研究与开发

SDN环境下双阶段DDoS攻击检测方法

包晓安[1]，范云龙[1]，涂小妹[2]，胡天缤[3]，张娜[1]，吴彪[4]
（1. 浙江理工大学计算机科学与技术学院，浙江 杭州 310018；
2. 浙江广厦建设职业技术大学城乡建设学院，浙江 金华 322100；
3. 河海大学人工智能与自动化学院，江苏 常州 213000；
4. 浙江理工大学理学院，浙江 杭州 310018）

摘　要：针对软件定义网络（software-defined network，SDN）中分布式拒绝服务（distributed denial of service，DDoS）攻击检测存在的特征丢失、模型计算复杂度高以及检测实时性不足等问题，提出了一种系统化的检测框架。首先，提出一种融合流级与包级双粒度信息的流量表征方法，以多尺度挖掘攻击行为的关键特征，提升流量表征信息的完整性。其次，构建基于Mamba架构的轻量级检测模型DDoSMamba。该模型首先利用状态空间建模与全局感受野机制，降低序列建模中的计算资源与内存消耗；然后引入双向信息交互机制，增强对序列前后文关系的建模能力；最后结合低秩近似分解与特征子空间划分策略，显著压缩参数规模与推理开销。最后，进一步设计双阶段DDoS攻击检测方法：第一阶段，利用Tsallis熵对粗粒度特征进行快速筛查，排除大量正常流量；第二阶段，基于细粒度特征进行高精度分类，实现快速响应与精准检测的平衡。在CIC-IDS2019数据集上的实验结果表明，本文所提方法在二分类与多分类任务中分别达到99.96%与99.93%的准确率，平均检测耗时仅为0.067 2 ms，参数量低至4.553 8 KB。

关键词：软件定义网络；DDoS攻击检测；流量表征；双阶段检测分类
中图分类号：TP393
文献标志码：A
doi: 10.11959/j.issn.1000−0801.2026018

Two-stage DDoS attack detection method in SDN environment

Bao Xiaoan[1], Fan Yunlong[1], Tu Xiaomei[2], Hu Tianbin[3], Zhang Na[1], Wu Biao[4]
1. School of Computer Science and Technology, Zhejiang Sci-Tech University, Hangzhou 310018, China
2. School of Urban and Rural Construction, Zhejiang Guangsha Vocational and Technical University of Construction, Jinhua 322100, China
3. School of Artificial Intelligence and Automation, Hohai University, Changzhou 213000, China
4. School of Science, Zhejiang Sci-Tech University, Hangzhou 310018, China

Abstract: To address issues such as feature loss, high computational complexity, and insufficient real-time perfor-

收稿日期：2025−08−05；**修回日期：**2025−10−17
通信作者：吴彪，biaowuzg@zstu.edu.cn
基金项目：浙江省重点研发计划项目（No.2020C03094）；浙江省教育厅项目（No.Y202250706，No.Y202147659）
Foundation Items: Zhejiang Provincial Key Research and Development Program (No.2020C03094)，Projects of Zhejiang Provincial Department of Education (No.Y202250706, No.Y202147659)

mance in distributed denial of service (DDoS) attack detection within software-defined networks (SDN), a systematic detection framework was proposed. Firstly, traffic characterization method integrateing dual-granularity information at both flow-level and packet-level was introduced to extract key features of various attack behaviors at multiple scales, thereby enhancing the completeness of traffic representation. Then, a lightweight detection model named DDoSMamba, based on the Mamba architecture, was constructed. By leveraging state space modeling and global receptive field mechanisms, the model reduced computational and memory overhead during sequence modeling. A bidirectional information interaction mechanism was introduced to enhance contextual modeling, while low-rank approximation and subspace feature decomposition strategies were employed to significantly compress parameter size and inference cost. Finally, a two-stage DDoS attack detection method was designed. In the first stage, Tsallis entropy was used to perform rapid filtering based on coarse-grained features, effectively eliminating a large amount of benign traffic. In the second stage, fine-grained features were used for high-precision classification, achieving a balance between fast response and accurate detection. Experiments conducted on the CIC-IDS2019 dataset demonstrate that the proposed method achieves 99.96% and 99.93% detection accuracy for binary and multi-class classification tasks, respectively, with an average inference latency of only 0.067 2 ms and a model size as low as 4.553 8 KB.

Key words: SDN, DDoS attack detection, traffic representation, two-stage detection and classification

0 引言

随着互联网用户数量的持续增长和相关技术的飞速发展，网络流量呈指数级激增，传统网络架构在带宽、灵活性以及安全性方面逐渐暴露出诸多瓶颈，难以满足新型业务和服务的需求。在此背景下，软件定义网络（software-defined network，SDN）应运而生。然而，SDN在提供灵活性与高效管理能力的同时，也引入了新的安全隐患。在SDN架构中，控制器负责全局网络的调度与决策，一旦遭受攻击，不仅会影响网络的正常运行，还可能被恶意利用，成为网络攻击的“单点故障”[1]。其中，分布式拒绝服务（distributed denial-of-service，DDoS）攻击因其扩展迅速、攻击手段多样且分布广泛，对网络流量监控、检测与防御提出了严峻的挑战。随着全球数字化进程的快速推进，DDoS攻击的规模、复杂度和成功率均显著上升[2]。因此，如何准确、快速地检测并及时应对DDoS攻击，已成为SDN安全领域亟待解决的关键问题之一[3]。

近年来，深度学习技术在流量异常检测和分类任务中取得了较高的检测精度。然而，现有方法仍存在以下不足。首先，为降低计算和存储开销，不少研究倾向于采用流级别的流量表示方式，但这往往会造成细粒度特征的丢失，尤其是有效载荷中与描述流量行为相关的信息，而这些信息对识别某些类型的攻击至关重要。其次，由于流量中各特征对分类贡献存在显著差异，模型在特征提取过程中往往会引入冗余信息，从而影响分类性能。针对上述问题，基于注意力机制的Transformer模型近年来受到广泛关注。Transformer模型的自注意力机制可以动态分配权重，使模型更精准地聚焦于关键特征。然而，Transformer架构的自注意力机制需要计算序列中所有元素之间的关系，导致在处理长序列时计算复杂度$O(n^2)$[4-5]呈二次指数增长，显著增加了计算负担和内存消耗。为突破这一瓶颈，Mamba[7]作为一种新型选择性结构状态空间模型，通过全局感受野和动态加权机制，缓解了卷积神经网络的建模约束，并提供了类似于Transformer的高级建模能力。重要的是，它既可以实现上述功能，又能避免计算复杂度高的问题，显著降低了长序列建模的计算复杂度，并在多模态任务中展现出媲美甚至超越Transformer的性能。值得注意的是，目

