DOI:10.11918/202410075

一种针对多分类的网络入侵检测系统模型

杨启成,全海燕,何玉琴

(昆明理工大学 信息工程与自动化学院,昆明 650504)

摘 要:为解决现有入侵检测模型在多分类检测中准确率低、误报率高,且难以在物联网等资源受限的边缘设备上高效部署的问题,提出一种卷积长短期记忆自注意力网络(convolutional long short-term self-attention network,CLSA-Net)深度学习模型。该模型通过自适应卷积模块、长短期记忆网络与改进的自注意力机制级联,增强对多样化时序攻击特征的捕捉能力;将模型转换为TFLite(TensorFlow Lite)格式,以实现在低成本ESP32-S3嵌入式平台上的高效部署。在多个公共数据集上进行综合对比实验,并在ESP32-S3平台上进行部署测试。实验结果表明:CLSA-Net在UNSW-NB15、CICIoT2023等多个公共数据集上的性能均优于现有主流模型,综合检出率与准确率分别达到了98.60%和97.48%;在边缘部署测试中,优化后的模型在ESP32-S3平台上保持了超过80%的准确率,并实现了低功耗下的实时检测。本研究验证了在资源受限的物联网边缘计算环境中部署高性能入侵检测系统的可行性,并实现了高精度检测与低功耗运行的有效平衡,为边缘安全防御提供了一个具备实用价值的解决方案。

关键词:深度学习;网络入侵检测;多分类;自注意力机制;边缘部署

中图分类号:TP393.08 **文献标志码**:A **文章编号**:0367-6234(2026)09-0196-13

A multi-class classification model for network intrusion detection

Yang Qicheng, Quan Haiyan, He Yuqin

(Faculty of Information Engineering and Automation, Kunming University of Science and Technology, Kunming 650504, China)

Abstract: To address the limitations of existing intrusion detection models, namely, low accuracy, high false positive rates in multi-class detection, and the difficulty of efficient deployment on resource-constrained edge devices such as those used in the Internet of Things (IoT), this paper proposes a deep learning model named the convolutional long short-term self-attention network (CLSA-Net). The proposed CLSA-Net first employs a cascaded structure comprising an adaptive convolutional module, a long short-term memory network, and an improved self-attention mechanism to enhance its capability in capturing diverse temporal attack features. Subsequently, the trained model is converted into the TFLite (TensorFlow Lite) format to enable efficient deployment on low-cost ESP32-S3 embedded platforms. Comprehensive comparative experiments were conducted on multiple public datasets, along with deployment tests on the ESP32-S3 platform. The experimental results demonstrate that CLSA-Net outperforms existing mainstream models on various public datasets, including UNSW-NB15 and CICIoT2023, achieving an overall detection rate and accuracy of 98.60% and 97.48%, respectively. Furthermore, in edge deployment tests, the optimized model maintained an accuracy exceeding 80% on the ESP32-S3 platform while achieving real-time detection under low power consumption. This study validates the feasibility and practical value of deploying high-performance intrusion detection systems in resource-constrained IoT edge computing environments, striking an effective balance between high-accuracy detection and low-power operation, thus providing a practical solution for edge security defense.

Keywords: deep learning; network intrusion detection; multi-class classification; self-attention mechanism; edge deployment

随着物联网与信息技术的深度融合,网络攻击的规模与复杂度均呈现出指数级增长,严重威胁着全球网络空间的安全与稳定。作为保障网络安全的关键技术,网络入侵检测系统(network intrusion detection system,NIDS)旨在实时监控并识别潜在的未授权访问、恶意滥用及网络攻击等异常活动,并及

收稿日期:2024-10-31;**录用日期**:2024-12-30;**网络首发日期**:2025-11-24
网络首发地址:https://link.cnki.net/urlid/23.1235.T.20251121.1756.012
基金项目:国家自然科学基金(61861023)
作者简介:杨启成(1997—),男,硕士研究生;全海燕(1970—),男,副教授,硕士生导师
通信作者:全海燕,quanhaiyan@163.com

时发出告警[1]。

在此背景下，机器学习，特别是深度学习（deep learning，DL）技术已成为推动 NIDS 发展的重要引擎。自 2006 年 Hinton 等提出深度信念网络（deep belief network，DBN）及有效的逐层预训练算法以来，DL 凭借其强大的分层特征学习与非线性建模能力，在计算机视觉、自然语言处理等多个领域取得了突破性进展，并被证明是解决复杂模式识别问题的有效工具[2-3]。

当前，将深度学习技术应用于网络入侵检测领域已成为研究的热点与主流趋势[4-5]。在深度学习方法被广泛采用前，该领域的研究主要依赖于传统机器学习算法。例如，支持向量机（support vector machine，SVM）、随机森林（random forest，RF）以及自适应增强算法（adaptive boosting，AdaBoost）等曾被广泛用于构建 NIDS 分类器[6-7]。然而，这些方法通常需要依赖专家经验进行复杂的人工特征工程，且在处理高维、海量的网络流量数据时，往往面临检测精度不足、误报率偏高及泛化能力受限等挑战。其根本原因在于传统算法在自动提取数据深层抽象特征方面能力有限，难以有效捕捉复杂攻击行为与网络流量数据之间的非线性映射关系[8]。

为克服传统机器学习方法在 NIDS 中处理海量高维数据时的性能局限，基于 DL 的模型已成为研究的主流。初期研究借鉴了卷积神经网络（convolutional neural network，CNN）在视觉领域的应用，利用其局部特征提取能力捕捉网络流量的高维空间特征[9-10]。在此基础上，为捕捉流量数据内在的时间序列特性，以长短期记忆网络（long short-term memory，LSTM）为代表的循环神经网络（recurrent neural network，RNN）变体被广泛引入[11-13]。上述技术路线进一步演化为混合（Hybrid）深度学习架构。在此类模型中，研究者通常将 CNN 提取的特征序列送入 RNN 进行时序建模，以实现对攻击行为的时空联合感知[14]。然而，现有研究仍存在局限性。首先，许多模型在追求高准确率的同时，未能有效控制误报率，这限制了其在实际部署中的价值[4]。其次，部分模型在以 NSL-KDD 为代表的早期数据集上表现良好，但在面对如 UNSW-NB15 及 CICIoT2023 等更能反映现代网络环境复杂性（如攻击类型多样、数据不平衡、流量动态性高）的数据集时，其多分类检测性能显著下降。

为应对现有模型在多分类任务中误报率高、准确率低的问题，本文提出一种卷积长短期记忆自注意力网络（convolutional long short-term self-attention network，CLSA-Net）深度学习模型。针对嵌入式边缘场景的资源限制，进一步引入模型量化与转换技术进行轻量化处理，旨在降低边缘部署计算与存储开销，并探索在低功耗硬件上构建兼顾高精度与实时性入侵检测系统的可行方案。

1　模型设计

1.1　结构概述

本研究设计一种用于网络入侵检测的分层混合深度学习模型 CLSA-Net，该模型融合一维卷积神经网络（one-dimensional convolutional neural network，1D-CNN）、LSTM 以及自注意力机制的优点，以实现对网络流量数据时空特征的协同感知与深度建模。模型的核心思想在于分层、分工的特征学习。在模型的整体架构中，数据首先流经 CNN 模块，该模块作为底层特征提取器，在不破坏数据时间顺序的前提下，从每个时间步的网络流量数据中提取局部和抽象的特征。随后，由 CNN 生成的特征向量序列被送入 LSTM 网络，以捕捉和学习攻击行为在时间维度上的依赖关系和演变模式。为进一步提升模型的判别能力，在时序建模之后引入自注意力机制，并融合位置编码，使模型能够动态评估并聚焦于序列中最具信息量的部分。最终，经过注意力加权的特征表示被传递至全连接网络进行分类判决。该设计使得 CNN 和 LSTM 能在各自擅长的维度上充分发挥作用，自注意力机制则进一步提升模型的精确性与可解释性。图 1 展示了 CLSA-Net 模型的整体网络架构，其中包含若干级联的处理单元。为进一步阐述其核心机制，图 2 详细展示了单个 CLSA（convolutional long short-term self-attention）块的内部结构设计。



图 1　CLSA-Net 整体架构

Fig. 1　Overall architecture of CLSA-Net

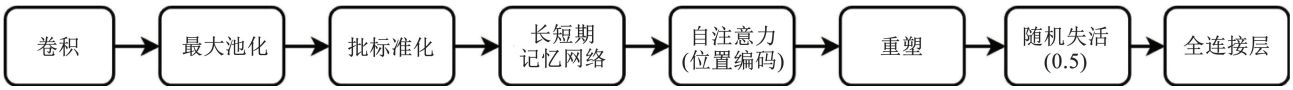


图 2　CLSA 块内部结构

Fig. 2　Internal structure of the CLSA block

在模型具体实现中,输入网络的原始流量数据首先经过预处理阶段,该阶段包含对类别型特征的热编码和对数值型特征的标准化处理,以消除不同特征间的量纲差异并提升后续训练的效率与稳定性。

