◎热点与综述◎

社交网络中用户隐私推理与保护研究综述

朴杨鹤然,崔晓晖
武汉大学 国家网络安全学院,武汉 430072

摘 要:如今微博和Twitter等社交网络平台被广泛地用于交流、创建在线社区并进行社交活动。用户所发布的内容可以被推理出大量隐私信息,这导致社交网络中针对用户的隐私推理技术的兴起。利用用户的文本内容及在线行为等知识可以对用户进行推理攻击,社交关系推理和属性推理是对社交网络用户隐私的两种基本攻击。针对推理攻击保护机制和方法的研究也在日益增加,对隐私推理和保护技术相关的研究和文献进行了分类并总结,最后进行了探讨和展望。

关键词:社交网络;推理攻击;隐私保护;机器学习
文献标志码:A **中图分类号:**TP391 doi:10.3778/j.issn.1002-8331.2005-0361

朴杨鹤然,崔晓晖.社交网络中用户隐私推理与保护研究综述.计算机工程与应用,2020,56(19):1-12.
PIAO Yangheran, CUI Xiaohui. Review on user privacy inference and protection in social networks. Computer Engineering and Applications, 2020, 56(19):1-12.

Review on User Privacy Inference and Protection in Social Networks

PIAO Yangheran, CUI Xiaohui
School of Cyber Science and Engineering, Wuhan University, Wuhan 430072, China

Abstract: Nowadays, social network platforms such as Weibo and Twitter are widely used to communicate, create online communities, and conduct social activities. The content posted by users can be inferred from a large amount of privacy information, which has led to the rise of privacy inference technology for users in social networks. By using knowledge such as the user's text content and online behaviors, inference attacks can be performed on users. Social relationship inference and attribute inference are two basic attacks on social network user privacy. The research on the mechanism and method of inference attack protection is also increasing, this paper classifies and summarizes the research and literature related to privacy inference and protection technology. Finally, it discusses and prospects the privacy inference and protection in social networks.

Key words: social networks; inference attacks; privacy protection; machine learning

1 引言

社交网络为人们在全球范围内的交流和互动提供了一种简便的平台。世界各地的用户都在使用社交网络共享信息,并通过互联网与其他人建立联系[1]。在社交网络上,用户可以与他们现实中认识或不认识的人进行交流,或者找到在政治、经济、音乐或体育方面具有相同兴趣或倾向的人。广告公司可以在社交媒体上宣传他们的产品,并在短时间内获得更多欢迎[2]。

Twitter、Facebook和其他社交媒体鼓励用户在平台上表达其思想、观点和生活中的一些细节[3]。从重大事件到看似无用的评论,都包含在其发布的推文、状态和在线互动中。大多数消息包含的信息价值很小,但是数百万条消息的聚集会产生重要的知识。例如,由于机器学习和深度学习技术的兴起,用户帖子和在线社交互动

基金项目:国家重点研发计划项目(No.2018YFC1604000);中央高校基本科研业务费专项基金(No.2042017gf0035)。
作者简介:朴杨鹤然(1995—),男,硕士研究生,研究领域为网络攻防、隐私安全;崔晓晖(1971—),通信作者,男,博士,教授,博士生导师,CCF会员,主要研究方向为大数据安全,E-mail:xcui@whu.edu.cn。
收稿日期:2020-05-26 **修回日期:**2020-07-02 **文章编号:**1002-8331(2020)19-0001-12
CNKI**网络出版:**2020-09-07, https://kns.cnki.net/kcms/detail/11.2127.TP.20200904.1358.004.html

可用于准确推理出许多用户角色属性、性别、种族、年龄、政治兴趣和位置等[4-7]。

据报道,诸如联合健康集团之类的医疗保健提供者会挖掘社交媒体数据以及其他临床信息,以评估医疗保健风险和保险费。企业也越来越多地使用社交媒体在招聘前筛选候选人[8]。FBI等政府机构现在也在社交平台上监视用户发布的内容。

2 简介

2.1 社交网络

在线社交网络平台已成为现代社会人们生活中不可或缺的一部分,这些企业已经获得了大量用户。截至2020年1月,Facebook已拥有24亿用户,排在所有社交网络应用的第一位。社交网络具有消息即时传递、信息共享以及为用户发布评论的优点[9]。

最初,人们主要使用社交网络来表达他们的一些想法。随着时间的流逝,在线活动变得越来越复杂和多样化。社交网络的蓬勃发展带来了大量用户生成的内容,有66%的用户推文是关于用户他们自己的,其中大部分是免费且可公开获得的[10]。

此外,越来越多的用户加入基于位置的社交网络(Location-Based Social Network,LBSN)以享受不同的位置相关服务,例如朋友查找、兴趣位置搜索、签到、带有地理标签的照片共享等[11]。位置信息不仅代表了个人的地理位置,而且还透露了他们的生活习惯、生活方式以及个人信息,这些导致用户面临较高的隐私风险。

在社交网络中,用户总是希望共享某些信息以获取收益,而将其他信息则隐藏起来以保护隐私。不幸的是,随着机器学习的飞速发展,各种强大的推理攻击可能会推测出其隐藏的信息[12]。

2.2 隐私推理

用户留存在社交网络平台上的好友互动记录、兴趣爱好标签、签到信息、消费记录等包含了大量社交关系信息和属性信息,为定向广告、推荐系统等应用提供了丰富的数据来源。用户的需求、喜好、属性、行为以及可能具有的关系等,被用于尽可能详细地构造用户个人画像[13]。随着社交平台的发展,能够用于确定用户真实身份的信息也越来越多,用户隐私泄露的隐忧也日益严重。社交网络中的隐私推理是用户隐私泄露的一种,即根据用户帖子内容、用户之间的关联和网络互动等公开信息,来对用户社会关系、敏感用户属性进行推理[14]。

进行隐私推理的攻击者可以是对用户隐私感兴趣的任何一方,例如可能是网络犯罪分子、社交网络提供商、广告商、数据经纪人或监视机构[15]。网络犯罪分子可以利用用户隐私信息进行有针对性的社会工程攻击;社交网络提供商和广告商可以根据用户数据用于定向目标广告;数据经纪人可以将用户信息出售给广告商、银行公司和保险业等其他方来获利;监视机构可以使用这些信息来识别用户并监视他们的活动[16]。

2.3 推理攻击分类

根据攻击的目的,即想要获得到的用户隐私信息,现有的推理攻击按攻击目的大致可分为两类:针对属性的推理和针对社交关系的推理。属性推理中,针对地理位置的推理又是领域内的一大研究重点,因此在本文中单独分类介绍。

针对属性的推理可以按技术和所利用的不同类型数据分为基于内容、基于社交链接和基于用户行为等几类属性推理方法;针对地理位置的推理包括基于社交图和基于社交行为等方法;而针对社交关系的推理则主要分为基于位置和基于主题标签两种方法[17]。

3 针对属性的推理攻击

3.1 敏感属性定义

用户属性存在类似二分类的概念,可以被分为两类:公开属性和私人敏感属性,用户应确定其属性属于何种类别[18]。某些属性(例如政治倾向和种族)可以被公开显示,因为用户的关注者可能会因为他的公共属性而关注他。而其他属性(例如性别和位置)是私人的且敏感的,用户不希望将其显示出来。

可以将属性推理视为从用户的在线发布和互动的信息中推理出用户不希望为他人所知道的一组敏感属性的方法[19]。

推理出的用户属性可以用于各种安全敏感活动,例如鱼叉式网络钓鱼和个人信息的身份验证[20]。此外,攻击者可以利用推理的属性在多个站点上识别同一用户或使用离线记录(例如,公开的选民登记记录)形成综合性的用户个人画像,给用户带来更大的安全和隐私风险[21]。

