社交网络中的隐私保护方法综述

王方怡、王镇宇、刘明伟

摘　要

近年来，随着社交网络的迅速发展，随之而来的用户隐私泄漏问题也引起了广泛关注。 如何设计一种更好的架构或者算法来保护用户隐私信息成为当前社交网络发展的一个重要问题。 文中主要从社交网络泄漏内容、途径以及防止泄漏的关键方法做了简单介绍，比较归纳了各种隐私保护的原理及特点，并对未来的隐私保护方法进行了展望。

关键词：社交网络、隐私保护、图结构、k-匿名算法

1. 引言

随着互联网技术的不断发展，大量社交网络逐渐兴起，对社交网络的分析已经成为诸多学科的研究热点。Facebook、Twitter、腾讯等公司都维护着庞大的社交网络图，在这些图结构中，用户被表示为带有标签(例如姓名、性别、兴趣、地理位置等)的结点，而用户之间的交互活动可以被抽象为点与点之间连接的边(有向边或者无向边，具体根据交互活动的性质而定)。

然而大量的隐私信息存在于社交网络用户数据中，如医疗诊断结果、个人消费习惯以及其它能够体现个人特征的数据，这些信息会随着数据集的发布和共享而被泄露。文献[1,2]基于真实数据，通过实验证明了社交网络面临很大的隐私攻击和泄露的威胁。

因此，研究社交网络图数据的匿名化发布和管理对实现隐私保护具有重要意义。

2. 社交网络隐私分类

在社交网络中，组成社交网络的各个元素均可能涉及到隐私信息，包括结点、边、图性质等。在本文中，社交网络隐私分类为结点隐私、边隐私、图性质隐私，表 2-1 给出了具体的分类结果。

表 2-1 社交网络中的隐私信息分类

社交网络隐私	结点隐私	结点存在性 结点再识别 结点属性值 结点图结构
	边隐私	边存在性 边再识别 边权重 边属性值
	图性质隐私	

2.1 结点隐私

在社交网络中，每个结点代表了社会中的真实个体，而与结点相关的任何信息均有可能成为隐私。本文将结点隐私具体分类为结点存在性、结点再识别、结点属性值、结点图结构等隐私信息。

1. 结点存在性

所谓结点存在性，是指某个人是否以结点的形式出现在某个社交网络中。在某些情况下，某些人会将自己出现在某特定社交网络视为隐私信息。如果某人将此视为隐私信息，发布数据时应防止攻击者结合背景知识推测出该人存在此社交网络中。例如，传染病传播网络对于研究公共健康和疾病传播途径等方面具有很大价值，然而 在发布传染病传播网络数据的同时，如果攻击者能够推断出某攻击目标存在于此传染病传播网络中。则导致了 该攻击目标隐私信息的泄露。

2. 结点再识别

在发布社交网络数据时，为了保护网络中实体的隐私信息，通常将所有结点的身份信息删除，使得攻击者不能识别和推测出攻击目标在社交网络中的准确位置。但是攻击者可以基于与攻击目标相关的背景知识对社交网络中的结点进行匹配识别，从而准确地或者以一定概率识别攻击目标在社交网络中的位置。在社交网络中，攻击者基于背景知识对攻击目标的位置进行匹配识别的过程称为结点再

识别。

例如，图 2-1 (b)是图 2-1 (a)删除身份信息后的发布数据，如果攻击者掌握了 Ada 的 1。邻居子图(如图 2-1 (c)所示)， 则可以推断出图 2-1 (b)中的结点 6 是 Ada，从而准确地识别出 Ada 在社交网络中的位置，导致 Ada 隐私信息泄露。

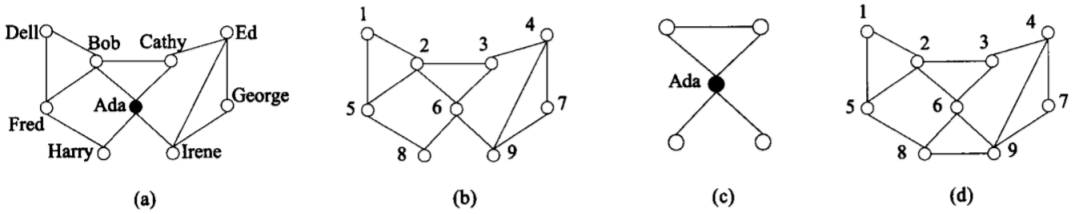

图 2-1 结点邻居图

3. 结点属性值

社交网络中的每个结点具有属性值，这些属性值描述了社会中每个人的真实信息，其中某些属性信息会涉及到个人隐私，例如收入信息、医疗记录中的患病信息等。发布社交网络数据时，结点之间的相互关系使得攻击 者具有更多的背景知识推测目标结点的敏感属性信息。例如在家族遗传病史社交网络中，即使删除了某个重要 结点的疾病信息，但是攻击者还可以基于其亲戚患有遗传疾病的情况，推测该目标结点可能患有的疾病。文献[3]提出采用结点尽匿名的方法来保护结点的敏感属性值，而文献[4 - 7]显示了基于社交网络基本常识即可 准确地推测出大部分结点的敏感属性信息。

