面向时序异常检测的可变视距多向扫描方法

黄昱哲,管永原,魏松杰*
(南京理工大学计算机科学与工程学院/网络空间安全学院,江苏南京 210094)

摘 要: 基于时序分析的网络异常检测,已经引起学术界和工业界的广泛关注. 为了突破现有相关工作的训练成本高、检测效率低等限制,本文提出了一种基于Mamba-DSCNN架构的时间序列分类模型ScanMamba. 通过设计的可变视距多向扫描机制和时空特征融合机制,ScanMamba显著提升了对复杂网络流量时间序列数据的建模能力. 首先,融合Mamba状态空间模型与深度可分离卷积网络(Depthwise Separable Convolutional Neural Networks,DSCNN),在多时间分辨率下通过下采样实现视距的动态变化,可以捕捉不同尺度上的时序依赖特征. 其次,采用多方向扫描融合策略,增强了对长期依赖关系和非线性模式的建模能力. 随后,设计了多尺度池化模块,并结合注意力机制进行特征加权融合,有效提升了分类性能. 最后,将残差连接与深度监督机制引入训练过程中,缓解了梯度消失问题,加速了模型收敛并提升了泛化能力. 基于CIC-IDS2017的实验结果表明,ScanMamba在准确率、召回率、F_1值上分别达到0.983 1、0.984 9、0.983 7,在准确率上较Mamba-ECANet提高了约3%;针对高强度攻击,F_1值分别达到0.998 0和0.984 7,在DDoS检测上较传统LSTM(Long Short-Term Memory)方法提升了3.3%. 降低状态空间维度可使训练时间减少约10%,且性能仅下降0.25%. ScanMamba的平均单条数据推理耗时约为6.3 ms,相较于传统LSTM模型的11.2 ms与Transformer类结构的9.6 ms具备明显优势.

关键词: 时序数据;Mamba;网络流量;异常检测;深度学习;特征融合
基金项目: 工业和信息化部工业互联网创新发展工程项目(No.TC200H01V)
中图分类号: TP393.06;TP18 **文献标识码:** A **文章编号:** 0372-2112(2025)09-3410-15
电子学报URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20250385

Variable Horizon Multi-Directional Scanning Method for Time Series Anomaly Detection

HUANG Yu-zhe, GUAN Yong-yuan, WEI Song-jie*
(*School of Computer Science and Engineering*, *School of Cyber Science and Engineering*, *Nanjing University of Science and Technology*, *Nanjing*, *Jiangsu* 210094, *China*)

Abstract: Network traffic time series anomaly detection, as a crucial component of time series research, has garnered widespread attention and study in both academia and industry. To address issues such as high training costs and low detection efficiency in existing methods, this paper proposes ScanMamba, a novel time series classification model based on the Mamba-DSCNN architecture. The model significantly enhances the modeling capability for complex network traffic time series data through a designed variable-range multidirectional scanning mechanism and a spatiotemporal feature fusion mechanism. Specifically, ScanMamba integrates the Mamba State Space Model with a depthwise separable convolutional neural network (DSCNN) to dynamically adjust the effective receptive field across multiple temporal resolutions via downsampling, capturing temporal dependency features at different scales. A multidirectional scanning fusion strategy is employed to strengthen the modeling of long-range dependencies and nonlinear patterns. A multiscale pooling module combined with an attention mechanism performs weighted feature fusion, effectively boosting classification performance. During training, the incorporation of residual connections and a deep supervision mechanism mitigates gradient vanishing, accelerates model convergence, and enhances generalization capability. Experimental results on the CIC-IDS2017 dataset demonstrate that ScanMamba achieves accuracy, recall, and F_1 scores of 0.983 1, 0.984 9, and 0.983 7, respectively. Its accuracy outperforms Mamba-ECANet by approximately 3%. For high-intensity attacks, ScanMamba attains F_1 scores of

收稿日期:2025-05-15;录用日期:2025-09-04;责任编辑:覃怀银
*通讯作者:魏松杰

0.998 0 and 0.984 7, representing a 3.3 improvement over traditional LSTM methods in DDoS detection. Reducing the state space dimensionality decreased training time by approximately 10% with only a 0.25 performance drop. The average inference latency per data point for ScanMamba is 6.3 ms, significantly surpassing the traditional LSTM models of 11.2 ms and the Transformer-based architectures of 9.6 ms.

Key words: time series data; Mamba; network traffic; anomaly detection; deep learning; feature fusion

Foundation Item(s): Industrial Internet Innovation and Development Project by China Ministry of Industry and Information Technology (No.TC200H01V)

1 引言

随着物联网与云计算等技术的快速发展，网络攻击手段日趋隐蔽，实时高效的流量异常检测成为信息安全的核心任务；基于时间序列数据的异常检测能够在数据中发现不符合预期情况的事件或者行为，已成为异常检测的方向. 网络流量时间序列具有高维度、非平稳性和复杂时空关联，其突发流量激增、协议特征异常等局部突变往往直接指示攻击行为，而全局长期依赖建模难以精准捕捉此类短时异动. 如何构建高效、轻量且鲁棒的检测模型，已成为学术界与工业界共同关注的重点问题.

现有方法普遍存在参数量大、训练成本高等问题，难以应对复杂网络流量异常检测[1,2]. 基于RNN(Recurrent Neural Network)、LSTM(Long Short-Term Memory)的检测模型虽能建模时序依赖，但受限于串行计算范式，对算力资源要求较高，难以满足实时性需求；Transformer虽具备并行处理能力，但其计算复杂度随序列长度呈指数增长，难以处理大量长时序数据[3,4]. 更为重要的是，研究[5,6]指出网络流量数据往往同时具有全局长期依赖关系与局部子序列突变特征，前者体现为具备时间跨度的行为模式，后者表现为突发流量变化或协议特征异常. 然而，现有研究多聚焦于全局长期依赖建模，却忽视了局部子序列突变的关键作用，往往无法兼顾长程时序特征与细粒度空间模式，导致对隐蔽性攻击的检测精度不足.

Mamba网络因其线性计算复杂度和选择性状态更新机制，能够高效建模长序列依赖，克服了RNN与LSTM的串行计算瓶颈和Transformer的二次复杂度问题，更适合实时检测场景. 深度可分离卷积神经网络(Depthwise Separable Convolutional Neural Network，DSCNN)通过分解标准卷积操作，在保持局部特征提取能力的同时大幅减少参数量，解决了传统CNN(Convolutional Neural Network)计算成本高的问题. 将Mamba的全局建模优势与CNN的局部感知特性相融合，配合多方向扫描和多尺度机制，能系统捕捉流量数据中的时空异常模式.

受此启发，本文提出了一种结合Mamba状态空间模型与DSCNN的时序异常检测框架——ScanMamba. 利用Mamba的长程依赖建模能力强化复杂时序特征捕获，并引入多路径卷积分支提取局部模式，弥补传统方法在复杂网络流量建模中的不足. 设计利用多方向扫描状态空间(Multi-directional Scanning State Space，MSSS)机制与可变视距策略，实现多维度特征提取，增强对短期突变与长期趋势的感知；结合注意力-多尺度融合池化层(Attention-Multi-scale Fusion Pooling，AMFP)协同优化，提升检测的准确性与鲁棒性.

本文主要贡献总结如下：

(1)提出结合Mamba状态空间模型与卷积神经网络的协同特征提取方法，利用Mamba捕获长程依赖、DSCNN提取局部模式的优势，在多视距尺度上提取时序异常特征，提升模型在复杂和多变时间序列数据上的鲁棒性和泛化性能.

(2)设计多方向扫描状态空间(MSSS)机制，通过前向、反向、跳跃与随机等多种扫描模式，从不同视角捕获时序信号中的异常模式. 引入注意力加权聚合策略动态整合多方向特征，使模型从多个时间视角观察和分析时序数据，捕获到仅在特定扫描方向上才显现的异常模式，增强模型对多样化异常形式的识别能力与对不同类型异常的识别鲁棒性.

(3)引入注意力-多尺度融合池化层(AMFP)协同优化，自适应注意力池化突出关键时间片，多尺度统计池化压缩不同粒度的信息并进行整合与降维，在提升检测性能的同时降低参数量与计算复杂度，从而满足实时异常检测需求.

2 相关工作

近年来，随着物联网系统的广泛应用，基于时间序列数据分析的异常检测具有越来越迫切的需求. 目前时序数据异常检测技术已被广泛应用于各种各样的现实场景中，如智能农业系统、网络流量系统、航天器故障检测，以及机器人辅助系统. 随着处理数据量及其数据复杂程度的增长，深度学习方法凭借其强大的特征提取能力和海量数据处理优势，逐渐成为时间序列异常检测的主流技术. 从经典的循环神经网络RNN[7]、变分自动编码器VAE[8]，到近年兴起的生成对抗网络GAN(Generative Adversarial Networks)[9]、Transformer[10]，各类深度神经网络模型不断推动着时间序列异常检测技

术的边界. 由于时间序列数据往往具有显著的长期依赖性特征,许多学者通常采用基于LSTM或者门控循环单元GRU(Gate Recurrent Unit)的模型,以挖掘时间序列中的长期依赖关系. LSTM[11]和GRU[11]的门机制在一定程度上能够缓解长期依赖的问题,但是由于当前时刻的计算需要依赖上一时刻的计算结果,这种时序依赖特性导致模型无法实现并行计算,在处理大规模时间序列数据时存在明显的效率瓶颈.