前尚未发现有研究将 Mamba 应用于 SDN 环境下的 DDoS 攻击检测。与此同时，深度学习方法虽然在检测精度上取得了巨大的成功，但其计算复杂度较高，训练和推理过程耗时较长，这使得深度学习难以在资源有限的网络设备上高效运行，也无法满足实时在线流量分类的需求[6]。

为更好地挖掘网络流量中隐含的多层次信息，本文提出了一种更全面的流量表征方案。该方案整合了流级别时序特征与包级别细粒度信息，既保留了流量行为的整体趋势，又能捕捉到关键数据包内的细微变化。为应对在计算序列过程中消耗大量计算资源和内存的问题，本文进一步提出一种基于 Mamba 架构的 DDoSMamba 模型。DDoSMamba 模型在 Mamba 模型的基础上引入双向信息交互机制，实现对序列数据前后文关系的全面建模。同时，为降低模型的存储需求和计算开销，DDoSMamba 模型对线性投影层的权重矩阵采用低秩近似分解策略，在保留关键特征信息的前提下大幅压缩参数量。此外，DDoSMamba 模型在卷积处理后将输入的序列特征按维度划分为多个子空间分别计算，进一步降低参数规模。该方案是首次将 Mamba 结构应用到 SDN 环境下 DDoS 攻击检测的尝试。为了满足实际网络环境中流量检测对低时延的需求，本文还设计了一种由 Tsallis 熵检测阶段和 DDoSMamba 分类阶段组成的双阶段 DDoS 攻击检测分类方法。具体而言，Tsallis 熵检测阶段利用熵值计算开销低、速度快的特点，快速筛选出可疑攻击流量，避免分类阶段对大量正常流量的冗余计算，减少分类耗时。

本文的主要贡献包括以下 3 个方面。

（1）提出一种融合流级别时序特征与包级别细粒度信息的流量表征方法。该方法既能反映流量行为的整体趋势，又可捕捉关键数据包中的细微变化，为多层次网络流量信息挖掘提供了新思路。

（2）构建了 DDoSMamba 模型。在 Mamba 模型基础上引入双向信息交互机制，并采用低秩近似和子空间划分策略，在有效提升序列建模与分类精度的同时，大幅降低了计算复杂性与参数规模。

（3）设计了一种由 Tsallis 熵检测阶段与 DDoSMamba 分类阶段组成的双阶段 DDoS 攻击检测分类方法，通过快速筛选攻击流量来避免冗余计算，满足实际网络中对低时延检测的需求。

1　相关工作

1.1　基于信息熵的方法

为提高 DDoS 攻击检测的实时性，研究者提出了多种基于信息熵的轻量级检测方法。例如，Neres Carvalho 等[8]提出利用 Shannon 熵检测 SDN 中的 DDoS 攻击。该方法虽然实时性高且耗时低，但存在检测准确率有限、误报率较高的问题。考虑到 Shannon 熵仅基于单一流量特征进行计算，忽略了数据包特征之间潜在的相关性，Ujjan 等[9]结合 Shannon 熵和雷尼熵，提出了一种基于广义熵的检测方法。Li 等[10]则提出了一种基于 φ-熵的检测方法。这些方法通过引入不同的熵算法并结合流量特征间的相关性，有效提高了 DDoS 攻击检测的准确性。然而，基于固定阈值的熵检测方法在处理动态变化的网络流量时，可能造成误报率的不稳定。为此，Hemmati 等[11]通过设置动态阈值的方法有效缓解了该问题，但由于动态阈值设置相对简单，误报率仍较高。总体而言，信息熵方法适用于结构简单的网络环境，而面对大规模流量和多样化攻击，其误报率和漏报率较高，且检测效果依赖阈值设定。不过，由于其实时性高、计算复杂度低、消耗资源较少，该类方法仍适合作为初级检测手段。基于上述分析，本文提出一种双阶段 DDoS 攻击检测分类方法，将基于 Tsallis 熵的检测方法作为初级检测阶段，旨在以较小的代价快速筛出大量正常网络流量，从而减少后续阶段的冗余计算。

1.2 流量表征方式

Ben Said 等[12]采用 CNN、BiLSTM 和注意力机制构建混合模型，并在实验中取得了 98.03% 的检测精度；Zainudin[13]则提出了基于 CNN-LSTM（convolutional neural network and long short-term memory）的 DDoS 攻击分类方法，借助 XGBoost 进行特征选择，实现了 99.50% 的高准确率。然而，这两种方法在流量表征上均存在显著缺陷：它们主要从单个流中提取静态特征，完全忽略了流之间的时序关联与包级别的细粒度数据。事实上，网络流量往往包含丰富的时序信息和微妙的包级变化，而这种粗糙的表征方式使得模型在应对复杂多分类任务时，无法捕捉到攻击行为的细微差别，导致整体精度下降。为了解决这一瓶颈问题，本文提出一种全新的流量表征方案，即综合利用包级别细粒度信息和流间时序特征，构建更精准、全面的流量表征方式，从而显著提升多分类检测任务的准确率。

1.3 基于深度学习的方法

Bhutto 等[14]提出一种基于 Transformer 的 VSI-DDoS 检测方法，该方法采用可学习时间表示架构。研究在测试平台和基准数据集上进行了系统性实验，并将 VSI-DDoS 与 Bi-LSTM、LSTM 和 DeROL 等最先进的基线模型进行对比，结果验证了 VSI-DDoS 的有效性。Le 等[15]构建了基于 Transformer 和 CNN 的 DDoS 攻击检测模型 DDosTC。该模型充分利用了 Transformer 的计算效率和扩展性，同时结合 CNN 强大的特征提取能力，在 CICDDoS2019 数据集上取得了 99.82% 的检测准确率。Wang 等[16]提出了将 Transformer 文本分类技术作为检测方法的 DDoSBERTDDoS 模型，并且用一套综合性评估框架证明了该方法的有效性。然而，上述基于 Transformer 的模型均受限于自注意力机制固有的二次计算复杂度问题：其计算量和内存开销随序列长度呈平方级增长。这一高昂的成本正成为制约该类模型在实际网络环境中部署的主要瓶颈。

1.4 状态空间模型

状态空间模型（state-space model，SSM）是一种用于描述由观测值和未知内部状态变量组成的动态变化系统的数字模型。Gu 等[7]提出的结构化状态空间序列（S4）模型，是一种替代 Transformer 架构的方法，能够在不使用注意力机制的情况下建模长程依赖关系。在 S4 的基础上，研究者们陆续提出多种改进策略：Madhwani 等[17]引入 MIMO SSM 结构和高效并行扫描机制，实现了隐藏层的并行初始化与状态重置；He 等[18]则通过增加稠密连接层，提升了浅层隐藏状态的特征表达能力；而 Bhat 等[19]通过加入门控单元，增强了隐藏层的记忆能力。近期，Dao 等[20]提出的通用语言模型 Mamba，在保持线性复杂度的同时，展现出超越 Transformer 的序列建模能力，为序列建模技术带来了显著进展。本文提出的 DDoSMamba 模型以 Mamba 为网络主干，旨在解决 Transformer 在长序列建模中自注意力机制所引发的二次复杂度问题，为长序列场景下的 DDoS 攻击检测提供更高效的解决方案。

