

面向网络会话的 TR-SAGE 流量异常检测方法研究

罗 文, 魏松杰

南京理工大学 计算机科学与工程学院 南京 中国 210094

摘要 鉴于网络流量交互关系本身具有高度的稀疏性和复杂性, 传统的网络流量异常检测方法很难有效地利用网络流量中的时序特征和拓扑信息, 在应对复杂多样的网络流量进行异常检测时, 往往存在准确性不足和适应性差的问题。为了解决这些关键问题, 本文在图神经网络 E-GraphSAGE 的基础上提出了一种融合会话特征和重启随机游走算法的集成检测方法 TR-SAGE。该方法通过利用会话级别的流量特征以及图的拓扑信息, 显著增强针对网络流量异常的检测能力。会话特征提取通过捕获会话生命周期内的动态变化和统计属性, 以发现传统方法可能忽略的隐藏流量模式和关系。通过图拓扑优化为重启随机游走算法提供了更有效的采样基础。通过提高模型采样质量, 该方法可以更有效地区分正常和异常流量模式, 即使在高度复杂的数据集中也是如此。在三个通用网络流量异常检测数据集上进行了实验, TR-SAGE 方法在召回率、精确度、F1 分数等评估指标上均表现出色, 尤其在面对复杂、动态变化的网络流量时, 能够有效地识别出多种异常模式。在 ISCXTor2016 数据集上不仅评估指标都达到了最优, 并且相比 SOTA 图神经网络模型提升了 19% 的召回率、17% 的精确度和 18% 的 F1 分数。实验结果证明了本文方法对于网络流量异常检测任务的有效性和鲁棒性。该方法在解决网络安全和流量分析挑战方面表现出显著的效果, 为网络流量异常检测提供了一种有希望的解决方案。

关键词 网络流量; 异常检测; 会话特征; 时间序列; 图表达; 拓扑优化
中图法分类号 TN92 **DOI 号** 10.19363/J.cnki.cn10-1380/tn.2026.05.03

Research on TR-SAGE Anomaly Detection of Network Sessions

LUO Wen, WEI Songjie

School of Computer Science and Engineering, Nanjing University of Science and Technology, Nanjing 210094, China

Abstract Given that network traffic interactions are highly sparse and complex, traditional network traffic anomaly detection methods are difficult to effectively utilize the temporal features and topological information in network traffic. When dealing with complex and diverse network traffic anomaly detection, they often have problems of insufficient accuracy and poor adaptability. To address these key issues, this paper proposes an integrated detection method TR-SAGE that integrates session features and restarted random walk algorithms based on the graph neural network E-GraphSAGE. This method significantly enhances its ability to detect network traffic anomalies by utilizing session-level traffic features and graph topological information. Session feature extraction captures dynamic changes and statistical properties within the life cycle of a session to discover hidden traffic patterns and relationships that traditional methods may ignore. In addition, graph topology optimization provides a more effective sampling basis for the restarted random walk algorithm. By improving the quality of model sampling, this method can more effectively distinguish normal and abnormal traffic patterns, even in highly complex data sets. We conduct experiments on three common network traffic anomaly detection datasets. The TR-SAGE method performs well in evaluation indicators such as recall, precision, and F1 score. In particular, it can effectively identify a variety of abnormal patterns when facing complex and dynamically changing network traffic. For example, on the ISCX-Tor2016 dataset, not only the evaluation indicators have reached the most advanced level, but also the recall rate, precision and F1 score of the proposed method have been improved by 19%, 17% and 18% compared with the SOTA graph neural network model. The experimental results prove the effectiveness and robustness of the proposed method for network traffic anomaly detection tasks. The proposed method has shown significant effects in solving network security and traffic analysis challenges, and provides a promising solution for network traffic anomaly detection.

Key words network traffic; anomaly detection; session features; time series; graph representation; topology optimization

通讯作者: 魏松杰, 博士, 副教授, Email: swei@njust.edu.cn.

本课题得到 2020 年工业互联网创新发展工程项目“工业企业网络安全综合防护平台”(No. TC200H01V)资助。

收稿日期: 2024-09-02; 修改日期: 2025-01-27; 定稿日期: 2026-04-07

1 引言

随着网络规模的不断扩大和网络攻击手段的日益复杂化, 对网络空间的安全构成了巨大隐患。网络流量异常检测是确保网络安全和保障服务质量的重要任务, 能够有效地发现并防御各类网络攻击^[1-2]。然而, 网络入侵行为的数据通常表现出高度稀疏性和复杂性, 使得传统基于预定义规则和特征工程的方法在处理大规模复杂网络流量数据时效果不佳。因此, 如何提高网络流量异常检测的准确性和效率, 成为一个亟待解决的问题。

网络流量异常检测的挑战主要源于数据本身的性质。首先, 网络流量数据高度稀疏, 与背景流量相比, 只有极少部分数据与恶意活动相关。这种稀疏性使异常检测变得复杂, 因为传统方法很难在这种条件下有效区分正常流量和恶意流量^[3-4]。其次, 网络的复杂拓扑结构给特征提取带来了困难, 因为使用标准的机器学习方法不易捕捉到节点和流量模式之间的交互。最后, 网络流量数据的高维特性要求模型能够处理非欧几里得数据结构, 这些结构更适合表示流量网络中的关系。研究人员已经开始探索使用图神经网络 (Graph Neural Networks, GNN) 进行网络流量异常检测^[5-6]。GNN 对图结构中节点和边之间的关系进行建模, 使其能够通过图拓扑结构的消息传递和特征聚合来捕获高阶特征关系^[7-8]。

为了应对这些挑战, 本研究在图神经网络 E-GraphSAGE (Edge Graph Sample and aggreGatE) 的基础上, 提出了一种新的基于会话特征和 RWR 算法的网络流量异常检测方法——TR-SAGE (Time-series and Random Walk Restart enhanced E-GraphSAGE)。E-GraphSAGE 模型通过其归纳学习框架, 可以有效地生成边嵌入, 从而实现节点特征和拓扑信息的集成, 该方法专门用于处理网络流量数据中的非欧几里得图结构。我们的方法结合了会话特征与重启随机游走算法 (Random Walk with Restart, RWR), 旨在提升网络异常流量检测的准确性和鲁棒性。与传统方法不同, 会话特征通过捕获会话级别的时间动态与统计特征, 有效提升了流量数据的表达能力。此外, RWR 算法通过重要性采样增强了采样的精准性与全面性, 使模型能够更高效地捕获网络流量中复杂的关联关系。本研究的主要贡献如下:

1) 针对网络流量交互关系的高度复杂性和动态性, 设计了一种面向会话的统计和时间序列特征提取方法, 分析会话级别的时间特征, 提升流量数据

的表达能力。

2) 为了克服网络流量复杂关联的采样问题, 提出了一种基于 RWR 算法的优化方法, 使用重要性采样替代 E-GraphSAGE 的随机均匀采样, 以提高采样质量, 实现对网络流量数据的高效捕捉和表示。考虑到网络流量的高度稀疏性, 设计了一种图拓扑优化技术, 通过改造图结构提升图的连通性, 提高 RWR 算法的运行效率和效果, 使得采样更加均匀和全面。

3) 通过融合会话特征提取和 RWR 算法, 提出了一种面向会话的网络流量异常检测的集成检测方法 TR-SAGE, 通过提取会话级别的时间序列和统计特征以及 RWR 算法优化采样, 增强网络流量特征的表达能力, 使得采样过程更加精准, 从而提升模型的检测性能和鲁棒性。

本文结构安排如下: 第 1 节是引言, 第 2 节介绍了网络流量异常检测方法的研究现状, 第 3 节介绍了本文所提出的 TR-SAGE, 第 4 节介绍了本文提出的方法在数据集上的实验并对实验结果进行分析, 第 5 节进行总结。

2 相关工作

近年来, 网络流量呈现爆炸式的增长, 网络流量异常检测方法也是层出不穷。由于传统网络异常检测方法的局限性, 研究者逐渐转向基于时间序列分析和图神经网络等更先进的技术, 以提高异常检测的准确性和鲁棒性。

2.1 基于时间序列的网络流量异常检测方法

Vu 等人^[9]提出了一种基于时间序列分析和深度学习的加密流量分类方法, 专注于通过时间序列特征来表示加密网络流量的行为。方法主要设计并利用 LSTM 网络提取时间序列中的时序依赖关系, 从而提高加密流量分类的准确性和效率。Pérez 等人^[10]提出了一种新方法, 将多重网络和时间序列分析结合起来建立入侵检测系统。该方法通过将网络流量中的时间序列属性表示为复杂的多重网络, 有效地降低了数据表示的维度。Koumar 等人^[11]提出了一种新颖的基于时间序列分析的方法, 称为 NetTiSA。该方法通过在 IP 流量导出器中直接进行时间序列分析, 生成一组扩展特征。这些特征能够捕获网络流量的时间和统计特性, 同时优化了计算复杂度, 以支持在高性能网络上的实时部署。Gao 等人^[12]提出了一种基于多维时间序列的加密 IoT 流量分类方法, 称为 MTS-IoT。该方法通过对网络流量构建多维时间序列并采用全局-局部-空间的深度学习框架, 实现对

IoT 流量的高效分类。

2.2 基于神经网络的网络流量异常检测方法

Kipf 等人^[13]首次提出了图卷积网络(Graph Convolutional Network, GCN)的概念。林宏刚等人^[14]提出了一种基于图神经网络的 P2P 僵尸网络检测方法。Cheng 等人^[15]提出了一种名为 Alert-GCN 的框架,该框架将网络流量结构图输入到两层 GCN 进行节点分类。Zhang 等人^[16]提出了一种新的网络流量异常检测方法,解决了工业物联网数据非线性和高维度等问题。Nguyen 等人^[17]提出了一种名为 TS-IDS 的流量感知自监督学习框架。

此外,在 GCN 的基础上还发展了许多变体。Veličković 等人^[18]提出了一种图注意力网络(Graph Attention Networks, GAT)。Hamilton 等人^[19]提出了一种名为 GraphSAGE 的通用归纳框架,该框架利用节点特征信息来有效地为以前未见过的数据生成节点嵌入。Lo 等人^[20]将 GraphSAGE 扩展到网络流量检测问题,提出了 E-GraphSAGE 算法,该架构可以捕获图的边缘特征和拓扑信息,用于网络流量检测。Caville 等人^[21]在 E-GraphSAGE 的基础上提出了一种名为 Anomal-E 的自监督图神经网络方法用于网络流量异常检测。Liu 等人^[22]提出了一种基于 Graph-

SAGE 的动态时空图卷积网络(DST-GraphSAGE)用于交通预测。Chang 等人^[23]对 E-GraphSAGE 架构和 GAT 架构进行了改进,关键思想是利用可用的图信息将残差学习集成到 GNN 中。加入残差连接作为处理高类不平衡的策略,旨在保留原始信息,提高少数类的检测效果。

3 TR-SAGE 网络流量异常检测方法

在网络流量异常检测中,传统的检测方法主要依赖于特征工程和预定义规则,难以应对网络流量数据的高维度、稀疏性和复杂性。GNN 在处理复杂图数据方面展现出了显著优势,但现有的 GNN 模型在网络流量数据的采样和特征提取上仍存在不足。因此,本文提出了一种融合会话特征和 RWR 算法的网络流量异常检测方法即 TR-SAGE。其中的模型算法在 E-GraphSAGE 模型的基础上进行改进,通过图拓扑优化技术提升网络图的性能,再使用重启随机游走算法^[24]进行采样,这样可以更好地获取到网络流量中的拓扑信息和流量特征。

