研究与开发

# 基于多尺度残差时间卷积网络的物联网入侵检测模型

刘丽伟[1]，赵红超[1]，李学威[2]，孙滨[1]
（1. 郑州工业应用技术学院大数据信息管理中心，河南 郑州 451150；
2. 周口职业技术学院信息工程学院，河南 周口 466002）

**摘　要：**入侵检测可主动鉴别物联网流量攻击，它是维护物联网安全的重要措施。为此，提出基于多尺度残差时间卷积网络的入侵检测模型（multiscale residual temporal convolutional networks-based intrusion detection model，MRID）。MRID采用多尺度残差时间卷积模块，以增强网络学习时空的表征能力。同时，MRID采用了一个改进的流量注意力机制，帮助模型在学习过程中更关注重要特征。MRID可便捷应用于基于雾层的物联网架构中，以提供高效的实时入侵检测。利用数据集CICIDS2017和CSE-CIC-IDS2018验证MRID的性能。性能分析表明，MRID提高了入侵检测的效率，并在保持计算效率的同时，增强了模型的鲁棒性。

**关键词：**物联网；入侵检测模型；时间卷积网络；多尺度残差；注意力机制
**中图分类号：**TN929.5
**文献标志码：**A
**doi:** 10.11959/j.issn.1000−0801.2025046

# Multiscale residual temporal convolutional networks-based intrusion detection model in Internet of things

LIU Liwei[1], ZHAO Hongchao[1], LI Xuewei[2], SUN Bin[1]
1. Big Data Information Management Center, Zhengzhou University of Industrial Technology, Zhengzhou 451150, China
2. College of Information and Engineering, Zhoukou Vocational and Technical College, Zhoukou 466002, China

**Abstract:** Intrusion detection can actively identify Internet of things (IoT) traffic attacks, which is an important measure to maintain IoT security. Therefore, multiscale residual temporal convolutional networks-based intrusion detection model (MRID) was proposed. In MRID, a multiscale residual temporal convolutional module was utilized to enhance the network capability in learning spatiotemporal representations. An improved traffic attention mechanism was introduced to estimate the importance score that helps the model to concentrate on important information during leaning. The proposed MRID was easily integrated into a fog-enabled IoT to offer efficient real-time intrusion detection. Finally, empirical evaluations on two recent datasets (CICIDS2017 and CSE-CIC-IDS2018) were conducted, demon-

收稿日期：2024−11−10；修回日期：2025−02−14
基金项目：河南省科技厅科技攻关支持项目（No.232102210200）；河南省高等学校重点科研项目（No.23B520036）
**Foundation Items:** The Key Scientific and Technological Research Project of Henan Provincial Department of Science and Technology (No. 232102210200), The Key Scientific Research Project of Henan Provincial Colleges and Universities (No.23B520036)

strating that MRID improved the efficiency of intrusion detection and increased the robustness of model while maintaining computational efficiency.

**Key words:** IoT, intrusion detection model, temporal convolutional network, multiscale residual, attention mechanism

## 0　引言

物联网（Internet of things，IoT）技术是信息通信技术领域的重要研究方向，其发展不仅提高了生产效率[1-2]，也便捷了人们的日常生活。但是，海量的IoT流量在各IoT设备之间传输，容易遭受网络攻击[3]（如DDoS攻击、数据窃取等）。尽管传统互联网中已有许多安全解决方案（如防火墙、入侵检测系统（intrusion detection system，IDS）等），但由于IoT设备在物理层上的资源限制（如计算能力、存储能力和能源限制）及节点间的异构性（如设备类型、通信协议和操作系统的多样性），这些安全解决方案并不适用于IoT环境。

入侵检测系统是近年来发展起来的一种动态监控、预防和抵御入侵行为的安全机制[4-5]，能为保护IoT安全提供有力保障。基于异常检测的IDS需要先构建正常流量的数据分布，若检测流量的数据分布与正常流量的数据分布不匹配，则将该流量判为入侵攻击，进而保护IoT免受网络攻击。

然而，IoT所连接的设备的计算资源、通信技术、电池容量、软件和操作系统都不尽相同，所遭受的入侵攻击是多样的，且可能是未知的，这给检测入侵攻击提出了挑战。传统的机器学习（machine learning，ML）算法[6]已被证明可以有效地识别IoT流量中的重要模式，从而有力地识别网络攻击。然而，ML也被证明无法扩展到巨大的数据集（即数百万条记录，具有100多个特征）。而深度学习（deep learning，DL）算法的不断改进推动了新IDS的演变，这使IDS能够很好地应对攻击。因此，本文提出了一种新的基于DL的入侵检测模型。

由于IoT流量是按顺序产生的，可以将其作为时间序列数据处理。循环神经网络（recurrent neural network，RNN）已被证实可有效处理这类数据，且表现出良好的性能。其中，长短期记忆（long short-term memory，LSTM）和门控循环单元（gated recurrent unit，GRU）是RNN的增强版，用于各种顺序数据应用[7]。但是RNN存在梯度消失问题，并且训练RNN的时间较长。

近期，由于强的空间特征提取能力，卷积神经网络（convolutional neural network，CNN）也用于入侵检测。但是CNN涉及的参数较多，训练CNN需要占用大量的计算资源。此外，CNN模型的解释性较差。这些不足在一定程度上限制了CNN在IDS中的应用。

为了克服CNN的不足，需要对CNN进行改进。时间卷积网络（temporal convolutional network，TCN）就是CNN的增强版。TCN的结构简单，更适应于资源受限的IoT系统，且TCN在许多序列问题中取得了比LSTM更好的性能。

为此，本文将采用TCN构建入侵检测模型。利用TCN构建入侵检测模型的原因如下。

（1）TCN在训练过程中更为稳定且效率更高。TCN采用因果卷积和膨胀卷积，能够有效捕捉长期依赖关系，有效地避免梯度消失或爆炸问题。此外，TCN在处理序列数据时不需要像CNN那样进行大规模并行处理，因此不会受到内存限制的影响，缩短了训练时间。