将预处理完成的数据送入特征提取模块。数据首先通过卷积层以捕捉攻击载荷的局部模式与关键指纹;随即进入最大池化层进行降维,在保留关键信息的同时降低计算复杂度;然后经过批量归一化(batch normalization,BN)层,以加速模型收敛并防止过拟合。

CNN 模块提取的特征序列随即被送入 LSTM 层进行时序建模。LSTM 网络凭借其特有的输入门、遗忘门和输出门结构,能够有效捕捉序列数据中的长期依赖关系,对于识别具有明显时序行为模式的攻击至关重要。在时序信息建模的基础上,模型进一步引入自注意力机制以聚焦关键特征。为确保模型能充分利用序列的位置信息,特征序列在进入自注意力层之前会融入正余弦位置编码。自注意力机制通过计算序列内部各元素间的相关性权重,动态地增强重要特征的表达,同时抑制无关信息的干扰。

最终,经过注意力加权的特征表示会通过多个随机失活(dropout)层减轻过拟合风险, 迭代 3 次后被送入全连接层进行最终的非线性映射,由 Softmax 激活函数输出各个网络攻击类别的概率,从而完成对入侵行为的精准检测与分类。

1.2 核心模块设计与实现

CLSA-Net 采用一种分层级的特征学习策略,通过在不同深度网络层级中配置不同数量的卷积核控制学习粒度。具体而言,设计了 3 个级别的 CNN-RNN 处理单元,其中卷积核数量从初始的 32 个逐步增加至末端的 256 个,以此实现从宽泛、概括性特征到精细、特异性特征的逐级提取。

1.2.1 卷积神经网络 CNN

CLSA-Net 的基础是 1D-CNN,其特别适用于处理以一维格式表示的网络流量序列[15]。在 CNN 模块中,卷积与池化是两大核心操作。卷积运算通过一组可学习的卷积核(kernel)扫描输入数据,将其映射为一系列特征图(feature map),从而有效凸显数据中的关键模式。其一维形式可定义为

$$y_t = (\boldsymbol{x} * \boldsymbol{w})(t) = \sum_{s=1}^{m} \boldsymbol{w}(s) \cdot \boldsymbol{x}\left(t - s + \frac{m}{2}\right) \tag{1}$$

式中:$\boldsymbol{x}$ 为一维输入序列(如网络流量向量),$\boldsymbol{w}$ 为长度为 m 的卷积核,$*$ 为离散卷积运算,t 为序列的时间步索引,s 为卷积核内部的滑动窗口索引,y_t 为输出特征图在位置 t 处的数值。

为引入非线性并加速训练,本模型选用整流线性单元(ReLU)作为激活函数。激活之后,通常会进行最大池化(max pooling)操作,通过对特征图的局部区域取最大值进行下采样,不仅能降低后续层次的参数数量与计算成本,还能保留最显著的特征,并为模型带来一定的平移不变性[16]。

1.2.2 批量归一化 BN

为保证多层卷积网络训练的稳定性并加速收敛,模型在卷积层后引入 BN。该技术通过对每一批(batch)数据在网络层间的输出进行标准化,解决深度网络训练过程中的内部协变量偏移问题,降低模型对参数初始化的依赖性,并允许使用更高的学习率[17]。对于批次中的任一激活值 x_k,其归一化过程可表示为

$$\hat{x}_k = \frac{x_k - \mu_{\mathrm{B}}}{\sqrt{\sigma_{\mathrm{B}}^2 + \epsilon}} \tag{2}$$

式中:x_k 为当前 batch 中第 k 个样本的输入值,μ_{B} 和 σ_{B}^2 分别为当前 batch 的均值和方差,ϵ 为防止分母为 0 而设置的微小常数。

随后,BN 层会通过两个可学习的参数 γ 和 β 对归一化后的值进行线性变换以恢复网络的表达能力。

$$\hat{y}_k = \gamma \hat{x}_k + \beta \tag{3}$$

1.2.3 长短期记忆网络 LSTM

通过 CNN 模块提取流量数据的局部特征之后,模型利用 LSTM 捕捉这些特征在时间维度上的依赖关系。传统 RNN 在处理长序列时面临的主要挑战是梯度消失或爆炸问题,而 LSTM 通过精巧的门控机制(gating mechanism)有效克服这一缺陷[13]。这些门控单元使 LSTM 能够有选择地读取、写入和遗忘信息,从而在细胞状态(cell state)中维持长距离的时序依赖,这对于理解复杂的攻击链条至关重要。LSTM 单元的更新过程如图 3 所示,其具体计算见式(4)~(8)。

$$\boldsymbol{i}_t = \sigma(\boldsymbol{W}_{\mathrm{xi}}\boldsymbol{x}_t + \boldsymbol{W}_{\mathrm{hi}}\boldsymbol{h}_{t-1} + \boldsymbol{W}_{\mathrm{ci}}\boldsymbol{c}_{t-1} + \boldsymbol{b}_{\mathrm{i}}) \tag{4}$$

$$\boldsymbol{f}_t = \sigma(\boldsymbol{W}_{\mathrm{xf}}\boldsymbol{x}_t + \boldsymbol{W}_{\mathrm{hf}}\boldsymbol{h}_{t-1} + \boldsymbol{W}_{\mathrm{cf}}\boldsymbol{c}_{t-1} + \boldsymbol{b}_{\mathrm{f}}) \tag{5}$$

$$\boldsymbol{c}_t = \boldsymbol{f}_t \odot \boldsymbol{c}_{t-1} + \boldsymbol{i}_t \odot \tanh(\boldsymbol{W}_{\mathrm{xc}}\boldsymbol{x}_t + \boldsymbol{W}_{\mathrm{hc}}\boldsymbol{h}_{t-1} + \boldsymbol{b}_{\mathrm{c}}) \tag{6}$$

$$\boldsymbol{o}_t = \sigma(\boldsymbol{W}_{\mathrm{xo}}\boldsymbol{x}_t + \boldsymbol{W}_{\mathrm{ho}}\boldsymbol{h}_{t-1} + \boldsymbol{W}_{\mathrm{co}}\boldsymbol{c}_{t-1} + \boldsymbol{b}_{\mathrm{o}}) \tag{7}$$

$$\boldsymbol{h}_t = \boldsymbol{o}_t \odot \tanh(\boldsymbol{c}_t) \tag{8}$$

式中:$\boldsymbol{x}_t$ 为当前 t 时刻的输入向量,$\boldsymbol{h}_t$、$\boldsymbol{c}_t$、$\boldsymbol{h}_{t-1}$、$\boldsymbol{c}_{t-1}$ 分别为 t 时刻、$t-1$ 时刻的隐藏状态、细胞状态,$\boldsymbol{i}_t$、$\boldsymbol{f}_t$ 和 $\boldsymbol{o}_t$ 分别为输入门、遗忘门和输出门,$\boldsymbol{W}_{\mathrm{x}\cdot}$、$\boldsymbol{W}_{\mathrm{h}\cdot}$、$\boldsymbol{W}_{\mathrm{c}\cdot}$ 分别为输入、隐藏状态及细胞状态对应的权重矩阵,$\boldsymbol{b}_{\cdot}$ 为对应的偏置向量,$\sigma(\cdot)$ 为 Sigmoid 函数,$\odot$ 表示矩阵的按元素相乘。

1.2.4　自注意力机制和位置编码

在 LSTM 完成对网络流量的长距离时序建模后，为使模型能够动态聚焦于序列中最重要的部分，在 LSTM 层之上进一步集成了改进的自注意力机制与位置编码技术。自注意力机制能够计算序列中任意两个位置之间的依赖关系，从而捕捉全局信息。该模块具体采用了结合残差连接的注意力机制结构[18-19]，如图 4 所示。

