软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2024,35(4):1774−1789 [doi: 10.13328/j.cnki.jos.007019]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

基于强化联邦 GNN 的个性化公共安全突发事件检测 *

管泽礼[1], 杜军平[1], 薛 哲[1], 王沛文[1], 潘圳辉[1], 王晓阳[2]

[1](智能通信软件与多媒体北京市重点实验室(北京邮电大学), 北京 100876)

[2](复旦大学 计算机科学技术学院, 上海 201203)

通信作者: 杜军平, E-mail: junpingdu@126.com

摘 要: 近年来, 将公共安全数据转换为图的形式, 通过图神经网络(GNN)构造节点表示应用于下游任务的方法, 充分利用了公共安全数据的实体与关联信息, 取得了较好的效果. 为了提高模型的有效性, 需要大量的高质量数据, 但是高质量的数据通常归属于政府、公司和组织, 很难通过数据集中的方式使模型学习到有效的事件检测模型.由于各数据拥有方的关注主题与收集时间不同, 数据之间存在 Non-IID 的问题. 传统的假设一个全局模型可以适合所有客户端的方法难以解决此类问题. 提出了基于强化联邦图神经网络的个性化公共安全突发事件检测方法 PPSED, 各客户端采用多方协作的方式训练个性化的模型来解决本地的突发事件检测任务. 设计了联邦公共安全突发事件检测模型的本地训练与梯度量化模块, 采用基于图采样的 minibatch 机制的 GraphSage 构造公共安全突发事件检测本地模型, 以减小数据 Non-IID 的影响, 采用梯度量化方法减小梯度通信的消耗. 设计了基于随机图嵌入的客户端状态感知模块, 在保护隐私的同时, 更好地保留客户端模型有价值的梯度信息. 设计了强化联邦图神经网络的个性化梯度聚合与量化策略, 采用 DDPG 拟合个性化联邦学习梯度聚合加权策略, 并根据权重决定是否对梯度进行量化, 对模型的性能与通信压力进行平衡. 通过在微博平台收集的公共安全数据集和 3 个公开的图数据集进行了大量的实验, 实验结果表明了所提方法的有效性.

关键词: 联邦学习; 图神经网络(GNN); 公共安全; 突发事件检测

中图法分类号: TP18

中文引用格式: 管泽礼, 杜军平, 薛哲, 王沛文, 潘圳辉, 王晓阳. 基于强化联邦 GNN 的个性化公共安全突发事件检测. 软件学报, 2024, 35(4): 1774–1789. http://www.jos.org.cn/1000-9825/7019.htm

英文引用格式: Guan ZL, Du JP, Xue Z, Wang PW, Pan ZH, Wang XY. Personalized Public Safety Event Detection Based on Reinforcement Federated GNN. Ruan Jian Xue Bao/ Journal of Software, 2024, 35(4): 1774–1789 (in Chinese). http://www.jos.org.cn/1000-9825/7019.htm

Personalized Public Safety Event Detection Based on Reinforcement Federated GNN

GUAN Ze-Li[1], DU Jun-Ping[1], XUE Zhe[1], WANG Pei-Wen[1], PAN Zhen-Hui[1], WANG Xiao-Yang[2]

[1](Beijing Key Laboratory of Intelligent Telecommunication Software and Multimedia (Beijing University of Posts and Telecommunications), Beijing 100876, China)

[2](School of Computer Science, Fudan University, Shanghai 201203, China)

Abstract: In recent years, the method of transforming public safety data into graph form and constructing node representations through graph neural networks for training and inference of downstream tasks has fully exploited the entity and association information of public safety data, achieving excellent results. Nevertheless, to enhance the effectiveness of the model, a large amount of high-quality data is needed, which is usually held by governments, companies, and organizations, making it difficult to learn an effective event detection

* 基金项目: 国家自然科学基金(62192784, U22B2038, 62172056, 62272058)
本文由“绿色低碳机器学习研究与应用”专题特约编辑封举富教授、俞扬教授、刘淇教授推荐.
收稿时间: 2023-05-15; 修改时间: 2023-07-07; 采用时间: 2023-08-24; jos 在线出版时间: 2023-09-11
CNKI 网络首发时间: 2023-11-24

model through data centralization. Moreover, due to different focuses and collection times of the data from various parties, there is a Non-IID (independent and identically distributed) problem among the data. Traditional methods that assume a global model can accommodate all clients are challenging to solve such issues. Therefore, this study proposes personalized public safety event detection (PPSED) method based on a reinforcement federated graph neural network. In this method, each client trains a personalized and more robust model through multi-party collaboration to solve local event detection tasks. A local training and gradient quantization module is designed for the federated public safety emergency event detection model and trained GraphSage through a minibatch mechanism based on graph sampling to construct a local model for public safety event detection. This approach reduces the impact of Non-IID data and supports the gradient quantization method to lower the consumption of gradient communication. A client state awareness module is also designed based on random graph embedding, which better retains the valuable information of the client model while protecting privacy. Furthermore, a personalized gradient aggregation and quantization strategy are designed for the federated graph neural network. Deep deterministic policy gradient (DDPG) is used to fit a personalized federated learning gradient aggregation weighting strategy, and it is determined whether the gradient can be quantized based on the weight, balancing the model's performance, and communication pressure. This study demonstrated the effectiveness of the method through extensive experiments on a public safety dataset collected from the Weibo platform and three public graph datasets.

Key words: federated learning; graph neural network (GNN); public safety; event detection

公共安全突发事件是指在一段时间内与公共安全相关的事件爆发并迅速传播, 引起公众广泛关注的现象.对这类事件进行及时检测和响应具有重要的意义, 可以帮助决策者更好地管理危机和做出决策[1,2]. 近年来,随着社交媒体的兴起, 公共安全突发事件的检测和演化发现已成为社交媒体挖掘的研究热点, 受到了学术界和工业界的广泛关注[3]. 相比传统的文本挖掘或社会网络挖掘, 公共安全突发事件检测任务更具挑战性, 因为它涉及社交网络和文本流的复杂交互. 在社交媒体平台如微博、Twitter 上, 公共安全事件通常以短文本的形式描述, 并通过时空共现、主题、发布信息、转发关系和标签信息等多个维度进行关联构建. 将公共安全数据转化为图的形式, 进一步进行事件检测和演化发现, 已成为主流方法[4−6].

图神经网络(GNN)已经成为机器学习领域的热门研究方向之一. 与传统的神经网络不同, 图神经网络是专门处理图数据的神经网络模型, 可以同时利用数据的特征信息与结构信息[7−9]. 图数据中每个节点代表一个实体, 每个边代表两个实体之间的关系, 如社交网络中的用户之间的关联、药物分子中的分子结构等[10,11]. 与只关注结构信息传统的图模型相比[12,13] , 图神经网络具有更好的表示能力和泛化性能. 通过特征的映射抽取有用的特征, 并根据图结构聚合节点的邻域特征信息, 构造节点表示并应用于下游任务的训练和推理[7,14]. 图神经网络已被广泛应用于社交网络分析[6,15]、交通预测[16]、药物结构预测[17]、推荐系统[18,19]、查询检索[20,21]等. 随着大数据的发展, 每天都会产生大量的原始公共安全数据, 高质量的数据可以提高模型的有效性. 但是, 大量数据缺少标注信息, 而人工标注成本高、时间长、效率低, 需要训练模型对图数据进行自动分析[22,23]. 由于高质量的数据通常归属于政府、公司和组织, 由于隐私、法规和利益的原因, 这些数据不能在各方之间自由流动[24,25], 很难通过数据集中的方式学习到有效的事件检测模型.

联邦学习是一种分布式机器学习方法, 它可以在数据不出本地的情况下, 采用多方协作的方式共同训练模型. 联邦学习不需要集中数据, 在一定程度上保护了数据的隐私, 还可以减少数据传输和存储的成本[26]. 在实际应用中, 拥有公共安全数据的各方由于关注的主题与任务不同, 导致各方数据是非独立同分布(Non-IID)的, 每个客户端中的数据都只有部分的标签. 与传统的数据 Non-IID 体现在标签分布不均匀不同, 这种 Non-IID 会同时体现在标签与图结构上. 然而, 在联邦设置中, 训练图神经网络仍然存在联邦图神经网络在 Non-IID 设置中表现不佳的问题[27−29], 其原因是因为错误地假设一个全局模型可以适合所有客户端[30]. 为了让各客户端可以在数据不出本地的条件下, 利用各方数据学习适用于本地任务的模型, 研究人员提出了个性化联邦学习, 允许各客户端采用差异化聚合策略, 将其他客户端的模型参数或梯度聚合到本地, 构建个性化的模型完成本地任务. 现有方法主要基于注意力机制[28,30]、微调全局模型[31]和正则化[32], 用于突发事件检测的个性化联邦图神经网络的研究存在通信量大、性能与通信压力难以平衡的问题.

强化学习可以根据环境与状态学习一个最优的动作策略, 已经广泛应用到机器人控制[33]、图神经网络节点选择[34]、自然语言处理[35]等任务中. 在强化学习中, 智能体通过与环境进行交互来学习动作策略, 通过尝

试和调整策略, 从而最大化长期奖励. 有研究[25]将强化学习引入到联邦学习的节点选择任务中, 使用客户端选择的方式减小通信压力, 但会造成联邦学习训练过程中梯度信息的损失. 状态空间设计是根据模型参数降维得到模型当前状态, 导致模型状态信息的损失. 构造合适的客户端模型状态, 可以帮助强化学习感知客户端信息, 更好地学习梯度聚合策略.

