XXXX

基于ResNet18的SRv6网络流量异常检测研究

摘　要：随着基于 IPv6 的段路由（Segment Routing over IPv6，SRv6）在新一代网络中的广泛部署，其可编程性和灵活性显著提升了网络性能，但也带来了新的安全挑战。传统的基于特征规则或阈值的方法在应对复杂、多样化的攻击流量时往往表现不佳，尤其难以识别针对 SRH（Segment Routing Header）的异常行为。因此，如何在 SRv6 环境下实现高效、准确的异常流量检测，成为亟待解决的问题。为此，本文提出了一种基于深度学习的 SRv6 网络流量异常检测方法。实验结果表明，本文方法在准确率、召回率和 F1-score 等指标上均优于传统机器学习算法和部分主流深度学习模型，能够有效识别多类攻击流量。本文的主要创新点包括：（1）构建了“异常类型—可观测特征—检测指标”三层映射机制，系统性刻画 SRv6 协议特有异常行为的可感知特征；（2）提出一种面向 SRv6 场景的流量图像化表示方法，并结合残差网络实现高维特征的自适应提取；（3）在缺乏公开 SRv6 异常数据集的条件下，设计了基于协议规范与威胁模型的特征扩展机制，实现了 SRv6 场景下的验证性实验框架。在 SRv6 场景下，该方法为面向可编程网络的安全防护提供了一种可扩展的技术路径。

关键词：SRv6；深度学习；异常检测；异常流量；ResNet18

中图分类号：TP393.08

文献标志码：A

doi: 10.11959/j.issn.1000−0801.

Research on SRv6 Network Traffic Anomaly Detection Based on ResNet18

Abstract: With the widespread deployment of Segment Routing over IPv6 (SRv6) in next-generation networks, its programmability and flexibility have significantly improved network performance, but have also brought new security challenges. Traditional methods based on feature rules or thresholds often perform poorly when dealing with complex and diverse attack traffic, especially struggling to identify anomalous behavior targeting the SRH (Segment Routing Header). Therefore, how to achieve efficient and accurate anomaly traffic detection in the SRv6 environment has become an urgent problem to be solved. To this end, this paper proposes a deep learning-based method for anomaly detection of SRv6 network traffic. Experimental results show that the proposed method outperforms traditional machine learning algorithms and some mainstream deep learning models in terms of accuracy, recall, and F1-score, and can effectively identify multiple types of attack traffic. The main innovations of this paper can be summarized as follows: (1) A three-layer mapping mechanism of "anomaly type - observable features - detection index" is constructed to systematically characterize the perceptible features of the unique abnormal behavior of the SRv6 protocol; (2) A traffic

收稿日期：2025−12−01；**修回日期：**XXXX−01−01

通信作者：通信作者：作者，邮箱

基金项目：国家自然科学基金资助项目（No.xxxxxxx）；浙江省教育厅科学基金资助项目（No.xxxxxxxx）

Foundation Items: The National Natural Science Foundation of China（No.xxxxxxx），Education Department Foundation of Zhejiang Province（No.xxxxxxxx）

image representation method for SRv6 scenarios is proposed, and adaptive extraction of high-dimensional features is achieved by combining residual networks; (3) In the absence of publicly available SRv6 anomaly datasets, a feature extension mechanism based on protocol specifications and threat models is designed to realize a verification experimental framework for SRv6 scenarios. In the SRv6 scenario, this method provides a scalable technical path for security protection of programmable networks.

Key words: srv6, deep learning, anomaly detection, abnormal flow, ResNet18

1 引言

随着互联网流量的迅猛增长以及对更高效、更灵活网络基础设施的需求不断增加，IPv6段路由（Segment Routing over IPv6，SRv6）作为下一代网络技术的解决方案，逐渐获得广泛关注。SRv6不仅简化了网络架构、增强了可扩展性，还实现了不同网络间的无缝互联，使其成为未来通信系统，特别是6G及未来网络中关键技术之一。然而，随着SRv6网络的快速发展以及其所处理的流量模式的日益复杂，使得网络的稳定性、性能和安全性变得愈加具有挑战性。

在现代通信网络中，流量监测是确保网络健康和安全的重要环节。通过持续监测网络流量，网络运营商能够及时发现流量异常、管理流量负载并优化资源分配。尤其在流量异常检测领域，通过识别与正常网络行为不符的流量模式，有效预防网络拥塞、攻击行为以及潜在的系统故障[17]。在SRv6网络中，其动态性为流量的监测和分析带来了更多复杂性，因此，流量异常检测在这一领域的应用尤为关键。传统的网络监测技术通常依赖人工配置和基于规则的静态检测方法，但这些方法在应对SRv6网络中产生的大规模流量时常显得不尽人意，尤其在面对现代网络环境的高度动态性和复杂性时，传统方法的适应性和扩展性受到极大限制。因此，越来越迫切需要智能化、自动化的流量监测方案，以适应网络条件的持续变化，并能够实时准确地检测潜在的流量异常。

