抵御推断攻击的在线社交网络用户位置隐私保护综述

马 卓[1], 曹玖新[2,3], 王 群[1], 胥 帅[4], 夏玲玲[1]

[1]江苏警官学院计算机信息与网络安全系 南京 中国 210031
[2]东南大学网络空间安全学院 南京 中国 211189
[3]紫金山实验室 南京 中国 211111
[4]南京航空航天大学计算机科学与技术学院 南京 中国 210016

摘要 作为一种通过位置交互连接数字空间和物理空间的新型移动应用, 在线社交网络能够为用户提供实时、便捷的在线服务。用户在使用服务时, 其隐私位置信息因需要提交给在线服务而面临严重的泄露风险, 包括设备劫持攻击、网络中间人攻击和服务器端推断攻击。本文针对服务器环境的潜在风险, 立足在线社交网络的主要特点, 分别对在线社交网络中特定推断攻击和组合推断攻击的防御方法与技术进行综述性研究, 从攻防视角出发清晰呈现在线社交网络用户位置隐私研究的最新进展。首先, 在对在线社交网络的位置服务模式与数据特征深入分析的基础上, 对传统特定攻击场景和新型组合攻击场景下的攻击模型的机理进行了对比与总结。然后, 从可抵御攻击的角度, 对用户位置隐私保护方法的分类进行详细分析。针对特定推断攻击, 将其抵御方法划分为针对解密攻击的数据加密、针对重识别攻击的身份干扰和针对位置推断攻击的位置失真; 针对组合推断攻击, 将其抵御方案归纳为针对三类同角度组合推断攻击的保护方案、针对三类双角度组合推断攻击的保护方案和针对全角度组合推断攻击的保护方案。通过对保护技术解析与归纳, 总结了不同推断攻击抵御方案的区别与特点, 全面描述了抵御效果的评价方法与指标。最后, 对未来在线社交网络中的新型推断攻击与热点隐私保护研究方向进行了总结与展望, 为本领域的研究提供思路指导和方法归纳。

关键词 在线社交网络; 推断攻击; 用户位置隐私
中图法分类号 TP309 **DOI 号** 10.19363/J.cnki.cn10-1380/tn.2026.03.15

A Survey for User Location Privacy Protection Against Inference Attacks in Online Social Networks

MA Zhuo[1], CAO Jiuxin[2,3], WANG Qun[1], XU Shuai[4], XIA Lingling[1]

[1] Department of Computer Information and Cybersecurity, Jiangsu Police Institute, Nanjing 210031, China
[2] School of Cyber Science and Engineering, Southeast University, Nanjing 211189, China
[3] Purple Mountain Laboratories, Nanjing 211111, China
[4] College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China

Abstract As a new type of mobile application that connects digital space and physical space by location interaction, online social networks can provide users with real-time and convenient online services. When users use the service, their private location information is submitted to the service facing a serious risk of disclosure, including hijacking attacks over mobile devices, man-in-the-middle attacks through network and inference attacks in server-side. This paper was targeted at the potential risk in server environment. It was based on the main characteristics of online social networks and conducted a review study on the defense techniques of both the specific and the combinational inference attack in online social networks. The paper started from the perspective of attack and defense to clearly present the latest progress of online social network users' location privacy studies. Firstly, based on the in-depth analysis of service model and data characteristics in online social networks, the mechanism of attack models was compared under the traditional specific attack scenario and new combinatorial attack scenario. Then, the classification of user location privacy protection methods was analyzed against inference attacks. For the defense of the specific inference attacks, it was divided into three parts, including data encryption against decryption attacks, identity jamming against re-identification attacks and location distortion against location inference attacks. For the defense of the combinational inference attack, it contains protection solution against three types of same angle combination inference attack, protection solution against three types of two-angle combination inference attack and protection solution against all-angle combination inference attack. By analyzing and summarizing,

通讯作者: 曹玖新, 博士, 教授, Email: jx.cao@seu.edu.cn。
本课题得到国家重点研发计划 (No. 2021QY2102); 国家自然科学基金 (No. 62172089, No. 62172090, No. 62106045, No. 62202209, No. 62302213); 江苏省自然科学基金项目(No. BK20210280); 中央高校基本科研业务费项目(No. NS2022089); 江苏省网络与信息安全重点实验室(No. BM2003201); 教育部计算机网络与信息集成重点实验室(东南大学资助(93K-9)); 紫金山实验室资助。
收稿日期: 2024-03-20; 修改日期: 2024-08-28; 定稿日期: 2026-01-26

this paper summarized the differences and characteristics of different inference attack defense schemes, and comprehensively described the evaluation methods and indicators of defense effect. Finally, the research direction of inference attack and hot privacy protection issues was summarized and prospected, which provides ideas and methods for the research in this field.

Key words online social network; inference attack; user location privacy

1 引言

随着在线社交网络的兴起和智能移动设备的普及, 一种兼具线上交互和线下位置的新型移动应用——基于位置的社交网络(Location-Based Social Network, LBSN)[1]应运而生, 将网络空间和物理空间紧密地连接起来, 为用户提供实时、便捷的、基于位置的在线服务。用户既可以通过在微博/微信发布附带定位的个人动态来开展线上社交活动, 也可以通过在大众点评/微信提交自己的定位信息来获取附近的美食/好友推荐。与此同时, 上述发布信息被在线社交网络作为一种数据资源收集并存储在服务器中, 但其中往往包含了用户位置隐私。这类私密信息是用户不愿公开的, 一旦泄露, 对平台可信度、平台用户的黏着度和活跃度都会造成不良影响, 同时有可能导致用户的人身安全、财产安全受到侵害。因此, 在在线社交网络中进行用户位置隐私保护具有重要意义, 在保障个人隐私的同时, 促进在线社交网络的良性发展。

用户位置隐私是指在线社交网络用户不愿为人知晓的特定位置信息或与位置相关的身份信息。在在线社交网络中, 用户位置隐私会遭受 3 类攻击: 一是在用户移动设备中遭遇劫持攻击, 二是在网络传输时遭受中间人攻击, 三是在在线社交网络服务器中遭遇推断攻击。本文假设用户的移动设备和网络传输信道是安全的, 重点关注服务器环境给用户位置隐私所带来的潜在威胁。在服务器环境中, 即使用户数据经过隐私保护处理, 攻击者也可以基于在线社交网络用户注册行为多平台化、访问行为周期性、社交好友相似性和定位精细性等主要特点, 并结合已有的背景知识发动相应的攻击来获取特定位置隐私, 称为推断攻击。

推断攻击由在线社交网络中潜在的单个或多个攻击者发动, 从攻击确定性的维度上可以分为 2 类。一是对于确定的单个攻击者, 其所能获取的用户数据和额外的背景知识都确定不变, 并采取自认为最强的攻击模型进行隐私推断, 称为特定推断攻击。二是单个或多个攻击者可以从不同的攻击角度推断不同的用户隐私, 另外, 攻击者获取额外背景知识的能力参差不齐, 存在背景知识不同的攻击者, 这些不确定性形成了组合推断攻击。相比而言, 组合推断攻击是实际更为常见的攻击方式, 同时也为用户行为偏好的精准捕捉、多手段推测埋下了更为严重的隐患。另一方面, 在攻防博弈持续升级过程中, 必然会产生新的攻击类型来进一步补充完善现有的组合推断攻击, 因此组合推断攻击强度较特定推断攻击而言显著提高, 已成为当前在线社交网络中用户位置隐私保护的重点研究内容。

目前, 许多研究人员针对基于位置的服务(Location-Based Service, LBS)的隐私保护技术进行了相关归纳与总结, 但尚未有全面考虑在线社交网络下特定推断和组合推断这两类攻击场景进行综述的研究, 且多数综述研究仅对攻击者进行了简单建模描述而未对攻击模型进行归纳。现有的位置隐私保护技术对本文的研究带来启发, 提供主要的保护理论基础。Jiang 等人[2]将 LBS 按服务持续时间划分为快照类服务和持续类服务, 并针对每一类服务总结了目前位置隐私保护的基本原理和最新发展, 其对于 LBS 的深入研究为本文提炼在线社交网络的服务模式提供借鉴与参考。Wu 等人[3]则从博弈关系的角度出发, 分别讨论了用户之间、用户与服务供应商之间、用户与攻击者之间、服务供应商与攻击者之间的博弈关系及解决方案, 帮助研究人员较为系统全面地了解了移动网络中的位置隐私保护问题, 所研究的保护框架主要面向车载移动网络和手机移动网络的应用场景, 这种从服务场景特点出发的研究思路也对本文的技术路线提供了启发。文献[4]则针对社交网络中的社交关系推理和属性推理及相应的保护分别进行了归纳, 文献[5]还针对在线社交网络的精细化定位这一特点对基于语义的位置隐私保护方法开展综述归纳, 这两篇综述的探索内容具有互补性, 都对于社交网络这一场景的研究思路为本文提供了参考价值。此外, 曹翰林等人[6]从轨迹数据处理的角度对于轨迹数据隐私保护思路进行了简要总结, 为本文抵御位置追踪推断攻击的相关归纳与总结提供理论基础。

