基于动态时空图神经网络的网络流量入侵检测方法

罗恒[1,2]，万良[1,2]

（1.贵州大学计算机科学与技术学院，贵州 贵阳 550025；2.贵州大学公共大数据国家重点实验室，贵州 贵阳 550025）

摘　要：网络攻击形式日益多样化，传统的入侵检测方法在捕捉复杂网络流量中的时空特征方面存在一定局限性。大多数传统方法主要依赖于静态特征分析，难以适应动态网络环境下的多变入侵行为。同时，现有的深度学习方法在分析网络流量时，往往忽视了网络节点间的拓扑结构以及流量的时间动态变化。因此，提出一种基于动态时空图神经网络（GNN）的入侵检测方法 DSTG-IDS。通过时间窗口对网络流量进行分段，将每个时间段内的数据包建模为图中的节点，并基于源 IP 和目标 IP 的关系建立连接，构建出时序上的动态图序列。为了更好地捕捉流量的时序特征，对图数据进行时间位置编码，以增强不同时间段内节点的时序信息表达能力。在模型设计上，首先利用图卷积网络（GCN）提取网络流量的空间特征，并结合图注意力网络（GAT）提升对关键节点信息的关注能力；其次，通过双向门控循环单元（Bidirectional GRU）对流量的时间序列进行建模，有效捕捉数据随时间变化的动态特征；最后，利用多头注意力机制融合时空特征并进行分类。在 BoT-IoT、ToN-IoT 和 NF-CSE-CIC-IDS2018 这 3 个广泛使用的数据集上进行实验，结果表明，在多分类实验中，DSTG-IDS 的准确率分别达到了 99.69%、98.61%和 93.26%，相较其他入侵检测方法，DSTG-IDS 在准确率、召回率、误报率（FAR）、F1 值等指标上均具有明显优势。

关键词：入侵检测；时空图神经网络；双向门控循环单元；图注意力网络；动态时空图；多头注意力机制

中图分类号：TP393　　**文献标志码：**A　　**DOI：**10.19678/j.issn.1000-3428.0070520

Network Traffic Intrusion Detection Method Based on Dynamic Spatio-Temporal Graph Neural Network

LUO Heng[1,2], WAN Liang[1,2]

(1.College of Computer Science and Technology, Guizhou University, Guiyang 550025, Guizhou, China;
2.State Key Laboratory of Public Big Data, Guizhou University, Guiyang 550025, Guizhou, China)

【Abstract】Cyberattacks are becoming increasingly diverse, and traditional intrusion detection methods exhibit limitations in capturing the spatio-temporal characteristics of complex network traffic. Most traditional methods rely primarily on static feature analysis, making it difficult to adapt to the ever-changing intrusion behaviors in dynamic network environments. When analyzing network traffic, existing deep learning methods often overlook the topological structure between network nodes and the temporal dynamics of traffic. To address these issues, this paper proposes a novel intrusion detection method based on a dynamic spatio-temporal Graph Neural Network (GNN), named DSTG-IDS. By segmenting network traffic through time windows, data packets within each time period are modeled as nodes in a graph, and connections are established based on the relationship between the source and destination IP, thereby constructing a sequence of dynamic graphs over time. To better capture the temporal characteristics of traffic, graph data are encoded with a temporal position to enhance the temporal information expression ability of the nodes within different time periods. In terms of model design, first, Graph Convolutional Network (GCN) are utilized to extract the spatial features of network traffic, and Graph Attention Network (GAT) are incorporated to enhance the focus on key node information. Second, Bidirectional Gated Recurrent Unit (Bidirectional GRU) are employed to model the temporal sequence of traffic, effectively capturing the dynamic characteristics of data changes over time. Finally, a multi-head attention mechanism is utilized to fuse spatio-temporal features and perform classification. Experiments on three widely used datasets—BoT-IoT, ToN-IoT, and NF-CSE-CIC-IDS2018—demonstrate that DSTG-IDS achieves accuracies of 99.69%, 98.61%, and 93.26%, respectively. Compared with other intrusion detection methods, DSTG-IDS exhibits significant advantages in terms of accuracy, recall, False Alarm Rate (FAR), and F1 value.

【Key words】intrusion detection; spatio-temporal Graph Neural Network (GNN); Bidirectional Gated Recurrent Unit (Bidirectional GRU); Graph Attention Network (GAT); dynamic spatio-temporal graph; multi-head attention mechanism

---

基金项目：国家自然科学基金地区科学基金项目（62262004）。

作者简介：罗恒（CCF 学生会员），男，硕士研究生，主研方向为入侵检测；万良（通信作者），教授、博士生导师。

收稿日期：2024-10-22　　**修回日期：**2024-12-09　　**E-mail：**lwan@gzu.edu.cn

计算机工程 www.ecice06.com

0 引言

网络入侵检测作为一种关键的网络安全技术，广泛应用于企业网络、政府机构、金融系统、医疗系统、工业控制系统等领域。随着智能物联网的深度融合，网络威胁的规模越来越大，形式也越来越多样化，网络威胁的种类已经扩大到包括钓鱼网络、视频会议攻击、分布式拒绝服务(DDoS)、潜在的国家认可的网络战等[1]。因此，一个高效、稳健的网络入侵检测系统(IDS)在保证网络安全方面至关重要。

传统 IDS 可以分为基于特征匹配和统计分析两类。特征匹配方法通过预定义攻击特征库来检测已知攻击，虽然其速度快、准确率高，但在应对未知和变种攻击时效果较差[2]。统计分析方法通过建立正常流量模型来检测异常行为，虽能识别未知攻击，但误报率(FAR)高，且对动态网络环境适应性差[3]。因此，各种机器学习(ML)技术被引入入侵检测任务，包括 k 近邻(k-NN)算法[4]、随机决策树算法[5]等。然而，传统 ML 方法对特征工程依赖较高，需耗费大量领域知识和人工参与，特征质量直接决定了系统性能。

深度学习(DL)以其强大的自动特征提取和复杂模式检测能力，为入侵检测提供了新的解决方案。研究人员已探索多种 DL 方法，包括卷积神经网络(CNN)[6]、递归神经网络(RNN)[7]、长短时记忆网络(LSTM)[8]、门控循环单元(GRU)[9]等。但是，已有方法局限于静态网络数据，忽视了网络模型的动态可扩展性，而现实世界中的许多网络呈现动态行为，包括拓扑演化、特征演化、扩散等[10]。CNN 虽擅长提取高维统计特征，但对网络拓扑信息的捕捉能力有限[11]。LSTM 和 GRU 主要关注时间序列关系，难以跟踪节点间的交互信息。实际网络中的入侵行为往往具有时空特征，捕捉网络拓扑结构及其时间动态变化，对提升检测性能至关重要。

针对上述问题，本文提出一种基于动态时空图神经网络(GNN)的入侵检测方法 DSTG-IDS。该方法通过将网络流量建模为动态时空图，并结合多级时间位置编码策略，捕捉网络流量的动态拓扑关系和时间动态特征。在构图过程中，通过时间窗口分段，将每个时间段内的数据包建模为图中的节点，并根据源 IP 和目标 IP 之间的关系建立连接，从而构建时序上的动态图序列。在模型设计上，结合图卷积网络(GCN)、图注意力网络(GAT)和双向门控循环单元(Bidirectional GRU)提取时空特征，并使用多头注意力(Multi-Head Attention)机制进行特征融合。

1 相关研究

GNN[12]作为一种处理图结构数据的深度学习模型，通过捕捉节点和边之间的复杂关系以及图的拓扑信息，为网络入侵检测提供强有力的工具。近几年，基于图分析的入侵检测方法相继被提出。文献[13]提出一种称为安全对象图的图类型，用于连接各种类型的安全事件，并使用自编码器检测图异常。文献[14]提出了一种利用图嵌入对组织结构语义进行编码的内部入侵检测方法。然而，文献[13-14]并没有考虑实际的网络拓扑结构，图数据只是作为整合异构信息的工具。为了更好地挖掘实际网络的空间信息，文献[15]提出了一种通过基于图的网络流量行为分析来检测僵尸网络的深度学习模型。然而，该模型只学习目标网络的拓扑信息，不学习节点和边缘特征。文献[16]构建了一个名为 E-GraphSAGE 的定制 GNN 来进行入侵检测，在 E-GraphSAGE 中，通过将原始 IP 地址映射到特定范围内，避免源 IP 地址提供没有意义的标签给攻击流。E-GraphSAGE 虽然考虑到了网络拓扑信息和网络流的统计特征，但在源 IP 映射过程中不可避免地改变了网络的实际空间分布。