3.2 基于内容的属性推理

基于内容的攻击主要利用主题、个人信息和推文文本等对用户的敏感属性进行推理。

Georgiou等[22]引入了一种基于社区趋势主题的属性推理攻击,从统计角度利用这些公开的社区感知趋势主题来推理在线社交网络用户的敏感属性,因为每个主题中的参与用户形成同质的组(社区),即使他们没有直接链接也是如此。

趋势主题是指与暂时流行的主题相关的一组单词或短语,用于理解和解释信息和模因如何通过具有数亿个节点的庞大社交网络传播[23]。

社交平台的用户表示为集合 $U=\{u_1,u_2,\cdots,u_n\}$。每个用户 u 与具有 k 个敏感属性(例如位置、年龄等)的向量 v 相关联。用户 u 的属性 a_i 可以采用一组可能的值 $\{a_{i1},a_{i2},\cdots,a_{im_i}\}$ 中的一个,其中 m_i 是相应属性的唯一值

总数。属性的值形成一个层次结构,对于某些属性,该层次结构可以具有很大的深度(例如对于城市、区域、国家、大洲乃至整个世界范围的位置信息)。

社交平台上的内容表示为推文的数据流 P。每个推文 $p\in P$ 有一个唯一的作者(用户) $p.u$,并且包含任意数量的主题关键字 $p.T=\{t_1,t_2,\cdots,t_k\}$。 将社区定义为属性中具有相同值的一组用户,但不一定存在社交连接。 例如,居住在武汉的年龄为25岁的男性用户可以形成一个同质社区,包含这些值为属性组合{位置,年龄,性别}标识的所有用户。纽约的用户形成了由单例属性组合{位置}定义的另一个同质社区。

趋势主题算法向攻击者返回提到了所提供主题的一组用户。攻击者对每个属性的先前分布有一般的了解,例如此类知识可能包括基于人口普查的位置分布、基于社交媒体服务发布的统计数据的年龄分布、基于公开此信息的用户的性别分布等[24]。不断增加的知识使攻击者可以针对给定用户的敏感属性逐渐提高其推理置信度。

给定主题和社区元组后,攻击者可能会尝试推理出至少提到一个主题 t_i 的用户的敏感属性。假设 L 是用户的敏感属性(例如位置)之一,用户提到了一些主题 $t_1,t_2,\cdots,t_k$,则 L 的概率分布为:

$$P(L|t_1,t_2,\cdots,t_k)=\frac{P(t_1,t_2,\cdots,t_k|L)P(L)}{P(t_1,t_2,\cdots,t_k)} \tag{1}$$

$P(L)$ 是属性 L 的先验多项式分布,可以基于攻击者对此类信息的一般知识而假定为已知。在给定 L,$Pt_1,t_2,\cdots,t_k|L$ 的情况下,提及主题 $t_1,t_2,\cdots,t_k$ 的用户的概率分布等于提及所有 k 个主题并具有 L 特定值的用户 u 的数量,该值等于 L 的用户总数。例如,对于 $L=a$:

$$P(t_1,t_2,\cdots,t_k|L=a)=\frac{|\{u|u.v.L=a,t_1\in u.T,\cdots,t_k\in u.T\}|}{|\{u|u.v.L=a\}|} \tag{2}$$

其中 $u.v.L$ 是用户的属性 v 的向量中的属性 L。类似的,先验概率 $P(t_1,t_2,\cdots,t_k)$ 等于在用户总数中提及这些主题的用户数。

虽然攻击者可能知道属性的多项式分布,并且能够计算任何主题组合的先验概率,但他们无法计算出具有特定属性值 $L=a$ 的用户集:$\{u|u.v.L=a\}$。取而代之的是,他们可以从趋势主题算法得到的元组来获得概率分布 $Pt_1,t_2,\cdots,t_k|L$ 的近似值。

如果对于 $L=1$ 的任何值,概率 $PL=1|u.T$ 变得大于阈值 θ,则认为该用户的隐私 L 受到侵犯。攻击者可以通过使用这些涉及用户的相应社区特征来提高其推理的可信度。

Thomas 等[25]使用多标签分类方法来使来推理属性,并且提出了多方隐私来防御属性推理。Zhang 等[5]表示,用户推文中的主题标签可以单独用于精确推理用户的位置,准确度为70%到76%。

Otterbacher[26]使用用户的写作风格研究了性别推理。Narayanan 等[27]展示了一个更强的结果,即作者身份可以通过写作风格分析而被去匿名。Adali 和 Golbeck 等[28-29]使用用户的推文研究如何推理出个性。

3.3 基于社交链接的属性推理

He 等[30]将属性推理转换为使用用户之间的社交链接构建的贝叶斯网络上的推理,使用具有合成用户属性的 LiveJournal 社交网络数据集评估了他们的方法。并讨论了通过先验概率、影响力和社会开放性对属性推理的影响。

假设仅考虑直接朋友 Y_1 的属性值来推理 X 的属性,知道 Y_1 的所有属性值后进行了朴素贝叶斯假设。

对于具有最大深度 i 的朴素贝叶斯网络,令 X 的值 x 是在给定观察到网络中其他节点的属性值的情况下具有最大条件概率的属性值(即最大后验概率):

$$\bar{X}=\arg\max_X P(X=x|Y_1,Y_2,\cdots,Y_i),\ x\in\{t,f\} \tag{3}$$

由于推理仅涉及彼此独立的直接朋友 Y_1,因此可以使用贝叶斯网络中编码的条件独立性进一步降低后验概率:

$$\begin{aligned}P(X=x|Y_1)&=P(X=x|Y_{11}=y_{11},\cdots,Y_{1n_1}=y_{1n_1})=\\&\frac{P(X=x,Y_{11}=y_{11},\cdots,Y_{1n_1}=y_{1n_1})}{P(Y_{11}=y_{11},\cdots,Y_{1n_1}=y_{1n_1})}=\\&\frac{P(X=x)\cdot P(Y_{11}=y_{11},\cdots,Y_{1n_1}=y_{1n_1}|X=x)}{\sum_x[P(X=x)\cdot P(Y_{11}=y_{11},\cdots,Y_{1n_1}=y_{1n_1}|X=x)]}=\\&\frac{P(X=x)\cdot\prod_{i=1}^{n_1}PY_{1i}=y_{1i}|X=x)}{\sum_x[P(X=x)\cdot\prod_{i=1}^{n_1}PY_{1i}=y_{1i}|X=x)]'}\end{aligned} \tag{4}$$

其中 x 和 y_{1j} 分别是 X 和 Y_{1j} 的属性值 $(1\leqslant j\leqslant n_1,x,y_{1j}\in\{t,f\})$,$y_{1j}$的值是已知的。使用 $P(Y=y|X=x)$ 表示 $P(Y_{1j}=y_{1j}|X=x)$。后验概率现在取决于 N_{1t},即具有属性值 t 的朋友数量,而不是各个属性值。因此将后验概率 $P(X=x|Y_1)$重写为 $P(X=x|N_{1t}=n_{1t})$。如果 $N_{1t}=n_{1t}$,得到:

$$P(X=x|N_{1t}=n_{1t})=\frac{P(X=x)\cdot P(Y=t|X=x)^{n_{1t}}\cdot P(Y=f|X=x)^{n_1-n_{1t}}}{\sum_x[P(X=x)\cdot P(Y=t|X=x)^{n_{1t}}\cdot P(Y=f|X=x)^{n_1-n_{1t}}]} \tag{5}$$

