

基于图神经网络的在线恶意用户识别研究

周昕元, 曹冉, 丁培锦, 刘渊, 杨凯

(扬州大学信息工程学院, 江苏扬州 225127)

摘要: 在当今数字化时代, 网络安全问题日益严峻, 恶意用户通过互联网和社交网络展开攻击和欺诈活动, 威胁个人隐私、企业安全和社会秩序。传统安全方法在面对复杂网络结构和恶意行为时效果有限, 利用图神经网络识别恶意用户已成为关注焦点。为此, 研究经典的图神经网络(GNNs)模型(如GCN、GAT和GraphSAGE)在恶意用户识别中的应用, 以及通过添加差分隐私保护数据的方法, 并在两个真实数据集上开展了实验。结果表明, 图神经网络模型性能优于传统方法, 该模型为改善恶意用户识别提供了新思路, 有助于提升网络安全和用户隐私保护水平。

关键词: 图神经网络; 在线社交网络; 恶意用户检测; 差分隐私

DOI: 10.11907/rjdk.241469

中图分类号: TP399

文献标识码: A

开放科学(资源服务)标识码(OSID):

文章编号: 1672-7800(2025)007-0067-06



Research on Online Malicious User Identification Based on Graph Neural Network

ZHOU Xinyuan, CAO Ran, DING Peijin, LIU Yuan, YANG Kai

(College of Information Engineering, Yangzhou University, Yangzhou 225127, China)

Abstract: In today's digital era, the issue of cybersecurity is becoming increasingly severe. Malicious users conduct attacks and fraudulent activities through the Internet and social networks, posing threats to personal privacy, corporate security, and social order. Traditional security methods have limited effectiveness in dealing with complex network structures and malicious behaviors. Therefore, using graph neural networks to identify malicious users has become a focus of attention. This paper explores the application of classic GNN models (such as GCN, GAT, and GraphSAGE) in identifying malicious users, as well as methods for adding differential privacy to protect data. We conduct experiments on two real datasets, the experimental results demonstrate that graph neural network models outperform traditional methods. This paper provides new insights into improving the identification of malicious users, which contributes to enhancing network security and user privacy protection levels.

Key Words: graph neural networks; online social networks; malicious user detection; differential privacy

0 引言

在当今数字化时代, 社交网络已经成为人们日常生活中不可或缺的一部分, 为人们提供了便利的交流、信息共享与合作平台。然而, 随着社交网络的普及和发展, 恶意用户的存在和行为也日益突出, 他们通过网络进行各种欺诈活动和网络攻击, 给个人隐私、企业安全以及社会秩序

带来了严重威胁。这些恶意行为不仅损害了用户的信任, 也影响了网络生态的健康发展。在网络空间中, 恶意用户以各种方式出现: 从发布虚假信息、恶意攻击到非法获取他人个人信息等。传统的安全防御手段往往局限于规则制定和特征工程设计, 在面对复杂的网络结构和多变的恶意行为时显得力不从心。因此, 寻找一种能够有效识别和防范恶意用户的新型安全机制变得尤为迫切。

近年来, 图神经网络(Graph Neural Networks, GNNs)

收稿日期: 2024-06-18

扫描二维码阅读全文:



基金项目: 江苏省高等学校基础学科(自然科学)研究面上项目(22KJD120002); 江苏省大学生创新创业训练计划项目(202311117120Y)

作者简介: 周昕元(2003-), 男, 扬州大学信息工程学院学生, 研究方向为网络安全; 曹冉(2002-), 男, 扬州大学信息工程学院学生, 研究方向为网络安全; 丁培锦(1997-), 女, 扬州大学信息工程学院硕士研究生, 研究方向为图联邦学习; 刘渊(1997-), 男, 扬州大学信息工程学院硕士研究生, 研究方向为图神经网络模型优化; 杨凯(1987-), 男, 博士, 扬州大学信息工程学院讲师, 研究方向为图神经网络、图联邦学习。本文通讯作者: 杨凯。