2 双阶段 DDoS 攻击检测分类方法

2.1 统计特征检测分类方法框架

本文提出的双阶段 DDoS 攻击检测分类方法包括 Tsallis 熵检测阶段和 DDoSMamba 分类阶段，整体架构如图 1 所示。在 Tsallis 熵检测阶段，首先计算流量窗口流量中源 IP 地址、目的 IP 地址和数据包大小的 Tsallis 熵值，并将其与阈值进行比较，从而快速筛选出异常流量。随后，针对异常流量，按 IP 地址和端口号进行分组，形成流数据。在此基础上，从流级别提取相邻流的时序特征，并结合包级别的细粒度信息，对流量进行全面表征。最后，将组合后的特征按步长输入 DDoSMamba 分类阶段，利用本文所提出的 DDoSMamba 模型进行流量分类。

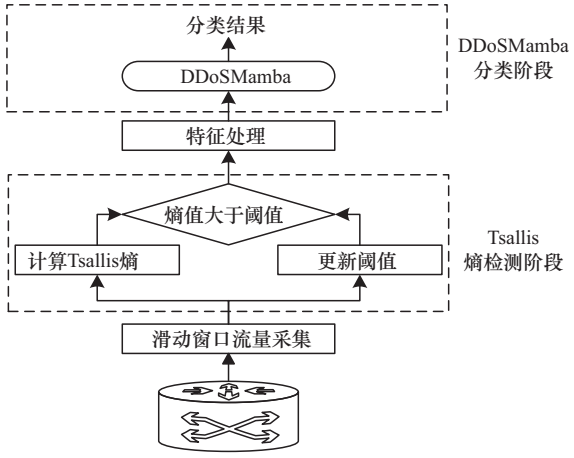

图1　双阶段DDoS攻击检测分类方法架构

2.2　流量表征Tsallis熵检测阶段

Tsallis熵检测阶段工作流程如图2所示。通过计算流量窗口流量中源IP地址、目的IP地址和数据包大小的Tsallis熵值并与阈值进行比较，快速筛选出攻击流量。同时，为了实现百分之百召回率，采用滑动窗口法根据窗口内流量的变化动态调整阈值。

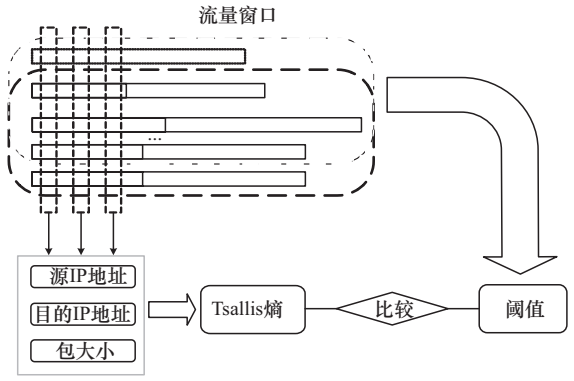

图2　Tsallis熵检测阶段工作流程

2.2.1　Tsallis熵计算

Tsallis熵是一种广义熵度量方法，因其非加性，相较于传统Shannon熵，能够更灵活地适应不同的概率分布。在DDoS攻击检测中，Tsallis熵能够有效捕捉低概率事件，如攻击流量中的异常模式或隐蔽威胁，从而提升对小概率攻击的检测能力，尤其适用于检测阶段对高召回率的需求。因此，本文选取Tsallis熵描述流量状态。

在流量窗口内，首先从每个数据包中提取源IP地址、目的IP地址和包大小3个特征。对于每个特征，统计它们在整个窗口中的出现频率，再将这些频率归一化为概率分布，其数学表达式如下。

$$p_i=\frac{\mathrm{count}(i)}{N} \tag{1}$$

基于这些概率分布，通过式（2）计算每个特征的Tsallis熵，以量化该特征在窗口的流量复杂度。

$$H_i=\frac{1}{q-1}\left(1-\sum_{i=1}^{N} p_i^q\right) \tag{2}$$

其中，p_i是数据集中第i个特征对应的概率分布函数，N表示特征组中不同值的总数，q是Tsallis熵的阶数，H_i代表第i个特征的Tsallis熵值，p_i^q代表概率p_i的q次幂。

最终，对源IP地址、目的IP地址和包大小3个特征的Tsallis熵进行求和，得到描述整个流量窗口复杂度的指标C_{win}。

$$C_{\mathrm{win}}=\sum_{j} H_q^j \tag{3}$$

其中，j为流量特征的索引，H_q^j为第j个特征的Tsallis熵。

2.2.2　滑动窗口设置动态阈值

固定阈值往往难以适应复杂多变的真实网络环境，还可能出现较大的检测误差。为了提高检测的精度并确保异常流量的百分百召回率，采用滑动窗口策略设置阈值。具体而言，根据流量窗口内源IP地址、目的IP地址及包大小3个特征的均值和标准差的实时变化，动态调整检测阈值。特征均值μ_t和标准差σ_t的数学表达式如式（4）、式（5）所示。

$$\mu_t=\frac{1}{n}\sum_{i=1}^{n} x_i \tag{4}$$

$$\sigma_t=\sqrt{\frac{1}{n}\sum_{i=1}^{n}\left(x_i-\mu_t\right)^2} \tag{5}$$

其中，n为窗口内的数据条目数量，x_i为特征值。

动态阈值$T_H(t)$的数学表达式如下：

$$T_h(t)=\mu_t+k\cdot\sigma_t \tag{6}$$

其中，k值控制着阈值的灵敏程度，当网络流量的标准差波动较大时，增大k值可以提高对异常流量检测的灵敏度；流量波动较小则说明网络较为平稳，此时，减小k值可以减少对正常流量的误判。k值与流量的波动密切相关，本文设计k值的数学表达式如式（7）、式（8）所示。

$$k_{(t)}=k_{(t-1)}+\Delta k_{(t)} \tag{7}$$

$$\Delta k_{(t)}=\alpha\cdot\left(\frac{\sigma(t)-\sigma(t-1)}{\sigma(t-1)}\right) \tag{8}$$

其中，式（7）中$k_{(t)}$为当前时刻的k值，$k_{(t-1)}$为上一时刻的k值，$\Delta k_{(t)}$为k值的变化量。式（8）中$\sigma(t)$为当前窗口流量特征的标准差，$\sigma(t-1)$为前一窗口流量标准差。α设置是为了调整变化率对k值的影响，本文将α设为0.5。

