基于本地差分隐私的分散图学习复现与改进

摘要

图学习通过聚合不同用户的子图以完成不同的学习任务，但子图信息通常包含了用户的隐私，因此在这一过程中保护用户的隐私就变得尤为重要。本文主要是针对基于差分隐私的 GNN 图学习算法 Solitude 进行复现，该算法不仅可以保护用户的隐私，还通过在 GNN 训练过程中校准用户分散图引入的噪声进一步提高了分类准确率，同时保护了用户的节点隐私和边隐私。本文首先对基于差分隐私的图学习背景和相关工作进行介绍，随后介绍本文复现的工作 Solitude，并在此基础上增加了注意力机制，使得 GNN 在图学习过程中可以自动更加关注到重要的节点。最后在 Cora 引文网络数据集上证明复现的准确性以及改进方法的有效性。

关键词：差分隐私；图神经网络；注意力机制；

1 引言

在将分散的社交网络图聚合学习的过程中，用户的个人社交图可能会包含其个人隐私。例如在社交网络中，用户的联系人列表、个人资料信息、喜好或评论等，应该保持隐私，因为大多数用户不愿意向陌生人发布他们的联系人列表。因此在图聚合学习的过程中很可能会侵犯用户的个人隐私。然而，大多数现有的 LDP 技术的图主要集中在图的统计分析，同时保护边或者链接信息的隐私。典型的图统计包括子图计数（例如，三角形和 k 星计数）和图形度量估计（例如，聚类系数、模块性或中心性估计），但它们都不是为 GNN 设计的。因此使用 GNN 学习加噪之后的图是相当具有挑战性的。一般来说，训练具有强差分隐私保证的深度学习模型在实用性方面付出了巨大的代价。具体而言，在图学习的上下文中，图数据通常包含节点特征信息和图结构信息。图结构的组合性质使得隐私学习问题比其他领域更复杂。

在 GNN 中，节点表示可以用于各种下游任务。在训练期间，通过消息传递机制聚合和传播节点信息。在节点分类任务或链接预测任务中，学习模型的训练样本是相互依赖的。相比之下，现有的基于表格数据的 LDP 技术假设每个用户的数据是独立同分布的，这对于相互依赖的图结构数据是不适用的。

虽然使用 GNN 进行隐私图学习仍然是一个新兴的研究课题，但最近的一项研究试图保护图节点特征的隐私。然而，这种方法也引入了一些隐私问题。由于它假设数据管理者拥有全局图结构，如果图的拓扑特征包含敏感信息，由于数据管理者可以直接访问消息传递过程的全局拓扑，那么这种方法很可能会导致信息泄漏。因此在进行隐私图学习任务的过程中，数据管理员不能直接访问图的全局结构，也就是说节点特征和图结构信息都应该受到保护。所

以为了更好地保护隐私，去中心化网络图就逐渐兴起，LDP 应用于社交网络图学习也变得更加合适，本文研究的也是在分散的网络图上使用 GNN 进行本地差分隐私图学习的问题。

2 相关工作

本节将从以下两个部分简要介绍基于本地差分隐私的图学习算法，它们分别是现有图结构中差分隐私的类型和基于 LDP 的图学习算法。

2.1 图结构中差分隐私类型

2.1.1 节点差分隐私

如果一个隐私查询对于每一对图 $G_1 = (V_1, E_1)$ $G_2 = (V_2, E_2)$，都满足差分隐私 $|(V_1 \cup V_2) - (V_1 \cap V_2)| = 1$ $\{(E_1 \cup E_2) - (E_1 \cap E_2)\} = \{(u, v)|u = x \vee v = x\}$，即两个图之间只能相差 1 个节点，$(u, v)$ 表示节点 u 和 v 之间的边，则可以说该隐私查询满足节点隐私。