（2）TCN具有强大的并行处理能力。TCN可以并行处理所有时间同步的数据，而RNN必须按序处理。

（3）TCN能捕捉更长序列的依赖关系。TCN通过膨胀卷积扩大了卷积层的感觉野，增强了捕

捉更长的序列依赖关系的能力，并且不增加参数数量。

此外，为了提升训练模型的效率和充分利用云层的丰富资源，本文采用基于雾层的IoT架构。由云层训练模型，并将已完成训练的模型部署在雾层。

为此，本文针对基于雾层的IoT架构，提出基于多尺度残差时间卷积网络入侵检测模型（multi-scale residual temporal convolutional networks-based intrusion detection model，MRID）。MRID利用多尺度残差和注意力机制构建TCN，利用扩张因果卷积（dilated causal convolution，DCC）替代传统卷积网络，克服传统卷积网络的不足。通过引用多尺度残差时序卷积块，增强网络捕获时空表征能力。而采用注意力机制使模型在训练模型时更关注重要特征。通过数据集CICIDS2017和CSE-CIC-IDS2018验证MRID的性能。性能分析表明，MRID提升了检测攻击的精度，并缩短了检测攻击的时间。该结果进一步证实了MRID具有强大的特征学习和时空表征的能力。

## 1 基于雾层的IoT入侵检测框架

基于雾层的IoT入侵检测系统模型如图1所示。该模型由云层、雾层和边缘层组成。考虑到云层具有强大的计算资源，且训练模型时需要访问大量的IoT流量数据，由云层训练入侵检测模型，有利于聚合流量数据，并可将数据存储在云中。

雾层往往由雾服务器/设备组成，使计算更接近IoT的边缘，降低处理时延。由于雾层是检测入侵样本的实时位置，在MRID中扮演着重要作用。具体而言，雾节点主要由3个模块组成：流量聚合模块、流量预处理模块和流量诊断模块。

流量聚合模块负责从边缘IoT的连接部分捕获和接收IoT的流量记录，然后将批量样本传递给流量预处理模块。流量预处理模块对流量数据

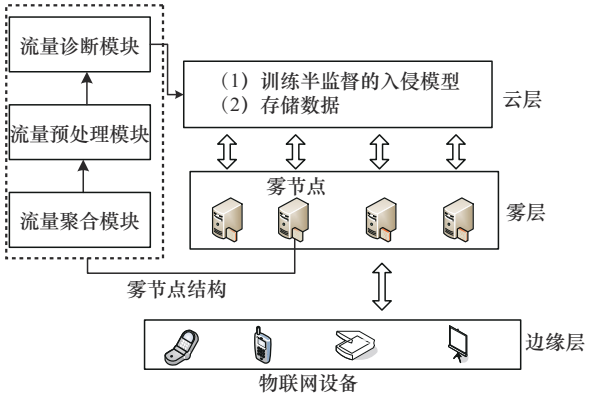


图1 基于雾层的IoT入侵检测系统模型

进行预处理，包括格式转换、数据清洗和规范化。随后进入流量诊断模块。在诊断模块，利用已训练的MRID对流量进行分类，无须与云后端进行任何通信，避免了不必要的通信时延。一旦检测到攻击，就将此流量传输至云端。

边缘层由边缘节点和边缘设备（即笔记本计算机、智能手机、智能手表等）组成，这些节点通过路由和交换设备与IoT进行通信，同时与特定的雾服务器/节点连接，作为到云后端的计算桥梁。

## 2 MRID构架

MRID由3个主要模块组成：多尺度残差模块（multiscale residual module，MS-Res）、流量注意力模块和检测输出模块。首先，利用MS-Res捕获时空表征能力，并将流量注意力模块以并行方式融入MRID，与MS-Res形成并行结构，进而量化输入数据的重要性，提升提取表征能力更强的特征。之后，通过反馈层（feed forward，FF）和分类层，输出最终的分类结果。MRID构架如图2所示。

### 2.1 MS-Res

由于CNN缺乏长期依赖性的记忆机制，它不适合对序列数据建模。作为CNN的增强版，TCN可有效弥补CNN在处理序列数据方面上的不足。为此，利用TCN构建MS-Res，以构建高

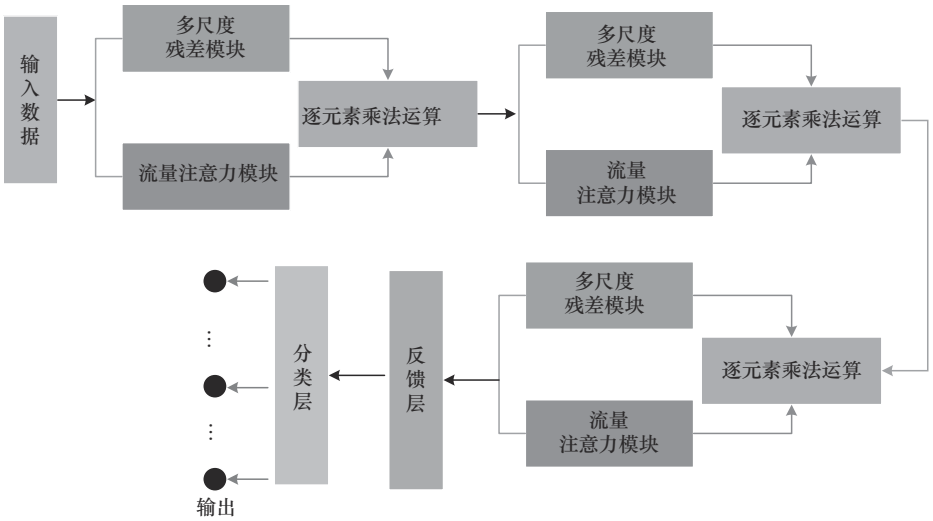


图2　MRID 构架

效的入侵检测模型。

DCC 是 TCN 的关键组件，而 DCC 是因果卷积的变体。与普通卷积不同，因果卷积在处理数据时，只考虑当前时刻及之前的输入数据，而未考虑未来时刻的数据。这种特性使得因果卷积在处理时间序列数据时能够保持数据的时序一致性，未来不会出现信息泄露的问题。