3.1 TR-SAGE 方法流程

本文所提出的 TR-SAGE 网络流量异常检测方法流程如图 1 所示,主要包括以下几个步骤。

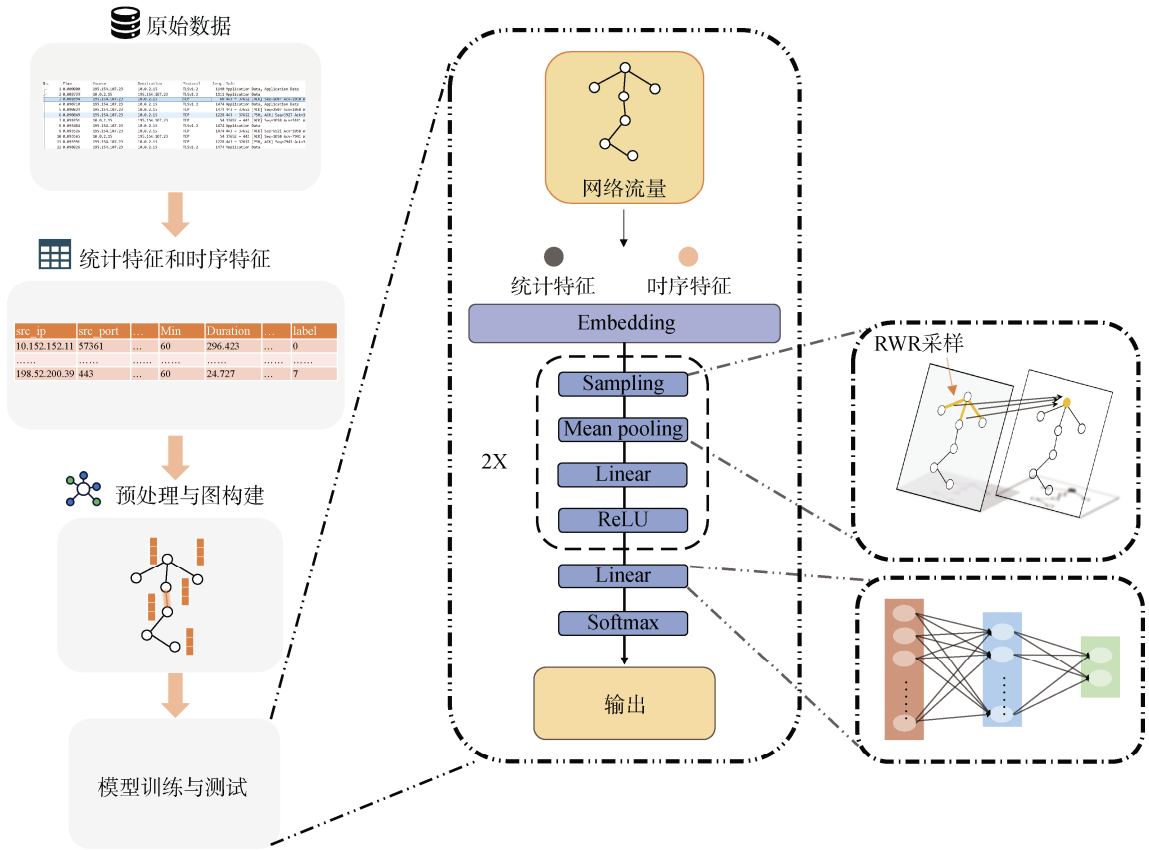


图 1 TR-SAGE 方法流程
Figure 1 TR-SAGE method flow

1) 面向会话的特征提取: 通过从原始 pcap 数据包中提取基础的流量特征和丰富的会话级特征, 并将其映射或聚合到会话的边的属性中, 为后续的图建模和分析提供更全面的信息基础。

2) 数据预处理与图构建: 将网络流数据通过独热编码和归一化处理得到标准化的数据, 然后将标准化的网络流量数据通过建模构建图, 并且引入一种图拓扑优化技术来增强网络图的连通性, 为后续的模型提供良好的数据条件。

3) 模型训练: 通过对网络流量中的边进行 RWR 采样和聚合来获得边嵌入, 并在训练集上进行监督学习。

4) 模型测试: 在网络流量测试集上测试模型的效果, 评估模型性能并且进行对比分析。

3.2 面向会话的特征提取

在网络流量分析中, 网络会话的生命周期(如连接的持续时间、开始和结束时间等)和行为模式(如数据传输量、时间差等)可以通过时间序列进行建模和分析。提取的时间序列信息, 能够更准确地分析网络流量的行为模式, 提供时间维度的动态性分析, 进而识别异常行为。时间序列不仅能够捕捉会话中的动态变化, 还能为后续的异常检测、预测建模提供更加细致的特征支持。

目前的时间序列分析大多只考虑观测之间的均匀间隔时间。然而, 网络流量自然会以不均匀间隔的时间戳产生。这意味着在时间序列 $\{X_n\} = \{x_1, \dots, x_n\}$ 中时间 $\{T_n\} = \{t_1, \dots, t_n\}$ 不满足等式 $t_{j+1} - t_j = t_j - t_{j-1}$, $\forall j \in \{2, \dots, n-1\}$ 。这种类型的时间序列称为不均匀间隔^[25]。不均匀间隔时间序列在网络流量分析中是可行的, 并且比均匀间隔时间序列具有显著的优势。

通过从原始 pcap 文件中非均匀间隔时间方法的分析与处理, 我们可获得更加多样化且细粒度的特征表示。其中包括基于统计的特征和基于时间序列的特征。基于统计的特征是在数据集初始特征基础上扩展的, 旨在为会话分析提供更丰富的信息, 而基于时间序列的特征强调数据在时间维度上的动态性。这些特征将为后续的会话行为分析和网络流量异常检测提供更为全面和深度的信息支撑。

3.2.1 基于统计的特征

基于统计的特征主要是对会话数据的整体属性进行量化。在原始数据集特征的基础上额外提取一些数据包的统计特征, 如表 1 所示。这些特征可能会和一些数据集的初始特征部分重叠。

以下是对部分特征的补充说明。

1) Kurtosis: 峰度是描述数据分布形态的统计量, 衡量的是流量中的数据包的传输是否呈现出突发的模

表 1 基于统计的特征描述

Table 1 Statistical Feature Description

特征	描述
Min	流中所有数据包有效载荷长度的最小值
Max	流中所有数据包有效载荷长度的最大值
Mean	流中数据包有效载荷长度的平均值
Max Minus Min	最小和最大有效载荷长度之间的差值
Root Mean Square	反映数据包大小的波动性, 捕捉异常变化
First Quartile	表示有 25% 的数据点小于或等于这个值
Third Quartile	表示有 75% 的数据点小于或等于这个值
Kurtosis	峰度
Directions	描述报文方向的百分比

式。高峰度表示数据集中在均值附近, 尾部较重; 低峰度表示数据分布较为平坦。公式如下:

$$\text{Kurtosis} = \frac{N(N+1)}{(N-1)(N-2)(N-3)} \sum_{i=1}^N \left(\frac{x_i - \mu}{\sigma} \right)^4 - \frac{3(N-1)^2}{(N-2)(N-3)} \quad (1)$$

其中, N 是数据包的总数, x_i 是第 i 个数据包的有效载荷长度, μ 是数据的均值, σ 是数据的标准差。

2) Directions: 报文方向比例描述在一个网络会话中, 各个数据包发送方向所占的百分比比例。这一特征在流量分类、异常检测和网络优化中具有重要的应用价值。通过准确计算和分析报文方向比例, 可以更好地洞察网络行为模式, 提升整体网络管理和安全防护的效果。公式如下:

$$\text{Directions} = \frac{d_0}{d_0 + d_1} \quad (2)$$

其中, d_0 是源到目的方向的报文数, d_1 是目的到源方向的报文数。

3.2.2 基于时间序列的特征

基于时间序列的特征关注流量在时间维度上的变化和模式, 主要捕捉流量的动态行为, 如表 2 所示。以下是对部分特征的补充说明。

1) Time Interval Entropy: 该特征用于衡量网络会话中数据包到达时间间隔分布的复杂性或不确定性。高熵可能代表噪声, 而低熵可能表明异常的周期性流量。

2) Intervals Change Ratio: 衡量相邻时间间隔之间的变化速率和波动性, 反映流量的动态变化。公式如下:

$$\text{ICR} = \frac{1}{n_t - 1} \sum_{i=1}^{n_t-1} \frac{|\Delta t_{i+1} - \Delta t_i|}{\Delta t_i} \quad (3)$$

其中, Δt_i 是第 i 个时间间隔, n_t 是总的时间间隔数。

3) Transients: 该特征用于检测时间序列中是否存在显著的瞬态事件, 瞬态指的是时间序列中的短暂无突变或异常变化。瞬态事件可能与突发的流量高峰、攻击活动或应用中的异常行为相关。