现有流量异常检测方法主要面向传统IP或MPLS网络环境展开，其特征构建通常依赖五元组统计特征或报文负载行为模式。然而，SRv6在协议结构与路径控制机制上具有显著差异：第一，SRv6通过SRH扩展头携带Segment List，实现显式路径编程，路径信息嵌入数据平面，传统检测方法难以解析其语义结构；第二，SRv6路径具有动态可编程性，攻击者可在合法SID格式下构造异常路径行为，使得基于固定规则的检测机制失效；第三，SRv6异常往往表现为协议字段合法但语义异常的行为模式，难以通过传统静态规则捕获。

针对上述问题，本文提出了一种基于深度学习技术的SRv6网络流量检测方法，重点在于流量异常检测。通过分析SRv6数据包的各种特征，如丢包率、延迟、带宽利用率和流量模式，开发一种智能系统，能够高效、准确地检测异常流量行为。该方法有望解决检测未知异常的挑战，并减少对手工标记数据的依赖，避免传统方法在大规模数据中的瓶颈问题。本文方法的差异体现在于：

（1）从协议语义层面对SRv6异常进行建模，而非仅基于统计流量特征；

（2）通过图像化映射增强空间结构表达能力，使深度残差网络能够捕获复杂特征交互；

（3）构建适配SRv6的特征工程体系，使模型具备针对SRH相关异常的专门感知能力。

因此，本文工作并非简单应用现有CNN模型，而是针对SRv6协议特性进行定向优化。

本文的其余部分组织如下：第二部分是相关技术介绍，回顾了SRv6技术概念和流量异常类

型，同时介绍了机器学习基础；第三部分介绍了本文方法的具体实现；第四部分描述了实验设置和结果；最后，第五部分对本文进行了总结，并展望了未来的研究方向

2　相关技术

2.1　SRv6 技术概述

SRv6 是一种基于 IPv6 的源路由协议，IPv6 数据平面中的段路由（SRv6）是通过添加一个名为段路由头（Segment Routing Header，SRH）[1] 的 IPv6 扩展头来实现的。这个 SRH 包含一个或多个 128 位的 IPv6 地址，用于编码路径上必须访问的节点和段。每个数据包的路径由源节点确定，路径的各个节点按顺序执行，路径信息通过 SRH 嵌入 IPv6 数据包中，其核心优势在于简化了路由机制，通过源节点指定路径，提高了网络的可编程性和灵活性[2]。SRv6 相比传统多协议标签交换 (Multi-Protocol Label Switching ,MPLS) 协议具有许多优点，包括完全兼容现有 IPv6 网络、简化 VPN 实现、支持高效的网络切片和服务功能链等[12]。它在 5G 核心网、边缘计算、虚拟专用网络等领域具有广泛应用，提供了更高的网络资源调度灵活性和性能。SRv6 通过路径段（Segment Identifier ,SID）实现网络路径的引导，数据包根据指定的段依次转发。分段机制将路径拆分成多个较小的段，并嵌入到数据包的 SRH 中，从而简化了路由决策和提高了网络的可扩展性。如图 1 所示，假设有报文需要从主机 1 转发到主机 2，主机 1 将报文发送给节点 A 处理。节点 A、B、C、D 均支持 SRv6，我们在源节点 A 上进行网络编程，希望报文经过 B-C、C-D 链路，由 D 节点送达主机 2。

2.2　流量异常类型

由于 SRv6 数据包在报文结构、路由机制及网络可编程性上与传统 IP 数据包存在显著差异，其流量异常类型也呈现出独特特征。这使得传统的流量异常检测方法，如基于五元组的统计检测或深度包检测，难以有效识别 SRv6 特有的攻击模式，主要原因可归结为三点：其一，协议复杂性较高，SRv6 头部携带 SRH 及动态 Segment List，传统检测方法无法解析这些信息的语义；其二，路径具有动态性，SRv6 的显式路径可实时编程，导致依赖固定模式的静态规则库完全失效；其三，状态存在隐蔽性，攻击者可利用 SID 的合法形式掩盖恶意行为，例如路径劫持等。

因此，要构建针对 SRv6 的流量异常检测系统，首先需系统性分析其异常类型。基于 SRv6 协议栈及攻击面特征，可将 SRv6 流量异常划分为以下三类：第一类是协议层异常，主要包含两种情况：一是包头字段篡改，攻击者通过伪造 SRH 中的关键字段（如 Segment List、Flags 或 TLV），引发路径劫持或路由循环，例如篡改 Segment List 的指针字段，可能导致报文在非预期节点终止；二是无效 SID 注入，向数据包中插入未分配或保留的 SID（如将本应用于 IPv4 流量的 End.DT4 用于非 IPv4 流量），会触发节点处理异