具体而言，对于一个输入序列 $x=(x_0,x_1,\cdots,x_{t-1},x_t)\in \boldsymbol{R}^n$ 和一个卷积核 $f$，它在时刻 $t$ 上的因果卷积可表示为：

$$F(t)=\sum_{i=0}^{k-1} f(i)x_{t-i} \tag{1}$$

其中，$f$ 是一个卷积核，且 $f:\{0,\cdots,k-1\}\rightarrow \boldsymbol{R}$；$k$ 为卷积核大小；$t-i$ 表示时刻 $t$ 之前的 $i$ 时刻。

然而，因果卷积存在覆盖历史信息不足的问题，并且因果卷积需要用非常大的核尺寸 $k$ 或非常深的模型才能具有较大的感受野，从而使模型覆盖更多的历史信息。然而，大的 $k$ 值可能会阻止网络收敛[8]，降低模型的检测精度。此外，增加网络深度就加重训练模型的工作，降低模型的训练效率。

为了克服上述问题，TCN 采用 DCC 代替卷积网络，进而降低训练模型的复杂度。DCC 通过膨胀因子 $d$ 调整网络深度。因此，采用 DCC，TCN 不仅可以在不增大 $k$ 值的环境下扩大感受野，还可以降低运算量。DCC 的操作过程可表述为：

$$F(t)=\sum_{i=0}^{k-1} f(i)\cdot x_{t-d\cdot i} \tag{2}$$

其中，$d$ 为膨胀因子。膨胀因子的取值与残差块（或者隐藏层）所在的层数有关。若残差块在第 1 层，则 $d=2^0=1$；若残差块在第 2 层，则 $d=2^1=2$；若残差块在第 3 层，则 $d=2^2=4$，以此类推。若残差块在第 $i$ 层，则膨胀因子 $d=2^{i-1}$。

一个 DCC 示例如图 3 所示。在图 3 中，共有 5 层，第一层为输入层；中间有 3 个隐藏层，它们的膨胀因子分别为 1、2、4；最后一层（即输出层）的膨胀因子为 8。

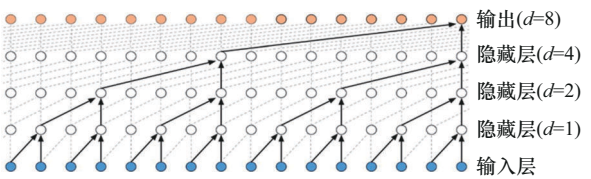


图3　一个 DCC 示例

尽管采用 DCC 可在不增加 TCN 复杂度的情况下扩大感受野，但是 TCN 稳定性并不够。为此，在 TCN 结构中引入残差模块，形成基于残差

结构的TCN，如图4所示。

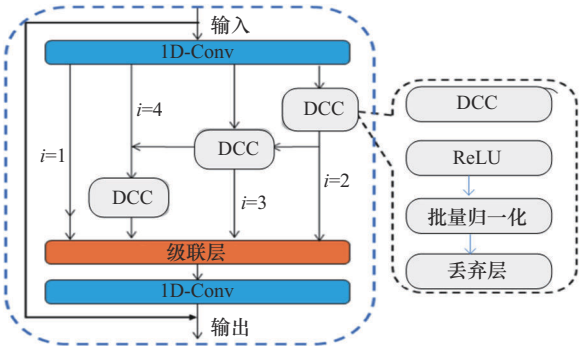


图4　基于残差结构的TCN

在图4中，输入数据先通过一维卷积层（1D-Conv）降低数据的维度，减轻训练模型的工作量。然后，将1D-Conv的输出（令$f_1$表示输出）以4个并行路径的形式传递。最靠左的路径不对$f_1$进行任何处理，直接将$f_1$传输至级联层（Concatenation）。其余的3条路径均经DCC层处理。利用DCC层替代传统的卷积层的目的在于降低模型的复杂度，减少训练模型的时间。

令$F_i$表示第$i$条路径的输出，且$i=1,2,3,4$。最靠左边的是第1条路径（$i=1$），最右边的是第2条路径（$i=2$），然后是第3条路径（$i=3$）和第4条路径（$i=3$）。据此，图4中的4条路径的输出可表述为：

$$F_i=\begin{cases} f_i, & i=1 \\ \mathrm{DCC}(f_1), & i=2 \\ \mathrm{DCC}(f_1+F_{i-1}), & 2<i\leqslant 4 \end{cases} \tag{3}$$

其中，$\mathrm{DCC}(f_1)$表示$f_1$经DCC层的操作。对于第1条路径（$i=1$）而言，直接将1D-Conv的输出$f_1$输入级联层。对于第2条路径（$i=2$）而言，先将1D-Conv的输出$f_1$输入DCC层，其输出为$\mathrm{DCC}(f_1)$，然后将$\mathrm{DCC}(f_1)$输入级联层；对于第3条路径（$i=3$）和第4条路径（$i=3$）而言，它们路径中DCC层中有2个输入，一个是$f_1$，另一个是DCC层的输出。

此外，图4右侧给出了DCC网络结构，其由基于ReLU的激活函数、批量归一化层和丢弃层（dropout层）构成。批量归一化层的主要作用是在训练期间稳定网络性能，从而加快模型收敛。dropout层用于避免训练过程中的过拟合问题。采用多尺度残差模型的目的在于提高模型对复杂场景的适应性和不同尺度对象的感知能力。

### 2.2　流量注意力模块

MRID引入流量注意力模块，强调流量数据中的重要特征，进而增强模型的性能。令$I^c=\left\{I_1^c,I_2^c,\cdots,I_n^c\right\}$表示输入的流量。流量注意力模块就利用输入的流量数据，计算其重要性：

$$\sigma_j=\frac{\exp\left(I_j^c\cdot w\right)}{\int\exp\left(I_j^c\cdot w\right)} \tag{4}$$