表 2 基于时间序列的特征描述
Table 2 Time series feature description

特征	描述
Time Interval Entropy	数据包到达时间间隔的熵
Min of Intervals	所有时间间隔的最小值
Max of Intervals	所有时间间隔的最大值
Mean of Intervals	所有时间间隔的平均值
Median of Intervals	所有时间间隔的中位数
Intervals Change Ratio	相邻数据包到达时间间隔的变化速率
Mean of Relative Times	相对时间的平均值
Transients	检测时间序列中是否存在瞬态事件
Coefficient of Variation	变异系数
Switching Ratio	描述数据包大小的变化频率
Protocol Switch-Ratio	流量中不同协议之间的切换频率
Hurst Exponent	赫斯特指数
Duration	会话持续时间
Burstiness	突发性
Packets Velocity Change Ratio	描述网络会话中数据包速率变化

4) Coefficient of Variation: 标准差与均值的比值, 用于衡量数据的相对变异程度。变异系数越高, 表示数据的波动性越大。公式如下:

$$CV = \frac{\sigma}{\mu} \quad (4)$$

其中, μ 是数据的均值, σ 是数据的标准差。

5) Switching Ratio: 该特征衡量网络会话中数据包大小变化的频率, 反映流量的多样性。

$$SR = \frac{s_n}{(n-1)/2} \quad (5)$$

其中, s_n 是有效载荷长度发生变化的相邻报文对数, $n-1$ 是相邻报文对的总数。

6) Protocol Switch-Ratio: 衡量会话中不同协议之间的切换频率, 高切换频率可能表示复杂的应用行为或混合协议使用, 低切换频率则可能表示单一协议的使用。

7) Burstiness: 突发性衡量流量中的数据包传输是否呈现出突发的模式。高突发性可能表示短时间内的流量活动, 如攻击、数据传输高峰或异常流量。公式如下:

$$Burstiness = \frac{\sigma^2 - \mu}{\sigma^2 + \mu} \quad (6)$$

其中, μ 是数据包到达时间的均值, σ^2 是数据包到达时间的方差。

8) Packets Velocity Change Ratio: 用于衡量网络流量会话中数据包速率的变化速率, 通过计算连续时间窗口内数据包数量变化的速率, 反映流量变化的加速度和趋势。该特征捕捉流量的动态变化, 帮助识别异常活动和突发事件。公式如下:

$$PVCR = \frac{1}{N-1} \sum_{i=2}^N \frac{P_i - P_{i-1}}{\Delta t_i} \quad (7)$$

其中, P_i 表示第 i 个数据包的数据传输量, Δt_i 是第 i 个时间间隔。

3.3 数据预处理与图构建

因为网络流量中会有很多的符号数据, 比如协议类型、连接状态等, 需要通过独热编码来将这些符号数据转换成数值数据。

将网络流量特征处理成数值特征数据之后需要经过归一化处理。本文使用最小最大归一化方法, 转换公式可表示为式(8):

$$x' = \frac{x - x_{\min}}{x_{\max} - x_{\min}} \quad (8)$$

其中, 对于每个数值特征计算其最小值 $x_{\min}$ 和最大值 $x_{\max}$, x 是原始值, x' 是归一化后的结果。

网络流数据由源地址、目标地址以及各种流特征这三个主要部分构成, 将源地址和目标地址作为图中的端点, 可以很自然地构建图。这种方法不仅直观, 而且高效, 最终将网络流量异常检测问题转化为分类任务, 使得问题的解决方案更具系统性和条理性。

3.4 图拓扑优化

考虑到 RWR 算法需要在一个连通的图中进行随机游走, 而网络流量具有很强的稀疏性, 导致 RWR 算法的性能在稀疏图上的效率会在一定程度上受限。因此本文引入一种图拓扑优化技术, 通过把 IP 相同端口不同的节点连接起来增强图的连通性。同一个 IP 不同端口的节点连接的过程可以用数学公式(9)表示:

$$E' = \{e_{i,i+1} | (v_i, v_{i+1}), \forall i \in \{1, 2, \dots, n-1\}\} \cup \{e_{n,1} = (v_n, v_1)\} \quad (9)$$

其中, $\{v_1, v_2, \dots, v_n\}$ 是一个包含 n 个节点的序列, 对于序列中的每个节点 $v_i (i=1, 2, \dots, n-1)$, 添加边 $e_{i,i+1}$ 连接节点 v_i 和 v_{i+1} , 并且最后一个节点 v_n 与第一个节点 v_1 连接, 形成闭环。

该方法不仅可以关联到同一主机上不同端口服

务之间的依赖关系, 还有效地增强了图的连通性, 为 RWR 算法提供了更加均匀的采样基础。表 3 中结果体现了优化前后图连通量的变化。

表 3 优化前后的连通量变化

Table 3 Changes in connectivity with optimization

数据集	优化前	优化后
ISCXTor2016	851	1
UNSW-NB15	50012	12
ToN-IoT	718	8

3.5 模型的训练和测试

在经过会话特征提取和图拓扑优化之后的网络流量图中, 通过对网络流量中的边进行 RWR 采样和聚合来获得边嵌入, 并将模型在训练集上进行监督学习。然后在网络流量测试集上测试模型的效果, 评估模型的性能并进行对比分析。

3.5.1 RWR 算法在网络流量上的应用

RWR 算法是一种有效的计算已构建图模型中网络节点之间连接的加权分数的方法, 算法通过图的拓扑结构(包括节点间的直接与间接连接、边的权重等)和重启机制传播信息, 计算节点之间的相似性, 从而能够更加有效地进行节点采样, 优化模型的性能。

数学上, 在节点 v 处的 RWR 算法可以表示为以下迭代公式:

$$P_v^{(t+1)} = (1-c)AP_v^{(t)} + cr \quad (10)$$

其中, $P_v^{(t)}$ 是在时间 t 的节点访问概率向量, c 是重启概率, r 是重启向量即 $P_v^{(0)}$, 通常初始化为在起始节点位置为 1, 其余位置为 0 的向量。 A 是图的转移概率矩阵, 其元素 A_{ij} 定义如下, 其中 d_i 为节点 i 的度:

$$A_{ij} = \begin{cases} \frac{1}{d_i}, & \text{if } d_i > 0 \\ 0, & \text{otherwise} \end{cases} \quad (11)$$