在节点隐私方面，给定网络图 G 的相邻图 G' 是通过删除或添加节点和与节点相关的所有边得到的图。节点差分隐私试图阻止攻击者确定单个节点 x 是否出现在图中。它保证了个人和关系的隐私保护，而不仅仅是单一关系，代价是严格限制查询和降低准确性结果。差分隐私算法必须隐藏相邻图之间的最坏情况差异，这在节点隐私下可能是实质性的。例如，如果我们考虑一个极端的情况，即一个节点连接到所有其他节点（一个星形图），那么灵敏度就会很高，并且增加的噪声也必须是显著的。一般来说，由于高灵敏度，节点隐私不可能提供高效用（准确的网络分析），但它提供了理想的隐私保护 [3]。

2.1.2 边差分隐私

如果一个隐私查询对于每一对图 $G_1 = (V_1, E_1)$ $G_2 = (V_2, E_2)$，都满足差分隐私 $V_1 = V_2$ $|(E_1 \cup E_2) - (E_1 \cap E_2)| = 1$，则可以说该隐私查询满足边隐私。在边隐私中，给定社会网络 G 的邻接图 G' 是通过从 G 中删除或添加一条边来获得的，它可以推广到允许至多 k 条边被改变。

边隐私保护了用户之间的特定关系，并防止攻击者确定两个人是否相连。与节点隐私相比，边隐私只能对用户之间的关系信息提供保护。尽管这些节点之间的关系受到了保护，度越高的节点对查询结果的影响依然越大。边缘隐私在许多实际应用中提供了有意义的隐私保护，并且比节点隐私得到更广泛的应用 [4]。例如，Kossinets 和 Watts [5] 使用边隐私来保护电子邮件关系。

2.2 基于 LDP 的图学习算法

2.2.1 度分布

度分布是研究最广泛的图特征之一。它反映了图的结构统计，并可能影响图操作的整个过程。度分布可以用来描述基本的社会网络结构、设计图模型和度量图的相似性。通过计算每种度的频率，可以将图的度分布简单地转化为度序列。在这里，我们使用度直方图来描述图中节点的度。

Hay 等人 [3] 将差分隐私的定义应用到图形结构数据中，并基于 [6] 中提出的后处理技术提出了一种差分私有算法，以获得图的度分布的近似。Kasiviswanathan [7] 等人提出了一种精心设计的投影方案，将输入图映射到有界度图，得到节点隐私下原始图的度分布。为了获得低灵敏度的统计信息，将原始网络投影到一组最大程度低于一定阈值的图上。Day 等人 [8] 提出了一种基于边加法的图投影方法，以降低节点隐私条件下图度分布问题的敏感性。这种改进的投影技术比以前的投影技术保留了更多的信息。Ahmed 等人 [9] 提出了一种随机矩阵的社交网络数据发布方法，该方法通过随机投影降低邻接矩阵的维数，实现存储和计算效率的差异隐私。

2.2.2 边权重

在社交网络中，社会关系被建模在具有权重的边上。边缘可以揭示个体之间的不同敏感信息，例如通信成本，两个社交网络用户之间的交互频率，商业交易的价格或两个组织之间的相似性。因此，释放边缘权重必须以隐私保护的方式进行。

Liu 等 [10] 研究了保护边权的隐私性和保护节点间最短路径统计量的效用问题。他们提出了两种边缘隐私保护方法，即贪婪摄动和高斯随机化乘法。前者主要关注于保持被扰动的最短路径的长度，而后者在被扰动前后保持相同的最短路径。Das 等人 [11] 在社交图中进行了边权匿名化。他们开发了一个线性规划模型来保护图的特征，如最短路径、最小生成树和 k-最近邻，它们可以形式化为边权值的线性函数。Li 等人 [12] 将边权序列作为一个非归属直方图，将所有计数相同的桶合并为一组，从而确保了组间 k 值的不可区分性。他们提出了一种方法，增加拉普拉斯噪声，以提高公布数据的准确性和实用性。