其中，$\sigma_j$表示第$j$个流量（$I_j^c$）的重要性；$w$表示在训练期间优化权重向量。

再依据$\sigma_j$计算当前时刻的上下文特征：

$$g=\sum_j\sigma_j\cdot I_j^c \tag{5}$$

### 2.3　MS-Res和流量注意力模块的融合

由图2可知，MRID需要将MS-Res的输出与流量注意力模块的输出进行逐元素乘法运算。令$W_{\mathrm{Res}}$和$W_{\mathrm{Ta}}$分别表示MS-Res的输出和流量注意力模块的输出，据此将它们的输出表示为：

$$W_{\mathrm{RT}}=W_{\mathrm{Res}}\otimes W_{\mathrm{Ta}} \tag{6}$$

其中，$\otimes$表示逐元素乘法运算。

将流量注意力模块引入MRID，使模型能够获得更具有包容性的上下文表示，进而获取流量序列中更重要的信息特征，即通过降低冗余特征对模型的干扰，帮助模型识别各种IoT特征的重要性。

### 2.4　合并、反馈和分类层

由图2可知，将数据经流量注意力模块和MS-Res融合后，再经FF处理。FF对捕获的时

空信息表征进行编码，使其成为适合预测最终类别标签的线性表示形式。将其线性表示输入分类层，由分类层进行流量分类。分类层采用 Softmax 函数，计算每个类别的概率，具有最高概率的类别被认为是最终的模型预测：

$$\begin{cases} p=\mathrm{Softmax}(X)=\dfrac{\exp(X)}{\int_1^c \exp(X)} \\ \tilde{y}=\arg\max(p) \end{cases} \tag{7}$$

其中，$X$表示FF层的输出；$p$表示概率值；$\tilde{y}$表示模型的最终输出。

此外，通过最小化交叉熵损失训练模型。交叉熵损失函数$L$的表达式如下。

$$L=-\sum\left[y_i\log\tilde{y}_i+(1-y_i)\log(1-\tilde{y}_i)\right] \tag{8}$$

其中，$y_i$表示第$i$类样本的真实标签，而$\tilde{y}_i$表示模型所预测的标签（预测标签）。

### 2.5　执行MRID的总体流程

执行 MRID 的总体流程如图 5 所示。选用典型的 IoT 数据集 CIC-IDS2017[9] 和 CSE-CIC-IDS2018[10-11]，其中数据集 CIC-IDS2017 包含了约 2 830 743 个 IoT 流量样本，有 78 个常规的特征，共有 1 个正常类和 14 个攻击类。

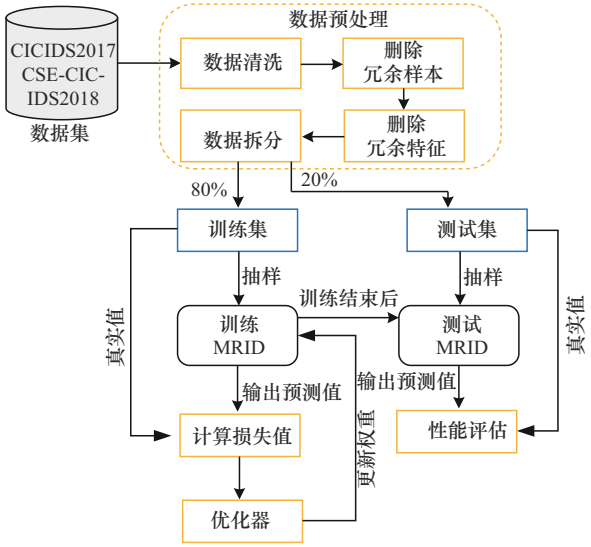


图5　执行MRID的总体流程

数据集 CSE-CIC-IDS2018 有 16 233 002 个样本，包含 79 个特征，且约 17% 的样本属于攻击类。相比于数据集 CICIDS2017，数据集 CSE-CIC-IDS2018 中的数据更为复杂，它是典型的异构入侵数据集。该数据集内的数据存在缺失值、不相关特征、离群值、错误实例和高度差异。

对这 2 个数据集进行清洗，删除一些冗余样本和冗余特征。最终用于训练模型的数据集样本数、特征数和分类数，以及各类样本的数据分布情况见表 1。

MRID 就利用表 1 所列的 CICIDS2017 和 CSE-CIC-IDS2018 数据集中的数据进行训练，并利用训练后的模型对测试样本进行测试。以 CICIDS2017 数据集为例，该数据集经清洗共有 2 827 876 个样本，78 个特征，7 类样本。按分层抽样方法，将这些样本拆分成训练集和测试集。前者用于训练 MRID，后者用于测试模型。

## 3　性能分析

利用 Python 3.7，并结合 TensorFlow 和 Keras API 构建实验平台。执行程序的 PC 机的主要参数为：Intel Xeon E52670 CPU@2.60 GHz，256 GB RAM。

### 3.1　性能指标

利用准确率、召回率、精确率和 F1 值（F1-score）4 个指标评估 MRID 模型的性能，它们依赖于 TP、TN、FP 和 FN。其中，TP 为真阳性（true positive），指模型正确分类为攻击类别的攻击样本数量；FP 为假阳性（false positive），指模型错误分类为攻击类别的攻击样本数量；FN 为假阴性（false negative），指模型错误分类为正常类别的正常样本数量；TN 为真阴性（true negative），指模型正确分类为正常类别的正常样本数量。

准确率（Accuracy）、精确率（Precision）、召回率（Recall）、F1 值的表达式如下。

表1 用于训练和测试的数据情况

| 数据集 | 样本数 | 特征数（分类数） | 数据分布 | | |
|---|---|---|---|---|---|
| | | | 类别 | 训练 | 测试 |
| CICIDS2017 | 原样本数：2 830 743<br>清洗后样本数：<br>2 827 876 | 78（7） | 良性（Benign） | 1 816 543 | 454 135 |
| | | | 机器人攻击（Bot） | 1 544 | 385 |
| | | | 拒绝服务攻击（DoS） | 304 419 | 76 104 |
| | | | 渗透攻击（Infiltration） | 29 | 7 |
| | | | 端口扫描攻击（PortScan） | 127 024 | 31 756 |
| | | | 网络攻击（Web） | 1 733 | 433 |
| | | | 暴力破解（Brute Force） | 11 012 | 2 752 |
| CSE-CIC-IDS-2018 | 原样本数：16 233 002<br>清洗后样本数：<br>15 450 706 | 79（7） | 良性（Benign） | 10 158 176 | 2 539 543 |
| | | | 机器人攻击（Bot） | 228 953 | 57 238 |
| | | | 拒绝服务攻击（DoS） | 494 036 | 123 508 |
| | | | 渗透攻击（Infiltration） | 129 548 | 32 386 |
| | | | 分布式拒绝攻击（DDoS） | 1 044 353 | 261 088 |
| | | | 网络攻击（Web） | 154 758 | 38 689 |
| | | | 暴力破解（Brute Force） | 150 744 | 37 686 |