公共安全突发事件检测任务的主要难点有:

(1) 在实际应用中, 公共安全数据通常归属于政府、公司或组织, 数据不能在各方之间自由流动, 很难集中数据去训练事件检测模型; 并且, 公共安全数据通常构造为图数据来处理, 各方图数据的实体特征与结构都存在 Non-IID 的问题, 传统的联邦学习方法难以学习一个统一的模型帮助各方检测突发事件;

(2) 现有的个性化联邦图神经网络存在通信量大、性能与通信压力难以平衡的问题, 这为联邦学习梯度聚合策略提出了更高的要求;

(3) 当采用强化学习来拟合客户端加权与梯度量化策略时, 如何在保护数据隐私的同时, 使智能体准确地感知客户端状态是十分困难的.

针对上述问题, 本文提出了基于强化联邦图神经网络的个性化公共安全突发事件检测方法, 帮助各客户端采用多方协作的方式训练个性化的模型, 完成本地公共安全事件检测任务的同时, 在不显著损失模型性能的前提下, 平衡模型的性能与通信压力.

本文的主要贡献包括:

1) 提出了联邦公共安全突发事件检测模型结构与梯度量化方法, 采用基于图采样的 minibatch 机制的 GraphSage 构造公共安全突发事件检测本地模型, 以减小数据 Non-IID 的影响, 采用梯度量化方法减小梯度通信的消耗;

2) 提出了基于随机图嵌入的客户端状态感知方法, 采用随机图嵌入的数据原型感知模型联邦训练的梯度状态, 在保护数据隐私的同时, 更好地保留客户端模型有价值的梯度信息, 帮助强化学习智能体感知客户端状态信息;

3) 提出了强化联邦图神经网络的个性化梯度聚合与量化策略, 采用深度确定性策略梯度(DDPG)拟合个性化联邦学习梯度聚合加权策略, 对梯度进行加权后聚合构造本地个性化模型. 根据权重决定是否对梯度进行量化, 对模型的性能与通信压力进行平衡.

本文第 1 节介绍事件检测、图神经网络、联邦学习和强化学习的研究现状. 第 2 节介绍本文构建的基于强化联邦图神经网络的个性化公共安全突发事件检测方法. 第 3 节通过对比实验、通信优化实验与消融实验表明了所提方法的有效性. 第 4 节最后总结全文.

1 相关工作

1.1 事件检测

公共安全突发事件检测是从海量的社交媒体数据中挖掘真实世界的事件[36]. 社交媒体平台已经成为突发事件传播的主要媒介, 在社交媒体上的事件通常会吸引带有观点和情感的评论和转发[15], 可以帮助决策者更好地管理危机和做出决策[1,2]. Allan 等人[37]在连续的结构化文本流中发现事件, 实现话题检测与跟踪. 为了更好地利用实体之间的复杂关联, 研究人员将公共安全数据结构化为图的形式, 既可以保存数据中心众多实体的信息, 也可以更好地利用实体之间的关联[4,38]. 图以微博或 Twitter 为实体, 根据实体、时间、地点、评论、转发和主题构建关联[39,40]. Peng 等人[15]将多种关联与实体通过异质图的结构进行建模, 通过元路径关联实体, 捕获图中的元模式和检测突发事件. 有研究提出了强化的、增量的、跨语言的社会事件检测架构 FinEvent[41], 采用强化学习对图节点进行筛选, 结合空间密度聚类来分析增量数据中的突发事件. Cao 等人[1]提出了基于知识保持的增量异质图神经网络 KPGNN, 采用小批量子图采样策略进行可扩展的训练, 并定期删除过时数据以保持动态嵌入空间. 现有方法缺少在联邦条件下公共安全突发事件检测的相关研究.

1.2 图神经网络

图神经网络(GNN)可以从不同领域的复杂图结构数据中学习表示, 如药物发现[42,43]、社交网络[1,15,41]、推荐系统[18,44]和交通流建模[16,45]. 采用图神经网络可以从公共安全数据中发现突发事件. 近年来, 图卷积网络(GCN)[8]和 GAT[46]显著提高了图模型节点分类的水平. 然而, 由于 GNN 同时利用实体节点特征和图结构中的拓扑信息进行推理, 因此它容易受到图结构扰动的影响[47,48]. 鲁棒 GNN 减少了因图结构扰动导致 GNN 性能退化的问题. 鲁棒 GNN 主要关注对修改节点特征的修剪[49]或在图中添加/删除边[50]的敏感性. 需要特别关注各个机构与组织由于关注的主题与任务不同导致的数据和图结构的 Non-IID 问题. GraphSage[7]可以融合实体与实体邻居信息构造实体节点的低维稠密向量化表示, 它的本质上是学习一个能够将节点邻居信息聚合到节点特征表示的聚合函数. GraphSage 采用了归纳学习的策略, 即: 它只需要节点的邻居信息, 而不需要整个图的结构, 因此可以更好地处理新的、未见过的节点或图, 具有较好的泛化能力.

1.3 联邦学习

联邦学习支持以多方协作的方式在不共享本地数据的情况下, 利用多方的知识训练模型[51]. FedAvg[26]中, 每个客户端在本地训练模型后将训练好的模型传输到服务器, 服务端聚合模型权重, 将聚合的模型发回给客户端. 然而, 客户端本地数据可能存在较大差异, 因此, 如何解决各客户端数据的 Non-IID 是一个关键问题. Li 等人提出了 FedProx[32], 采用一个联邦正则化项, 最小化局部模型和全局模型之间的权重差异, 防止局部模型发散的同时, 保留了一定的个性化自由度. 当各个客户端数据极度异构时, 就不能错误地假设一个全局模型可以适合所有客户端. 需要为每个客户端协同训练个性化模型, 而不是学习单一的全局模型. Arivazhagan 等人[52]提出了 FedPer 在共享基本层的同时, 为每个客户端提供本地个性化层, 利用全局知识的同时保留本地知识, 克服数据 Non-IID 带来的不良影响.

个性化联邦学习在联邦图神经网络的研究中有着广泛的应用. He 等人[27]提出了一个联邦图神经网络框架 FedGraphNN, 对现有的 GCN[8], GAT[46]和 GraphSage[7]等图神经网络模型结合 FedProx, FedAvg 方法实现了联邦化, 但是没有考虑到数据的 Non-IID 对模型的影响. GraphFL[53]采用元学习与自我监督技术, 更充分地利用数据信息, 增强模型泛化能力, 提高联邦学习效果. SpreadGNN[28]提出了去中心化的个性化联邦学习方法, 分散周期平均随机梯度下降方法与任务正则化方法, 来提高个性化联邦学习应对 Non-IID 问题的能力. 但是这两种方法的效果还不够理想. Scardapane 等人[54]提出了一种分布式 GNN 训练算法, 在客户之间分享邻居特征和 GNN 层中间输出特征. BDS-GCN[55]在联邦训练的过程中, 对跨客户端邻居进行采样. 这两种方法不但通信成本很高, 而且有泄露隐私的风险. FedGCN[56]对联邦训练过程中邻居信息的通信与采样过程进行了优化, 但是没有解决有泄露隐私风险的问题. FedSage+[57]基于节点表示补全客户端图数据缺失的邻居信息, 需要分享具有生成客户端本地数据能力的模型, 存在数据泄露的风险容易受到数据重构攻击的问题, 对缺失节点与特征的补全能力有限.

1.4 强化学习

强化学习已经广泛应用到机器人控制[33]、图神经网络节点选择[34]、自然语言处理[35]等任务中. Q-Learning[58]是一种经典的强化学习方法, 适用于离散状态和动作空间, 它将智能体与环境交互的过程建模为马尔科夫决策过程, 通过迭代更新 Q 函数, 从而得到最优策略. DQN[59]是一种结合深度学习和 Q-Learning 的方法, 使用深度神经网络拟合 Q 函数. DQN 解决了传统 Q-Learning 在处理高维、连续状态空间时的困难. 强化学习在联邦学习和图神经网络中有着广泛的应用, 在 GNN 的节点聚合过程中, 采用强化学习对节点进行选择, 拟合节点选择策略[34,41]. 将强化学习引入到联邦学习模型聚合过程中, 客户端状态是通过模型参数降维得到的[25]. 随着模型训练参数的重要性会发生改变, 如果不改变降维规则, 参数信息就会损失; 如果改变降维规则, 则状态空间会发生改变使强化学习失效. 个性化联邦学习中根据各客户端模型差异对梯度进行加权后聚合[28,29], 解决了数据 Non-IID 的问题, 也降低了梯度信息的损失.

策略梯度(PG)方法[60]直接在策略空间中优化策略, 通过梯度上升最大化累积奖励, PG 能够处理连续动作

空间, 但可能会收敛到局部最优. 确定性策略梯度(DPG)[61]是一种在连续动作空间中使用的策略梯度方法, 直接在确定性策略空间中进行优化. 相比于随机策略的 PG, DPG 在连续动作空间中有更高的采样效率, 但是模型缺乏稳定性并存在收敛困难. DDPG[62]是基于深度神经网络的确定性策略梯度算法, 可以更有效地处理高维连续状态和动作空间. 有效的强化学习智能体需要准确的感知客户端状态. 为了使强化学习智能体感知客户端状态的同时保护数据的隐私, 可以通过梯度信息感知客户端状态的变化. 但是, 直接将模型梯度作为状态, 维度过大且稀疏, 会导致强化学习模型难以训练与收敛. 需要构造合适的客户端状, 帮助智能体感知客户端信息.