[1-6]作为一种深度学习技术崭露头角,在图数据分析领域取得了显著进展[7-8]。GNNs能够有效地捕捉图结构中的信息和关系,已广泛应用于社交网络分析[9-11]、推荐系统[12-14]、生物信息学[15-16]等领域。特别地,在网络安全领域,利用图神经网络识别恶意用户成为备受关注的研究方向。图神经网络作为一种新兴的深度学习技术,在图数据分析领域取得了显著进展。图神经网络利用社交网络固有的图结构,能够有效地进行信息传播和邻居节点聚合,这对于捕捉复杂的模式和关系至关重要。近年来,一些研究探索了图神经网络在欺诈检测[17-22]和社交网络中恶意用户识别方面的应用。例如, Schlichtkrull 等[23]提出了 RGCN,它可以处理包含复杂关系的图,如实体关系图和知识图谱等,其基于边的卷积可以处理不同类型和方向的边。Bai 等[24]提出了 SimGNN,其采用图形相似性以学习图的表征,可以在没有标签的情况下进行无监督学习。

本文研究了图神经网络中的经典模型,如 GCN[25]、GAT[26]和 GraphSAGE[27-28],以及在恶意用户识别任务中的应用和在恶意用户识别方面的有效性,进一步推动社交网络中的欺诈检测方法研究。在恶意用户检测任务中,本文采用图神经网络生成的节点嵌入,并将其输入到逻辑回归分类器中,以预测用户是否恶意。同时,使用精确率、召回率、AUC 和 F1-score 等指标以评估模型性能。

本文利用图神经网络捕获社交网络中丰富的结构信息,并探索从邻居节点聚合信息的新方法,可以更好地理解和利用 GNNs 在社交网络安全领域的潜力,从而提高识别和应对网络中恶意行为的能力,维护网络环境安全与稳定。

1 模型概述

基于 GNNs 的恶意用户检测实质是一个在图上的节点分类任务,首先根据原始数据构造一个多关系不平衡图,图中部分节点被标记为“正常”或“欺诈”,然后通过已知的节点信息训练一个 GNNs 检测模型,最后使用该模型去预测未标记节点的标签类型,找出图中的“欺诈”节点。基于 GNNs 的恶意用户检测模型如图 1 所示。

图神经网络是一种深度学习框架,通过邻域聚合的方式迭代更新图中节点的表示。在多关系不平衡图中,定义经过 l 次迭代后节点 v 的表示 $h_v^{(l)}$ 如式(1)所示。

$$h_v^{(l)} = \sigma(DP(W^{(l)} \cdot \text{CONCAT}(h_v^{(l-1)}, h_v^{(l)}) + b^{(l)})) \quad (1)$$

其中, $h_v^{(l)}$ 表示节点 v 在第 l 次迭代后的表示; $W^{(l)}$ 和 $b^{(l)}$ 分别是第 l 层的权重矩阵和偏置项; σ 是激活函数; CONCAT 表示将 $h_v^{(l-1)}$ 和 $h_v^{(l)}$ 进行连接; DP 表示应用差分隐私机制,包括梯度裁剪和噪声注入。