4. 结点图结构

不仅结点的某些属性值是敏感的，结点在社交网络中的图结构性质在某些情况下也被视为敏感和隐私，例如结点的度、两个结点间的最短距离、结点到社交网络中某个社区中心的距离等。例如在商品供货网络中，每 个结点的入度和出度分别表示其供货渠道数目和销售渠道的数目，这些信息属于需要保护的敏感信息而防止 其被竞争对手获得。表 2-1 所示了目前尚无相关工作针对保护结点的图结构隐私信息进行深入研究。

2.2 边隐私

社交网络中，一条边表示其两端结点具有某种关系，结点由于相互间具有各种关系从而形成庞大的网络 图。在某些情况下，边相关信息可能是敏感的，例如两点之间是否具有某种关系、参与某种敏感关系的结点信息、 边权重、边的

相关属性等。本文将边隐私具体分类为边存在性、边再识别、边权重、边属性值等隐私信息。

1. 边存在性

所谓边存在性，是指社交网络中的两个指定结点是否具有某种关系。如果某两个结点的边是敏感的，简单地 将此两个目标结点的敏感边删除并不能很好地保护隐私信息，攻击者可以通过背景知识推测两个目标结点是 否具有敏感边。文献[7]假设攻击者采用 noisy-or 概率模型并基于现有结点之间的边连接来计算目标结点间具 有敏感关系的概率，从而对可能被删除的敏感边进行恢复。在文献[8]中，通过实验验证了在真实社交网络数据 上采用链接推演技术可以高概率地预测两个目标结点之间是否具有边连接。

2. 边再识别

对于社交网络中的某条边，识别该边两端结点的过程称为边再识别。在社交网络中，每条边的两端连接着社交网络中的两个结点，表明两个结点所代表的个人具有某种关系，该关系可能被视为敏感信息。例如在异性交友 网络中，两个结点之间的边表示了两个结点所代表的个人曾经具有男女朋友关系，显然，此种关系可能涉及个人隐私。文献[9, 10, 11, 12]研究了如何使边再识别概率小于指定阈值。文献[13]同样将两结点之间的边连接视为隐私信息，并提出技术保证在不得知结点之间边连接情况的同时，较准确地计算任意两点之间的最短路径长度。

3. 边权重

在不同应用背景中，社交网络中的边具有权重。在电子邮件通信网络中，边权重可以表示两个人之间收发电 子邮件数目;在商业网络中，边权重可以表示两个商业公司之间的贸易额。类似商业公司之间的贸易额等边权重 信息可能被视为敏感信息。在文献[14]中，研究了在防止边权重值泄露的同时保持某些重要结点间的最短路径 不变;而文献[15]提出的技术在对边权重提供隐私保护的同时保证线性图性质不变。

4. 边属性值

与结点属性值相似，社交网络中的边也可以具有属性值，例如边上的标签可以表示边两端结点的关系类型。边的敏感属性值对于边的两端结点所代表的个人来说属于隐私信息。文献[16, 17]研究了在社交网络中，如何防 止攻击者基于背景

知识推测出边的敏感属性值。

2.3 图性质隐私

很多图性质是社交网络分析的重要评估标准，例如中间性(结点位于其他结点连接路径上的度)、中心性(结 点与其他结点具有关系的数目)、路径长度(网络中两结点间的最短距离)、可达性(任意结点与其他结点联通的度)等。某些结点的图性质亦被视为个人隐私信息，目前尚无相关工作对结点图性质提供隐私保护。

对社交网络中的隐私信息进行分类归纳意义重大，因为社交网络中，不同类型隐私信息泄露均会威胁到个 人隐私信息安全，只有对社交网络中的隐私信息做好辨识和分类工作，才能对不同隐私信息提出相应保护技术。从表 2-1 可以看出，社交网络中很多方面的隐私信息需要深入研究来为其提供保护。

3. 社交网络隐私保护技术

针对不同背景知识可能导致的隐私泄露，提出了相应的社交网络隐私保护技术。本节分别从隐私保护方法、动态性、并行性等方面介绍当前社交网络隐私保护技术，并指出不同隐私保护技术的优缺点。

表 3-1 给出了当前社交网络隐私保护的具体分类。

表 3-1 社交网络隐私保护技术

隐私保护方法						动态性	并行性
结点 *K*-匿名	子图 *K*-匿名			数据扰乱				
					图结构			
结点聚类	加伪点	加伪边	删除边	概括数值	增、删边	交换端点	推演控制	
√		√						
√								
√								
				√				
					√	√		
√		√		√				
		√	√					√
	√	√						
		√						√
	√	√		√				
		√						
				√				
		√		√				
		√						
		√						
							√	
		√						
√								√

3.1 k-匿名算法

k-匿名方法的出现源自于数据发布中频繁出现的一个问题，即数据可用性与个人隐私泄露风险之间的矛盾。为了便于数据的使用，建立良好的数据挖掘系统，需要满足用户从数据库中发现有价值信息的需求，但是同时又要限制系统能够挖掘出个人隐私的能力。即通过发布出的数据进行挖掘的结果，不能确定某个人（或组织）的身份。进一步说，不能够泄露个人或者组织的信息。