在入侵检测中，通常将特征信息与图结构相结合，通过特征传播和聚合来获得更好的图表示。文献[17]提出了图注意力网络 GATs，该神经网络利用隐式的自注意层，为图数据中的不同节点分配不同的特征重要性，避免了计算密集型的矩阵操作。文献[18]将 LSTM 和 GCN 结合起来，学习长短期依赖关系。文献[19]提出了 EvolveGCN，该算法沿时间维度调整 GNN 的模型权重。然而，入侵检测任务侧重于网络流量之间的通信，一般的图数据将网络表示为一个图，其中节点是 IP 地址，这就导致将节点分类任务转换成了边缘分类任务，而典型的 GNN 通常考虑节点特征嵌入而不是边缘特征，因此，通过一般的图卷积操作很难得到有效的边表示。针对该问题，文献[20]提出了一种基于图边缘特征注意力的入侵检测模型，利用图边缘注意力对边缘特征进行加权聚合，将边缘特征与节点特征进行拼接，生成边缘嵌入用于入侵检测分类。

然而，现有的大多数图嵌入方法都是为静态图设计的，并不适合网络表示必须不断更新的动态环境。为此，文献[21]提出了一种基于 Transformer 的动态图异常检测框架 TADDY，通过节点编码增强节点在动态图中的特征表达。文献[22]提出了一个端到端结构的时态图神经网络模型 StrGNN，

计算机工程 www.ecice06.com

用于检测动态图中的异常边缘。文献[23]提出了时间图注意力层(TGAT),并引入基于 Bochner 定理的时间位置编码,将节点嵌入识别为时间函数,用于增强动态图特征表达。文献[24]提出了一种线图结构,用来增强空间特征的表达,并采用动态图神经网络(DGNN)进行空间特征提取,通过直接生成网络快照的边缘嵌入来增强图卷积的信息聚合能力。但是,该方法在利用线图对原有图数据进行变换时,会产生大量的边,计算成本很高,并且不能很好地适用于所有的图类型。

总体而言,现有研究在入侵检测中取得了重要进展,但仍存在不足之处:第一,大多数方法未能全面捕捉网络流量中的动态拓扑变化与时间特征的结合关系;第二,现有时间建模方法多采用单一时间窗口策略,无法适应多时间尺度特征的表达需求;第三,空间和时间特征的融合能力仍然有限,难以充分利用网络流量的复杂特征关系。因此,本文提出一种基于动态时空图神经网络的入侵检测方法 DSTG-IDS,通过动态图建模、时间位置编码以及时空特征融合,实现对动态网络环境中复杂入侵行为的高效检测。

2 入侵检测方法 DSTG-IDS

本文基于动态时空图神经网络的网络流量入侵检测方法如图 1 所示,包括动态图构建与时间位置编码、时空特征提取与融合模块以及节点分类模块。

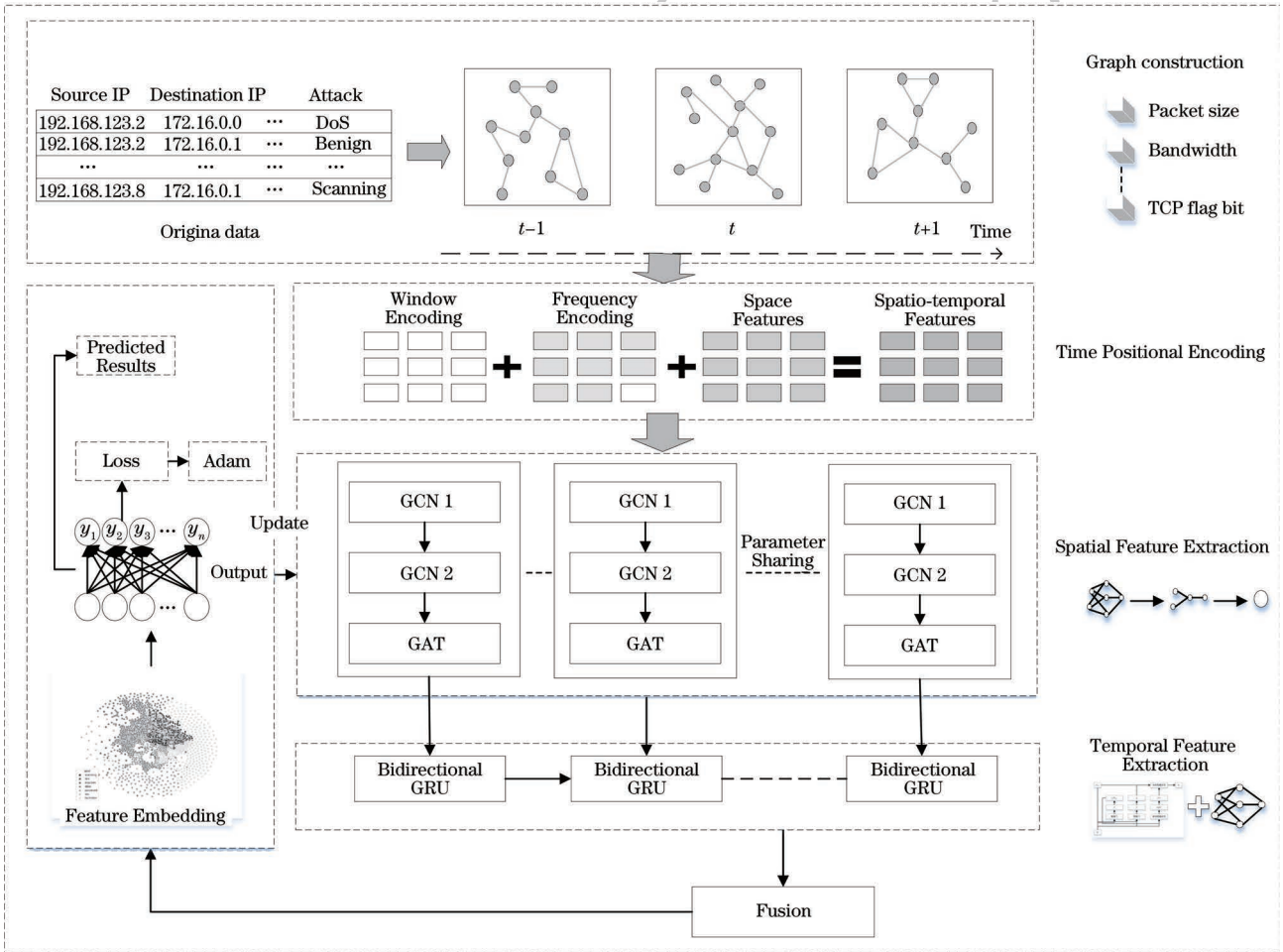

图 1 DSTG-IDS 整体框架

Fig. 1 The overall framework of DSTG-IDS

2.1 架构概述

DSTG-IDS 的检测过程如算法 1 所示。首先(第 2 行),从网络流量数据中提取每个时间段的数据并构建图 G_t,每个图的节点表示特定时间段内的数据包,节点之间的边基于源 IP 和目标 IP 之间的通信关系建立,形成时序上的动态图序列。在第 4 行对图进行基于时间窗口和频率的时间位置编码,生成带有时间信息的节点特征矩阵 $\boldsymbol{X}_t$。第 5 行、第 6 行通过两层 GCN 对每个图 G_t 的节点特征进行聚合与传播,生成空间特征 H_{s2},这些空间特征表示了节点在网络拓扑中的结构信息。随后,在第 7 行使用 GAT 对空间特征进行增强,生成 H_{s3},更精确地关注关键节点信息。在第 8 行,通过双向 GRU 对这些增强后的空间特征进行建模,提取随时间变化的动态特征 H_t,捕

捉节点特征在时间维度上的变化趋势。在第 9 行，采用多头注意力机制将当前时间段和历史时间段的特征进行融合，得到最终的时空特征表示 H_f，融合网络流量的时间与空间信息。最后，第 10～14 行将融合后的特征输入分类器，通过 Log-Softmax 计算得到预测结果 P，并通过损失函数优化模型参数。在整个检测过程结束后，输出最终的预测结果。