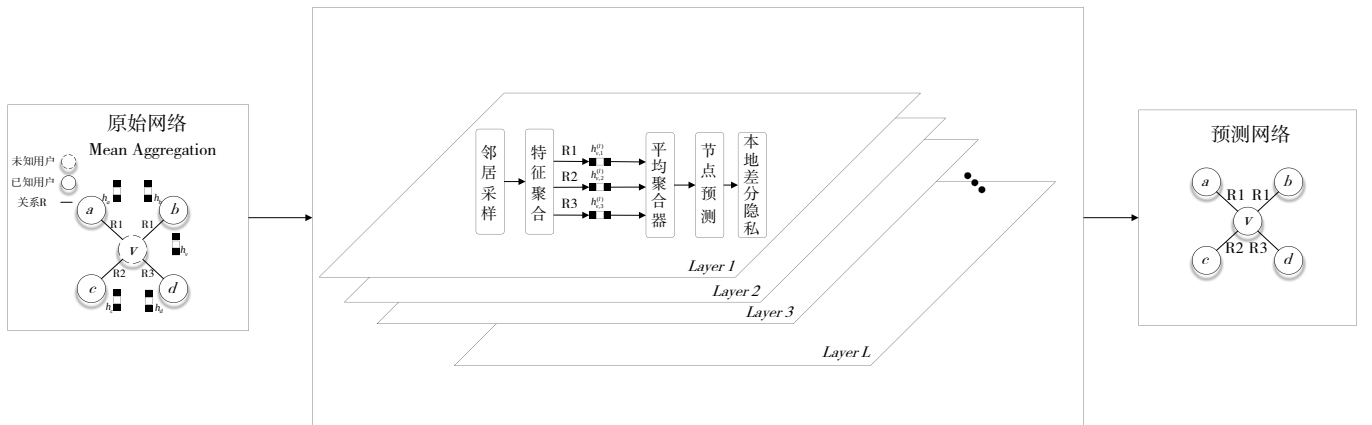


Fig. 1 GNNs-based malicious user detection model

图1 基于GNNs的恶意用户检测模型

点特征表示 $h_v^{(l)}$, 其中 l 表示层数。该步骤可用式(2)表示。

$$h_v^{(l)} = \sigma \left(\sum_{u \in N(v)} \frac{1}{\sqrt{d_v d_u}} h_u^{(l-1)} W^{(l-1)} \right) \quad (2)$$

其中, N_v 表示节点 v 的邻居节点集合, d_v 和 d_u 分别表示节点 v 和节点 u 的度(邻居节点的数量), $W^{(l-1)}$ 表示第 $l-1$ 层到第 l 层的权重矩阵, σ 表示激活函数 ReLU。

然后,将第 l 层的节点表示进行归一化,得到第 l 层的节点表示如式(3)所示。

$$h_v^{(l)} = \frac{h_v^{(l)}}{\|h_v^{(l)}\|_2} \quad (3)$$

这一步骤有助于平衡不同节点的度对聚合结果的影响。重复上述步骤,直到达到所需层数,通过将最后一层

2 研究方法

2.1 GCN 模型

GCN(Graph Convolutional Network)是一种用于图数据的深度学习方法。它通过对图的节点进行多层次的信息传播和聚合以学习节点的表示。GCN在处理节点分类、图节点嵌入等任务时表现出色。本文对数据集构建图模型为 $G = (V, E)$, 其中 V 表示节点集合, E 表示边集合。每个节点 $v \in V$ 都有一个特征向量 $x_v \in \mathbb{R}^d$, 表示节点的特征。GCN模型通过逐层进行信息传播以学习节点的表示。

对每个节点 v 的邻居节点进行聚合,得到聚合后的节

节点表示输入到 *Softmax* 函数中,可以进行节点分类任务。

2.2 GAT 模型

图注意力网络(Graph Attention Network, GAT)是一个经典的图神经网络算法,GAT将注意力机制引入信息聚合过程中,为每一个邻居节点分配一个可训练的注意力系数,最后融合邻居节点的特征信息以生成目标节点的嵌入表示。GAT模型包含两个主要步骤:①训练节点间的注意力系数;②聚合邻居节点的特征信息。

注意力机制:对于节点 v 的邻居节点 u ,注意力权重 e_{uv} 通过一个注意力函数 α 加以计算,如式(4)所示。

$$e_{uv} = \alpha(h_u, h_v) \quad (4)$$

其中, h_u, h_v 表示节点 v 和节点 u 的特征表示, α 是一个前馈神经网络,用于计算节点与节点之间的相关性。

计算完注意力权重后,对其进行归一化,得到每个节点 v 的注意力系数,如式(5)所示。

$$\alpha_{uv} = \frac{\text{softmax}(e_{uv})}{\sum_{k \in N(v)} \text{softmax}(e_{uk})} \quad (5)$$

其中, N_v 是节点 v 的邻居节点集合, *softmax* 函数用于将权重归一化到 $[0, 1]$ 区间。使用归一化后的注意力系数 α_{uv} ,更新节点 v 的表示如式(6)所示。

$$h'_v = \sigma\left(\sum_{u \in N(v)} \alpha_{uv} W\right) \quad (6)$$

其中, W 是权重矩阵,用于线性变换。

2.3 GraphSAGE 模型

GraphSAGE 模型是一种用于学习图结构数据中节点嵌入的重要图神经网络算法。与 GAT 等常见模型不同, GraphSAGE 专注于从节点的邻居中进行采样和聚合信息。该模型包含两个关键步骤:采样和聚合。

GraphSAGE 是一个 *inductive* 框架,针对图 $G = (V, E)$, 其中特征 $\{x_v, \forall v \in V\}$; K 个聚合器;权重矩阵 W^k , $\forall k \in \{1, \dots, K\}$ 。

算法主要步骤为:①初始化每个节点的特征向量 $v \in V$;②对于每一个节点拿到它采样后的邻居的特征向量 $u \in N(v)$,并将其聚合 $h_{N(v)}^k$,这里 $N(v)$ 表示对邻居采样;③根据聚合后的邻居 $h_{N(v)}$ 和自身 h_v 通过一个非线性变换 σ 更新自身特征。