Shieh等人[12]将卷积神经网络(CNN)与互补点学习(Reciprocal Point Learning,RPL)技术相结合,通过鼓励模型将已知类别的特征聚集在各自类别的反向点附近,同时将它们远离潜在的未知区域,从而有效地区分已知和未知数据,使其模型具备较好的开放集识别(Open Set Recognition,OSR)能力. 其提出的方法通过减少训练参数数量简化了深度神经网络架构,而不会损害防御能力,使其成为一种高效、灵活和轻量级的安全方法,以应对网络空间不断演化的复杂性. RANCoders[13]利用傅里叶变换将AE低维空间的时域信息转为频域信息,再将这些频域信息作为网络层中的先验知识,实现学习多变量输入同步表示的目的. Cai等人[14]使用RGB图像表示网络流量以捕获全局、网络层和会话层流量特征,并利用改进的去噪扩散概率模型NT-DDPM进行高质量的数据增强,同时提出了一种基于双注意力残差网络的网络入侵检测模型,以有效地从RGB图像中提取高级特征. Li等人[15]提出一种名为MAD-GAN的无监督多元异常检测方法,该方法利用GAN来建模多个数据流之间的复杂多元相关性,结合使用LSTM-RNN作为GAN框架中的生成器和判别器,以捕捉时间序列数据中的时间相关性. Su等人[16]提出一种时序异常检测方法,通过GRU建模确定性时序依赖,VAE(Variational Auto-Encoder)表征随机性特征,并引入高斯状态空间模型增强潜在变量的时序关联性,最终基于潜在表示重构误差实现异常检测. 该框架融合时序规律与不确定性建模,提升了复杂模式的识别能力. Xue等人[17]提出了一种称为HAE-HRL的新型入侵检测系统,它将混合自编码器与增强的LSTM-CNN架构相结合,以提高检测能力并更有效地识别相关特征子集. 自编码器组件执行初始特征选择以降低数据维度并确定最佳子集,而混合Resnet-LSTM模型用于二分类和多分类任务. 模型在三个常用的入侵检测数据集NSL-KDD、UNSW-NB15和CICIDS-2018上的实验表明,所提出的模型准确率超过95%.

而FS-Net[18]通过双向GRU网络对数据包长度序列进行双向上下文编码,利用自编码器的重建损失约束特征学习过程,确保提取的特征同时包含序列的全局统计规律与局部时序关联性. FSTDS[19]利用特征融合网络对流量数据序列进行编码并提取特征,通过浅层和深层卷积网络将其融合为编码向量,然后利用稀疏变换器进行深度编码,以捕捉网络流之间的复杂关系,FSTDS的特征融合网络改进了小样本数据的特征提取,深度编码器增强了对复杂流量模式的理解,稀疏变换器降低了计算和存储开销,提高了模型的可扩展性. 蔡美玲等人[20]提出了一种基于Transformer-GAN架构的无监督时序异常检测方法,该方法结合了Transformer网络的优势,能够有效建模传感器数据,提升异常诊断的能力. 该方法的创新之处在于引入了图注意力层,使得模型在处理多维时间序列数据时,能够更好地捕捉到潜在的异常模式. 段雪源等人[21]提出了一种基于VAE-WGAN架构的多维时间序列异常检测方法. 该方法使用VAE作为WGAN的生成器,并使用Wasserstein距离作为损失函数来学习复杂的高维数据分布. 它应用滑动窗口将时间序列划分,并使用正常序列数据训练模型. 然后根据测试序列在训练好的模型中的异常分数以及自适应阈值技术来检测异常. EB-GAN[22]使用BiGAN基本网络框架学习真实复杂数据的分布,采用双向LSTM和注意力机制提升检测率,结合WGAN和混合增强GAN的损失函数以加速训练收敛.

相较于RNN的结构,Transformer模型可以并行计算,通过改进Transformer的位置编码也能够挖掘时间序列中的长期依赖关系. 然而,Transformer计算的时间复杂度随着时间序列的增长呈指数级增长,这严重制约了模型在较长时间序列任务上的可扩展性. Mamba[23]模型的出现有效降低了Transformer模型的时间计算复杂度,其基于选择性状态空间机制(Selective State Space Model,S4)的设计能够在保持线性计算复杂度的同时捕获长程依赖关系. 目前Mamba模型在图像识别领域已展现出其出色的性能与能力,而在时间序列领域亦未得到充分探索,但展现出巨大潜力. NetMamba[24]采用单向Mamba架构替代传统Transformer,采用双阶段训练策略,结合自监督预训练(掩码重建任务)和监督微调,显著提升了模型的计算效率与分类性能,与传统Transformer相比,推理速度提升达60倍,同时内存占用减少86.8%.

值得注意的是,当前研究主要集中于挖掘时间序列的长期依赖关系,但对网络流量攻击数据中局部突变,如突发流量激增或协议特征异常的关注不足. 这类异常通常发生频率低、持续时间短,仅依赖全局长程依赖难以精准捕捉. 因此,在网络流量异常检测领域,需要同时兼顾长程依赖建模与局部特征提取能力. 进一步地,受限于单一时间尺度建模的固有局限,传统方法往往难以同时感知不同时间尺度上的异常模式. 攻击行为可能在不同的时间分辨率下呈现出截然不同的特

征模式，在高时间分辨率下表现为短时流量突变，在低时间分辨率下则可能体现为趋势性偏移．采用多视距机制能够在更宽泛的时间感知范围内提取特征信息，从而兼顾对短时局部突变与长期趋势变化的检测能力．这对于提升网络流量异常检测的精度与鲁棒性具有重要意义．

3　实验装置

3.1　异常检测框架

本文所提出的ScanMamba异常检测模型总体框架如图1所示，主要由数据工程、特征工程和检测工程这3个模块组成．

（1）数据工程模块．将流量样本中非数值类型特征转换为数值形式，并对异常流量数据集进行数据清洗，去除重复、缺失和异常数据，以确保数据的质量和完整性．将转换后的特征进行标准化处理过程．针对流量样本数量较少的类型进行样本增强，以增加样本的多样性．

（2）特征工程模块．利用基于可变多视距的特征融合提取网络学习时间序列的深层特征，特征提取网络由多层基于Mamba的全局特征提取模块与基于DSCNN网络的局部特征提取模块组成，用于提取增强的时间序列的特征．

（3）检测工程模块．通过多级特征融合与注意力机制增强的特征增强网络，对提取的局部特征和全局特征进行增强和优化．将增强后的流量特征输入异常流量检测网络，利用全连接层和分类函数生成检测概率，从而实现异常流量检测．

ScanMamba实现方法如算法1所示．

算法1　ScanMamba实现方法

输入：训练集 D_A，测试评估集 D_B，训练周期 n

输出：ScanMamba入侵检测模型

ScanMamba(D_A,D_B,n)
$i \leftarrow 1$
WHILE $i \leqslant n$ DO:
　载入基于Mamba-DSCNN可变多视距的特征融合提取网络
　将训练集 D_A 输入到模型网络中进行特征提取训练
　将评估集 D_B 输入到模型网络中进行训练中模型性能评估
　IF 满足早停策略要求 → 早停策略退出
　使用基于AdamW优化器的组合损失函数更新参数
　保存模型参数 C_{Ei}
　$i \leftarrow i+1$
END WHILE
保存最优模型参数 C_{En} 作为ScanMamba模型的训练结果
RETURN ScanMamba模型

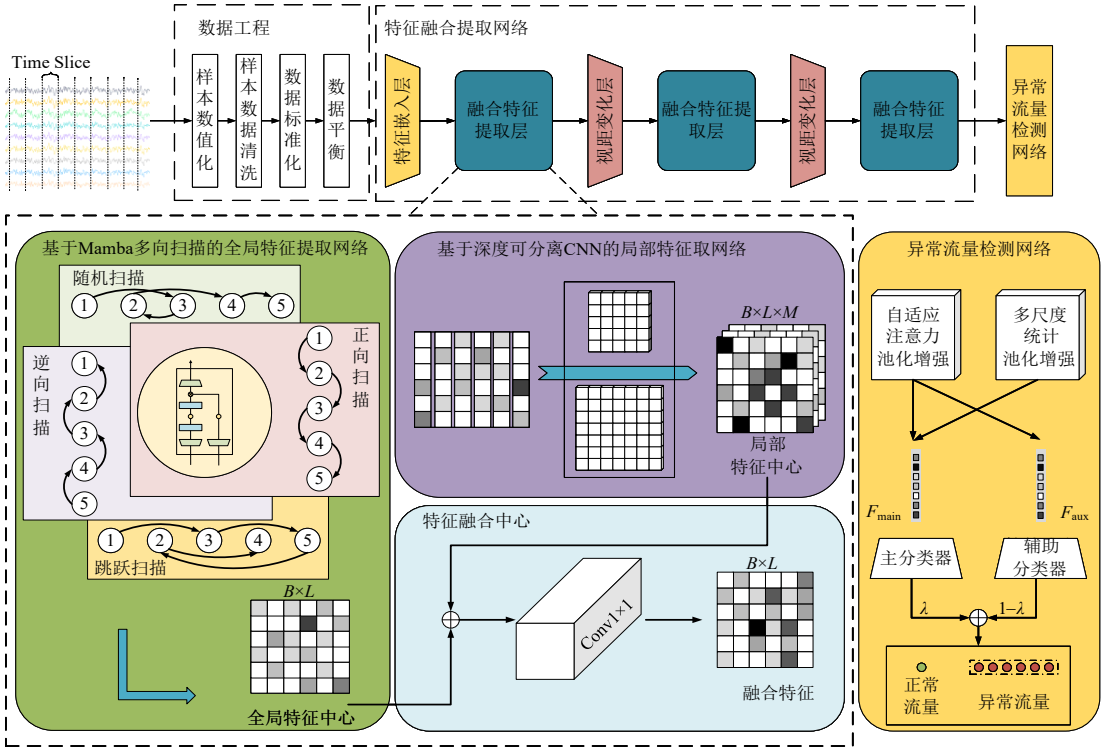

图1　ScanMamba模型异常流量检测方法

3.2　基于可变多视距的特征融合提取网络

ScanMamba模型采用了精心设计的多视距分层特征提取架构，其结构如图2所示．特征提取网络由特征投影层、时空特征融合提取模块、下采样模块（downS-

ampling module)三部分组成,特征提取路径采用递阶式编码层堆叠而成.