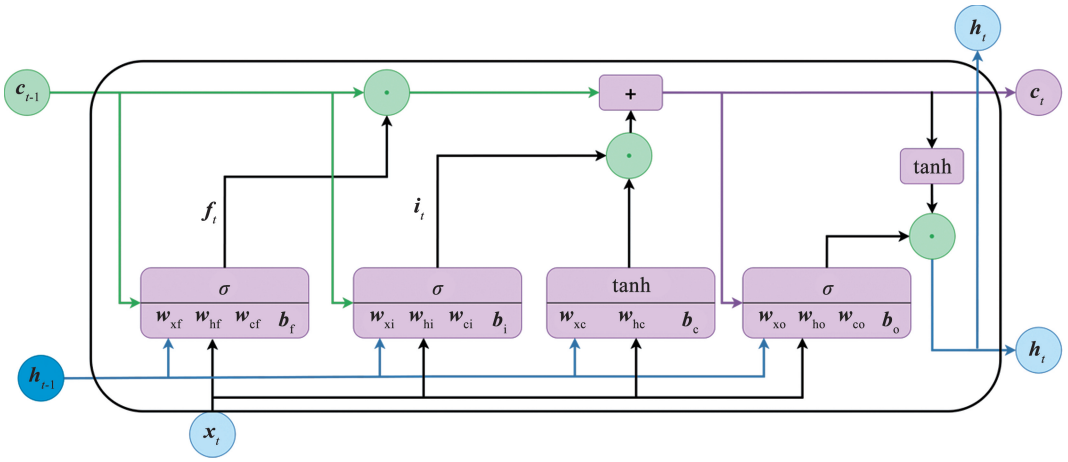


图 3　长短期记忆网络结构

Fig. 3　Structure of long short-term memory network

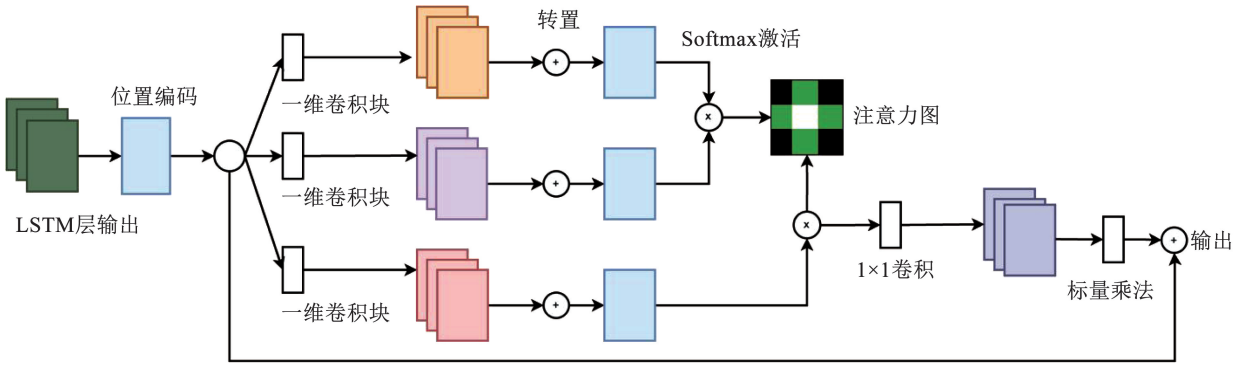


图 4　基于卷积运算与残差连接的自注意力机制

Fig. 4　Convolutional self-attention mechanism with residual connections

根据注意力权重对值矩阵 $\boldsymbol{V}$ 进行加权求和得到输出，可表示为

$$f_{\text{Attention}}(\boldsymbol{Q},\boldsymbol{K},\boldsymbol{V}) = \text{Softmax}\left(\frac{\boldsymbol{Q}\boldsymbol{K}^{\text{T}}}{\sqrt{d_{\text{k}}}}\right)\boldsymbol{V} \tag{9}$$

式中：$f_{\text{Attention}}(\cdot)$ 为映射函数；$\boldsymbol{Q}$、$\boldsymbol{K}$ 分别为查询矩阵、键矩阵，在本文中通过对输入序列施加一维卷积操作映射得到；d_{k} 为键向量的维度，分母引入缩放因子 $\sqrt{d_{\text{k}}}$ 旨在调节点积结果的数值范围，防止 Softmax 函数进入饱和区而引发梯度消失问题。

为让模型感知到序列的顺序信息，在送入注意力层之前，为输入序列叠加正、余弦位置编码，其定义分别为：

$$\boldsymbol{P}_{t,2j} = \sin\left(\frac{t}{1\,000^{\frac{2j}{d}}}\right) \tag{10}$$

$$\boldsymbol{P}_{t,2j+1} = \cos\left(\frac{t}{1\,000^{\frac{2j}{d}}}\right) \tag{11}$$

式中：j 为隐藏维度的索引，d 为隐藏层的总维度数。

通过这种方式，位置编码为每个输入位置生成一个独特的数值模式，从而使模型能够识别事件的相对顺序。

此编码方式不仅使模型具备对输入事件顺序的感知能力，还保留了输入的时序结构特征，提高网络入侵检测任务中的效果。此外，由于正弦和余弦函数的平滑性与周期性，所设计的位置编码能够较好地泛化到不同长度的序列，增强模型对未知数据的适应能力。因此，引入位置编码使得模型更好地理解和处理复杂的时序关系，增强模型在检测网络攻击时的表现力。

2　仿真分析

2.1　数据集

为全面验证本文所提模型的有效性与泛化能力，选取网络入侵检测领域中具有代表性的 6 个公开数据集进行实验评估，分别为 NSL-KDD、UNSW-

NB15、CICIDS2017、CICIDS2019、LuFlow 和 CICIoT2023。在这些数据集中,UNSW-NB15 因其复杂性而备受关注。现有研究表明,尽管在 NSL-KDD 数据集上,传统机器学习模型的表现优异,但在 UNSW-NB15 数据集上的表现仍有待提升。具体而言,现有主流模型在该数据集上的准确率指标均表现一般。其中,传统机器学习算法,如 SVM[6] 和 AdaBoost[8] 的准确率分别为 74.80% 和 73.19%;即便是基于深度学习的模型,如 CNN[9]、MLP[20]、LSTM[20] 的准确率也主要集中在 82% ~ 84% 之间;部分改进模型,如 HAST-IDS[21] 和 LuNet[5] 虽然有所提升,但也仅分别达到了 80.03% 和 85.35%。这一现状表明,在 UNSW-NB15 等复杂数据集上提升检测精度仍是当前研究的重点。

NSL-KDD 数据集是新不伦瑞克大学(University of New Brunswick)提供的,其改进了原KDDCup'99 数据集的固有缺陷,消除了冗余记录,并优化了数据集的可用性,成为网络入侵检测研究中的经典数据集之一[22]。NSL-KDD 数据集中的攻击类别及数量见表 1。

UNSW-NB15 数据集由新南威尔士大学(University of New South Wales)于 2015 年发布,并得到了广泛的应用。该数据集包含了更广泛的攻击类型、提取的特征数、用于模拟和收集数据的不同 IP 地址数[23] 并且由现实世界的正常网络活动和合成攻击活动的网络流量混合而成。UNSW-NB15 数据集中的攻击类别及数量见表 2。

表 1 NSL-KDD 数据集攻击类别及数量

Tab. 1 NSL-KDD dataset attack categories and quantities

正常(Normal)	拒绝服务攻击(DoS)	探测攻击(Probe)	远程到本地攻击(R2L)	本地到远程攻击(U2R)
77 054	53 385	14 077	3 749	252

表 2 UNSW-NB15 数据集攻击类别及数量

Tab. 2 UNSW-NB15 dataset attack categories and quantities

正常(Normal)	拒绝服务攻击(DoS)	漏洞利用攻击(Exploits)	模糊测试(Fuzzers)	通用攻击(Generic)
9 300	16 353	44 525	24 246	58 871

侦察(Reconnaissance)	Shell 代码(Shellcode)	蠕虫(Worms)	后门(Backdoor)	分析(Analysis)
13 987	1 511	174	2 329	2 677

CICIDS2017 和 CICIDS2019 数据集是由加拿大网络安全研究所提供的,其模拟真实网络流量,涵盖各种攻击类型(如 DoS、DDoS、Web 等)。CICIDS2019 是 CICIDS2017 的更新版,增加了更多的攻击种类[23]。

LuFlow 是基于流量的入侵检测数据集,结合了威胁情报服务,特别适合于模拟与现实威胁的检测分析。

CICIoT2023 数据集是由加拿大网络安全研究所提供的,旨在促进物联网(IoT)环境中大规模攻击安全分析应用程序的开发。该数据集包含 34 种攻击,分为 DDoS、DoS、侦察、基于 Web 的攻击、暴力破解、Mirai 和欺骗 7 类[24]。

2.2 数据预处理与验证方法

为保证实验的公平性与结果的可靠性,所有实验均采用标准化的数据处理与模型验证流程。

首先,在数据预处理阶段,由于 6 个数据集中均包含符号型或类别型特征,本文采用独热编码(one-hot encoding)将其转换为数值型向量,以便深度学习模型能够处理。同时,对数值型特征进行标准化,确保所有特征处于统一的尺度空间,这对于加速模型收敛和提升性能至关重要[5]。

其次,为应对数据不平衡问题,本研究针对 UNSW-NB15 和 CICIoT2023 数据集中的少数类样本实施了随机过采样(random oversampling)。以 UNSW-NB15 为例,其中"Worms"类别的样本仅有 174 条,与总样本量(257 673 条)相比极不均衡。通过复制少数类样本,可以有效缓解模型在训练过程中对多数类的偏好,提升对稀有攻击的检测能力。

最后,在模型评估阶段,采用分层 k 折交叉验证(stratified k-fold cross-validation,$k = 10$)方案。该方案将数据集划分为 k 个互斥的子集(或称"折"),并确保每个子集中各类别的样本比例与原始数据集保持一致。在每次迭代中,使用 k-1 个子集进行模型训练,用剩余的子集进行验证。此过程重复 k 次,直至每个子集均被用作一次验证集。最终的性能指标是 k 次验证结果的平均值。相比于简单的训练/测试集划分,该方案能提供更稳健、更无偏的模型性能评估[25]。