随着迭代次数的增加, $P_v^{(t)}$ 会收敛到一个稳定的概率分布, 这个分布反映了从起始节点到图中其他节点的相对重要性或相似度。

通过 RWR 算法的引入, 模型能够更全面地覆盖图的结构, 高效地捕捉节点间的关系, 提高特征表示的质量。

3.5.2 E-GraphSAGE 算法

在 E-GraphSAGE 算法^[20]中, 采样方法是采样节点邻居的一个固定大小的子集, 以便邻居消息传

播。E-GraphSAGE 算法对图 $G(V, E)$ 执行图卷积操作, 其中节点表示为 V , 边表示为 E , 节点特征表示为 x_v 。

为了指定 GNN 的深度, 设置参数 K -hop 邻居表示在每次迭代中需要聚合的 K -hop 邻居边信息。选择 GNN 可微聚合函数 $AGG_k (k \in \{1, 2, \dots, K\})$ 用于聚合 K -hop 邻居边的信息。

对于每个节点, E-GraphSAGE 模型迭代地聚合 K -hop 深度的相邻边信息。在每次迭代中, 可以对一组相邻节点进行固定数量的采样, 以降低算法的空间和时间复杂度。然后取来自采样节点与源节点之间的边的嵌入表示用于生成下一层的节点嵌入。在第 k 层 ($k \in \{1, 2, \dots, K\}$), 基于采样到的邻居 $k \in \{1, 2, \dots, K\}$, 节点 v 处聚合的节点邻居信息 $h_{N(v)}^k$ 可表示为式(12):

$$h_{N(v)}^k = AGG_k(\{e_{uv}^{k-1}, \forall u \in N(v), uv \in E\}) \quad (12)$$

边嵌入 e_{uv}^{k-1} 表示上一层的边 uv 的边嵌入。这些相邻的边嵌入聚合成节点 v 在第 k 层的嵌入, 基于聚合函数对每个图节点的 K -hop 邻域边特征进行聚合。

然后将来自采样邻居的聚合表示与自身的节点表示 h_v^{k-1} 连接起来。之后, 可以应用模型权重 W_k , 将结果传递给非线性激活函数 σ (如 ReLU), 得到最终节点嵌入 h_v^k , 如式(13)所示:

$$h_v^k = \sigma(W_k \cdot \text{CONCAT}(h_v^{k-1}, h_{N(v)}^k)) \quad (13)$$

节点 v 的最终节点表示可以表示为 z_v , 它描述了最终层的节点嵌入, 如式(14)所示。

$$z_v = h_v^k, \quad \forall v \in V \quad (14)$$

最后, 为了得到最终的边嵌入 z_{uv}^k , 计算节点 u 和 v 的第 k 层的边嵌入的拼接结果, 如式(15)所示。为了进行边分类, 将边嵌入 z_{uv}^k 送到 softmax 层进行分类任务。

$$z_{uv}^k = \text{CONCAT}(z_u^k, z_v^k), uv \in E \quad (15)$$

3.5.3 融合会话特征和 RWR 算法的 TR-SAGE

在本节中, 我们详细介绍了 TR-SAGE 方法中图神经网络模型的运行流程和算法, 展示了模型如何将网络会话特征与 RWR 算法相结合。图 2 展示了 TR-SAGE 方法中图神经网络模型的具体运行流程, 明确了各个模块的交互与数据流转方式。算法 1 进一步阐述了图神经网络模型的详细流程。

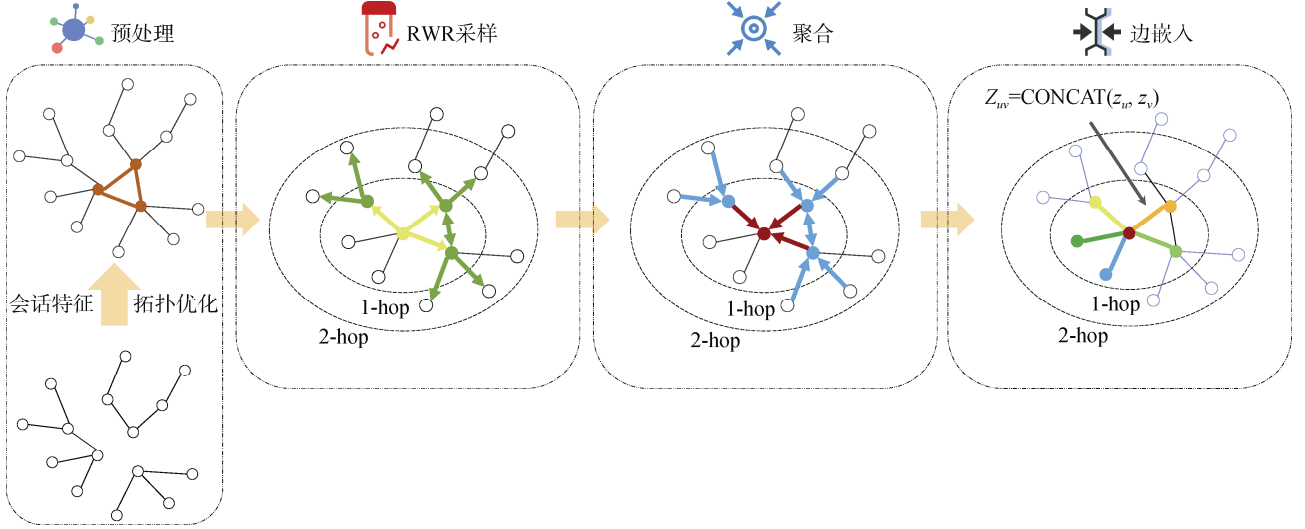


图 2 模型运行流程

Figure 2 Model running process

4 实验与分析

4.1 数据集

本文方法在多个通用的网络异常流量数据集上进行了实验验证, 包括 ISCXTor2016^[26]、UNSW-NB15^[27]、ToN-IoT^[28], 这些数据集广泛用于图神经网络的性能评估, 并且它们都会存在一定的数据不平衡的情况, 数据集的每一类百分比分布如图 3 所示。

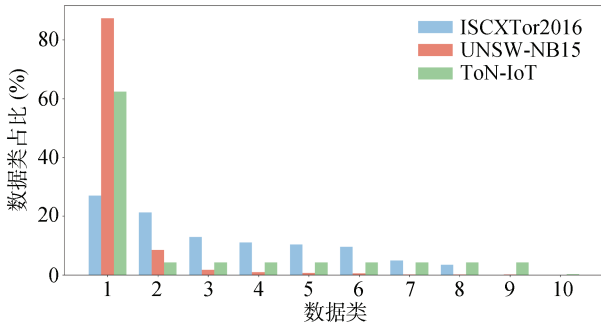


图 3 数据集类百分比分布

Figure 3 Class Percentage Distribution in datasets

在 ISCXTor2016 数据集中包括 Scenario A 和 Scenario B, 分别对应二分类任务和多分类任务。其中二分类任务包括 NonTor 和 Tor 流量, 多分类任务只包括 Tor 流量。UNSW-NB15 和 ToN-IoT 数据集都在一个场景下包含二分类和多分类任务。将这些数据集按照 70%、10%、20% 的比例来划分训练集、验证集和测试集, 并且进行多次实验, 将评估指标的平均值作为实验结果。