2 基于强化联邦图神经网络的个性化公共安全突发事件检测方法 PPSED

2.1 问题定义与方法概述

- 问题定义

在个性化联邦学习中, 通常包一组客户端 $C=\{C^1,\ldots,C^n\}$, 其中, n 是客户端的数量, C^m 是第 m 个客户端, 当不需要区分数据与变量来自于哪个客户端时, 会省略上角标. 每个客户端都保存了本地的图数据 $G=(V,E)$, 其中, V 是节点集合, E 是边集合. 节点 $v_i \in V$ 的特征向量表示为 h_i. 对于邻接矩阵 A, 如果节点 i 和节点 j 之间存在边, 则 $A_{i,j}=1$; 否则 $A_{i,j}=0$. 各客户端由于关注的主题与任务不同, 导致本地数据的特征、标签与图结构都存在 Non-IID 问题. 并且, 由于公共安全数据的敏感性, 各客户端之间的数据无法自由流动, 只允许共享梯度信息. 本方法的目标是在数据不出本地的条件下, 帮助各客户端利用多方资源, 训练本地个性化的模型, 帮助完成本地公共安全突发事件检测任务.

- 方法概述

本文提出了基于强化联邦图神经网络的个性化公共安全突发事件检测方法(personalized public safety event detection, PPSED), 采用多方协作的方式帮助各客户端训练个性化的模型, 完成本地公共安全事件检测任务. 设计联邦公共安全突发事件检测模型的本地训练与梯度量化方法, 将突发事件检测建模为一个分类任务, 采用基于图采样的 minibatch 机制训练 GraphSage 构造公共安全突发事件检测本地模型, 减小全局结构的 Non-IID 对其他客户端的影响. 提高模型对公共安全数据流中新旧数据 Non-IID 问题的鲁棒性. 采用梯度量化方法对模型梯度进行量化, 支持各客户端在聚合其他客户端模型梯度时, 根据 DDPG 得到的权重选择量化程度. 设计基于随机图嵌入的客户端状态感知方法, 在不暴露客户端本地数据的情况下, 将客户端的模型梯度信息转换为低维向量的形式, 保留客户端模型有价值的信息. 设计强化联邦图神经网络的个性化梯度聚合与量化策略, 基于准确率的提升构建强化学习的奖励 r, 采用深度确定性的策略梯度模型 DDPG, 拟合一个个性化联邦学习梯度聚合加权策略, 根据权重决定是否可以对梯度进行量化. 联邦过程是去中心化的, 客户端之间可以直接通信, 在每轮训练后, 各客户端需要分享公共安全突发事件检测模型的梯度、DDPG 模型的梯度、梯度量化指令和客户端梯度状态. 在生成随机图时, 各客户端需要分享本地数据节点间存在边的比例和节点特征的均值与标准差信息. 模型的整体结构如下文图 1 所示.

2.2 联邦公共安全突发事件检测模型结构与梯度量化

本文采用基于图采样的 minibatch 机制训练 GraphSage, 本质上是学习一个只需要节点的邻居信息, 而不需要整个图结构的 GNN, 这样可以更好地处理新的、未见过的节点或图. 采用节点采样和邻居采样抽取较小的子图训练模型, 从图中随机选择一定数量的节点作为 minibatch 的目标节点, 对于每个目标节点, 从其邻居节点中随机选择一定数量的节点作为的一阶邻居. 得到一个包含目标节点及其邻居节点的节点集合. 从原图中抽取相应的边, 生成一个子图. 这个子图包含了目标节点以及多跳邻居节点的信息, 适用于 minibatch 训练.

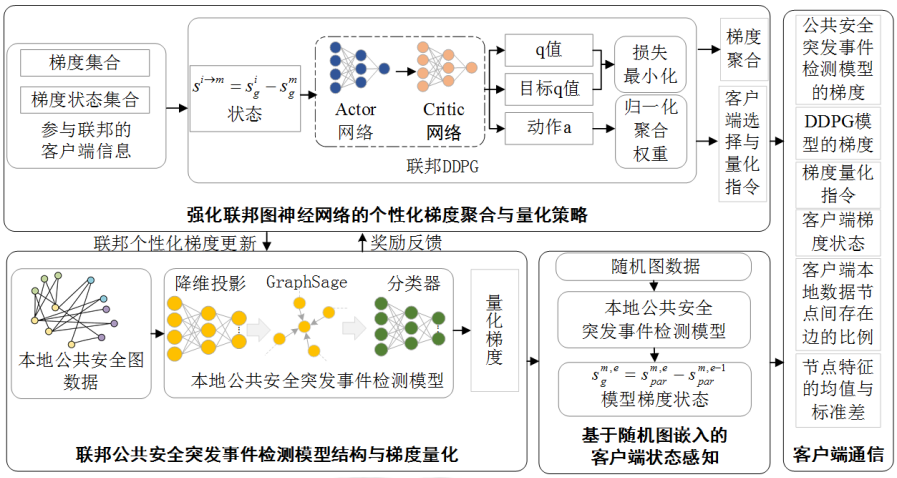


图 1 PPSED 模型的结构

在图神经网络中, 节点特征的维度对模型的性能有直接影响. 在 GraphSage 中, 如果节点特征的维度过大, 导致模型难以学习到有效的节点表示. 这是因为在图中一个节点的特征不仅仅取决于自身的特征, 还取决于其周围邻居节点的特征. 如果特征维度过大, 在聚合周围邻居节点的特征时会产生噪声. 在 GraphSage 之前, 先通过全连接层将节点特征维度降低. 这个全连接层可以看作是非线性的映射, 将高维的节点特征映射到低维的空间. 在这个低维空间中, 原本的高维特征中的冗余信息被剔除, 保留了更加关键的信息.在后续的 GraphSage 中, 模型只需要处理低维的特征, 从而提高模型的性能. 降维过程如公式(1)所示:

$$h_{v_i}^0=\sigma(w_{input}\cdot h_{v_i}+b_{input}) \tag{1}$$

其中, w_{input} 和 b_{input} 是特征降维隐层的参数; h_{v_i} 是节点 v_i 的初始特征; σ是一个非线性激活函数, 通常是 *ReLU*. 得到降维后的特征后, 对于每个节点 v_i, GraphSage 首先从其邻居节点 N_{v_i} 中收集特征, 通过聚合函数得到邻居节点特征的聚合表示. 通过一个非线性映射, 融合节点 v_i 自身的特征与邻居节点的聚合表示, 得到新的节点表示, 如公式(2)所示:

$$h_{v_i}^{(k)}=\sigma(w_s^{(k)}\cdot CONCAT(h_{v_i}^{(k-1)},AGG(\{h_u^{(k-1)},\forall u\in N(v_i)\}))) \tag{2}$$

其中, $h_{v_i}^{(k)}$ 表示在第 k 层的节点 v_i 的特征, $w_s^{(k)}$ 是第 k 层 GraphSage 的可学习参数, *CONCAT* 表示特征向量的拼接, *AGG* 是平均池化聚合函数.

在节点分类任务中, 在 GraphSage 的输出层后接一个分类器来进行分类任务. 经过 GraphSage 的学习后, 得到新的节点表示 $h_{v_i}^{(k)}$. 通过一个全连接层和一个 *softmax* 函数得到节点 v_i 的分类概率分布, 如公式(3):

$$p_{v_i}=softmax(w_{c_l}\cdot h_{v_i}^{(k)}+b_{c_l}) \tag{3}$$

其中, w_{c_l} 和 b_{c_l} 是分类器的可训练参数. 采用交叉熵构造分类损失, 如公式(4)所示:

$$L_{c_l}=-\sum\nolimits_{v_i\in V}\log(p_{v_i},y_{v_i}) \tag{4}$$

其中, y_{v_i} 是节点 v_i 的真实标签. 在获得了分类损失后, 使用反向传播算法计算 GraphSage 和分类器的梯度 $\frac{\partial L_{c_l}}{\partial w}$ 和 $\frac{\partial L_{c_l}}{\partial w_{c_l}}$, $grad^m$ 表示来自客户端 m 的梯度数.

采用梯度量化[63,64]的方式对梯度进行压缩. 梯度量化需要遍历所有的梯度, 找到梯度的最大和最小值, 确定量化范围, 根据梯度的范围与量化范围计算缩放因子和零点. 缩放因子表示浮点值和量化值之间的比例关系. 在梯度传到其他客户端后需要进行聚合计算. 使用量化过程中计算出的缩放因子和零点, 将量化的梯度值恢复回浮点数. 在不显著损失模型性能的前提下, 大幅降低了梯度所需的存储空间和传输带宽.

2.3 基于随机图嵌入的客户端状态感知

为了在保护客户端数据隐私的同时使 DDPG 更好地感知各个客户端的状态, 从而更有效地进行联邦学习中梯度的加权操作, 本文提出了一种基于随机图嵌入的客户端状态感知方法. 参考 Baek 等人[29]将随机数据输入到不同的模型中, 根据输出随机图嵌入的差异判断模型差异的思想, 本方法通过数据原型技术[65,66]消除随机图嵌入数据冗余, 通过随机图嵌入的数据原型, 帮助智能体感知客户端状态.