要计算式(5),需要使用参数估计进一步学习条件概率 $P(Y=y|X=x)$。

Lindamood 等[31]修改了朴素贝叶斯分类器,以社交链接和用户的其他公开属性来推理某些属性,例如,为了推理用户的专业使用了用户的其他属性(用户的雇主、用户居住的城市、用户的社交朋友及其属性)。但是,他们的方法不适用于根本不共享任何属性的用户。

Bhagat 等[32]利用基于 ICA 框架的 K 最近邻算法来

推理LiveJournal数据集的属性,提出了一种局部迭代算法,通过选择在用户节点的本地邻居中出现频率最高的值来推理属性,这可以称为本地邻居的多数投票。

Macskassy和Provost[33]提出了一种邻居关系模型,并提出了两种算法,即迭代关系邻居和概率关系邻居来进行属性推理。

Mo等[34]提出了一种基于图的属性推理模型,该模型使用好友关系、组成员身份和网络关系进行相似性计算,并将其作为转换矩阵来执行标签传播。

Yin等[35]使用随机游走并重新启动基于社交属性的网络(Social Attributes Network,SAN)来进行属性排名。他们将属性建模为节点,并在用户节点和属性节点之间建立链接。但在推理过程中不考虑属性相关性,随机游走会使标签在网络中传播,并在最接近的节点处停止。基于投票分配的方法与此类似,都使用转移矩阵在标签中进行标签传播,并最终选择最接近的属性值。

Misolve等[36]提出了一种基于社区属性的属性推理方法。他们根据同一社区中用户的公共属性来推理用户的敏感属性。在Facebook数据集上进行了实验,以推理用户的工作部门等。

Traud等[37]将社区结构与基于Facebook的给定类别的分区进行了比较,以检查在二元级数据上公共属性的影响。

3.4　基于用户行为的属性推理

用户行为包括点赞、关注、转发评论等行为,以此对属性进行推理。

Kosinski[38]提出的方法可以轻松使用用户行为中的点赞(Facebook Likes)来自动、准确地预测一系列高度敏感的个人属性,包括:性取向、种族、宗教和政治观点,人格特质、智力、家长离异情况、年龄和性别等。用户和他们的点赞表示为稀疏的用户相似矩阵,如果用户和点赞之间存在关联,则将其项设置为1,否则设置为0。使用奇异值分解(Singular-Value Decomposition,SVD)可以减少像用户一样的矩阵的维数。使用线性回归模型预测年龄或智力等数字变量,而使用逻辑回归预测诸如性别或性取向等二分变量。在这两种情况下都应用了10倍交叉验证,研究的设计如图1所示。

Weinsberg等[39]使用用户对不同电影给予的评分来调查性别的推论。特别是,他们为每个用户构造了一个特征向量。特征向量的第i个项是:如果用户查看了第i个电影,则用户对第i个电影给予的评分分数,否则第i个项为0。他们比较了一些分类器,包括逻辑回归[40]、支持向量机[41]和朴素贝叶斯[42],发现逻辑回归胜过其他方法。具体来说调查了用户看的哪些电影可以最大程度地提高推理准确性,但是此方法可能不适用于现实情况。

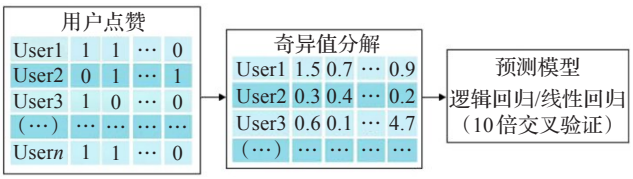

图1　基于点赞行为的推理模型设计

Chaabane等[43]的研究证明用户的行为数据也可以是用户喜欢或共享的页面或列表。攻击者(例如,社交平台提供商、广告商或数据经纪人)可以使用机器学习分类器来推理目标用户的私人属性(例如,性别、居住城市和政治倾向)。

3.5　基于多类型的属性推理

Mao等[44]等提出一种基于社交链接和属性关联的高效社会属性推理方案,方法包括三个主要阶段:预处理、构造社交属性相关性网络(Social Relevance Attribute Network,SRAN)图和推理属性,方法如图2所示。

第一阶段:预处理将社会数据作为输入,其中包括三个组成部分:社会结构抽象(PI-ss)、用户属性抽象(PI-ua)和属性相关性分析(PI-ar)。PI-ss用于提取用户之间的社交链接并输出社交节点(用户)图Gs。PI-ua用于建立用户(社交节点)与社交属性值之间的映射,并输出属性矩阵A。PI-ar测量两个属性值之间的相关性,并输出属性邻接矩阵R。

第二阶段:以社交图Gs构造SRAN图,以属性矩阵A和属性邻接矩阵R为输入,并输出SRAN图。SRAN图具有两种节点:社交节点和属性节点,其中社交节点代表用户,属性节点是目标社交网络中包含的属性值。

定义了三种类型的边来描述这些节点之间的关系。具体而言,社交边代表两个社交节点之间的社交链接;社交节点与属性节点之间的用户属性边由该社交节点是否具有该属性值确定;属性相关性边由两个属性值(即SRAN中的属性节点)之间的相关性加权,该值在第一阶段由PI-ar量化。

第三阶段:以从第二阶段获得的SRAN图作为输入来推理未知属性,进行具有重启的随机游走(Rndom walk with Restart,RwR)以执行基于相关性的属性推理,

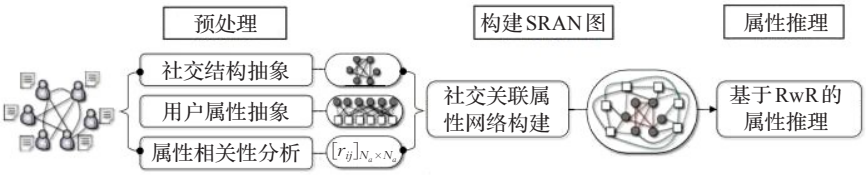

图2　基于社交链接和属性关联的推理方法

并在结果中输出目标用户的所有未知用户属性链接。

Gong等[45]通过友谊和行为联系来推理用户雇主和城市等属性。

3.6 其他

Mei等[46]提出了一种新的基于图像和属性的卷积神经网络属性推理攻击框架,框架集成和修改了现有的最新CNN模型。如图3,它包含三个主要部分,分别是R-CNN面部识别器、基于图像和属性的CNN年龄分类器以及基于属性的FCNN年龄分类器。但是其仅考虑一个目标的敏感属性,即年龄范围。

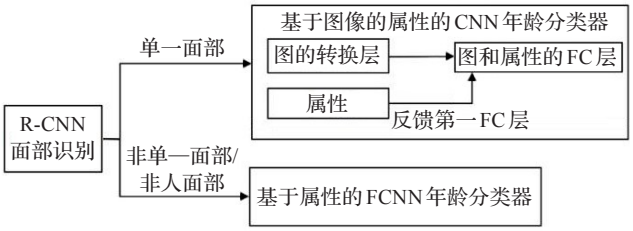

图3 基于图像和属性的推理攻击系统

Labitzke等[47]通过面向情感的挖掘来推理用户对Facebook页面的兴趣程度。Zamal等[48]使用移动通信来推理性别和年龄,并考虑其特征以及节点属性值之间的联系。Chen等[49]提出了ChiSquare,基于卡方统计来计算用户和属性值之间的相关性。