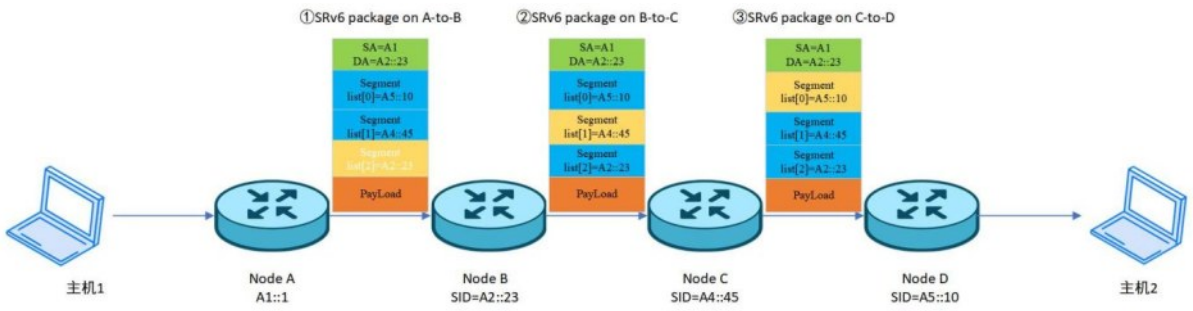


图 1　SRv6 数据报传输图

常，甚至造成CPU、内存等资源耗尽，导致节点性能大幅下降。第二类是流量行为异常，常见表现为两种攻击形式：一是突发性流量泛洪（DDoS攻击），攻击者伪造源地址后，利用SRv6路径聚合特性，向目标发送高密度的UDP或ICMP报文，这类攻击的典型特征是单位时间内SID跳数急剧增加；二是速率慢攻击（LDoS攻击），通过周期性发送微小流量（如每秒仅1个报文）干扰SRv6控制平面，例如影响BGP-LS同步，最终导致路径计算出现振荡，其核心特征是流量时序的自相关性呈现异常。第三类是操作异常，主要包括路径劫持和径循环攻击两种类型：路径劫持是指恶意节点篡改Segment List中的SID序列，将正常流量重定向至窃听节点或攻击节点，该异常的识别特征为路径跳数突然增加，且往返时延（Round-Trip Time，RTT）偏离正常基线；径循环攻击则是通过构造环形SID序列（如A→B→C→A的循环路径），使数据包在环形路径中不断传输，持续消耗网络带宽与节点计算资源，其明显特征是日志记录中会出现同一报文多次经过相同节点的情况。

这些异常通常会反映在以下关键性能指标的偏离中：网络层指标，包括丢包率（异常路径的循环冗余校验（Cyclic Redundancy Check，CRC）错误计数）、端到端延迟（劫持路径的额外跳数延迟）；流量模式指标，包括SID切换频率的熵值、单位时间内SRH解析失败次数；资源利用率指标，例如CPU/内存占用率与流量规模的线性关系断裂。通过量化上述性能指标，结合机器学习模型实现多维度异常检测，具体方法将在第三章详述。

2.3 机器学习基础

人工智能（AI）是实现可持续SRv6网络生态系统的关键组成部分，特别是通过分析和决策，有助于网络运营的自动化和智能化[13]。智能网络运营以机器驱动的自动化取代传统的人工监督，检测和维护过程。随着网络架构从传统计算机网络向软件定义网络（Software Defined Networking，SDN）、物联网（Internet of Things，IoT）和SRv6等新一代网络演进，网络安全面临前所未有的挑战。网络流量的快速增长和服务质量要求的提升，使得传统的基于规则的异常检测方法难以应对复杂的网络环境。机器学习技术凭借其强大的模式识别和自适应能力，在网络流量异常检测领域展现出巨大潜力。现有研究已证实机器学习在该领域的有效性。如D-PACK框架[3]通过结合卷积神经网络和无监督深度学习模型，实现了对异常流量的自动分析和过滤；文献[4]提出的混合学习方法则通过融合监督和无监督学习，有效缓解了标记数据不足的问题。这些研究为机器学习在新型网络环境中的应用提供了重要参考。

在流量异常检测领域，机器学习方法主要可划分为监督学习、无监督学习以及混合学习三大类，各类方法在适用场景、性能表现及核心特性上存在显著差异，具体如下：第一类是监督学习方法[5]，其核心优势在于，当标记数据充足时，能够展现出优异的检测性能，实现较高的检测准确率；但其局限性也十分明显，一方面严重依赖大量高质量的标记数据，另一方面，由于模型训

表1 异常类型与检测指标之间的逻辑关联

异常类型	可观测特征	检测指标
SRH字段篡改	Segments_Left异常、SRH_Flags非零	SRH解析失败次数
无效SID注入	SID_Validity=0	丢包率上升
路径劫持	Segment_List_Length突增	RTT偏移
DDoS攻击	SRH_Overhead_Ratio升高	单位时间报文密度

练依赖已知攻击样本，对于未出现在训练集中的攻击类型，难以实现有效检测。第二类是无监督学习方法[6]，其区别于监督学习的最大的优势是不依赖标记数据，仅通过对未标记数据的特征分析与模式挖掘，就能发现数据集中的异常模式，因此在检测未知攻击方面具备天然优势；但其不足也很明显，一是受数据分布及异常模式复杂性影响，误报率通常较高，二是模型的决策过程缺乏直观解释，难以清晰追溯异常判定的依据，不利于后续的异常分析与验证。第三类是混合学习方法[7]，其核心思路是融合监督学习与无监督学习的优势，既借助监督学习对已知攻击类型的精准识别能力，又利用无监督学习挖掘未知异常的特性，使其能够很好地适应现实网络中标记数据有限的场景，在检测覆盖率与准确率之间实现更好的平衡，成为近年来流量异常检测领域的重要研究方向之一。[14]如表 2 展示了常用机器学习算法在网络异常监测中的对比。

