文章编号：2095-2163(2019)01-0028-04 中图分类号：TP309 文献标志码：A

一种基于差分隐私保护的社交网络发布图模型

石秀金，李寒悦
（东华大学 计算机科学与技术学院，上海 201620）

摘 要：针对现有差分隐私保护方法构建噪声时忽略社交网络中数据相关性的不足，提出一种新型的基于差分隐私保护的社交网络发布图模型。利用度分布、最短路径等统计分析方法，通过实验验证了新型的基于差分隐私保护的社交网络发布图模型能够有效地达到保护用户隐私的效果。

关键词：差分隐私保护；社交网络；发布图模型

A social network publishing model based on differential privacy protection

SHI Xiujin, LI Hanyue
(School of Computer Science and Technology, Donghua University, Shanghai 201620, China)

【Abstract】 The new social network publishing graph model, which aims at the differential privacy protection ignoring the lack of data correlation in social network, uses the statistical analysis method such as degree distribution, shortest path to detect this model. This new model is proved to be effective in protecting users´ privacy.

【Key words】 differential privacy protection; social network; publishing models

0 引 言

社交网络分析是一种重要的预测工具，由于社交网络的数据需要通过“发布”来面向大众，往往可以通过深层次的分析获得一些藏匿在已经“发布”信息中的真实知识，甚至包括部分隐私信息。在满足社交网络分析应用的前提下，对隐私数据进行有效的保护是非常必要的。

社交网络图隐私保护技术的研究大多是对于图匿名化的研究[1-3]，这种方法可将一条记录隐藏在一组记录当中，其缺陷是很容易受到去匿名化的攻击，无法真正地达到保护社交网络中的隐私[4-5]。差分隐私机制[6-7]的提出解决了上述方法所遇到的问题，可以达到很好的保护效果，确保数据不会被泄露。本文的主要工作：

(1)将社交网络原始图按照节点分成多个子图，每个子图中边的联系较为紧密，子图之间边的联系较弱；

(2)将分类后的每个子图通过层次随机图模型进行子图区域划分，并在生成树的叶子节点上添加相应的噪声，再构建待发布图；

(3)基于对度发布和聚类系数等攻击者最希望获得的统计数据，通过实验分析，验证了生成的待发布图与原始图的一致性，证明算法是有效的。

1 基本概念

社交网络表示为无向图 G，G 中的每个节点代表社交网络中的用户，每一条边代表 2 个对象之间的联系，如果 2 个节点之间没有边则代表两者没有联系。数学符号表达如下：

图 G：$G(U,E)$，U 是所有节点的集合，E 是所有边的集合；

节点集：$U=\{U_i \mid i=1,2,\cdots,n\}$，其中 n 是节点的个数；

边集：$E=\{(V_i, V_j) \mid i,j=1,2,\cdots,m, i\neq j\}$，若图 G 全连通，m 取最大值 C_n^2。

1.1 层次随机图模型(HRG)

层次随机图模型是基于无向图的。假设：

(1)社交网络 G 是具有 n 个结点的简单无向图；

(2) 树状图 D 是一颗二叉树，由 n 个叶子节点和 $n-1$ 个父节点所组成，n 个叶子节点代表了社交网络中的 n 个用户，每个父节点 r 有 2 个子树；

(3)连接强度 p_r 是父节点 r 的属性，表示在该父节点下，左右子树之间的连接强度，由左右子树之间的边的个数 E_r 除以左右子树的节点个数 L_r 和 R_r 之积得来，公式如下：

作者简介：石秀金 (1976-)，男，博士，副教授，主要研究方向：大数据、隐私保护、移动互联网应用；李寒悦 (1993-)，男，硕士研究生，主要研究方向：隐私保护、大数据。

收稿日期：2018-10-09

$$\bar{p}_r = \frac{E_r}{L_r * R_r} \tag{1}$$

层次随机模型由以上 3 个概念组合而成，是将无向图转化为二叉树的形式，而二叉树的结构是由树中每个父节点的连接强度决定。

1.2　差分隐私保护(DP)

差分隐私的方法是基于“邻居”数据集的概念下发展起来的，邻居数据集指的是和原来的数据集有差别且差别仅为一条记录的数据集。

定义　ε-差分隐私保护：设有随机算法 M，P_M 为算法 M 所有可能输出结构的集合。对于任意两个邻近数据集 D 和 D' 以及 P_M 的任意子集 S_M，若算法 M 满足：

$$P_r[M(D) \in S_M] \leqslant e^{\varepsilon} * P_r[M(D') \in S_M]$$

则算法 M 提供 ε -差分隐私保护，其中，参数 ε 称为隐私保护预算，ε 越小，隐私保护水平越高。

性质　序列组合性：设有算法 M_1，M_2，…，M_n，其隐私保护预算分别为 $\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_n$，那么对于同一数据集 D，由这些算法构成的组合算法 $M(M_1(D), M_2(D), \cdots, M_n(D))$ 提供 $\sum_{i=1}^{n} \varepsilon_i$ - 差分隐私保护，其提供的隐私保护水平为全部预算的总和。