2.3 仿真环境与复杂度分析

2.3.1 仿真环境与训练效率

实验在一台配置为 Apple M1 Pro CPU 的 Macbook Pro 和一台搭载 NVIDIA RTX 4090 GPU(24 GB 显

存)的服务器上进行。

以 CICIoT2023 数据集为例，仅使用 CPU 训练时，平均每轮(epoch)耗时约 9 min，模型在第 27 轮左右达到最优，总耗时约 243 min。而在服务器端启用 GPU 加速后，平均每轮耗时缩短至 3 min，且模型在第 23 轮左右收敛至最优并停止训练，总耗时仅约 69 min。对于像 NSL-KDD 这类相对简单的数据集，训练总耗时在 40 ~ 80 min。然而，对于数据量和复杂度均较高的 UNSW-NB15 数据集，总训练时长约 300 min(5 h)，这反映出该数据集对计算资源要求更高，也从侧面印证其数据分布的复杂性。

2.3.2　模型复杂度

CLSA-Net 采用 CNN 与 RNN 的级联结构，理论上的时间与空间复杂度相对较高。具体地，时间复杂度主要由卷积、自注意力和 LSTM 构成，约为 $O(n\times m\times c_{in}\times c_{out})+O(n^2\times d_k)+O(n\times h^2)$，空间复杂度约为 $O(n\times c_{out})+O(n\times d_k)+O(4\times h^2)$，其中 n 为输入序列的长度，m 为卷积核大小，c_{in} 和 c_{out} 分别为输入和输出通道数，h 为 LSTM 的隐藏层大小，d_k 为键向量维度。尽管理论复杂度较高，但得益于模型优化的架构设计，能够更高效地提取特征，实现更快的收敛速度，从而缩短达到最优性能所需的训练周期。因此，在实际应用中，其总体的资源消耗和训练时间成本被控制在可接受的范围内。

2.3.3　边缘部署测试

ESP32 系列微控制器凭借其低功耗、高性价比及集成的无线通信模块，已成为物联网边缘计算领域的首选平台。鉴于嵌入式设备资源受限的特性，TFLite(TensorFlow Lite)框架通过模型量化与结构压缩技术，能够显著降低模型的存储占用与计算开销，从而实现对深度学习模型的高效推理。为此，本研究采用该技术对训练后的模型进行转换与优化，并将其部署至 ESP32-S3-WROOM-2 嵌入式开发板，以验证模型在真实物理环境中的工程应用潜力。

图 5 和图 6 直观地展示了边缘部署方案的实际运行效果。其中，图 5 为模型在 ESP32 开发板上进行实时网络流量分类的推理过程，串口监视器的输出清晰地显示模型对输入流量的实时判决结果与各类别置信度。图 6 记录了在注入特定异常流量时，模型的快速检出与告警表现。这些结果验证了 CLSA-Net 在边缘端进行即时安全威胁响应的可行性与有效性。这一部署测试证明所提模型架构具备良好的灵活性和可扩展性，为其实际应用奠定了基础。

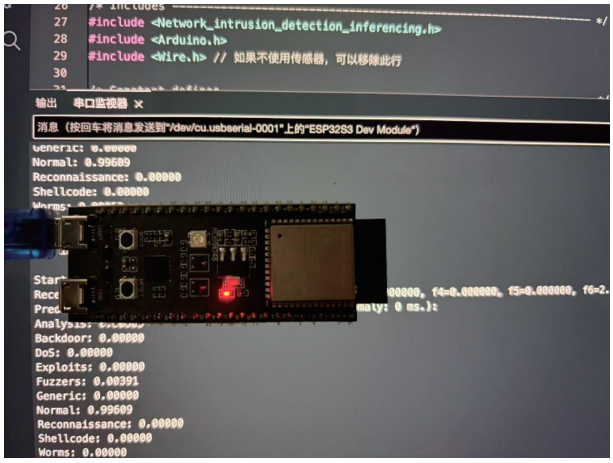


图 5　ESP32 实时推理效果

Fig. 5　ESP32 real-time inference performance

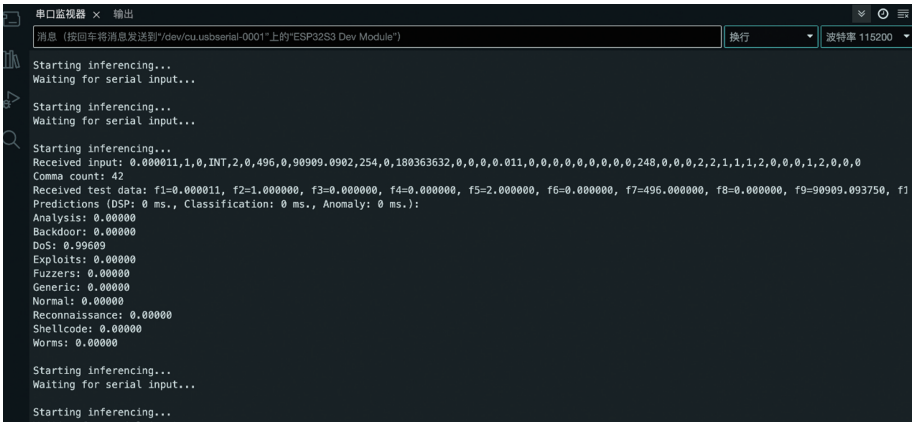


图 6　在 ESP32 上模型对异常流量的实时推理结果

Fig. 6　Real-time inference results of the model on ESP32 for abnormal traffic

2.4　评价指标与实验设置

为全面评估模型的检测性能，采用准确率(accuracy，A)、检出率(detection rate，R_D)、误报率(false positive rate，R_{FP})和 F_1 分数(F_1-score，F_1)作为评价指标[5]。其计算公式分别为：

$$A=\frac{T_P+T_N}{T_P+T_N+F_P+F_N} \tag{12}$$

$$R_D=\frac{T_P}{T_P+F_N} \tag{13}$$

$$R_{FP}=\frac{F_P}{F_P+T_N} \tag{14}$$

$$F_1=\frac{2\times T_P}{2\times T_P+F_P+F_N} \tag{15}$$

式中:T_P为正确分类的攻击次数,T_N为正确分类的正常流量次数,F_N为误分类为正常流量的攻击次数,F_P为误分类为攻击的正常流量次数。

在实验参数设置方面,为提升模型的收敛速度与稳定性,训练阶段采用 RMSprop 优化器对网络参数进行更新[26],初始学习率设置为 0.001。此外,为增强模型的泛化能力并防止过拟合,在网络结构中引入 dropout 层,其神经元随机失活率设定为 0.5。

2.5 仿真结果

CLSA-Net 分别在 6 个数据集上进行多分类实验,结果见表 3 ~ 5。为综合考察模型的鲁棒性,本文对多尺度交叉验证指标进行了宏平均处理。

表 3 NSL-KDD 和 UNSW-NB15 数据集多分类任务结果

Tab. 3 Results of multi-class classification task on NSL-KDD and UNSW-NB15 datasets %

k	NSL-KDD			UNSW-NB15		
	R_D	A	R_{FP}	R_D	A	R_{FP}
2	99.21 ±0.13	99.13 ±0.07	0.82 ±0.05	96.31 ±0.11	94.83 ±0.08	2.12 ±0.02
4	98.86 ±0.04	98.92 ±0.03	0.54 ±0.02	96.21 ±0.09	95.38 ±0.04	1.97 ±0.02
6	99.33 ±0.05	99.66 ±0.03	0.72 ±0.02	96.42 ±0.08	95.71 ±0.04	1.51 ±0.04
8	99.26 ±0.07	98.87 ±0.04	0.79 ±0.09	95.96 ±0.07	95.35 ±0.05	1.99 ±0.03
10	98.32 ±0.11	99.29 ±0.04	0.63 ±0.07	95.88 ±0.07	94.85 ±0.06	2.07 ±0.02

表 4 CICIDS2017 和 CICIDS2019 数据集多分类任务结果

Tab. 4 Results of multi-class classification task on CICIDS2017 and CICIDS2019 datasets %

k	CICIDS2017			CICIDS2019		
	R_D	A	R_{FP}	R_D	A	R_{FP}
2	98.16 ±0.11	96.93 ±0.07	0.82 ±0.09	99.01 ±0.29	98.83 ±0.09	0.06 ±0.03
4	97.82 ±0.09	97.34 ±0.09	0.64 ±0.09	98.91 ±0.11	99.09 ±0.09	0.05 ±0.03
6	98.01 ±0.09	97.86 ±0.12	0.82 ±0.08	99.12 ±0.09	99.11 ±0.10	0.07 ±0.04
8	97.77 ±0.08	97.87 ±0.08	0.99 ±0.09	99.21 ±0.11	98.85 ±0.15	0.10 ±0.05
10	97.89 ±0.12	97.19 ±0.14	1.23 ±0.17	99.88 ±0.11	99.15 ±0.09	0.07 ±0.06