3 本文方法

3.1 本文方法概述

本文主要复现的工作是于 2022 年发表在 TIFS 期刊上的论文 “Towards Private Learning on Decentralized Graphs With Local Differential Privacy” [1]。该文章提出了一种新的算法称为 Solitude，主要用于对私有图数据进行 GNN 的差分隐私训练，包括节点特征向量和分散到所有用户中的邻居列表。具体来说，本文的框架分为两个阶段。在第一阶段，数据管理员向每个用户 v_i 发送一次查询，然后每个用户 v_i 独立回应一个结果，但回应的结果会对节点特征向量 x_i 和邻接列表 a_i 进行加噪处理。在第二阶段，数据管理员在由所有用户的混淆数据组成的噪声图上对 GNN 进行训练，在这一过程中会对加噪后的混合图进行噪声校准以提高图学习准确率。下面分别对第一阶段的加噪过程与第二阶段的噪声校准过程进行详细介绍。

3.2 基于 LDP 混淆本地数据

在分散网络图中，每个用户 v_i 持有整个图的一个数据部分，包括他们的特征向量 x_i 和邻接列表 a_i，这两者都是用户私有的，如图 1所示。因此接下来，我们将分别描述用于保护特征向量和邻接列表的隐私机制。

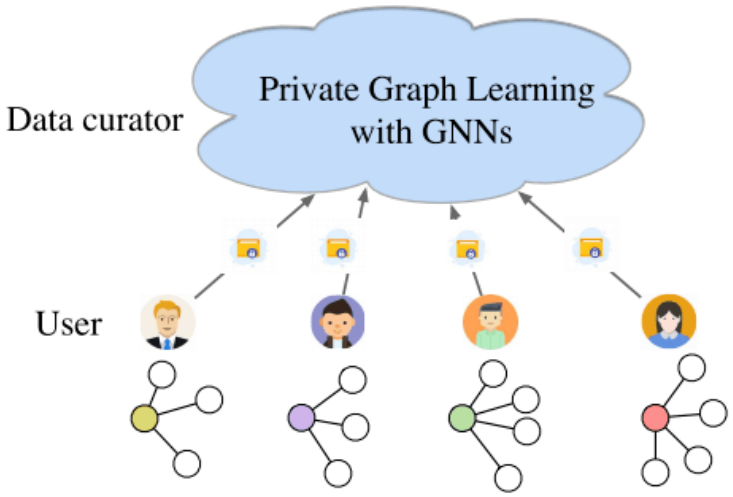

图 1. 分散网络隐私学习示意图

3.2.1 混淆邻接列表

本质上，邻接列表是一个二进制位向量，表示为 $a_i = \{a_{i,1}, \cdots, a_{i,|V|}\}$，其中 $a_{i,j} = 1$ 表示 v_i 和 v_j 之间是相互连接的。一般情况下，我们利用一种十分普遍的方法随机响应来实现本地差分隐私。具体来说，每个用户按照给定隐私预算约束的概率 p 翻转它的邻接列表的每一位。更正式地，假设在给定隐私预算 ϵ_a 的情况下爱，随机邻接列表将表示为 $\tilde{a_i} = \{\tilde{a_{i,1}}, \cdots, \tilde{a_{i,|V|}}\}$，具体关系表达式如下：

$$\tilde{a_{i,j}} = \begin{cases} a_{i,j}, & q = \frac{e^{\varepsilon a}}{1+e^{\varepsilon a}} \\ 1 - a_{i,j}, & p = \frac{1}{1+e^{\varepsilon a}} \end{cases} \tag{1}$$

其中 $q = 1 - p$ 表示邻接列表中保留原有连接关系的概率，p 表示改变原有连接关系的概率。通过理论证明可以得出随机邻接列表机制 M_a 满足 ε_a-边本地差分隐私。