流量窗口向前滑动过程中，阈值会不断更新。通过比较窗口内流量的Tsallis熵值与阈值大小，实现对网络流量的初步检测。

2.3 特征处理

当Tsallis熵检测阶段识别出异常流量后，深度学习模型会对异常流进行进一步分类。为充分融合包级别与流级别的多维信息，本文提出一种全新的流量表征方案，其工作流程如图3所示。

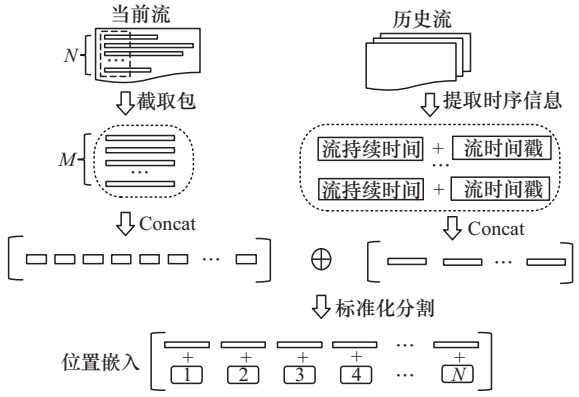

图3 流量表征方案工作流程

首先，将流量窗口内的数据包按源IP地址、目的IP地址、源端口号、目的端口号分为不同的流。在包级别特征提取中，为确保后续模型输入的标准化与高效性，对每个数据包采用固定长度截取处理：短于预设长度的包进行零填充，超长包则进行截断。为提取应用协议中的关键字段并降低噪声干扰，仅截取有效载荷的前256 byte，该部分往往包含请求方法、协议版本及状态码等描述流行为的重要信息。用于描述流行为的关键信息往往集中在通信初始阶段，如TCP三次握手过程和HTTP请求报文中的头部信息，故进一步选取流中前5个经过统一处理的数据包进行拼接，构造出一个包级别的流量特征表示。在流级别特征提取中，为充分挖掘时序信息，从当前异常流之前的历史流中提取每个流的持续时间和流时间戳。其中，流持续时间反映了每个流在网络中的活跃时长，是判断连接稳定性和业务逻辑一致性的关键指标；而流时间戳则记录了每个流的发生时间，能够反映流量在各时段内的分布趋势及潜在的周期性或突发性模式。将这两个特征进行拼接，构成流级别的流量特征表示。

其次，将包级别和流级别的流量特征表示进行拼接，组成当前流的特征表示。为进一步优化模型输入，对该长序列特征进行标准化分割，将其划分为固定长度的子序列，以消除不同序列长度差异带来的不一致性。

最后，按子序列的顺序进行位置嵌入，为每个子序列添加位置信息，以保留原始时序结构。

2.4 DDoSMamba分类阶段

2.4.1 DDoSMamba模型

DDoSMamba模型架构如图4所示。该模型在Mamba基础架构上引入了双向信息交互的Bi-Mamba模块，并采用低秩近似对线性层进行参数优化，同时在序列输入BiMamba模块前对子空间进行划分，以进一步提升计算效率。

具体过程如下：首先，输入流量特征经过一维卷积处理（卷积核大小为3），将特征维度扩展至20。随后，对卷积输出进行归一化和非线性激

活处理，得到的特征矩阵被均匀划分为多个子空间，每个子空间序列分别输入BiMamba模块进行前向与反向状态建模。将各子空间的输出在特征维度上进行拼接，再经过最大池化处层（窗口大小为2，步长为2）进行下采样。池化后的输出与一维卷积输出经最大池化处理后的特征矩阵相加，这一操作帮助模型结合不同层次的特征表示。接着，对融合结果进一步执行平均池化操作（窗口大小为2×2，步长为2），以减少冗余信息并优化特征表示。最后，将池化后的特征矩阵展平为向量，输入Softmax层完成最终流量分类。

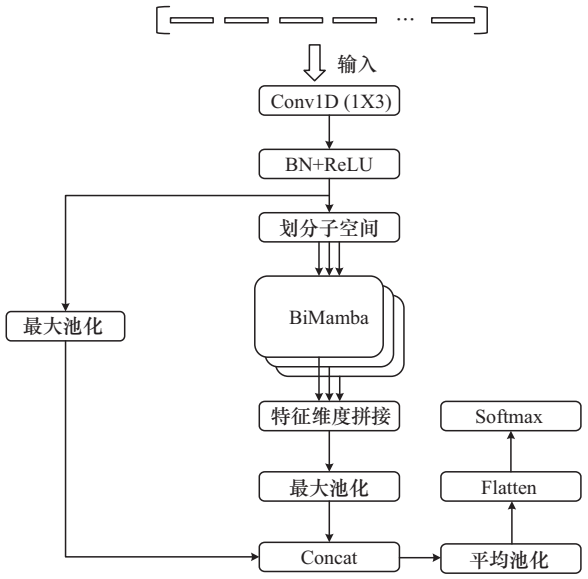

图4　DDoSMamba模型架构

下文将详细阐述线性层低秩近似、子空间划分以及BiMamba模块的具体设计与实现。

2.4.2　线性层低秩近似

标准Mamba模型的参数数量主要由其内部的线性投影层决定，在Linear中通过一个矩阵 $\boldsymbol{W}\in\mathbf{R}^{M\times N}$ 和偏置项 b 实现，其参数数量为 $M\times N$。变换表达式如式（9）所示。

$$y=\boldsymbol{W}x+b \tag{9}$$

其中，x为输入向量，y为输出向量。为减少模型参数量并加速推理，用截断奇异值分解（Truncated SVD）对线性投影层权重矩阵 $\boldsymbol{W}$ 进行低秩近似。

首先，计算矩阵 $\boldsymbol{W}$ 对其进行特征分解得到左奇异向量矩阵 $\boldsymbol{U}\in\mathbf{R}^{M\times M}$；接着，计算矩阵 $\boldsymbol{W}\boldsymbol{W}^{\mathrm{T}}$ 对其进行特征分解得到右奇异向量矩阵 $\boldsymbol{V}\in\mathbf{R}^{N\times N}$；然后，计算分块对角矩阵 $\boldsymbol{\Sigma}_{MN}$，其数学表达式如下。

$$\boldsymbol{\Sigma}_{MN}=\begin{bmatrix}\boldsymbol{\Sigma}_1 & 0\\ 0 & 0\end{bmatrix} \tag{10}$$

其中，$\boldsymbol{\Sigma}=\mathrm{diag}(\sigma_1,\sigma_2,\cdots,\sigma_r)$ 是将 $\boldsymbol{W}\boldsymbol{W}^{\mathrm{T}}$ 求出的非零特征值从大到小排列后开根号的值。