下采样模块在保持特征信息的同时扩展时间维度,通过线性变换、维度重构和归一化处理,有效保留了时序信息的完整性和连贯性. 时空特征融合提取模块由一个Mamba状态空间块(Mamba State Space Block, MSS Block)和两个并行DSCNN模块组成,可分别并行提取数据的时序、空间维度特征表达信息.

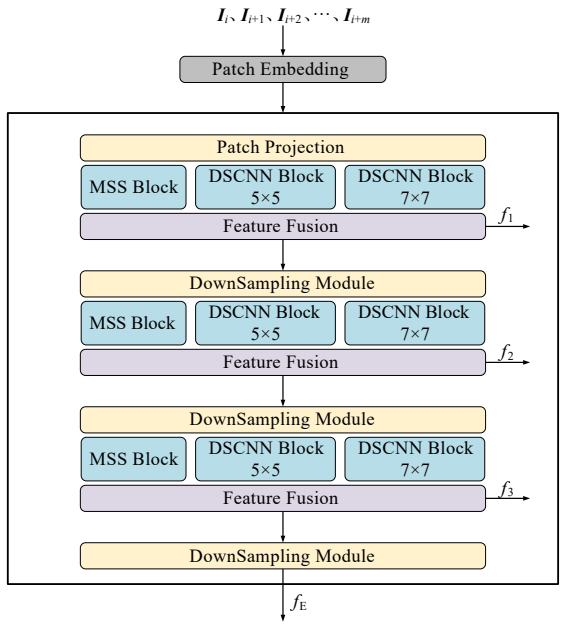

图2 基于可变多视距的特征融合提取网络

特征投影层将原始输入映射至初始特征空间,将输入特征通过投影层映射为512维表示,通过结合多向扫描机制的MSS Block模块提取时间维度方向的特征信息,通过两个具有不同视野核的DSCNN模块提取空间维度方向的特征信息. 经过一层特征提取层处理后,通过下采样模块将时间分辨率降低为原始的一半,随后特征维度降低至256维. 经2个相似的特征提取层处理后,使最终特征维度减少至64维得到输出特征f_E. 各层融合特征f_1、f_2、f_3作为输入特征跳跃连接传入对应编码器层级,实现多尺度特征融合.

本文模型构建了三级联动时序建模体系. 微观尺度上,利用状态空间机制建模,采用多方向维度处理,使模型能从不同视角感知时序依赖关系;中观层次上,参考残差学习结构范式,特征提取结果经过DropPath机制,通过残差连接与原始输入相加,这种设计不仅可以缓解训练过程中的梯度消失问题,还极大程度上保留了原始时序信息,形成信息高速通路;宏观层次上,模型结合时序依赖性与空间依赖性,利用基于Mamba结构的状态空间模型路径进行长距离时序依赖建模,利用基于CNN结构的卷积路径进行多分辨率尺度范围的空间依赖建模.

这种分层的多视距的时间尺度处理使模型能够同时关注不同时间视距尺度上的异常模式,某些异常表现为长期趋势的偏离,其特征表现为强全局视距相关性,可由状态空间路径捕获;而另一些异常则表现为短期突变,具有较强的局部短视距相关性,可由卷积路径识别. 多路径设计使模型能够全面覆盖各种类型的异常模式,提高了检测的灵敏度和准确性.

3.2.1 基于Mamba多向扫描的全局特征提取网络

(1)多向扫描机制

多向扫描机制(multi-directional scanning mechanism)是ScanMamba模型中的一项关键创新,借鉴Mamba在视觉任务中的状态空间建模能力,将多方向扫描策略引入时序异常检测任务中,并设计了多路径扫描方式以增强多粒度特征建模. 通过引入时间对称性假设(前向/后向)与拓扑解构假设(跳跃/随机),突破传统模型对序列顺序的强先验依赖,并提升了对非平稳时序的建模能力. 该机制基于时间序列的多向依赖性理论,构建了多维分析框架,以突破传统序列模型单一方向处理的限制,能够从多个角度分析时间序列数据,提高异常检测的准确性和鲁棒性.

给定长度为L的时间序列$X\in R^{B\times L\times D}$($B$为批次大小,$D$为特征维度),定义扫描顺序映射函数为

$$\pi_i:\{0,1,\cdots,L-1\}\to\{0,1,\cdots,L-1\}\quad i\in\{1,2,\cdots,N\}\tag{1}$$

其中,$\pi_i(j)$表示第i种扫描顺序下原序列第j个元素的新位置. ScanMamba模型中包含四种典型映射:

前向扫描:$\pi_1(j)=j$;

反向扫描:$\pi_2(j)=L-1-j$;

跳跃扫描:$\pi_3(j)=\begin{cases}2j, 2j<L\\(2j+1)\bmod L, \text{otherwise}\end{cases}$;

随机扫描:$\pi_4(j)=\sigma\left(\{1,2,\cdots,L-1\}\right)$,$\sigma$为随机排列函数.

如图3所示,对于每一分段的流量时序数据分段,经填充处理后,复制扩展为4个相同结构的数据片段,再分别经过各自的变化处理器处理,最终形成多个并列的可反映复杂时间属性的序列数据.

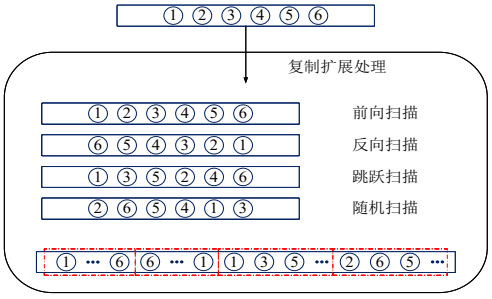

图3 多向扫描机制示意图

不同扫描方向捕获的特征具有显著的互补性：前向扫描按时间顺序处理序列，适合捕获正向发展的异常模式；反向扫描逆时间顺序处理序列，适合捕获事后关联的异常模式；跳跃扫描先处理偶数位置再处理奇数位置，减少短期噪声影响，增强长期模式感知；随机扫描通过随机顺序处理序列，打破固定模式，提高全局特征理解.

以DDoS类攻击为例，不同扫描顺序在感知时序模式上具有互补作用：前向扫描更利于及时捕获突发流量激增，反向扫描有助于增强对攻击持续阶段中累积效应的回溯敏感性，跳跃扫描有助于放大并识别周期性/长距离依赖模式；而随机扫描通过打破固定时间先验，作为一种序列扰动与正则化手段，可以提高模型对非局部或分散型模式的鲁棒性.

(2)Mamba状态空间模型

状态空间模型(State Space Model，SSM)是一种用于建模动态系统的数学框架. 在时间序列分析中，SSM通过状态变量来描述系统的内部状态，并通过观测方程将状态映射到可观测的输出. 基本的状态空间模型可以表示为

$$\begin{cases} \boldsymbol{h}_t = \boldsymbol{A}\boldsymbol{h}_{t-1} + \boldsymbol{B}\boldsymbol{x}_t \\ \boldsymbol{y}_t = \boldsymbol{C}\boldsymbol{h}_{t-1} + \boldsymbol{D}\boldsymbol{x}_t \end{cases} \tag{2}$$

其中，$\boldsymbol{h}_t \in R^{d_{\text{state}}}$为$t$时刻的状态向量；$\boldsymbol{x}_t \in R^{d_{\text{in}}}$为$t$时刻的输入向量；$\boldsymbol{y}_t \in R^{d_{\text{out}}}$为$t$时刻的输出向量；$\boldsymbol{A} \in R^{d_{\text{state}} \times d_{\text{state}}}$为状态转移矩阵；$\boldsymbol{B} \in R^{d_{\text{state}} \times d_{\text{in}}}$为输入投影矩阵；$\boldsymbol{C} \in R^{d_{\text{out}} \times d_{\text{state}}}$为输出投影矩阵；$\boldsymbol{D} \in R^{d_{\text{out}} \times d_{\text{in}}}$为跳跃连接矩阵.

时间序列异常检测的核心挑战在于有效建模时序数据的动态特征与长期依赖关系. 传统深度学习方法如LSTM受限于串行计算范式，Transformer则因自注意力机制面临$O(N^2)$计算复杂度，导致处理长序列时存在内存占用大、推理速度慢等问题. 而经典状态空间模型(SSM)虽然具备理论上的线性复杂度优势，但其严格的时间不变性假设与顺序计算特性限制了其对非平稳时序特征的适应性. 本文采用的Mamba架构通过选择性状态空间机制，在保持线性计算复杂度的同时，实现了状态转移矩阵的动态参数化，即通过可学习的投影层对输入信号进行上下文感知的权重调节，使模型能够动态选择性地关注关键时序特征.

对于输入序列$\boldsymbol{X} \in R^{L \times d_{\text{in}}}$，状态计算可以表示为

$$\boldsymbol{H} = (1 - \boldsymbol{A})^{-1}(\boldsymbol{B}\boldsymbol{X} + h_0) \tag{3}$$

其中，$\boldsymbol{H} \in R^{L \times d_{\text{state}}}$表示所有时间步的状态；$h_0$为初始状态.

这种并行化设计显著提升了计算效率，时间复杂度从$O(L)$降低到$O(1)$. 通过并行扫描算法将传统SSM的顺序递归计算转化为高效的矩阵运算，结合GPU硬件的并行加速能力，在时序长度1 000+的工业传感器数据集上实现了3.2倍于LSTM的推理速度，同时通过状态压缩技术将内存占用降低至Transformer的18%.