表 5 LuFlow 和 CICIoT2023 数据集多分类任务结果

Tab. 5 Results of multi-class classification task on LuFlow and CICIoT2023 datasets %

k	LuFlow			CICIoT2023		
	R_D	A	R_{FP}	R_D	A	R_{FP}
2	99.34 ±0.08	95.88 ±0.07	0.56 ±0.04	99.82 ±0.13	99.19 ±0.11	0.004 7 ±0.002 2
4	99.56 ±0.07	95.79 ±0.03	0.49 ±0.09	99.79 ±0.09	99.07 ±0.09	0.006 6 ±0.002 7
6	99.47 ±0.05	96.08 ±0.09	0.59 ±0.06	99.86 ±0.11	99.10 ±0.08	0.007 8 ±0.004 5
8	99.55 ±0.07	95.97 ±0.05	0.52 ±0.06	99.83 ±0.08	99.25 ±0.13	0.005 6 ±0.003 9
10	99.39 ±0.11	95.83 ±0.06	0.58 ±0.07	99.88 ±0.07	94.16 ±0.11	0.008 8 ±0.002 9

由表 3 可知,CLSA-Net 在 NSL-KDD 和 UNSW-NB15 上的验证平均准确率分别达到了 99.17% 和 95.22%。其中,NSL-KDD 数据集上的最高准确率为 99.66%,而 UNSW-NB15 数据集上的最高准确率为 95.71%。CLSA-Net 在保证高检出率的同时,也维持了较低的误报率。平均来看,NSL-KDD 数据集上的平均检出率为 98.99%,平均误报率为 0.70%,而 UNSW-NB15 数据集上的平均检出率及平均误报率分别为 96.16% 和 1.93%。

由表 4 可知,CLSA-Net 在 CICIDS2017 和

CICIDS2019 中表现较为优异，其中在 CICIDS2019 数据集上的平均检出率达到了 99.23%，平均准确率及误报率分别达到了 99.01% 和 0.07%。

表 5 为 CLSA-Net 在最新的网络入侵检测数据集 LuFlow 和大规模的物联网入侵检测数据集 CICIoT2023 的多分类结果。在 CICIoT2023 数据集 34 种攻击类别情况下，CLSA-Net 的平均检出率为 99.84%，平均准确率为 98.15%，而平均误报率仅为 0.006 7%。

在 NSL-KDD 数据集上，CLSA-Net 展现出了良好的总体检测性能，但在 U2R 和 R2L 两类攻击上检出率明显不足。说明模型未能有效捕获 U2R 和 R2L 攻击的独特鉴别性特征，可能归因于这些攻击模式与其他类别间的特征高度相似。类似地，CLSA-Net 在检测 Worms、Shellcode 和 Backdoor 攻击时也面临同样的问题。

为进一步验证模型在不同训练集划分下的稳定性，图 7 和图 8 分别展示了 CLSA-Net 在 UNSW-NB15 和 NSL-KDD 数据集上，随着交叉验证折数的变化，各攻击类别的检出率与误报率的动态趋势。由图 7 可知，尽管少数类攻击受限于特征混淆，导致检出率较低，但模型在 Normal、Generic、DoS 及 Exploits 等主要类别上表现出较好的稳定性，各项指标曲线相对平滑，随 k 值变化未出现大幅波动，且大多数类别的误报率维持在 1% 以下。而在图 8 中，Normal、DoS 和 Probe 类别的检出率保持在较高水平。值得注意的是，前文提到的 U2R 和 R2L 类别在图 8 中呈现出一定的波动性，这与前述的特征难以捕获的分析一致；但整体而言，CLSA-Net 仍将该数据集上所有类别的误报率控制在较低范围，验证了模型在复杂数据分布下的可靠性。

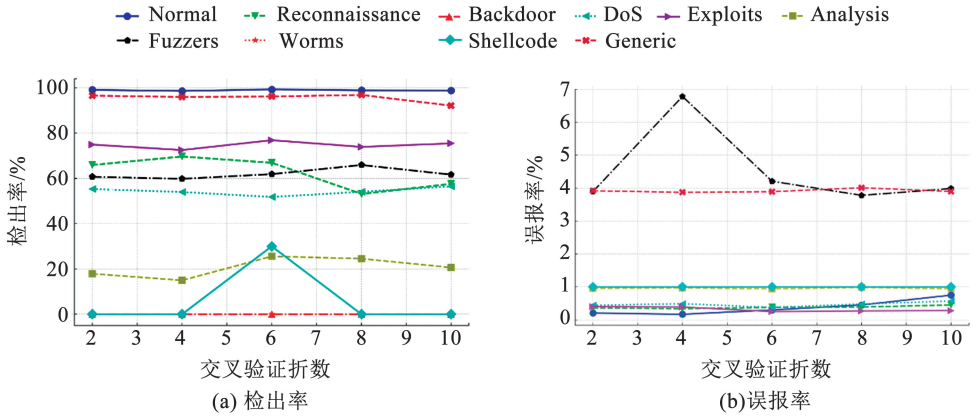


图 7　UNSW-NB15 数据集中多分类比较

Fig. 7　Multi-class classification comparison on UNSW-NB15 dataset

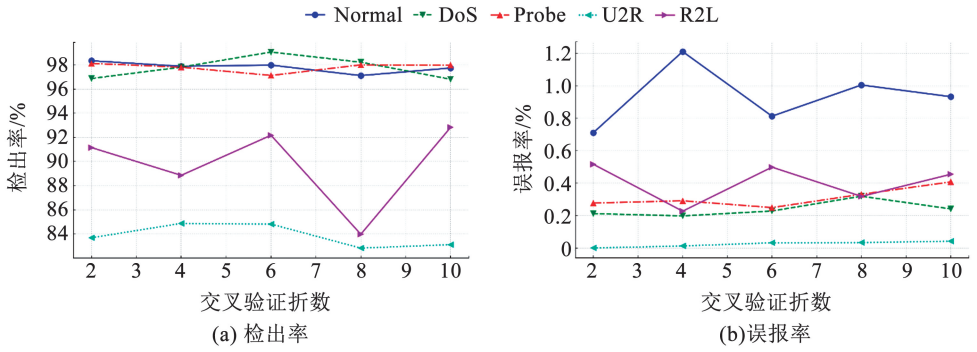


图 8　NSL-KDD 数据集中多分类比较

Fig. 8　Multi-class classification comparison on NSL-KDD dataset

图 9 为当 $k=10$ 时，UNSW-NB15 数据集进行多分类的混淆矩阵。由图 9 可知，CLSA-Net 将大部分 Backdoor、Worms 和 Shellcode 误分类为 Exploits。这种显著的跨类别误分类现象的原因首先可归因于攻击模式的高度相似性，Backdoor、Worms 和 Shellcode 常利用程序漏洞并监听远程连接，导致其攻击签名与 Exploits 的特征高度重叠。此外，严重的类别不平衡问题也制约了模型的性能。这 3 类攻击在数据

集中均属极端稀有类别(占比分别为 0.903%、0.068% 和 0.586%),样本的稀疏性导致模型无法充分学习其独特的鉴别性特征。

图 10 为 CLSA-Net 在 CICIoT2023 数据集上的 34 种攻击的训练结果。由图 10 可以看出,CLSA-Net 对数据集中的多数攻击类别做出了准确检测,但是在面对小样本的攻击类别时还存在一定的局限,如后门恶意软件(Backdoor_Malware)、DDoS ICMP 泛洪攻击(DDoS-ICMP_Flood)、DDoS RST/FIN 泛洪攻击(DDoS_RSTFINFlood)、字典暴力破解(DictionaryBruteForce)、SQL 注入攻击(SqlInjection)、文件上传攻击(Uploading_Attack)并未有效检出。