4.2 实验设置

实验在 Windows 11 操作系统、AMD Ryzen 7 5800H CPU、16GB 内存、NVIDIA GeForce RTX 3060 GPU 的环境中进行, 通过 ipfixprobe 从 pcap 文件中进行流量导出, 使用 Python 3.8.18 和 PyTorch 2.1.1 搭建和训练模型并对模型进行评估。并且对于本文提出的模型和对比的模型统一使用相同的超参数进行实验。

算法 1. 结合 RWR 算法的 E-GraphSAGE

输入: Graph $\mathcal{G}(\mathcal{V}, \mathcal{E})$; 输入边特征 $u \{e_{uv}, e \forall uv \in E\}$;
 输入节点特征 $x_v = \{1, \dots, 1\}$; 深度 K ; 权重矩阵 $W^k, \forall k \in \{1, \dots, K\}$; 采样数量 N ; 非线性激活函数 σ ; 聚合函数 AGG_k ; 重启向量 e_v 的长度为 $|\mathcal{V}|$ 且 $e_v = \{1 \text{ if } u = v, 0 \text{ otherwise}, \forall u \in \mathcal{V}, \forall v \in \mathcal{V}\}$; 重启概率 c ; 转移矩阵 A ; 迭代上限 T ;
 输出: 边嵌入 $z_{uv}, \forall uv \in E$

```

1  $h_v^0 \leftarrow x_v, \forall v \in \mathcal{V}$ 
2 FOR  $v \in \mathcal{V}$  DO
3   //RWR 算法迭代过程
4    $P_v^{(0)} \leftarrow e_v$ 
5    $t \leftarrow 0$ 
6   DO
7      $P_v^{(t+1)} \leftarrow (1-c)AP_v^{(t)} + cP_v^{(0)}$ 
8      $t \leftarrow t+1$ 
9   WHILE  $P_v^{(t)}$  未收敛或者  $t \leq T$ 
  
```

```

10   $N_{\text{RWR}}(v) \leftarrow \text{从 } P_v^{(t)} \text{ 选择 TOP-}N \text{ 个节点}$ 
11  FOR  $k \leftarrow 1$  TO  $K$  DO
12    FOR  $v \in \mathcal{V}$  DO
13       $h_{N_{\text{RWR}}(v)}^k \leftarrow \text{AGG}_k \left( \left\{ e_{uv}^{k-1}, \forall u \in N_{\text{RWR}}(v), uv \in E \right\} \right)$ 
14       $h_v^k \leftarrow \sigma \left( W^k \cdot \text{CONCAT} \left( h_v^{k-1}, h_{N_{\text{RWR}}(v)}^k \right) \right)$ 
15   $z_v = h_v^K$ 
16  FOR  $uv \in \mathcal{E}$  DO
17     $z_{uv}^K \leftarrow \text{CONCAT} \left( z_u^K, z_v^K \right)$ 

```

4.3 评价指标

本文实验使用召回率(Recall)、精确率(Precision)、F1-score 和 AUC 作为评价指标。因为数据集的类别不平衡性, 在多分类任务中简单地计算上述指标的加权平均值可能会使得少数类的预测性能被忽略, 因此引入宏平均召回率(Macro Recall, MR)、宏平均精确度(Macro Precision, MP)、宏平均 F1-score(Macro F1-score, MF1)、宏平均 AUC(Macro AUC, MAUC) 评价指标, 评估模型在异常检测分类任务上的性能。公式如下:

$$\begin{aligned}
 \text{MR} &= \frac{1}{N} \sum_{i=1}^N \text{Recall}_i \\
 \text{MP} &= \frac{1}{N} \sum_{i=1}^N \text{Precision}_i \\
 \text{MF1} &= 2 \times \frac{\text{MP} \times \text{MR}}{\text{MP} + \text{MR}}
 \end{aligned} \tag{16}$$

其中, N 是类别数, Recall_i 表示第 i 个类别的 Recall, Precision_i 表示第 i 个类别的 Precision。

4.4 结果分析

本节将详细分析在 ISCXTor2016、UNSW-NB15 和 ToN-IoT 数据集上各方法的实验结果, 验证的模型包括 E-GraphSAGE^[20]、GAT^[18]、E-ResSAGE、E-ResGAT^[23], 还有仅使用了会话特征的 Based-SC、仅使用了 RWR 方法的 Based-RWR 以及融合使用会话特征和 RWR 方法的 TR-SAGE。二分类结果如表 4 所示, 多分类结果如表 5 所示。

对于 ISCXTor2016 数据集, 在二分类任务中, Recall、Precision 和 F1-score 分别达到了 0.9910、0.9911 和 0.9910, 优于其他方法。在多分类任务中, Recall、Precision 和 F1-score 为 0.9950、0.9952 和 0.9951, 显著高于其他方法。这表明本文的方法在准确识别和分类异常流量方面具有很强的能力。此外, 该方法在宏观平均指标中表现优异, 进一步展示了其在解决网络异常检测数据集中常见的类别不平衡

问题方面的优势。这些结果凸显了该模型能够有效识别少数类别, 而不会牺牲更常见类别的性能, 从而提供平衡而全面的检测机制。

表 4 二分类实验结果

	方法	Recall	Precision	F1	AUC
ISCXTor2016	E-GraphSAGE	0.9783	0.9781	0.9782	0.99
	GAT	0.9672	0.9665	0.9668	0.99
	E-ResSAGE	0.9778	0.9779	0.9778	0.99
	E-ResGAT	0.9653	0.9646	0.9649	0.99
	Based-SC	0.9814	0.9810	0.9812	0.99
	Based-RWR	0.9788	0.9803	0.9795	0.99
	TR-SAGE	0.9910	0.9911	0.9910	0.99
UNSW-NB15	E-GraphSAGE	0.9926	0.9934	0.9930	1
	GAT	0.9938	0.9948	0.9943	1
	E-ResSAGE	0.9910	0.9917	0.9913	1
	E-ResGAT	0.9944	0.9951	0.9947	1
	Based-SC	0.9932	0.9933	0.9932	1
	Based-RWR	0.9930	0.9937	0.9933	1
	TR-SAGE	0.9945	0.9950	0.9947	1
ToN-IoT	E-GraphSAGE	0.9991	0.9992	0.9991	1
	GAT	0.9972	0.9974	0.9973	1
	E-ResSAGE	0.9995	0.9997	0.9996	1
	E-ResGAT	0.9980	0.9981	0.9980	1
	Based-SC	0.9985	0.9986	0.9985	1
	Based-RWR	0.9997	0.9996	0.9996	1
	TR-SAGE	0.9992	0.9993	0.9992	1