3.1.1 主要思想

k-匿名方法主要对记录的准标识符进行了泛化和压缩处理。将数据集里与攻

击者背景知识相关的属性定义为准标识符，通过对记录的准标识符值进行泛化、压缩处理，使得所有记录被划分到若干个等价类(Equivalence Group)，每个等价类中的记录具有相同的准标识符值，从而实现将一个记录隐藏在一组记录中。因此，这类模型也被称为基于分组的隐私保护模型。

3.1.2 k-匿名算法及其衍生

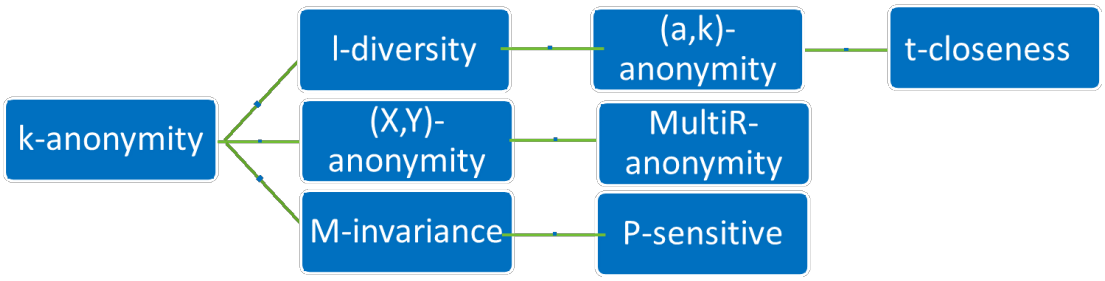

图 3-1 k 匿名方法及其各种衍生

图 3-1 展示了由最初的 K-匿名方法出发，针对于各种不同应用场景，以及 K-匿名方法中存在的某些问题，提出的各种衍生成果。

K-匿名技术是由 Samarati 和 Sweeney 提出的，要求发布的数据中存在一定数量(至少为 K)的在准标识符上不可区分的记录，使攻击者不能判别出隐私信息所属的具体个体，从而保护了个人隐私，在一定程度上保护了个人的隐私，但同时会降低数据的可用性。

l-diversity 由 Machanavajjhala 和 Gehrke 等提出，主要解决了在 K-匿名中，有时划分到同一个等价类的所有记录都有相同的敏感属性，这点会被攻击者利用从而直接获取个体的敏感属性值。方法对每个等价类，即每个 QI-group 做了处理，至少包含一个与同组其他记录不相同的 Well-represented 敏感属性，防止出现全部一样的情况。

(α，k)-匿名由 Wong 和 Li 等提出，主要适用于一些必须要保护某项特定敏感属性的场景，例如在个人资料数据中，每个人是否患病的属性等。该方法主要实在 K-匿名基础上增加了一个参数α，用于控制在每个等价类当中，特定敏感属性值所占的比例，这样可以有效的对身份和属性实现保护。

t-closeness 由 Ninghui Li 和 Tiancheng Li 等提出，主要是为了解决相似攻击，即根据语义相似性关联得到敏感信息的问题。该方法定义了一个参数 t，用于限制每个等价类中敏感属性值的分布与原数据中分布的差别，要求每个 QI-group 中

敏感属性分布与原数据中分布的距离不能大于 t，即接近于原数据。

(X,Y)-匿名由 Ke Wang 和 Fung 等提出，主要是为了解决攻击者从以前发布的数据，和现在发布的数据中获取关系，进行攻击的问题。

Multi-R 匿名由 Nergiz 和 Clifton 等提出，主要是将只针对单关系的 K-匿名拓展到了适用于多关系数据的场景。

M-invariance 由 Xiao 和 Tao 等提出，主要考虑到很多数据不是一次发布就不再更改，而是不断更改多次发布的，在这种情况下，多次发布的数据之间存在的某些联系容易被攻击者所利用，因此采用参数 M 来限制多次发布的数据之间，敏感属性值的变化。

P-sensitive 由 Truta 和 Vinay 等提出，主要解决了 K-匿名方法只能解决身份泄露，而不能解决属性泄露的问题。

3.1.3 性能评价

K-匿名方法是数据发布中一种重要的隐私保护方法，自 1998 年被提出以来，不断在各个方面得到发展和进步，在许多领域得到运用，是被实践证明了的有效方法。

但是匿名化方法还是有不足之处。匿名化隐私保护的一些方法存在的最大缺点是当攻击者拥有大量的背景知识时，通过结合发布的信息进行关联分析，还是容易推断出某个记录的敏感信息. 大数据环境下，为了减少数据共享或发布时无意的数据泄露，数据在传输前应该匿名化，并结合其他技术使接受者对收到数据无法作关联推断，这样既能利用那些数据，又能避免牵扯到具体的个人。

3.2 差分隐私保护算法

差分隐私[18]是 Dwork 在 2006 年针对统计数据库的隐私泄露问题提出的一种新的隐私定义。在此定义下，对数据集的计算处理结果对于具体某个记录的变化是不敏感的，单个记录在数据集中或者不在数据集中，对计算结果的影响微乎其微。所以，一个记录因其加入到数据集中所产生的隐私泄露风险被控制在极小的、可接受的范围内，攻击者无法通过观察计算结果而获取准确的个体信息。