基于上述分析, 本文根据在线社交网络的位置服务模式与数据新特点, 归纳了在线社交网络中的特定推断攻击, 并基于攻击组合的机理, 给出了在线社交网络中的组合推断攻击场景; 然后对用户位

置隐私保护方法进行了归纳总结，分析了面向不同推断攻击的不同隐私保护方案的区别与特点，并从隐私保护评价指标的角度展开进一步描述；最后，对未来新型在线社交网络中的推断攻击与热点隐私保护研究方面进行了探讨，为从事相关领域研究的学者提供研究思路和方法归纳。

本文组织结构如图 1 所示，全文共分为 6 节。具体而言，第 2 节基于在线社交网络的基本特征，提出特定推断攻击与组合推断攻击共同构成的攻击场景，并对对应的攻击模型进行归纳与对比。第 3 节对抵御特定推断攻击的用户位置隐私保护分类标准进行介绍。第 4 节对抵御组合推断攻击的用户位置隐私保护方法进行分类总结。第 5 节分别给出了上述位置隐私保护方案在抵御不同推断攻击时所采用的评价方法与指标。本文最后总结全文并展望未来抵御在线社交网络中的推断攻击需要解决的问题和热点研究方向。

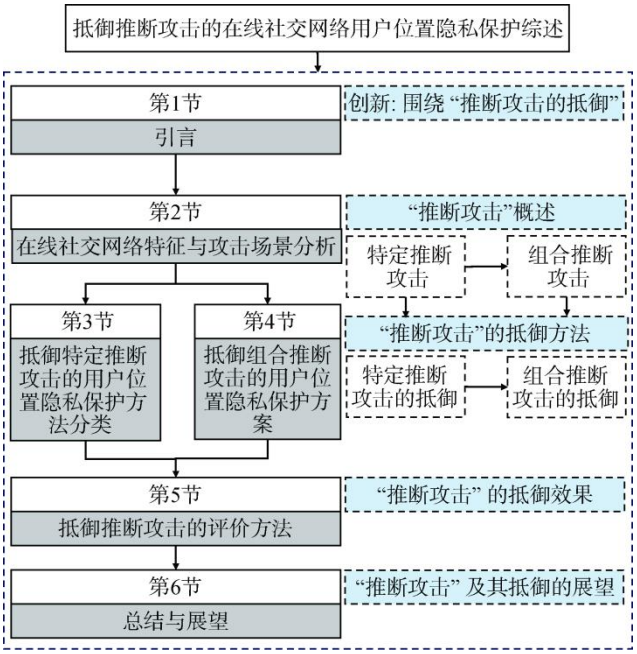

图 1　论文组织结构图

Figure 1　Paper structure diagram

2　在线社交网络特征与攻击场景分析

本节将从在线社交网络中的多样化位置服务模式出发，对在线社交网络的用户注册行为多平台化、用户行为可预测性和位置定义精细化特征进行分析，进而归纳潜在攻击场景。

2.1　在线社交网络的基本特征

在线社交网络的位置服务一般涉及用户和服务供应商这两方角色。在服务过程中用户通过主动/被动地提交带有当前定位信息的请求，获取相应的在线服务；服务供应商在收到用户的服务请求后，将根据用户需求进行响应，提供相应的基于位置的服务，并记录用户使用本次服务的相关信息(包括时空信息)以方便后续的数据分析与挖掘工作。

基于位置服务形成的在线社交网络可以看作由<用户，位置>这两类节点构成的图结构，如图 2 所示，用户间连边表示其在线社交关系，用户与位置之间的连边表示用户对位置的访问行为。在线社交网络数据主要存在以下 4 个新特点:

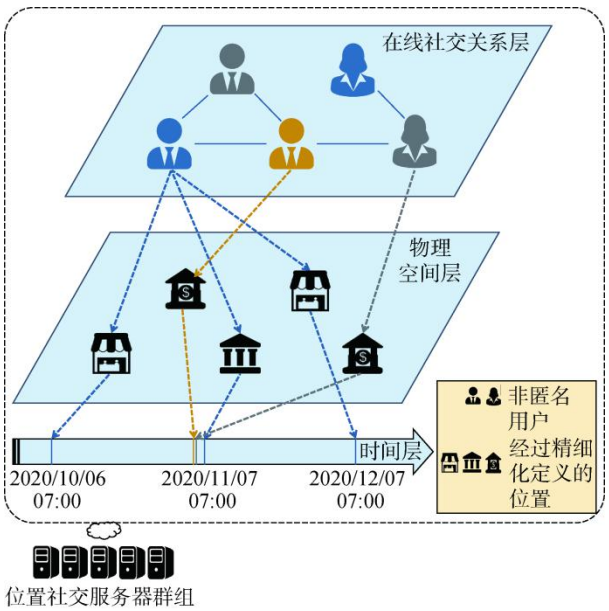

图 2　在线社交网络的网络结构

Figure 2　The network structure of online social network

(1) 用户注册行为多平台化。在传统手机移动网络中，用户可以通过匿名化操作使用基于位置的服务(如在我国手机实名制之前存在的非实名手机)，但身份匿名化在许多在线社交网络中是难以实施的。用户申请账户时必须绑定手机号，并通过号码验证(如 Facebook、微信、新浪微博、大众点评)，这就形成了线上多个虚拟账户之间的对应关系。只要有账户的个人主页信息和行为轨迹信息是真实有效的(如求职平台领英的个人主页信息)，这些真实信息就可成为身份标识信息，这也决定了在线社交网络用户位置隐私的内涵;

(2) 用户访问行为较为稀疏，但仍具有周期性。在传统手机移动网络中，用户的移动轨迹被 GPS 定位并连续记录下来；相比之下，在线社交网络中的用户访问行为只有在用户提交服务请求时才会被服务供应商捕捉到，无法构成连续的访问序列，而呈

现离散形式。但用户访问行为在周模式和日模式的时间窗口映射中仍呈现关联性[1], 存在被攻击的潜在风险, 成为在线社交网络用户位置隐私的重要组成部分;

(3) 用户间存在在线社交关系, 且用户与其好友的访问行为具有相似性。相比于传统手机移动网络, 在线社交网络新引入了在线社交关系, 经统计研究表明, 在线社交网络的用户对于地点的访问偏好会受到其在线好友的影响, 因此, 用户好友的访问行为在一定程度上可以反映用户自身的访问行为, 成为影响在线社交网络用户位置隐私的重要因素;

(4) 位置是经过精细化定义的。与传统手机移动网络中的实时 GPS 位置[7]相比, 在线社交网络中的位置信息虽然也可以采用经纬度坐标表示, 但其本质是含有实际语义信息的位置实体, 包含多定位要素(如地理要素、语义要素), 位置信息的丰富性提升了其被攻击概率, 这进一步丰富了在线社交网络用户位置隐私的内涵。

2.2 在线社交网络中的攻击场景分析

本文重点关注服务器环境给用户位置隐私所带来的潜在威胁, 并给出所研究的潜在攻击场景, 如图 3 所示。用户在使用位置服务时, 其轨迹信息被服务供应商持续收集[2, 8]以支持个性化服务。然而服务供应商是不可信的, 一是因为服务供应商可能会受利益驱动使主动泄露服务器中的用户数据, 例如有研究[9]发现有一半的安卓应用程序(例如 Evernote 和 MySpace)在未经用户知情同意的情况下将其位置信息披露给了第三方广告; 二是因为服务供应商在数据存储和发布的过程中保护力度不够, 仍然存在漏洞。一旦攻击者掌握和利用这些漏洞, 就可以直接获取到服务器中的用户数据。如果服务器中的用户数据未经任何保护处理, 则攻击者可直接获得蕴含位置隐私的用户数据; 如果服务器中的用户数据经过隐私保护处理, 攻击者也可以结合已有的背景知识发动相应的攻击来获取特定位置隐私。

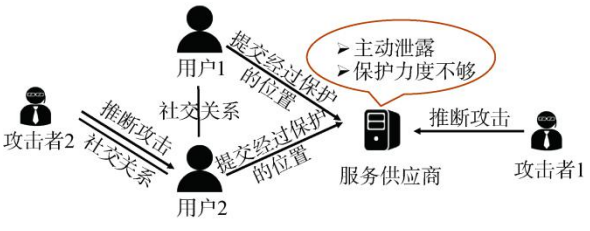

图 3 在线社交网络中面向服务器环境的潜在攻击场景

Figure 3 The potential attack scenario for server-oriented environment in online social network