AL-QATF 等人[8]提出了一种基于深度学习的入侵检测方法，结合了稀疏自编码器（Sparse Autoencoder, SAE）与支持向量机（Support Vector Machine SVM），构建了一个自学学习（Self-Taught Learning, STL）框架用于网络流量异常检测。该方法首先通过 SAE 对 NSL-KDD 数据集中的网络流量特征进行无监督学习，提取出低维稀疏特征表示，随后将该特征输入至 SVM 分类器进行入侵检测。该方法实现了高效的特征表示与降维，显著降低了 SVM 的训练与测试时间；提升了检测性能，在 NSL-KDD 数据集上进行了二分类与五分类实验，均优于传统单一 SVM 与其他浅层分类模型（如 Naive Bayes、Random Forest 等）。实验显示该方法在二分类准确率达 99.42%，多分类准确率达 99.41%（10 折交叉验证条件下），同时显著减少了支持向量数量和模型的计算复杂度。该研究表明，将无监督特征学习与监督分类方法结合是提升网络入侵检测系统性能的有效路径，尤其适用于处理高维网络流量数据。

Wang 等人[9]中，提出一种 HAST-IDS，它使用深度神经网络，可以直接从原始网络流量数据中自动学习分层时空特征，然后使用长短期记忆网络（Long Short-Term Memory，LSTM）学习多个网络数据包之间的时间特征。作为一种学习方法，实验结果表明，HAST-IDS 与现有的入侵检测方法相比，有效地提高了检测的准确率和 DR，并且目前的入侵检测方法的 FAR 普遍较高。

3　SRv6 流量异常检测模型设计

3.1　需求分析

为应对 SRv6 网络中的流量异常检测挑战，本研究旨在开发一种智能检测系统，以实现对异常流量行为的高效、精准识别。该系统不仅致力于解决传统检测方法面临的关键问题包括有效检测未知异常的难题、减少对人工标记数据的依赖，同时规避传统方法在处理大规模数据时易出现的性能瓶颈。因此需满足以下两大核心需求，以保障检测能力的实用性与可靠性。

（1）多维度异常检测：能够识别协议层异常（如 SRH 字段篡改）、行为异常（如 DDoS 攻击）和路径异常（如路由劫持）。

表 2　常用算法对比情况表

算法类型	代表算法	优点	缺点	适用场景
决策树	C4.5,CART	解释性强，计算效率高	容易过拟合	特征选择，实时监测
神经网络	CNN, LSTM	特征提取能力强	需要大量数据	复杂模式识别
集成方法	随机森林	抗过拟合	计算成本较高	高精度需求场景
无监督学习	孤立森林	无需标记数据	误报率高	新型攻击检测

（2）解释性输出：提供异常检测结果的详细解释，比如异常类型概率分布。

根据以上两大核心需求，综合考虑SRv6流量图像化后的特征分布特性，本研究选择ResNet18模型作为基础模型，主要基于以下优势：

（1）SRv6流量图像在空间维度上表现为局部特征簇结构，不同协议字段间存在非线性交互关系，适合卷积提取局部关联特征；

（2）在时间维度上，流量窗口形成连续结构，残差连接有助于捕获跨尺度特征；

（3）相较于更深网络（如ResNet50），ResNet18参数规模更小（约11M），推理延迟更低，适合未来边缘节点部署；而较浅网络则难以刻画高维特征组合。

此外，为确保CNN算法在SRv6流量检测中的最佳性能，本研究采用以下优化策略：

（1）SRv6专用特征工程。结合SRv6领域的专业知识，针对性构造适配该网络环境的专用特征，确保特征能有效反映SRv6流量的核心属性。

（2）模型调优。为提升其泛化能力与检测精度，研究从模型训练过程与结构设计两方面入手优化：一方面，通过交叉验证的方法对模型训练过程进行把控，反复验证不同参数组合下的模型性能，最终确定使模型损失最小的最优参数配置，保障模型在训练阶段的稳定性与有效性；另一方面，在模型结构设计中融入早停、Dropout等经典策略，两者结合有效防止模型出现过拟合问题，提升模型对未知SRv6流量数据的适应能力与检测准确性。

本研究的CNN方法在保持较好检测性能的同时，兼具计算效率和模型可解释性，特别适合SRv6网络环境下的异常流量监测需求。

3.2 ResNet18模型

研究采用ResNet-18（Residual Network-18）作为基础骨干网络，用于提取图像的深层特征表示。ResNet-18由He等人于2015年提出，是ResNet系列中最轻量的结构之一，共包含18层可训练权重层（不含池化与全连接层）。其核心创新在于引入了残差连接（residual connection），通过恒等映射（identity mapping）有效缓解了深层网络中的梯度消失与退化问题，使得网络在保持较低计算开销的同时，具备较强的表达能力[15]。该模型的基本构建单元为残差块[16]（residual block），每个残差块由两个3×3卷积层组成，并辅以批归一化（Batch Normalization）与ReLU激活函数。

试验阶段，我们发现随着训练轮数的增加，实验结果逐渐出现过拟合的症状，为了解决该问题我们在ResNet-18的模型基础上做了两点优化：1.采用凯明初始化（Kaiming Initialization）[10]替代随机初始化。传统的参数随机赋值容易导致深层网络在前向传播过程中出现梯度消失或梯度爆炸问题。而凯明初始化能够根据激活函数的特性（尤其是ReLU函数）自适应地设定权重初值，使得不同层的输入与输出方差保持一致，从而加快模型收敛速度并提升训练稳定性；在卷积层与全连接层之间加入失活层（Dropout Layer）[11]。卷积神经网络在训练过程中容易出现过拟合现象，即模型在训练集上表现优异但在测试集上泛化能力不足。引入失活层后，能够以一定概率随机“丢弃”部分神经元，使得模型在训练过程中不会过度依赖某些特定特征，从而提升网络的鲁棒性和泛化性能。