3.2.1 主要特点及思想

差分隐私能够解决传统隐私保护模型的两个缺陷。首先，差分隐私保护模型假设攻击者能够获得除了目标记录外所有其它记录的信息，这些信息的总和可以

理解为攻击者所能掌握的最大背景知识。在这一最大背景知识假设下，差分隐私保护无需考虑攻击者所拥有的任何可能的背景知识，因为这些背景知识不可能提供比最大背景知识更丰富的信息。其次，它建立在坚实的数学基础之上，对隐私保护进行了严格的定义并提供了量化评估方法，使得不同参数处理下的数据集所提供的隐私保护水平具有可比较性，保证任一个体在数据集中或者不在数据集中时，对最终发布的查询结果几乎没有影响。

差分隐私保护要实现的目标是：设有两个几乎完全相同的数据集(两者的区别仅在于一个记录不同)，分别对这两个数据集进行查询访问，使同一查询在两个数据集上产生同一结果的概率的比值接近于 1。

3.2.2 具体概念和机制

差分隐私的定义：设有随机算法 M，P_M为 M 所有可能的输出构成的集合. 对于任意两个邻近数据集 D 和D′以及P_M的任何子集S_M，若算法 M 满足：

$$\Pr[M(D) \in S_M] \leq \exp(\varepsilon) \times \Pr[M(D') \in S_M]$$

则称算法 M 提供ε −差分保护，其中参数ε称为隐私保护预算。图 3-2 直观反映了符合ε −差分隐私的随机算法 M。

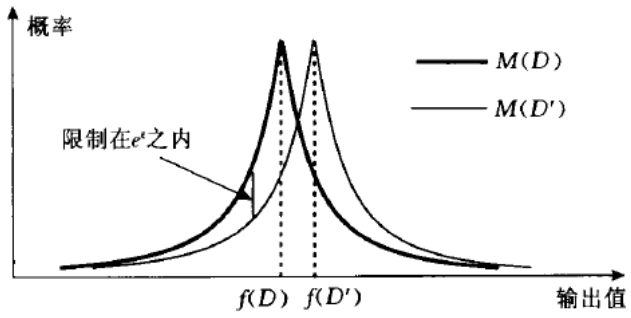

图 3-2 随机算法在临近数据集上的输出概率

差分隐私保护的实现机制主要有两种：Laplace 机制和指数机制。

Laplace 机制[19]：Laplace 机制的原理是向确切的查询结果当中加入一些服从 Laplace 分布的随机噪声，以此来实现差分隐私保护的目的。

给定数据集 D，设有函数 f：D → R^d，其敏感度为Δf，那么随机算法 M(D)=f(D)+Y 提供ε −差分隐私保护，其中y~Lap(Δf/ε)为随机噪声，服从尺度参数为Δf/ε的 Laplace 分布.

从不同参数的 Laplace 分布(如图 3-3)可以看出，e 越小，引入的噪声越大。

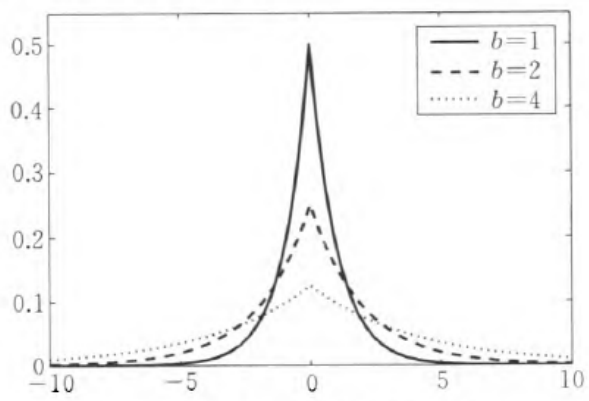

图 3-3 Laplace 概率密度函数

指数机制[20]：指数机制相对于 Laplace 机制的补充主要在于，Laplace 机制仅适用于数值型查询结果，但是在需要查询的是实体对象时，无法处理。

设随机算法 M 输入为数据集 D，输出为一实体对象$r \in Range$，$q(D,r)$为可用性函数，Δq为函数$q(D,r)$的敏感度．若算法 M 以正比于$\exp(\frac{\varepsilon q(D,r)}{2\Delta q})$的概率从 Range 中选择并输出 r，那么算法 M 提供ε－差分隐私保护．

指数机制的应用实例之一，就是在以投票结果作为依据进行决策时，以得票数量为可用性函数，按照指数机制，在给定的隐私保护预算ε下，可以计算出输出概率。

如图 3-4 所示，在举行一场体育比赛时，需要投票来选择比赛项目，根据票数多少进行输出的概率如下。

项目	可用性 $\Delta q=1$	概率		
		$\varepsilon=0$	$\varepsilon=0.1$	$\varepsilon=1$
足球	30	0.25	0.424	0.924
排球	25	0.25	0.330	0.075
篮球	8	0.25	0.141	1.5E-05
网球	2	0.25	0.105	7.7E-07