算法 1 DSTG-IDS 检测算法

输入 网络流量数据集 D

输出 预测结果 P

1. 从数据集 D 中加载数据，并对其进行预处理
2. {G_1，G_2，…，G_t}←D//通过时间窗口划分数据集，对//每个时间段的数据构建图序列
3. For t = 1 to T do //特征提取与融合
4. X_t←TimePosEnc(G_t，time)//对每个节点进行时//间位置编码
5. H_{s1}← GCN1(G_t，X_t)
6. H_{s2}← GCN2(H_{s1})//空间特征提取
7. H_{s3}← GAT(H_{s2})//空间特征增强
8. H_t←BiGRU(H_{s3})//时间特征提取
9. H_f←MultiHeadAttention(H_t，{H_{t-1}，…，H_1})//时空特征融合
10. P_t←Log-Softmax(Classifier(H_f))//将融合特征//输入到分类器中
11. 使用损失函数进行优化
12. 更新模型参数
13. End For
14. Return P

DSTG-IDS 检测算法的时间复杂度主要来源于动态图构建、特征提取和融合过程。通过时间窗口划分流量数据并构建动态图序列，该步骤的复杂度为 $O(N+TV+E)$，其中，N 是流量记录数，T 为时间窗口数，V 和 E 分别是节点数和边数。在时间位置编码阶段，对节点集合 V_t 的特征矩阵进行编码，复杂度为 $O(TVd)$，其中，d 为特征维度。两层 GCN 用于提取空间特征，复杂度为 $O(T(E+Vd^2))$，通过 GAT 增强空间特征，复杂度为 $O(ThEd)$，其中，h 为注意力头数量。双向 GRU 对时间序列进行建模，复杂度为 $O(TVd^2)$。时空特征融合的多头注意力机制复杂度为 $O(ThVd^2)$。总时间复杂度为 $O(T(N+V+E+Vd^2+hEd))$。在稀疏图条件（$E \ll V^2$）下，算法具有较好的扩展性和适应性。针对大规模网络流量，模型可以通过稀疏存储优化邻接矩阵、减少特征维度 d 等方式来提升运行效率。

2.2 动态图构建与时间位置编码

为捕捉网络流量中的时空特征，本文采用基于时间窗口的动态图构建方法，并结合时间位置编码来增强模型对时间信息的感知能力。整个过程如图 2 所示。

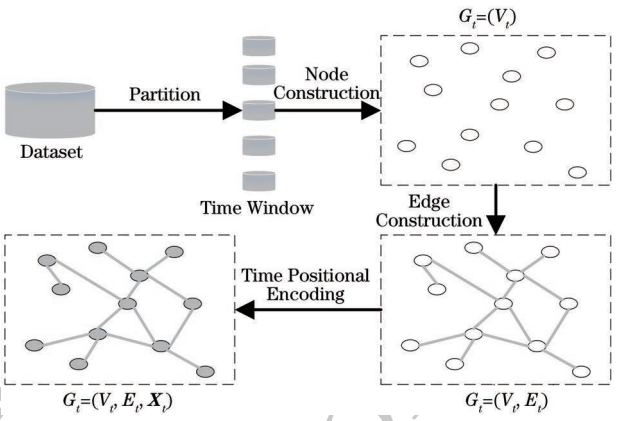

图 2 动态图构建与时间位置编码

Fig. 2 Dynamic graph construction and time location coding

给定一个网络流量数据集 D，通过时间窗口 Δt 对数据集进行划分，生成一系列时序图{G_1，G_2，…，G_t}，其中，$G_t=(V_t,E_t)$ 表示第 t 个时间段内的图。每个图 G_t 中包含的节点集合为 V_t，表示在该时间段内的数据包，每个边 E_t 表示在该时间段内存在通信关系的数据包对。每个数据包被视为一个节点 $v_i \in V_t$，其特征向量 $\boldsymbol{x}_i$ 包含该数据包的网络属性（流量大小、源 IP、目标 IP 等）。特征向量的维度为 d。如果数据包 v_i 和 v_j 在时间段 t 内存在通信关系（如共享相同的源 IP 或目标 IP），则在 G_t 中添加一条边 $e_{ij} \in E_t$，边的权重可以表示通信的强度。构建的图序列表示如下：

$$\{G_t\}=\{(V_t,E_t,\boldsymbol{X}_t)\}_{t=1}^{T} \tag{1}$$

式中：T 表示第 t 个时间段内的节点数量。

基于时间窗口的动态图构建能够将网络流量按时间分段，捕捉每段内的节点和边关系及其时序变化，同时保留局部拓扑结构的特征。这种方法适用于动态网络的特征建模，平衡了模型的动态表达能力和计算复杂度。

为了更好地捕捉节点特征在时间维度上的变化，设计一种基于多级时间窗口和递增频率编码的时间位置编码方法。网络流量数据集 D 被划分为 M 个不同级别的时间窗口，每个时间窗口具有不同的时间跨度 Δt_m，从短期到长期逐级递增。多级时间窗口的划分方式由式(2)表示：

$$\{G_{t,m}\}=\{(V_{t,m},E_{t,m},\boldsymbol{X}_{t,m})\}_{t=1}^{T},m\in\{1,2,\cdots,M\} \tag{2}$$

式中：$G_{t,m}$ 表示在第 m 个时间窗口下第 t 个时间段的子图；$V_{t,m}$、$E_{t,m}$ 和 $\boldsymbol{X}_{t,m}$ 分别表示该时间窗口下的节点集合、边集合以及节点特征矩阵。通过不同

时间尺度的划分，多级时间窗口能够捕捉动态网络的短期和长期变化特征。

在多级时间窗口的基础上，为了进一步增强时间特征的表示能力，时间位置编码通过正弦和余弦函数生成时间步 t 的时间特征，具体如下：

$$\mathrm{PE}_m(t,2i)=\sin\left(\frac{t}{k_m\cdot 10\ 000^{2i/d}}\right) \tag{3}$$

$$\mathrm{PE}_m(t,2i+1)=\cos\left(\frac{t}{k_m\cdot 10\ 000^{2i/d}}\right) \tag{4}$$

式中：$\mathrm{PE}_m(t,2i)$和 $\mathrm{PE}_m(t,2i+1)$分别表示在第 m 个时间窗口下第 i 维特征对应的正弦和余弦编码；k_m 是第 m 级时间窗口的递增频率参数，用于调节编码的频率。递增频率时间编码生成的特征表示能够区分不同时间步的节点特征，增强了时间动态变化的表达能力。

在完成多级时间窗口和递增频率编码后，最终的时间位置编码将这两部分进行融合，形成编码后的节点特征矩阵 $\boldsymbol{X}_t$，具体融合过程如下：

$$\boldsymbol{X}_t=\boldsymbol{X}_{t,m}+\mathrm{PE}_m(t) \tag{5}$$

式中：$\boldsymbol{X}_t$ 表示经过时间位置编码后的节点特征矩阵；$\boldsymbol{X}_{t,m}$ 是第 m 级时间窗口下的原始节点特征矩阵；$\mathrm{PE}_m(t)$是第 m 级时间窗口下的时间位置编码函数，反映节点在不同时间步的变化特征。

通过时间位置编码，动态图不仅保留了原有的空间特征，还能够在不同时间尺度上反映节点特征的变化趋势，为后续的时空特征提取和分类提供了高质量的节点特征。算法 2 表示具体的动态图构建与时间位置编码过程。

算法 2 动态图构建与时间位置编码

输入 网络流量数据集 D

输出 动态图序列$\{G_1,G_2,\cdots,G_T\}$

1. $\{G_1,G_2,\cdots,G_T\}\leftarrow\varnothing$//初始化图字典 G 为空

2. $\{\Delta t_1,\Delta t_2,\cdots,\Delta t_T\}\leftarrow$D//使用时间窗口对数据集进//行划分

3. For t = 1 to T do//对每个时间段 t 构建图

4. $V_t\leftarrow\{v_i\mid v_i\in\Delta t\}$//将时间段内的每个数据包映//射为节点集合

5. $X_t\leftarrow\{x_i\mid x_i\in R^d,\forall v_i\in V_t\}$//提取每个节点的特//征向量 x_i，维度为 d