最后，将3个矩阵相乘得到矩阵 $\boldsymbol{W}$，计算表达式如下：

$$\Omega=\boldsymbol{U}\boldsymbol{\Sigma}\boldsymbol{V}^{\mathrm{T}} \tag{11}$$

其中，Ω为待分解的原始矩阵 $\boldsymbol{W}$，$\boldsymbol{U}$为左奇异向量矩阵，$\boldsymbol{\Sigma}$为奇异值矩阵，$\boldsymbol{V}^{\mathrm{T}}$为右奇异向量矩阵的转置。

在 $\boldsymbol{\Sigma}$ 矩阵中，前10%甚至1%的奇异值往往能够占全部奇异值之和的99%。基于这一性质，可通过仅保留最大的 r 个奇异值及其对应的左右奇异向量来实现对原矩阵的有效近似。John von Neumann在数值线性代数中提出的理论表明，奇异值分解（SVD）的截断操作在Frobenius范数意义下能够实现最佳逼近，即截断后的矩阵与原矩阵之间的误差最小。因此，在低秩近似中将 $\boldsymbol{\Sigma}$ 截断，只保留前 r 个最大奇异值及其对应的奇异向量，从而减少计算量和存储需求，并尽可能保持原矩阵的核心信息。其数学表达式如下：

$$\boldsymbol{W}_r=\boldsymbol{U}_r\boldsymbol{\Sigma}_r\boldsymbol{V}_r^{\mathrm{T}} \tag{12}$$

其中，$\boldsymbol{U}_r\in\mathbf{R}^{M\times N}$，$\boldsymbol{\Sigma}_r\in\mathbf{R}^{r\times r}$，$\boldsymbol{V}_r\in\mathbf{R}^{r\times N}$。

通过低秩近似，线性投影层的数学表达式如式（13）所示。

$$y=\boldsymbol{U}_r\boldsymbol{\Sigma}_r\boldsymbol{V}_r^{\mathrm{T}}x+b \tag{13}$$

其中，$\boldsymbol{U}_r$和$\boldsymbol{V}_r$维度分别为$M\times r$和$r\times N$。由于$r<d$，参数量从原来的$M\times N$减少为$M\times r+r\times N+r\times r$，并且使得计算的复杂度从$O(MN)$降低为$O(Mr+rN)$。

2.4.3　子空间划分

使用20个卷积核对输入特征序列$\boldsymbol{X}=\{x_1, x_2, \cdots, x_L\}$进行卷积，通过批归一化和ReLU激活输出特征矩阵$\hat{\boldsymbol{X}} \in \mathbf{R}^{L' \times 20}$。由于各个子空间之间的关联性较弱，直接进行全局建模会导致冗余信息的增加且计算效率较低。此外，BiMamba模块的参数量与输入维度呈平方级增长，在高维情况下会显著增加计算成本和存储开销。因此，对特征矩阵进行子空间划分处理，其过程如图6所示。

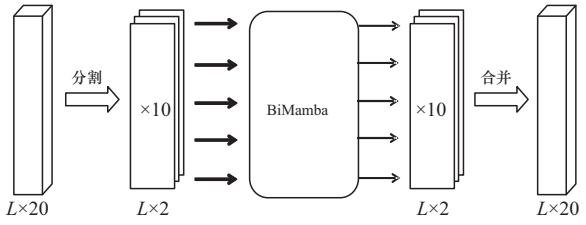

图6　子空间划分过程

首先，将矩阵的20个序列维度划分为10个子空间，得到10个维度为2的子矩阵，即$\hat{\boldsymbol{X}}_i \in \mathbf{R}^{L' \times 2}$，其数学表达式如式（14）所示。

$$\hat{\boldsymbol{X}}=\left[\hat{\boldsymbol{X}}_1, \hat{\boldsymbol{X}}_2, \cdots, \hat{\boldsymbol{X}}_{10}\right] \tag{14}$$

然后，将10个子矩阵输入BiMamba模块处理。

最后，将经过BiMamba模块处理后得到的各子矩阵在特征维度上进行拼接，合并为一个新的全局特征表示，用于后续分类。

2.4.4　BiMamba模块

为了使模型更好地适应DDoS攻击流量的高动态性和时变性，并提取更丰富的特征信息，受LSTM到BiLSTM的启发，采用双向Mamba（BiMamba）进行建模。BiMamba模块的架构如图7所示。

输入序列矩阵$\boldsymbol{T} \in \mathbf{R}^{D \times L}$，其中，$D$是输入维度，$L$是序列长度。将矩阵$\boldsymbol{T}$归一化后，通过低秩线性层映射到$\boldsymbol{X} \in \mathbf{R}^{E \times L}$，其中，$E=2D$是扩展后的维度。同时，另一个低秩线性层将$\boldsymbol{T}$映射到$\boldsymbol{Z} \in \mathbf{R}^{E \times L}$，用于SSM输出门控操作。对序列X并行进行前后向SSM处理。SSM的输出通过门控操作$\sigma(z)$进行调节，得到输出序列$\boldsymbol{Y}_{\text{forward}}$和$\boldsymbol{Y}_{\text{backward}}$。对$\boldsymbol{Y}_{\text{forward}}$和$\boldsymbol{Y}_{\text{backward}}$的和进行线性投影后与初始矩阵$\boldsymbol{T}$相加得到最终输出$\boldsymbol{R} \in \mathrm{R}^{D \times L}$。

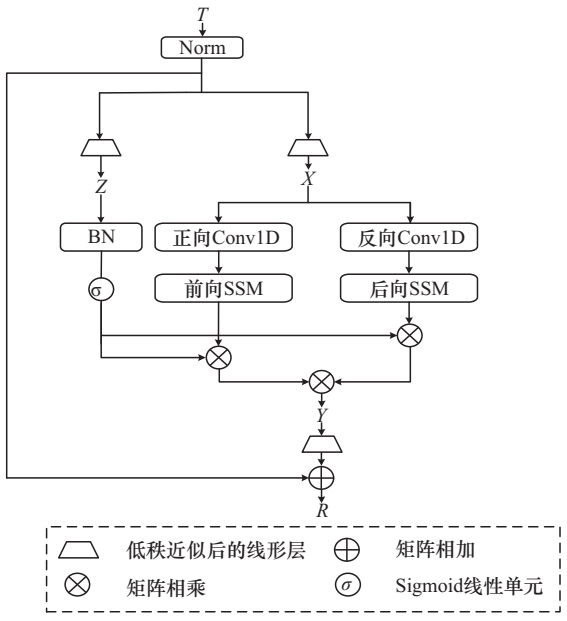

图7　BiMamba模块的架构

3　实验与分析

本实验基于Linux环境下的PyTorch深度学习框架开展，采用Python 3.8版本及CUDA 12.0进行高效计算加速，硬件平台选用NVIDIA® GeForce RTX™4080 SUPER显卡。