图 3-4 指数机制应用实例

3.2.3 性能评价

差分隐私是一种严格可证明的安全模型，近年来关于差分隐私保护的研究很多。使其在理论上不断发展和完善，并且在社交网络等领域得到了初步应用。

但是差分隐私还是存在一些难点和不足，需要进一步的研究。

首先，对于复杂数据的处理存在局限。目前的差分隐私保护并没有考虑数据

之间的联系，因此无法有效处理过于复杂，记录之间存在各种联系的数据集。

其次，对连续数据发布的处理能力不足。已有的差分隐私机制大多针对于静态数据发布，但是在实际应用中，很多数据集有动态更新的特点。

3.3 数据扰动算法

3.3.1 主要思想

数据扰乱技术是主要的隐私保护基础技术之一，它通过一定的隐私策略，对原始数据进行修改，使数据挖掘的一方无法从最终发表的数据中提取出原始数据信息或隐私的统计规则，达到保护隐私的目的。

数据扰乱的思路主要有：对数据添加一定的噪声，使得无法从单个数据中恢复出原始数据。通过对社交网络图进行随机化修改，使得攻击者不能准确推测出原始真实数据，从而起到保护社交网络数据隐私的作用。

3.3.2 常用方法

数据扰动常用的方法有两种，一种是数值扰动，另一种是图结构扰动。

数值扰动：通过对数值信息进行随机化的扰乱和修改，可以使得攻击者不能猜测出原始真实数值。但是在数值扰动的过程中，必须注意的重点在于，扰乱之后，结点间最短路径序列不能改变，否则图的可用性会受到影响。

图结构扰动：通过随机进行图数据扰乱和修改，可以阻止攻击者获知原始图结构，主要方法是随机添加、删除边和交换边端点等。在进行图结构扰动时，需要注意的是：（1）图的邻接矩阵最大特征值γ不能变；（2）图的拉普拉斯矩阵最小特征值μ不能改变。

常用的两种思路是基于贪心的扰动和高斯随机乘法扰动。

基于贪心的扰动[21]：在运用扰动策略时，并不是所有的最短路径的节点及权重都是重要的。仅需要在数据拥有者的限制范围内，以社交网络最短路径和相应长度在扰动前与被扰动后的差异在预先规定的范围之内，来达到使边权重的隐私得到保护的目的。基本方法是将图中的边，按照被最短路径序列经过的次数分为全次边、零次边和缺次边，然后分别做不同的处理。

图 3-5 展示了一个图中三种不同权重类别的边。其中，粗实线代表部分被访问的缺次边，细实线代表从未被访问的缺次边，虚线代表全次边。

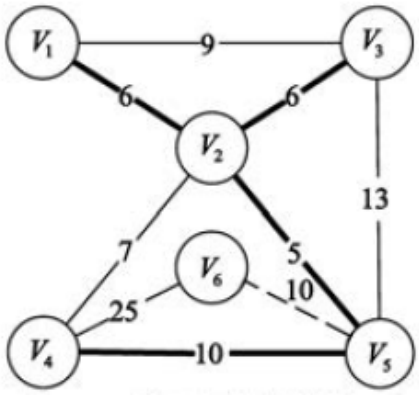

图 3-5 三种不同类别的权重

高斯随机乘法扰动[21]的基本思想是：把每两个相关联的实体与一组满足高斯分布的随机数相乘，即两实体间的边权重乘以一个随机数，同时公开个人的扰乱权重。因为每条边的随机数与边的权重扰乱，仅与这条边所连接的 2 个实体及该组的随机数有关，与其它边无关，即所有边的权重都可以在分布的环境下进行扰乱，并且每个权重的最大增减幅度只与该分布环境的参数有关，所以如果能合理地选择高斯分布的各个参数，就可以保存最短路径及其对应的长度。