4 针对地理位置的推理攻击

4.1 基于社交图的位置推理

文献[50]显示社交图分析可以从朋友和关注者的位置揭示用户位置。

将用户 v 的位置图定义为从目标用户 G_v 的社交网络获得的加权图 $L_v=<I_v,S_v>$,如下所示:

$$I_v=I(\tau_v)\bigcup_{u\in E(v)}I\tau_u) \tag{6}$$

节点集 I_v 是 τ_v 的解释集以及 v 朋友的地名集合。定义链接集 S_v,以便在下列情况下在 $i_1\in I_v$ 和 $i_2\in I_v$ 之间存在双向链接:

i_1 和 i_2 为同一地区的一部分或者同一地区,该链接的权重为 w_{co}。

i_1 和 i_2 是同一省/州(或其他等效的地区行政区划)或者它们属于同一州和国家/地区,该链接的权重为 w_s。

i_1 和 i_2 是同一城市,该链接的权重为 w_{ci}。

与链接相关联的权重指示解释之间关系的强度。例如认为如果 i_1 和 i_2 代表同一城市,则两个解释 i_1 和 i_2 之间的关系要强于它们代表同一状态下的两个不同城市。

出于相同的原因,与 i_1 和 i_2 对应于同一地区相比,i_1 和 i_2 对应于同一省/州(或等效的行政区划)。链接(i_1,i_2)的权重衡量的是 i_1 和 i_2 共享的地区规划的粒度,粒度越细,重量越大。基于此有 $w_{co}<w_s<w_{ci}$。

4.2 基于社交行为的位置推理

在基于位置的社交网络中,用户的互动主要是通过签到和照片共享进行的。文献[51]提出了一种基于历史签到和照片的空间分布的推理模型,并表明通过对包括签到和照片在内的多个事件进行时空分析,可以高精度地推理出用户的位置。

这是一种内容遗忘的推理模型,该模型不会以处理照片的内容来查找用户的位置,而是仅考虑不同的位置签到和照片共享概率。

Ilaria等[52]提出了一种基于视觉技术的位置推论模型,该模型使用Twitter签到数据,表明人们仅使用一小部分位置点就可以推理出人们最常在的和最私人的位置,例如工作和家庭。Souza等[53]研究了用户在Instagram上共享自拍照的集体行为。

4.3 其他

在移动应用中,Michalevsky等[54]表明攻击者可以使用机器学习根据用户的智能手机的总功耗来推理用户的位置。Narain等[55]的研究中发现,攻击者可以使用用户智能手机上的陀螺仪、加速度计和磁力计数据来推理用户的位置。

5 针对社交关系的推理攻击

5.1 基于位置的关系推理

诸如Foursquare之类的基于位置的社交网络以及诸如Uber之类的基于位置的在线服务的广泛普及,为人们带来了大量的人类轨迹数据。事实证明,了解基本的人员流动模式对于各种应用(例如下次访问位置预测)具有重要价值[56]。

Hsieh等[57]使用用户的离线地理活动(例如签到记录和会议事件)来推理在线社交关系。首先构建了一个共址图,其中节点是用户,边是用户之间的共址,边权重是组合的特征值。具有较高的紧密度、概率和共同位置相似性的两个节点彼此相识的可能性很高。其次,如果会议活动的位置对两个节点都更有意义或更重要,则应为此类共址分配更高的权重,有较高的开会频率的两个人倾向于存在社交关系。

该模型是一种基于图的半监督学习方法,可以使用节点对的提取特征来推理社交联系。中心思想有三个方面。首先,具有相似特征分数的节点对往往具有相同的联系(即是否具有社会纽带)。构造一个链接图(Link Graph,LG),以表示节点对之间的特征相关性[58]。其次,由于不同的特征对社交联系的推理有多种影响,因此针对每个特征分别学习与LG中每个边相关联链接的值,以建模节点对的特征差异与成为朋友的可能性之间的关系。最后使用算法迭代地计算节点对与LG中相

邻节点成为朋友的概率,接着确定每个特征的重要性,从而可以推理出节点对之间的社会关系[59]。

Zhang等[60]通过将用户对的空间、时间和社交属性视为有效用户链接的不同视图,研究了给定LBSN中社交关系推理的问题。

如图4,通过将3个因素中的每一个视为任何目标用户对的一个视图,设计了一种新颖的多视图匹配网络(Multi-View Matching Network,MVMN)。MVMN包括位置匹配模块、时间序列匹配模块和关系匹配模块。每个模块都学习特定视图的匹配表示,而MVMN将它们融合以进行最终的关系推理。

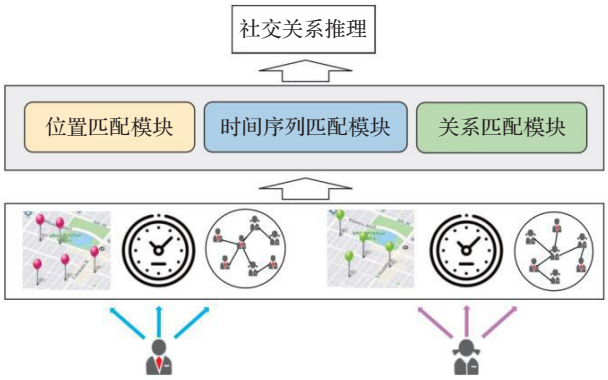

图4　时空轨迹多视图匹配网络

Backes等[61]从用户所在位置推理社交关系,采用深度学习方法来学习用户的移动功能并将其用于社交关系推理。诸如文献[62-66]此类的工作可以从同一时空推理出社会联系,为其中两个用户共享共同的朋友或位置。

Wu等[67]从用户轨迹数据推理社会关系在诸如好友推荐和乘车共享等现实应用中具有重要价值。模型利用图卷积网络(Graph Convolutional Network,GCN)以无监督的方式学习用户在用户移动异构图上的嵌入。

Olteanu等[68]研究同位置信息对位置隐私的影响。最近,Zhou等人[69]从好友和流动性数据推理出社交联系。

5.2　基于主题标签的关系推理

Zhang[70]使用用户主题标签二分图嵌入模型来推理关系,以学习每个用户画像的主题标签,并根据两个用户画像的余弦距离进行无监督的关系预测。

具体来说,即将用户和主题标签组织成一个加权二分图。对于连接用户和主题标签的边,其权重等于用户共享主题标签的次数。在图上模拟了从每个用户开始的随机游走,从每个节点到下一个节点的过渡概率遵循相应边的权重。每次游走都有一定的长度,留下了一组随机的行走轨迹。然后,分别依靠下面的优化目标函数来学习每个用户的主题标签:

$$\arg\max_{\theta}\prod_{v\in U\cup H}p(v|N(v);\theta) \tag{7}$$

这里,$N(v)$表示节点v的邻域,而$\theta(v)$是节点v的学习结果。此外,$p(v|N(v);\theta)$使用softmax函数建模。目标函数本质上是连续词袋(Continuous Bag-of-Words,CBOW)模型[71],采用负采样方法来加快学习过程。

最后对于任何两个用户,会计算他们学习到的余弦距离,并在余弦距离低于所选阈值时预测他们的社交关系[72]。

5.3　其他

Rahman等[73]提出了一种推理社交关系的多模式方法,利用用户的5个不同维度特征,即图像、推文文本、主题标签、地理位置和(不完整的)社会关系评估了一个真实的数据集,该数据集包含从Instagram收集的2 200万用户帖子。使用数据集的特征向量训练5个随机森林分类器,然后使用5个训练过的分类器各自的AUC值(Area Under the ROC Curve),即ROC曲线下的面积为每个分类器分配置信度a。他们将这些AUC值用作目标集上5个分类器预测的强度或可信赖性的指标。结果证明,当多种模式组合在一起时,社交关系推理攻击的成功率将大大提高。