3.2.2 混淆节点特征向量

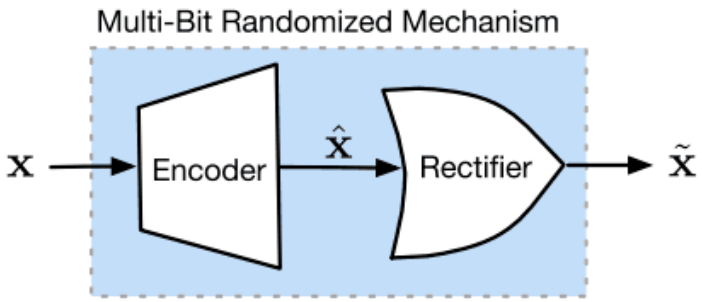

图 2. 多位机制示意图

对于节点特征，本文将利用多位机制 [13] 来保护每个用户的隐私。具体来说，多位机制由两个组成部分：一个编码器和一个校正器，如图 2所示。为了随机化一个特征向量 $x_i \in R^{|D|}$，

其中每个元素 $x_{i,j}$ 都在 $[x_{min}, x_{max}]$ 范围内。编码器首先从 D 维中均匀地采样 m 个特征。每个被选择的特征都被编码成-1 或 1，其概率表示为：

$$P = \frac{1}{e^{\varepsilon_x/m}+1} + \frac{x_{i,j}-x_{min}}{x_{max}-x_{min}} \cdot \frac{e^{\varepsilon_x/m}-1}{e^{\varepsilon_x/m}+1} \tag{2}$$

相应地，其余的 $d-m$ 个特征被映射为 0。校正器是为了校准编码的向量 $\hat{x}$，以确保随机机制 $\tilde{x}$ 的结果在统计上是无偏的。在形式上，校正器被实例化为：

$$Rec(\hat{x_{i,j}}) = \frac{|D| \cdot (x_{max}-x_{min})}{2m} \cdot \frac{e^{\varepsilon_x/m}+1}{e^{\varepsilon_x/m}-1} \cdot \hat{x_{i,j}} + \frac{x_{max}+x_{min}}{2} \tag{3}$$

可以在理论上证明对每一个用户来说，随机机制 M_a 和 M_x 共同满足 $\varepsilon_a + \varepsilon_x$ 的差分隐私。

3.3 隐私 GNN 的校准与训练

现在，通过从所有用户收集的图数据，数据管理员可以重建全局图，同时可以利用消息传递 GNN 进行图分析，为了让图学习更实例化，本文采用节点分类任务进行分析。但是当前收集到的子图都是有噪声的，加噪信息的传递会导致过拟合，从而使泛化能力下降。因此在接下来的内容中，我们将介绍利用图数据的固有属性分别对图结构数据和特征向量数据进行噪声校准之后再利用 GNN 进一步训练，以此提高分类精度，具体过程如图 3所示。