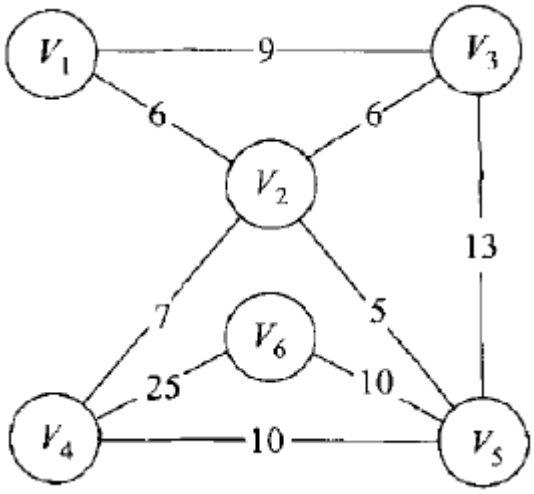

图 3-6 高斯乘法扰动之前的图

如图 3-6，在扰动之前，图中存在三条最短路径。分别是：

$P_{1,6} = \{V_1 \to V_2 \to V_5 \to V_6\},\ d_{1,6} = 21$

$P_{3,6} = \{V_3 \to V_2 \to V_5 \to V_6\},\ d_{3,6} = 21$

$P_{4,6} = \{V_4 \to V_5 \to V_6\},\ d_{4,6} = 20$

进行扰动后，变为下图 3-7，三条最短路径均无变化。

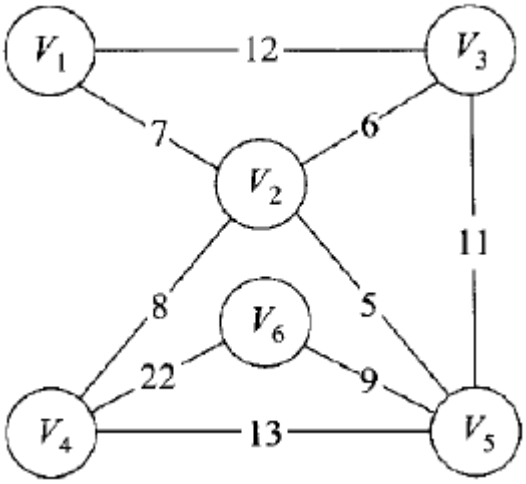

图 3-7 高斯乘法扰动以后的图

3.3.3 性能评价

数据扰动方法是解决社交网络图隐私的重要方法，也被很多实际场景证明了可用性，但是仍然存在不足之处和需要发展的方面。

首先，数据扰乱可能会影响整个社交网络图的某些性质，导致数据可用性变差；其次，很多数据扰动方法无法对扰动效果进行量化，虽然在某些方面做到了对外来攻击的防御，但是依然存在隐私泄漏的风险。另外，还有扰动代价高等问题。

该领域的进一步发展，主要集中于对于动态变化、更新频繁的网络场景的支持，以及对于扰动效果的量化评估等方面。

4. 挑战

如今匿名化方法对用户隐私保护的可靠性很难评估，因此研究者们设计了不同的方法对图进行去匿名化，验证社交网络供商对社交数据进行匿名保护的有效性。

在下图4-1中，左边的图是通过爬虫获得的，称为匿名网络，带有用户的公开信息；而右边的图是运营商发布的，称为辅助网络，隐藏了用户的身份信息，但是又有一些其他信息（如地址）。去匿名是指通过辅助网络 数据找出匿名网络数据中匿名数据的原始信息。

若将匿名网络或辅助网络视为含有若干节点 (用户)的有向图:G=(V，L)，其中集合V表示 图节点集合，L表示节点之间连接边的集合(用户 之间的好友/粉丝关系)，那么我们去匿名的目标 转化为:找出匿名图Gs和辅助图Gt中节点的映射关 系σ: Gs→Gt。对于节点p∈Vs，q∈Vt，如果p，q匹 配，则σ(p,q)= 1，否则σ(p,q) =0。我们的目标是最大程度地找出两个网络中匹配节点p和q的集合。

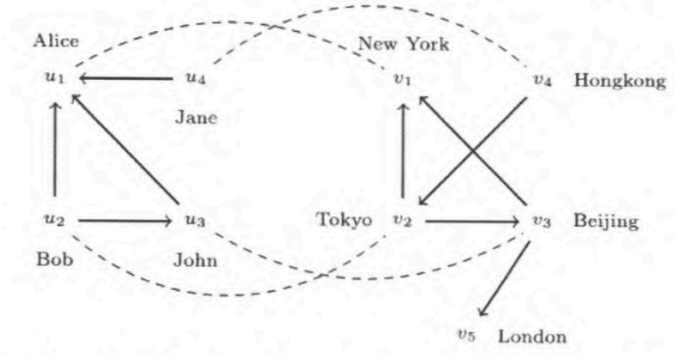

图 4-1 **匿名网络**

早期的去匿名化方法或者需要高质量的种子匹配，对种子的可靠性非常依赖，在实际操作中往往匹配错误率较高，在精确度上和效率上颇有不足。针对当前去匿名算法的不足，文献[22]提出了一种高效高精度的无种子去匿名化算法RoleMatch，不需要初始的正确种子对，只基于图的结构信息.具体来说，只是利用图的拓扑结构信息，将每个可能点对的匹配程度用一个数值进行抽象，从而完成了从复杂多维空间到简单一维空间的有效映射，便于进行比较判断，解决了图结构信息多而杂的问题。实验部分利用 LiveJournal 的数据，证明了 Rolematch 在算法上的优越性。

文献[23]提出了一种基于随机森林分类器的社交网络去匿名化方案，将去匿名

化问题转化为辅助网络与匿名网络之间的结点匹配问题，将网络结构特征作为结点特征向量训练分类器。主要研究思路是，首先，分别从匿名网络和辅助网络中找 出其网络节点的特征，包括节点度、聚类系数、特征向量的中心性等，并将这些特征组合为节点的特 征向量，然后将匿名网络和辅助网络节点间的匹配 问题视为二分类问题，最后采用随机森林分类器根据节点的特征向量进行评估分类，判定两个节点是否属于同一节点。其中用到的网络结构特征参数有度中心性、中介中心性、接近中心性以及特征向量中心性特征。