Gupta等[74]研究了社交网络用户所发布视频中人们的社交关系推理,使用视听特征和运动轨迹来计算视频中每个场景的社交关系的度量,同时利用人脸识别来计算每个场景中人物的出现。

Zhao等[75]提出一种基于多源信息的两阶段的深度学习框架TDFI,用于社交关系推理,这种方法可以在拥有低复杂度的同时利用多源信息。应用扩展邻接矩阵(Extended Adjacency Matrix,EAM)来表示多源信息,然后采用改进的深度自动编码器网(improved Deep AutoEncoder Network,iDAEN)为每个用户提取融合的特征向量。TDFI框架还提供了一种改进的深度孪生神经网络(improved Deep Siamese Network,iDSN),用于推理来自iDAEN的用户是否存在社交关系。

6　相关防御方案

6.1　针对属性推理的防御

6.1.1　基于文本的防御方法

(1)隐藏:隐藏(也称为删除)[76]建议用户选择属性关键字或主题标签Hp的子集(共有$2^{Hp}-1$个此类子集),可以通过阈值th限制要删除的关键字或主题标签的数量,以优化运行时间。将所有生成的主题标签的子集发送到推理模型以验证它们是否满足位置隐私约束,然后发布推文。

(2)替换:该机制用一组主题标签H中的其他主题标签替换了原始标签以误导攻击者[77]。为了保持合理的搜索复杂度,必须限制一组潜在的标签以替换每个原始标签。 固定了一个阈值ts,并集中在ts上在语义上最接近原始主题标签的主题标签,这确保了候选主题标

签的集合将损失降至最低,将搜索空间限制为$(ts+1)^{Hp}-1$。与隐藏机制一样,可以通过用类似于th的阈值限制要替换的标签的数量来进一步降低时间复杂度[78]。

(3)泛化:这种机制将每个原始主题标签概括为一个语义上更广泛的类别。由于并非所有主题标签都可以泛化(例如#love),因此将给定推文中可泛化主题标签的子集表示为v。为降低时间复杂度,还可以固定要泛化的最大标签数的阈值[79]。

(4)混淆:即基于噪声的扰动,以在发布数据之前对其进行掩盖[80-81]。BlurMe会对用户的电影分级进行模糊处理,以减少泄露其性别信息的风险[39]。根据项目与除i之外的属性值之间的相关性将项目分类到列表Li中。具体来说,对于每个属性值i,通过使用学习逻辑回归分类器数据向量作为特征向量;将逻辑回归分类器中某项的负系数视为与i以外的属性值的相关性。Attri-Guard利用对抗性机器学习技术将噪声添加到用户的公共数据中,以防御属性推理攻击[82]。

6.1.2 基于博弈论的防御方法

Chanthaweethip等[83]提出了一种博弈论的方法来防御属性攻击。这些方法具有理论上的隐私保证,但是它们难以解决应用于属性推理攻击时在计算上的优化问题。Shokri等[84]提出的方法对于防御属性推理攻击是很容易处理的,因为这样的问题本质上是一维的公共数据向量。防御者将位置混淆,以保护用户免受最佳推理攻击。

Salamatian等[85]提出了量化概率映射(Quantization Probabilistic Mapping,QPM)来解决Han等人提出的博弈论优化问题。具体来说,他们聚集用户的公共数据,并使用群集代表他们,然后使用聚类近似解决优化问题。由于使用了量化,因此QPM没有理论上的隐私保证,即QPM不一定能防御最佳属性推理攻击,但是QPM使其在实践中更易于防御。

6.2 针对位置推理的防御

6.2.1 基于k匿名的防御方法

k匿名性的概念是文献中基于位置的系统最广泛使用的隐私定义。已用于保护用户的位置,要求它在一组k个点之间是无法区分的(通常需要共享某些位置属性)[86]。

一种实现此目的的方法是使用虚拟位置[87-88]。该技术涉及使用实际和虚拟位置生成k-1个正确选择的虚拟点,并向服务提供商执行k个查询。实现k匿名性的另一种方法是通过隐藏[89-91]。这涉及到创建一个包含k个点的共享区域,这些共享点共享一些感兴趣的属性,然后向服务提供商查询该隐藏区域。

Sun等[92]解决了身份披露问题,并通过确保至少有k个朋友对共享相同的数量,提出了一种新颖的k-NMF匿名性。

6.2.2 基于差分隐私的防御方法

差分隐私[93]是统计数据库领域的隐私概念。其目标是在发布有关数据库的汇总信息时保护个人数据。差分性隐私要求修改单个用户的数据对查询结果的影响可以忽略不计。更确切地说,它要求将查询应用于数据库D时返回值v的概率与应用于相邻数据库D'时相同值的概率相比,同用户在D,D'中的值应该在e范围内[94]。实现此概念的一种典型方法是向查询输出中添加受控的随机噪声,例如从拉普拉斯分布中提取的随机噪声[95]。

差分隐私已在位置隐私中被使用。Machanavajjhala等[96]的研究表明可以使用合成数据生成技术以差分隐私的方式发布有关通勤模式的统计信息。Ruan等[97]使用四叉树空间分解技术来确保具有位置模式挖掘功能的数据库中的差异优先权。Dewri等[98]使用了k个位置的匿名集,以求从k个位置中的任何一个推理出相同混淆位置z的概率为相似(范围e内)。

6.2.3 其他防御方法

Cheng等[99]提出了一种位置隐蔽机制,并着重于基于位置的范围查询。隐私的程度由隐蔽区域的大小(也称为不确定区域)和敏感区域的覆盖率来衡量,覆盖率是隐蔽区域的面积与用户认为敏感的区域的面积之比。PrivCheck[100]通过混淆基于位置的社交网络中用户签到行为的数据,来最大程度地减少用户私人数据的泄露。

在文献[101]研究中,基于特定的传感技术或环境条件,假定用户的真实位置具有某种程度的不精确性。然后使用不同的模糊处理技术来增加这种不精确性,以达到一定程度的隐私级别。此隐私级别定义为应用模糊处理技术前后的准确度之比。

6.3 针对社交关系推理的防御

郭耀[102]提出了一种基于关键节点与连接关系的社交网络隐私保护方法KLPP,可以保护社交网络中关键节点和连接的隐私,且通过随机度扰动算法对网络中的关键节点施加更多保护。同时通过对节点进行聚类,将网络划分为子图,并在子图内部扰动网络中的连接,可以减少扰动过程对网络结构的影响。

黄海平等[103]设计了带权社交关系网络中的节点和边的扰动策略,采用改进的单源最短路径约束模型构建边权值噪音。

Shahabi等[104]提出一种名为PLACE的可扩展框架,并提出了4个新颖的隐私保护基块,包括位置邻近度、共现向量、位置熵和跟随度。陈伟鹤等[105]提出L-intimacy隐私保护模型,该模型能够根据用户与好友的亲密度级别进行隐私保护。

7 总结与展望

社交网络中的推理攻击与保护技术处于不断的对

抗中,双方技术都在提升。目前攻击者所掌握的知识越来越多,攻击能力越来越强;社交网络数据包含的内容也越来越复杂,既包含用户的各种属性,也包含用户之间的关系等多种敏感信息[106]。