6. $E_t\leftarrow\{e_{ij}\mid\forall(v_i,v_j)\}$//如果节点之间存在通信关//系，则添加边

7. $G_t=(V_t,E_t,X_t)$//构建时间段 t 的图 G_t

8. $X_t\leftarrow X_{t,m}+PE_m(t)$//对图 G_t 中的节点特征进行//时间位置编码

9. $G_t=(V_t,E_t,X_t)$//生成带有时间位置编码的图

10. $\{G_1,G_2,\cdots,G_T\}\leftarrow\{G_1,G_2,\cdots,G_T\}\cup\{G_t\}$//将//时间编码后的图添加到图序列中

11. End For

12. Return $\{G_1,G_2,\cdots,G_T\}$

在算法 2 中，动态图构建与时间位置编码的计算复杂度主要由时间窗口划分、节点和边的构建以及时间位置编码的计算组成。假设数据集被划分为 T 个时间段，每个时间段包含的节点数量为 n_t，节点特征的维度为 d，采用 M 个多级时间窗口，则总体复杂度为 $O(Tn_t^2+TMn_td)$。其中，$O(n_t^2)$来源于边集合构建的最坏情况，$O(Mn_td)$来源于多级时间窗口下的时间位置编码。

2.3 时空特征提取与融合

DSTG-IDS 的整体模型架构包括 4 个模块，即空间特征提取模块、时间特征提取模块、时空特征融合模块以及节点分类模块，具体架构如图 3 所示。

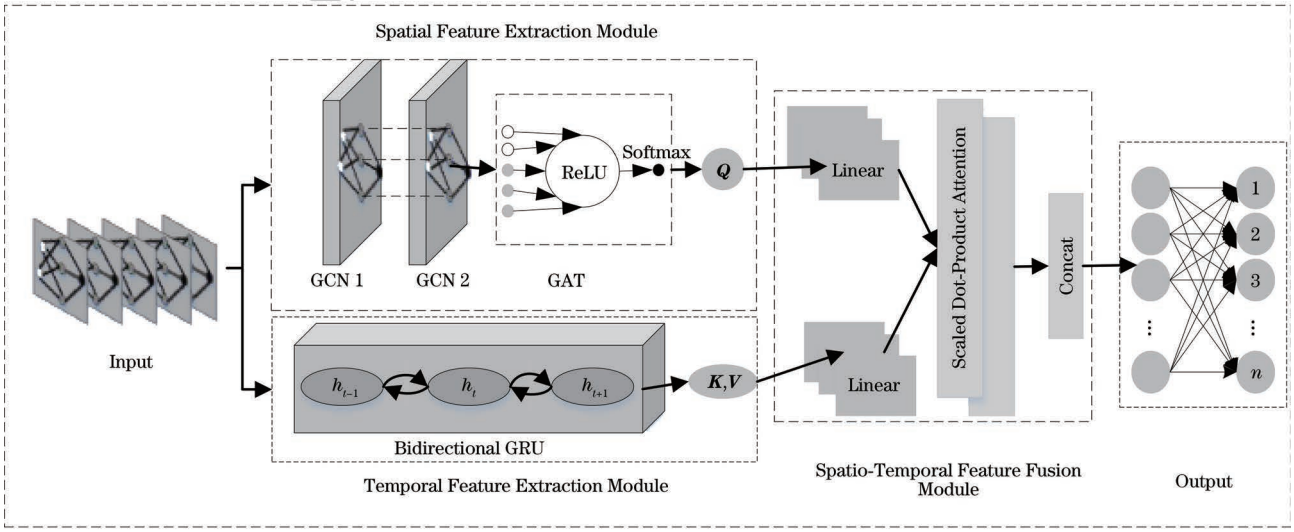

图 3 DSTG-IDS 模型结构

Fig. 3 DSTG-IDS model structure

2.3.1 空间特征提取模块

空间特征提取模块采用两层 GCN 和 GAT 对网络流量的局部结构信息进行学习。两层 GCN 利用消息传递机制提取领域特征，数学表达式如下：

$$H_{s1}=\sigma(\boldsymbol{D}_t^{-1/2}A_t\boldsymbol{D}_t^{-1/2}\boldsymbol{X}_t\boldsymbol{W}_1) \tag{6}$$

$$H_{s2}=\sigma(\boldsymbol{D}_t^{-1/2}A_t\boldsymbol{D}_t^{-1/2}H_{s1}\boldsymbol{W}_2) \tag{7}$$

式中：$\boldsymbol{X}_t$ 为时间位置编码后的节点特征矩阵；$\boldsymbol{D}_t$ 是邻接矩阵的度矩阵；$\boldsymbol{W}_1$ 和 $\boldsymbol{W}_2$ 是 GCN 的可学习权重矩阵；σ 是非线性激活函数。通过两层 GCN 的堆叠，可以在不同的图结构尺度上捕捉节点特征，提升对网络结构信息的表达能力。

为进一步增强网络对关键节点的关注，引入 GAT，通过自适应注意力机制分配邻居权重。具体的注意力系数计算和特征聚合如下：

$$a_{ij}=\text{Attention}(\boldsymbol{W}_{\text{gat}}[H_{s2}[i]\,\|\,H_{s2}[j]]) \tag{8}$$

$$H_{s3}=\sum_{j\in N(i)}a_{ij}\boldsymbol{W}_{\text{gat}}H_{s2}[j] \tag{9}$$

式中：a_{ij} 表示节点 i 和 j 之间的注意力权重；$\boldsymbol{W}_{\text{gat}}$ 表示 GAT 的权重矩阵；$H_{s2}[i]$ 代表节点 i 的空间特征；$H_{s2}[j]$ 代表节点 j 的空间特征；$\|$ 表示向量的拼接操作；$N(i)$ 表示节点 i 的邻居节点集合；H_{s3} 表示节点 i 经过 GAT 层后的特征表示。

2.3.2 时间特征提取模块

为了捕捉网络流量中时序的动态变化，DSTG-IDS 采用双向 GRU 对空间特征进行时间序列建模，以捕捉流量随时间变化的动态特征。双向 GRU 能够同时考虑时间序列的前后依赖性，使得每个时间段的节点特征既能受到过去时刻的信息影响，也能融合未来时刻的信息。前向、后向以及时间特征融合分别如式(10)～式(12)所示：

$$\overrightarrow{h}_t=\text{GRU}(H_{s3},\overrightarrow{h}_{t-1}) \tag{10}$$

$$\overleftarrow{h}_t=\text{GRU}(H_{s3},\overrightarrow{h}_{t+1}) \tag{11}$$

$$H_t=\overrightarrow{h}_t\oplus\overleftarrow{h}_t \tag{12}$$

式中：$\overleftarrow{h}$ 代表反向 GRU 在时间 t 的隐藏状态；$\overrightarrow{h}$ 代表正向 GRU 在时间 t 的隐藏状态；$\oplus$ 表示连接操作，用于将正向和反向的隐藏状态拼接。

2.3.3 时空特征融合模块

受 Transformer[25] 的启发，在提取空间和时间特征后，为了将这两者进行高效融合，本文引入多头注意力机制。多头注意力机制能够从不同的子空间中同时学习时间和空间之间的复杂关系，从而提升模型对时空特征的表达能力。多头注意力机制可以通过同时计算多个注意力头来学习不同的时空模式。单个注意力头的计算、多头注意力计算以及注意力机制的计算分别如式(13)～式(15)所示：

$$h_{\text{head},i}=\text{Attention}(H_t\boldsymbol{W}_i\boldsymbol{Q},H_t\boldsymbol{W}_i\boldsymbol{K},H_t\boldsymbol{W}_i\boldsymbol{V}) \tag{13}$$

$$H_f=\text{Concat}(h_{\text{head},1},\cdots,h_{\text{head},h})\boldsymbol{W}_O \tag{14}$$

$$\text{Attention}(\boldsymbol{Q},\boldsymbol{K},\boldsymbol{V})=\text{Softmax}\left(\frac{\boldsymbol{Q}\boldsymbol{K}^{\text{T}}}{\sqrt{d_k}}\right)\boldsymbol{V} \tag{15}$$