3.3 整体框架

为支撑智能SRv6流量异常检测系统实现高效、精准的检测功能，系统设计三层核心模块，各模块分工明确且协同配合，实现“数据预处理-特征提取-分析决策”完整闭环，如图2所示：

具体功能说明如下：

第一层是数据预处理层，该层作为系统的数

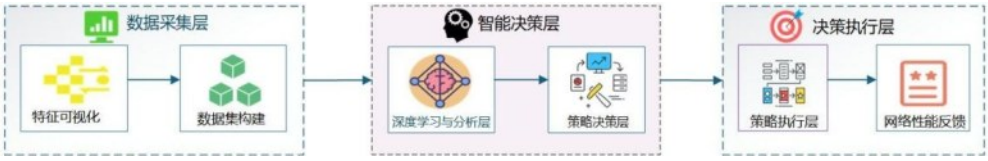


图 2　系统结构图

据输入基础，主要提供 SRv6 报文解析的核心功能。通过对原始流量报文进行深度解析，精准提取出报文结构中的关键信息，包括 SRH 字段、IPv6 基础头字段等与 SRv6 协议特性紧密相关的核心数据，为后续的特征处理与异常分析提供标准化、结构化的原始数据支撑。

第二层是特征处理层，该层围绕数据特征的提取与优化展开，通过多维度处理将原始数据转化为可用于异常检测的有效特征，具体包含以下关键工作：

（1）协议特征提取，结合 SRv6 网络的检测需求，重点分析丢包率、延迟、带宽利用率及流量模式等，从协议运行状态角度挖掘反映流量正常或异常的核心特征。

（2）行为特征计算，采用滑动窗口机制（默认窗口时长为 1 秒）对流量数据进行动态截取与统计，生成流量矩阵特征，捕捉流量在时间维度上的变化规律与行为模式；

第三层是分析决策层，该层负责基于处理后的特征数据完成异常判定与响应，主要包含两部分功能：

（1）ResNet-18 的推理计算。最大深度限制在 18 层以内，通过模型推理输出当前流量属于异常的概率（取值范围为 0-1），为异常判定提供量化依据；

（2）差异化响应策略，根据模型输出结果执行对应操作。对于判定为正常的流量，不施加任何限制，保障其正常传输；对于判定为异常的流量，立即触发预设的处置机制，通过流量重路由将异常流量引导至安全路径，或采用限速措施降低异常流量对网络的影响，实现对 SRv6 网络的实时保护。

4　实验设计与结果分析

4.1　数据集描述

在本研究中，我们选用了 CICIDS2018 数据集作为基础实验数据。该数据集包含丰富的正常流量与多种攻击流量（包括 DoS、DDoS、Brute Force、Infiltration 等），被广泛应用于网络异常检测研究。然而，该数据集并未覆盖 SRv6（Segment Routing over IPv6）的特有流量特征，故我们在 CICIDS2018 数据集的基础上，构造了 SRv6 特有的特征（如 SRH 长度、SID 类型等），用于模拟 SRv6 场景下的流量异常检测。为了验证所提出方法在 SRv6 场景下的有效性，我们在原始数据集的基础上，人工构造了若干 SRv6 专有特征列。表 2 详细说明了我们构造的若干 SRv6 专有特征列以及它们的取值和取值依据。

其中，正常流量对应的 SRv6 特征取值主要反映协议的合法使用情况（如 SRH 长度较短、SID 合法、seg_left 于路径匹配）；而异常流量则通过构造于攻击行为一致的异常取值及逆行模拟（如过长的 Segment List、无效 SID、seg_left 异常等）这些特征的取值设计基于 SRv6 协议规范（以及 常见安全威胁模型。正常流量对应特征取值符合协议的合理范围，而异常流量则模拟攻击场景下的不合理取值，从而保证了特征构造的科学性与可解释性。