聚合器架构定义了如何聚合节点的邻居特征。在 GraphSAGE 中,聚合器通过平均聚类实现,它会将邻居节点的特征取平均作为节点的新特征表示。GraphSAGE 提供了多种聚合器,实验中效果最好的均值聚合器,每个维度取对邻居特征相应维度的均值,如式(7)所示。

$$h_v^k = \sigma(W \cdot \text{Mean}(h_v^{k-1} \cup h_u^{k-1}, \forall u \in N(v))) \quad (7)$$

其中, *Mean* 是均值聚合, $\cup$ 则是将节点 v 和所有邻居节点的嵌入合并成一个新的集合。

2.4 恶意用户检测

对于恶意用户检测任务, GNN 模型生成的嵌入表示输入到二分类器(本文采用逻辑回归方法)中,以预测用户是

恶意的概率。评估指标如 AUC(ROC 曲线下的面积)用来评估恶意用户检测结果的准确性。

算法首先根据已知的在线社交网络关系生成负样本,使其与正样本数量相匹配。然后,将数据集划分为训练集和测试集。将“真边”和“假边”的嵌入生成,通过将相应节点对的嵌入连接起来。使用训练集训练逻辑回归分类器,并在测试集上评估其性能,以测量标签预测的准确性。

3 实验与结果分析

3.1 数据集

本文使用 Yelp 评论数据集和 Amazon 评论数据集来研究欺诈者伪装和基于 GNNs 的欺诈检测问题。Yelp 数据集包括由 Yelp 过滤(垃圾邮件)和推荐(合法)的酒店和餐馆评论;亚马逊数据集包括乐器类别下的产品评论。将超过 80% 的有用投票的用户标记为良性实体,而少于 20% 的有用投票的用户标记为欺诈实体。本文利用欺诈用户检测 Yelp 数据集和 Amazon 数据集上的任务,这是一个二元分类任务。人工选取 32 个重要特征(分别从中选取了 25 个重要特征),作为 Yelp(Amazon Resp.)的原始节点功能数据集。数据集与图表统计结果如表 1 所示。

Table 1 Dataset and chart statistics results

表 1 数据集与图表统计结果

	节点 (恶意用户/%)	关系	边	平均特征	平均标签
				相似	相似
Yelp	45 954 (14.5%)	R-U-R	49 315	0.83	0.90
		R-T-R	573 616	0.79	0.05
		R-S-R	3 402 743	0.77	0.05
		ALL	3 846 979	0.77	0.07
		U-P-U	175 608	0.61	0.19
Amazon	11 944 (9.5%)	U-S-U	3 566 479	0.64	0.04
		U-V-U	1 036 737	0.71	0.03
		ALL	4 398 392	0.65	0.05

对于 Yelp 数据集,将评论作为图中的节点,并设计了 3 种关系:①R-U-R:其连接由同一用户发布的评论;②R-S-R:它连接在同一产品具有相同的星星(1-5 星);③R-T-R:它连接同一个月发布的同一产品下的两个评论。

对于 Amazon 数据集,将用户作为图中的节点,并设计了 3 种关系:①U-P-U:其连接评论至少一个相同产品的用户;②U-S-V:连接一周内至少有一个相同星星的用户;③U-V-U:其连接所有用户中具有前 5% 的互评文本相似性(通过 TF-IDF 测量)的用户。

3.2 评价指标

为了评估模型恶意用户预测的表现,本文使用精确率(Accuracy)、召回率(Recall)、AUC 和 F1-score 值以评估模型性能。

其中, AUC 的计算过程如式(8)所示。

$$AUC = \frac{\sum_{i \in p} \text{rank}_i - \frac{M(M+1)}{2}}{M \times N} \quad (8)$$