为了使随机图的数据原型可以更好地表示客户端状态, 需要构建一个数据多样的全局统一随机图 $G_r=(V_r, E_r,H_r)$. 图节点数目可以根据需求定义, 节点之间存在边的概率是根据各客户端节点之间存在边的概率均值决定的. 节点的特征 H_r 是基于各客户端节点特征的分布信息. 构造一个全局数据的分布, 通过对新的分布进行随机采样得到随机图节点特征. 将随机图输入客户端 m 的 GraphSage, 得到所有节点的表示后取均值, 作为本地模型的状态表示, 如公式(5)所示:

$$s_{par}^{m}=mean(GraphSage^{m}(G_r,H_r)) \tag{5}$$

可以得到特定客户端的模型状态. 在联邦学习中, 各客户端需要聚合的是梯度. 为了使强化学习感知梯度的状态, 使用本轮训练后的模型状态减去本轮训练前的模型状态获取梯度的状态 $s_g^{m,e}$, 其中, m 代表来自第 m 个客户端, e 代表第 e 轮训练, 如公式(6)所示:

$$s_g^{m,e}=s_{par}^{m,e}-s_{par}^{m,e-1} \tag{6}$$

随着训练的进行, 各个客户端的模型状态会发生变化, 这种变化可以通过梯度的状态得到体现. 通过分析梯度的状态, 可以帮助强化学习模型感知模型参数更新的情况, 从而对梯度的加权与量化进行决策. 解决了传统降维方法可能存在的信息丢失问题, 在保留了客户端信息的同时减小状态的维度, 提高模型训练的效率, 同时减小了通信的压力.

2.4 强化联邦图神经网络的个性化梯度聚合与量化策略

在个性化联邦梯度聚合工作中, 通过多方协作的方式, 为每个客户端训练一个本地的突发事件检测模型和 DDPG 模型. 在第一轮训练中, 各客户端对模型参数进行统一的初始化. 每轮训练中, 每个客户端都会接收到其他客户端本轮训练的梯度. 除了学习最优的客户端选择策略以外, 还需要根据不同客户端梯度对本地模型的重要性赋予梯度权重. 根据重要性决定是否对梯度进行量化后再传输, 以减小通信压力.

本文采用 DDPG 拟合一个最优的梯度加权与量化策略. DDPG 包含采用深度神经网络构建的行动者(actor)和评论家(critic). Actor f_a 根据状态 s 选择最优的梯度聚合权重 $a=f_a(s)$. Critic f_c 评估 Actor 选择的动作, 根据给定的状态-动作对(s,a), 预测期望的回报 $q=f_c(CONCAT(s,a))$.

在训练过程中, DDPG 采用了经验回放(experience replay)和目标网络(target networks)两种机制来增强模型的稳定性. 经验回放是指从环境中采样状态 s, 根据状态 s 使用 Actor 网络 f_a 选择动作 a. 执行动作 a, 从反馈中得到奖励 r 和新的状态 s', 得到经验(s,a,r,s')后存储到缓冲区, 然后从缓冲区中随机采样一批经验来进行训练. 评论家网络和 Actor 网络的训练可以看作是最小化两个损失函数的过程. 对于 Critic 网络, 定义损失函数为预测的 q 值和目标 q 值之间的均方误差, 如公式(7)所示:

$$L_{w_c}=\mathbb{E}_{s,a,r,s'\sim D}[(f_c(CONCAT(s,a))-z)^2] \tag{7}$$

其中, D 是缓冲区, 用来保存经验, z 是目标 q 值, 计算方法见公式(8):

$$z=r+\gamma f_{c'}(CONCAT(s',f_{a'}(s'))) \tag{8}$$

其中, γ是折扣因子, $f_{a'}$和 $p_{c'}$分别为目标 Actor 网络和目标 Critic 网络. 此损失函数表示了 Critic 网络预测的 q 值和实际经验的目标 q 值之间的差距. 对于行动者网络, 定义损失函数为预期回报的负值, 如公式(9)所示:

$$L_{w_a}=-\mathbb{E}_{s\sim D}[f_c(CONCAT(s,f_a(s)))] \tag{9}$$

本研究将客户端加权过程构建为马尔科夫决策过程, 具体设计如下.

状态设计. 在聚合梯度过程中, DDPG 需要决定如何为本地和其他客户端的梯度分配权重. 状态 s 的设计

包含源客户端梯度和本地梯度的信息, 采用拼接或差值的方式构造状态 s. 采用梯度状态的差值作为状态 s, 可以减小 DDPG 参数量, 增加联邦模型的稳定性;

动作设计. 定义动作空间, 即 Actor 网络的输出为一维, 代表源客户端梯度聚合到本地的动作, 如式(10):

$$a^{m\to j,e}=f_a(s_g^{m,e}-s_g^{j,e}) \tag{10}$$

其中, $a^{m\to j,e}$ 是第 e 轮聚合客户端 m 聚合到客户端 j 的动作. 将所有客户端的动作归一化后, 就得到了梯度聚合的权重;

奖励设计. 如果模型的准确率提升, 那么奖励值就是准确率提升的数值, 得到积极的反馈; 相反, 如果模型的准确率下降, 奖励值就是准确率下降的负值, 得到负面的反馈. 如公式(11):

$$r=\begin{cases}acc-acc_{pre}, & (acc-acc_{pre})>0\\ -(acc-acc_{pre}), & (acc-acc_{pre})<0\end{cases} \tag{11}$$

梯度请求与量化指令, 支持用户选择参与聚合的客户端比例 p_c 和被选中的客户端梯度量化的比例 p_q, 将梯度聚合的权重从大到小排序, 选择权重大的前$\lceil n*p_c\rceil$个客户端参与下一轮聚合. 前$\lceil n*p_c*(1-p_q)\rceil$个客户端的梯度不需要量化, 其他被选中客户端的梯度在传输到本地前需要进行量化.

2.5 训练过程

各个客户端在初始化参数之后, 执行本地突发事件检测模型的训练, 获取初始的梯度信息和客户端状态. 接收其他客户端传输的梯度、状态以及量化指令信息, 然后根据这些客户端的 DDPG 梯度, 采用 FedAvg 方法对本地 DDPG 参数进行更新. 本地 DDPG 根据各个客户端的状态信息, 决定梯度的聚合权重和量化策略. 将经过量化并传输到本地的梯度进行反量化处理后, 再根据梯度聚合权重来聚合梯度, 从而更新本地突发事件的参数. 计算出强化学习的奖励, 并将奖励、状态和动作信息存储到本地的经验缓冲区中. 利用这些状态、动作和奖励信息, 进一步训练本地的 DDPG. 在新一轮的本地突发事件检测模型训练结束后, 根据其他客户端的参数请求和量化指令, 向其他客户端传输梯度信息, 同时也发送出本地的梯度请求和量化指令.

在传统的联邦训练过程中, 数据被安全地保存在客户端本地, 只有模型参数被传输至中央服务器. 此方式保证了原始数据不会离开其所在的客户端, 显著降低了隐私泄漏的风险[26]. 有部分方法共享数据分布信息, 提高模型性能[66]. 同理, PPSED 也仅共享模型参数与少量分布信息, 而从这些信息中推断出准确的训练数据是极为困难的. 在需要严格保护隐私的场景下, 差分隐私[67,68]技术可以有效地保护客户端数据隐私, 进一步减轻数据泄露的风险, 从而提升整个过程的安全性. PPSED 同样可以在本地训练阶段融入差分隐私技术, 以适应对隐私保护要求更为严格的用户需求.

PPSED 客户端训练的过程见算法 1.

算法 **1**. PPSED 中客户端 m 的训练过程.

Input: 客户端集合 $C=\{C^1,\ldots,C^n\}$, 数据集合$\{G^1,\ldots,G^n\}$, 标签集合, 通信轮次 E, 客户端总数 n;

Output: 本轮模型梯度、状态.

1 初始化各客户端突发事件检测模型参数: w_{input}, w_{c_l}, w_s 和 DDPG 模型参数: w_a, w_c, $w_{a'}$, $w_{c'}$的参数.

2 根据公式(1)~公式(5)训练本地突发事件检测模型, 得到准确率 acc, 梯度 $grad^{m,0}$.

3 根据公式(5)、公式(6)得到状态 $s_g^{m,0}$.

4 **for** 轮次 $e\leftarrow 0,1,2\ldots,E-1$ **do**

5 接收其他客户端的梯度与本地梯度的集合 $\{grad^{1,e},...,grad^{n,e}\}$, $\{grad_{DDPG}^{1,e},...,grad_{DDPG}^{n,e}\}$、其他客户端的状态与本地状态的集合 $\{s_g^{1,e},...,s_g^{n,e}\}$ 以及本轮梯度在传往其他客户端时是否需要量化的指令.

6 根据 $\{grad_{DDPG}^{1,e},...,grad_{DDPG}^{n,e}\}$, 采用 FedAvg 更新本地 DDPG 参数.

7 **for** 客户端 $i\leftarrow 1,2\ldots,n-1$ **do**

8 $s'^{i\to m,e}=s_g^{i,e}-s_g^{m,e}$

9 $a^{i\to m,e}=f_a(s'^{i\to m,e})$

end

客户端梯度聚合权重 $softmax([a^{1\to m,e},...,a^{\lceil n*p_c\rceil\to m,e}])$.

对量化梯度进行反量化.

根据权重聚合梯度更新参数 w_{input}, w_{c_l}, w_s.