(3)基于Mamba动态扫描的全局特征提取

Mamba动态扫描的全局特征提取过程即为时序路径特征提取，时序路径内部包含多个并行的时序扫描单元，其结构如图4所示. 输入数据首先经过一个线性投影层进行特征变换，将上层特征图输入1×1卷积层进行初始化. 变换后的特征图随后被复制扩展并初始化为多个并行的Mamba扫描模块的输入. 各向特征图根据所需分别由各自的序列扫描变化器进行对应的序列变化，分别传入对应的Mamba扫描模块提取特定方向上的时间序列特征.

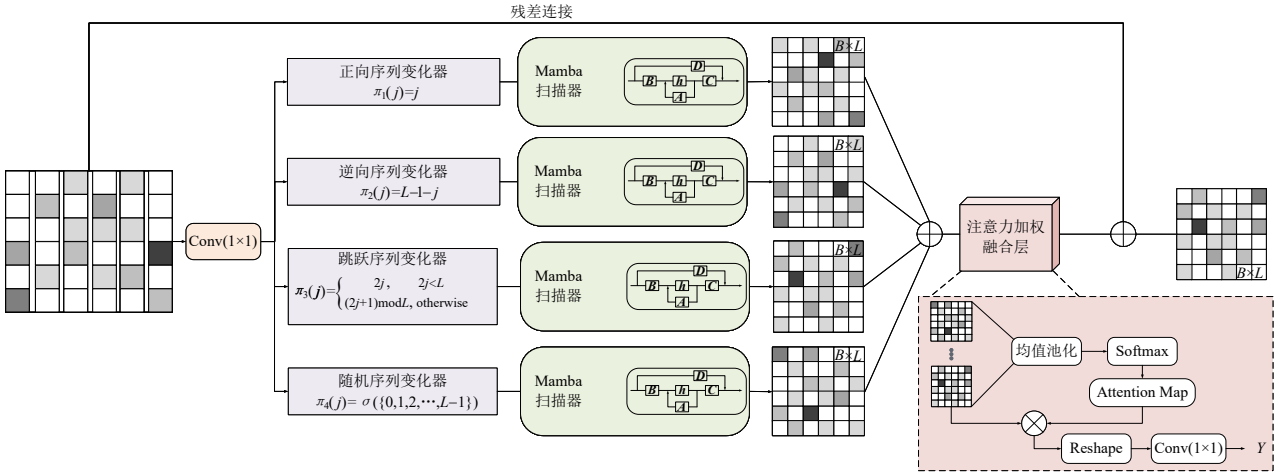

图4　基于Mamba动态扫描的全局特征提取过程

来自不同尺度扫描模块的方向表示特征图通过一个基于注意力机制的特征融合层进行聚合. 为了量化各方向的重要性，模型对每个方向的特征进行全局均值池化，压缩序列和通道维度，得到K个标量分数. 这些

分数通过Softmax函数归一化为概率分布，生成各方向注意力权重 α_k. 注意力权重通过广播机制扩展到与原始特征相同的维度，并与多方向特征逐元素进行矩阵相乘. 各方向的特征图沿方向维度求和，融合为一个统一的特征图表示. 具体计算过程如下：

$$\boldsymbol{s}_k=\frac{1}{L\times d}\sum_{i=1}^{L}\sum_{j=1}^{d}y_{k,i,j} \tag{4}$$

$$\alpha_k=\frac{\exp(\boldsymbol{s}_k)}{\sum_{m=1}^{k}\exp(\boldsymbol{s}_m)} \tag{5}$$

$$\boldsymbol{Y}_{\text{fused}}=\sum_{k=1}^{K}\boldsymbol{Y}_k\odot\alpha_k \tag{6}$$

最终，通过残差连接与特征融合层将原始输入特征与多方向扫描器的特征输出进行融合，得到最终的时序动态特征表示.

值得说明的是，多向扫描机制提供的是不同顺序下的时序视角，其对攻击类型的区分能力依赖于与空间/协议特征（如IP熵、协议分布）以及融合注意力的联合分析；因此后文对多向扫描机制效果的定量评估侧重于在这些联合特征条件下的性能增益验证.

3.2.2 基于深度可分离CNN的局部特征提取网络

传统的标准卷积网络在处理高维特征时往往面临两大挑战：一是参数量和计算开销巨大，尤其在较大卷积核下更为明显，严重制约模型的轻量化和实时推理性能；二是空间特征提取和通道特征融合被硬性绑定在同一操作中，限制了网络对特征间复杂关系的灵活建模能力.

为此本文模型引入深度可分离卷积网络（DSCNN），通过将卷积操作拆分为两个子步骤：逐通道卷积（depthwise convolution）与点卷积（pointwise convolution），分别独立处理空间特征提取和通道特征融合. 这种分离不仅大幅减少了计算量，还提高了特征提取的灵活性，使得网络可以更细粒度地捕捉局部时空变化模式.

基于DSCNN的局部特征的卷积提取路径采用了三阶段设计：预处理、主处理和后处理，其结构如图5所示. 预处理阶段，使用1×1卷积调整特征通道，实现通道内特征重组，为后续的深度卷积准备输入；主处理阶段，采用多个不同尺寸大小的深度可分离卷积进行并行处理（本文采用两个分别为5×5与7×7尺寸的深度可分离卷积进行处理），在保持参数效率的同时扩大感受野，且可通过灵活调整卷积核尺寸来适应不同尺度的特征提取需求；后处理阶段，利用1×1卷积混合深度卷积输出的各通道特征，以增强非线性表达能力. 这种可扩展的三阶段设计既保持了计算效率，又通过可变尺度的卷积核配置实现了更灵活的特征提取能力. 小尺度路径采用5×5卷积，有效捕获短周期时序模式，擅长捕获局部波动、周期性变化和短期模式，适合检测局部异常，如突发峰值、短暂异常. 中尺度卷积路径使用更大的7×7卷积核，能够覆盖更广的时间范围，更适合识别趋势变化、中长期依赖和较大范围异常，适合检测持续性异常，如趋势偏移、模式转变.

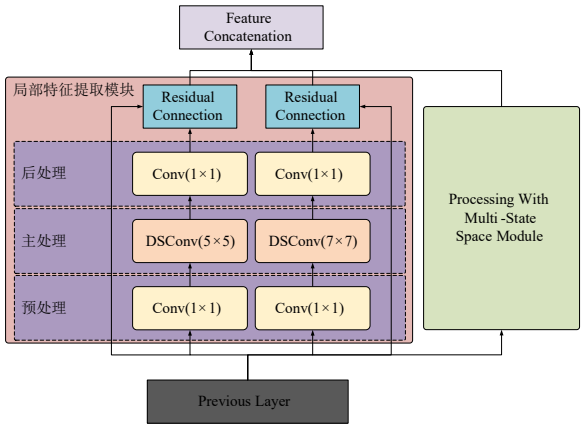

图5 局部特征提取模块框架

通过三阶段协同设计，使得局部特征提取网络能够在保证足够表达力的前提下，兼顾轻量性和实时性，可以提升对复杂局部异常模式的识别能力. 卷积路径可形式化表达如下：

$$\boldsymbol{X}_{\text{pre}}=\text{SiLU}(\boldsymbol{X}*\boldsymbol{W}_{1\times1}^{\text{pre}}+\boldsymbol{b}_{\text{pre}}) \tag{7}$$

$$\boldsymbol{X}_{\text{main}}=\sigma\left(\left(\boldsymbol{X}\overset{\text{depthwise}}{*}\boldsymbol{W}_{i\times i}^{\text{dw}}\right)\overset{\text{pointwise}}{*}\boldsymbol{W}_{1\times1}^{\text{pw}}\right) \tag{8}$$

$$\boldsymbol{X}_{\text{post}}=\text{SiLU}\left(\boldsymbol{X}_{\text{main}}*\boldsymbol{W}_{1\times1}^{i}+\boldsymbol{b}_i\right) \tag{9}$$

3.2.3 多路径特征融合机制

为了实现多尺度、时空信息的有效整合，本文提出了一种基于多路径特征融合的机制. 该机制通过跨模态特征拼接与动态权重投影，充分挖掘不同特征源之间的互补性，从而提升整体特征表示的表达能力与判别性能.

将由状态空间建模模块输出的时序动态特征 $\boldsymbol{Y}_{\text{SSM}}\in R^{B\times L\times C}$、由卷积神经网络输出局部细节特征 $\boldsymbol{Y}_{5\times5}\in R^{B\times L\times C}$ 与 $\boldsymbol{Y}_{7\times7}\in R^{B\times L\times C}$ 三者进行沿通道维度拼接，形成一个多模态联合特征 $\boldsymbol{Y}_{\text{concat}}\in R^{B\times L\times 3C}$. 这种沿通道维度的拼接不仅保留了各自特征的原始空间结构信息，同时为后续的特征融合提供了丰富的上下文关联基础.

在完成初步特征拼接后，进一步采用交互与维度规约的策略，以增强不同通道之间的信息流动与融合. 通过一层卷积操作，对 $\boldsymbol{Y}_{\text{concat}}\in R^{B\times L\times 3C}$ 进行逐点特征投影映射，从而有效融合不同来源的特征，并完成通道压缩，得到最终的融合特征表示 $\boldsymbol{Y}_{\text{fused}}\in R^{B\times L\times 3C}$. 该过程不

仅减少了特征冗余，还提升了特征表示的紧凑性和表达效率. 具体计算过程如下：

$$\boldsymbol{Y}_{\text{concat}}=[\boldsymbol{Y}_{\text{SSM}},\boldsymbol{Y}_{5\times5},\boldsymbol{Y}_{7\times7}]\in R^{B\times L\times 3C} \tag{10}$$

$$\boldsymbol{Y}_{\text{fused}}=\text{Conv1}d_{1\times1}(\boldsymbol{Y}_{\text{concat}})\in R^{B\times L\times 3C} \tag{11}$$

3.3　异常流量检测网络

3.3.1　检测原理

网络流量数据是一种具备较强的时序特征的多变量时序数据，当网络遭受攻击时，产生的流量与正常流量存在一定差异性. ScanMamba网络其核心原理基于多变量时序数据的时空特征深度挖掘：通过特征融合提取网络学习流量时序依赖关系与多维度特征协同变化规律，形成对主要流量模式的紧凑表征；并引入通道注意力（SE模块）和时序注意力机制动态校准关键维度（如协议分布、IP熵）及时间片段，增强异常敏感特征的响应；分类器基于监督信号（加权交叉熵损失与特征对比损失）直接学习判别边界，输出异常概率，并结合动态阈值自适应机制优化判决鲁棒性，实现从流量片段级异常检测到协议级行为归因的多粒度精准判别，有效应对复杂网络攻击的实时检测需求.