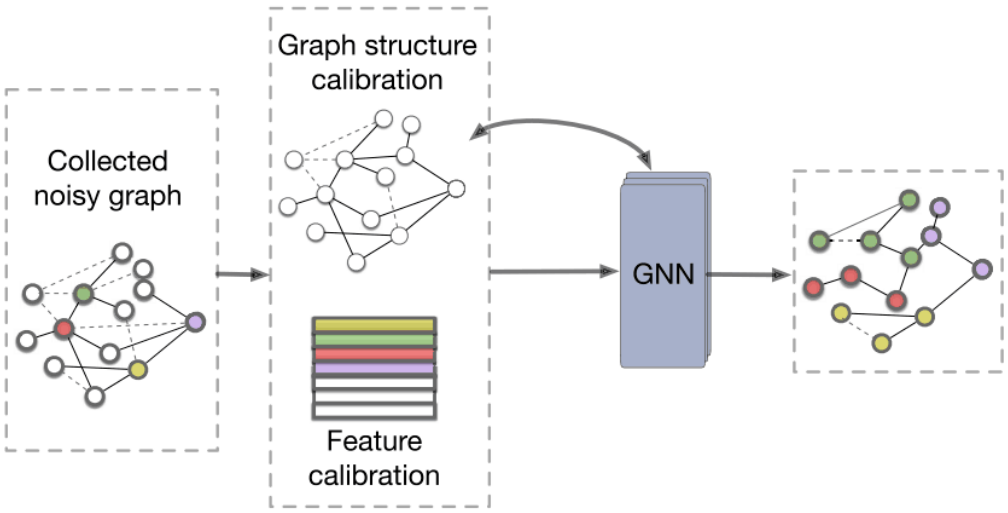

图 3. GNN 隐私学习示意图

3.3.1 图结构去噪

随机翻转引入了“有噪声”的边，这可能会降低 GNN 的泛化性能。这些边倾向于连接不同社区内的节点或具有不同标签的节点，因此应该对它们进行修剪，以获得更好的学习性能。根据上述分析，随机翻转增加了图的密度。因此，我们通过鼓励图结构的稀疏性来校准收集到的噪声图。具体而言，我们通过最小化校准的邻接矩阵的 l_1 范数来校准图结构，记为 $||A^c||_1$。因此，图结构的校准过程可以表述为一个优化问题，优化目标如下：

$$min_{A^c}\|\tilde{A} - A^c\|_F^2 + \lambda\|A^c\|_1 \tag{4}$$

其中，A^c 表示校准后的邻接矩阵，而 λ 控制相关的校准水平。第一个式子是为了确保校准后的矩阵能够尽量接近收集到的真实图拓扑数据，具体来讲，使用 Frobenius 范数来衡量校准矩阵与收集到的矩阵之间的距离。第二个式子利用最小化 l_1 范数距离使得最终的矩阵尽量稀疏。

3.3.2 节点特征向量去噪

在 GNN 中，通常是通过聚合和消息传递来自其邻居的信息来计算一个节点新的信息表示，连接节点的学习表示倾向于相似。换句话说，要使消息传递图神经网络工作，必须保持某种假设，称为平滑假设。这反映了来自不同领域的图形上的真实现象。例如，一个社交图中的两个连接用户很可能共享相似的特征，满足了特征平滑性的特性。然而，在噪声图中，由于非光滑特征聚集，GNN 可能导致节点表示退化，导致 GNN 的学习性能下降。

为了解决上述问题，本文利用了一个特征平滑组件，该组件使用了一个平均聚合器来增强节点特征，通过对来自邻居的节点特征的平均聚合来去噪。具体来说，本文没有使用修正后的特征 $\tilde{x}$，而是通过平均 $l-hop$ 内其邻居的特征向量来细化每个节点的特征。在形式上，$1-hop$ 内的特征平滑过程可以表述为：

$$x_i^c = \sum_{v_j \in N(v_i)} \frac{\tilde{x_j}}{|N(v_i)||N(v_j)|} \tag{5}$$

以上特征平滑组件会执行 l_x 次，这是数据驱动的，因此需要调整以避免过度平滑问题。

这些去噪过程，包括图结构去噪和特征向量去噪，可以看做为更好地学习 GNN 的校准步骤。根据 LDP [14] 的转换不变性，这些过程不会影响隐私保证。换句话说，这些过程的输出仍然是有噪声的，并不反映每个用户的隐私数据部分。同时特征平滑操作还削弱了可能降低 GNN 泛化能力的噪声影响。

我们的最终目标是获得一个具有最佳泛化能力的 GNN 模型，该泛化能力由测试集上的预测精度来衡量。从这个角度来看，我们可以将图结构去噪的过程视为正则化的一种形式，因此，用于模型训练的损失函数可以公式化为：

$$min_{A^c,\theta} L_{GNN}(A^c, X^c, \theta) + \lambda_1\|\tilde{A} - A^c\|_F^2 + \lambda_2\|A^c\|_1 \tag{6}$$

其中 λ_1 和 λ_2 控制正则化比率。求解上式，使用 $Adam$ 的交替优化方案来迭代地更新 θ 和 A^c。

4 复现细节

4.1 与已有开源代码对比

本篇论文的作者公布了算法相应的源代码 [1]，本次复现工作参考了作者发布的源代码，采用了与上述论文相同的数据集，以确保算法复现的准确性。实验结果与原文论文报告中较