根据公式(11)计算奖励 r.

if e>0 **then**

将经验$(s^{m,e},a^{m,e},r^{m,e},s'^{m,e})$存入本地经验缓冲区 D^m.

从缓冲区中采样, 根据公式(4)~公式(6)、公式(12)训练 DDPG, 得到梯度 $grad^{m,e}_{DDPG}$.

根据公式(1)~公式(5)训练本地突发事件检测模型, 得到准确率 acc、梯度 $grad^{m,e+1}$.

根据公式(5)、公式(6)得到状态 $s_g^{m,e+1}$.

传输 $s_g^{m,e+1}$、$rad^{m,e+1}_{DDPG}$、根据量化指令量化的 $grad^{m,e+1}$ 和量化指令至其他客户端.

根据聚合权重选择下一轮参与联邦的$\lceil n*p_c\rceil$个客户端, 请求梯度、状态, 并向前$\lceil n*p_c*(1-p_q)\rceil$个客户端发送梯度不需要量化的指令

end

3 实验分析

3.1 实验数据

在微博平台收集的公共安全数据集 Weibo 和 3 个公开的图数据集 Cora[69], Citeseer[69]和 MSAcademic[70]上进行了大量的实验, 表 1 给出了数据集所对应的详细信息.

表 1 实验数据集

数据集名称	Weibo	Cora	Citeseer	MSAcademic
类别数量	50	7	6	15
节点数量	45 275	2 708	3 312	18 333
边数量	1 785 079	5 429	4 715	81 894
特征维度	1 000	1 433	3 703	6 805

Weibo 数据集收集了 2023 年 1 月–3 月与电信诈骗相关的微博内容、参与用户、转发关系、标签和多媒体信息. 根据“缅北”“东南亚”“缅甸”“东南亚诈骗”“电信诈骗”“保险诈骗”“信用证诈骗”“有价证券诈骗”等关键词获取. 共获取微博数据 45 275 条, 采用词袋模型来构造节点的初始特征. 以微博为实体节点, 添加节点间的关联作为边: (1) 如果微博提到了相同的组织或用户, 它们描述的事件就可能存在语义上的相似; (2) 如果微博内容中包含了相同的‘tag’, 通常描述的事件相同; (3) 如果两条微博包含了相同的图像“URL”, 则被判定存在边.

类别的标签需要尽量有概括性, 随着事件的发展, 新出现的内容可以包含在已经定义好的标签中. 本文将数据分为 50 类, 类别中包含了“集资诈骗”“养老保险诈骗”“校园诈骗”和“边境风险”等和电信诈骗高度相关的类别标签, 也包含了“境外诈骗警示”“诈骗报道”和“反诈宣传活动”这类官方发布的警示与教育类内容, 还包含“宗教文化”“旅游留学”等其他内容. 可以帮助捕获到电信诈骗各类事件的语义信息, 具备将关键信息筛选出来的能力.

在数据划分方面, 为了构建划分各客户端本地的子图数据, 利用了 Louvain 算法[71]在每个数据集上进行层次图聚类, 分别划分为 3 个、5 个和 10 个数据规模相近的聚类结果, 为数据所有者生成子图. 每个子图中, 训练、验证和测试数据的比例被设置为 60%, 20%和 20%. Weibo 数据的训练、验证和测试数据的划分是按照时间来划分的, 抽取 60%时间较旧的数据作为训练集, 较新的 40%数据随机划分为验证和测试集.

3.2 实验设置

公共安全突发事件检测网络包含一个映射层、两层 GraphSage 和一个分类层. 在 GraphSage 的每一层中的节点采样数为 5, batch 大小 32, 训练 epoch 设置为 80. 学习率分别为 0.001 和 0.000 1. 在 Python 中实现了所有方法, 在具有 1 个 NVIDIA 3080 Ti GPU 的服务器上执行了所有实验. 本文将图神经网络 GCN[8], GAT[46] 和 GraphSage[7]分别用联邦学习方法 FedAvg[26]和个性化联邦学习 FedProx[32]进行联邦化, 构造联邦图神经网络. GCN, GAT, GraphSage 设置参考 FedGraphNN[27]. 除了通过上述方法构造的 6 个基线算法方法以外, 还对比了采用 minibatch 机制的 FedSage[57]、采用元学习与自我监督技术的 GraphFL[53]和去中心化的个性化联邦学习方法 SpreadGNN[28]. 其中, GraphFL 的编码器采用了 GCN, SpreadGNN 的编码器为 GraphSage, 分类层采用了一层神经网络. 基线算法的分类器设置参考 FedGraphNN, 学习率设置是在 0.1–0.0001 中选择最优的学习率记录分类准确率[57]结果. 对客户端数量 n 设置为[3,5,10], 参与聚合的客户端比例 p_c 设置为[1,0.8,0.5]. 在通信优化实验中, 探索了被选中的客户端梯度量化的比例 p_q 对通信量与模型效果的影响. 在消融实验中, 探索了各组件的有效性.

3.3 对比实验

分别在 Weibo, Cora, Citeseer 和 MSAcademic 数据集上比较了 PPSED 方法与所有基线算法方法. 在不同客户端数量 n 和不同参与聚合的客户端比例 p_c 的设置下进行了大量的实验, 实验结果见表 2–表 5. PPSED 方法在所有的数据集和不同的设置中都显著优于其他的方法, 这表明 PPSED 方法对于公共安全突发事件检测以及图数据处理的效果是显著的, 在不同环境下都能保持稳定的高性能. GraphFL 和 SpreadGNN 的效果在所有数据集上的性能均不突出, 与其他基于 GCN 和 GraphSage 的方法相比提升不明显, 无法有效地处理数据分布的异质性. FedSage 方法的性能通常弱于 PPSED, 但仍优于其他方法. 这是因为 FedSage 同样采用了图采样与 minibatch 机制来训练本地模型, 具有一定的鲁棒性. 但是该方法的联邦过程没有根据各客户端梯度的重要性来对梯度加权, 导致不重要的客户端对其他客户端进行干扰, 没有预先剔除冗余特征. 其他方法在客户端数量和选择率变化时, 它们的性能波动更大. 这是由于它们对于非独立同分布(Non-IID)数据的处理能力较弱. 如图 2 所示, 其中, 图 2(a)是参与聚合的客户端比例 p_c 设置为 1 的结果, 图 2(b)是 p_c 设置为 0.8 的结果. 在这些方法中, FedAvg+sage 与 FedProx+sage 的 GraphSage 虽然是全采样的, 但是结构的异质性对它影响也较小, 与基于 GCN 与 GAT 的方法相比较, 更能适应这种异质性. 当参与聚合的客户端比例下降时, 所有方法的性能会下降. 然而, PPSED 的性能下降较少, 这表明本方法更能适应数据稀疏性的影响. 在所有数据集中, 随着客户端数量的增加, 所有方法的性能会下降, 这是因为数据在被划分为多个客户端时会损失大量的边. PPSED 的性能下降幅度较小, 这表明本方法可以更好地处理这种结构上的损失.

表 2　在数据集 Weibo 上的准确率对比

方法	p_c=1			p_c=0.8			p_c=0.5		
	n=3	n=5	n=10	n=3	n=5	n=10	n=3	n=5	n=10
FedAvg+GCN	0.468 9	0.459 0	0.430 8	0.467 6	0.437 2	0.421 5	0.397 5	0.484 3	0.500 6
FedAvg+GAT	0.506 1	0.503 4	0.456 1	0.507 0	0.471 8	0.555 4	0.496 5	0.535 7	0.561 4
FedAvg+sage	0.618 7	0.585 3	0.496 9	0.602 9	0.550 1	0.516 0	0.472 3	0.481 7	0.542 3
FedProx+GCN	0.471 2	0.433 8	0.424 1	0.469 2	0.429 8	0.403 2	0.410 5	0.504 4	0.524 9
FedProx+GAT	0.524 9	0.517 3	0.455 3	0.498 6	0.435 2	0.419 1	0.468 1	0.515 3	0.556 9
FedProx+sage	0.604 0	0.557 5	0.493 0	0.620 9	0.569 3	0.519 5	0.352 2	0.461 8	0.568 7
GraphFL	0.463 9	0.434 1	0.450 3	0.463 7	0.439 5	0.447 0	0.454 5	0.451 5	0.437 9
SpreadGNN	0.630 3	0.608 4	0.601 3	0.624 3	0.547 4	0.552 6	0.625 7	0.568 5	0.522 0
FedSage	0.700 0	0.680 0	0.643 8	0.677 1	0.650 1	0.624 2	0.625 0	0.612 5	0.598 9
PPSED	**0.782 9**	**0.734 9**	**0.702 3**	**0.745 2**	**0.718 5**	**0.692 9**	**0.732 6**	**0.703 5**	**0.675 2**