在属性推理方面,未来攻击者可以通过对抗性机器学习得到更强大的分类器,利用它们来进行推理[107];收集更多的用户信息,包括跨平台的数据,利用属性之间的相关性执行更好的属性推理。针对位置的推理则可以利用计算机视觉技术更好地识别推文中照片的位置,考虑更多的连续社交行为之间的时空相关性等[108]。对于社交关系推理,未来工作的一些方向包括加强对社交图模型链路权重的学习[109],扩展投票分配攻击以推理用户之间的隐藏社交关系等[110]。

而在防御方面未来主要分为两大方向:其一是以服务为中心的方法,即依靠可信机制来阻止社交网络服务发布揭示有关用户信息的内容,例如使用点对点的社交网络增强用户的匿名性[111]。其二是以用户为中心的方案,即通过用户部署的防御框架将用户信任从社交网络提供商转移到本地计算机,例如使用内容自动生成对抗文本进行混淆[112];自动生成社交行为来创建无法区分的网络,从而对隐私推理攻击进行预防。

参考文献:

[1] Nettleton D F,Estivill-Castro V,Salas J.Privacy in multiple on-line social networks re-identification and predictability[J]. Transactions on Data Privacy,2019(12):29-56.

[2] Kim Y,Seo J.Detection of rapidly spreading Hashtags via social networks[J].IEEE Access,2020(8):39847-39859.

[3] Mauw S,Ramírez-Cruz Y,Trujillo-Rasua R.Robust active attacks on social graphs[J].Data Mining and Knowledge Discovery,2019,33:1357-1392.

[4] Paul N J,Dredze M.You are what you tweet:Analyzing twitter for public health[C]//Proceedings of the 15th International AAAI Conference on Weblogs and Social Media, July 17-21,2011:265-272.

[5] Zhang Y,Humbert M,Rahman T,et al.Tagvisor:A privacy advisor for sharing hashtags[J].arXiv:1802.04122,2018.

[6] Zheleva E,Getoor L.To join or not to join:the illusion of privacy in social networks with mixed public and private user profiles[C]//Proceedings of the 18th International Conference on World Wide Web,April 20-24, 2009:531-540.

[7] Hu X,Wang L,Tang J,et al.Anonymizing approach to resist label neighborhood attacks in dynamic releases of social networks[C]//Proceedings of the 19th International Conference on e-Health Networking,Applications and Services,Oct 12-15,2017.

[8] Sharon T,John N.Unpacking(the)secret:Anonymous social media and the impossibility of networked anonymity[J].New Media and Society,2018:381-407.

[9] Mauw S.Ramírez-Cruz Y,Trujillo-Rasua R.Conditional adjacency anonymity in social graphs under active attacks[J].Knowledge and Information Systems,2019,61: 485-511.

[10] Ding S H,Fung B C,Iqbal F,et al.Cheung.learning stylometric representations for authorship analysis[J].IEEE Transactions on Cybernetics,2019,49(1):107-121.

[11] Wang Q,Xue H,Li F,et al.DontTweetThis:Scoring private information in social networks[J].Privacy Enhancing Technologies,2019(4):72-92.

[12] Wang G,Wang B,Wang T,et al.Ghost riders:Sybil attacks on crowd sourced mobile mapping services[J].IEEE/ACM Transactions on Networking,2018,26(3):1123-1135.

[13] Alexander E,Vanathi R,Dhikhi T,et al.Privacy shield: Securing privacy in social networks[C]//Proceedings of the 2018 IEEE International Conference on Computational Intelligence and Computing Research(ICCIC), Dec 13-15,2018.

[14] Qian J,Li X,L,Zhang C,et al.Social network de-anonymization and privacy inference with knowledge graph model[J].IEEE Transactions on Dependable and Secure Computing,2019,16(4):679-691.

[15] Dwork C,Naor M,Pitassi T,et al.Pan-private streaming algorithms[C]//Proceedings of The First Symposium on Innovations in Computer Science,2010.

[16] Gupta P,Gottipati S,Jiang J,et al.Your love is public now:Questioning the use of personal information in authentication[C]//Proceedings of the 8th ACM SIGSAC Symposium on Information Computer and Communications Security,2013.

[17] Qian J,Tang S,Liu H,et al.Privacy inference on knowledge graphs:Hardness and approximation[C]//Proceedings of the 2016 12th International Conference on Mobile Ad-Hoc and Sensor Networks,Dec 16-18,2016.

[18] Heatherly R,Kantarcioglu M,Thuraisingham B.Preventing private information inference attacks on social networks[J]. IEEE TKDE,2013,25(8):1849-1862.

[19] Georgiou T,El Abbadi A,Yan X.Extracting topics with focused communities for social content recommendation[C]// Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing, 2017:1432-1443.

[20] Kantor P,Muresan G,Roberts F,et al.Intelligence and security informatics[C]//Proceedings of the International Conference on Intelligence and Security Informatics, May 19-20,2005.

[21] Schwartz H A,Eichstaedt J C,Kern M L,et al.Personality,gender,and age in the language of social media:

The open vocabulary approach[J].PloS One,2013,8(9):e73791.

[22] Georgiou T,Abbad A E,Yan X.Privacy-preserving community-aware trending topic detection in online social media[C]//Proceedings of the IFIP Annual Conference on Data and Applications Security and Privacy,July 19-21,2017:205-224.

[23] AL-Kharji S,Al-Rodhaan M.A novel(K,X)-isomorphism method for protecting privacy in weighted social network[C]//Proceedings of the 21st Saudi Computer Society National Computer Conference(NCC),April 25-26,2018.

[24] Abid Y,Imine A,Rusinowitch M.Online testing of user profile resilience against inference attacks in social networks[C]//Proceedings of the 22nd European Conference on Advances in Databases and Information Systems,September 2-5,2018:105-117

[25] Thomas K,Grier C,Nicol D M.UnFriendly:Multi-party privacy risks in social networks[C]//Proceedings of the 10th International Conference on Privacy Enhancing Technologies,2010:236-252.

[26] Otterbacher J.Inferring gender of movie reviewers:Exploiting writing style,content and metadata[C]//Proceedings of the 19th ACM Conference on Information and Knowledge Management,October 26-30,2010.

[27] Narayanan A,Paskov H,Gon Zhenqiang,et al.On the feasibility of internet-scale author identification[C]//Proceedings of the IEEE Symposium on Security & Privacy 2012,May 20-23,2012.

[28] Adali S,Golbeck J.Predicting personality with social behavior[C]//Proceedings of the 2012 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining,Aug 26-29,2012:302-309.

[29] Golbeck J,Robles C,Turner K.Predicting personality with social media[C]//Proceedings of the International Conference on Human Factors in Computing Systems,May 7-12,2011:253-262.

[30] He J,Chu W,Liu Z.Inferring privacy information from social networks[C]//Proceedings of the International Conference on Human Factors in Computing Systems,May 23-24,2006.

[31] Lindamood J,Heatherly R,Kantarcioglu M,et al.Inferring private information using social network data[C]//Proceedings of the 18th International Conference on World Wide Web,April 20-24,2008:1145-1146.

[32] Bhagat S,Cormode G,Rozenbaum I.Applying link-based classification to label blogs[C]//Proceedings of the 1st International Workshop on Social Networks Analysis,August 12-15,2007:97-117.

[33] Macskassy S A,Provost F.A simple relational classifier[C]//Proceedings of the 9th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining,Aug 27,2003:64-76.

[34] Mo M,Wang D,Li B,et al.Exploit of online social networks with semi-supervised learning[C]//Proceedings of the 2010 International Joint Conference on Neural Networks,May 23,2010:1-8.