式中：H_f 表示最终时空融合后的特征表示；$\boldsymbol{Q}$、$\boldsymbol{K}$、$\boldsymbol{V}$ 分别表示查询、键和值矩阵；$\boldsymbol{W}_i\boldsymbol{Q}$、$\boldsymbol{W}_i\boldsymbol{K}$、$\boldsymbol{W}_i\boldsymbol{V}$ 分别表示第 i 个注意力头的查询、键和值的投影矩阵；d_k 表示缩放因子；Concat 表示拼接操作；$\boldsymbol{W}_O$ 表示线性变换矩阵。

2.4 节点分类

通过将网络流量建模为动态时空图，结合时间位置编码和多级时间窗口策略，将网络流量中的数据包建模为图的节点，并基于源 IP 和目标 IP 之间的通信关系构建边，从而构建能够捕捉时间动态变化和空间结构特征的图模型。在这个图模型中，节点代表特定时间段内的网络数据包，包含了丰富的流特征信息，而边代表节点间的通信关系。通过利用 GCN 和 GAT 进行空间特征提取，再通过双向 GRU 进行时间动态特征捕捉，最后利用多头注意力融合历史和当前特征，实现对节点特征的深度聚合与学习。传统入侵检测方法将网络流量建模为边来进行边分类，与传统方法不同，本文方法将入侵检测任务转变为节点分类任务，通过对每个节点进行分类来判断其是否为异常流量。这种节点分类方法能够更好地利用图神经网络的特征聚合能力，使得模型可以更有效地捕捉节点间的复杂交互关系和时间特征变化。节点分类的数学表达式如下：

$$P_t=\text{Log-Softmax}(\text{Classifier}(H_t^{\text{fusion}})) \tag{16}$$

式中：P_t 表示当前时间段的预测结果。利用交叉熵损失函数计算预测结果与真实标签之间的差异，并通过反向传播优化模型参数，这个过程在多个时间段上重复进行，最终输出预测结果。

3 实验结果及分析

3.1 实验数据集

本文使用 BoT-IoT[26]、ToN-IoT[27] 和 NF-CSE-CIC-IDS2018[5] 这 3 个数据集来评估所提方法的性能。数据集的具体统计信息如表 1 所示。

BoT-IoT 数据集由澳大利亚的网络安全合作研究中心(CSCRC)于 2018 年创建，旨在模拟物联网(IoT)环境中的各种网络攻击。该数据集包含了正常流量和多种攻击流量，包括拒绝服务(DoS)、DDoS、端口扫描、信息窃取等。

计算机工程 www.ecice06.com

表 1 数据集统计信息

Table 1 Dataset statistics

Dataset	Class Name	Number
BoT-IoT	Reconnaissance	91 082
	DDoS	1 926 624
	DoS	1 650 260
	Theft	500
	Normal	600
ToN-IoT	Backdoor	508 116
	DoS	3 375 328
	DDoS	6 165 008
	Injection	452 659
	Password	1 718 568
	Scanning	7 140 161
	XSS	2 108 944
	Normal	795 269
NF-CSE-CIC-IDS2018	Brute Force	287 597
	Bot	15 683
	DoS	269 361
	DDoS	380 096
	Infiltration	62 072
	Normal	7 373 563

ToN-IoT 数据集是由澳大利亚的新南威尔士大学(UNSW)开发,旨在全面分析 IoT 环境中的网络流量。该数据集包括网络流量数据、操作系统日志、应用程序数据和传感器数据,覆盖了正常流量和各种攻击流量,如 DoS、DDoS、信息窃取、恶意软件攻击等。

NF-CSE-CIC-IDS2018 数据集是 CSE-CIC-IDS2018 数据集的 NetFlow 格式版本,通过转换 CSE-CIC-IDS2018 数据集中的网络流量数据生成。该数据集通过模拟真实网络环境,收集了大量正常和攻击流量数据,攻击类型包括 DoS、DDoS、Web 攻击、暴力破解(Brute Force)、僵尸网络(Botnet)、渗透攻击(Infiltration)、Heartbleed 漏洞利用等。NF-CSE-CIC-IDS2018 数据集详细记录了协议类型、源 IP、目的 IP、端口号、字节数、包数等网络流量特征。

3.2 数据准备

数据准备阶段包括以下主要步骤:

1)按照时间窗口将网络流量转换为动态图序列,其中每条网络流量记录对应一个节点,通信关系被建模为边。

2)为保持真实网络场景中的交互信息,将动态图序列按时间顺序划分为 3 个部分,其中前 80%作为训练集,中间 10%和后 10%分别作为验证集和测试集。在训练集中,采用滑动窗口机制对动态图进行批量划分,每个窗口包含连续的 10 个动态图,窗口之间的重叠率为 90%,以最大限度地保留时间步之间的信息连贯性。需要注意的是,滑动窗口仅作为数据增强的手段,不会影响节点的标签分配。在二分类实验中,由于数据集大小从 3 669 066～22 264 053 条记录不等,为保证实验的可行性,对数据集按照 5%的比例进行采样,确保采样数据能够代表原始分布。对于多分类实验,部分数据集中不同攻击类型的样本数量差异较大,例如,在 BoT-IoT 数据集中,DDoS 攻击的样本数为 1 926 624,而 Theft 攻击仅有 500 条记录。因此,简单的比例采样可能会忽略某些小类别的攻击样本。为解决此问题,本文结合比例采样和实际攻击分布对数据集进行采样,并在采样后针对类别不平衡问题,利用过采样技术和焦点损失函数(Focal Loss)缓解模型性能退化的问题。此外,由于原始数据集中统计特征的取值范围存在数量级差异(如流量的字节数、数据包的长度等),因此所有数值型特征均经过归一化处理,以确保模型输入特征的标准化。

3.3 实验实现

实验基于 PyTorch 和 PyTorch Geometric 框架实现。模型的主要结构包括 2 层 GCN、1 层 GAT、1 层双向 GRU 以及多头注意力层,注意力头数为 4,使用 ReLU 作为非线性激活函数。在 GCN 和 GRU 单元中,隐藏层维度设置为 128,对应动态图中节点特征的嵌入维度。在具体实现中,滑动窗口大小为 10,重叠比例为 0.9,模型在每个滑动窗口内依次处理动态图序列,逐步提取节点的空间特征、时间特征并通过多头注意力机制进行融合,最后使用全连接层完成分类任务。

为防止过拟合,训练过程中在输入层和隐藏层均应用 0.5 的丢弃率(Dropout)。此外,为提高图神经网络在稀疏数据上的泛化能力,采用基于边丢弃(DropEdge)的传播策略。

模型优化采用 Adam 优化器,初始学习率为 0.001,批次大小为 1,并通过梯度累积(每 4 步更新一次梯度)实现更大的有效批次。训练轮次为 100,采用交叉熵损失函数监督分类任务,并在验证集上选择最佳模型参数,以确保测试阶段的最优性能。

3.4 实验结果分析

首先,设计一个二分类实验,以评估 DSTG-IDS 方法区分良性和攻击网络流量的能力;接着,为证明方法识别攻击类型的能力,设计更复杂的多分类实

验;最后,为验证方法中各个组件的有效性,进行消融实验。

3.4.1 二分类实验

在二分类实验中,将 DSTG-IDS 与 E-GraphSAGE、Extra Tree Classifier、Line Graph 等入侵检测方法进行比较。准确率(Accuracy)、召回率(Recall)、精确率(Precision)、F1 值(F1)和 FAR 结果如表 2 所示,最优结果加粗标注。

表 2 二分类实验结果

Table 2 Binary classification experiment results %

Method	Dataset	Accuracy	Recall	Precision	F1	FAR
DSTG-IDS	BoT-IoT	99.79	99.76	99.76	94.44	**0.02**
E-GraphSAGE[16]	BoT-IoT	99.99	99.99	**100.00**	**100.00**	0.05
Extra Tree Classifier[5]	BoT-IoT	**100.00**	**100.00**	99.99	**100.00**	1.05
DSTG-IDS	ToN-IoT	**99.76**	**99.00**	99.76	**99.23**	**0.01**
E-GraphSAGE[16]	ToN-IoT	97.87	97.86	**100.00**	99.00	1.92
Extra Tree Classifier[5]	ToN-IoT	97.86	97.86	99.30	99.00	2.10
DSTG-IDS	NF-CSE-CIC-IDS2018	**99.98**	**99.99**	**99.97**	**99.97**	**0.02**
Extra Tree Classifier[5]	NF-CSE-CIC-IDS2018	95.33	94.71	74.20	83.00	4.59
Line Graph[24]	NF-CSE-CIC-IDS2018	98.15	92.97	99.96	96.34	6.02