表 3 在数据集 Cora 上的准确率对比

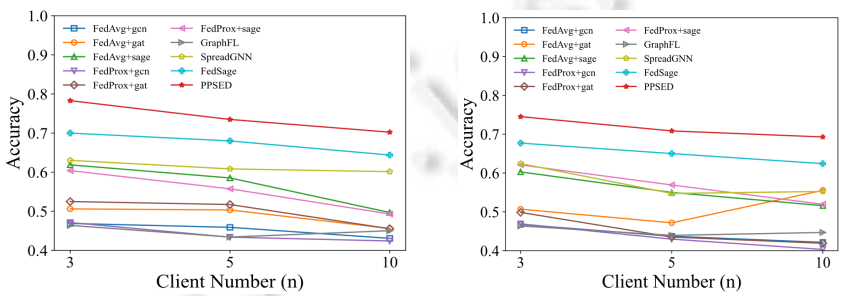
方法	p_c=1			p_c=0.8			p_c=0.5		
	n=3	n=5	n=10	n=3	n=5	n=10	n=3	n=5	n=10
FedAvg+GCN	0.543 7	0.542 1	0.505 4	0.528 0	0.521 9	0.496 5	0.541 8	0.520 0	0.513 2
FedAvg+GAT	0.541 9	0.509 4	0.488 7	0.476 5	0.455 2	0.427 0	0.542 3	0.505 4	0.485 4
FedAvg+sage	0.687 4	0.703 2	0.626 9	0.677 3	0.624 9	0.644 0	0.591 0	0.542 7	0.569 9
FedProx+GCN	0.575 0	0.562 5	0.518 6	0.553 5	0.534 3	0.516 0	0.517 1	0.533 2	0.571 9
FedProx+GAT	0.490 8	0.610 7	0.643 9	0.555 4	0.610 6	0.664 8	0.468 4	0.512 0	0.444 6
FedProx+sage	0.705 6	0.696 0	0.660 4	0.676 2	0.672 7	0.634 9	0.628 5	0.606 4	0.589 2
GraphFL	0.658 2	0.659 7	0.645 5	0.649 6	0.654 2	0.655 7	0.654 7	0.642 3	0.669 7
SpreadGNN	0.720 9	0.727 4	0.643 4	0.676 5	0.647 1	0.524 2	0.615 6	0.562 4	0.627 0
FedSage	0.739 6	0.730 0	0.715 2	0.751 7	0.725 0	0.683 8	0.700 4	0.698 8	0.676 9
PPSED	**0.786 7**	**0.785 9**	**0.749 5**	**0.796 0**	**0.765 3**	**0.729 4**	**0.771 3**	**0.746 7**	**0.738 9**

表 4 在数据集 Citeseer 上的准确率对比

方法	p_c=1			p_c=0.8			p_c=0.5		
	n=3	n=5	n=10	n=3	n=5	n=10	n=3	n=5	n=10
FedAvg+GCN	0.535 2	0.537 7	0.515 3	0.571 5	0.515 6	0.499 8	0.533 2	0.569 3	0.554
FedAvg+GAT	0.535 7	0.546 7	0.504 5	0.527 9	0.545 6	0.499 8	0.601 9	0.582 0	0.557 2
FedAvg+sage	0.709 1	0.654 0	0.510 3	0.712 8	0.622 6	0.524 1	0.525 6	0.514 3	0.544 0
FedProx+GCN	0.546 0	0.553 5	0.488 8	0.540 2	0.555 1	0.445 8	0.522 9	0.577 5	0.521 9
FedProx+GAT	0.564 4	0.545 2	0.484 1	0.526 6	0.553 4	0.496 0	0.554 9	0.547 6	0.499 9
FedProx+sage	0.704 8	0.649 3	0.561 5	0.689 4	0.608 8	0.525 7	0.719 7	0.630 5	0.607 9
GraphFL	0.629 1	0.628 5	0.631 7	0.624 6	0.647 8	0.642 8	0.644 7	0.659 6	0.649 8
SpreadGNN	0.659 4	0.682 1	0.717 4	0.656 0	0.680 3	0.735 2	0.710 3	0.704 5	0.693 4
FedSage	0.708 3	0.681 3	0.712 5	0.656 2	0.687 5	0.625 0	0.677 1	0.657 5	0.700 0
PPSED	**0.735 3**	**0.710 5**	**0.739 3**	**0.681 1**	**0.712 1**	**0.654 2**	**0.704 0**	**0.686 1**	**0.730 3**

表 5 在数据集 MSAcademic 上的准确率对比

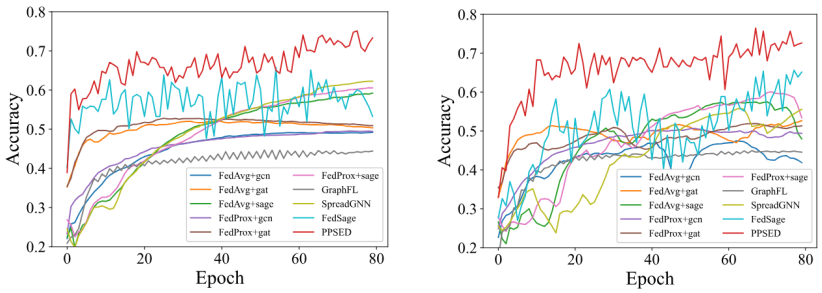
方法	p_c=1			p_c=0.8			p_c=0.5		
	n=3	n=5	n=10	n=3	n=5	n=10	n=3	n=5	n=10
FedAvg+GCN	0.924 3	0.905	0.883 3	0.911 3	0.895 2	0.895	0.895 4	0.889 9	0.906 2
FedAvg+GAT	0.916 7	0.915 1	0.885 5	0.912 1	0.913 5	0.908 8	0.911 4	0.852 0	0.880 8
FedAvg+sage	0.916 6	0.914 5	0.878	0.932 9	0.888 0	0.886 0	0.805 9	0.901 3	0.847 6
FedProx+GCN	0.905 8	0.887 9	0.884 7	0.910 9	0.896 3	0.889 0	0.896 8	0.914 2	0.886 4
FedProx+GAT	0.915 2	0.907 7	0.886 6	0.919 3	0.914 5	0.868 2	0.902 6	0.920 8	0.897 9
FedProx+sage	0.901 6	0.881 5	0.900 0	0.924 8	0.909 2	0.893 1	0.882 0	0.907 0	0.888 9
GraphFL	0.925 3	0.892	0.850 5	0.872 4	0.873 6	0.893 6	0.899 4	0.881 6	0.875 4
SpreadGNN	0.925 3	0.892	0.850 5	0.872 4	0.873 6	0.893 6	0.899 4	0.881 6	0.875 4
FedSage	0.964 1	0.937 0	0.911 5	0.915 5	0.906 9	0.918 5	0.898 7	0.888 0	0.878 6
PPSED	**0.985 4**	**0.955 4**	**0.935 3**	**0.938 9**	**0.926 4**	**0.924 4**	**0.948 3**	**0.925 6**	**0.910 7**



(a) p_c=1 (b) p_c=0.8

图 2 在 Weibo 数据集中客户端数量对模型结果的影响

针对模型的收敛性分析，在 Weibo 数据上从表 2 的实验结果可以看出：p_c=0.8 时，准确率的降低不明显. 本实验将参与聚合的客户端比例 p_c 设置为 1 和 0.8，探索 p_c 对实验结果的影响，实验结果如图 3 所示.



(a) p_c=1　　(b) p_c=0.8

图 3　在 Weibo 数据集中模型收敛性分析

实验结果表明, PPSED 是所有方法里面效果最好、稳定性较高的方法.

3.4　通信优化实验

为了探索客户端参与联邦聚合的比例 p_c 和客户端梯度量化的比例 p_q 对模型准确率和通信成本的影响, 本实验在 Weibo 数据集上, 将客户端数量设置为 5, p_c 设置为 1, 0.8 和 0.5, p_q 设置为 1, 0.7 和 0.4, 分别进行实验, 实验结果见表 6.

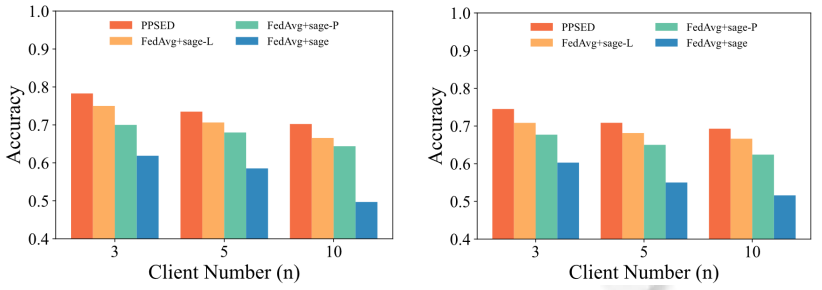
表 6　在数据集 Weibo 上的通信优化实验

p_q	p_c=1		p_c=0.8		p_c=0.5	
	准确率	通信成本(MB)	准确率	通信成本(MB)	准确率	通信成本(MB)
1	0.734 9	12.5	0.718 5	10	0.703 5	7.5
0.7	0.710 3	11.3	0.710 4	8.8	0.675 4	6.3
0.4	0.685 6	8.9	0.670 3	7.6	0.652 8	5.1

实验结果表明, p_c 与 p_q 的值与模型准确率的关系相似. p_c 与 p_q 的值更接近于 1, 也就是所有的客户端都参与到联邦聚合中, 并且不需要量化时, 模型的准确率是最高的, 但通信成本也相应最大. 降低 p_c 与 p_q 的值, 虽然模型准确率有所下降, 但通信成本也相应减小. 这意味着: 在这个实验中, 降低客户端的参与比例可以有效地降低通信成本, 但这同时也会对模型准确率造成一定的影响. 从结果可以看到: 当 p_q=0.7, p_c=0.8 时, 通信成本减少 30%, 准确率只下降了 3.4%; 当 p_c=0.5, p_q=0.4 时, 通信成本降低了 59%, 准确率下降了约 11%. 这个结果表明: 在带宽有限或者通信成本高昂的场景下, 可以通过适当降低客户端的参与比例和增加梯度量化的比例, 来有效地减少通信成本, 尽管这可能会对模型的准确率产生一些影响. 然而, 相比通信成本的大幅降低, 模型准确率的下降在可接受的范围内, 这是一个非常值得考虑的优化策略. 实验结果表明, PPSED 可以有效地通过调节 p_c 与 p_q 的值来平衡模型性能与通信压力.