在此, 本文将面向服务器环境的潜在攻击总体上称为推断攻击, 而位置推断攻击由攻击者基于服务器中被保护的用户隐私数据和攻击者背景知识而发动, 通过推断模型的构建来获取用户的位置隐私。如图 4 所示, 在数据层面, 推断攻击的输入数据由两部分构成, 一是经隐私保护的用户数据, 从被攻破的服务器中获得; 二是攻击者从保护框架之外的任意数据库可以获取到的信息, 称为攻击者的背景知识; 推断攻击的输出数据是用户的隐私位置。在方法层面, 推断攻击通过构建攻击模型从经过保护的用户数据中挖掘对应的隐私位置; 每个攻击者会采取自认为最强的攻击模型, 不同攻击者所采取攻击模型不一定相同。从攻击数量的维度上, 推断攻击可以分为 2 类, 一类推断攻击是唯一确定的, 称为特定推断攻击; 另一类推断攻击包含多个特定推断攻击, 称为组合推断攻击。

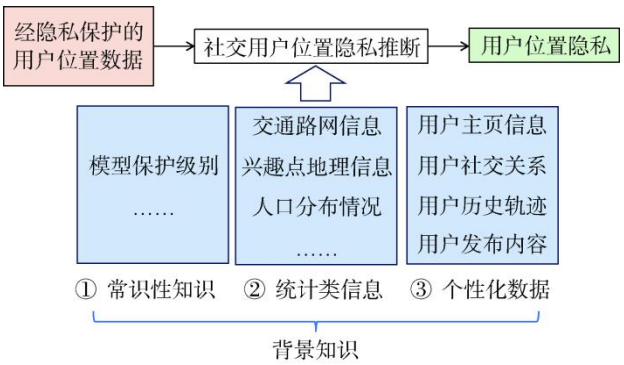

图 4 在线社交网络中已有攻击的逻辑结构

Figure 4 The logical structure of existing attacks in online social network

2.2.1 特定推断攻击方法

特定推断攻击假设攻击者获取的用户数据和额外的背景知识都确定不变, 此时攻击者想要推断的用户隐私也确定不变, 攻击者会采取自认为最强的攻击模型进行隐私推断。如表 1 所示, 从攻击者使用的用户数据来看, 特定推断攻击可以被划分为 3 类: **解密攻击、重识别攻击、位置推断攻击**, 每种特定推断攻击的形式化定义如下。

(1) **解密攻击 H_d**: 对于含有位置隐私的加密用户数据 C, 攻击者可能另外掌握相应的明文 M、加密算法 Enc(M,K)或解密算法 Dec(C,K), 此时采用传统的密码学攻击方式 H_d[10-13]对密钥 K 进行解密攻击, 具体过程可以表示为

$$K = H_d(C, \prod) \tag{1}$$

其中, $\prod$表示攻击者的背景知识, 即攻击者可能掌握的明文 M、加密算法 Enc(M,K)或解密算法 Dec(C,K)。$\prod$也可能为空, 表示攻击者没有额外的背景知识。

表 1 不同特定推断攻击的分析与比较

Table 1 Analysis and comparison of different specific inference attacks

攻击类型	攻击交互性	攻击名称	攻击模型输入		攻击模型输出	常见攻击模型	代表方案
			攻击者使用的用户数据	攻击者背景知识	隐私推断目标		
解密攻击	被动攻击	唯密文攻击	仅密文	-	含位置隐私的明文或密钥	穷举	[10]
		已知明文攻击	含位置隐私的部分明文和密文对	-	密钥和加密算法	面向密钥重用的攻击或频率分析	[11], [21]
	主动攻击	选择明文攻击	含位置隐私的选定明文和对应密文	加密算法	密钥	基于皮尔逊相关系数的攻击	[12], [22], [23]
		选择密文攻击	含位置隐私的选定密文和对应明文	-	密钥	针对公钥密码体制的攻击	[13]
重识别攻击	被动攻击	链式攻击	匿名精确社交轨迹集合以及相对应的用户(身份)标识集合	相对应的用户社交主题集合或该轨迹数据集的多次公开记录	用户(身份)标识与其访问记录间的关联关系	关键字搜索缩小范围	[24]
		重构攻击	合成的社交用户轨迹数据集	-		基于对抗网络的攻击	[25], [26], [27]
		同质化攻击	匿名精确轨迹及对应的位置语义等敏感属性信息	-		基于位置语义或查询语义的攻击	[28]
位置推断攻击	被动攻击	位置依赖攻击	模糊轨迹	社交用户对位置的先验访问概率或社交用户的最大运动速度、社交用户共现记录等用户运动模式	社交用户所在的真实位置	机会选择优先模型，基于马尔可夫模型或条件随机场的贝叶斯攻击或最优化攻击	[9], [15], [16], [29], [30], [31], [9], [32], [33]
		长期观测攻击	社交用户从同一地点提交的模糊位置序列	-		基于频率统计的逆向攻击	[34]
	主动攻击	位置注入攻击	攻击者在社交用户附近并注入虚假位置	-		三角定位和空间分割策略	[17-20]
		位置重放攻击	攻击者将推测位置重新代入保护算法	-		穷举	-

(2) **重识别攻击 H_{r}**: 对于明文匿名轨迹集合 A, 攻击者可以通过重识别攻击 H_{r} 来分辨用户 i' 的身份信息与匿名集合 A 中任意轨迹 j 的匹配程度 $P_{i'\to j}$[14](其中 $j\in A$), 具体过程可以定义为

$$P_{i'\to j}=H_{\mathrm{r}}\left(i',A,\prod\right)\quad\left(j\in A\right)\tag{2}$$

其中, $\prod$ 表示攻击者额外掌握的背景知识, $\prod$ 也可能为空, 表示攻击者没有额外的背景知识。

(3) **位置推断攻击 H_l**: 对于明文模糊位置 v_{o}, 攻击者可以利用位置推断攻击 H_l 来推断用户的真实位置信息 v_{r}[15-20]。具体推断框架有两种, 包括概率框架和最优化框架。在概率框架下, 攻击者需要求解真实位置为 v_{r} 的可能性, 往往将位置推断攻击 $H_l(v_{\mathrm{r}}|v_{\mathrm{o}},t,\prod)$ 表示为后验概率的形式, 并采用一定的模型假设进行估计; 在最优化框架下, 攻击者会尽可能降低位置推断攻击 H_l 所引起的期望误差 EXPDIST, 最终的优化目标可以表示为

$$\min_{H}\mathrm{EXPDIST}(G,H,\prod\mathrm{DIST})\tag{3}$$

其中, G 表示当前保护机制, $\prod$ 表示攻击者额外掌握的背景知识, DIST 用于度量真实位置 r 与模糊位置 o 之间的距离。

这三类攻击在用户数据的攻击角度上互相补充, 构成了在线社交网络的基础攻击体系, 是在线社交网络组合推断攻击的重要基础。此外, 从攻击者与位置服务交互的维度上, 特定攻击模型可以被划分为被动攻击模型和主动攻击模型。被动攻击模型仅通过监听和分析的方式获取服务器中的用户数据, 而主动攻击模型则通过主动改写或添加用户数据流进一步获取用户位置隐私的相关信息。

2.2.2 组合推断攻击方法

组合推断攻击是由若干特定推断攻击组合而成的, 如图 5 所示。从攻击维度上, 组合推断攻击可以分为 2 类。一类组合推断攻击由单个或多个攻击者发动, 从不同的攻击角度推断不同的用户隐私。根据 2.2 节分析, 在线社交网络呈现用户注册行为多平台化、用户行为周期性的主要特点, 这些特点充分支持了关联身份统一性评估、空间位移趋势分析、时空重叠分析等多样化的攻击视角, 构成多角度组合推

断攻击[35-39,40]。另一类组合推断攻击的攻击者采用统一的攻击视角, 构成同角度组合推断攻击[41-43]。给定一组特定推断攻击 $\{H_0(U_0,\Pi_0),\cdots,H_X(U_X,\Pi_X)\}$, 其中, $H_X(U_X,\Pi_X)$ 表示第 X 个特定推断攻击 $H_X(\cdot)$, 该攻击所利用的用户数据为 U_X, 该攻击所需要的背景知识为 Π_X。这组特定推断攻击所利用用户数据 $\{U_0,\cdots,U_X\}$ 的表示空间为 $\theta_U \subseteq \{C,(i',A),|v_o,t|\}$, 其中, C、(i',A)、(v_o,t)分别表示加密用户数据、明文轨迹信息和明文位置信息。在此, 将攻击所利用用户数据的表示复杂度定义为其所对应表示空间的元素个数, 即 $|\theta_U|$, $|\theta_U|$ 的取值范围为[1,4]。当且仅当该组攻击所利用用户数据的表示复杂度 $|\theta_U|>1$ 时, 该组攻击为多角度组合推断攻击; 当 $|\theta_U|=1$ 时, 该组攻击为同角度组合推断攻击。