$$\text{Accuracy}=\frac{\text{TP}+\text{TN}}{\text{TP}+\text{TN}+\text{FP}+\text{FN}} \quad (9)$$

$$\text{Precision}=\frac{\text{TP}}{\text{TP}+\text{FP}} \quad (10)$$

$$\text{Recall}=\frac{\text{TP}}{\text{TP}+\text{FN}} \quad (11)$$

$$\text{F1}=\frac{2\text{Precision}\cdot\text{Recall}}{\text{Precision}+\text{Recall}} \quad (12)$$

### 3.2 消融实验

MRID主要由流量注意力模块、多尺度残差模块和检测输出模块构成。为此，本节分析流量注意力模块、多尺度残差模块对MRID性能的影响。

#### 3.2.1 MS-Res的影响

首先，分析MS-Res对MRID性能的影响。为此，通过2个卷积层（标记为CNN）、残差模块[12]（标记为ResNet）和TCN模块[13]（标记为TCN）替代多尺度残差模块，形成3个变体。即分别用CNN、ResNet和TCN替代文中形成的MS-Res模块。

MS-Res、CNN、ResNet和TCN模型在数据集CICIDS2017和CSE-CIC-IDS2018上的准确率和F1值如图6所示。

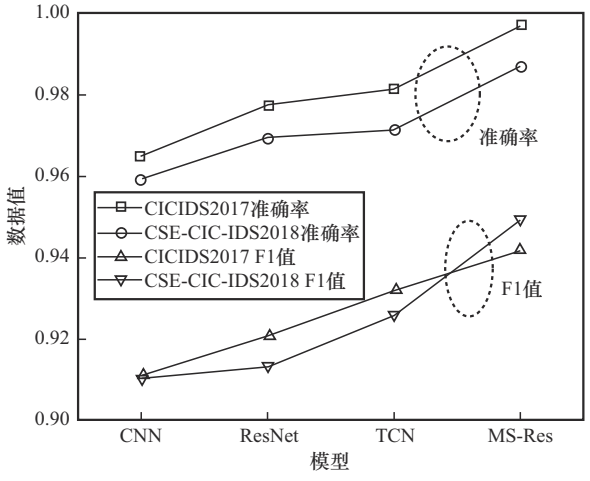


图6 MS-Res在CICIDS2017和CSE-CIC-IDS2018上的准确率和F1值

从图6可知，CNN模型的性能最差，它在数据集CICIDS2017和CSE-CIC-IDS2018上的准确率分别为0.964 9和0.954 9，F1值分别为0.911 2和0.910 3。原因在于卷积层无法捕获IoT流量中固有的时间依赖性，导致后续层的信息丢失。

ResNet较好地解决了信息丢失问题，它在层之间采用了残差连接。因此，ResNet模型的准确率和F1值均优于CNN。由于TCN模型融合了残

差模块，它的检测性能优于ResNet模型的性能。原因在于，TCN可以通过时间卷积捕获IoT流量的时间特征。

相比于CNN、ResNet和TCN模型，MS-Res模型的性能最优。这说明，利用多尺度残差网络处理IoT流量数据，可增强网络的表征能力，最终提升了入侵检测模型的性能。

### 3.2.2　流量注意力模块

令MRID-uTA表示未采用流量注意力模块。在数据集CICIDS2017和CSE-CIC-IDS2018上，MRID-uTA和MRID的准确率和F1值如图7所示。

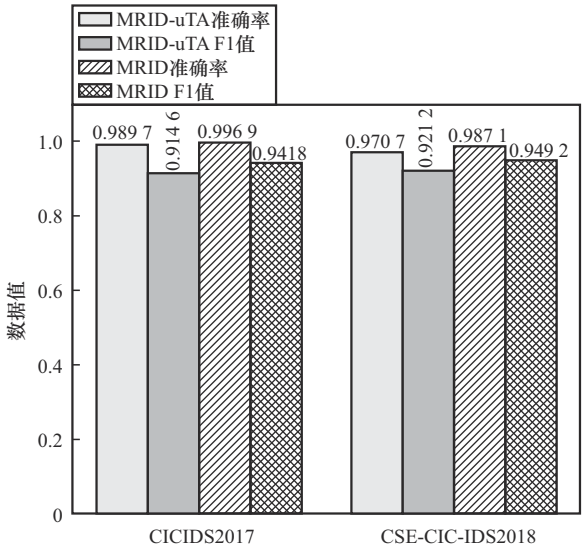


图7　MRID-uTA和MRID的准确率和F1值

从图7可知，相比于MRID-uTA，MRID采用流量注意力模块提升了准确率和F1值。例如，在数据集CICIDS2017上，MRID-uTA的准确率为0.989 7，而MRID将准确率提升了0.72个百分点。同时，也将F1值提升了2.72个百分点。这说明，流量注意力模块使模型在学习过程中能更关注更重要的特征。

## 3.3　MRID在数据集CICIDS2017和CSE-CIC-IDS2018上的预测性能

首先，分析MRID对数据集CICIDS2017中的7类样本的预测性能。MRID在数据集CICIDS2017上的热力图如图8所示。MRID在数据集CICIDS2017上预测7类样本的性能见表2。