从表 2 可以看出,DSTG-IDS 在 BoT-IoT、ToN-IoT 和 NF-CSE-CIC-IDS2018 数据集上的二分类性能表现优异。总体来看,DSTG-IDS 在这 3 个数据集上的准确率、F1 值和误报率均优于其他对比方法。在 BoT-IoT 数据集中,DSTG-IDS 实现了 99.79%的准确率和 99.76%的召回率,同时将误报率控制在 0.02%,体现了较高的检测性能和较低的误报水平。在 ToN-IoT 数据集中,DSTG-IDS 的准确率达到 99.76%,误报率仅为 0.01%,进一步验证了其对复杂流量数据的适应能力。而在 NF-CSE-CIC-IDS2018 数据集中,DSTG-IDS 的准确率和 F1 值分别达到 99.98%和 99.97%,误报率仅为 0.02%。这些结果表明,DSTG-IDS 具备识别网络流量中的复杂特征并准确检测异常行为的能力。

3.4.2 多分类实验

表 3~表 5 分别展示了 DSTG-IDS 在 BoT-IoT、ToN-IoT 和 NF-CSE-CIC-IDS2018 数据集上的多分类实验结果。

表 3 BoT-IoT 数据集上的多分类实验结果

Table 3 Multi-classification experimental results on BoT-IoT dataset %

Class Name	Accuracy	F1
DDoS	99.76	99.79
DoS	99.69	99.77
Reconnaissance	98.74	99.36
Theft	98.00	98.19
Weighted Average	99.69	99.79

表 4 ToN-IoT 数据集上的多分类实验结果

Table 4 Multi-classification experimental results on ToN-IoT dataset %

Class Name	Accuracy	F1
DDoS	99.24	99.26
DoS	98.88	98.89
Backdoor	100.00	99.30
Injection	99.88	97.34
Password	97.22	98.50
Scanning	97.69	98.78
XSS	97.34	98.28
Weighted Average	98.61	98.61

表 5 NF-CSE-CIC-IDS2018 数据集上的多分类实验结果

Table 5 Multi-classification experimental results on NF-CSE-CIC-IDS2018 dataset %

Class Name	Accuracy	F1
DDoS	99.93	99.88
DoS	90.70	87.34
Bot	50.00	66.67
Brute Force	87.12	89.12
Infiltration	100.00	100.00
Weighted Average	93.26	93.19

总体来看,DSTG-IDS 在 DDoS 和 DoS 攻击检测中表现出色,在 BoT-IoT、ToN-IoT 和 NF-CSE-CIC-IDS2018 数据集上的平均准确率和 F1 值分别达到 99.69%和 99.79%、98.61%和 98.61%、93.26%和 93.19%。此外,对 Backdoor、Injection、

计算机工程 www.ecice06.com

Password 等攻击的检测也表现优异，特别是在 ToN-IoT 数据集上，Backdoor 和 Injection 攻击检测的准确率分别达到 100.00%和 99.88%。结果表明，DSTG-IDS 在识别多种攻击类型时具有良好的泛化能力和鲁棒性。

为了进一步验证 DSTG-IDS 的有效性，将其与其他入侵检测方法进行对比，包括 E-GraphSAGE、Extra Tree Classifier、Line Graph、k-NN 和 GSM-IDS[28]。表 6 展示了不同方法在 BoT-IoT、ToN-IoT 和 NF-CSE-CIC-IDS2018 数据集上的多分类实验结果。

表 6 不同方法的多分类实验结果

Table 6 Multi-classification experimental results of different methods %

Method	Dataset	Accuracy	F1
DSTG-IDS	BoT-IoT	99.69	99.79
E-GraphSAGE[16]	BoT-IoT	**99.99**	**100.00**
k-NN[4]	BoT-IoT	99.30	99.25
DSTG-IDS	ToN-IoT	**98.61**	**98.61**
E-GraphSAGE[16]	ToN-IoT	86.78	87.00
GSM-IDS[28]	ToN-IoT	98.16	95.27
DSTG-IDS	NF-CSE-CIC-IDS2018	**93.26**	**93.19**
Extra Tree Classifier[5]	NF-CSE-CIC-IDS2018	71.92	80.00
Line Graph[24]	NF-CSE-CIC-IDS2018	91.75	92.02

从表 6 可以看出，在 BoT-IoT 数据集上，DSTG-IDS 的准确率和 F1 值均优于 k-NN，与 E-GraphSAGE 仅相差 0.30 和 0.21 百分点，表现出稳定的检测性能。在 ToN-IoT 数据集上，DSTG-IDS 的准确率和 F1 值分别为 98.61%和 98.61%，优于 E-GraphSAGE 和 GSM-IDS。在 NF-CSE-CIC-IDS2018 数据集上，DSTG-IDS 的准确率和 F1 值分别为 93.26%和 93.19%，同样优于其他对比方法。这些结果进一步验证了 DSTG-IDS 在多分类任务中的有效性和先进性。

值得注意的是，在 DDoS 和 DoS 攻击检测中，DSTG-IDS 表现尤为突出。这类攻击通常通过大量伪造的流量来使目标系统瘫痪，具有显著的时间相关性。DDoS 和 DoS 攻击的流量模式往往在短时间内迅速增加，形成异常高的流量峰值，这种显著的时间特征，使得基于时空图神经网络的方法能够有效地捕捉和识别这类攻击。

DSTG-IDS 在 ToN-IoT 数据集上的混淆矩阵如图 4 所示，可以看出，DSTG-IDS 在 DDoS 和 DoS 攻击中的分类效果出色，几乎所有的攻击样本都能被正确分类，这进一步验证了 DSTG-IDS 在检测时间相关性攻击中的优势。降维后的特征嵌入分布如图 5 所示，可以看出，不同类型的攻击在特征空间中形成了明显的簇结构，特别是 DDoS 和 DoS 攻击样本，形成了高度集中的簇，这表明 DSTG-IDS 能够有效区分这类时间相关性强的攻击类型。

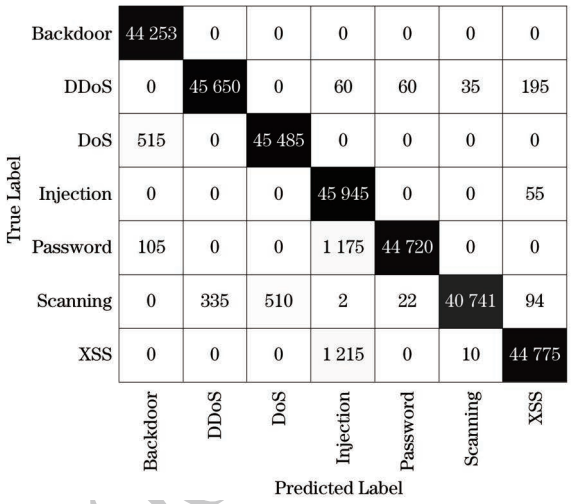

图 4 ToN-IoT 数据集上的多分类混淆矩阵

Fig.4 Multi-class confusion matrix on the ToN-IoT dataset

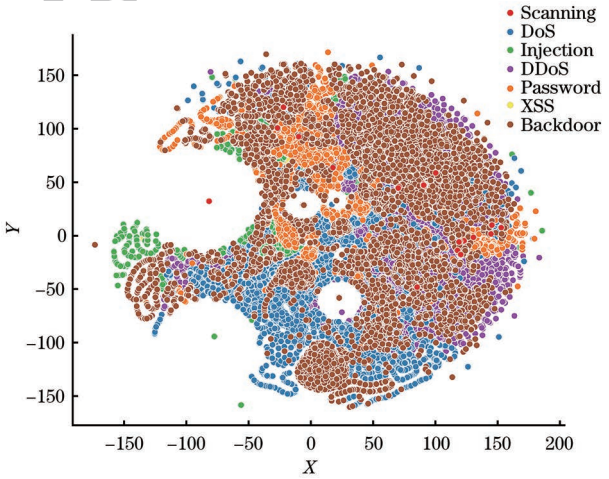

图 5 ToN-IoT 数据集上的多分类特征嵌入

Fig.5 Multi-classification feature embedding on the ToN-IoT dataset

3.4.3 消融实验

为了验证 DSTG-IDS 中各个组件(时间位置编码、动态图构建、空间特征提取、时间特征建模、关键节点增强等)对时空特征提取的有效性，进行了全面的消融实验。消融实验 1 的结果如图 6 所示，具体实验设置如下：