2　CHRG-DP 算法设计

将社交网络图分成若干个内部具有很高关联度的子图，分别用 HRG 模型将每个子图变成一颗二叉树，图中的节点都在二叉树的叶子节点上，并对节点进行噪声添加，将扰动后的每个 HRG 合并形成一个完整的 HRG，最后将经过扰动的完整的 HRG 还原成社交网络发布图发布，可以使社交网络图的噪声添加更为合理，更有效率。

2.1　图分类

首先对社交网络图 G 进行深度优先的搜索，同时计算出图中每个节点完成深度搜索的时间 t，再按照订单完成深度搜索的速度进行排序，对图的逆图也进行深度优先搜索，逆图 *DFS* 得到的森林即为连通区域。

2.2　HRG 生成及加噪

将社交网络图分类成若干个子图后，算法通过随机层次图模型将生成的子图序列中每一个子图转化成对应二叉树，图中的每个节点都分布在二叉树的叶子节点当中，一个原始社交网络图均存在多种 HRG 的方案。当图的规模很大时，无法逐一寻找得到最优 HRG 方案。使用马尔科夫蒙特卡洛方法，可以缩短计算过程。算法随机构建一个 HRG 作为马尔科夫链的初始状态，然后当马尔科夫链未收敛时进行多次循环，每次循环决定了状态转移的顺序。在生成 HRG 时，使用指数机制进行一定程度的隐私保护。生成 HRG(SG,ε) 算法的过程如下：

算法：生成 HRG(SG,ε)

输入：子图(SG)，隐私预算 ε

输出：HRG T’

(1)随机构建一个 HRG 作为马尔科夫链的初始状态；

(2)当马尔科夫链未收敛时；

(3)选择 HRG 中一个节点；

(4)变换 n 的相邻子树后，得到 HRG 方案 T’；

(5)变换概率小于 min 时，接受转变；

(6)返还最优 HRG 方案。

2.3　HRG 合并生成社交网络发布图

算法的第三步，是将添加噪子图的 *HRG* 集合合并成一个完整的 *HRG*，再还原成社交网络的形式生成发布图。满足差分隐私保护模型的目的在于对原始社交网络图添加噪声扰动从而保护数据的安全性和稳定性，所以首先要将子图的 *HRG* 集合合并成一个完整的 *HRG*，并在发布之前，将其还原为复杂图的形式。社交网络发布图生成(G,T) 算法的过程如下：

输入：原始图 G，*HRG* T

输出：社交网络发布图 G’

(1)将原始图中所有节点加入输入结果 G’ 中；

(2) 选择 G’ 中任意两个节点 i 和 j；

(3) 在层次随机图 T 中找出节点 i 和 j 最低祖先节点的概率值；

(4) 根据最低祖先节点的概率值选择是否在 i 和 j 中间添加一条边；

(5) 返还社交网络发布图。

2.4　隐私预算分配

本论文将隐私保护预算值 ε 分成了 3 个部分 $\varepsilon_c, \varepsilon_g, \varepsilon_a$，其中把 ε_c 添加给连接 2 个子图之间的边，ε_g 在生成 *HRG* 图时使用指数机制对边进行差分隐私保护，ε_a 在合并生成 *HRG* 图时进行差分隐私保护。

3　实验结果及分析

算法在 Window10 64 位操作系统中用 Java 语言实现。实验采用了 2 个数据集 Douban 和 Flixster，Douban 是中国在线推荐网站豆瓣，只要用户与用户对于同一话题关注，2 个用户之间就存在一条“边”。

Flixster 是一家美国社交电影网站,当 2 个用户对于同一类的电影感兴趣的时候,2 个用户之间就存在联系。算法选取节点的度分布与图聚类系数,这 2 个攻击者最希望能从社交网络图获取的特征作为指标,通过和传统的差分隐私保护方案 Tr-DP 及基于密度的节点探索和重构方法 DER 算法的对比来检测 CHRG-DP 算法的性能。实验数据集可见表 1。

表 1 实验数据集

Tab. 1 Experimental dataset

Datasets	$\|V\|$	$\|E\|$	Edge density
Douban	327,162	154,908	0.001 06
Flixster	7,918,801	2,523,386	0.001 540