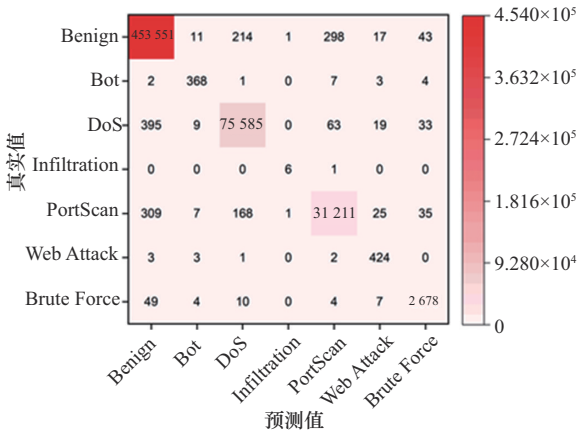


图8　MRID在数据集CICIDS2017上的热力图

表2　MRID在数据集CICIDS2017上预测7类样本的性能

| 类别 | 精确率 | 召回率 | F1值 |
|---|---|---|---|
| Begnign | 0.998 3 | 0.998 7 | 0.998 5 |
| Bot | 0.915 4 | 0.955 8 | 0.935 1 |
| DoS | 0.994 8 | 0.993 1 | 0.993 9 |
| Infiltration | 0.75 | 0.857 1 | 0.80 |
| PortScan | 0.988 1 | 0.982 8 | 0.985 4 |
| Web Attack | 0.856 5 | 0.979 2 | 0.913 7 |
| Brute Force | 0.958 8 | 0.973 1 | 0.965 9 |

从表2可知，MRID对Infiltration分类性能最差，精确率和F1值只有约0.75和0.80；其次是Web Attack类，它的精确率和F1值只有约0.86和0.91；然后是Bot类，它的精确率和F1值只有约0.92和0.94。这可能是数据中类别不平衡的负作用，因为这3个类别中的样本数量远远小于其他类别。MRID对其他类别的预测性能不错，F1值在0.96～0.99，对Begnign类样本的预测性能最好，F1值达到0.998 5。

接下来，分析MRID对数据集CSE-CIC-IDS2018中的7类样本的预测性能。MRID在数据集CSE-CIC-IDS2018上的热力图如图9所示。MRID在数据集CSE-CIC-IDS2018上预测7类样本的性能见表3。

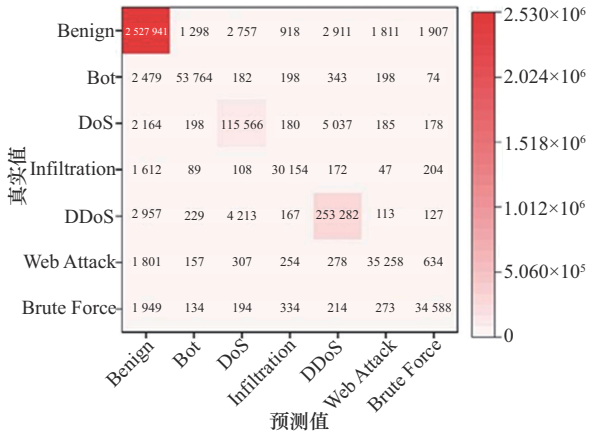


图9　MRID在数据集CSE-CIC-IDS2018上的热力图

表3　MRID在数据集CSE-CIC-IDS2018上预测7类样本的性能

| 类别 | 精确率 | 召回率 | F1值 |
|---|---|---|---|
| Begnign | 0.994 9 | 0.995 4 | 0.995 1 |
| Bot | 0.962 3 | 0.939 3 | 0.950 7 |
| DoS | 0.937 1 | 0.935 7 | 0.936 4 |
| Infiltration | 0.936 4 | 0.931 1 | 0.933 7 |
| DDoS | 0.965 9 | 0.970 1 | 0.967 9 |
| Web Attack | 0.930 7 | 0.911 3 | 0.920 9 |
| Brute Force | 0.917 2 | 0.917 7 | 0.917 5 |

从表3可知，MRID对Brute Force类样本的检测性能最差，精确率和F1值分别为0.917 2和0.917 5。其次是Web Attack类样本，它的精确率和F1值分别为0.930 7和0.920 9。然后是Infiltration类样本，它的精确率和F1值分别为0.936 4和0.933 7。

尽管这些类别的样本数量差异很大，但所提出的MRID仍然表现出良好的性能。此外，DoS流量和DDoS流量之间存在相对较高的混淆，导致F1值分别为0.936 4和0.967 9。与CICIDS2017相比，由于该CSE-CIC-IDS2018的噪声和异构性对Benign类样本的错误识别相对较高，精确率、召回率和F1值下降。

### 3.4　与其他分类器的性能分析

为了更好地分析MRID的性能，选择传统的机器学习和深度学习模型作为基准模型，这些基准模型分别是支持向量机（support vector machine，SVM）[14]、随机森林（random forest，RF）[15]、人工神经网络（artificial neural network，ANN）[16]和LSTM[17]。用基准模型对样本进行分类。

MRID、SVM、RF、ANN和LSTM在数据集CICIDS2017上的检测性能如图10所示。

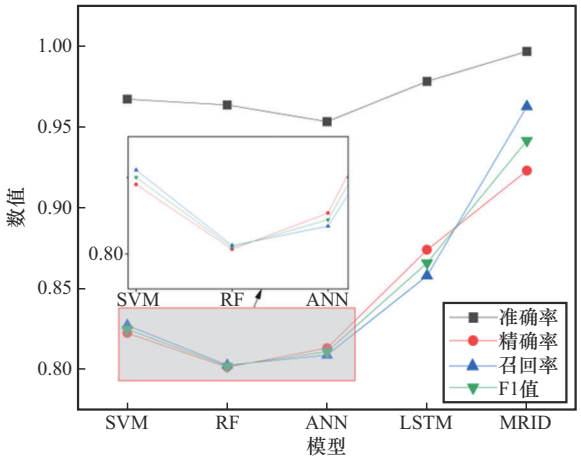


图10　MRID、SVM、RF、ANN和LSTM在数据集CICIDS2017上的检测性能

从图10可知，SVM、RF和ANN模型的性能较差，它们的F1值分别为0.825 0、0.802 2和0.811 2。原因在于：它们不具有区分不同攻击类别的能力，缺乏鲁棒的特征工程技术。相比之下，LSTM模型达到了较高的检测性能，它的F1值达到0.866 1。

