合；软池化；残差连接

doi：10.3969/j.issn.1672-9528.2026.01.023

0 引言

IIoT 作为 IoT 在工业领域的垂直应用与优化，广泛应用于军事、制造、能源、交通等多个领域，连接着各种设备和系统，将工业物联网技术应用于工业生产和运营的各个方面 [1]。随着 IIoT 的应用程度加深，极大增加了攻击面，使 IIoT 面临各种网络威胁，这已经成为一个重大挑战。入侵检测系统在保护 IIoT 网络安全、确保数据完整性和可靠性以及保证正常工业生产中发挥着关键作用 [2]。

面对日益复杂的攻击和大规模入侵数据，传统检测方法难以直接处理高维和稀疏数据。而近年来深度学习凭借其强大的自动特征提取能力，在入侵检测领域的研究和应用变得越来越广泛 [3]。Nandanwar 等 [4] 提出了一种针对工业物联网环境的 CNN 和 GRU 相结合的入侵检测模型，相比其他方法实现了出色的准确率。Ayodeji 等 [5] 提出了一种名为 Wavy-attention 入侵检测模型用于核电站传感器攻击检测，该模型由多层 CNN 与自注意力机制组成，在自建的数据集上，对各类别流量检测都达到了优异的性能。Attique 等 [6] 开发了一种用于工业物联网环境的入侵检测模型，使用 BiLSTM 与注意力机制结合对流量进行检测，并且使用 Shapley 加法解释机制来增强模型的透明度。Popoola 等 [7] 开发了一种联邦深度学习模型（FDL），经过验证展现了与传统集中式深度学习模型（CDL）相当的高分类性能。

上述多种方法所使用的流量数据集并未涉及或充分涵盖工业设备场景下的真实数据，容易导致训练的入侵检测模型在真实工业环境中的表现受限，且其检测性能还有进一步提高的空间。为了解决这些问题，本文利用深度学习技术，提出了一种基于多路径特征提取的 1D CNN 工业物联网入侵检测模型，在工业物联网数据集 X-IIoTD 上进行验证。

1 模型原理

基于多路径特征提取的 1D CNN 工业物联网入侵检测模型的总体框架如图 1 所示，将经过预处理后的流量数据输入到模型中，为了减少模型复杂度先经过卷积核大小为 1 的卷积层 Conv_1 初步进行提升通道数量，将单通道的流量数据扩展到 32 个通道。随后使用卷积核大小为 3 的 Conv_2 卷积层在增强特征提取能力的同时将通道数量增加到 64 个通道。构建 MP 模块，在每个路径上利用不同大小的卷积核提取多尺度的特征表示，并确保在信息流经 MP 模块后，信息的通道与长度都保持不变。构建 DMA 模块，能够根据 MP 模块提取的丰富信息来为其各路径分配相应的权重，以使不同路径上的信息充分融合。下一步，使用卷积核大小为 3 的 Conv_8 层对融合后的特征进一步提取关键特征，同时把通道数压缩到 32 来恢复通道规模。在模型中还引入了残差连接，来减少信息丢失。然后使用软池化精细地保留关键特征，同

1. 沈阳理工大学信息科学与工程学院 辽宁沈阳 110159
[基金项目] 国家自然科学基金资助项目（61971291）

时抑制冗余特征。最后经过展平层（Flatten）与线性层（Linear）得到分类结果。此外还在 Conv_1、Conv_2、Conv_3 层和特征融合后分别加入 ReLU 激活函数， 进行增强模型的稳定性和非线性表达能力。Conv_1、Conv_2、Conv_8 层中的卷积操作都进行等距填充，设置步长为 1，来保证提取更多的细节信息。

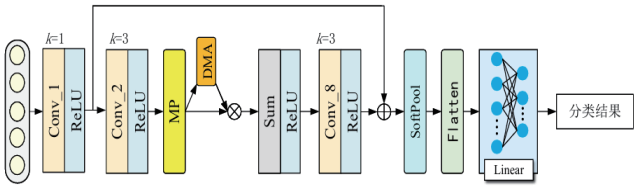

图 1 总体框架图

1.1 MP 模块

为了实现在同一网络层级提取不同尺度的特征，设计了一种多路径特征提取模块，如图 2 所示，通过并行构建具有不同大小卷积核的 3 条一维卷积路径，相对应路径的卷积核大小分别为 3、5、7，且每条路径上卷积层的步长都设置为 1，这能够使得提取到不同感受野的信息，从而增强模型特征的表达能力。一维卷积的运算公式为：