其中, $rank_i$ 表示正样本的预测概率从小到大的排序值; M 表示正类样本总数; N 表示负样本总数。

精确率(Accuracy)的计算公式如式(9)所示。其中, TP 表示正样本被正确识别的数量, FP 表示负样本被识别错误的数量。

$$Accuracy = \frac{TP}{TP + FN} \quad (9)$$

召回率(Recall)的计算公式如式(10)所示。其中, FN 表示识别错误的正样本数量。

$$Recall = \frac{TP}{TP + FN} \quad (10)$$

F1-score(F1)的计算过程如式(11)所示。

$$F1 = \frac{2 \cdot P \cdot R}{P + R} \quad (11)$$

在图神经网络的应用中,多关系图提供了更丰富的信息,可以帮助模型更准确地学习和推断节点之间的关系,从而提升模型性能和泛化能力。

3.3 实验设置

实验通过选择数据集(Yelp 或 Amazon)和模型(GraghSAGE、GCN、GAT)以比较不同模型在节点分类任务上的性能,结果如图2、图3、表2、表3所示。批量大小为1 024,初始学习率为0.001,损失函数权重包括相似性损失权重($\lambda_1=2$)和权重衰减($\lambda_2=0.001$)。节点嵌入大小为64,训练周期数为31,每3个周期在验证集上进行一次评估。欠采样比例为1,支持CUDA加速,随机种子为72。若需差分隐私,噪声倍增器为0.1。实验通过训练、验证和测试步骤,

记录结果以评估模型性能。详细实验设置旨在全面评估模型在给定数据集上的性能。

本文与两个经典的机器学习方法——支持向量机(Support Vector Machine, SVM)和逻辑回归(Logistic Regression, LR)进行了对比。

3.4 实验结果分析

在 Amazon 数据集上, GraghSAGE、GCN 和 GAT 这些图神经网络模型相对于传统的机器学习模型(如 SVM 和逻辑回归)在准确度和 AUC 方面表现优秀,特别是在不同训练集百分比下。它们在各训练集百分比下保持着较高的准确率和 AUC 分数,表现相对稳定。这些模型特别适用于具有复杂关系结构的数据集,能够有效地捕捉和利用数据点之间的潜在关系,从而在任务中取得更高的性能。在 Yelp 数据集上,同样的模型相对于传统模型也表现出优势,尤其在准确率和 AUC 方面。它们在不同训练集百分比下都能保持较高的准确率和 AUC 分数,并且在不同训练集大小下表现相对稳健。这可以归因于它们能够更好地捕捉数据中的复杂关系,尤其是在具有复杂关系结构的数据集上,如 Yelp 数据集。结果表明,在 Amazon 数据集和 Yelp 数据集上, GraghSAGE、GCN 和 GAT 这些图神经网络模型相较于传统的机器学习模型表现更好。它们能够更有效地利用数据中的复杂关系,从而在分类任务中实现更高的准确率和 AUC 分数。此外,这些模型在不同训练集大小下都能保持相对稳健的性能,尤其是在较小的训练集下仍展现出了优秀的泛化能力。