对于 UNSW-NB15 数据集, 在二分类任务中, 本文的方法在各项指标上均表现出色。特别是 Recall 和 F1-score 分别达到了 0.9945 和 0.9947, 高于其他方法。在多分类任务中, 本文的方法在 Recall、Precision 和 F1 上表现尤为突出, 分别达到了 0.9940、0.9938 和 0.9939, 明显高于其他方法。在宏观平均指标方面, 本文的方法依旧表现出色。

对于 ToN-IoT 数据集, 在二分类任务中, Recall 和 F1 均达到了 0.9992, Precision 达到了 0.9993, 略低于 E-ResSAGE 和基于 RWR 的方法, 但仍高于其他方法。在多分类任务中, 本文的方法在 Recall、Precision 和 F1 分别达到了 0.9870、0.9868 和 0.9869, 只有 Precision 略低于 E-ResGAT, 但依然高于其他方法。在宏观平均指标方面, 本文的方法均表现优异。与 E-ResGAT 相比, TR-SAGE 性能略有下降, 这可以归因于 IoT 流量的独特特征, 这种流量通常涉及设备之间更频繁和多样化的交互。尽管存在这些挑战, 但 TR-SAGE 的性能仍然很稳健, 显示出它处理不同网络流量的普遍适用性。

表 5 多分类实验结果

Table 5 Multi-classification experimental results

	方法	Recall	Precision	F1	AUC	MR	MP	MF1	MAUC
ISCXTor2016	E-GraphSAGE	0.7985	0.8237	0.8109	0.98	0.7384	0.7998	0.7679	0.98
	GAT	0.7742	0.7718	0.7730	0.96	0.6308	0.6759	0.6526	0.94
	E-ResSAGE	0.7922	0.8112	0.8016	0.98	0.7469	0.7520	0.7494	0.98
	E-ResGAT	0.8051	0.8206	0.8128	0.96	0.6781	0.7226	0.6996	0.95
	Based-SC	0.8025	0.8371	0.8194	0.97	0.7390	0.7721	0.7552	0.97
	Based-RWR	0.9905	0.9906	0.9905	1	0.9897	0.9893	0.9895	1
	TR-SAGE	0.9950	0.9952	0.9951	1	0.9952	0.9958	0.9955	1
UNSW-NB15	E-GraphSAGE	0.9838	0.9866	0.9852	1	0.6414	0.6124	0.6266	0.9
	GAT	0.9842	0.9848	0.9845	1	0.6314	0.5423	0.5835	0.99
	E-ResSAGE	0.9820	0.9793	0.9806	1	0.5615	0.5127	0.5360	0.9
	E-ResGAT	0.9872	0.9873	0.9872	1	0.5802	0.5651	0.5726	0.98
	Based-SC	0.9920	0.9911	0.9915	1	0.6240	0.5741	0.5980	0.9
	Based-RWR	0.9840	0.9853	0.9846	1	0.6446	0.5814	0.6114	0.98
	TR-SAGE	0.9940	0.9938	0.9939	1	0.7031	0.6575	0.6795	0.97
ToN-IoT	E-GraphSAGE	0.9841	0.9852	0.9846	1	0.9284	0.9292	0.9288	1
	GAT	0.9960	0.9961	0.9960	1	0.9923	0.9920	0.9921	1
	E-ResSAGE	0.9838	0.9849	0.9843	1	0.9335	0.9301	0.9318	1
	E-ResGAT	0.9968	0.9969	0.9968	1	0.9934	0.9932	0.9933	1
	Based-SC	0.9901	0.9920	0.9910	1	0.9670	0.9711	0.9690	1
	Based-RWR	0.9904	0.9910	0.9907	1	0.9660	0.9686	0.9673	1
	TR-SAGE	0.9970	0.9968	0.9969	1	0.9940	0.9930	0.9935	1

总体而言，在实验的数据集中，TR-SAGE 在二分类和多分类任务中多优于其他模型。通过引入会话级别的时间序列与统计特征，为采样过程提供了更加丰富的上下文信息，凸显了集成会话特征和基于 RWR 的采样在提高边嵌入质量和提高模型检测异常能力方面的优势。此外，该方法在处理不平衡数据方面具有稳健性和有效性。

为了直观地展示本文提出的算法的采样质量，本文以 ISCXTor2016 数据集为例，将模型最后一层的边嵌入通过 t-SNE 算法降维到二维并进行可视化。如图 4 所示，左边为原始模型边嵌入分布，右边为本文提出模型的边嵌入分布，可以看到本文提出的方法采样质量更高。

5 结论

本研究探讨了在网络流量异常检测任务中通过融合会话特征和 RWR 算法，提升基于 E-GraphSAGE 的图神经网络模型在处理复杂网络数据时的性能和鲁棒性。实验结果表明，TR-SAGE 方法显著提高了模型在不同数据集上的关键评价指标。特别是，通过优化采样过程，本研究提升了模型的泛化能力，突显了采样优化在图神经网络性能提升中的关键作用。

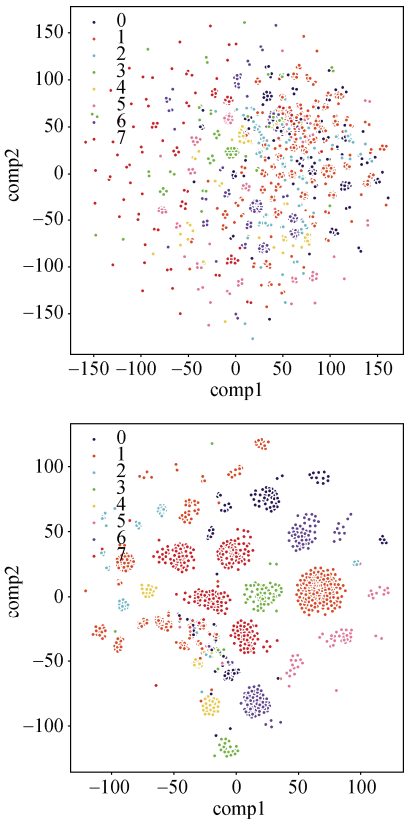


图 4 t-SNE 算法降维

Figure 4 t-SNE algorithm dimensionality reduction

此外, 通过网络会话特征提取和图结构改造策略, 本文的方法为网络流量处理提供了一种创新的解决思路。

尽管本研究取得了积极的实验结果, 但也存在一定的局限性。尤其是图结构改造方法在不同类型图数据上的适应性有所差距, 某些特定类型的网络数据可能无法完全发挥该方法的优势。因此, 未来的研究将探索更多样化的图改造策略, 以进一步增强模型对不同网络结构和类型的适应能力。此外, 还将考虑结合其他深度学习技术和优化算法, 进一步提升 TR-SAGE 方法在网络流量异常检测中的综合性能。