$$y_i=\sum_{c=1}^{C}\sum_{j=0}^{k-1}x_{c,i+j}\cdot w_{c,j} \tag{1}$$

式中：C 表示输入通道数；$x_{c,i+j}$ 表示第 c 通道的输入值；$w_{c,j}$ 表示相应的卷积核参数。

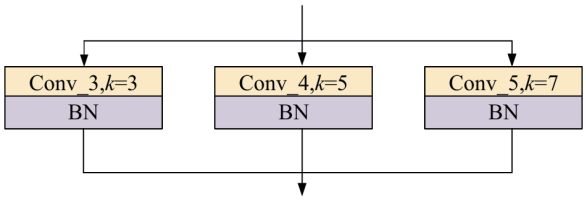

图 2 MP 模块图

并对每条路径的卷积层后都引入批量归一化层（batch normalization, BN），可以将信息映射到统一的量纲下，缓解内部协变量偏移，提高网络收敛速度并增强泛化能力[8]。此外，还可以减少不同路径输出特征数值上的不一致问题，有利于后续不同路径间的特征融合。

1.2 DMA 模块

将来自 MP 模块中各路径中提取到的不同层次的信息有效综合起来，可以增强模型对多样化的入侵行为的识别能力。而以往的特征融合方法常常采用简单的拼接或加权平均，无法灵活的调整不同路径上信息的贡献程度，导致感受野僵化，因此不能充分地整合来自各个路径的信息。DMA 模块图如图 3 所示。

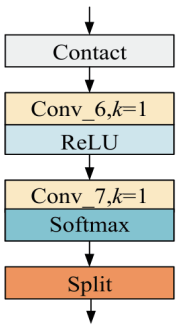

图 3 DMA 模块图

所以本文实现一个特征融合模块，实现更具选择性的特征融合。首先对来自多路径的不同尺度的特征信息按通道维度进行拼接，这不仅能够保留各路径的完整信息，还能为后续权重生成提供充分依据和支持，计算公式为：

$$P_{\text{contact}}=\text{Contact}(P_1,P_2,P_3) \tag{2}$$

式中：P_1、P_2、P_3 为来自不同路径的信息。

为了减少模型参数量，本模块的两个一维卷积层 Conv_6、Conv_7 卷积核大小都设置为 1，且步长也都为 1，用来逐步压缩通道数量。Conv_6 先把通道数量压缩为 64，并在 Conv_6 层后使用 ReLU 激活函数来增强非线性表达能力。再用 Conv_7 把通道数量压缩为 3，这是一个生成每个路径上权重的中间表示，得到的每个通道上的信息分别为每个路径上的初始权重图，所以在 Conv_7 层后使用 Softmax 激活函数沿着通道维度对原始权重图进行归一化处理，按每个路径的贡献程度来调整每个路径的权重，确保各路径上相同空间位置上的权重之和为 1，通过这种方式生成对应每个路径上权重，计算公式为：

$$\text{ReLU}(x)=\max(0,x) \tag{3}$$

$$F=\text{ReLU}(\text{Conv}_6(P_{\text{concat}})) \tag{4}$$

$$\text{Softmax}(x)=\frac{e^{x_i}}{\sum e^{x_i}} \tag{5}$$

$$W=\text{Softmax}(\text{Conv}_7(F)) \tag{6}$$

最后为能给不同路径分配到相应的权重，以便对各路径的输出的不同尺度信息进行加权融合，需要在通道维度 W 进行拆分得到 W_1、W_2、W_3，得到每个路径对应的单独权重图，融合过程计算公式为：

$$F_{\text{fused}}=W_1\odot P_1+W_2\odot P_2+W_3\odot P_3 \tag{7}$$

这一过程确保了模型有效综合来自不同路径的信息，保证能够有效提升模型对不同攻击的检测能力。

1.3 残差连接

残差网络最早是由 He 等[9]提出的，来解决伴随神经网络深度不断增加，导致训练过程中的梯度消失的问题。通过在模型中引入残差连接，将前面层次的特征信息直接与后面层次的输出相加，避免信息丢失。计算公式为：