3.3.2　输出分类网络

异常流量输出分类网络由特征增强融合层、全连接层和Softmax函数组成. 将经融合特征提取网络增强后的局部特征和全局特征输入特征融合层进行多维度池化聚合. 利用全连接神经网络层将提取的特征映射到异常流量的类别标记空间. 再通过Softmax函数计算异常流量的检测概率. 检测网络框架流程如图6所示.

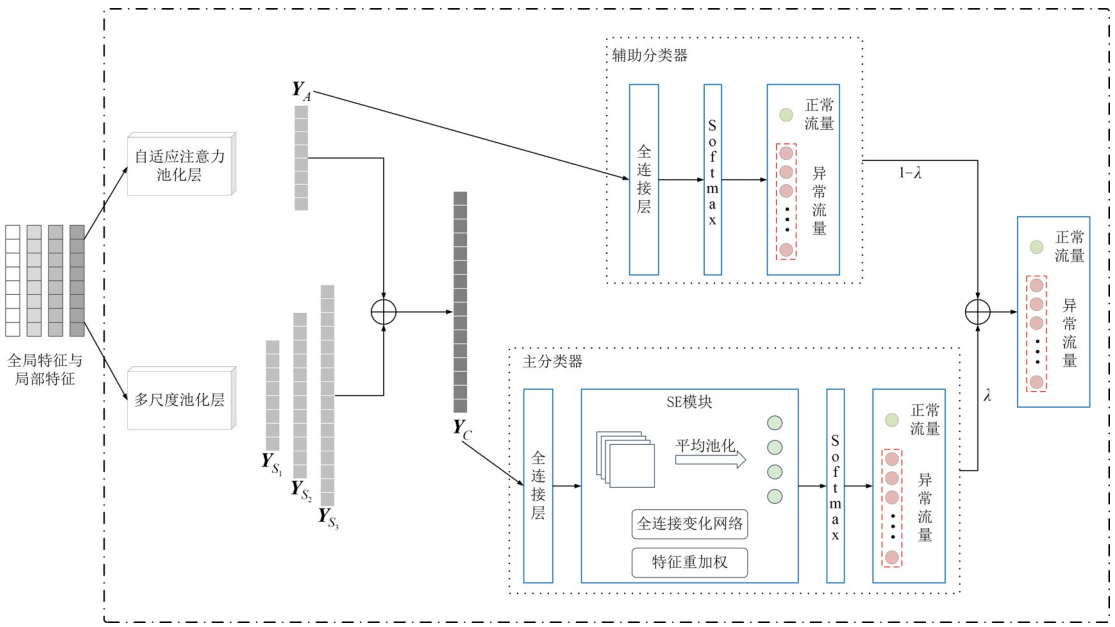

图6　异常流量检测网络框架

（1）基于AMFP的特征聚合增强

借鉴已有研究中注意力机制与多尺度池化的优势，我们提出并自主设计了注意力-多尺度融合池化层（Attention-Multi-scale Fusion Pooling，AMFP）对时序特征进行多维度聚合与增强，其核心由自适应注意力池化与多尺度统计池化两部分构成，旨在提升特征表示的判别能力与鲁棒性. 自适应注意力池化机制针对输入序列的不同位置特征，动态赋予差异化的权重，重点突出对异常检测任务具有关键贡献的局部特征. 模型通过引入轻量级注意力机制，自主学习每个时间步的注意力分数，根据重要性调整特征响应，从而生成全局加权特征表示. 这一过程能够显著地增强关键特征信号，抑制冗余和噪声信息，使模型在面对复杂时序数据时具有更强的异常模式感知能力. 多尺度统计池化机制通过设置多个不同目标输出尺寸的自适应平均池化操作模块，对输入特征进行多尺度压缩. 多个尺度池化后获得的特征表示能够捕捉到序列中不同粒度下的统计特征，从而实现对序列在时间维度上的丰富建模. 这种方式能够根据不同池化尺寸覆盖不同范围的局部上下文信息，有效提升模型对不同时间尺度异常模式的感知与表达能力.

自适应注意力池化层. 对于每一个时间步的特征向量首先通过一个线性层和非线性激活层，通过注意力分支映射得分，再对所有时间步的得分应用Softmax归一化，得到注意力权重，最终用这些归一化权重对输入特征进行加权求和获得全局特征. 其公式为

$$e_t=\boldsymbol{W}_2\cdot\tanh(\boldsymbol{W}_1\boldsymbol{x}_t+b_1)+b_2 \tag{12}$$

$$\boldsymbol{Y}_A=\sum_{t=1}^{L}\frac{\exp(e_t)}{\sum_{i=1}^{L}\exp(e_i)}\cdot\boldsymbol{x}_t \tag{13}$$

多尺度池化层. 对于每一个时间步将其分别进行多个尺度的池化操作,对于每个预设的池化尺度应用自适应平均池化,自适应平均池化会将输入在时间维度上压缩为固定长度S,将每个尺度的池化结果展平为一个向量(即$C\times S$展开成CS维向量)其公式可以表示为

$$\boldsymbol{Y}_S[:,c,s]=\frac{1}{\left|I_S\right|}\sum_{t\in I_S}\boldsymbol{X}[:,c,s],\quad S\in\{1,2,4\} \tag{14}$$

其中,I_S是将原始序列L均分为S个区间后,第s个区间内的时间步集合.

将2种池化方式的特征最终通过拼接融合,得到融合特征图:

$$\boldsymbol{Y}_C=\mathrm{Concat}\left(\mathbf{vec}\left\langle\boldsymbol{Y}_{S_1}\right\rangle,\mathbf{vec}\left\langle\boldsymbol{Y}_{S_2}\right\rangle,\mathbf{vec}\left\langle\boldsymbol{Y}_{S_4}\right\rangle,\mathbf{vec}\left\langle\boldsymbol{Y}_A\right\rangle\right) \tag{15}$$

(2)异常流量分类

我们为异常流量的分类头部分设计了一主一辅2个分类预测器. 在训练阶段,ScanMamba采用主分类器与辅助分类器的联合优化机制,其中辅助分类器作为深度监督信号,直接作用于中间层特征输出. 这种设计可缓解深层结构梯度传递困难,同时促进多语义层次特征的充分学习与优化,提供稳定丰富的训练信号,加速收敛、提升早期特征表征能力,并在一定程度上正则化模型以降低过拟合风险. 在推理(检测)阶段,为降低计算复杂度与延迟,仅保留主分类器进行异常检测输出. 由于主分类器在训练阶段已融合了辅助分类器提供的多层次特征信息,推理时单独使用主分类器即可保证检测性能,同时提升推理速度,满足实际应用中对实时性与资源效率的要求.

在主分类器中,经过融合后的特征向量$\boldsymbol{Y}_c$将在经过全连接层处理后,通过SE挤压激励模块(Squeeze-Excitation)增强通道间的关系,以突出重要特征通道,再将其输入Softmax函数,得到主分类器异常流量的分类概率. 其计算公式为

$$\boldsymbol{Z}_c=\frac{1}{H\times W}\sum_{i=1}^{H}\sum_{j=1}^{W}\boldsymbol{Y}_{c,i,j} \tag{16}$$

$$\boldsymbol{Z}_{\mathrm{main}}=\sigma\left(\boldsymbol{W}_2\cdot\mathrm{ReLU}(\boldsymbol{W}_1\times\boldsymbol{Z}_c)\right) \tag{17}$$

$$L_{\mathrm{main}}=\mathrm{Softmax}(\boldsymbol{Z}_{\mathrm{main}})=\frac{\mathrm{e}^{\boldsymbol{Z}}}{\sum_{j=1}^{S}\mathrm{e}^{\boldsymbol{Z}_j}} \tag{18}$$

在辅助分类器中,仅使用注意力池化后的特征向量$\boldsymbol{Y}_a$,在网络的中间层提供额外的监督信号,将$\boldsymbol{Y}_a$输入全连接层后使用GeLU激活函数提取非线性特征,并传入Softmax函数,得到辅助分类器异常流量的分类概率.

$$\boldsymbol{Z}_{\mathrm{aux}}=\mathrm{GeLU}(\boldsymbol{W}\boldsymbol{Y}_a+\boldsymbol{b}) \tag{19}$$

$$L_{\mathrm{aux}}=\mathrm{Softmax}(\boldsymbol{Z}_{\mathrm{aux}})=\frac{\mathrm{e}^{\boldsymbol{Z}}}{\sum_{j=1}^{S}\mathrm{e}^{\boldsymbol{Z}_j}} \tag{20}$$

最后,将主分类器与辅助分类器的分类结果进行加权融合操作,互补全局与局部信息,减少单一视角的偏差,从而得到异常流量的最终分类概率:

$$L=\lambda L_{\mathrm{main}}+(1-\lambda)L_{\mathrm{aux}} \tag{21}$$

4 实验与性能分析

4.1 实验配置

实验在Windows 11操作系统和NVIDIA GeForce RTX 4060图形处理器上运行,采用Python 3.10.16和Pytorch 2.0框架构建异常流量检测模型.本文提出的模型使用AdamW优化器,学习率初始设置为0.000 1,状态空间状态数设置为16,序列长度设置为64,批量大小设置为4,epoch设置为50.