同SVM、RF、ANN和LSTM相比，MRID提升了准确率、精确率、召回率和F1值，分别为0.996 9、0.923 1、0.962 9和0.941 8。尽管LSTM模型的性能是SVM、RF、ANN和LSTM 4个模型中最优的，但它的准确率、精确率、召回率和F1值也只有0.978 4、0.874 2、0.858 2和0.866 1。这些数据说明：将MS-Res和流量注意力模块进行融合，能有效地提取流量中的强特征，最终增强了模型的分类能力。

MRID、SVM、RF、ANN和LSTM在数据集CSE-CIC-IDS2018上的检测性能如图11所示。从图11可知，在数据集CSE-CIC-IDS2018上，MRID的准确率、精确率、召回率和F1值仍优于SVM、RF、

ANN和LSTM模型。MRID的准确率、精确率、召回率和F1值分别达到0.987 1、0.949 1、0.943 0和0.949 2，而LSTM模型（它是SVM、RF、ANN和LSTM 4个模型中最优的）的准确率、精确率、召回率和F1值也只有0.970 1、0.870 7、0.926 7和0.897 8。

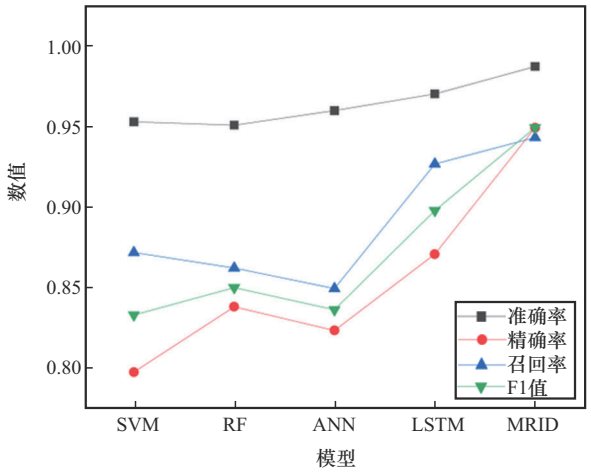


图11　MRID、SVM、RF、ANN和LSTM在数据集CSE-CIC-IDS2018上的检测性能

此外，对比图11和图10数据不难发现，同一个模型在这2个数据集上的检测性能并不同，为了更直观地反映同一模型在CSE-CIC-IDS2018和CICIDS2017上的差异。MRID、SVM、RF、ANN和LSTM在数据集CICIDS 2018和CICIDS2017的准确率和F1值如图12所示。

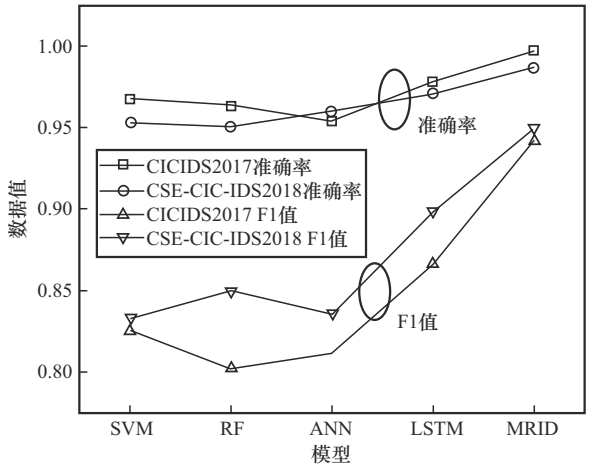


图12　MRID、SVM、RF、ANN和LSTM在数据集CSE-CIC-IDS2018和CICIDS2017上的准确率和F1值

从F1值指标上来看，5个模型在CSE-CIC-IDS2018上的性能优于在CICIDS2017。但是，若从准确率指标上来看，5个模型在CSE-CIC-IDS2018上的性能并不全优于CICIDS2017。SVM和RF模型在CICIDS2017上所获取的准确率高于在CSE-CIC-IDS2018上的准确率，而ANN、LSTM和MRID模型正好相反。

### 3.5　MRID的运算时间

最后，分析MRID模型在云层和雾层的运算时间，即训练时间和检测时间（在云层训练模型，在雾层检测样本，判断是否有攻击样本）。MRID、RF、ANN和LSTM在数据集CICIDS2017和CSE-CIC-IDS2018上的运算时间见表4。

表4　MRID、RF、ANN和LSTM在数据集CICIDS2017和CSE-CIC-IDS2018上的运算时间

| 模型 | CICIDS 2017 | | CSE-CIC-IDS 2018 | |
|---|---|---|---|---|
| | 训练时间（云层）/s | 测试时间（雾层）/s | 训练时间（云层）/s | 测试时间（雾层）/s |
| RF | 171 | 57.2 | 351 | 60.3 |
| LSTM | 82 | 68.9 | 234 | 71.4 |
| ANN | 46 | 3.8 | 302 | 5.1 |
| MRID | 79 | 3.2 | 213 | 3.4 |

从表5可知，相比于RF、LSTM和ANN模型，MRID有最低测试时间，其次是ANN模型。MRID选用改进的TCN构建分类器，极大限度缩短模型的训练时间，并且能快速地对样本进行分类。此外，由于数据集CSE-CIC-IDS2018中数据的样本数和复杂性高于CICIDS2017，利用数据集CSE-CIC-IDS2018训练模型的时间远大于利用数据集CICIDS2017训练模型的时间。

## 4　结束语

本文针对IoT的入侵攻击问题，提出一种基于TCN的入侵检测模型MRID。MRID采用一个改进的TCN作为分类器。TCN由多尺度

卷积模块和注意力模块构成，一方面提升模型捕获时空表征的能力，另一方面增强模型在训练阶段关注重要特征的能力。利用数据集 CICIDS2017 和 CSE-CIC-IDS2018 分析 MRID 的性能，并与 CNN、ANN、RF、LSTM 和 SVM 模型进行性能比较。性能分析表明，本文提出的 MRID 比对照模型的检测性能提升 1%～3%，并提升了检测样本的速度。MRID 可应用于车联网和工业物联网场景，以检测网络中潜在的攻击。

本文并没有考虑数据隐私保护问题，后期拟将联邦学习算法与 MRID 相结合，并通过加密算法或者差分隐私算法维护数据隐私安全。

## 参考文献：


[1] 罗国宇, 汪学舜, 戴锦友. 物联网入侵检测的随机特征图神经网络模型[J]. 计算机工程与应用, 2024, 60(21): 264-273.
LUO G Y, WANG X S, DAI J Y. Random feature graph neural network for intrusion detection in Internet of Things[J]. Computer Engineering and Applications, 2024, 60(21): 264-273.