[35] Yin Z,Gupta M,Weninger T,et al.A unified framework for link recommendation using random walks[C]//Proceedings of the 2010 International Conference on Advances in Social Networks Analysis and Mining,Aug 9-11,2010:152-159.

[36] Misolve A,Viswanath B,Gummadi K P,et al.You are who you know:Inferring user profiles in online social networks[C]//Proceedings of the Third ACM International Conference on Web Search and Data Mining,Feb 4,2010:251-260.

[37] Traud A L,Mucha P J,Porter M A.Social structure of Facebook networks[J].Tatistical Mechanics and its Applications,2012,391:4165-4180.

[38] Kosinski M,Stillwell D,Graepel T.Private traits and attributes are predictable from digital records of human behavior[J].National Academy of Sciences,2013,110:5802-5805.

[39] Weinsberg U,Bhagat S,Ioannidis S,et al.Blurme:Inferring and obfuscating user gender based on ratings[C]//Proceedings of the ACM Conference on Recommender Systems,Sep 9-13,2012:195-202.

[40] Jr D W H,Lemeshow S.Applied logistic regression[M].[S.l.]:John Wiley & Sons,2004.

[41] Cortes C,Vapnik V.Support-vector networks[J].Machine Learning,1995,20(3):273-297.

[42] McCallum A,Nigam K.A comparison of event models for naive bayes text classification[C]//Proceedings of AAAI Conference,1998.

[43] Chaabane A,Acs G,Kaafar M A.You are what you like! information leakage through users' interests[C]//Proceedings of the 19th Annual Network & Distributed System Security Symposium,Feb 5-8,2012.

[44] Mao J,Tian W,Yang Y,et al.An efficient social attribute inference scheme based on social links and attribute relevance[J].IEEE Access,2019,7:153074-153085.

[45] Gong N Z,Liu B.You are who you know and how you behave:attribute inference attacks via users' social friends and behaviors[C]//Proceedings of the 25th USENIX Security Symposium,August 16-18,2016:979-995.

[46] Mei B,Xiao Y,Li R,et al.Image and attribute based convolutional neural network inference attacks in social networks[J].IEEE Transactions on Network Science and Engineering,2018,7(2):869-879.

[47] Labitzke S,Werling F,Mittag J.Do online social network friends still threaten my privacy?[C]//Proceedings of the Third ACM Conference on Data and Application Security and Privacy,Feb 18-20,2013.

[48] Zamal F A,Liu W,Ruths D.Homophily and latent attribute inference:Inferring latent attributes of twitter users from neighbors[C]//Proceedings of the 6th International AAAI Conference on Weblogs and Social Media,June 4,2012.

[49] Chen T,Boreli R,Kaafar M,et al.On the effectiveness of obfuscation techniques in online social networks[C]//Proceedings of the 14th Privacy Enhancing Technologies Symposium,July 16-18,2014.

[50] Ghufran M,Quercini G,Bennacer N.Toponym disambiguation in online social network profiles[C]//Proceedings of the 23rd ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems(ACM SIGSPATIAL 2015),Nov 3-6,2015.

[51] hahid A R,Pissinou N,Iyengar S S,et al.Check-ins and photos:Spatiotemporal correlation-based location inference attack and defense in location-based social networks[C]//Proceedings of the 2018 17th IEEE International Conference On Trust,Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering(TrustCom/BigDataSE),Aug 1-3,2018.

[52] Ilaria L,Alfie A,Chen M.I know where you live:Inferring details of people's lives by visualizing publicly shared location data[C]//Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems,May 7-12,2016:1-12.

[53] Souza F,Casas D D,Flores V,et al.Dawn of the selfie era:The whos,wheres,and hows of selfies on instagram[C]//Proceedings of the ACM Conference on Online Social Networks,Nov 2-3,2015:221-231.

[54] Michalevsky Y,Nakibly G,Schulman A,et al.Powerspy:Location tracking using mobile device power analysis[C]//Proceedings of the 24th USENIX Security Symposium,August 10-12,2016.

[55] Narain S,Vo-Huu T D,Block K,et al.Inferring user routes and locations using zero-permission mobile sensors[C]//Proceedings of the IEEE Symposium on Security and Privacy,May 23-25,2016.

[56] Kokciyan N,Yolum P.PRIGUARD:A semantic approach to detect privacy violations in online social networks[J].IEEE Transactions on Knowledge and Data Engineering,2016,28(10):2724-2737.

[57] Hsieh H P,Li C T.Inferring online social ties from offline geographical activities[C]//Proceedings of the ACM Transactions on Intelligent Systems and Technology,2019.

[58] Sun Y,Yin L,Liu W.Defending sybil attacks in mobile social networks[C]//Proceedings of the 2014 IEEE Conference on Computer Communications Workshops,April 27,2014:163-164.

[59] Li H,Chen Q,Zhu H,et al.Privacy leakage via de-anonymization and aggregation in heterogeneous social networks[J].IEEE Transactions on Dependable and Secure Computing,2020,17(2):350-362.

[60] Zhang W,Lai X,Wang J.Social link inference via multiview matching network from spatiotemporal trajectories[J].Transactions on Neural Networks and Learning Systems(Early Access),2020(4):1-12.

[61] Backes M,Humbert M,Pang J,et al.walk2friends:Inferring social links from mobility profiles[C]//Proceedings of the ACM Conference on Computer and Communications Security 2017(CCS 2017),Nov 3,2017.

[62] Eagle N,Pentland A S,Lazer D.Inferring friendship network structure by using mobile phone data[J].National Academy of Sciences,2009,106:15274-15278.

[63] Wang H,Li Z,Lee W C.PGT:Measuring mobility relationship using personal,global and temporal factors[C]//Proceedings of the 2014 IEEE International Conference on Data Mining,Dec 14-17,2014:570-579.

[64] Crandall D J,Backstrom L,Cosley Dan,et al.Inferring social ties from geographic coincidences[J].National Academy of Sciences,2010,107:22436-22441.

[65] Scellato S,Noulas A,Mascolo C.Exploiting place features in link prediction on location-based social networks[C]//Proceedings of the 17th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining,Aug 21-24,2011:1046-1054.

[66] Pham H,Shahabi C,Liu Y.Ebm:An entropy-based model to infer social strength from spatiotemporal data[C]//Proceedings of the ACM Special Interest Group on Management of Data,June 22-27,2013:265-276.

[67] Wu Y,Lian D,Jin S,et al.Graph convolutional networks on user mobility heterogeneous graphs for social relationship inference[C]//Proceedings of the 28th International Joint Conference on Artificial Intelligence(IJCAI 2019),Aug 10-16,2019.

[68] Olteanu A,Huguenin K,Shokri R,et al.Quantifying interdependent privacy risks with location data[J].IEEE Transactions on Mobile Computing,2017,16(3):829-842.

[69] Zhou F,Wu B,Yang Y,et al.vec2Link:Unifying heterogeneous data for social link prediction[C]//Proceedings of the 27th ACM International Conference on Information and Knowledge Management,Oct 22-26,2018:1843-1846.

[70] Zhang Y.Language in our time:An empirical analysis

of hashtags[C]//Proceedings of the International World Wide Web Conference,2019:2378-2389.

[71] Mikolov T,Chen K,Corrado G,et al.Efficient estimation of word representations in vector space[C]//Proceedings of the International Conference on Learning Representations,May 2-4,2013.

[72] Mikolov T,Sutskever I,Chen K,et al.Distributed Representations of Words and Phrases and their Compositionally[C]//Proceedings of the Neural Information Processing Systems 26(NIPS 2013),Dec 5-8,2013:3111-3119.