3.1　评价指标

为了评估模型在不同场景下的表现，采用多种常见的性能分类指标，包括准确率（Accuracy）、精确率（Precision）、召回率（Recall）、F1值（F1-score）以及时间开销。具体的表达式如下。

$$\text{Accuracy}=\frac{\text{TP}+\text{TN}}{\text{TN}+\text{FN}+\text{FP}+\text{TP}} \tag{15}$$

$$\text{Precision}=\frac{\text{TP}}{\text{TP}+\text{FP}} \tag{16}$$

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}} \tag{17}$$

$$\text{F1} = 2 \cdot \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \tag{18}$$

其中，TP 表示被正确分类为正类的样本数，TN 表示被正确分类为负类的样本数，FP 是指被错误分类为正类的负样本数，FN 则表示被错误分类为负类的正样本数。

3.2　数据集描述

CIC-DDoS2019 数据集作为网络安全领域的权威基准，由加拿大网络安全研究所（Canadian Institute for Cybersecurity，CIC）与新布伦瑞克大学联合构建。该数据集通过模拟 12 种真实 DDoS 攻击（如 SYN Flood、SSDP 反射攻击）和正常流量，在复杂网络环境中精准还原了攻击者伪造源 IP 地址、利用反射服务器淹没受害者的攻击行为特征。原始数据以 PCAP 格式存储，完整保留了网络层至应用层的协议头部与负载信息，支持细粒度的流量解析与行为分析。本文实验使用 Scapy 解析原始 PCAP 文件，并对 PCAP 文件中的敏感字段（IP 地址、HTTP URL、MAC 地址）进行了匿名化处理。

3.3　模型超参数实验

3.3.1　Tsallis 熵阶参数 q

对比使用不同 Tsallis 熵阶参数 q 值（0，0.5，1，1.5，2）时，Tsallis 熵检测阶段的检测效果。具体实验结果见表 1。

表 1　不同 Tsallis 熵阶参数检测结果

q 值	Accuracy	Recall	F1 值	耗时/ms
0	0.852 2	0.921 2	0.906 8	0.023 3
0.5	0.887 3	0.945 3	0.928 6	0.022 5
1	0.938 8	0.972 2	0.960 5	0.021 7
1.5	0.996 9	1.000 0	0.996 4	0.020 5
2	0.996 5	1.000 0	0.997 7	0.017 2

实验结果表明，虽然当 q=1.5 时，Tsallis 熵检测达到了百分之百的召回率，且在准确率方面表现最佳，但处理时延较高。相比之下，当 q=2 时召回率达到百分之百，且处理时延最低仅需 0.017 2 ms/条。在 Tsallis 熵检测阶段的设计中，低耗时是关键目标，确保系统能够快速响应。因此，选择 Tsallis 熵的熵阶参数 q 为 2。

3.3.2　截断流量长度和包数

针对不同截断流量长度和包数配置，模型在 DDoS 分类任务中的表现存在差异。设置实验分析不同流量截断长度（64 byte、128 byte、256 byte、384 byte、512 byte）与包数（从 1 到 10 包）的组合下分类准确率的变化趋势，实验结果如图 8 所示。实验结果表明，截断长度为 256 byte 时，模型的准确性在多个测试场景中表现最佳，尤其是当截断包数为 5 时，分类准确率达到最高。这是因为这一配置能够在提供充足流量信息的同时有效避免冗余信息的引入。相比之下，截断长度为 64 byte 时，由于无法提供足够的流量信息，其分类准确率普遍较低；而截断长度为 512 byte 和 384 byte 时，虽然包含更多流量信息，但过多的冗余信息反而降低了分类的准确率。

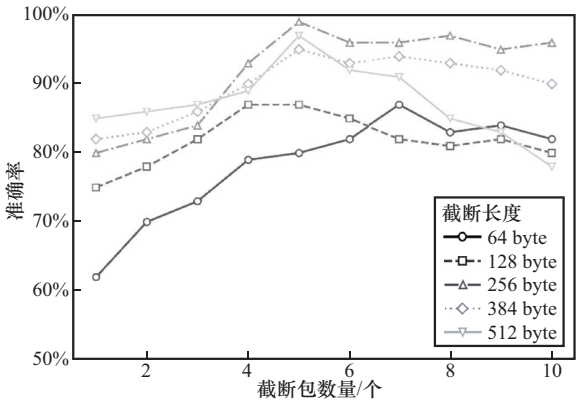

图 8　不同截断流量长度和包数组合下准确率的变化趋势

3.3.3　流量窗口大小和滑动步长

流量窗口大小和滑动步长对熵值计算及动态阈值调整起着关键作用，实验测试了窗口大小（20～70 s）与步长（5～15 s）的多种组合下准确率的变化，结果如图 9 所示。

实验结果表明，随着窗口的增大，检测准确

率会有所提升。这是因为大窗口能够尽可能覆盖攻击周期（如持续30～50 s的洪泛攻击），从而增强流量熵值异常特征的表征，进而提升检测准确率，但同时也增加了检测延时。此外，固定窗口下，步长越小准确率越高。这是因为小步长通过高重叠率确保攻击起始阶段的快速捕获，而大步长因窗口分割效应导致攻击特征分散在多窗口中，熵值异常被稀释。通过方差分析得到最优参数组合为60 s窗口+5 s步长，该配置平衡了检测准确性与检测实时性要求，在可接受的延迟范围内能够实现对DDoS攻击的高效识别。

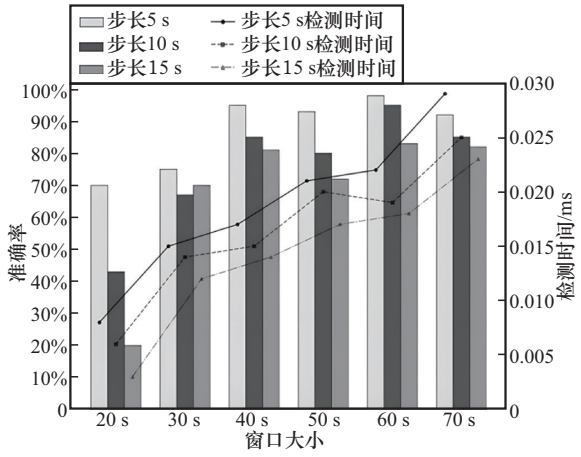

图9　不同窗口策略下准确率的变化

3.4　双阶段DDoS攻击检测分类方法实验

3.4.1　双阶段有效性实验

为验证双阶段结构的有效性，设计了对比实验。每组实验设置如下。

M1：仅有Tsallis熵检测阶段。

M2：仅有DDoSMamba检测阶段。

M3：双阶段检测。

DDoS攻击检测结果见表2，DDoS攻击分类结果见表3。实验结果表明，双阶段检测（M3）的Accuracy、Recall和F1值指标均优于单阶段方法（M1、M2），且检测耗时相比M2明显降低。这主要归因于Tsallis熵检测阶段能够快速筛选正常网络流量，使DDoSMamba分类模型仅对筛选后的异常流量进行处理，从而减少冗余计算并提升检测效率。