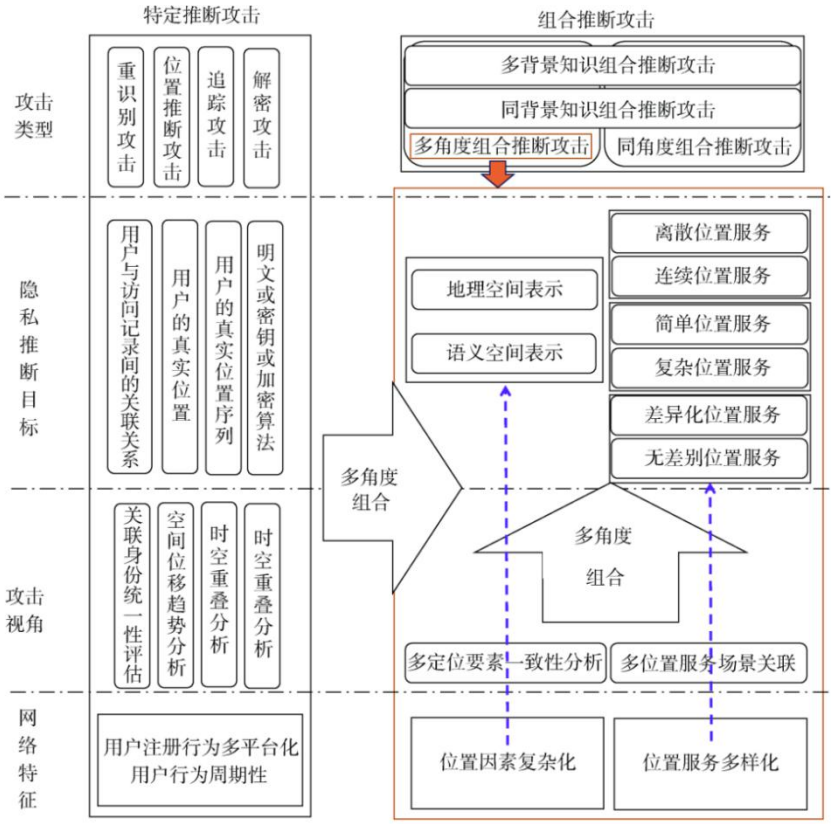

图 5 在线社交网络组合推断攻击与特定推断攻击间的关系示意图

Figure 5 Diagram of the relationship between combinational inference attacks and specific inference attacks in online social network

此外, 根据组合推断攻击与特定推断攻击的对应关系可以推知: 在攻防博弈持续升级的过程中, 必然会源源不断地补充产生新的攻击类型, 由此形成一个开放的在线社交网络组合推断攻击体系。

3 抵御特定推断攻击的用户位置隐私保护方法分类

在在线社交网络中, 用户位置隐私的保护往往针对需要抵御的攻击模式, 采取相应的保护机制(*k*-匿名性、差分隐私、事实隐私), 设计相应的保护方法(数据加密、身份干扰、位置失真), 构建保护框架(也称为保护方案)。该框架在实际应用中还将考虑与部署环境的交互, 形成一个完整的保护系统。本节将针对位置隐私保护的系统结构和抵御攻击类型进行分析和总结。

3.1 按传统系统结构划分

从系统设计角度出发的位置隐私保护方案, 按照其体系结构类型分为集中式体系结构和分布式体系结构两大类。集中式体系结构的保护方案往往需要在用户与服务供应商之间引入可信的第三方(如中心匿名服务器、隐私代理等), 通过第三方服务器对位置数据进行模糊操作或对用户真实身份进行隐藏操作, 从而实现对于用户位置隐私的保护。而分布式体系结构则不依赖于第三方服务器, 其中以用户为

中心的隐私保护方案, 可以看作一种特殊的不存在分布式协作的分布式体系结构。这两类系统的优缺点比较详见表 2。

3.2 按抵御攻击类型划分

当前, 学术界针对用户位置隐私保护研究已经取得了较好的成果, 站在特定推断攻击的角度, 现有位置隐私保护方法可分为三类。

(1) 针对解密攻击的数据加密$\mathbf{Pr_E}$: 对于用户需提交的位置数据 M, 利用加密技术设计一套加密算法M'=Enc(M,K)和对应的解密算法 Dec(C,K)来进行位置隐私保护。具体而言, 用户通过提交加密后的位置M'并对所获得的服务返回 C 在本地或服务器端通过 Dec(C,K)过程解密, 实现相应的位置服务体验。保护方法通常包含基于私人信息检索(Private Information Retrieval, PIR)协议和基于同态加密方法等两类。

表 2 集中式体系结构与分布式体系结构的位置隐私保护方案间的比较

Table 2 Comparison of location privacy protection schemes between centralized architecture and distributed architecture

方案类别	优点	缺点	代表方法
集中式体系结构的位置隐私保护方案	①服务器集中, 方便管理; ②响应时间快	①性能提升有瓶颈。 ②存在单点失效的问题。 ③第三方服务器被攻击, 则会严重泄露用户隐私。 ④需量化用户对第三方的信任	身份干扰类的假名方法, 位置失真
分布式体系结构的位置隐私保护方案	①不涉及可信第三方; ②不存在单点失效, 系统更加可靠	对于大多数的分布式方案, 都面临: ①分布式协作, 需大量通信, 易过载。 对于非加密的分布式方案, 还面临: ②用户间的同步问题。 ③服务延迟。 ④组内恶意成员会使得保护失效	数据加密, 身份干扰类的随机化方法, 位置失真

私有信息检索协议[44-45]是将用户在位置服务的加密查询请求M'与数据库中相应记录的索引值 X 进行私密的匹配得到 C=XM', 并在本地使用 Dec(C,K)解密使得数据服务器不知道用户检索的具体内容。PIR 协议主要可分为两类: 一类是计算性私有信息检索(Computational PIR, C-PIR)协议[45], 将私密匹配工作转移到不联网的单台计算设备上, 但这种方法的计算资源受到了限制, 对于移动用户而言缺乏便携性; 另一类是信息论私有信息检索(Information Theoretic PIR, IT-PIR)协议[46], 将私密匹配的计算工作布置在 n 台互联的服务器之上, 这里查询结果可以表示为 C=$X_1M'_1\oplus\cdots\oplus X_nM'_n$, 其中用户向第 s 台服务器提交的加密查询请求为M'_s, 而该服务器中的记录索引值为X_s, 要求服务器之间不共谋。在基于同态加密的位置服务框架[47-48]中, 数据加密技术是为了抵御恶意用户的攻击。位置通过 LBS 公钥在用户端加密为M', 并在用户间进行一定的传输与计算之后被以密文 C 提交给 LBS 服务器。LBS 服务器在收到位置 C 之后在计算中心利用私钥K_s和 Dec(C,K_s)过程解密。最终, 可对选择明文攻击实现密文与随机序列的不可区分性[23]。

(2) 针对重识别攻击的身份干扰$\mathbf{Pr_F}$: 对于用户在 t 时刻需提交的真实位置v_r和查询语义q_r, 可表示为三元组(t,v_r,q_r), 记作一次真实查询Q_r; 经过身份干扰的保护后将向服务器发送真假混合的匿名查询集 set(Q_r+Q_f)以获得位置服务的答复, 其中Q_f为虚假查询(t,v_f,q_f)。利用身份干扰技术进行位置隐私保护的方法, 通常包含假名方法和随机化方法。

对于假名方法, 用户采用假名或别名进行通信, 通过特定区域 Mix-zone[14]向用户提供假名交换, 以切断用户身份与位置(或轨迹)的联系, 使得用户当前所提交的位置信息至少与其他 k-1 个用户提交的位置信息在 Mix-zone 内无法分辨, 在此对于用户而言, 其他 k-1 个用户提交的位置信息可被认为是虚假信息, 但用户长时间停留的地点仍会暴露他们真实的身份; 随机化方法[49]则通过同时发布哑元位置与真实位置的混合来增加用户数据的不确定性。