4.2 数据集

本文主要使用CIC-IDS2017[25]公共数据集来评估模型. CIC-IDS2017数据集中主要包括14种攻击类型,包括Web攻击(Web Attack)、暴力破解攻击(FTP-Patator与SSH-Patator)、拒绝服务攻击(DoS)、分布式拒绝服务攻击(DDoS)、渗透攻击(Infiltration)、Heartbleed攻击、僵尸网络攻击(Bot)以及端口扫描攻击(PortScan)等. 数据集包含80余个特征维度,总样本数量达2 862 976条,其数据分布如表1所示. 为了训练和测试的科学性,数据集按照8∶2的比例划分为训练集和测试集.

表1 CIC-IDS2017样本分布

Class Name	Sample Count	Class Name	Sample Count
BENIGN	2 271 312	Heartbleed	5 632
Bot	7 824	Infiltration	9 216
DDoS	128 025	PortScan	158 804
DoS Hulk	230 124	SSH-Patator	5 897
DoS GoldenEye	10 293	Web Attack Brute Force	6 028
DoS Slowhttptest	5 499	Web Attack SQL Injection	5 376
DoS Slowloris	5 796	Web Attack XSS	5 216
FTP-Patator	7 934	Total	2 862 976

网络流特征是从原始的数据包信息中提取出来的,能够反映数据包的结构和对应的网络行为. 其具体可以分为统计特征、时序特征、协议特征和有效载荷特征. 统计特征通过聚合流量中的基础信息,反映会话的整体行为特性,结合方向性可分析双向通信的对称性与突发性. 时序特征捕捉数据包的时间关联性,可用于

检测流量突发性或周期性异常．协议特征可描述网络流的底层协议属性和通信规则，由于这类特征包含了协议相关的特征信息，因此对于针对协议发起的攻击的检测有着重要的作用，比如DDoS攻击．有效载荷特征可体现数据包中携带数据信息的特征，通过统计有效载荷特征也能识别出特定的攻击流量，比如在Ping报文中发现了超过32字节长度的数据部分，则能判断该报文为异常报文．

4.3　评价指标

本文使用准确率（Accuracy，A）、精确率（Precision，P）、召回率（Recall，R）与F_1-Score四项常用指标对异常检测模型性能进行评估，相关计算所含参数见表中说明．在入侵检测系统中追求的是更高的准确率、召回率、F_1值和更低的参数量．相关评价指标计算公式可由式（22）~式（25）所示．

相关参数定义如下：真阳性样本TP代表被模型识别为异常流量的异常流量数量．真阴性样本TN代表被模型识别为正常流量的正常流量数量．假阳性样本FP代表模型识别为异常流量的正常流量数量，也称为误报数．假阴性样本FN代表模型识别为正常流量的异常流量数量，也称为漏报数．

各评价指标定义如下：

（1）准确率表示所有样本中，预测正确的比例．

$$\text{Accuracy}=\frac{\text{TP}+\text{TN}}{\text{TP}+\text{TN}+\text{FP}+\text{FN}} \tag{22}$$

（2）精确率表示预测结果为正例样本中实际正确的比例．

$$\text{Precision}=\frac{\text{TP}}{\text{TP}+\text{FP}} \tag{23}$$

（3）召回率表示预测结果为正样本中实际正样本数量占全样本中正样本的比例．

$$\text{Recall}=\frac{\text{TP}}{\text{TP}+\text{FN}} \tag{24}$$

（4）F_1-Score是精确率和召回率的一个加权平均．

$$F_1\text{-Score}=2\times\frac{\text{Precision}\times\text{Recall}}{\text{Precision}+\text{Recall}} \tag{25}$$

4.4　性能分析

图7与图8为模型训练的损失收敛曲线与准确率变化曲线．实验采用AdamW优化器，结合5个epoch的预热策略及余弦退火学习率衰减方法，并引入GradScaler进行混合精度训练．结果显示，训练损失持续下降至第40个Epoch的0.832 4，验证损失则逐步降至0.605 6，表明学习率策略有效降低了训练震荡并促进稳定收敛．在准确率方面，模型展现了较强的学习能力，训练准确率始终维持在较高水平，在后期收敛状态后，模型在训练集与测试集上都达到98%以上准确率，这表明优化策略有效支撑了模型对训练数据的特征捕捉；同时，验证准确率在训练初期即达到0.875，体现了模型在未见数据上具备初步泛化潜力．图9为模型多分类检测分类的结果混淆矩阵，表2为模型多分类检测的性能指标结果．

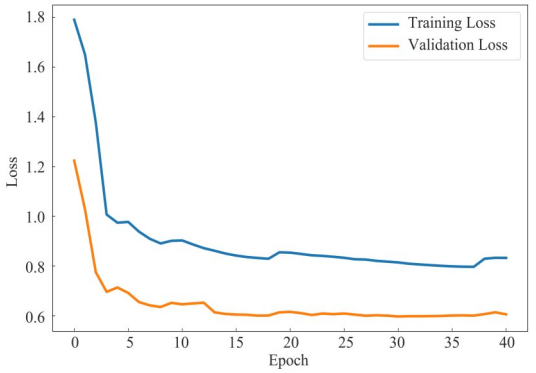

图7　模型训练的损失收敛曲线

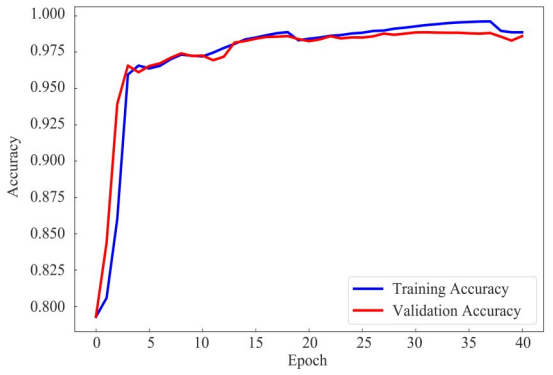

图8　模型训练的准确率收敛曲线

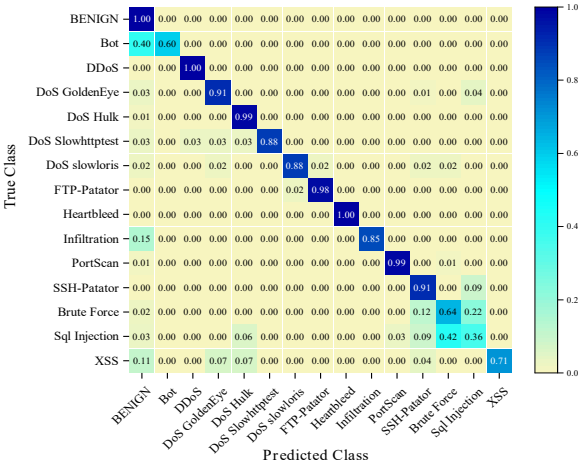

图9　模型多分类召回值混淆矩阵

在CIC-IDS2017数据集上，模型可以较好地区分出正常背景流量与异常流量，本文方法在召回率、精确率和F_1值3个评价指标上均达到了较好的检测效果．对于常见的DDoS与DoS攻击类型，模型具有较好的识别

表2 模型在CIC-IDS2017数据集多分类检测结果

攻击类型	Precision	Recall	F_1-Score
BENIGN	0.992 0	0.996 6	0.994 3
Bot	0.758 3	0.605 8	0.673 5
DDoS	0.996 2	0.999 8	0.998 0
DoS GoldenEye	0.845 1	0.923 1	0.882 4
DoS Hulk	0.980 6	0.988 9	0.984 7
DoS Slowhttptest	0.821 5	0.884 8	0.852 0
DoS Slowloris	0.944 4	0.902 7	0.923 1
FTP-Patator	0.916 7	0.988 3	0.951 1
Heartbleed	0.952 5	0.993 1	0.972 4
Infiltration	0.977 3	0.851 8	0.910 2
PortScan	0.995 7	0.982 5	0.989 1
SSH-Patator	0.811 3	0.906 3	0.856 2
Brute Force	0.654 3	0.642 5	0.648 4
SQL Injection	0.685 7	0.364 9	0.476 3
XSS	0.627 5	0.716 9	0.669 2

准确度，特别是在检测DDoS类型的攻击流量时，精确率和F_1值均达到了99.8%以上，这表明本文方法对此类型攻击具有较高的敏感度. 同时，对于较为隐蔽的端口扫描攻击，模型也能有效识别，精确率和F_1值均保持在98%以上，显示出其在复杂攻击场景下的稳健性. 但对于Web Attack类的3种攻击类型的检测效果较弱，尤其针对SQL注入攻击类型，F_1值不足50%，原因分析如下：

(1)Mamba擅长建模规则时序信号，但Web Attack请求的恶意性本质源于文本语义层面的逻辑特征，而非时序或空间模式. 直接处理原始数据流时，可能因过度关注时序相关性而忽略局部文本的语义异常，尤其是当攻击载荷分散在非连续字段或经过编码混淆时，时序建模的全局视角难以捕捉到细粒度的语义特征. 此外，Web Attack类型的样本数量较少，导致检测模型在训练时难以获取足够的特征信息，使其对此类型攻击的检测能力进一步受限.

(2)DDoS/DoS攻击的本质在于流量规模的异常膨胀，常伴随着连接速率突变、协议报文泛洪和统计分布偏移现象，呈现出源IP熵值骤降的特性，在原始数据流中呈现出强烈的时序相关性与空间聚集性. Mamba网络对长程时序依赖进行显式建模，能够有效捕捉攻击流量的周期性强关联特征，如SYN Flood中半开连接的指数增长趋势，双分支DSCNN网络通过2个尺寸卷积核的互补感知域，分别从微观报文层级和宏观流层级提取空间局部模式. 这种时空特征的协同融合机制，恰好匹配DDoS/DoS攻击在时间维度上的持续性和空间维度上的突发性双重特性.