总之, 本文提出的方法和研究发现为利用图神经网络处理网络流量数据提供了新的视角, 并对推动网络流量异常检测领域的发展做出了重要的贡献。

参考文献

- [1] Wang Z X, Li J L, Wang Y T, et al. Optimal Repair Strategy Against Advanced Persistent Threats under Time-Varying Networks[J]. *IEEE Transactions on Information Forensics and Security*, 2023, 18: 5964-5979.
- [2] García-Teodoro P, Díaz-Verdejo J, Maciá-Fernández G, et al. Anomaly-Based Network Intrusion Detection: Techniques, Systems and Challenges[J]. *Computers & Security*, 2009, 28(1/2): 18-28.
- [3] Wang W, Jian S L, Tan Y S, et al. Representation Learning-Based Network Intrusion Detection System by Capturing Explicit and Implicit Feature Interactions[J]. *Computers & Security*, 2022, 112: 102537.
- [4] Layeghy S, Portmann M. On Generalisability of Machine Learning-Based Network Intrusion Detection Systems[EB/OL]. 2022: arXiv: 2205.04112. <https://arxiv.org/abs/2205.04112>.
- [5] Scarselli F, Gori M, Tsoi A C, et al. The Graph Neural Network Model[J]. *IEEE Transactions on Neural Networks*, 2009, 20(1): 61-80.
- [6] Jiang W W. Graph-Based Deep Learning for Communication Networks: A Survey[J]. *Computer Communications*, 2022, 185: 40-54.
- [7] Wu Z H, Pan S R, Chen F W, et al. A Comprehensive Survey on Graph Neural Networks[J]. *IEEE Transactions on Neural Networks and Learning Systems*, 2021, 32(1): 4-24.
- [8] Luo W, Li H T, Niu K X, et al. Research on Network Traffic Anomaly Detection Method Integrating Graph Topology Optimization and Random Restart Walk Algorithm[M]. *Artificial Intelligence and Machine Learning*. SingaporeSpringer Nature Singapore2025: 142-157.
- [9] Vu L, Thuy H V, Nguyen Q U, et al. Time Series Analysis for Encrypted Traffic Classification: A Deep Learning Approach[C]. *2018 18th International Symposium on Communications and Information Technologies*, 2018: 121-126.
- [10] Iglesias Pérez S, Moral-Rubio S, Criado R. A New Approach to Combine Multiplex Networks and Time Series Attributes: Building Intrusion Detection Systems (IDS) in Cybersecurity[J]. *Chaos, Solitons & Fractals*, 2021, 150: 111143.
- [11] Koumar J, Hynek K, Pešek J, et al. NetTiSA: Extended IP Flow with Time-Series Features for Universal Bandwidth-Constrained High-Speed Network Traffic Classification[J]. *Computer Networks*, 2024, 240: 110147.
- [12] Gao T Y, Qi W, Liu K H, et al. MTS-IoT: A Robust Encrypted IoT Traffic Classification via Multi-Dimensional Time Series[C]. *2024 27th International Conference on Computer Supported Cooperative Work in Design*, 2024: 323-328.
- [13] Kipf T N, Welling M. Semi-supervised classification with graph convolutional networks[C]. *In International Conference on Learning Representations*, 2017.
- [14] Lin H G, Zhang Y L, Guo N X, et al. P2P Botnet Detection Method Based on Graph Neural Network[J]. *Advanced Engineering Sciences*, 2022, 54(2): 65-72.
(林宏刚, 张运理, 郭楠馨, 等. 基于图神经网络的 P2P 僵尸网络检测方法[J]. *工程科学与技术*, 2022, 54(2): 65-72.)
- [15] Cheng Q M, Wu C M, Zhou S Y. Discovering Attack Scenarios via Intrusion Alert Correlation Using Graph Convolutional Networks[J]. *IEEE Communications Letters*, 2021, 25(5): 1564-1567.
- [16] Zhang Y C, Yang C H, Huang K K, et al. Intrusion Detection of Industrial Internet-of-Things Based on Reconstructed Graph Neural Networks[J]. *IEEE Transactions on Network Science and Engineering*, 2023, 10(5): 2894-2905.
- [17] Nguyen H, Kashef R. TS-IDS: Traffic-Aware Self-Supervised Learning for IoT Network Intrusion Detection[J]. *Knowledge-Based Systems*, 2023, 279: 110966.
- [18] Veličković P, Cucurull G, Casanova A, et al. Graph Attention Networks[EB/OL]. 2017: arXiv: 1710.10903. <https://arxiv.org/abs/1710.10903>.
- [19] Hamilton W L, Ying R, Leskovec J. Inductive Representation Learning on Large Graphs[C]. *The 31st International Conference on Neural Information Processing Systems*, 2017: 1025-1035.
- [20] 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*, 2022: 1-9.
- [21] Caville E, Lo W W, Layeghy S, et al. Anomal-E: A Self-Supervised Network Intrusion Detection System Based on Graph Neural Networks[J]. *Knowledge-Based Systems*, 2022, 258: 110030.
- [22] Liu T, Jiang A M, Zhou J, et al. GraphSAGE-Based Dynamic Spatial-Temporal Graph Convolutional Network for Traffic Prediction[J]. *IEEE Transactions on Intelligent Transportation Systems*, 2023, 24(10): 11210-11224.
- [23] Chang L Y, Branco P. Embedding Residuals in Graph-Based Solutions: The E-ResSAGE and E-ResGAT Algorithms. a Case Study in Intrusion Detection[J]. *Applied Intelligence*, 2024, 54(8): 6025-6040.
- [24] Page L, Brin S, Motwani R, et al. The PageRank citation ranking: Bringing order to the web[R]. Stanford infolab, 1999.
- [25] Koumar J, Čejka T. Unevenly Spaced Time Series from Network Traffic[C]. *2023 7th Network Traffic Measurement and Analysis Conference*, 2023: 1-4.
- [26] Habibi Lashkari A, Draper Gil G, Mamun M S I, et al. Character-

zation of Tor Traffic Using Time Based Features[C]. *The 3rd International Conference on Information Systems Security and Privacy*, 2017: 253-262.

- [27] Moustafa N, Slay J. UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection Systems (UNSW-NB15 Network

Data Set)[C]. *2015 Military Communications and Information Systems Conference*, 2015: 1-6.

- [28] Alsaedi A, Moustafa N, Tari Z, et al. TON_IoT Telemetry Dataset: A New Generation Dataset of IoT and IIoT for Data-Driven Intrusion Detection Systems[J]. *IEEE Access*, 2020, 8: 165130-165150.



罗文 于 2022 年在海南大学信息安全专业获得学士学位, 现在南京理工大学网络与信息安全专业攻读硕士学位。研究领域为网络流量异常检测、机器学习。Email: xlangyu@njust.edu.cn



魏松杰 博士, 副教授, CCF 高级会员。就职于南京理工大学计算机科学与工程学院。研究领域为网络体系结构、网络与信息安全、流量分析与建模等。Email: swei@njust.edu.cn