需要特别说明的是，本研究中 SRv6 特征并非来自真实抓包环境，而是基于 RFC 8754 协议规范及典型威胁模型进行语义一致性构造。该方法保证了：

表3　异常检测特征说明表

特征名称	含义说明	正常取值范围	异常表现	RFC依据与安全意义
SRH_Presence	指示IPv6数据包是否包含SRH (Routing Tyoe == 4)	0（无SRH，传统IPv6）1（启用SRv6）	在非SRv6域强制设为1（伪造路由）在SRv6策略中缺失（设为0）	RFC 8754：SRH为可选扩展头。异常值可能反映注入攻击或篡改攻击
Segment_List_Length	SRH中段列表长度（Last Entry + 1）	0－16（典型1－5跳）	>16（过长列表，放大攻击）负值或非法索引	RFC 8754：由 Hdr Ext Len 和 Last Entry 字段定义。过长列表增加处理负载，可用于DDoS
Segment_Left	剩余未处理段数，逐跳递减	0 ≤ Segments_Left ≤ Segment_List_Length	>Last Entry 或 <0	RFC 8754：非法值触发 ICMP Parameter Problem。异常值可能为路由欺骗
SRH_Flags	8-bit 标志字段（当前未定义）	恒为 0	非 0 值（未定义行为）	RFC 8754：当前所有标志位保留。非零值可能用于绕过过滤
HMAC_TLV_Presence	是否包含 HMAC TLV (Type=5)	0（信任域）1（高安全场景）	缺失（0，导致未认证）HMAC校验失败	RFC 8754：HMAC用于保护段列表完整性。缺失或校验失败可能为中间人攻击
SID_Validity	SID（128-bit IPv6）是否合法（最长前缀匹配验证）	1（匹配本地SID	0（无匹配，伪造SID）	RFC 8754：无效SID将触发丢弃或异常转发。可检测伪造路径攻击
SRH_Overhead_Ratio	SRH长度占总包长度比例((Hdr Ext Len+1)×8)/Total Length	<0.1（典型低开销）	>0.15~0.2（异常高比例	RFC 8754 + RFC 2473：高比例会增加带宽与处理负担，可作为放大攻击指标

（1）构造特征严格遵循SRH字段定义与取值范围；

（2）异常特征模拟符合现实攻击逻辑；

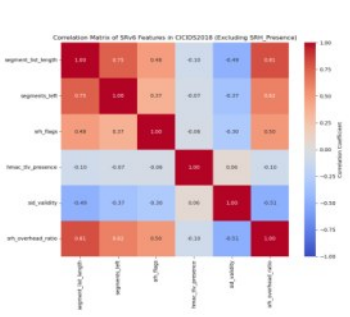
（3）协议一致性不被破坏。

因此，本研究的实验仅作为方法有效性验证（proof-of-concept）。未来工作将进一步在真实SRv6流量环境中采集数据，以提升结论的普适性和实用性。

图3展示了数据集中SRv6特征的相关性矩阵，排除SRH_Presnce因冗余性问题。红/蓝色分别表示正/负相关，系数范围[-1, 1]。Segment_List_Length与Segments_Left高度相关（r=0.75），表明路径长度特征间存在冗余，可能影响ResNet18模型性能。SRH_Overhead_Ratio与SID_Validity呈负相关（r=-0.51），提示其在异常流量检测中的潜在互补作用。未来可结合特征选择（如PCA）进一步减少维度。

4.2　数据预处理

为了将原始的网络流量记录转换为适合ResNet-18处理的图像形式，本文设计了一套系统化的数据预处理流程。首先，逐个读取数据集的CSV文件，并对其中的异常值进行清理，将



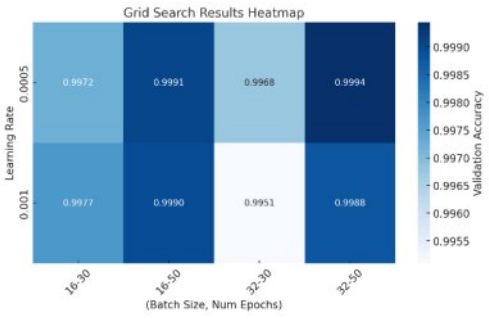


图3　SRv6特征相关性矩阵 图4.网格搜索结果图

NaN、inf以及-inf替换为缺失值后删除，以保证输入特征的有效性。在标签处理阶段，我们将原始的多类别标签统一映射为二分类任务：正常流量标记为：Normal（对应为Benign），其余攻击类型（包括Bot、Infiltration、SSH等）统一标记为Attack，并剔除无法归类的标签。

在特征处理方面，仅保留数值类型特征列，并采用Z-score标准化（均值为0，方差为1），以消除不同特征间的量纲差异。随后，将数据流量按照固定长度序列进行划分，每个序列包含50条记录。若某一类别样本不足50条，则舍弃该部分数据。为降低高维特征的冗余性，每个序列通过主成分分析（PCA）压缩为单维表示。接着，将得到的一维序列填充或裁剪为1024个元素，并重塑为32×32的二维矩阵，从而构造出灰度图像。

为了充分利用卷积神经网络在空间特征提取方面的优势，本文将滑动窗口内的流量特征转换为二维图像形式输入ResNet-18进行分类。近年来，流量图形化表示方法已被广泛应用于网络异常检测任务，其核心思想是通过结构化映射将多维统计特征转换为规则二维矩阵，从而利用卷积网络的局部感知与参数共享能力提取高阶模式特征。在特征转换过程中，考虑到原始流量特征维度较高且不同特征之间可能存在冗余相关性，本文首先采用主成分分析（PCA）对窗口内特征进行压缩处理。PCA能够在最大化保留数据方差信息的同时降低维度，减少噪声干扰，并提高模型训练稳定性。为进一步构建统一尺寸的卷积输入结构，本文将压缩后的特征序列通过零填充方式扩展至固定长度1024，并重塑为32×32的二维矩阵形式。该尺寸设计兼顾以下因素：

（1）典卷积网络结构（如ResNet-18）的输入规格匹配；

（2）保持特征排列的结构连续性；

（3）控制模型计算复杂度与推理开销。

通过上述映射方式，原始流量的统计特征被组织为具有空间结构的特征图，使卷积网络能够自动学习局部相关模式与全局异常分布特征，从而提升异常检测能力。

在图像生成过程中，所有的像素值被归一化到[0,255]区间，并以PNG格式保存。为避免类别过度失衡，每个标签最多生成1000张图像。最终Attack与Normal两类图像分别储存在对应的文件夹中，构成可直接输入卷积神经网络的标准图像数据集。