[2] 李聪宇, 赵利辉, 安洋. 基于图神经网络的物联网入侵检测研究[J]. 中北大学学报(自然科学版), 2024, 45(2): 194-204.
LI C Y, ZHAO L H, AN Y. Research on intrusion detection of Internet of things based on graph neural network[J]. Journal of North University of China (Natural Science Edition), 2024, 45(2): 194-204.

[3] 刘奇旭, 肖聚鑫, 谭耀康, 等. 工业互联网流量分析技术综述[J]. 通信学报, 2024, 45(8): 221-237.
LIU Q X, XIAO J X, TAN Y K, et al. Survey of industrial Internet traffic analysis technology[J]. Journal on Communications, 2024, 45(8): 221-237.

[4] 项睿涵, 潘巨龙, 李玲艺, 等. 一种物联网入侵检测和成员推理攻击研究[J]. 传感技术学报, 2024, 37(2): 317-325.
XIANG R H, PAN J L, LI L Y, et al. A new study of an IoT intrusion detection and membership inference attack[J]. Chinese Journal of Sensors and Actuators, 2024, 37(2): 317-325.

[5] 吴昊, 郝佳佳, 卢云龙. 物联网场景下基于蜜场的分布式网络入侵检测系统研究[J]. 通信学报, 2024, 45(1): 106-118.
WU H, HAO J J, LU Y L. Research on distributed network intrusion detection system for IoT based on honeyfarm[J]. Journal on Communications, 2024, 45(1): 106-118.

[6] SHAFIQ M, TIAN Z H, BASHIR A K, et al. CorrAUC: a malicious bot-IoT traffic detection method in IoT network using machine-learning techniques[J]. IEEE Internet of Things Journal, 2021, 8(5): 3242-3254.

[7] STOYANOVA M, NIKOLOUDAKIS Y, PANAGIOTAKIS S, et al. A survey on the Internet of Things (IoT) forensics: challenges, approaches, and open issues[J]. IEEE Communications Surveys & Tutorials, 2020, 22(2): 1191-1221.

[8] 毛智强, 徐耀松, 王丹丹, 等. 基于模态分解和时间卷积网络的瓦斯涌出量组合预测[J]. 传感技术学报, 2024, 37(10): 1795-1802.
MAO Z Q, XU Y S, WANG D D, et al. Combined prediction of gas emergence based on modalihj decomposition and temporal convolutional networks[J]. Chinese Journal of Sensors and Actuators, 2024, 37(10): 1795-1802.

[9] ZHOU X K, HU Y Y, LIANG W, et al. Variational LSTM enhanced anomaly detection for industrial big data[J]. IEEE Transactions on Industrial Informatics, 2021, 17(5): 3469-3477.

[10] 胡炜晨, 许聪源, 詹勇, 等. 一种适用于小样本条件的网络入侵检测方法[J]. 电信科学, 2023, 39(10): 85-100.
HU W C, XU C Y, ZHAN Y, et al. A network intrusion detection method designed for few-shot scenarios[J]. Telecommunications Science, 2023, 39(10): 85-100.

[11] 江魁, 卢橹帆, 苏耀阳, 等. 基于 Attention-GRU 的 SHDoS 攻击检测研究[J]. 信息网络安全, 2024, 24(3): 427-437.
JIANG K, LU L F, SU Y Y, et al. SHDoS attack detection research based on attention-GRU[J]. Netinfo Security, 2024, 24(3): 427-437.

[12] 吴锋振, 杨德宏, 李俊, 等. 非对称卷积金字塔残差网络的遥感影像建筑物提取[J]. 遥感技术与应用, 2023, 38(6): 1467-1476.
WU F Z, YANG D H, LI J, et al. Building extraction from remote rensing images using asymmetric convolution pyramid residual network[J]. Remote Sensing Technology and Application, 2023, 38(6): 1467-1476.

[13] CHENG Y L, XU Y, ZHONG H, et al. Leveraging semisupervised hierarchical stacking temporal convolutional network for anomaly detection in IoT communication[J]. IEEE Internet of Things Journal, 2021, 8(1): 144-155.

[14] LIN C F, WANG S D. Fuzzy support vector machines[J]. IEEE

Transactions on Neural Networks, 2002, 13(2): 464-471.

[15] KURNIABUDI, STIAWAN D, DARMAWIJOYO, et al. CICIDS-2017 dataset feature analysis with information gain for anomaly detection[J]. IEEE Access, 2020, 8: 132911-132921.

[16] GAMAGE S, SAMARABANDU J. Deep learning methods in network intrusion detection: a survey and an objective comparison[J]. Journal of Network and Computer Applications, 2020, 169: 102767.

[17] DI MAURO M, GALATRO G, LIOTTA A. Experimental review of neural-based approaches for network intrusion management[J]. IEEE Transactions on Network and Service Management, 2020, 17(4): 2480-2495.

[作者简介]

**刘丽伟**（1983– ），男，郑州工业应用技术学院大数据信息管理中心副教授，主要研究方向为数据安全与通信网络。

**赵红超**（1976– ），男，郑州工业应用技术学院大数据信息管理中心副教授，主要研究方向为数据安全与通信网络。

**李学威**（1983– ），男，周口职业技术学院信息工程学院副教授，主要研究方向为计算机应用。

**孙滨**（1983– ），男，郑州工业应用技术学院大数据信息管理中心教授，主要研究方向为机器学习与教育大数据。