为一致。

由于 GNN 图学习过程会根据其相邻的节点来更新自身节点的信息，同时不同节点之间本身也是加噪的。而 GNN 在进行图节点更新过程中，并没有考虑到不同节点的重要性，只是简单的将与主节点相连的节点进行平均聚合。受到注意力机制启发，因此我在 GNN 训练过程中加入了图注意力机制，并且使用多头注意力机制，以此让图学习过程中会自动关注到更重要的节点。具体而言，加入注意力机制后，原来的 GNN 训练聚合相邻的节点过程如下。

首先对于顶点 i，逐个计算它的邻居们（$j \in N_i$）和它自身的相似系数：

$$e_{ij} = a([Wh_i||Wh_j]), j \in N_i \tag{7}$$

其中 W 表示共享参数，主要用于对特征进行增维，将两个节点的特征拼接起来后，通过 $a(\cdot)$ 将拼接后的高维特征映射到一个实数从而得到相似系数。

然后将前面得到的所有节点相似系数进行归一化，简单来说就是通过一层 $softmax$ 函数实现

$$\alpha_{ij} = \frac{exp(LeakyReLU(e_{ij})}{\sum_{k \in N_i} exp(LeakyReLU(e_{ik})} \tag{8}$$

最后根据计算好的注意力系数将特征加权求和，同时为了提高注意力的健壮性，使用多个注意力头进行聚合：

$$h_i' = \sigma(\sum_{j \in N_i} \alpha_{ij} W h_j) \tag{9}$$

$$h_i'(K) = \|_{k=1}^{K} \sigma(\sum_{j \in N_i} \alpha_{ij}^k W^k h_j) \tag{10}$$

而后通过实验验证发现单纯的加入注意力机制效果并不理想，仔细分析结果发现可能是因为数据集中同一类邻居节点对于不同中心节点注意力也会有所区别，因此我又在注意力机制的基础上进一步增加了动态注意力机制 [2]。具体而言，静态注意力指的是对于一组固定的 $keys$(邻居)，如果不同的 $query$ 对这组 $keys$ 求解注意力系数时，得到的注意力系数相对不变，那么这个注意力系数计算函数就是静态的。而动态注意力指的是对于一组固定的 $keys$(邻居)，如果不同的 $query$ 对这组 $keys$ 求解注意力系数，得到的注意力系数会改变，那么这个注意力系数计算函数就是动态的。因此此时求解注意力系数公式应为：

$$e(h_i, h_j) = a^T LeakyReLU(W \cdot [h_i||h_j]), j \in N_i \tag{11}$$

4.2 实验

本次实验采用的实验环境是 Python3.9.18 和 Pytorch2.1.0，接下来将详细介绍实验采用的数据集、基准模型和参数设置。

4.2.1 数据集

本次实验使用是 Cora 这类引文网络数据集，该数据集是节点分类的基准数据集。在 Cora 数据集中，节点代表科学出版物，边对应于引用链接，节点特征包含每个出版物的词袋特征向

量，每个出版物都有一个类别标签。我们将数据集随机分为三部分：50% 用于训练，25% 用于验证，25% 用于测试。其中 LDP 的随机化机制应用于所有训练集，验证集和测试集的节点特征和邻接列表。

4.2.2 模型对比

在原文基础上，我们将改进后的 GAT 和 GATv2 分别在 Solitude 和 Base 两种框架下与 GCN [15] 和 GraphSage [16] 方法进行了比较。GCN 和 GraphSage 是两种具有代表性的图神经网络。通过使用各种 GNN 主干评估我们的方法，我们可以证明 Solitude 能够通过与任何 GNN 合并来保护边缘隐私和节点特征隐私，同时注意力机制在一定程度上可以提高节点分类准确率。

特别地，我们使用相同的随机化机制来混淆特征向量和邻接列表。主要区别在于，基本方法直接在噪声图上训练，没有任何校准过程。该方法假设数据管理员可以访问全局拓扑，并提出了保护节点特征的隐私。虽然基准模型和我们的设置是不同的，为了具有可比性，我们适应基准模型到我们的设置随机邻接表与我们提出的机制，不考虑标签的训练样本作为用户的私人信息。