$$H(x)=F(x)+x \tag{8}$$

式中：$H(x)$ 为目标的输出映射；x 为残差块的输入；$F(x)$ 为残差映射。

1.4 软池化

使用软池化操作来替代传统的最大池化与平均池化操

作 [10]。最大池化容易损失细节信息，而平均池化则容易弱化重要信息。软池化使用加权的方式不仅突出关键信息，还能保留更多的细节信息，来增强模型在特征压缩阶段保留有效信息的能力。软池化计算公式为：

$$\text{SoftPool}(x)=\frac{\sum x_i e^{x_i}}{\sum e^{x_i}} \tag{9}$$

2 实验结果与分析

使用 PyTorch2.5.1 深度学习框架，并在搭载了 Intel Core i7-12650H 处理器、NVIDIA GeForce RTX 4070 显卡的 Windows 11 笔记本电脑上进行实验。批次大小设置为 64，并且训练轮次为 150 轮。在训练中使用 Adam 优化器和交叉熵损失函数训练。

2.1 数据预处理

使用 X-IIoTID 数据集，该数据集是由堪培拉新南威尔士大学的 Al-Hawawreh 等 [11] 创建，由实时工业物联网网络生成，数据集包含新的 IIoT 连接协议、最近的设备活动、多样化的攻击场景和攻击协议。

（1）数据清洗

从数据集中删除时间、IP 地址、端口这些不相关特征，并删除包含单个值的特征列，选择“class2”作为标签数据。随后，对数据集进行去重。对于数据集中的缺失值用众数或中值进行填充。最后采用分层抽样的方式，将数据集按 7:3 比例划分为训练集和测试集，保持各类别比例相同。

（2）数据编码及归一化

对于数据集中存在的非数值类型使用标签编码转化为机器能够识别的数值类型。

数据记录中的数值差异显著会对模型的收敛速度以及训练效果产生不利的影响。通过 Min-Max 归一化将输入数据缩放到 [0, 1] 的区间内来统一量纲。计算公式为：

$$x_i'=\frac{x_i-x_{\min}}{x_{\max}-x_{\min}} \tag{10}$$

式中：$x_{\min}$ 为特征 x 列中的最小值；$x_{\max}$ 为最大值；x_i 为特征 x 第 i 行的值。

2.2 实验结果

混淆矩阵如图 4 所示，其中类别 C&C 容易被错误归纳到 Normal 类上，而类别 Exploitation 容易被错误归纳到 Lateral _movement、Normal 和 Reconnaissance 类别上。

多分类检测结果如表 1 所示，除 C&C 与 Exploitation 类别外，其余各类别在精确率、召回率、F_1 值上都达到了 98% 以上，证明了模型对大多数类别具有优异的检测效果。

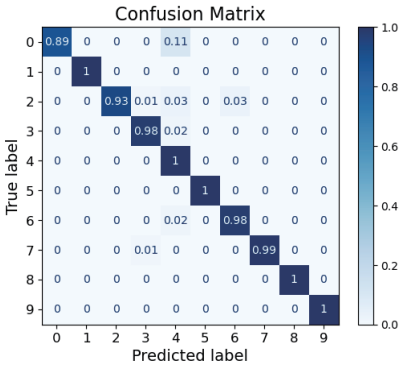

图 4 混淆矩阵

表 1 多分类检测结果

单位：%

类型	精确率	召回率	F_1 值
0	93.86	89.36	91.55
1	100.00	99.83	99.92
2	96.91	92.90	94.86
3	98.77	97.56	98.16
4	99.30	99.71	99.51
5	100.00	99.98	99.99
6	99.13	97.86	98.49
7	97.05	98.76	97.89
8	99.99	99.99	99.99
9	98.56	100.00	99.28

2.3 消融实验

不同的特征融合策略、池化方式以及是否引入残差连接均可能会对模型的性能造成影响。为验证模型各个部分的贡献程度，将模型中各个部分依次消除或用常用的方法进行替换来进行消融实验。

不同方法检测结果对比如表 2 所示，其中 contact 与 add 分别指的是对 MP 模块中不同路径输出的特征采取按通道维度拼接与加权平均的方式来进行特征融合；max-pool 与 avg-pool 分别指在模型中使用最大池化与平均池化来代替本模型所使用的软池化操作；no-pool 指不使用任何池化操作；no-res 指在模型中取消使用残差连接。

表 2 不同方法检测结果对比

单位：%

方法	精确率	召回率	F_1 值
add	97.65	95.79	96.68
contact	97.74	95.44	96.48
max-pool	98.16	95.94	96.96
avg-pool	96.69	96.07	96.36
no-pool	97.71	96.88	97.28
no-res	96.00	90.89	93.17
本文	98.36	97.60	97.96