3.5　消融实验

为了充分验证本文中每个组件的有效性, 在以数据集 Weibo 为例进行消融实验. 实验结果如图 4 所示, 其中, 图 4(a)是参与聚合的客户端比例 p_c 设置为 1 的结果, 图 4(b)是参与聚合的客户端比例 p_c 设置为 0.8 的结果. 从实验结果可以看出, 每个组件的改进都带来了性能的提升, 验证了在实验中使用的每个组件的有效性. FedAvg+sage 是基础全采样方法, 提供了实验的基线性能. FedAvg+sage-P 是在 FedAvg+sage 的基础上添加了 minibatch 机制的图采样方法, 在所有设置下的性能都超过了基础方法. 这表明, minibatch 机制的图采样方法对于性能的提升是有效的. FedAvg+sage-L 在 FedAvg+sage-P 的基础上添加了降维的方法. FedAvg+sage-L 在所有情况下的性能都超过了 FedAvg+sage-P, 这说明降维方法能够有效剔除高维特征中的冗余信息, 保留了更加关键的信息. PPSED 在 FedAvg+sage-L 的基础上添加了强化学习 DDPG, 并在梯度聚合前根据客户端状态评估重要性对梯度进行加权. PPSED 在所有情况下的性能都超过了 FedAvg+sage-L, 这表明强化学习 DDPG 和基于客户端状态的梯度加权策略能够进一步提升模型的性能. 消融实验结果展示了每个组件对于模型性能的重要性. 强化学习 DDPG 和基于客户端状态的梯度加权策略取得了显著的性能提升.



(a) p_c=1 (b) p_c=0.8

图 4 消融实验结果

4 总 结

本文提出了基于强化联邦图神经网络的个性化公共安全突发事件检测方法 PPSED, 此方法解决了在传统全局联邦方法中由于非独立同分布(Non-IID)数据分布和隐私约束所带来的挑战, 通过使客户端能够协同训练个性化且鲁棒的模型, 来处理本地的突发事件检测任务. PPSED 方法包含几种创新的设计策略. 设计了联邦公共安全突发事件检测模型结构与梯度量化方法, 利用基于图采样的 minibatch 机制结合 GraphSage 来构建本地模型, 并且选择客户端梯度进行量化, 减轻 Non-IID 数据的影响, 同时减少梯度通信消耗. 设计了一个基于随机图嵌入的客户端状态感知方法, 以在保证隐私的同时, 更好地保留客户端模型的有价值梯度信息. 设计了强化联邦图神经网络的个性化梯度聚合和量化策略, 以加强联邦图神经网络. 通过采用 DDPG, 拟合个性化的联邦学习梯度聚合加权策略, 并根据权重决定是否对梯度进行量化, 从而在模型性能和通信压力之间找到平衡. 在微博平台收集的公共安全数据集和 3 个其他公开的图数据集上进行了广泛的实验, 结果表明了所提方法的有效性.

References:

[1] Cao Y, Peng H, Wu J, *et al*. Knowledge-preserving incremental social event detection via heterogeneous GNNs. In: Proc. of the Web Conf. 2021. 3383−3395.

[2] Liu Z, Yang Y, Huang Z, *et al*. Event early embedding: Predicting event volume dynamics at early stage. In: Proc. of the 40th Int'l ACM SIGIR Conf. on Research and Development in Information Retrieval. 2017. 997−1000.

[3] Fedoryszak M, Frederick B, Rajaram V, *et al*. Real-time event detection on social data streams. In: Proc. of the 25th ACM SIGKDD Int'l Conf. on Knowledge Discovery & Data Mining. 2019. 2774−2782.

[4] Aggarwal CC, Subbian K. Event detection in social streams. In: Proc. of the 2012 SIAM Int'l Conf. on Data Mining. Society for Industrial and Applied Mathematics, 2012. 624−635.

[5] Peng H, Li J, Song Y, *et al*. Streaming social event detection and evolution discovery in heterogeneous information networks. ACM Trans. on Knowledge Discovery from Data, 2021, 15(5): 1−33.

[6] Cui W, Du J, Wang D, *et al*. Extended search method based on a semantic hashtag graph combining social and conceptual information. World Wide Web, 2019, 22: 2589−2610.

[7] Hamilton W, Ying Z, Leskovec J. Inductive representation learning on large graphs. In: Advances in Neural Information Proccesing Systems, Vol.30. 2017

[8] Kipf TN, Welling M. Semi-supervised classification with graph convolutional networks. arXiv:1609.02907, 2016.

[9] Bo D, Wang X, Liu Y, *et al*. A survey on spectral graph neural networks. arXiv:2302.05631, 2023.

[10] Baek J, Kang M, Hwang SJ. Accurate learning of graph representations with graph multiset pooling. arXiv:2102.11533, 2021.

[11] Wu Z, Pan S, Chen F, *et al*. A comprehensive survey on graph neural networks. IEEE Trans. on Neural Networks and Learning Systems, 2021, 32(1): 4−24.

[12] Perozzi B, Al-Rfou R, Skiena S. DeepWalk: Online learning of social representations. In: Proc. of the 20th ACM SIGKDD Int'l Conf. on Knowledge Discovery and Data Mining. 2014. 701−710.

[13] Grover A, Leskovec J. Node2vec: Scalable feature learning for networks. In: Proc. of the 22nd ACM SIGKDD Int'l Conf. on Knowledge Discovery and Data Mining. 2016. 855−864.

[14] Yang JX, Du JP, Shao YX, *et al*. Construction method of intellectual-property-oriented scientific and technological resources portrait. Ruan Jian Xue Bao/Journal of Software, 2022, 33(4): 1439−1450 (in Chinese with English abstract). https://www.jos.org.cn/1000-9825/6483.htm [doi: 10.13328/j.cnki.jos.006483]

[15] Peng H, Li J, Gong Q, *et al*. Fine-grained event categorization with heterogeneous graph convolutional networks. arXiv:1906.04580, 2019.

[16] Liu J, Ong GP, Chen X. GraphSAGE-based traffic speed forecasting for segment network with sparse data. IEEE Trans. on Intelligent Transportation Systems, 2020, 23(3): 1755−1766.

[17] Bongini P, Bianchini M, Scarselli F. Molecular generative graph neural networks for drug discovery. Neurocomputing, 2021, 450: 242−252.

[18] Chen JS, Meng XW, Ji WY, *et al*. POI recommendation based on multidimensional context-aware graph embedding model. Ruan Jian Xue Bao/Journal of Software, 2020, 31(12): 3700−3715 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/5855.htm [doi: 10.13328/j.cnki.jos.005855]

[19] Shi C, Han X, Song L, *et al*. Deep collaborative filtering with multi-aspect information in heterogeneous networks. IEEE Trans. on Knowledge and Data Engineering, 2019, 33(4): 1413−1425.

[20] Zhang Y, Shi Y, Zhou Z, *et al*. Efficient and secure skyline queries over vertical data federation. IEEE Trans. on Knowledge and Data Engineering, 2022, 35(9): 9269−9280.

[21] Pan X, Tong Y, Xue C, *et al*. Hu-Fu: A data federation system for secure spatial queries. Proc. of the VLDB Endowment, 2022, 15(12): 3582−3585.

[22] Shen X, Dai Q, Chung FL, *et al*. Adversarial deep network embedding for cross-network node classification. Proc. of the AAAI Conf. on Artificial Intelligence, 2020, 34(3): 2991−2999.

[23] Guan Z, Li Y, Xue Z, *et al*. Federated graph neural network for cross-graph node classification. In: Proc. of the 2021 IEEE 7th Int'l Conf. on Cloud Computing and Intelligent Systems (CCIS). IEEE, 2021. 418−422.

[24] Li Q, He B, Song D. Model-contrastive federated learning. In: Proc. of the IEEE/CVF Conf. on Computer Vision and Pattern Recognition. 2021. 10713−10722.

[25] Wang H, Kaplan Z, Niu D, *et al*. Optimizing Federated learning on non-iid data with reinforcement learning. In: Proc. of the IEEE Conf. on Computer Communications (INFOCOM 2020). IEEE, 2020. 1698−1707.

[26] McMahan B, Moore E, Ramage D, *et al*. Communication-efficient learning of deep networks from decentralized data. In: Proc. of the Artificial Intelligence and Statistics. 2017. 1273−1282.

[27] He C, Balasubramanian K, Ceyani E, *et al*. FedGraphNN: A Federated learning system and benchmark for graph neural networks. arXiv:2104.07145, 2021.

[28] He C, Ceyani E, Balasubramanian K, *et al*. SpreadGNN: Serverless multi-task Federated learning for graph neural networks. arXiv:2106.02743, 2021.

[29] Baek J, Jeong W, Jin J, *et al*. Personalized subgraph Federated learning. arXiv:2206.10206, 2022.

[30] Huang Y, Chu L, Zhou Z, *et al*. Personalized cross-silo Federated learning on non-iid data. Proc. of the AAAI Conf. on Artificial Intelligence, 2021, 35(9): 7865−7873.