实验部分，我们使用 MAG 数据集的辅助图识别匿名图，实现识别出匿名网络中作者的信息，在 0.7%的假阳率情况下，算法 实现了去匿名 84%的节点，相对于其他方案较优，在 0.5%假阳性率的情况下仍能实现 81%的社交网络节点去匿名化效果。

其他关于去匿名化办法的研究也是从不同的匹配度量方法入手，例如文献[24]提出了一种新的去匿名攻击方法。作者首先设计了一个基于统一相似度(US)测量的去匿名化框架，并在此基础上推出了自适应去匿名化 (ADA)框架。实验结果表明，该框架对噪声非常有效且鲁棒。

以上研究表明目前数据挖掘技术的发展与算法的改进，对社交网络图数据发布和管理过程中的隐私保护带来更大挑战。

5. 未来研究趋势

社交网络隐私保护是一个新兴的研究方向，尚有许多值得深入探索的问题。在本文的最后。我们基于大量的 调研和近几年来的研究经验，提出一些值得进一步挖掘的研究点，希望对本领域的其他研究者有所启发。

1. 深入研究并行化社交网络隐私保护技术

当前，基于单工作站的社交网络分析和隐私保护技术不适合海量社交网络数据，例如，对于 Facebook 这种用户数目达到上亿级别的社交网络，单工作站的社交网络算法的执行效率、数据处理能力均不能满足实际应用需求。因此，有必要研究并行化社交网络隐私保护技术。基于网络和并行计算思想的云计算技术使得进行社交网络海量数据的并行化分析和隐私保护成为了可能，例如，文献[25]初步尝试了云环境中的社交网络隐私保护研究。可以从两方面深入研究并行化社交网络隐私保护技术:1. 隐私保护的并行化社交网络分析 2. 并行化社会网络隐私保护算法。对于隐私保护的并行化社交网络分析，侧重研究并行化社交网络分析中如何防止隐私泄露;对于并行化社交网络隐私保护算法，侧重研究如何将现有的隐私保护技术和模型移植到并行计算环境中。不论对于哪种研究方向，并行化社交网络隐私保护技术都会面临无法载入海量数据、基于分割的图数据无法得到正确结果、数据处理效率非常低等诸多困难，需要深入研究并解决相应难点，实现社交网络隐私保护的并行化计算。

2. 支持丰富数据应用的社交网络隐私保护

如前所述，在当前社交网络隐私保护研究中，并未指定发布数据的用途，而现实中发布的社交网络数据常被用于各种特定用途，例如进行社区中心发现、链接挖掘、可达性计算等。以前的研究工作并未基于数据发布用 途来设计相应的隐私保护方法，而只是设计了通用的隐私保护方法，影响了发布数据的可用性。因此，有必要基 于发布数据的用途实现社交网络隐私保护的定制化，从而提高发布数据的可用性。例如，文献[26]研究了保持图 社区结构的图匿名化技术，开启了支持指定数据应用的社交网络隐私保护研究。图匿名过程包含了边添加和删除等操作，会对结点之间的可达性造成影响。如何在实现图匿名的同时减少结点间可达性的影响，是一个挑战性问题。

3. 阻止社交网络预测模型导致的隐私泄露

目前只有文献[27]研究了如何阻止基于预测模型推演获得隐私信息。因此，有必要研究防范不同社交网络预测模型的隐私保护技术。例如，文献[40]仅研究了如何防范基于相似度的敏感链接推演攻击，没有对最大似然链接推演攻击和概率模型链接推演攻击给出隐私保护方法。隐私推演模型的复杂性和图中结点、边之间的高度相关性，对研究相应的隐私保护技术提出了挑战。

4. 社交网络隐私保护模型亟待多样化

当前，社交网络隐私保护技术基本采用尽匿名、数据扰乱和推演控制等隐私保护思想。由于隐私保护模型 和方法缺乏多样性，从而导致隐私泄露威胁大、数据可用性低等缺点，亟待提出多样化的社交网络隐私保护模 型。例如，相关工作已初步尝试将关系数据中的差分隐私移植到社交网络隐私保护[29, 30]。然而，结点间的高度 相关性以及大数据规模会导致图数据差分隐私的高复杂度，如何降低图差分隐私复杂度是一个挑战性问题。

6. 总结

本文以社交网络的重要性、复杂性作为出发点，讲述了社交网络当中隐私保护的意义，和对于保护算法进行归纳综述的必要性。

在论文主体部分中，概述了社交网络数据隐私保护的主要算法以及发展历程，描述了各种保护算法的原理、创新点、适用场景以及性能分析。对于常用的隐私保护算法作了对比和总结，并分析了所面临的挑战。最后对隐私保护未来研究趋势进行了展望。

参考文献

[1] Samarati P，Sweeney L.Generalizing data to provide anonymity when disclosing information. In:Proe.ofthe 7th ACM SIGACT. SIGMOD—SIGART Symp.on Principles of Database Systems.1998.188-202.

[2] SweeneyL.K-Anonymity:Amodelforprotectingprivacy.Int'lJournalonUncertainty, Fuzziness and Knowledge — Based System,2002,lO(5):557—570.

[3] Campan A，Truta TM.A clustering approach for data and structural anonymity in social networks.In:Proc.of the 2nd ACM SIGKDD Works hop on Privacy，Security，andTrustinKDD.2008.33-54.