为了避免滑动窗口带来的样本重叠导致数据泄露问题，本文采用时间隔离式数据划分策略，首先我们将原始流量按照时间戳排序，并按时间顺序划分为训练时间段（前70%）和测试时间段（后30%）；随后在各自时间段内部执行滑动窗口操作生成样本。由于训练样本与测试样本来源于完全不用的时间区间，因此不存在窗口重叠或数据共享问题，从而有效避免了数据泄露。

4.3　实验设置

为了获得较优的超参数组合，我们采用了网格搜索的方法对关键超参数进行调优。网格搜索是一种系统的超参数优化方法，它通过在预定义的参数空间中穷举不同的超参数组合，并在验证集上评估其性能，从而选择最佳的超参数配置。本研究主要针对学习率(Learn rate)、批大小（Batch size）和训练轮数（epoch）三个参数进行调优。具体而言，学习率取0.001、0，0005、0，0001；批大小取16、32、64；训练轮数取30、60、90.最终我们根据验证机准确率的最高值来确定最有参数组合。图4展示了不同的超参组合最终的模型准确率情况。

4.4　实验结果

为了获得更鲁棒、更准确、更适合进一步分析和比较的结果并且在分析网络流量时，首要任务是区分正常场景和恶意攻击，故我们使用ResNet18进行了二元分类。在经过了50个epoch之后，ResNet18在测试集和验证集上获得的结

果是：

● 训练损失从初始值0.35下降到0.05，呈快速下降后趋于平稳趋势。验证损失从约0.30开始下降，最终在0.10左右。

● 训练准确率从约0.88上升至0.9994，呈现稳定上升趋势。验证准确率最终上升至0.98。两者间的差距（约2%-3%）在可接受的范围内。

● 验证召回率在0.88至0.98之间波动，整体保持较高水平，这表明对Attack类的检测能力较强。

● 验证集F1-Score在0.93至0.96之间波动。F1分数整体较高，这表明模型在二分类任务中表现良好，但优化空间仍存。

在入侵检测领域，传统方法通常依赖于五元组特征（源IP、目的IP、源端口、目的端口、协议）进行规则匹配或浅层机器学习分析，本节将我们提出的基于深度学习的模型与传统五元组方法进行对比，包括基于规则的防火墙、浅层机器学习模型以及签名匹配方法。对比重点聚焦于检测准确率、鲁棒性和计算复杂度以及各自的局限性和优势。通过这些分析，突出我们模型的创新点和优越性。表4展示了各方法的关键性能指标。

表4　关键性能指标结果对比表

方法名称	准确率	假阳性率	假阴性率	鲁棒性下降
基于规则的防火墙	93.3%	55.2%	6.7%	25.0%
SVM	95%	16.9%	4.1%	18.0%
Decision Tree	92.8%	51.9%	7.2%	15.0%
ResNet18	99.4%	8.6%	2.2%	6.0%

从表中可见，我们的深度学习模型在准确率、假阳性率、和假阴性率上显著优于传统方法。具体而言，在本实验设置与数据构造条件下，与SVM相比准确率提升约2.8%，假阳性率相对下降约49%，表明在当前验证环境中模型具有较好的性能优势。这些改进得益于深度学习对流量图像化特征的自动提取，而传统方法依赖于手动设计的五元组规则，难以应对变异攻击。除准确率等指标外，本文进一步对模型复杂度与部署可行性进行定性分析：

（1）模型参数规模约为11M，单次推理时间在CPU环境下约为毫秒级（基于标准配置测试）；

（2）相比传统规则匹配方法虽计算复杂度更高，但在高维特征场景下具有更强扩展性；

（3）在边缘节点部署时，可结合模型剪枝或量化技术进一步压缩模型规模。

需要指出的是，该结果受数据构造方式影响，仍需在真实SRv6场景中进一步验证。

此外，为验证所构造的SRv6协议特征对异常检测性能的贡献，本文设计对比实验，对比了原始CICIDS2018特征与加入SRv6特征后的模型性能差异。在该实验中，模型结构、训练参数、数据划分策略以及滑动窗口设置均保持一致，仅改变输入特征集合，实验结果如表5所示。

表5　SRv6特征对模型性能的影响

特征集合	准确率	假阳性率	假阴性率	F1-Score
原始数据	94.5%	7.5%	6.9%	0.90
构造后的数据	99.4%	8.6%	2.2%	0.94

从表5可以看出，在引入SRv6协议特征后，模型的准确率和F1值均有明显提升。其中F1值提升约为4.6%，说明SRv6特征在异常流量判别过程中提供了额外的判别信息。这是因为SRv6特征能够反映路径行为、段列表异常以及协议头部状态变化等信息，这些信息在原始流量统计过程中均难以体现。因此，引入协议层特征有助于提升异常检测的敏感性与鲁棒性。

4.5　推理时间评估

为评估所提方法在实际部署中的可行性，本文对模型 的推理延迟和计算开销进行了测试。实验环境为：NVIDIA GeForce RTX 5070Ti Laptop GPU, 13th Gen Intel(R) Core(TM) i9-13900HX,