实验结果表明，无论移除模型中的哪个部分或者用常用的方法对其进行替换，都会造成整体的精确率、召回率、F_1 值不同程度下降。

2.4 综合对比实验

为了评估本文模型在识别工业物联网攻击方面的有效性，在多分类上与近期现有模型进行比较，不同模型的结果对比如表 3 所示。

经过对比，本文的模型在精确率、召回率、F_1 值上分别达到了 98.36%、97.60%、97.96 出色性能，均优于另外四种模型，表明本文模型在工业物联网进行入侵检测中具有优越性与有效性。

表 3 不同模型的结果对比

单位：%

模型	精确率	召回率	F_1 值
CNN-GRU[4]	97.35	96.65	96.98
Wave-attention[5]	97.44	96.30	96.86
SABiLSTM[6]	97.30	83.79	88.90
FDL[7]	96.47	94.55	95.47
本文	98.36	97.60	97.96

3 结论

本文提出了一种基于多路径特征提取的 1D CNN 工业物联网入侵检测模型，该模型通过在每个路径上使用不同尺寸卷积核提取多尺度特征，结合权重分配实现对不同路径特征的有效融合，增强了特征表达能力。引入残差连接和软池化技术，有效提升了模型的信息保留能力和对关键信息的筛选。实验结果表明，该模型针对复杂的工业物联网环境表现出色的检测能力。

参考文献：

[1]SHU J, LU J Z. Two-stage botnet detection method based on feature selection for industrial internet of things[J/OL]. IET information security, 2025[2025-12-02].https://www.semanticscholar.org/paper/Two-Stage-Botnet-Detection-Method-Based-on-Feature-Shu-Lu/3b0a928754546e00bcff745a3f1ce298d05a7b32.DOI:10.1049/ise2/9984635.

[2]LU Y Y, CHAI S C, SUO Y H, et al. Intrusion detection for industrial internet of things based on deep learning[J]. Neurocomputing, 2024, 564: 126886.

[3]DAI W, LI X H, JI W X, et al. Network intrusion detection method based on CNN-BiLSTM-Attention model[J]. IEEE access, 2024,12: 53099-53111.

[4]NANDANWAR H, KATARYA R. Deep learning enabled intrusion detection system for Industrial IOT environment[J]. Expert systems with applications, 2024, 249: 123808.

[5]AYODEJI A, DI BUONO A, PIERCE I, et al. Wavy-attention network for real-time cyber-attack detection in a small modular pressurized water reactor digital control system[J]. Nuclear engineering and design, 2024, 424: 113277.

[6]ATTIQUE D, WANG H, WANG P, et al. Explainable and data-efficient deep learning for enhanced attack detection in IIoT ecosystem[J]. IEEE internet of things journal, 2024, 11(24): 38976-38986.

[7]POPOOLA S I, IMOIZE A L, HAMMOUDEH M, et al. Federated deep learning for intrusion detection in consumer-centric internet of things[J]. IEEE transactions on consumer electronics, 2023, 70(1): 1610-1622.

[8]SANTURKAR S, TSIPRAS D, ILYAS A, et al. How does batch normalization help optimization?[EB/OL]. (2019-04-15)[2025-12-02].https://doi.org/10.48550/arXiv.1805.11604.

[9]HE K M, ZHANG X Y, REN S Q, et al. Deep residual learning for image recognition[C]//2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR). Piscataway: IEEE, 2016: 770-778.

[10]STERGIOU A, POPPE R, KALLIATAKIS G. Refining activation downsampling with SoftPool[C]//Proceedings of the IEEE/CVF international conference on computer vision. Piscataway: IEEE, 2021: 10357-10366.

[11]Al-HAWAWREH M, SITNIKOVA E, ABOUTORAB N. X-IIoTID: a connectivity-agnostic and device-agnostic intrusion data set for industrial Internet of things[J]. IEEE internet of things journal, 2021, 9(5): 3962-3977.

【作者简介】

张学欢（2000—），男，山东菏泽人，硕士，研究方向：网络安全。

黄迎春（1976—），通信作者（email:welcomspring@163.com），男，辽宁瓦房店人，硕士，副教授、硕士生导师，研究方向：网络服务与信息安全。

（收稿日期：2025-07-03 修回日期：2025-12-30）