1)完整方法(DSTG-IDS)。使用完整的基于动态时空图神经网络的入侵检测方法，包括 2 层 GCN 提取空间特征，GAT 增强关键节点信息，双向 GRU 提取时间特征，并结合动态时空图表示方法。该实验在 ToN-IoT 数据集上的准确率为 98.61%，F1 值

为 98.61%。实验结果表明，动态时空特征提取对于提升入侵检测性能至关重要。

2）NoGRU。在该实验中，移除了双向 GRU 层，即不考虑时间特征提取，仅通过 2 层 GCN 进行空间特征提取，并结合 GAT 进行增强。结果显示，准确率下降至 61.37%，F1 值下降至 57.00%。这一结果表明，时间特征提取在入侵检测任务中具有重要性，双向 GRU 能够有效捕捉网络流量中的时间依赖关系，显著提升检测性能。

3）NoGAT。在该实验中，移除了 GAT 层，即不对空间特征进行关键节点增强，仅通过 2 层 GCN 进行空间特征提取。结果显示，准确率下降至 72.85%，F1 值下降至 70.50%。这一结果表明，GAT 的注意力机制对于捕捉重要节点的特征贡献显著，有助于增强对关键节点的关注，提高检测的准确性。

4）NoDynamicGraph。在该实验中，取消了动态图表示方法，改用静态图来表示网络流量，即每个时间段的数据包都被视为独立节点，忽略时间动态特征。结果显示，准确率为 80.32%，F1 值为 78.90%。这一结果表明，动态图构建在捕捉随时间变化的网络流量特征上起到了重要作用，使用静态图会显著降低模型性能。

5）NoGCN。在该实验中，移除了 2 层 GCN，仅通过双向 GRU 提取时间特征，不考虑空间特征提取。结果显示，准确率为 68.45%，F1 值为 65.10%。这一结果表明，空间特征提取在入侵检测中具有重要性，GCN 能够有效捕捉网络中节点之间的结构信息，从而提升检测性能。

6）GraphSAGE+DynamicGraph。为了对比不同的图表示方法，将本文提出的动态图表示与 GraphSAGE 相结合进行实验。结果显示，准确率为 94.99%，F1 值为 95.00%，尽管性能略低于 DSTG-IDS，但依然表现出较好的效果，这说明本文的动态图表示方法具有有效性，且具有较好的兼容性。

7）E-GraphSAGE。为了验证动态图表示方法的优势，与 E-GraphSAGE 进行对比实验。E-GraphSAGE 是一种边分类模型，通过映射 IP 地址来简化入侵检测任务。结果显示，E-GraphSAGE 的准确率为 86.78%，F1 值为 87.00%。相比之下，DSTG-IDS 在准确率和 F1 值上均有明显提升，说明本文提出的时空特征提取与融合策略在捕捉复杂时空关系方面表现出色。

8）NoTimeEncoding。在该实验中，移除了时间位置编码策略，仅保留原始节点特征进行时间特征提取。结果显示，在 ToN-IoT 数据集上，模型的准确率下降至 87.62%，F1 值下降至 86.99%。这一结果表明，时间位置编码能够有效增强节点在时间维度上的动态特征表示能力，从而提高检测性能。

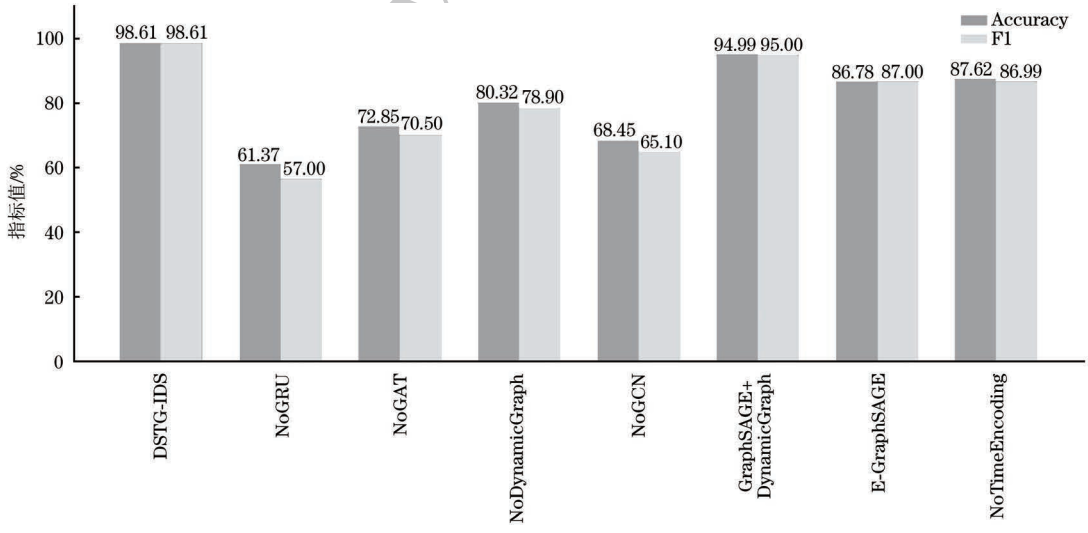

图 6 消融实验 1 的结果

Fig. 6 Result of ablation experiment 1

为了进一步验证 DSTG-IDS 中时间位置编码策略和动态时间窗口设计对模型性能的影响，特别是对时空特征提取的改进效果，进行消融实验 2 和实验 3，结果如图 7、图 8 所示。

1）不同时间窗口大小。测试不同时间窗口大小对模型性能的影响，窗口大小分别为 3、5、7、10、13 和 15。实验结果显示，当窗口大小为 10 时，模型性能最佳，准确率为 98.61%，F1 值为 98.61%。当窗口过小（3）和过大（15）时，准确率分别下降至 93.54%和 90.87%。这一结果表明，适中的时间窗

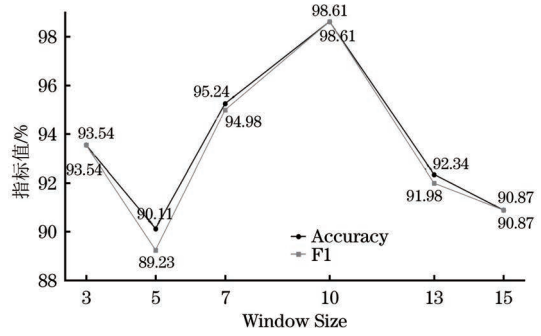

图 7 消融实验 2 的结果

Fig. 7 Result of ablation experiment 2

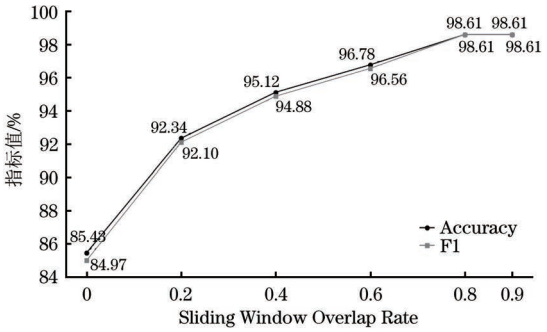

图 8 消融实验 3 的结果

Fig. 8 Result of ablation experiment 3

口大小能够平衡短期和长期特征的捕捉能力。

2)不同滑动窗口重叠率。测试不同滑动窗口重叠率(0、0.2、0.4、0.6、0.8、0.9)下的模型性能。实验表明,随着重叠率的增加,模型性能逐渐提高,重叠率为 0.8 时,准确率和 F1 值分别达到 98.61%和 98.61%,此后性能提升趋于平缓。重叠率为 0 时,模型性能下降至 85.43%的准确率和 84.97%的 F1 值,验证了滑动窗口机制在长序列特征稳定性上的增强效果。