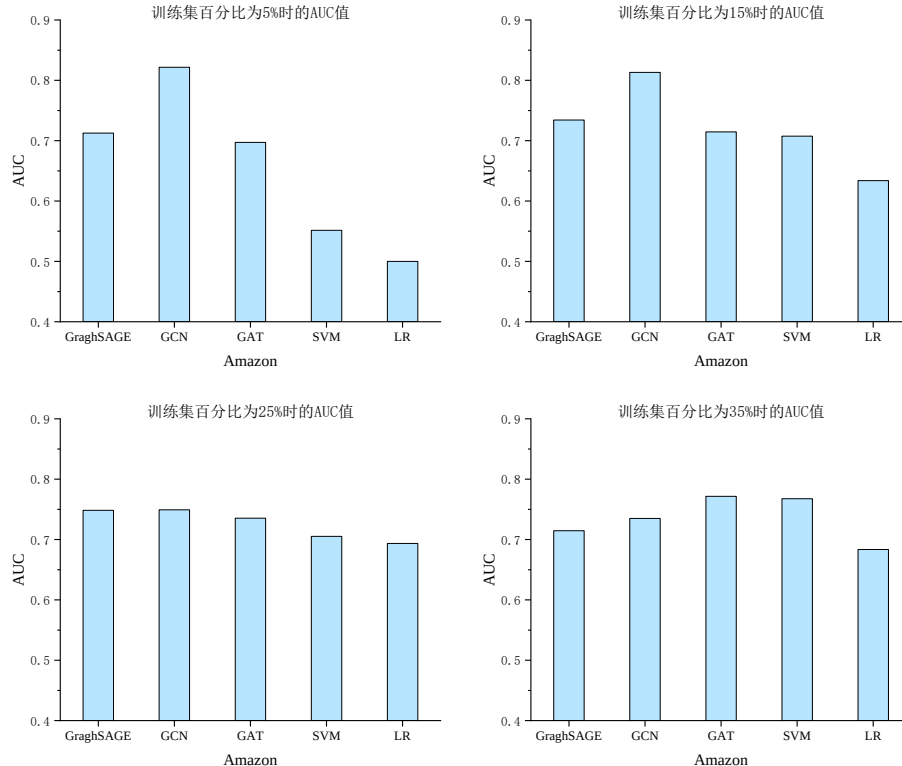


Fig. 2 Experimental results of malicious user prediction on the Amazon dataset

图2 在 Amazon 数据集上进行恶意用户预测的实验结果

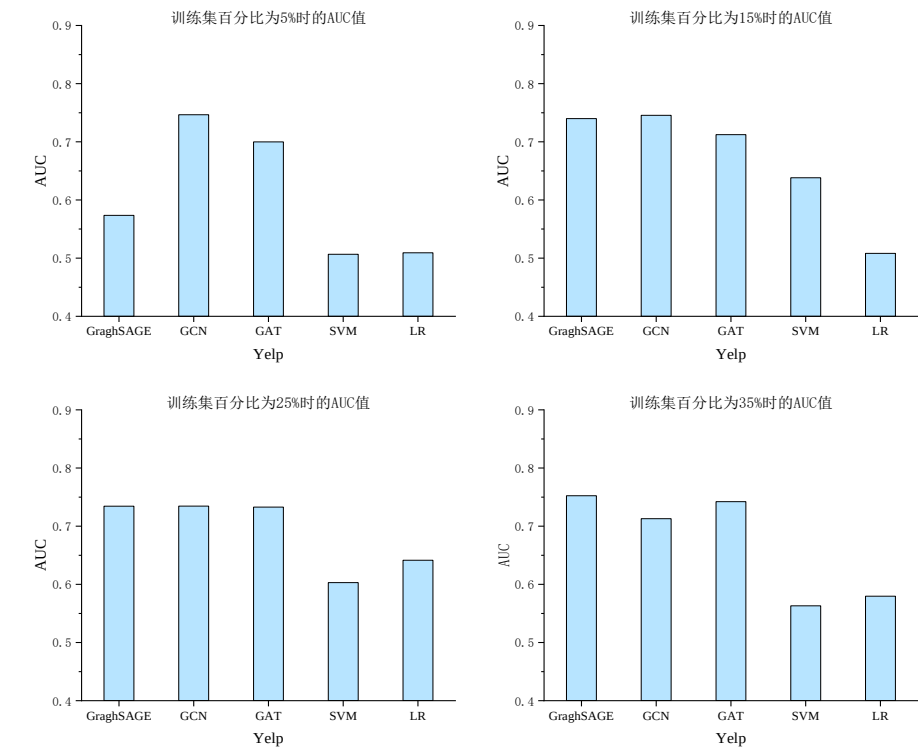


Fig. 3 Experimental results of malicious user prediction on the Yelp dataset
图 3 在 Yelp 数据集上进行恶意用户预测的实验结果

Table 2 Amazon dataset experiment results
表 2 Amazon 数据集实验结果

数据集	训练集 百分比/%	模型	Accuracy	AUC
Amazon	5	GraghSAGE	0.669 6	0.712 6
		GCN	0.908 5	0.821 6
		GAT	0.905 2	0.697 2
		SVM	0.914 5	0.551 5
		LR	0.914 5	0.5
	15	GraghSAGE	0.907 1	0.734 2
		GCN	0.829 3	0.813 1
		GAT	0.869 5	0.714 6
		SVM	0.914 5	0.707 5
		LR	0.948 3	0.633 8
	25	GraghSAGE	0.903 2	0.748 4
		GCN	0.852 5	0.749 2
		GAT	0.903 2	0.735 3
		SVM	0.971 2	0.705 2
		LR	0.959 2	0.693 5
	35	GraghSAGE	0.903 4	0.714 6
		GCN	0.903 4	0.734 9
		GAT	0.903 4	0.771 5
		SVM	0.970 9	0.767 6
		LR	0.966 1	0.683 4