4.2.3 实验设置

所有 GNN 模型，包括基准和 Solitude 框架的骨干模型，都由两个图卷积层组成，每个层的隐藏维度为 16 并设有一个 SeLU 激活函数。

对于评估指标，我们采用在各种隐私预算下测试集的节点分类准确率来评估学习模型的泛化能力。同时所有实验均进行 5 次以确保统计学显著性，具体而言，我们报告了 5 次运行的平均值。

关于参数设置，我们应用网格搜索来找到最佳选择：在 $[10^{-4}, 10^{-3}, 10^{-2}, 10^{-1}]$ 中调整学习率、dropout rate 和权重衰减。同时我们从 0，2，4，8 中搜索特征平滑步骤 l_x 和标签平滑步骤 l_y，在 $[10^{-5}, 10^{-4}, 10^{-3}, 10^{-2}]$ 选择 λ_1 和 λ_2。我们对所有模型使用了 Adam SGD 优化器。此外，最大 epoch 设置为 200。对于所有 ϵ_a 和 ϵ_x 对，我们遍历了所有参数，以获得其在实验环境中的最佳性能。

4.3 创新点

本次实验的创新点在于，在 GNN 隐私图学习的基础上考虑不同节点之间的重要性。通过对加噪后的节点加入注意力机制，使得 GNN 在图学习过程中可以自动关注对中心节点更加重要的节点，以此提高分类准确率。

5 实验结果分析

为了验证复现算法的准确性，本文在复现阶段，采用的是原论文的数据集进行建模。为了更好地与原文模型进行对比，我们固定了部分参数，验证了在不同隐私预算的条件下模型分类准确率，实验结果见表 1。

表 1. 模型效果对比表

Dataset	**Model**	ε_a	**7.4**	**7.5**	**7.7**	**7.8**	**8.0**	**Inf**
Cora	GCN	Base	65.0	66.5	68.5	68.8	69.3	87.9
		Solitude	**68.8**	**72.8**	**73.4**	**75.6**	**76.2**	**87.8**
	GraphSage	Base	57.6	59.8	60.4	61.4	61.9	88.2
		Solitude	**70.0**	**73.7**	**75.8**	**76.2**	**76.7**	**88.6**
	GAT	Base	66.5	67.7	68.9	69.2	70.5	88.3
		Solitude	**67.9**	**72.7**	**74.4**	**76.1**	**77.1**	**87.7**
	GATv2	Base	64.8	65.9	68.2	68.3	69.9	88.7
		Solitude	**69.1**	**73.2**	**75.9**	**76.9**	**77.5**	**89.1**

由表中的结果，我们可以看到，Solitude 在较低隐私级别（具有较高的隐私预算）下实现了更好的性能。这可以通过以下事实来解释：由于隐私预算的增加，预测变得更加准确。有趣的是，我们还观察到，当节点-隐私预算固定时，Solitude 通过边功能的更高隐私预算实现了更好的性能增益。最大的性能增益在数据集和隐私预算中是不同的。这一结果表明，本文的去噪机制有效地减轻了隐私保护的噪声所造成的过拟合问题，提高了模型的实用性。

同时可以看到加入注意力机制之后的模型在本文的 Solitude 框架下取得了部分提升，但是注意到这种提升当边隐私预算 ε_a 达到 7.5 以上时才较为明显，而当隐私预算较低时，模型效果与基准模型相差不大。分析原因可能是注意力机制会根据邻居的特征与自身的关联计算其重要性，但本文的图数据是加噪过的，会多出部分无关的边，这导致注意力机制会计算到部分本和自己无关的节点，从而降低效果。而隐私预算越低时，加入的噪声就越大，因此注意力起到的效果就越小从而导致效果不显著。