(3) 针对位置推断攻击的位置失真$\mathbf{Pr_O}$: 对用户的真实位置信息v_r通过不同的算法进行失真化处理, 最终生成模糊位置v_o以达到保护效果, 主要包括隐匿方法[50]和扰动方法[15]等。其中, 隐匿方法通过将细粒度的位置或时间信息粗粒度化来增加用户数据的不确定性, 而扰动方法则通过对真实位置的扰动得到有偏差的定位信息来增加用户数据的不确定性。这两类方案既可采用集中式体系结构, 也可基于用户终端构建、采用分布式体系结构构建, 后者可消除

可信第三方的系统瓶颈, 为在线社交网络用户提供可行的在线保护。

以上这三大类保护方法主要从系统设计和用户的角度出发为位置隐私的保护提供了相应的解决方案, 这些方案之间具体的比较如表 3 所示。

4 抵御组合推断攻击的用户位置隐私保护方案

在面临组合推断攻击时, 研究学者以特定推断攻击的抵御方法为基础, 针对具体的攻击组合设计了相应的用户位置隐私保护方案。在此, 按照同角度组合推断攻击的抵御方案和多角度组合推断攻击的抵御方案进行展开。值得注意的是, 这些保护方案并不仅限于特定推断攻击所对应保护方案的简单叠加, 还由此衍生了缓存协作和访问控制等通用保护方案。

4.1 抵御同角度组合推断攻击的保护方案

在同角度组合推断攻击中, 潜在攻击者采用统一的攻击视角, 可能发动组合解密攻击、组合重识别攻击和组合位置推断攻击, 其对应的保护方案多为特定保护方法的叠加实现。

表 3 位置隐私保护方法的归纳与比较

Table 3 Summary and comparison of location privacy protection methods

角度	类别	方法名称	特点	局限性	代表方案
系统设计	集中式体系结构	假名方法	用户采用假名或别名进行通信, 以切断用户身份与位置的联系	①单独使用时, 可以通过用户所在的位置推断其真实身份; ②过量的通信和延迟	Mix-Zone[14]
		位置失真「隐匿方法」	将细粒度的位置或时间信息粗粒度化, 增加数据的不确定性	当隐私保护程度高时, 隐匿提交的位置面积会很大, 此时可能会造成高通信量和低服务质量	[51], Casper[52], HHScloak[50].
		位置失真「扰动方法」	通过修改真实位置, 提交一个有偏差的定位信息	可能引起服务质量的损失	[15]
		数据加密	通过加密方法保护用户数据	需要大量的计算量, 资源占用量大, 通信代价高	[44-45, 47-48].
用户	分布式体系结构	位置失真「扰动方法」	通过修改真实位置, 提交一个有偏差的定位信息	可能引起服务质量的损失	[9, 30, 53-54], AdaTrace[55].
		位置失真「随机化方法」	通过哑元与真实位置的混合来混淆视听	①在连续查询中, 生成的哑元位置可能与真实对象移动特征具有很大的差别, 则哑元位置的迷惑性可能降低; ②浪费服务器资源	[49, 56]

4.1.1 抵御组合解密攻击的保护方案

(1) 形式化概述

在抵御组合解密攻击 $\{H_{d_0},\cdots,H_{d_X}\}$ 的位置隐私保护方案中, 数据加密最典型的两种技术——私有信息检索技术和全同态加密技术都可分别用于抵御这类组合推断攻击, 形成基于数据加密的保护方案 $\{\mathrm{Pr}_{\mathrm{E}_0},\cdots,\mathrm{Pr}_{\mathrm{E}_Y}\,|Y\geq 0\}$, 但在计算和通信方面存在巨大开销, 因此, 这类保护方案在实践应用中仍存在难度。

(2) 具体方案分析

目前, 大多组合解密攻击都为选择明文攻击和任一解密攻击的同角度叠加。Zhang 等人[57]基于 IT-PIR 协议和双服务器模型提出一种面向任意几何范围查询的移动群智感知位置隐私保护方案, 该方案利用了多项式拟合和随机矩阵乘法技术, 能够在不泄露数据请求者敏感位置隐私的前提下找到位于查询用户任意几何范围内的工作节点, 通过理论证明可以抵御唯密文攻击和选择明文攻击这两类攻击。文献[58]面向将数据和计算外包到云的众包应用, 允许用户自己对发出的每一条查询规定其隐私保护级别, 以防止云服务商探查到用户的查询意图, 保护用户的查询隐私; 同时使用了基于密钥策略的属性加密, 还可抵御选择明文攻击。此外, 还有研究[59]基于属性基加密、线性加密和 RSA 加密提出了一种保护查询用户隐私的时空关键字搜索框架, 所得到的保护方案经理论分析可成功抵御选择明文攻击、选择关键字攻击和外部关键字推断攻击, 同时通过实验证明在面对大量密文时其搜索效率得到了显著提升。其中, 对选择明文攻击的抵御用以保证当攻击者仅获得密钥而无法解密密文时将无法获取移动用户发布的内容信息; 对选择关键字攻击的抵御用以保证保护框架构建的索引不会向攻击者泄露任何关键字信息; 而对外部关键字攻击的抵御则用以保证保护框架中的后门不会向潜在攻击者泄露任何关键字信息。这里的组合推断攻击由解密攻击与保护框架引入的额外攻击等不同目标的攻击组成。

此外, 针对其他的组合解密攻击方式, Zhang 等人[41]提出了 PTCPIR 模型, 通过将数据空间划分为子空间并允许用户选择扫描的子空间比例, 实现隐私与性能的灵活平衡。该模型设计了一个分层加密的安全索引结构, 以支持高效的子空间信息检索, 抵

御已知背景攻击对用户查询隐私的破坏; 还提出一种混淆查询关键字的生成方法, 以防止服务器通过已知背景攻击利用查询模式推断用户的真实意图。

4.1.2 抵御组合重识别攻击的保护方案

(1) 形式化概述

抵御组合重识别攻击 $\{H_{r_0},\cdots,H_{r_X}\}$ 的位置隐私保护方案主要针对路网中连续查询的应用场景, 需要考虑用户轨迹间和用户轨迹内的拆分片段所面临的两种重识别攻击, 对此, 相关研究主要从以随机化方法为代表的身份干扰 Pr_F 和以隐匿方法为代表的位置失真 Pr_O 着手开展保护方案的设计。

(2) 具体方案分析

常见的组合重识别攻击为链式攻击和重构攻击的同角度叠加。针对这一组合重识别攻击, 往往采用基于隐匿方法的保护方案, 通过同时对至少 k 个用户提供同一个隐匿空间来实现对 k-匿名身份保护。相关研究工作主要从隐匿空间的选择方面开展设计。在基于集中式体系结构的隐匿保护中, 文献[43]面向路网环境提出了兼顾查询执行成本和查询质量的位置隐私保护方案, 可同时抵御重放攻击(攻击者已知保护算法、用户位置集合和目标函数所采用的统计指标, 但不知道用户位置集合所对应的用户身份信息, 攻击者将在给定的模糊片段集合中寻找与给定查询同属于同一查询用户的片段, 即本文的重构攻击)和隐蔽区域中心攻击(攻击者已知用户位置集合, 但不知道用户位置集合所对应的用户身份信息, 基于给定的模糊片段集合和查询信息推断该查询所在的真实位置, 即本文的链式攻击)。而基于分布式体系结构的隐匿保护, 文献[56]设计了一个基于司机智能手机的分布式停驻点分配系统, 基于真实目的地与其地理邻居之间的距离构建满足 k-匿名的隐匿区域, 用于抵御分别针对目的地和针对两次停车之间时空关联性的链式攻击(即本文的重构攻击), 同时可用于抵御司机假名与真实轨迹之间的重识别攻击(即本文的链式攻击), 此外, 相比于集中式停驻点分配系统还节约了旅行时间。

此外, 还有工作针对三个及以上重构攻击的同角度组合研究抵御方法, 这些工作往往采用随机化方法, 从哑元用户移动模式的构造入手。Kang 等人[60]针对在线社交网络中位置因素复杂化的特点提出了新的位置隐私保护手机代理应用 MoveWithMe。该应用考虑了基于不同分类器模型的重构攻击, 从移动模式、日常安排和社交行为等多方面来构建哑元用户的行为模式, 确保哑元用户的移动在语义上不同于真实用户的轨迹并满足地理限制, 并通过实验验证了该应用的实用性、有效性和保护效果。

4.1.3 抵御组合位置推断攻击的保护方案

(1) 形式化概述

抵御组合位置推断攻击 $\{H_{l_0},\cdots,H_{l_X}\}$ 的位置隐私保护方案主要从身份干扰和位置失真这两个角度开展设计, 包含①身份干扰中的假名方法或随机化方法形成保护方案 Pr_F 和②位置失真中的隐匿方法或/和扰动方法, 形成保护方案 $\{Pr_{o_0},\cdots,Pr_{o_Y}\,|Y\geq 0\}$。