Table 3 Yelp dataset experiment results
表 3 Yelp 数据集实验结果

数据集	训练集 百分比/%	模型	Accuracy	AUC
Yelp	5	GraghSAGE	0.739 4	0.537 5
		GCN	0.854 8	0.746 5
		GAT	0.854 2	0.699 8
		SVM	0.854 7	0.5
		LR	0.853	0.5
	15	GraghSAGE	0.789 5	0.739 9
		GCN	0.839 7	0.745 5
		GAT	0.854 8	0.712 3
		SVM	0.812 2	0.638 2
		LR	0.794 2	0.508 2
	25	GraghSAGE	0.828 3	0.734 4
		GCN	0.893 9	0.734 5
		GAT	0.830 4	0.732 8
		SVM	0.872 3	0.602 9
		LR	0.816 8	0.641 5
	35	GraghSAGE	0.855 3	0.752 3
		GCN	0.889 6	0.712 9
		GAT	0.839 8	0.742 1
		SVM	0.868 3	0.563 1
		LR	0.852 9	0.579 6

4 结语

图神经网络(GNNs)作为一种强大的机器学习工具,在恶意用户识别方面展示了巨大潜力。恶意用户识别是网络安全领域的一项关键任务,其目标是识别并阻止网络平台

上存在恶意行为的用户。传统的恶意用户识别方法通常依赖于特征工程和传统的机器学习算法,这些方法往往无法充分捕捉用户之间复杂的关系和行为模式。而GNNs能够有效地利用用户之间的网络结构和交互行为,从而提高了恶意用户识别准确性和效率。GNNs可以将用户和其交互行为建模为图结构,其中用户即为节点,用户之间的交互即

为边。通过这种方式,GNNs能够从全局的网络拓扑结构中学习到更丰富的特征表示,从而提高了恶意用户识别的性能。GNNs可以通过消息传递机制聚合用户节点及其邻居节点的信息,从而实现对用户行为的建模和预测。这种消息传递机制能够有效地捕捉用户之间的影响和依赖关系,进而提高了恶意用户识别鲁棒性和泛化能力。

但同时,GNNs在恶意用户识别领域也存在一些挑战和局限性。恶意用户行为的多样性和复杂性使得图模型的精准构建变得更加困难,恶意用户识别涉及隐私和安全等敏感信息,如何在保护用户隐私的前提下进行有效的模型训练和预测是一个重要问题。当前,大部分GNNs模型还存在着计算效率低、可解释性差等问题,限制了其在实际应用中的推广和应用。然而,GNNs作为一种新兴的机器学习方法,在恶意用户识别领域具有广阔的应用前景和发展空间。图神经网络算法层出不穷,构建更加高效、准确和可靠的恶意用户识别系统是未来热点研究方向。

参考文献:

- [1] WU Z, PAN S, CHEN F, et al. A comprehensive survey on graph neural networks[J]. IEEE Transactions on Neural Networks and Learning Systems, 2021, 32(1): 4–24.
- [2] XU B B, CEN K T, HUANG J J, et al. A survey on graph convolutional neural networks[J]. Journal of Computer Science, 2020, 43(5): 755–780.
徐冰冰, 岑科廷, 黄俊杰, 等. 图卷积神经网络综述[J]. 计算机学报, 2020, 43(5): 755–780.
- [3] AWASTHI A K, GAROV A K, SHARMA M, et al. GNN model based on node classification forecasting in social network[C]//2023 International Conference on Artificial Intelligence and Smart Communication, 2023: 1039–1043.
- [4] SARLIN P E, DETONE D, MALISIEWICZ T, et al. SuperGlue: learning feature matching with graph neural networks[C]//IEEE/CVF Conference on Computer Vision and Pattern Recognition, 2020: 4937–4946.
- [5] ZHANG Z, CUI P, ZHU W. Deep learning on graphs: a survey[J]. IEEE Transactions on Knowledge and Data Engineering, 2022, 34(1): 249–270.
- [6] LI Z, LIU F, YANG W, et al. A survey of convolutional neural networks: analysis, applications, and prospects[J]. IEEE Transactions on Neural Networks and Learning Systems, 2022, 33(12): 6999–7019.
- [7] ZHUKOV D, PEROVA J. A model for analyzing user moods of self-organizing social network structures based on graph theory and the use of neural networks[C]//2021 3rd International Conference on Control Systems, Mathematical Modeling, Automation and Energy Efficiency, 2021: 319–322.
- [8] XIAO S, LIN H, WANG C, et al. Graph neural networks with multiple prior knowledge for multi-omics data analysis[J]. IEEE Journal of Biomedical and Health Informatics, 2023, 27(9): 4591–4600.
- [9] LIU J, XING X, WANG T, et al. A survey on graph neural networks method under social recommendation[C]//Proceedings of the 2023 9th Annual International Conference on Network and Information Systems for Computers, 2023: 583–588.
- [10] WANG Y. Research on media communication based on graph neural network[C]//Proceedings of the 2023 International Conference on Blockchain Technology and Applications, 2023: 44–47.
- [11] ZHUKOV D, PEROVA J. A model for analyzing user moods of self-organizing social network structures based on graph theory and the use of neural networks[C]//Proceedings of the 2021 3rd International Conference on Control Systems, Mathematical Modeling, Automation and Energy Efficiency(SUMMA), 2021: 319–322.
- [12] ZHAO C X, XIE R D, KUANG J F. Research on product recommendation system of online mall based on graph neural network[C]//Chengdu: The 2023 6th International Conference on Software Engineering and Computer Science, 2023.
- [13] YU M, HE W T, ZHOU X C, et al. Review of recommendation system[J]. Journal of Computer Applications, 2022, 42(6): 1898–1913.
于蒙, 何文涛, 周绪川, 等. 推荐系统综述[J]. 计算机应用, 2022, 42(6): 1898–1913.
- [14] CHEN X, SHAN M. A recommendation method for process modeling based on clustering and graph neural network[C]//2021 8th International Conference on Dependable Systems and Their Applications, 2021: 195–201.
- [15] LI R, YUAN X, RADFAR M, et al. Graph signal processing, graph neural network and graph learning on biological data: a systematic review[J]. IEEE Reviews in Biomedical Engineering, 2023, 16: 109–135.
- [16] CHANG Q, LI C C, TIAN Q, et al. Classification of first-episode schizophrenia, chronic schizophrenia and healthy control based on brain network of mismatch negativity by graph neural network[J]. IEEE Transactions on Neural Systems and Rehabilitation Engineering, 2021, 29: 1784–1794.
- [17] YANG K, LIU Y, ZHAO Z, et al. Local structure-aware graph contrastive representation learning[J]. Neural Networks, 2024, 172: 106083.
- [18] LI K H, HUANG Z H. Noise filtering and feature enhancement based graph neural network method for fraud detection[J]. Acta Electronica Sinica, 2023, 51(11): 3053–3060.
李康和, 黄震华. 基于噪声过滤与特征增强的图神经网络欺诈检测方法[J]. 电子学报, 2023, 51(11): 3053–3060.
- [19] WANG H R, DOU Y T, CHEN C Y, et al. Attacking fake news detectors via manipulating news social engagement[C]//Proceedings of the ACM Web Conference, 2023: 3978–3986.
- [20] BONIOL P, PALPANAS T, MEFTAH M, et al. GraphAn: graph-based subsequence anomaly detection[C]//Proceedings of the VLDB Endowment, 2020: 2941–2944.
- [21] POURHABIBI A, ONG K L, KAM B H, et al. Fraud detection: a systematic literature review of graph-based anomaly detection approaches[J]. Decision Support Systems, 2020, 133: 113303.
- [22] ZHAO L, SAWLANI S, SRINIVASAN A, et al. Graph anomaly detection with unsupervised GNNs[DB/OL]. <https://arxiv.org/abs/2210.09535>.
- [23] SCHLICHTKRULL M, KIPF T, BLOEM P, et al. Modeling relational data with graph convolutional networks[C]//The Semantic Web: 15th International Conference, 2017: 593–607.
- [24] BAI Y, DING H, BIAN S, et al. SimGNN: a neural network approach to fast graph similarity computation[C]//Proceedings of the Twelfth ACM International Conference on Web Search and Data Mining, 2018: 384–392.
- [25] DEFFERRARD M, BRESSON X V, ERGHEYNST P. Convolutional neural networks on graphs with fast localized spectral filtering[C]//Proceedings of the 30th International Conference on Neural Information Processing Systems, 2016: 3844–3852.
- [26] VELIČKOVIĆ P, CUCURULL G, CASANOVA A, et al. Graph attention networks[C]//Vancouver: International Conference on Learning Representations, 2018.
- [27] HAMILTON W, YING Z, LESKOVEC J. Inductive representation learning on large graphs[C]//Proceedings of the 31st International Conference on Neural Information Processing Systems, 2017: 1025–1035.
- [28] LIU J, XING X, WANG T, et al. A survey on graph neural networks method under social recommendation[C]//2023 9th Annual International Conference on Network and Information Systems for Computers, 2023: 583–588.