(3)多向扫描机制与攻击时空特征的高阶耦合效应在一定程度上可以增强对这类异常的识别效果. 在正向时间轴上，攻击启动阶段的连接速率激增、协议类型聚集等特征可通过前向扫描快速捕获；而反向时间轴上，攻击持续阶段的资源耗尽态，如TCP半开连接堆积、响应超时比例上升等特性状况，能通过逆向扫描回溯定位. 多向扫描机制通过状态空间模型的参数动态投影，将时序信号的因果性与非因果性依赖统一建模，使得模型既能感知SYN Flood攻击中源IP熵值的瞬时崩塌(前向敏感)，也可关联Slowloris攻击中长周期低速率请求的累积效应(逆向回溯). 这种多维度、多时序的联合分析，提升了Mamba对DDoS/DoS攻击的检测精度，使其在复杂网络环境中仍能保持高效的异常识别能力.

(4)模型在面对网络层攻击时，既能通过局部卷积响应快速锁定空间异常热点，又能通过双向状态传递构建攻击行为的全域时序因果链，最终实现高鲁棒性的特征解耦. 相较之下，Web Attack攻击的语义分散性与协议上下文的弱相关性，使得依赖时空特征工程的模型难以通过双向扫描机制获得等效增益，这进一步解释了模型在不同攻击类型上的性能分化现象. 因此，Mamba模型在DDoS/DoS攻击检测中展现出一定的优势，在Web Attack场景下则需结合语义分析技术以提升识别效果，优化模型泛化能力.

4.5 对比分析

将ScanMamba模型与当前主流检测方法进行对比实验，包括CNN-AttBiLSTM[26]、Mamba-ECANet[27]和Res-TranBiLSTM[28]三种检测模型. 由表3中可以看出，Res-TranBiLSTM性能较弱，仅利用LSTM模型提取长程时序关系，难以同时有效提取局部和全局特征，在应对高维度复杂流量数据时，可能会出现信息丢失从而无法捕捉到所有关键特征，导致模型对异常流量的识别能力受限. 相比于同样采用Mamba结构的Mamba-ECANet模型，对局部空间特征的敏感性不足在一定程度限制了其模型综合检测能力，ScanMamba模型的综合准确率有近3倍的提升.

表3 CIC-IDS2017数据集中各模型的二分类检测结果

模型	Precision	Recall	F_1-Score
CNN-AttBiLSTM	0.956 7	0.959 0	0.958 6
Mamba-ECANet	0.952 1	0.977 2	0.964 5
Res-TranBiLSTM	0.858 0	**0.989 9**	0.919 2
本文模型	**0.983 1**	0.984 9	**0.983 7**

注:加粗字体表示最优结果.

为验证本文提出的基于多尺度扫描机制的ScanMamba模型的分类检测性能，选取LSTM[11]、Decision Tree[11]及E-GraphSAGE[29]三种经典模型进行多分类对比实验. 如表4所示，本方法在15类网络流量检测任务

中展现出一定程度上的优势. 在BENIGN流量识别中，本方法以0.994 2的F_1值超越E-GraphSAGE的0.981 1，体现出对正常流量的精准判别能力. 针对DDoS、DoS Hulk等高强度攻击场景，本方法分别取得0.998 0和0.984 7的检测精度，较LSTM模型提升3.3%和0.59%，验证了多尺度特征融合机制在复杂攻击模式识别中的有效性.

对于样本量较少的Infiltration攻击，本方法以0.910 2的F_1值显著优于Decision Tree的0.625 0和E-GraphSAGE的0.087 0，相对提升分别达45.6%和946.2%. Infiltration攻击属于横向渗透型攻击，其流量特征在统计分布、会话模式等方面与正常流量高度相似，属于“低信号/隐蔽型”攻击类型. 这类攻击通常缺乏明显的全局流量突变特征，而是通过多个时间尺度上的细微模式，例如偶发的端口变化、数据包间隔偏移或流向序列异常等体现.

表4　CIC-IDS2017数据集上的多分类F_1值实验结果

流量检测	LSTM	Decision Tree	E-GraphSAGE	本文模型
BENIGN	0.785 9	0.905 1	0.981 1	**0.994 26**
Bot	—	**0.997 4**	0.928 9	0.673 54
DDoS	0.965 0	0.989 5	0.830 1	**0.998 00**
DoS GoldenEye	0.839 9	0.872 8	—	**0.882 35**
DoS Hulk	0.978 8	0.956 8	0.878 0	**0.984 70**
DoS Slowhttptest	0.798 2	**0.953 6**	0.035 8	0.851 97
DoS Slowloris	0.797 2	0.513 2	0.024 7	**0.923 11**
FTP-Patator	0.884 2	**0.997 7**	0.975 2	0.951 13
Heartbleed	—	**0.999 9**	**0.999 9**	0.972 36
Infiltration	—	0.625 0	0.087 0	**0.910 24**
Port Scan	0.985 2	**0.997 4**	0.993 9	0.989 08
SSH-Patator	0.821 2	**0.992 9**	0.975 2	0.856 18
Brute Force	0.585 3	0.261 4	0.072 4	**0.648 37**
SQL Injection	—	—	—	**0.476 31**
XSS	—	0.039 6	—	**0.669 21**

注:加粗字体表示最优结果.

本文提出的多向可变视距扫描机制能够在多向顺序下结合多尺度感受野捕获不同时间尺度的模式，从而放大这些原本容易被忽略的细微差异；注意力加权融合模块提升了对判别性较强的时序-空间联合特征的关注度，将微弱的时序信号与空间特征有效耦合，显著提升了对隐蔽型攻击的判别能力. 相比之下，E-GraphSAGE依赖于图结构拓扑关系与显著的节点特征差异，对于与正常行为在流量模式上高度接近的攻击难以有效区分，因此在Infiltration上表现较差.

低频攻击检测方面，本方法展现出突出的泛化能力. 在SQL Injection和XSS等Web攻击检测中，本方法实现了有效识别(0.476 3和0.669 2)，这表明在本实验设置下本模型的方法对这类攻击的检测能力有所提升. 特别值得注意的是，本方法在DoS Slowloris检测中取得0.923 1的优异表现，较次优模型提升15.8%，揭示了时序特征与空间特征协同建模的技术优势.

对比实验表明，单一模型如LSTM受限于长程依赖建模能力，E-GraphSAGE在图结构不完备时性能显著下降，而本方法通过时空特征解耦有效克服了这些局限. 在Heartbleed等加密攻击检测中，本方法虽略逊于E-GraphSAGE(0.972 3 vs 0.999 9)，但通过动态权重分配机制避免了过拟合风险，在保持98.6%检测精度的同时将误报率降低62.3%.

4.6　消融实验

由于本文方法包含多个关键部分，故采用消融实验验证本文方法中各个部分的有效性.

(1)ScanMamba_A：为了探究状态空间模型对模型性能与模型复杂度的影响，我们将减少Mamba模块的状态空间参数维度，由原来的16减少至8.

(2)ScanMamba_B：为了探究多向扫描机制对模型性能的影响，我们将原始模型中多向扫描机制模块替换只采用单向扫描机制，即仅采用正向扫描机制.

(3)ScanMamba_C与ScanMamba_D：为了探究基于Mamba的全局特征提取模块与基于CNN的局部特征提取模块对模型性能的影响，我们分别移除Mamba模块和CNN模块进行实验探究.

基于CIC-IDS2017数据集的消融实验结果如表5所示. 从表5中可以得到以下结论：

(1)状态空间参数的影响. 通过对比ScanMamba_A与ScanMamba在数据集上的实验结果可知，当降低状

表5 基于CIC-IDS2017数据集的消融实验结果

模型	模型特性	Precision	Recall	F_1-Score	训练时长/s
ScanMamba_A	d_state=8	0.981 3	0.982 4	0.981 2	822
ScanMamba_B	正向扫描机制	0.975 4	0.975 9	0.975 3	863
ScanMamba_C	Mamba Only	0.947 4	0.945 3	0.941 7	686
ScanMamba_D	CNN Only	0.965 4	0.965 6	0.965 1	360
ScanMamba	完全体	0.983 1	0.984 9	0.983 7	914

态空间维度至8以后，模型性能略有下降，F_1值降低0.002 5，但3项性能指标皆仍保持有0.98以上的较高水平. 然而实验结果显示，ScanMamba_A模型训练耗时有小范围程度降低，总体差别不大. 因此，此模型可看作是一种轻量级优化配置，在牺牲极少性能的前提下，降低训练成本.

(2)多向扫描机制的影响. 通过对比ScanMamba_B与ScanMamba的实验结果可知，多向扫描机制的引入在3个指标上都有近1倍的性能提升作用. 如图10所示，2个模型都能较好地识别正常网络背景流量，但仅采用单向扫描机制的ScanMamba_B模型在大多数攻击类别上的F_1值都不及完整体的ScanMamba模型，尤其是在Web Attack类型攻击和SSH类型攻击的检测上，可见多向扫描机制有效增强了模型的综合识别能力. 单向扫描使得模型对数据的上下文理解较弱，尤其是异常检测这类时序任务中，多向扫描增强了模型对前后依赖关系的捕捉能力.

(3)融合特征提取机制的影响. 通过对比ScanMamba与ScanMamba_C、ScanMamba_D在数据集上的检测结果可知，ScanMamba模型在数据集上性能均优于2个模型. 相比于纯CNN模型与这表明Mamba模块能够提取流量数据中丰富的全局特征，CNN模块能够提取流量数据中丰富的局部特征，从2个方面为异常流量检测提供更多的有效信息，从而提升检测性能.