表2　DDoS攻击检测结果

方法	Accuracy	Recall	F1值	耗时/ms
M1	0.766 5	1.000 0	0.903 3	0.022 2
M2	0.998 3	0.998 4	0.998 3	0.102 3
M3	0.999 6	1.000 0	0.999 2	0.062 4

表3　DDoS攻击分类结果

方法	Accuracy	Recall	F1值	耗时/ms
M2	0.997 3	0.998 4	0.998 2	0.132 2
M3	0.999 3	1.000 0	0.999 3	0.067 2

3.4.2　分类算法

为验证DDoSMamba模型作为分类算法的有效性，在DDoS攻击流量分类任务上将DDoSMamba与其他深度学习方法进行对比，结果见表4。

表4　DDoS攻击分类结果

方法	Accuracy	F1值	参数量/KB	耗时/ms
Transformer	0.974 3	0.928 5	98.337 2	0.485 2
BiLSTM	0.927 7	0.872 4	85.354 7	0.528 7
TCN	0.991 4	0.946 7	68.744 2	0.357 3
CNN	0.824 5	0.809 1	17.957 7	0.284 4
DNN	0.763 3	0.748 7	8.495 3	0.185 4
DDoSMamba	0.997 1	0.996 5	4.974 4	0.123 2

在相同特征工程条件下，DDoSMamba模型展现出显著的分类性能优势，其准确率与F1值均优于其他模型，且实现了0.123 2 ms的检测耗时和4.974 4 KB的极低参数量。DDoSMamba模型的动态参数化状态空间模型（SSM）的序列建模机制，有效克服Transformer在长序列下的注意力稀释问题及TCN固定感受野导致的跨会话时序特征丢失问题。同时，通过选择性扫描算法替代传统注意力机制，将计算复杂度从$O(L^2)$降至$O(L)$，规避了Transformer的二次计算瓶颈，参数量大幅降低。在计算架构层面，DDoSMamba模型采用CUDA内核融合和状态复用机制，使模型在保持分类精度的同时也提高了运算速度。

3.4.3　混合检测分类方法

为评估本文提出的DDoSMamba方法的分类性能，将其与现有多种方法进行对比实验，实验结果见表5。所有实验均在CIC-DDoS2019数据集上进行，并对数据进行了相同的预处理操作，以确保实验条件的一致性与公平性。

表5　不同方法评估指标

方法	分类	耗时/ms	参数量/KB	Accuracy
文献[13]	4	0.179 2	4.832 5	0.995 0
文献[16]	2	0.953 2	105.330 4	0.998 2
文献[21]	2	0.535 4	75.658 2	0.987 6
文献[22]	2	0.423 7	56.326 7	0.986 2
文献[23]	12	0.723 2	63.324 2	0.923 2
文献[24]	2	0.195 2	4.952 8	0.995 0
文献[25]	2	0.152 6	2.235 3	0.955 8
文献[26]	2	0.822 7	1.054 0	0.996 8
文献[27]	12	0.455 2	12.830 4	0.995 0
DDoSMamba	2	0.062 4	3.875 4	0.999 6
	12	0.067 2	4.553 8	0.999 3

表5表明，DDoSMamba模型通过融合流级别时序特征与包级别细粒度信息实现了对多层级特征的挖掘，在二分类任务中，准确率达99.96%，较文献[16]方法提升0.14%；12分类任务中准确率达99.93%，优于其他模型。通过低秩近似与子空间划分，将模型参数量压缩至3.875 4 KB，仅为RNN+AE的7.2%，有效地降低了计算资源的消耗。文献[26]中的FP-Growth签名提取方法虽参数量仅1.054 KB，但因缺乏筛选机制，耗时高达0.822 7 ms；DDoSMamba模型通过双阶段架构快速筛选出攻击流量，在二分类任务中的耗时降至0.062 4 ms，12分类任务中的耗时降低至0.067 2 ms。实验证明，DDoSMamba模型的双阶段DDoS攻击检测分类方法不仅提高了检测效率，还在实际应用中展现了高效、可靠的特性，在计算资源需求较高的环境中部署时，具有明显的优势。

3.5　消融实验

为验证低秩近似、子空间划分和双向Mamba在DDoSMamba模型中的有效性，设计了4种模型结构，并在CIC-DDoS2019数据集上进行多分类消融对比实验。消融实验结果见表6。实验结果表明，完整DDoSMamba结构（即双向Mamba+低秩近似+空间划分）在仅4.553 8 KB参数量的情况下，实现了99.93%的准确率与0.087 2 ms的检测耗时。双向Mamba通过双向状态传递增强了时序特征提取能力，较单向Mamba有效提升了分类性能。在此基础上，引入低秩近似和空间划分，进一步大幅降低了参数量。消融实验结果验证了本文所采用各方法在提升模型性能与控制计算复杂度方面的有效性。

表6　消融实验结果

模型结构	Accuracy	耗时/ms	参数量/KB
单向Mamba	0.977 5	0.052 2	3.556 4
双向Mamba	0.995 3	0.132 7	17.877 5
双向Mamba+低秩近似	0.997 5	0.127 3	8.974 6
双向Mamba+空间划分	0.997 4	0.096 2	13.650 7
双向Mamba+低秩近似+空间划分	0.999 3	0.087 2	4.553 8

4　结束语

针对现有DDoS攻击检测分类模型中存在的问题，本文提出了一种新的流量表征方案和双阶段DDoS攻击检测分类方法。该流量表征方案融合流级别信息和包级别信息，从多维度表征流量，从而提高流量的分类准确率。在DDoS攻击检测分类方法中，初检阶段利用Tsallis熵和动态阈值方法快速筛选出攻击流量，大幅减少DDoS攻击分类耗时。在实现攻击分类时，本文提出了DDoSMamba模型，该模型在Mamba的基础上，引入双向结构，并通过模型结构优化，在保持高精度的同时，减少了计算复杂度和网络规模。在CIC-DDoS2019数据集上的实验结果表明，本文

所提出的方法在DDoS攻击2分类和多分类任务中，相较于现有混合检测分类方法，具有更高的精度和更低的计算资源消耗。未来研究将探索迁移学习和集成学习等方向，以增强模型对小样本类别的学习能力，从而提升整体分类性能。

参考文献：

[1] De Melo L H, de Carvalho Bertoli G, Nogueira M, et al. Anomaly-flow: a multi-domain federated generative adversarial network for distributed denial-of-service detection[PP]. V1. arXiv (2025-03-18)[2025-07-05]. arXiv: arXiv. 2503.14618.

[2] KöKsal S, Dalveren Y, Maiga B, et al. Distributed denial-of-service attack mitigation in network functions virtualization-based 5G networks using management and orchestration[J]. International Journal of Communication Systems, 2021, 34(9): e4825.