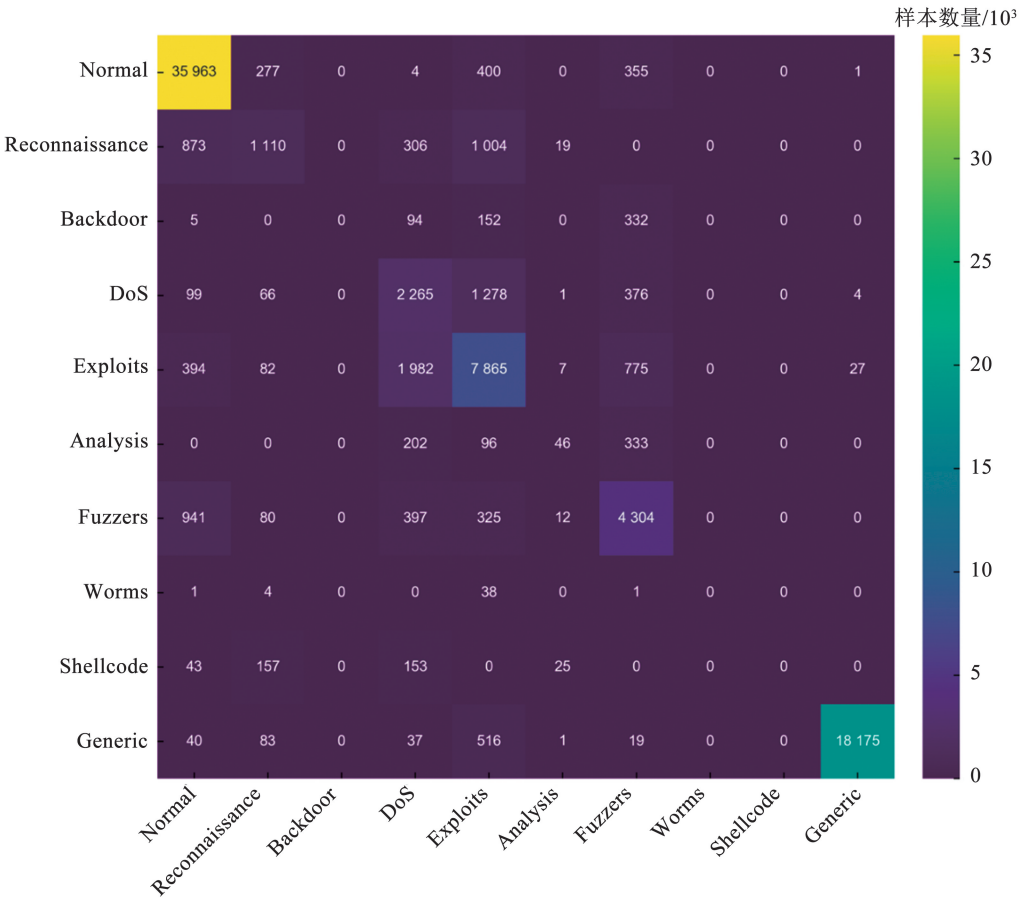


图 9 $k=10$ 时对 UNSW-NB15 数据集进行多分类的混淆矩阵

Fig. 9 Confusion matrix for multi-class classification of the UNSW-NB15 dataset at $k=10$

2.6 消融实验

为验证所提模型中各关键组件的有效性及其对整体性能的贡献,设计了消融实验,对通过逐步添加模块构建的 3 种改进模型变体进行了评估。3 种模型结构具体定义如下:

1) CNN-LSTM:作为基线模型,该结构结合了 CNN 与 LSTM,旨在同时捕捉网络流量的空间特征与时间序列依赖,从而构建基础的全面网络流量表示,以保证基本的泛化能力和预测准确性。

2) CNN-LSTM-Self-Attention:在基线模型的基础上引入自注意力机制,旨在更好地捕捉输入数据的长距离依赖性和关键特征。该改进旨在提升模型对复杂攻击模式的理解能力与检测精度,使其在处理复杂的网络入侵行为时表现出更显著的优势。

3) CNN-LSTM-Encoding-Self-Attention:针对网络流量数据模式复杂、结构多变,导致仅引入注意力机制的模型在训练过程中可能产生波动的问题,该模型进一步引入了编码技术。此改进旨在增强模型对流量时序与位置信息的感知,从而提高模型的训练稳定性与综合处理能力。

本研究选取复杂度较高且具有代表性的 UNSW-NB15 数据集作为实验对象,对上述 3 种模型进行对比测试,具体实验结果见表 6。

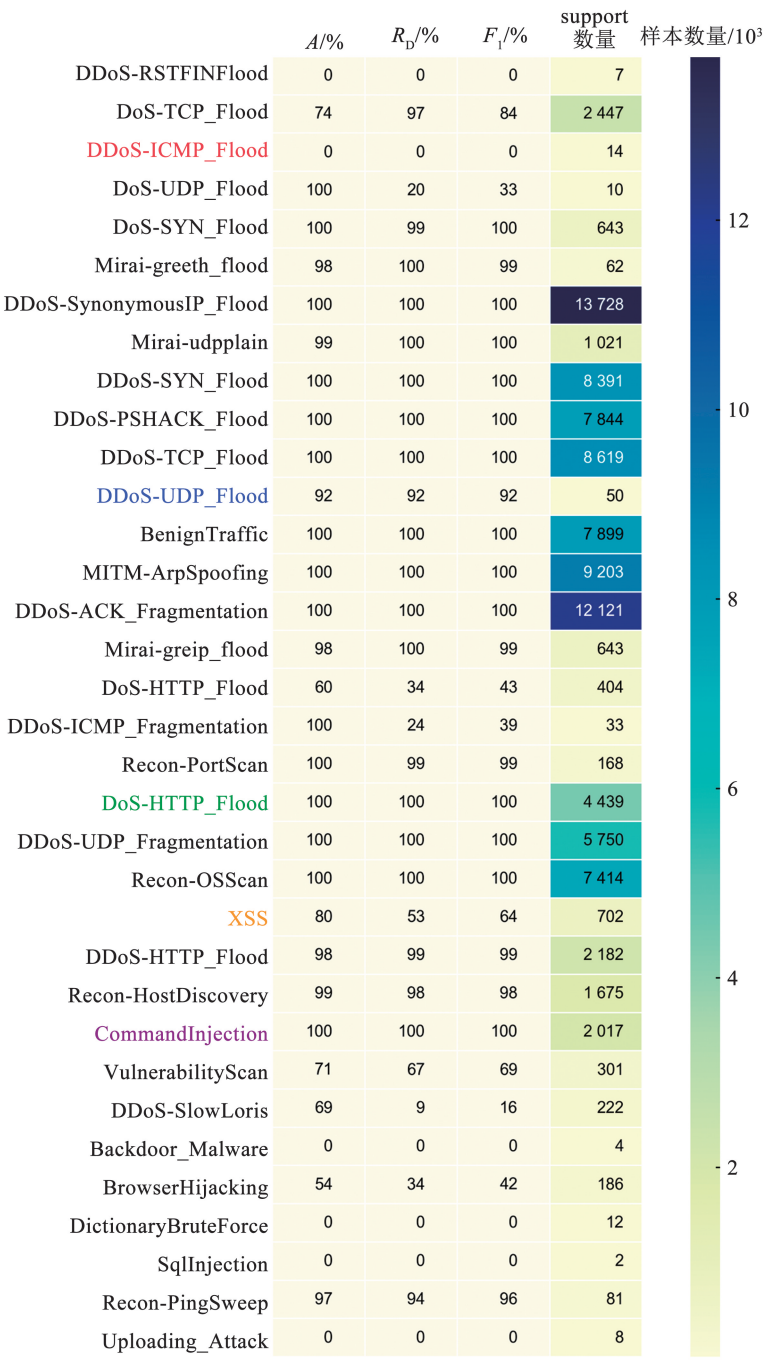


图 10　$k=10$ 时 CICIoT2023 数据集 34 种攻击类别的分类报告

Fig. 10　Classification report for 34 attack categories in the CICIoT2023 dataset at $k=10$

表 6　3 种改进模型的消融实验结果

Tab. 6　Results of ablation experiment with three improved models　%

模型	R_D	A	R_{FP}
CNN-LSTM	95.073	83.521	2.893
CNN-LSTM-Self-Attention	95.862	94.983	2.378
CNN-LSTM-Encoding-Self-Attention	96.162	95.221	1.931

由表 6 可以看出模型各组件的增量贡献。基线模型 CNN-LSTM 结合了 CNN 的空间特征提取与 LSTM 的时间序列分析能力，检出率和准确率分别达到了 95.073% 和 83.521%。在此基础上，引入自注意力机制的 CNN-LSTM-Self-Attention 模型带来了性能提升，其准确率提升了 11.462%，误报率降低了 0.515%，有力地证明了自注意力机制在提升检测精度上的关键作用。然而，该模型在训练过程中也暴露了误报率指标波动较大的不稳定性。为了解决此问题，CNN-LSTM-Encoding-Self-Attention 进一步集成了编码技术。此举不仅使模型的检测性能得到进一步优化，还显著提升了模型的稳定性。

为直观验证编码技术对模型稳定性的贡献，图 11 对比了引入位置编码前后的误报率散点分布。由图 11可以看出：未采用位置编码时，误报率散点

分布较为离散,显示出随机波动;而引入该技术后,散点在低误报率区域的分布更为集中,纵向离散度明显减小,说明位置编码有效增强了模型的稳定性。

此外,图 12、图 13 记录了 CLSA-Net 在 100 轮(epoch)训练过程中的性能散点轨迹。由图 12、图 13可以看出:模型表现出极快的收敛特性,仅在训练初期的前 3 个 epoch,准确率散点即迅速跃升至 90% 以上。随着训练推进,各项指标散点逐渐在最优值附近形成紧密聚集态势,损失函数同步收敛至较低水平。