(2) 具体方案分析

目前, 大多组合位置推断攻击都为位置依赖攻击和任一位置推断攻击的同角度叠加。为抵御这类组合位置推断攻击, 存在两类保护方案。

①身份干扰类保护方案: 文献[8]基于假名方法设计最优的无线接入方案, 该方案将无线网络的覆盖区域天然看作一个圆形的 Mix-zone, 针对位置推断攻击(推断用户当前位置)和追踪攻击(推断用户未来路径)设计了三种位置隐私度量指标, 用以捕捉周围环境对用户位置隐私的影响, 并将上述指标用于构建基于最优停止、隐私感知的无线接入方案。文献[52]提出一种基于半可信第三方服务器的随机化位置保护系统结构, 针对攻击者的位置同质性攻击, 提出了一种基于假位置和位置偏移的位置匿名算法; 针对攻击者的位置依赖攻击, 引入斯坦伯格博弈模型对匿名结果进行优化; 最终通过基于滴滴打车数据集的实验证明, 算法可以在满足服务质量要求的前提下保证用户的位置隐私。还有一类随机化方法在构造哑元用户时主要考虑由于攻击者多样化所引入的组合攻击, 文献[61]分别考虑了攻击者仅能获得单次查询信息和攻击者可获得两次查询信息来分别组织最优的位置推断攻击, 并通过贝叶斯博弈对用户与攻击者之间的攻防交互进行建模分析并提出相应的位置提交策略, 最终实验表明所提方法在较小的 k 值下($k\leqslant 3$)明显优于 k-匿名机制。此外, 梁慧超等人[55]针对路网中潜在的位置重放攻击和位置依赖攻击提出哑元集合的构建方法, 使得攻击者识别真实用户位置的概率不大于 $1/k$。

②位置失真类保护方案: 在扰动方法中, 针对服务多样化的特点, 文献[54]设计了一种兼顾了用户在连续使用位置服务时的位置隐私保护方案, 在权衡服务质量损失的同时, 可保护用户当前位置和整条轨迹的差分隐私。还有扰动方案在攻防交替升级的过程中持续涌现出来, 文献[51]发现了一种长期观测攻击, 该攻击表明用户的行为可能被收集并存储

一段时间, 这些累积的信息可能被攻击者利用进行推断攻击来获取某些敏感信息。这种新型攻击对能够成功抵御贝叶斯推断攻击和最优推断攻击等短期观测攻击的保护框架带来了新的威胁, 因此, 文献[51]通过对地理不可区分性、k-匿名性和推断误差期望这三种隐私度量标准进行组合提出了新的保护方案, 该方案既可以抵御位置依赖攻击中的贝叶斯推断攻击和最优推断攻击, 又可以抵御长期观测攻击。Zheng 等人[62]发现了针对数据隐私(可抵御从扰动位置 z 推断真实位置 x_j 和 x_{j+1} 的位置推断攻击)和针对语义隐私(可抵御基于兴趣点分布和扰动轨迹的访问语义推断攻击)的位置推断攻击, 并针对这种组合攻击场景提出了一种基于语义感知和隐私保护的在线位置共享机制, 经基于私家车轨迹数据集的实验验证, 新构造方案在保护数据隐私和语义隐私方面具有有效性。文献[63]也兼顾了用户定位的地理要素和语义要素, 研究了 3D 空间地理不可区分性, 并解决了复杂 3D 空间下的维度灾难问题, 最终基于强化学习方法实现了对用户地理位置隐私和语义位置隐私的双重保护。

4.2 抵御多角度组合推断攻击的保护方案

面向多角度组合推断攻击的保护方案根据攻击角度数量可分为面向双角度组合推断攻击的保护方案和面向全角度组合推断攻击的保护方案。

这些保护方案主要包含特定保护方案的有机组合和通用保护方案的提出与实现。在此, 通用保护方案主要是指缓存协作、访问控制、身份干扰和位置失真这四种保护方案。下面介绍前两种新的通用保护。

(1) 访问控制保护方案$\mathrm{Pr}_{\mathrm{AC}}$: 该方案通过建立位置服务中信息管理政策和访问规则来对用户个人信息的访问、存储和使用进行限制, 往往可以抵御多种不同的推断攻击。但访问控制保护方案的落地实施依赖于服务供应商的实际配合, 如图 6 所示, 其中最基本的原则是服务供应商在访问、存储和使用用户的个人信息时应当告知用户并获得其授权, 主要考虑对重识别攻击和位置推断攻击的抵御能力。

(2) 缓存协作$\mathrm{Pr}_{\mathrm{C2}}$: 该方案往往依靠用户之间的协作, 借助自己或地理邻居的手持设备来缓存自己即将访问的地点信息, 以此来减少查询次数, 保护自己当前的位置隐私信息。基于缓存协作的保护方案往往依托于分布式体系结构。如图 7 所示, 在这一体系结构中, 用户往往依靠相互之间的协作, 借助多级 Cache[65]或其他用户的手持设备[66]来缓存自己即将访问的地点信息, 以此来减少查询次数, 保护自己当前的位置隐私信息。然而这类保护方案由于依托地理相邻用户之间的协作, 往往面临恶意节点对用户身份和定位信息发起的双重推断攻击, 因此在设计时大多需要考虑对重识别攻击和位置推断攻击的抵御能力。

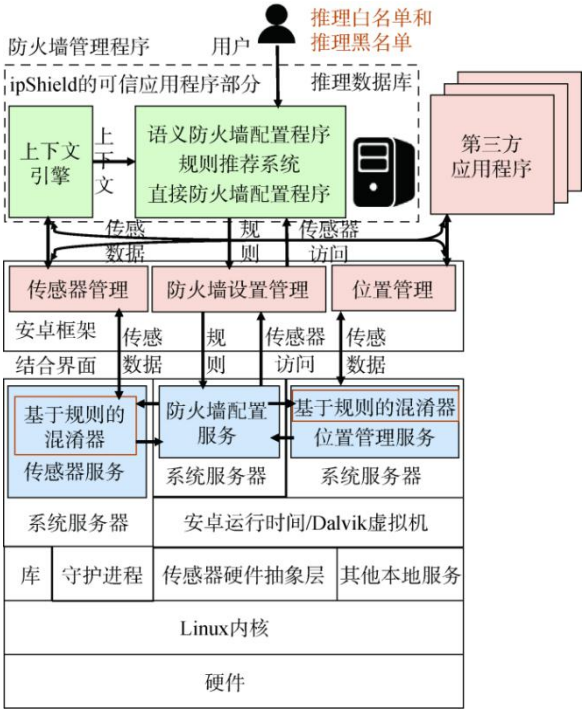

图 6 以 ipShield[64]为例的访问控制保护示意图

Figure 6 Protection diagram of access control using ipShield[64] as an example

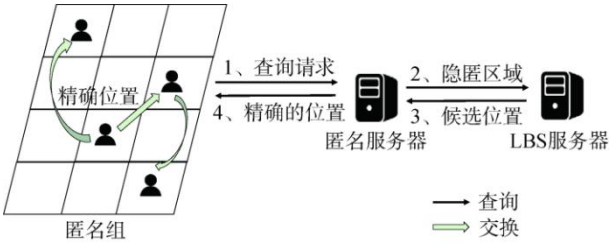

图 7 借助第三方匿名服务器的缓存协作保护示意图

Figure 7 Protection diagram of caching and cooperation using a third-party anonymous server

4.2.1 面向双角度组合推断攻击的保护方案

(1) 面向加密和重识别的双角度组合推断攻击抵御

相关研究利用缓存协作$\mathrm{Pr}_{\mathrm{C2}}$或混合保护构建抵御方案。在基于缓存协作的保护方案$\mathrm{Pr}_{\mathrm{C2}}$中, Zhang 等人[36]针对连续位置服务采用了两级缓存机制, 并在隐蔽区域形成的过程中, 提出的隐蔽区域机制通过考虑用户移动方向来提高命中率, 最终经过安全性分析表明所设计的保护方案能够抵御链式攻击以及窃听攻击(即本文的解密攻击)中的唯密文攻击和

已知明文攻击。宋成等人[67]基于拉普拉斯噪声对用户轨迹进行失真保护, 同时利用椭圆曲线离散对数对用户身份进行加密, 形成的混合保护方案{$\mathrm{Pr_E}$,$\mathrm{Pr_O}$}可用于抵御假冒攻击(即本文的唯密文攻击)、选择明文攻击和链式攻击。