图 1 将 3 种算法在不同的隐私保护预算下对 2 组社交网络数据集的度分布分别进行了计算,以 *KL* 散度作为检测指标,代表隐私保护后的社交网络数据与原始数据之间的分布趋势, *KL* 散度越小表示分布相似性越高。实验结果显示,CHRG-DP 算法不会随着隐私控制参数 ε 进行大幅度改变,无论隐私保护水平如何, *KL* 散度百分比波动很小,都可以达到很好的保护效果。由此可见,CHRG-DP 算法相较于传统的差分隐私,基于密度的重构法有较大的优越性。

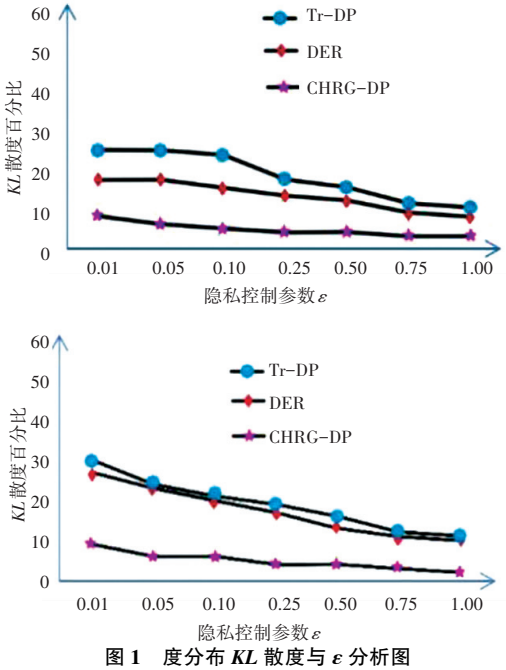

图 1 度分布 *KL* 散度与 ε 分析图

Fig. 1 Degree distribution *KL* divergence and ε analysis chart

图 2 利用平均相对误差指标从聚类系数的角度比较 CHRG-DP、DRG 和 Tr-DP 这 3 种算法的社交网络发布图的可用性。实验结果表明,随隐私保护预算的增加,CHRG-DP 算法的差值呈平稳下降的趋势,并且误差始终是 3 种算法中最小的;在预算值较大的时,CHRG-DP 产生的查询结果准确性较高。此外,Flixster 数据集比 Douban 拥有更多的数据,CHRG-DP 算法在对较大数据集时产生查询结果的准确性依然比较高。

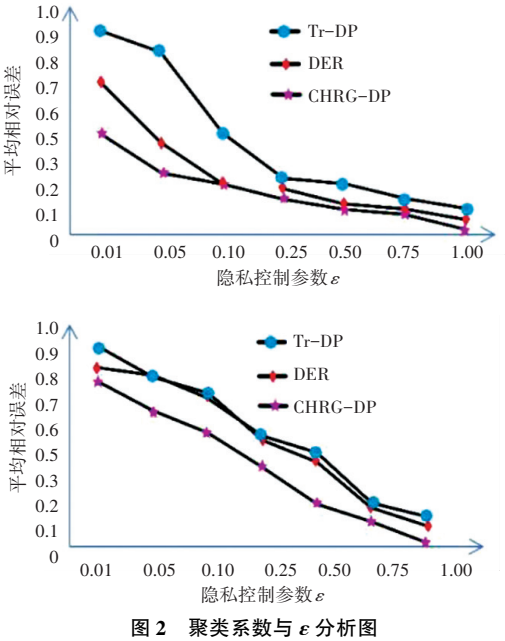

图 2 聚类系数与 ε 分析图

Fig. 2 Clustering coefficient and ε analysis chart

4 结束语

本文从社交网络发布数据的用户隐私保护方向出发,在保证发布图的有用性与原社交网络图的结构一致性的基础上,设计了一种新的算法,主要包含 3 个过程:将社交网络原始图分类成若干个内部关联度较高的子图,再将子图通过层次随机图模型建立最适合的 HRG,合并形成总 HRG,通过 HRG 再还原生成社交网络发布图。最后通过度分布与聚类系数等社交网络最基本的特性指标验证了发布图的有用性,实验结果表明提出的 CHRG-DP 算法比传统的差分隐私保护算法以及基于密度的重构法具有更好保护性和查询准确性。

参考文献

[1] ZOU Lei, CHEN Lei, OZSU M T. K-automorphism: A general framework for privacy preserving network for privacy preserving networks publication [J]. PROCEEDINGS OF THE VLDB ENDOWMENT, 2009, 2(1): 946-957.

[2] WANG Jun, LIU Shubo, LI Yongkai. A review of differential privacy in individual data release [J]. International Journal of Distributed Sensor Networks, 2015, 2015(9): 1.

[3] LIU Kun, TERZI E Towards identity anonymization on graphs [C]//Proceedings of the 2008 ACM SIGMOD international conference on Management of data. Vancouver, Canada: ACM, 2011: 93-106.

(下转第 35 页)