6 总结与展望

本文首先对基于本地差分隐私的图学习算法的背景以及相关工作进行了简要介绍，随后对复现的 Solitude 算法进行了介绍，其中详细阐述了文中提到的基于 LDP 对节点和边加噪以及在 GNN 训练过程中对加噪数据进行校准的方法。随后本文基于 Pytorch 对该算法进行了复现（作者也已提供了源代码）并提出了在原文图学习的基础上加入注意力机制以使模型在聚合邻居节点信息的过程中可以自动关注更重要的节点，最终通过实验结果验证了复现结果的准确性以及改进后算法的有效性。

但从结果可以看出本次提出的改进方案对于模型的性能提升的并不明显，主要体现在隐私预算较低的情况，这种情况下噪声过多会导致对模型得影响过大，因此后续可以结合更多的校准噪声的机制适配注意力机制，使其发挥出更大的效果。同时由于当前图学习的不同隐私形式的固有局限性，本文模型需要一定数量的隐私预算来获得可比较的学习性能，因此未来的工作有许多可能的方向，如建立新的局部微分隐私形式边缘差分隐私等。

参考文献

[1] Wanyu Lin, Baochun Li, and Cong Wang. Towards private learning on decentralized graphs with local differential privacy. *IEEE Transactions on Information Forensics and Security*, 17:2936–2946, 2022.

[2] Shaked Brody, Uri Alon, and Eran Yahav. How attentive are graph attention networks? In *International Conference on Learning Representations*, 2022.

[3] M. Hay, C. Li, G. Miklau, and D. Jensen. Accurate estimation of the degree distribution of private networks. In *2009 Ninth IEEE International Conference on Data Mining*, pages 169–178. IEEE, 2009.

[4] C. Task and C. Clifton. A guide to differential privacy theory in social network analysis. In *2012 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining*, pages 411–417. IEEE, 2012.

[5] G. Kossinets and D. J. Watts. Empirical analysis of an evolving social network. *science*, 311(5757):88–90, 2006.

[6] M. Hay, V. Rastogi, G. Miklau, and D. Suciu. Boosting the accuracy of differentially private histograms through consistency. *Proceedings of the VLDB Endowment*, 3(1-2):1021–1032, 2010.

[7] S. P. Kasiviswanathan, K. Nissim, S. Raskhodnikova, and A. Smith. Analyzing graphs with node differential privacy. In *Theory of Cryptography Conference*, pages 457–476. Springer, 2013.

[8] W.-Y. Day, N. Li, and M. Lyu. Publishing graph degree distribution with node differential privacy. In *Proceedings of the 2016 International Conference on Management of Data*, pages 123–138, 2016.

[9] F. Ahmed, A. X. Liu, and R. Jin. Publishing social network graph eigenspectrum with privacy guarantees. *IEEE Transactions on Network Science and Engineering*, 2019.

[10] L. Liu, J. Wang, J. Liu, and J. Zhang. Privacy preserving in social networks against sensitive edge disclosure. *Technical report, Technical Report CMIDA-HiPSCCS 006-08*, 2008.

[11] S. Das, Ö. Eğecioğlu, and A. El Abbadi. Anonymizing weighted social network graphs. In *2010 IEEE 26th International Conference on Data Engineering (ICDE 2010)*, pages 904–907. IEEE, 2010.

[12] X. Li, J. Yang, Z. Sun, and J. Zhang. Differential privacy for edge weights in social networks. *Security and Communication Networks*, 2017.

[13] S. Sajadmanesh and D. Gatica-Perez, "Locally private graph neural networks," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Nov. 2021.

[14] W.-Y. Day, N. Li, and M. Lyu, "Publishing graph degree distribution with node differential privacy," in *Proc. Int. Conf. Manage. Data*, Jun. 2016.

[15] T. N. Kipf and M. Welling, "Semi-supervised classification with graph convolutional networks," in *Proc. Int. Conf. Mach. Learn. (ICML)*, 2017.

[16] W. Hamilton, Z. Ying, and J. Leskovec, "Inductive representation learning on large graphs," in *Proc. Adv. Neural Inf. Process. Syst. (NeurIPS)*, 2017.