为了评估 DSTG-IDS 模型在实际场景中的运行效率,对模型在 3 个数据集(BoT-IoT、ToN-IoT 和 NF-CSE-CIC-IDS2018)上的推理时间进行测试。实验环境包括 Intel i7-10700 CPU、16 GB RAM 和 NVIDIA RTX 3060 GPU。实验结果如表 7 所示。

表 7 推理时间分析

Table 7 Inference time analysis

Dataset	Average Inference Time/ms	Average Number of Nodes	Inference Time/ms
BoT-IoT	12.34	500	0.024 7
ToN-IoT	15.78	750	0.021 0
NF-CSE-CIC-IDS2018	18.23	1 000	0.018 2

推理时间测试结果表明,DSTG-IDS 的运行效率能够满足实时流量监测的需求。在 BoT-IoT 数据集上,每张图的平均推理时间为 12.34 ms,在 ToN-IoT 和 NF-CSE-CIC-IDS2018 数据集上,每张图的平均推理时间分别为 15.78 ms 和 18.23 ms。进一步对比节点数量的影响,推理时间与节点数量基本呈线性关系,平均每个节点的推理时间约为 0.02 ms。结果表明,DSTG-IDS 在大规模流量环境下具有良好的扩展性和运行效率,能够满足实时入侵检测的需求。

4 结束语

本文提出一种基于动态时空图神经网络的网络流量入侵检测方法 DSTG-IDS,通过将网络流量数据转化为动态时空图,结合 GCN、GAT 和 Bidirectional GRU,有效捕捉流量中的时空特征,展示了动态图在网络流量入侵检测中的潜力,证明了动态时空图神经网络在处理复杂网络拓扑和时空特征方面的优越性。与传统的静态图方法和仅注重统计特征的深度学习方法相比,DSTG-IDS 具有更高的检测准确率和鲁棒性。未来将致力于结合迁移学习和自监督学习等深度学习技术,进一步提升模型的泛化能力和鲁棒性。

参考文献

[1] FERRAG M A, MAGLARAS L, MOSCHOYIANNIS S, et al. Deep learning for cyber security intrusion detection: approaches, datasets, and comparative study[J]. Journal of Information Security and Applications, 2020, 50: 102419.

[2] XU X, WANG X N. An adaptive network intrusion detection method based on PCA and support vector machines[EB/OL]. [2024-09-05]. https://link.springer.com/chapter/10.1007/11527503_82.

[3] LIAO H J, RICHARD L C H, LIN Y C, et al. Intrusion detection system: a comprehensive review[J]. Journal of Network and Computer Applications, 2013, 36(1): 16-24.

[4] CHURCHER A, ULLAH R, AHMAD J, et al. An experimental analysis of attack classification using machine learning in IoT networks[J]. Sensors, 2021, 21(2): 446.

[5] BOOIJ T M, CHISCOP I, MEEUWISSEN E, et al. ToN-IoT: the role of heterogeneity and the need for standardization of features and attack types in IoT network intrusion data sets[J]. IEEE Internet of Things Journal, 2022, 9(1): 485-496.

[6] XU C Y, SHEN J Z, DU X. A method of few-shot network intrusion detection based on meta-learning framework[J]. IEEE Transactions on Information Forensics and Security, 2020, 15: 3540-3552.

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

[8] IMRANA Y, XIANG Y P, ALI L, et al. A bidirectional LSTM deep learning approach for intrusion detection[J]. Expert Systems with Applications, 2021, 185: 115524.

[9] AGARAP A F M. A neural network architecture combining Gated Recurrent Unit (GRU) and Support Vector Machine

(SVM) for intrusion detection in network traffic data[C]// Proceedings of the 10th International Conference on Machine Learning and Computing. New York, USA: ACM Press, 2018: 26-30.
[10] 李青, 王一晨, 杜承烈. 图表示学习方法研究综述[J]. 计算机应用研究, 2023, 40(6): 1601-1613.
LI Q, WANG Y C, DU C L. Survey on graph representation learning methods[J]. Application Research of Computers, 2023, 40(6): 1601-1613. (in Chinese)
[11] VINAYAKUMAR R, SOMAN K P, POORNACHANDRAN P. Applying convolutional neural network for network intrusion detection[C]//Proceedings of the International Conference on Advances in Computing, Communications and Informatics (ICACCI). Washington D. C., USA: IEEE Press, 2017: 1222-1228.
[12] LIU Z, ZHOU J. Introduction to graph neural networks[M]. San Rafael, USA: Morgan & Claypool Publishers, 2022.
[13] LEICHTNAM L, TOTEL E, PRIGENT N, et al. Sec2graph: network attack detection based on novelty detection on graph structured data[EB/OL]. [2024-09-05]. https://link.springer.com/chapter/10.1007/978-3-030-52683-2_12.
[14] ZERHOUDI S, GRANITZER M, GARCHERY M. Improving intrusion detection systems using zero-shot recognition via graph embeddings[C]//Proceedings of the 44th IEEE Annual Computers, Software, and Applications Conference (COMPSAC). Washington D. C., USA: IEEE Press, 2020: 790-797.
[15] ZHOU J W, XU Z Y, RUSH A M, et al. Automating botnet detection with graph neural networks[EB/OL]. [2024-09-05]. https://arxiv.org/abs/2003.06344.
[16] LO W W, LAYEGHY S, SARHAN M, et al. E-GraphSAGE: a graph neural network based intrusion detection system for IoT[C]//Proceedings of the IEEE/IFIP Network Operations and Management Symposium. Washington D. C., USA: IEEE Press, 2022: 1-9.
[17] VELIČKOVIĆ P, CUCURULL G, CASANOVA A, et al. Graph attention networks[EB/OL]. [2024-09-05]. https://arxiv.org/abs/1710.10903.
[18] MANESSI F, ROZZA A, MANZO M. Dynamic graph convolutional networks[J]. Pattern Recognition, 2020, 97: 107000.
[19] PAREJA A, DOMENICONI G, CHEN J, et al. EvolveGCN: evolving graph convolutional networks for dynamic graphs[J]. Proceedings of the AAAI Conference on Artificial Intelligence, 2020, 34(4): 5363-5370.
[20] 沈学利, 刘士枫. 基于图边缘特征注意力的入侵检测模型[J]. 计算机工程, 2024, 50(11): 236-245.
SHEN X L, LIU S F. Intrusion detection model based on graph edge feature attention[J]. Computer Engineering, 2024, 50(11): 236-245. (in Chinese)
[21] LIU Y X, PAN S R, WANG Y G, et al. Anomaly detection in dynamic graphs via Transformer[J]. IEEE Transactions on Knowledge and Data Engineering, 2023, 35(12): 12081-12094.
[22] CAI L, CHEN Z Z, LUO C, et al. Structural temporal graph neural networks for anomaly detection in dynamic graphs[C]// Proceedings of the 30th ACM International Conference on Information & Knowledge Management. New York, USA: ACM Press, 2021: 3747-3756.
[23] XU D, RUAN C W, KORPEOGLU E, et al. Inductive representation learning on temporal graphs[EB/OL]. [2024-09-05]. https://arxiv.org/abs/2002.07962.
[24] DUAN G H, LV H W, WANG H Q, et al. Application of a dynamic line graph neural network for intrusion detection with semisupervised learning[J]. IEEE Transactions on Information Forensics and Security, 2023, 18: 699-714.
[25] VASWANI A. Attention is all you need[EB/OL]. [2024-09-05]. https://arxiv.org/abs/1706.03762.
[26] KORONIOTIS N, MOUSTAFA N, SITNIKOVA E, et al. Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: BoT-IoT dataset[J]. Future Generation Computer Systems, 2019, 100: 779-796.
[27] SARHAN M, LAYEGHY S, MOUSTAFA N, et al. NetFlow datasets for machine learning-based network intrusion detection systems[EB/OL]. [2024-09-05]. https://arxiv.org/abs/2011.09144.
[28] 李晓佳, 赵国生, 汪洋, 等. 面向 CNN 和 RNN 改进的物联网入侵检测模型[J]. 计算机工程与应用, 2023, 59(14): 242-250.
LI X J, ZHAO G S, WANG Y, et al. Improved Internet of Things intrusion detection model for CNN and RNN[J]. Computer Engineering and Applications, 2023, 59(14): 242-250. (in Chinese)

文字编辑 吴云芳
栏目编辑 赖玉玲

计算机工程 www.ecice06.com