[31] Schneider J, Vlachos M. Mass personalization of deep learning. arXiv:1909.02803, 2019.

[32] Li T, Sahu AK, Zaheer M, *et al*. Federated optimization in heterogeneous networks. Proc. of the Machine Learning and Systems, 2020, 2: 429−450.

[33] Kober J, Bagnell JA, Peters J. Reinforcement learning in robotics: A survey. The Int'l Journal of Robotics Research, 2013, 32(11): 1238−1274.

[34] Sun Q, Li J, Peng H, *et al*. SUGAR: Subgraph neural network with reinforcement pooling and self-supervised mutual information mechanism. In: Proc. of the Web Conf. 2021. 2081−2091.

[35] Yang M, Li C, Sun F, *et al*. Be relevant, non-redundant, and timely: Deep reinforcement learning for real-time event summarization. Proc. of the AAAI Conf. on Artificial Intelligence, 2020, 34(5): 9410−9417.

[36] Zhou H, Yin H, Zheng H, *et al*. A survey on multi-modal social event detection. Knowledge-based Systems, 2020, 195: 105695.

[37] Allan J. Introduction to Topic Detection and Tracking. Topic Detection and Tracking: Event-based Information Organization. Boston: Springer, 2002. 1−16.

[38] Angel A, Koudas N, Sarkas N, *et al*. Dense subgraph maintenance under streaming edge weight updates for real-time story identification. The VLDB Journal, 2014, 23: 175−199.

[39] Yu W, Li J, Bhuiyan MZA, *et al*. Ring: Real-time emerging anomaly monitoring system over text streams. IEEE Trans. on Big Data, 2017, 5(4): 506−519.

[40] Allan J. Topic Detection and Tracking: Event-based Information Organization. Springer Publishing Company, Incorporated, 2002.

[41] Peng H, Zhang R, Li S, *et al*. Reinforced, incremental and cross-lingual event detection from social messages. IEEE Trans. on Pattern Analysis and Machine Intelligence, 2022, 45(1): 980−998.

[42] Sun M, Zhao S, Gilvary C, *et al*. Graph convolutional networks for computational drug development and discovery. Briefings in Bioinformatics, 2020, 21(3): 919−935.

[43] Rong Y, Bian Y, Xu T, *et al*. Self-supervised graph transformer on large-scale molecular data. In: Advances in Neural Information Proccesing Systems, Vol.33. 2020. 12559−12571.

[44] Xiao ST, Shao YX, Li YW, *et al*. LECF: Recommendation via learnable edge collaborative filtering. Science China Information Sciences, 2022, 65(1): 112101.

[45] Li Y, Yuan Y, Wang Y, *et al*. Distributed multimodal path queries. IEEE Trans. on Knowledge and Data Engineering, 2020, 34(7): 3196−3210.

[46] Veličković P, Cucurull G, Casanova A, *et al*. Graph attention networks. arXiv:1710.10903, 2017.

[47] Li H, Shao Y, Du J, *et al*. An I/O-efficient disk-based graph system for scalable second-order random walk of large graphs. arXiv:2203.16123, 2022.

[48] Dai H, Li H, Tian T, *et al*. Adversarial attack on graph structured data. In: Proc. of the Int'l Conf. on Machine Learning. 2018. 1115−1124.

[49] Chen L, Li JT, Peng QB, *et al*. Understanding structural vulnerability in graph convolutional networks. In: Proc. of the IJCAI. 2021. 2249−2255.

[50] Zhu D, Zhang Z, Cui P, *et al*. Robust graph convolutional networks against adversarial attacks. In: Proc. of the 25th ACM SIGKDD Int'l Conf. on Knowledge Discovery & Data Mining. 2019. 1399−1407.

[51] Li Q, Wen Z, Wu Z, *et al*. A survey on Federated learning systems: Vision, hype and reality for data privacy and protection. IEEE Trans. on Knowledge and Data Engineering, 2021, 35(4): 3347−3366.

[52] Arivazhagan MG, Aggarwal V, Singh AK, *et al*. Federated learning with personalization layers. arXiv:1912.00818, 2019.

[53] Wang B, Li A, Pang M, *et al*. GraphFL: A Federated learning framework for semi-supervised node classification on graphs. In: Proc. of the ICDM IEEE Int'l Conf. on Data Mining. 2022. 498−507.

[54] Scardapane S, Spinelli I, Di Lorenzo P. Distributed training of graph convolutional networks. IEEE Trans. on Signal and Information Processing over Networks, 2020, 7: 87−100.

[55] Wan C, Li Y, Li A, *et al*. BNS-GCN: Efficient full-graph training of graph convolutional networks with partition-parallelism and random boundary node sampling. Proc. of the Machine Learning and Systems, 2022, 4: 673−693.

[56] Yao Y, Jin W, Ravi S, *et al*. FedGCN: Convergence-communication tradeoffs in Federated training of graph convolutional networks. arXiv:2201.12433, 2023.

[57] Zhang K, Yang C, Li X, *et al*. Subgraph Federated learning with missing neighbor generation. In: Advances in Neural Information Proccessing Systems, Vol.34. 2021. 6671−6682.

[58] Watkins CJCH, Dayan P. *Q*-learning. Machine Learning, 1992, 8: 279−292.

[59] Mnih V, Kavukcuoglu K, Silver D, *et al*. Playing atari with deep reinforcement learning. arXiv:1312.5602, 2013.

[60] Sutton RS, McAllester D, Singh S, *et al*. Policy gradient methods for reinforcement learning with function approximation. In: Advances in Neural Information Processing Systems, Vol.12. 1999.1057−1063.

[61] Silver D, Lever G, Heess N, *et al*. Deterministic policy gradient algorithms. In: Proc. of the 31st Int'l Conf. on Machine Learning. 2014. 387−395.

[62] Lillicrap TP, Hunt JJ, Pritzel A, *et al*. Continuous control with deep reinforcement learning. arXiv:1509.02971, 2019.

[63] Banner R, Hubara I, Hoffer E, *et al*. Scalable methods for 8-bit training of neural networks. In: Advances in Neural Information Processing Systems, Vol.31. 2018.

[64] Li Y, Li W, Xue Z. Federated learning with stochastic quantization. Int'l Journal of Intelligent Systems, 2022, 37(12): 11600−11621.

[65] Zhang XX, Zhu ZF, Zhao YW, *et al*. Prototype learning in machine learning: A literature review. Ruan Jian Xue Bao/Journal of Software, 2022, 33(10): 3732−3753 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/6365.htm [doi: 10.13328/j.cnki.jos.006365]

[66] Tan Y, Long G, Liu L, *et al*. FedProto: Federated prototype learning across heterogeneous clients. Proc. of the AAAI Conf. on Artificial Intelligence, 2022, 36(8): 8432−8440.

[67] Abadi M, Chu A, Goodfellow I, *et al*. Deep learning with differential privacy. In: Proc. of the ACM SIGSAC Conf. on Computer and Communications Security. 2016. 308−318.

[68] Xu R, Baracaldo N, Zhou Y, *et al*. HybridAlpha: An efficient approach for privacy-preserving Federated learning. In: Proc. of the ACM Workshop on Artificial Intelligence and Security. 2019. 13−23.

[69] Sen P, Namata G, Bilgic M, *et al*. Collective classification in network data. AI Magazine, 2008, 29(3): 93−106.

[70] Shchur O, Mumme M, Bojchevski A, *et al*. Pitfalls of graph neural network evaluation. arXiv:1811.05868, 2019.

[71] Blondel VD, Guillaume JL, Lambiotte R, *et al*. Fast unfolding of communities in large networks. Journal of Statistical Mechanics: Theory and Experiment, 2008(10): P10008.

附中文参考文献:

[14] 杨佳鑫, 杜军平, 邵蓥侠, 等. 面向知识产权的科技资源画像构建方法. 软件学报, 2022, 33(4): 1439−1450. https://www.jos.org.cn/1000-9825/6483.htm [doi: 10.13328/j.cnki.jos.006483]

[18] 陈劲松, 孟祥武, 纪威宇, 等. 基于多维上下文感知图嵌入模型的兴趣点推荐. 软件学报, 2020, 31(12): 3700−3715. http://www.jos.org.cn/1000-9825/5855.htm [doi: 10.13328/j.cnki.jos.005855]

[65] 张幸幸, 朱振峰, 赵亚威, 等. 机器学习中原型学习研究进展. 软件学报, 2022, 33(10): 3732−3753. http://www.jos.org.cn/1000-9825/6365.htm [doi: 10.13328/j.cnki.jos.006365]

管泽礼(1994−), 男, 博士生, CCF 学生会员, 主要研究领域为联邦学习, 图神经网络.

王沛文(2000−), 男, 硕士生, 主要研究领域为机器学习, 联邦学习.

杜军平(1963−), 女, 教授, CCF 会士, 主要研究领域为人工智能, 机器学习, 模式识别.

潘圳辉(1995−), 男, 博士生, CCF 学生会员, 主要研究领域为机器学习, 联邦学习.

薛哲(1987−), 男, 博士, 副教授, CCF 专业会员, 主要研究领域为机器学习, 人工智能, 数据挖掘, 图像处理.

王晓阳(1960−), 男, 教授, CCF 会士, 主要研究领域为时空移动数据分析, 数据系统安全及私密, 大数据并行式分析.