[4] ZhelevaE,GetoorL.Tojoinornottojoin:Theillusionofprivacyinsocialnetworkswithmixedpublicandprivateuser profiles. In: Proc. of the 18th Int'l Cone on World Wide Web.2009.531-540.

[5] Xu W，Zhou X，Li L. Inferring privacy information via social relations. In: Proc.of the 24th Int'l Cone on Data Engineering Workshop.2008.525—530.

[6] HeJ，Chu ww，Liuz. Inferring privacy information from social networks. In: Proc. of the Intelligence and Security Informatics.2006.154—165.

[7] GetoorL.Preservingtheprivacyofsensitiverelationshipsingraphdata.In:Proc.ofthe1stACMSIGKDDWorkshop on Privacy, Security,andTrustinKDD.2007.153-171.

[8] Liu X，Yang X. Protecting sensitive relationships against inference attacks in social networks. In: Proc. of the l7tll Int'l Cone on Database Systems for Advanced Applications.2012.335—350.

[9] CormodeG,SrivastavaD,Yu,TZhangQ.Anonymizingbipartitegraphdatausingsafegroupings.In:Proc.of the 34nd Int'l Cone on Very Large Databases. ACMPress，2008.833-844.

[10] BhagatS ， CormodeG ， KrishnamurthyB, SrivastavaD.Class Based graph anonymization for social network data. In: Proc.of the 35th Int'l Cone on Very Large Databases.2009.766-777.

[11] Yuan M，Chen L，Yu PS. Personalized privacy protection in social networks. In:Proc.of the 36th Int'l Conf.on Very Large Databases.2010.14l—150.

[12] TaiCH，YuPS，YangDN，ChenMS.Privacy-Preserving social network publication against friendship attacks. In:Proc.ofthe 17th

[13] ACM SIGKDDInt'1Cone on Knowledge Discovery and DataMining.2011.1262-1270.

[14] Gao J，Xu JY，Jin R，Zhou J，Wang T，Yang D. Neighborhood Privacy protected shortest distance computing in cloud. In: Proc.of the2011 ACMSIGMODInt'1ConeonManagementofData.2011.409-420.

[15] Das S， Egecioglu O， Abbadi AE.Anonymizing weighted social network graphs.In:Proc.of the 26th Int'l Cone on Data Engineering.2010.904—907.

[16] ZhelevaE, GetoorL.Preservingtheprivacyofsensitiverelationshipsingraphdata.In:Proc.ofthe1stACMSIGKDDWorkshop on Privacy，Security，and Trustin KDD.2007.153-171.

[17] Campan A，Truta TM.A clustering approach for data and structural anonymity in social networks. In:Proc.of the 2nd.

[18] Dwork C．Differential privacy：A survey of results Proceedings of the 5th International Conference on Theory and Applications of Models of Computation．Xi'an，China，2008：1—19

[19] Dwork C．McSherry F．Nissim K，Smith A．Calibrating noise to sensitivity in private data anaIysis Proceedings of the 3rd Conference on Theory of Cryptography．New York，USA，2006：265-284

[20] McSherry F．Talwar K．Mechanism design via differential privacy, Proceedings of the 48th Annual IEEE Symposium on Foundations of Computer Science．Providence，Rhode Island，USA，2007：94—10.

[21] 刘华玲，郑建国，孙辞海，基于贪心扰动的社交网络隐私保护研究[J]

[22] Liu，ShiSY，Zhang YM，Shao YX，Cui B.Effective and efficient approach for graph de·anonymization.Ruan Jian Xue Bao/Journal ofSoftware，2018，29(3):772-785(in Chinese).http://www.jos.org.cn/1000·9825/5436.html

[23] Classifier-based De-anonymization Method for Social Networks HU Guangwu1, ZHANG Pingan1, MA Jiangtao2,3

[24] Structure based Data De-anonymization of Social Networks and Mobility Traces

[25] Shouling Ji1, Weiqing Li1, Mudhakar Srivatsa2, Jing S. He3, and Raheem Beyah1

[26] Gao J，Xu JY，Jin R，Zhou J，Wang T，Yang D. Neighborhood Privacy protected shortest distance computing in cloud. In:Proc.of the2011 ACMSIGMODInt'1Coneon Management of Data.2011.409-420.

[27] Wang Y，Xie L，Zheng B，Lee KCK.Utitily-Oritented k-anonymization on social networks.In:Proc.of the 16th Int'l Cone on Database Systems for Advanced Applications.201 1.78—92.

[28] Liu X，Yang X.Protecting sensitive relationships against inference attacks in social networks. In: Proc. of the l7tll Int'l Cone on Database Systems for Advanced Applications.2012.335—350.

[29] Karwa V，Sofya R，Smith A，Yaroslavtsev G. Private analysis of graph structure. In: Proc. of the 37th Int'l Cone on Very Large Databases.20l 1.1 147-l 157.

[30] Chen S，Zhou S. Recursive mechanism: Towards node differential privacy and unrestricted joins. In: Proc. Of the 2013 Int'l Cone on Management of Data.2013.653—664.