(2) 面向重识别和位置推断的双角度组合攻击抵御

相关研究利用缓存协作$\mathrm{Pr_{C2}}$、访问控制$\mathrm{Pr_{AC}}$、身份干扰、位置失真或混合保护等构建抵御方案。在基于缓存协作的保护方案$\mathrm{Pr_{C2}}$中, Nisha 等人[37]则通过考虑攻防博弈过程中引入的推断攻击, 提出用户通过与地理空间邻近的其他用户建立临时群组来访问本地化的服务, 从而减少与不可信位置服务器的交互。该方案采用了基于群组内权威的身份认证机制和虚拟身份机制来保障用户的身份隐私, 防止用户身份受到盗取攻击(即本文的重构攻击)和错误节点攻击(即本文的位置注入攻击)。还有缓存协作方案考虑了服务多样化的情况。针对用户在使用查询或参与协作时面临的不同潜在攻击, Zhu 等人[38]设计了一种基于用户协作的查询信息分割交换方案, 既可以对用户查询时所提交的位置信息提供保护, 又可以保护用户参与协作时的位置隐私。文献[39]考虑了连续协作过程中的不同攻击方式, 基于协作用户间可信程度设计了缓存协作模型, 用于抵御基于定点观测的身份识别攻击(即本文的链式攻击)、基于高频访问的重识别攻击(即本文的重构攻击)、位置依赖推断攻击和长期观测攻击等四类潜在的攻击。

而基于访问控制的保护方案$\mathrm{Pr_{AC}}$往往考虑攻击者多样化的情况, 最著名的访问控制保护方案为国际互联网工程任务组(The Internet Engineering Task Force, IETF)提出的 Geopriv 访问控制协议[68], 该服务协议考虑了三种威胁(即协议威胁、存储威胁和信息滥用的威胁), 旨在对位置信息在 Internet 协议中的合理表示和安全传送给出一个具有普适性的规范说明, 进而抵御三大类具有不同方面(传输协议、存储机制、用户信息发布机制)背景知识的攻击者。此后, 针对在线社交网络提供的基于位置的服务, 有研究[64]提出了一种手机传感器的监控架构 ipShield(如图 6 所示), 该架构会对传感器的授权进行隐私风险评估, 并将可能造成的攻击列表推送给用户, 该框架加强了用户在应用服务运行期间对数据分享的控制能力, 同时根据偏好感知实现了个性化的隐私设置推荐, 并通过攻击列表定义有待抵御的攻击组合。文献[40]则提出了一种面向社交网络用户的属性隐私泄露风险评估框架, 该框架收集了在线社交网络中潜在的多种属性推断攻击模型, 以用于评估用户属性隐私(如当前所在城市、性别和年龄)被正确预测的可能性。对于暴露风险较高的用户, F-PAD 在隐藏某些暴露属性的同时, 通过通知用户自身的风险变化, 提供相应的对策, 同时有助于政府或组织的监管部门制定社交网络隐私标准。文献[49]基于用户当前和历史的位置社交信息进行访问控制决策, 提出一种面向在线社交网络内部来自共谋社区、邻近威胁和可疑用户的组合推断攻击的访问控制框架, 并通过大量仿真实验评估所提框架, 验证其有效、高效和可扩展。

此外, 基于假名法的设计方案$\mathrm{Pr_F}$大多针对路网的实际应用背景, 往往也会因此在设计时大多需要考虑对重识别攻击和位置推断攻击的抵御能力。从攻击者多样化的角度出发, 文献[35]讨论了应对定时攻击(即本文的重构攻击)、转移攻击(即本文的位置依赖推断攻击)和组合定时转移攻击的用户位置隐私保护方案, 通过同时考虑 Mix-zone 的几何形状(如图 8 所示)、用户人口统计以及用户移动模式在空间和速度方面的限制, 设计了一种有效的 Mix-zone 框架 MobiMix, 向路网用户提供了对不同位置依赖攻击的更强防护。考虑到多样化服务中存在的连续位置服务, 文献[69]在文献[35]所提出攻击的基础上, 考虑了一种新的重构攻击——连续查询关联攻击, 并针对这四种攻击设计并实现了基于时空延迟容忍 Mix-zone 的假名保护方案, 该方案中的 Mix-zone 在时空扰动的用户位置上引入了随机的时间和空间转移, 可在连续查询中获得最高的匿名性, 同时在匿名查询处理成本和匿名查询处理产生的时间延迟之间做出了可接受的权衡。

另外, 在基于随机化的保护方案中, Wu 等人[53]在构造哑元集合的过程中, 同时考虑了用户的位置隐私和查询隐私, 并通过理论分析和实验验证所提方法能够有效地保护 LBS 查询背后的位置隐私、属性隐私以及位置隐私和属性隐私间的语义联系; 文献[70]将众包工作者和众包任务发布者这两类对象的精确位置划分到有噪声的多级网格中, 成功实现了用户在参与众包应用的不同角色时对其位置隐私的保护。而文献[42]则针对路网中潜在的语义同质性攻击和位置重放攻击, 提出了兼顾位置匿名性、分段语义多样性和差分隐私的隐匿保护方案 PrivSem, 并通过基于真实路网数据的大量实验证明了我们所提出保护框架的保护效率和服务有效性。

在混合保护方案中, 中国科学技术大学李卫海等人[71]假设服务供应商和协作用户半可信, 采用了匿名协作和数据扰动形成混合保护方案{$\mathrm{Pr_{C2}}$,$\mathrm{Pr_O}$},

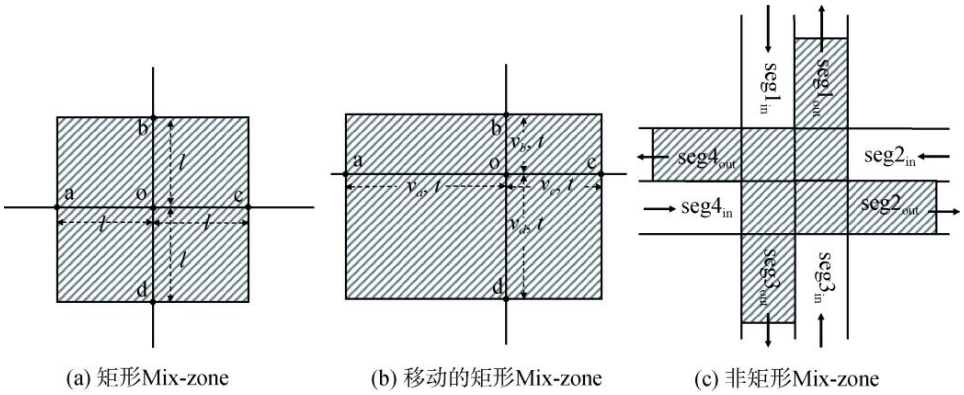

图 8 Mix-zone 形状

Figure 8 Mix-zone shape

可防御关联攻击(即本文的链式攻击)和位置推断攻击。还有方案将假名方法和扰动方法相结合形成保护方案 $\{\mathrm{Pr_F},\mathrm{Pr_{O_0}},\cdots,\mathrm{Pr_{O_Y}}\,|Y\geq 0\}$，文献[72]针对连续的、基于位置的服务场景，采用动态匿名机制、位置选择机制和 k 匿名技术。在最终的保护方案中，当用户选择 k-1 个模糊位置并提交 k 个查询内容的时候，匿名服务器和位置服务器都无法获取用户的轨迹，经验证可抵御共谋攻击(攻击者与匿名服务器共谋)、推断攻击和监听攻击。Shokri 等人[73]则设计了假名方法和扰动方法相结合的混合保护方案$\{\mathrm{Pr_F},\mathrm{Pr_O}\}$用于抵御基于攻击者误差期望的最优化攻击和贝叶斯推断攻击，该方案采用了两步联合保护，首先对个体轨迹进行扰动模糊，然后对个体组成的用户群体进行假名法保护，如图 9 所示，以此保护用户在社交网络发布位置时的相关隐私。

4.2.2 面向全角度组合推断攻击的保护方案

当前，面向全角度组合推断攻击的保护方案开始受到研究界关注，但总体数量仍相对较少，主要难点集中在数据加密与身份干扰和位置失真的有效结合。Wu 等人[74]面向以用户位置隐私、用户查询隐私和服务器数据隐私为目标的三类潜在攻击，讨论了群组内其他用户发起共谋攻击的情况，设计了基于同态加密和随机化保护的近邻搜索框架$\{\mathrm{Pr_E},\mathrm{Pr_F}\}$，对上述三种攻击可起到同时抵御的效果。文献[75]则针对路网环境，假设除用户自身外其他实体均不可信，并基于 Palliar 密码系统的同态特性和假名机制形成混合保护框架$\{\mathrm{Pr_E},\mathrm{Pr_F}\}$，提出了一种无需用户提供真实位置及查询内容的 k 近邻兴趣点查询方法，实现了对用户位置隐私和查询内容隐私的保护及对兴趣点的精确检索，可抵御基于查询内容的链式攻击和位置依赖攻击。田静等人[76]则针对众包计算最短路径的应用，提出一种基于同态加密和安全多方计算的最短路径隐私保护算法，可分别对有障碍物查询和无障碍物查询中的用户(指用户的源/目的地址信息)和 LBS 服务器(指 LBS 服务器中的路网图和冗余的最短路径集合)提供隐私保护。