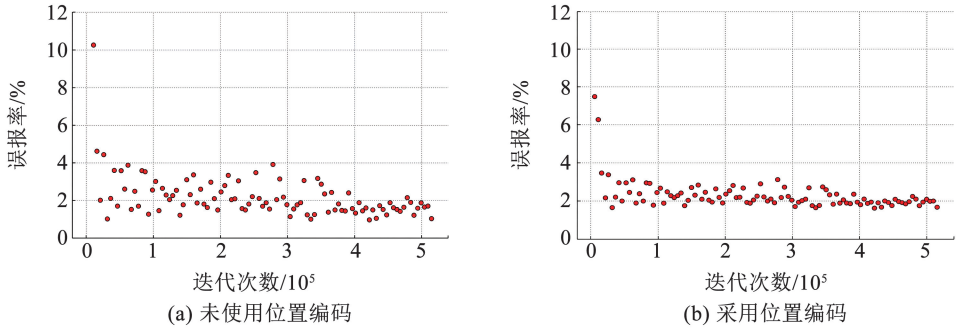


图 11 误报率对比

Fig. 11 Comparison of false alarm rates

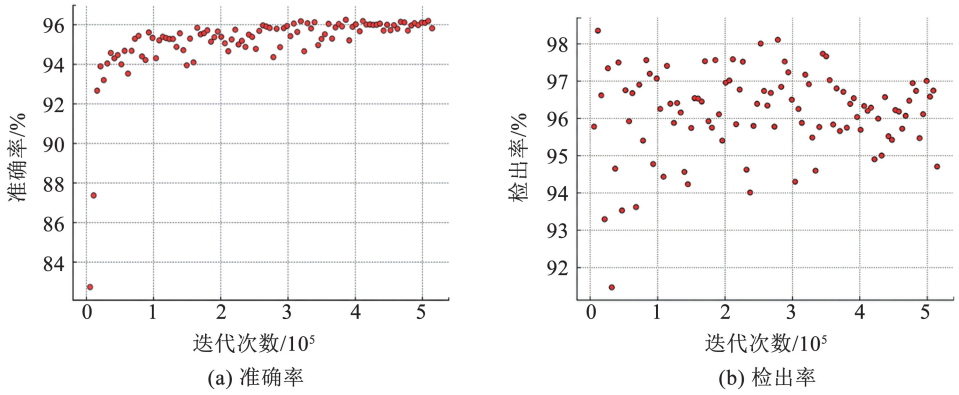


图 12 UNSW-NB15 数据集上模型训练过程中准确率与检出率变化

Fig. 12 Changes in accuracy and detection rate during training on UNSW-NB15 dataset

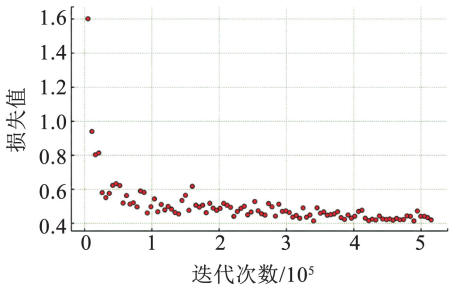


图 13 UNSW-NB15 数据集上模型训练过程中损失值变化

Fig. 13 Changes in loss during training on UNSW-NB15 dataset

综上所述,自注意力机制显著提升了检测精度,而编码技术关键性地解决了稳定性问题。两者协同作用,确保了模型在保持高准确率的同时具备优异的鲁棒性。

2.7 对比研究

为验证 CLSA-Net 的有效性,选取多种基线模型进行性能对比。这些模型包括传统机器学习模型,如使用高斯核的支持向量机(SVM)[6]、随机森林(RF)[7]、自适应增强(AdaBoost)[8]、多层感知机(MLP)[20]等;近年来的深度学习模型,如 LuNet[5]、CNN-BiLSTM[9]、HAST-IDS[21]等;最新的深度学习模型,如 D-CFA[27]、前馈神经网络(feed-forward neural networks, FFNN)[28]、双重入侵检测系统(Dual-IDS)[29]、简单循环神经网络(SimpleRNN)[30]、基于行为的威胁分析(BTA-IDS)[31]和先进的 CANET 模型[32]等。在 UNSW-NB15 和 CICIoT2023 数据集的交叉验证结果见表 7 和表 8。

由表 7、表 8 可知,CLSA-Net 在关键性能指标上的综合表现优于传统的机器学习模型和其他先进的深度学习模型。在 CICIoT2023 数据集上,CLSA-Net 表现优异,其平均误报率仅为 0.006 7%,同时准确率保持在 99% 以上。在全部 34 种攻击中,绝大多数被成功检出,但也有少数训练样本严重不足的稀有类别未能被理想分类。

表 7　基于 UNSW-NB15 数据集的 16 种分类模型的交叉验证结果

Tab. 7　Cross-validation results of 16 classification models on UNSW-NB15　%

模型	R_D	A	R_{FP}
LuNet[5]	97.43	85.35	2.89
SVM(RBF)[6]	83.71	74.80	7.73
RF[7]	92.24	84.59	3.01
AdaBoost[8]	91.13	73.19	22.11
CNN[9]	92.28	82.13	3.84
CNN-BiLSTM[9]	92.56	82.08	6.09
MLP[20]	96.74	84.00	3.66
LSTM[20]	92.76	82.40	3.63
HAST-IDS[21]	93.65	80.03	9.60
D-CFA[27](2020)	—	92.12	—
FFNN[28](2023)	—	94.00	—
Dual-IDS[29](2023)	92.12	92.24	4.38
SimpleRNN[30](2023)	93.38	87.07	—
BTA-IDS[31](2023)	93.07	94.48	3.54
CANET[32](2023)	97.84	87.53	2.66
CLSA-Net	96.16	95.22	1.93

表 8　基于 CICIoT2023 数据集的 14 种分类模型的交叉验证结果

Tab. 8　Cross-validation results of 14 classification models on CICIoT2023　%

模型	R_D	A	F_1
LogisticRegression[33](2023)	59.52	80.23	49.38
Perceptron[33](2023)	50.75	81.95	44.72
AdaBoost[33](2023)	60.76	60.78	47.34
RF[33](2023)	83.15	99.16	71.40
Extra Trees[33]	94.08	97.07	94.57
Gradient Trees[33]	95.39	96.40	94.89
DNN[33](2023)	73.18	98.61	67.23
MLP[33](2024)	97.00	97.47	97.00
Autoencode(AE)[24](2024)	84.00	83.92	80.00
LSTM[24](2024)	98.75	98.75	98.59
Blending[24]	99.63	99.51	99.07
PCC-CNN[34](2023)	87.00	85.00	86.00
RFMRMR + BRFC[35](2023)	83.13	99.55	95.23
CLSA-Net	99.84	99.19	99.17

需要指出的是，LuNet 模型在结构上采用了 CNN 与 RNN 的级联结构，虽在 NSL-KDD 和 UNSW-NB15 数据集上表现良好，但 RNN 在处理长序列时易发生遗忘，导致其在 UNSW-NB15 等复杂数据集上的特征提取能力受限[5]。另一方面，CANET 采用注意力机制关注全局的时序信息，避免了训练过程中丢失时序信息的问题。尽管其在 NSL-KDD、CICIDS2017 和 CICIDS2019 等基准数据集上展现出了良好的检测性能，但其依赖单一注意力机制，在面对复杂数据集时，暴露了其在处理全局时序信息方面的局限性[32]。因此，搭配 RNN 的注意力机制能更好捕获全局时序信息，并搭配位置编码进行加权处理。

尽管 LuNet、D-CFA 及 CANET 等先进模型在检出率与准确率方面已取得优异的效果，但在衡量模型综合鲁棒性的误报率与 F_1 分数指标上，本文提出的 CLSA-Net 表现更为均衡且优异。与 LuNet、Dual-IDS 等存在明确误报率数据的模型相比，CLSA-Net 显著降低了误报风险；同时，在 F_1 分数上也优于 Blending 及 RFMRMR + BRFC。这种均衡的性能表现归功于其独特的混合架构，即通过 CNN 模块实现高效的特征提取，并结合 LSTM 精确捕获数据的时间序列依赖性，从而提升了模型对复杂网络攻击行为的识别与预测能力。

3　结　论

1）针对传统模型在多分类任务中特征提取能力不足且难以在微控制器上部署的问题，提出了一种 CLSA-Net 深度学习模型。该模型通过自适应卷积模块、长短期记忆网络与改进自注意力机制级联结构，有效增强了对时序流量中多样化攻击特征的捕捉能力。同时，通过结合 TFLite 模型量化与转换技术，成功解决了复杂深度学习模型在低算力、低存储物联网设备上的适配难题。

2）基于 UNSW-NB15 和 CICIoT2023 等多个基准数据集的对比实验表明，CLSA-Net 在多分类入侵检测任务中表现卓著，综合检出率与准确率分别达到了 98.60% 和 97.48%。该结果证实了其在处理高维、非线性网络流量数据时，相比现有主流模型具有更高的分类精度和泛化能力。

3）本研究成功将优化后的模型部署于 ESP32-S3 微控制器平台。实测结果显示，在边缘计算资源极其受限的条件下，系统仍保持了超过 80% 的检测准确率，并实现了低功耗下的实时推理。这一成果有效平衡了模型复杂度与硬件性能约束，验证了在物联网边缘侧部署高性能入侵检测系统的可行性，为物联网安全防御提供了一种具备实际应用价值的解决方案。

参考文献

[1] Bhuyan M H, Bhattacharyya D K, Kalita J K. Network anomaly detection: methods, systems and tools[J]. IEEE Communications Surveys & Tutorials, 2014, 16(1): 303. DOI: 10.1109/SURV.2013.052213.00046

[2] Kwon D, Kim H, Kim J, et al. A survey of deep learning-based network anomaly detection[J]. Cluster Computing, 2019, 22: 949. DOI: 10.1007/s10586-017-1117-8

[3] Hubballi N, Suryanarayanan V. False alarm minimization techniques in signature-based intrusion detection systems: a survey[J]. Computer Communications, 2014, 49: 1. DOI: 10.1016/j.comcom.