[3] Han T, Jan S R U, Tan Z Y, et al. A comprehensive survey of security threats and their mitigation techniques for next-generation SDN controllers[J]. Concurrency and Computation: Practice and Experience, 2020, 32(16): e5300.

[4] Zhu L H, Liao B C, Zhang Q, et al. Vision mamba: efficient visual representation learning with bidirectional state space model[PP]. V3. arXiv (2024-11-14)[2025-07-05]. arXiv: arXiv. 2401.09417.

[5] Qu J, Ma X B, Li J F. TrafficGPT: breaking the token barrier for efficient long traffic analysis and generation[PP]. V2. arXiv (2024-03-18)[2025-07-05]. arXiv: arXiv. 2403.05822.

[6] 郑承蔚, 王海凤, 刘瑞 . SDN 中 DDoS 攻击检测研究综述[J]. 计算机工程与应用, 2024, 60(24): 79-96.
Zheng C W, Wang H F, Liu R. Review of research on DDoS attack detection in SDN[J]. Computer Engineering and Applications, 2024, 60(24): 79-96.

[7] Gu A, Dao T. Mamba: linear-time sequence modeling with selective state spaces[PP]. V2. arXiv (2024-05-31) [2025-07-05]. arXiv: arXiv. 2312.00752.

[8] Neres Carvalho R, Luiz Bordim J, Adilio Pelinson Alchieri E. Entropy-based DoS attack identification in SDN[C]//Proceedings of the 2019 IEEE International Parallel and Distributed Processing Symposium Workshops (IPDPSW). Piscataway: IEEE Press, 2019: 627-634.

[9] Ujjan R M A, Pervez Z, Dahal K, et al. Entropy based features distribution for anti-DDoS model in SDN[J]. Sustainability, 2021, 13(3): 1522.

[10] Li R Y, Wu B. Early detection of DDoS based on φ-entropy in SDN networks[C]//Proceedings of the 2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC). Piscataway: IEEE Press, 2020: 731-735.

[11] Hemmati Z, Mirjalily G, Mohtajollah Z. Entropy-based DDoS attack detection in SDN using dynamic threshold[C]//Proceedings of the 2021 7th International Conference on Signal Processing and Intelligent Systems (ICSPIS). Piscataway: IEEE Press, 2022: 1-5.

[12] Ben Said R, Askerzade I. Attention-based CNN-BiLSTM deep learning approach for network intrusion detection system in software defined networks[C]//Proceedings of the 2023 5th International Conference on Problems of Cybernetics and Informatics (PCI). Piscataway: IEEE Press, 2023: 1-5.

[13] Zainudin A, Ahakonye L A C, Akter R, et al. An efficient hybrid-DNN for DDoS detection and classification in software-defined IIoT networks[J]. IEEE Internet of Things Journal, 2023, 10(10)：8491-8504.

[14] Bhutto A B, Vu X S, Elmroth E, et al. Reinforced Transformer learning for VSI-DDoS detection in edge clouds[J]. IEEE Access, 2022, 10: 94677-94690.

[15] Le T T H, Heo S, Cho J, et al. DDoSBERT: Fine-tuning variant text classification bidirectional encoder representations from transformers for DDoS detection[J]. Computer Networks, 2025, 262: 111150.

[16] Wang H M, Li W. DDosTC: a Transformer-based network attack detection hybrid mechanism in SDN[J]. Sensors, 2021, 21(15): 5047.

[17] Madhwani P P, Kutty A P K, Mookerjea B, et al. A compact cryogenic configurable slit unit for a multi-object infrared spectrograph: Design and Development of a prototype at TIFR[PP]. V1. arXiv (2023-08-31)[2025-07-05]. arXiv: arXiv. 2309.00063.

[18] He W, Han K, Tang Y H, et al. DenseMamba: state space models with dense hidden connection for efficient large language models[PP]. V2. arXiv (2024-03-05) [2025-07-05]. arXiv: arXiv. 2403.00818.

[19] Bhat S. Mathematical formalism for memory compression in selective state space model[PP]. V2. arXiv (2024-10-04) [2025-07-05]. arXiv : arXiv. 2410.03158.

[20] Dao T, Gu A. Transformers are SSMs: generalized models and efficient algorithms through structured state space duality[PP]. V1. arXiv (2024-05-31)[2025-07-05]. arXiv: arXiv. 2405.21060.

[21] Elsayed M S, Le-Khac N A, Azer M A, et al. A flow-based anomaly detection approach with feature selection method

against DDoS attacks in SDNs[J]. IEEE Transactions on Cognitive Communications and Networking, 2022, 8(4): 1862-1880.

[22] Elsayed M S, Le-Khac N A, Dev S, et al. DDoSNet: a deep-learning model for detecting network attacks[C]//Proceedings of the 2020 IEEE 21st International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM). Piscataway: IEEE Press, 2020: 391-396.

[23] Wei Y Y, Jang-Jaccard J, Sabrina F, et al. AE-MLP: a hybrid deep learning approach for DDoS detection and classification[J]. IEEE Access, 2021, 9: 146810-146821.

[24] Salih A A, Abdulrazaq M B. Cybernet model: a new deep learning model for cyber DDoS attacks detection and recognition[J]. Computers, Materials and Continua, 2024, 78(1): 1275-1295.

[25] 傅友, 邹东升 . SDN 中基于条件熵和决策树的 DDoS 攻击检测方法[J]. 重庆大学学报, 2023, 46(7): 1-8.
Fu Y, Zou D S. A DDoS attack detection method based on conditional entropy and decision tree in SDN[J]. Journal of Chongqing University (Natural Science Edition), 2023, 46(7): 1-8.

[26] Srivastava A, Sinha D. FP-growth-based signature extraction and unknown variants of DoS/DDoS attack detection on real-time data stream[J]. Journal of Information Security and Applications, 2025, 89: 103996.

[27] Ali M, Saleem Y, Hina S, et al. DDoSViT: IoT DDoS attack detection for fortifying firmware Over-The-Air (OTA) updates using vision transformer[J]. Internet of Things, 2025, 30: 101527.

[作者简介]

包晓安（1973– ），男，浙江理工大学计算机科学与技术学院教授，主要研究方向为网络安全、软件可靠性、深度学习。

范云龙（2000– ），男，浙江理工大学计算机科学与技术学院硕士生，主要研究方向网络安全、网络流量分类。

涂小妹（1995– ），女，浙江广厦建设职业技术大学城乡建设学院讲师，主要研究方向为多模态网络入侵检测、信息处理。

胡天缤（1998– ），女，河海大学博士生，主要研究方向为人工智能、软件定义网络。

张娜（1977– ），女，浙江理工大学计算机科学与技术学院教授，主要研究方向为智能信息处理、边缘与分布式安全防护。

吴彪（1989– ），男，博士，浙江理工大学理学院讲师，主要研究方向为软件定义网络、深度学习。