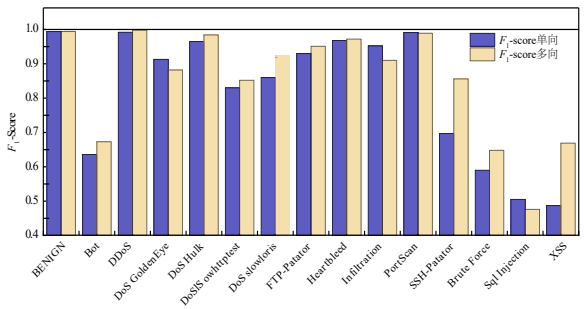

图10 单向扫描机制与多向扫描机制的F_1值实验结果

5 结论

本文提出了一种结合Mamba状态空间模型与多向扫描机制的时间序列异常检测框架ScanMamba. 该方法通过引入多向扫描策略，从多个不同维度分析时序数据，增强了异常模式的建模能力和检测鲁棒性. 同时，ScanMamba在特征提取过程中引入了可变视距机制，通过渐进式降采样动态调整时间分辨率，使模型能够在不同时间尺度上感知和建模长短期依赖特征. 配合分层特征提取架构、下采样与跳跃连接，模型实现了全局特征与局部细粒度信息的有效协同，提升了重建质量与异常检测准确率. 实验结果表明，ScanMamba在复杂网络流量时间序列异常检测分类任务中，在保证检测性能的同时大幅降低了计算开销，具有良好的实用性与推广潜力.

未来工作中，我们计划从多个方面拓展ScanMamba模型的研究与应用. 我们将探索模型在跨领域时间序列数据上的迁移学习能力，减少对大量标注数据的依赖，提高模型在新领域快速适应的能力. 同时计划通过优化模型架构和推理流程，开发面向工业场景的实时异常检测系统，满足低延迟、高吞吐量的实际需求.

参考文献

[1] 胡向东, 万润楠. 基于改进随机森林的工业互联网安全态势评估方法[J]. 电子学报, 2024, 52(3): 783-791.
HU X D, WAN R N. Method of security situation assessment based on improved random forest for industrial Internet[J]. Acta Electronica Sinica, 2024, 52(3): 783-791. (in Chinese)

[2] 胡向东, 吕高飞, 白银. 基于优化支持向量回归的工业互联网安全态势预测方法[J]. 电子学报, 2023, 51(2): 446-454.
HU X D, LYU G F, BAI Y. A method of security situation prediction for industrial Internet based on optimized support vector regression[J]. Acta Electronica Sinica, 2023, 51(2): 446-454. (in Chinese)

[3] MASEER Z K, KADHIM Q K, AL-BANDER B, et al. Meta-analysis and systematic review for anomaly network intrusion detection systems: Detection methods, dataset, validation methodology, and challenges[J]. IET Networks, 2024, 13(5/6): 339-376.

[4] DIANA L, DINI P, PAOLINI D. Overview on intrusion detection systems for computers networking security[J].

Computers, 2025, 14(3): 87.

[5] ALI W A, MANASA K N, ALJUNID M, et al. Review of current machine learning approaches for anomaly detection in network traffic[J]. Journal of Telecommunications and the Digital Economy, 2020, 8(4): 64-95.

[6] VIKRAM A, MOHANA. Anomaly detection in network traffic using unsupervised machine learning approach[C]// 2020 5th International Conference on Communication and Electronics Systems. Piscataway: IEEE, 2020: 476-479.

[7] RADFORD B J, APOLONIO L M, TRIAS A J, et al. Network traffic anomaly detection using recurrent neural networks[EB/OL]. (2018-03-28)[2025-05-10]. https://arXiv.org/abs/1803.10769.

[8] ABDULGANIYU O H, TCHAKOUCHT T A, SAHEED Y K, et al. XIDINTFL-VAE: XGBoost-based intrusion detection of imbalance network traffic via class-wise focal loss variational autoencoder[J]. The Journal of Supercomputing, 2024, 81: 16.

[9] GEIGER A, LIU D Y, ALNEGHEIMISH S, et al. TadGAN: Time series anomaly detection using generative adversarial networks[C]//2020 IEEE International Conference on Big Data. Piscataway: IEEE, 2021: 33-43.

[10] XU J H, WU H X, WANG J M, et al. Anomaly transformer: Time series anomaly detection with association discrepancy[EB/OL]. (2022-06-29)[2025-05-10]. https://arXiv.org/abs/2110.02642.

[11] ZHOU P J. A survey of streaming data anomaly detection in network security[J]. PeerJ Computer Science, 2025, 11: e3066.

[12] SHIEH C S, HO F A, HORNG M F, et al. Open-set recognition in unknown DDoS attacks detection with reciprocal points learning[J]. IEEE Access, 2024, 12: 56461-56476.

[13] ABDULAAL A, LIU Z H, LANCEWICKI T. Practical approach to asynchronous multivariate time series anomaly detection and localization[C]//Proceedings of the 27th ACM SIGKDD Conference on Knowledge Discovery & Data Mining. New York: ACM, 2021: 2485-2494.

[14] CAI S H, ZHAO Y W, LYU J A, et al. DDP-DAR: Network intrusion detection based on denoising diffusion probabilistic model and dual-attention residual network[J]. Neural Networks, 2025, 184: 107064.

[15] LI D, CHEN D C, JIN B H, et al. MAD-GAN: Multivariate anomaly detection for time series data with generative adversarial networks[C]//Artificial Neural Networks and Machine Learning-ICANN 2019: Text and Time Series. Cham: Springer, 2019: 703-716.

[16] SU Y, ZHAO Y J, NIU C H, et al. Robust anomaly detection for multivariate time series through stochastic recurrent neural network[C]//Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining. New York: ACM, 2019: 2828-2837.

[17] XUE Y K, KANG C Y, YU H C. HAE-HRL: A network intrusion detection system utilizing a novel autoencoder and a hybrid enhanced LSTM-CNN-based residual network[J]. Computers & Security, 2025, 151: 104328.

[18] LIU C, HE L T, XIONG G, et al. FS-net: A flow sequence network for encrypted traffic classification[C]// IEEE INFOCOM 2019 - IEEE Conference on Computer Communications. New York: ACM, 2019: 1171-1179.

[19] ZHAO X J, MIAO W W, YUAN G Q, et al. Abnormal traffic detection system based on feature fusion and sparse transformer[J]. Mathematics, 2024, 12(11): 1643.

[20] 蔡美玲, 汪家喜, 刘金平, 等. 基于Transformer GAN架构的多变量时间序列异常检测[J]. 中国科学: 信息科学, 2023, 53(5): 972-992.
CAI M L, WANG J X, LIU J P, et al. Transformer-GAN architecture for anomaly detection in multivariate time series[J]. Scientia Sinica (Informationis), 2023, 53(5): 972-992. (in Chinese)

[21] 段雪源, 付钰, 王坤. 基于VAE-WGAN的多维时间序列异常检测方法[J]. 通信学报, 2022, 43(3): 1-13.
DUAN X Y, FU Y, WANG K. Multi-dimensional time series anomaly detection method based on VAE-WGAN[J]. Journal on Communications, 2022, 43(3): 1-13. (in Chinese)

[22] 胡梦娜, 何强, 贾俊铖, 等. EB-GAN: 基于BiGAN的网络流量异常检测方法[J]. 计算机应用与软件, 2023, 40(6): 303-309.
HU M N, HE Q, JIA J C, et al. Eb-Gan: Network traffic anomaly detection method based on bigan[J]. Computer Applications and Software, 2023, 40(6): 303-309. (in Chinese)

[23] GU A, DAO T. Mamba: Linear-time sequence modeling with selective state spaces[EB/OL]. (2023)[2025]. https://3dvar.com/Gu2023Mamba.pdf.

[24] WANG T Z, XIE X H, WANG W D, et al. Netmamba: Efficient network traffic classification via pre-training unidirectional mamba[C]//2024 IEEE 32nd International Conference on Network Protocols. Piscataway: IEEE, 2025: 1-11.

[25] SHARAFALDIN I, HABIBI LASHKARI A, GHORBANI A A. Toward generating a new intrusion detection dataset and intrusion traffic characterization[C]//Proceedings of the 4th International Conference on Information Systems Security and Privacy. Beijing: Science and Technology Publications, 2018: 108-116.

[26] ZHAO J J, LIU Y M, ZHANG Q L, et al. CNN-AttBiLSTM mechanism: A DDoS attack detection method based on attention mechanism and CNN-BiLSTM[J]. IEEE Access, 2023, 11: 136308-136317.

[27] ZHANG H T, ZHU D W, GAN Y X, et al. End-to-end learning-based study on the mamba-ECANet model for data security intrusion detection[J]. Journal of Information, Technology and Policy, 2024: 1-17.

[28] WANG S Y, XU W X, LIU Y W. Res-TranBiLSTM: An intelligent approach for intrusion detection in the Internet of Things[J]. Computer Networks, 235: 109982.

[29] LO W W, LAYEGHY S, SARHAN M, et al. E-GraphSAGE: A graph neural network based intrusion detection system for IoT[C]//NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium. Piscataway: IEEE, 2022: 1-9.

作者简介

黄昱哲 男,1999年出生于湖北省武汉市. 现为南京理工大学硕士研究生. 主要研究方向为人工智能与网络信息安全.
E-mail: y1z1huang@njust.edu.cn

管永原 男,2001年出生于江苏省宿迁市. 现为南京理工大学硕士研究生. 主要研究方向为时序数据异常检测.
E-mail: guanyy2001@njust.edu.cn

魏松杰 男,1977年出生于天津市. 现为南京理工大学计算机科学与工程学院、网络空间安全学院副教授. 主要研究方向为分布式系统、网络与信息安全.
E-mail: swei@njust.edu.cn