2014. 04. 012
[4] Mukherjee B, Heberlein L T, LEVITT K N. Network intrusion detection[J]. IEEE Network, 1994, 8(3): 26. DOI:10. 1109/65. 283931
[5] Wu Peilun, Guo Hui. LuNet: a deep neural network for network intrusion detection [C]//2019 IEEE Symposium Series on Computational Intelligence (SSCI). Xiamen: IEEE, 2019: 617. DOI:10. 1109/SSCI44817. 2019. 9003126
[6] Ahmad I, Basheri M, Iqbal M J, et al. Performance comparison of support vector machine, random forest, and extreme learning machine for intrusion detection[J]. IEEE Access, 2018, 6: 33789. DOI:10. 1109/ACCESS. 2018. 2841987
[7] Zhang Jiong, Zulkernine M, Haque A. Random-forests-based network intrusion detection systems [J]. IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), 2008, 38(5): 649. DOI:10. 1109/TSMCC. 2008. 923876
[8] Hu Weiming, Gao Jun, Wang Yanguo, et al. Online adaboost-based parameterized methods for dynamic distributed network intrusion detection[J]. IEEE Transactions on Cybernetics, 2013, 44(1): 66. DOI:10. 1109/TCYB. 2013. 2247592
[9] Sinha J, Manollas M. Efficient deep CNN-BiLSTM model for network intrusion detection [C]//Proceedings of the 3rd International Conference on Artificial Intelligence and Pattern Recognition. Xiamen: ACM, 2020: 223. DOI:10. 1145/3430199. 3430224
[10] Azizion M, Jumabek A, Kim W. 1D CNN based network intrusion detection with normalization on imbalanced data [C]//2nd International Conference on Artificial Intelligence in Information and Communication (ICAIIC). Fukuoka: IEEE, 2020: 218. DOI:10. 1109/ICAIIC48513. 2020. 9064976
[11] Khan R U, Zhang Xiaosong, Alazab M, et al. An improved convolutional neural network model for intrusion detection in networks[C]//2019 Cybersecurity and Cyberforensics Conference (CCC). Melbourne: IEEE, 2019: 74. DOI: 10. 1109/CCC. 2019. 000 - 6
[12] Vinayakumar R, Soman K P, Poornachandran P. Evaluation of recurrent neural network and its variants for intrusion detection system (IDS) [J]. International Journal of Information System Modeling and Design (IJISMD), 2017, 8(3): 43. DOI:10. 4018/IJISMD. 2017070103
[13] Hochreiter S, Schmidhuber J. Long short-term memory[J]. Neural Computation, 1997, 9(8): 1735. DOI:10. 1162/neco. 1997. 9. 8. 1735
[14] Anani W, Samarabandu J. Comparison of recurrent neural network algorithms for intrusion detection based on predicting packet sequences[C]//2018 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE 2018). Quebec City: IEEE, 2018: 8447793. DOI:10. 1109/CCECE. 2018. 8447793
[15] Lecun Y, Bengio Y, Hinton G. Deep learning[J]. Nature, 2015, 521(7553): 436. DOI:10. 1038/nature14539
[16] Zhou Y T, Chellappa R. Computation of optical flow using a neural network [C]//IEEE 1988 International Conference on Neural Networks. San Diego: IEEE, 1988: 71. DOI:10. 1109/ICNN. 1988. 23914
[17] Ioffe S, Szegedy C. Batch normalization: accelerating deep network training by reducing internal covariate shift[C]//32nd International Conference on Machine Learning. Lile: IMLR, 2015: 448
[18] Lin Yun, Wang Jie, Tu Ya, et al. Time-related network intrusion detection model: a deep learning method[C]//2019 IEEE Global Communications Conference (GLOBECOM). Waikoloa: IEEE, 2019: 9013302. DOI:10. 1109/GLOBECOM38437. 2019. 9013302
[19] Phan H, Nguyen H L, Chen O Y, et al. Self-attention generative adversarial network for speech enhancement [C]//2021 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). Toronto: IEEE, 2021: 7103. DOI:10. 1109/ICASSP39728. 2021. 9414265
[20] Esmaly J, Moradinezhad R, Ghasemi J. Intrusion detection system based on multi-layer perceptron neural networks and decision tree [C]//7th Conference on Information and Knowledge Technology (IKT). Urmia: IEEE, 2015: 7288736. DOI:10. 1109/IKT. 2015. 7288736
[21] Wang Wei, Sheng Yiqiang, Wang Jinlin, et al. HAST-IDS: learning hierarchical spatial-temporal features using deep neural networks to improve intrusion detection[J]. IEEE Access, 2017, 6: 1792. DOI:10. 1109/ACCESS. 2017. 2780250
[22] Dhanabal L, Shantharajah S P. A study on NSL-KDD dataset for intrusion detection system based on classification algorithms[J]. International Journal of Advanced Research in Computer and Communication Engineering, 2015, 4(6): 446. DOI:10. 17148/IJARCCE. 2015. 4696
[23] Moustafa N, Slay J. UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)[C]//2015 Military Communications and Information Systems Conference (MilCIS). Canberra: IEEE, 2015: 1. DOI:10. 1109/MilCIS. 2015. 7348942
[24] Jony A I, Arnob A K B. A long short-term memory based approach for detecting cyber attacks in IoT using CICIoT2023 dataset[J]. Journal of Edge Computing, 2024, 3(1): 28. DOI:10. 55056/jec. 648
[25] Kohavi R. A study of cross-validation and bootstrap for accuracy estimation and model selection [C]//Proceedings of the 14th International Joint Conference on Artificial Intelligence (IJCAI). San Mateo: Morgan Kaufmann, 1995: 1137
[26] Hinton G, Srivastava N, Swersky K. Lecture 6a overview of mini-batch gradient descent[EB/OL]. [2024-01-05]. https://class. coursera. org/neuralnets - 2012 - 001/lecture
[27] Al-Daweri M S, Ariffin K A Z, Abdullah S, et al. An analysis of the KDD99 and UNSW-NB15 datasets for the intrusion detection system[J]. Symmetry, 2020, 12(10): 1666. DOI: 10. 3390/sym12101666
[28] Telidevara M, Kothandaraman D. Improving intrusion detection in Internet of Things networks with feed-forward neural networks based on the UNSW-NB15 dataset[C]//14th International Conference on Computing Communication and Networking Technologies (ICCCNT 2023). Delhi: IEEE, 2023: 1. DOI: 10. 1109/ICCCNT56998. 2023. 10307804
[29] Louk M H L, Tama B A. Dual-IDS: a bagging-based gradient boosting decision tree model for network anomaly intrusion detection system[J]. Expert Systems with Applications, 2023, 213: 119030. DOI:10. 1016/j. eswa. 2022. 119030
[30] Kasongo S M. A deep learning technique for intrusion detection system using a recurrent neural networks based framework[J]. Computer Communications, 2023, 199: 113. DOI: 10. 1016/j. comcom. 2022. 12. 010
[31] 方介波, 陶重犇. 应对零日攻击的混合车联网入侵检测系统[J]. 计算机应用, 2024, 44(9): 2763
Fang Jiepo, Tao Chongben. Hybrid internet of vehicles intrusion detection system for zero-day attacks[J]. Journal of Computer Applications, 2024, 44(9): 2763. DOI:10. 11772/j. issn. 1001 - 9081. 2023091328
[32] Ren K, Yuan Shuai, Zhang Chun, et al. CANET: a hierarchical CNN-Attention model for network intrusion detection[J]. Computer Communications, 2023, 205: 170. DOI: 10. 1016/j. comcom. 2023. 04. 018
[33] Neto E C P, Dadkhah S, Ferreira R, et al. CICIoT2023: a real-time dataset and benchmark for large-scale attacks in IoT environment[J]. Sensors, 2023, 23(13): 5941. DOI:10. 3390/s23135941
[34] Bhavsar M, Roy K, Kelly J, et al. Anomaly-based intrusion detection system for IoT application[J]. Discover Internet of Things, 2023, 3(1): 5. DOI:10. 1007/s43926 - 023 - 00034 - 5
[35] Narayan K R, Mookherji S, Odelu V, et al. IIDS: design of intelligent intrusion detection system for internet-of-things applications [C]//7th IEEE Conference on Information and Communication Technology (CICT). Jabalpur: IEEE, 2023: 1. DOI:10. 1109/CICT59886. 2023. 10455720