[73] Rahman T,Fritz M,Backes M,et al.Everything about you:A multimodal approach towards friendship inference in online social networks[J].arXiv:2003.00996,2020.

[74] Gupta A,Yilmaz A.Social network inference in videos[J].Academic Press Library in Signal Processing,2018,6:395-424.

[75] Zhao Y,Qiao M,Wang H.TDFI:Two-stage deep learning framework for friendship inference via multi-source information[C]//Proceedings of the IEEE Conference on Computer Communications,April 29,2019:1981-1989.

[76] Khoory S,Roken N A,Abdooli M A,et al.Speculo:A tool for multiple identities exploration and detection in social networks[J].IEEE Access,2019(8):297-300.

[77] 闫光辉,刘婷,张学军,等.抵御背景知识推理攻击的服务相似性位置k匿名隐私保护方法[J].西安交通大学学报2020,54(1):9-11.

[78] 宋畅,禹可,吴晓非.基于改进边权重的成对马尔可夫随机场模型的社交异常账号检测方法[J].计算机科学,2020,47(2):251-255.

[79] Zhou Y,Kim D,Zhang J,et al.ProGuard:Detecting malicious accounts in social-network-based online promotions[J].IEEE Access,2017(5):1990-1998.

[80] Cai Z,He Z,Guan X,et al.Collective data-sanitization for preventing sensitive information inference attacks in social networks[J].IEEE Transactions on Dependable and Secure Computing,2018,15(4):577-590.

[81] Li X B,Sarkar S.Class-restricted clustering and micro perturbation for data privacy[J].Management Science,2013,59(4):796-812.

[82] Jia J,Gong N Z.AttriGuard:A practical defense against attribute inference attacks via adversarial machine learning[C]//Proceedings of the 28th USENIX Security Symposium,2018:513-529.

[83] Chanthaweethip W,Han X,Crespi N,et al."Current City" prediction for coarse location based applications on Facebook[C]//Proceedings of the 2013 IEEE Global Communications Conference,2018:3188-3193.

[84] Shokri R,Theodorakopoulos G,Troncoso C.Protecting location privacy:Optimal strategy against localization attacks[C]//Proceedings of the 19th ACM Conference on Computer and Communications Security,Oct 16-18,2012.

[85] Salamatian S,Zhang A,Calmon F P,et al.Managing your private and public data:Bringing down inference attacks against your privacy[J].arXiv:1408.3698,2014.

[86] Ferrag M A,Maglaras L.Privacy-preserving schemes for Ad Hoc social networks:A survey[J].IEEE Communications Surveys & Tutorials,2017,19(4):3015-3045.

[87] Kido H,Yanagisawa Y,Satoh T.Protection of location privacy using dummies for location-based services[C]//Proceedings of the 21st International Conference on Data Engineering,2005:1248.

[88] Shankar P,Ganapathy V,Iftode L.Privately querying location-based services with sybilquery[C]//Proceedings of the 11th International Conference on Ubiquitous Computing,April 17,2009:31-40.

[89] Bamba B,Liu L,Pesti P,et al.Supporting anonymous location queries in mobile environments with privacygrid[C]//Proceedings of the 17th International World Wide Web Conference(WWW 2008),April 21-25,2008:237-246.

[90] Duckham,Kulik L.A formal model of obfuscation and negotiation for location privacy[C]//Proceedings of the International Conference on Pervasive Computing,April 6-8,2005:152-170.

[91] Xue M,Kalnis P,Pung H.Location diversity:Enhanced privacy protection in location based services[C]//Proceedings of the International Symposium on Location- and Context-Awareness,2009:70-87.

[92] Sun C,Yu P S,Kong X,et al.Privacy preserving social network publication against mutual friend attacks[C]//Proceedings of the IEEE 13th International Conference on Data Mining Workshops,2014:71-97.

[93] Dwork C.Differential privacy[C]//Proceedings of ICALP 2006,2006:1-12.

[94] Xie Y,Zheng M.A differentiated anonymity algorithm for social network privacy preservation[J].Algorithms,2016,9(4):85.

[95] Li M,Liu Z,Dong K.Privacy preservation in social network against public neighborhood attacks[C]//Proceedings of the 2016 IEEE Trustcom/BigDataSE/ISPA,Aug 23-26,2016:1575-1580.

[96] Machanavajjhala A,Kifer D,Abowd J M,et al.Privacy:Theory meets practice on the map[C]//Proceedings of the IEEE 24th International Conference on Data Engineering,April 7-12,2008:277-286.

[97] Ho S S,Ruan S.Differential privacy for location pattern mining[C]//Proceedings of the 4th ACM SIGSPATIAL International Workshop on Security and Privacy,2011:17-24.

[98] Dewri R.Local differential perturbations: Location pri-

vacy under approximate knowledge attackers[J].IEEE Transactions on Mobile Computing,2012,12(12):2360-2372.

[99] Cheng R,Zhang Y,Bertino E,et al.Preserving user location privacy in mobile data management infrastructures[C]//Proceedings of the 6th International Conference on Privacy Enhancing Technologies,2006:393-412.

[100] Yang D,Zhang D,Qu B,et al.Cuevas PrivCheck:Privacy-preserving check-in data publishing for personalized location based services[C]//Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing,Sep 12-16,2016:545-556.

[101] Ardagna C A,Cremonini M,Damiani E,et al.Location privacy protection through obfuscation-based techniques[C]//Proceedings of the IFIP Annual Conference on Data and Applications Security and Privacy,2007:47-60.

[102] 郭耀.基于关键节点与连接关系的社交网络隐私保护方法研究[D].西安:西安电子科技大学,2019.

[103] 黄海平,张东军,王凯,等.带权值的大规模社交网络数据隐私保护方法[J].计算机研究与发展,2020,57(2):363-377.

[104] Shahabi C,Fan L,Nocera L,et al.M.Privacy-preserving inference of social relationships from location data[C]//Proceedings of the 23rd SIGSPATIAL International Conference on Advances in Geographic Information Systems,2015:1-4.

[105] 陈伟鹤,李文静,朱江基.基于社交网络好友攻击的位置隐私保护模型[J].计算机研究与发展,2015,37(4):692-698.

[106] 王玲玲,刘国柱,马春光.位置服务中基于二分图的身份推理攻击算法[J].计算机工程与应用,2016,52(9):67-70.

[107] Schlesinger A,Chandrasekharan E,Masden C A,et al.Situated anonymity:Impacts of anonymity,ephemerality,and hyper-locality on social media[C]//Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems,2017:6912-6924.

[108] 吴铮,于洪涛,刘树新,等.基于信息熵的跨社交网络用户身份识别方法[J].计算机应用,2017,37(8):2374-2480.

[109] Ma H,Cheng H,Yu B,et al.Effects of anonymity,ephemerality,and system routing on cost in social question asking[C]//Proceedings of the ACM on Human-Computer Interaction,July 26-28,2019.

[110] Garms L,Martin K,Ng S L.Reputation schemes for pervasive social networks with anonymity[C]//Proceedings of the 15th Annual Conference on Privacy,Security and Trust,2017.

[111] Jing D,Liu T.Context-based influence maximization with privacy protection in social networks[J].EURASIP Journal on Wireless Communications and Networking,2019,142:1-21.

[112] Qian J W,Li X Y,Wang Y,et al.Social network de-anonymization:More adversarial knowledge,more users re-identified?[J].arXiv:1710.10998,2017.