32GB 内存，PyTorch 框架实现。

测试过程中，模型设置为评估模式，在进行 100 次预热后，对同一输入进行 1000 次前向传播，统计平均推理时间。实验结果表明，在 batch size = 1 的情况下，GPU 上单样本平均推理时间为 2.15ms。GPU 平台下吞吐量可达 465samples/s。模型总参数量为 11.7M，模型存储大小约为 44.6MB。

结果表明，该模型在毫秒级别即可完成一次异常检测，满足近实时网络流量分析的需求。

5　结束语

本文针对 SRv6 网络环境中传统异常检测方法适应性差、难以应对动态路由和高维流量特征的挑战，提出了一种基于机器学习的流量异常检测方案。通过系统分析 SRv6 特有的异常类型，并构建融合数据预处理、多维度 KPI 特征提取以及 ResNet18 模型的检测框架，该方法实现了对已知与未知异常的有效识别。实验结果表明，在模拟数据集上与传统五元组方法对比，本模型展现出优异的性能和可解释性。该方案为 SRv6 网络的安全监控提供了可靠、可扩展的解决方案。然而，本研究存在一定局限性：由于缺乏公开 SRv6 异常流量数据集，实验基于协议知识和威胁模型的模拟数据进行验证，未来需在真实环境采集数据以增强普适性。此外，模型在极高资源约束下的实时性优化仍有潜力。未来工作将聚焦于真实 SRv6 流量的采集与标注，探索更先进的混合模型（如结合无监督学习），并集成轻量化技术以支持边缘部署，进一步提升系统在实际网络中的应用价值。

参考文献：

[1] Stefano Previdi, Clarence Filsfils, et al. 2018. IPv6 Segment Routing Header (SRH). Internet-Draft draft-ietf-6man-segment-routing-header-14.

[2] Mo Z, Long B. An Overview of SRv6 Standardization and Application towards 5G-Advanced and 6G[C]//2022 IEEE 5th International Conference on Computer and Communication Engineering Technology (CCET). IEEE, 2022: 266-270.

[3] Hwang R H, Peng M C, Huang C W, et al. An unsupervised deep learning model for early network traffic anomaly detection [J]. IEEE Access, 2020, 8: 30387-30399.

[4] Wang J, Yu P, Xu S, et al. High-Accuracy Fault Diagnosis for SRv6 TE Policy in Computer Power Networks[C]//2024 IEEE/CIC International Conference on Communications in China (ICCC Workshops). IEEE, 2024: 60-65.

[5] Liu B. Supervised learning[M]//Web Data Mining: Exploring Hyperlinks, Contents, and Usage Data. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011: 63-132.

[6] James G, Witten D, Hastie T, et al. Unsupervised learning[M]// An introduction to statistical learning: with applications in Python. Cham: Springer International Publishing, 2023: 503-556.

[7] Van Engelen J E, Hoos H H. A survey on semi-supervised learning[J]. Machine learning, 2020, 109(2): 373-440.

[8] M. Al-Qatf, Y. Lasheng, M. Al-Habib and K. Al-Sabahi, "Deep Learning Approach Combining Sparse Autoencoder With SVM for Network Intrusion Detection," in IEEE Access, vol. 6, pp. 52843-52856, 2018, doi: 10.1109/ACCESS.2018.2869577.

[9] W. Wan get al., "HAST-IDS: Learning Hierarchical Spatial-Temporal Features Using Deep Neural Networks to Improve Intrusion Detection," in IEEE Access, vol. 6, pp. 1792-1806, 2018, doi: 10.1109/ACCESS.2017.2780250.

[10] He K, Zhang X, Ren S, et al. Delving deep into rectifiers: Surpassing human-level performance on imagenet classification [C]//Proceedings of the IEEE international conference on computer vision. 2015: 1026-1034.

[11] Srivastava N, Hinton G, Krizhevsky A, et al. Dropout: a simple way to prevent neural networks from overfitting[J]. The journal of machine learning research, 2014, 15(1): 1929-1958.

[12] 王强,杨宏.基于SRv6技术实现高可靠网络传输研究[J].通信技术,2025,58(01):39-49.

[13] Wang J, Yu P, Xu S, et al. High-Accuracy Fault Diagnosis for SRv6 TE Policy in Computer Power Networks[C]//2024 IEEE/CIC International Conference on Communications in China (ICCC Workshops). IEEE, 2024: 60-65.

[14] Wang S, Balarezo J F, Kandeepan S, et al. Machine learning in network anomaly detection: A survey[J]. IEEe Access, 2021, 9: 152379-152396.

[15] Szegedy C, Ioffe S, Vanhoucke V, et al. Inception-v4, inception-resnet and the impact of residual connections on learning[C]// Proceedings of the AAAI conference on artificial intelligence.

2017, 31(1).

[16] He K, Zhang X, Ren S, et al. Deep residual learning for image recognition[C]//Proceedings of the IEEE conference on computer vision and pattern recognition. 2016: 770-778.

[17] Floristean G R, Udrea A. Detection and Classification of Anomalies in IP Communications Networks[J]. Journal of Control Engineering and Applied Informatics, 2021, 23(4): 25-32.