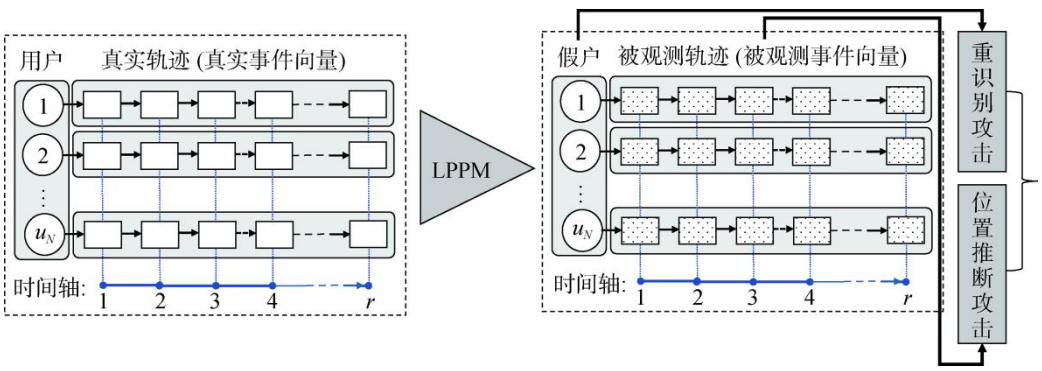

图 9 Shokri 等人提出的位置隐私保护框架，通过假名和扰动保护用户真实轨迹

Figure 9 Location privacy protection framework proposed by Shokri et. al preserve user's real trajectory through pseudonym and perturbation

5 抵御推断攻击的评价方法

按照推断攻击的种类划分, 下面将从特定推断攻击和组合推断攻击的角度归纳评价方法。

5.1 抵御特定推断攻击的评价方法

对于位置隐私保护的评价标准主要从两方面进行归纳, 一是对位置隐私保护程度进行评价的方法与指标归纳, 二是对位置隐私保护所引起的服务质量代价进行评估。

5.1.1 抵御特定推断攻击的保护效果评价指标

位置隐私评价指标是为了评估用户位置隐私保护的性能而提出的。研究界提出了五种比较典型的位置隐私评价指标, 按照是否与攻击事实有关, 本文将这些评价分为基于攻击事实的相对评价和基于理论证明的绝对评价。

(1) 基于理论证明的保护效果评价指标

基于理论证明的评价指标通过明确的定义或过程证明, 对用户位置隐私保护的程度提供绝对评价, 从理论上保证评价结果的绝对正确性。当前能够对位置隐私保护方案提供绝对评价的指标有三种: *k*-匿名性、差分隐私和互信息, 下面将进行依次介绍。

***k*-匿名性(*k*-anonymity)**: 指在基于位置的服务中所涉及的 k 个用户[77]或 k 个位置[78]总体不可区分, 即给定一个用户或位置, 保护将使得该用户或位置隐藏在用户组或位置组中, 并保证该用户或位置能够被猜测的概率不超过 $1/k$。根据 *k*-匿名性的定义, 位置隐私保护方案会采取不同的方法来强制执行这一保证, 因此 k 可作为位置隐私保护框架的参数, 用来表示位置隐私保护的级别。

考虑到 *k*-匿名性针对链式攻击提出, 无法抵御同质化攻击、背景知识攻击、未排序匹配攻击和补充数据攻击等一系列攻击, 学术界又陆续提出了对于 *k*-匿名性的补充概念。*l*-多样性[28]对 *k*-匿名性的匿名组进行属性多样化的限定, 要求匿名组在敏感属性方面都至少有 l 个不同的取值, 可解决同质性攻击和背景知识攻击所带来的隐私泄露问题, 但仍不能防止概率推断攻击; *t*-相近性[79]则是 *l*-差异性的进一步发展, 要求组内每种敏感属性的分布必须与属性在整个数据集的分布尽可能相似, 使其在整体统计中被区分的概率不能超过 t, 通过降低数据表示的粒度来防止该表示类之下的同质性攻击和背景知识攻击。由于 *t*-相近性可防止属性泄露, 但不能防止身份泄露; 因此, 部分研究将 *k*-匿名性和 *t*-相近性结合起来, 用来同时保护用户的身份隐私和属性隐私。

差分隐私(Differential Privacy): 针对数据库查询场景提出, 该指标[80]要求对于聚合数据进行统计查询的结果应不随单个用户的新加入而发生很大改变。在此, 差分隐私被证明可抵御基于任意背景知识的推断攻击。对于社交网络中的用户位置隐私保护, 学界经过概念的衍化提出“地理不可区分性”[33]来保证用户单次使用基于位置的服务时的差分隐私。“地理不可区分性”要求两个位置若地理距离相近则模糊生成某个位置的概率也应当相近。这就意味着如果距离不超过 r 的任意两个位置模糊到某个位置集合的概率分布相似, 则用户在 r 距离的范围内享有εr-隐私, 参数ε代表用户的隐私保护级别[33], 其公式定义表示如下:

$$E[K(v_1)=z]\le \mathrm{e}^{\varepsilon\times d(v_1,v_2)}\times E[K(v_2)=z] \tag{4}$$

其中, v_1和v_2为数据集中的任意两个位置, z 为任意模糊候选位置, 且 $\mathrm{d}(v_1,v_2)<r$。$\mathrm{d}(\cdot)$在此指代欧氏距离。在具体应用时, 地理不可区分性将基于参数ε生成不同类型的噪声(例如, 拉普拉斯噪声或指数噪声), 并通过将噪声添加到保护框架的输出(模糊位置), 以调整发布数据(位置)概率分布的方法来实现对用户位置隐私的保护。在这种保护机制下, ε越小, 保护效果越好(即噪声越大)。

地理不可区分性与 *k*-匿名性原理相比有以下三个特点: ① 由于地理不可区分性是从差分隐私衍化而来的, 因此, 这一指标只能用于衡量基于差分隐私构建的位置隐私保护框架所提供保护的效果; ② 在单次服务中, 基于地理不可区分性构建的位置隐私保护框架不会受到攻击者可能含有的背景知识的影响; ③ 但在多次使用服务时, 地理不可区分性这种指标不再能够抵御所有基于背景知识的攻击, 特别是当攻击者对目标用户的相关位置进行了概率分布统计之后, 该指标将不再能提供对位置隐私保护水平的客观量化和证明[81]。

互信息(Mutual Information): 互信息衡量的是两个随机变量之间相互关联的程度, 被 Zhang 等人[82]提出用于刻画保护前后用户轨迹分布的相似程度, 并以此作为用户轨迹隐私的度量指标, 具体计算公式如下:

$$I(\mathcal{M}_\mathrm{r},\mathcal{M}_\mathrm{o})=\sum\nolimits_{v_\mathrm{o}\in\mathcal{M}_\mathrm{o}}\sum\nolimits_{v_\mathrm{r}\in\mathcal{M}_\mathrm{r}}P(v_\mathrm{r}\in\mathcal{M}_\mathrm{o})\log\left(\frac{P(v_\mathrm{r},v_\mathrm{o})}{P(v_\mathrm{r})P(v_\mathrm{o})}\right) \tag{5}$$

其中, $\mathcal{M}_\mathrm{r}$为用户的真实轨迹, $\mathcal{M}_\mathrm{o}$为用户经过保护的模糊轨迹。此外, 互信息与信息熵、条件熵之间还存在如下关系:

$$I(\mathcal{M}_\mathrm{r},\mathcal{M}_\mathrm{o})=H(\mathcal{M}_\mathrm{r})-H(\mathcal{M}_\mathrm{r}|\mathcal{M}_\mathrm{o}) \tag{6}$$

其中, $H(\mathcal{M}_\mathrm{r})$是轨迹$\mathcal{M}_\mathrm{r}$的信息熵, $H(\mathcal{M}_\mathrm{r}|\mathcal{M}_\mathrm{o})$表示

在观察到$\mathcal{M}_{\mathrm{o}}$时, 其所对应的真实轨迹为$\mathcal{M}_{\mathrm{r}}$的不确定性, 两者相减得到互信息, 刻画了$\mathcal{M}_{\mathrm{o}}$的发布与否对真实轨迹$\mathcal{M}_{\mathrm{r}}$不确定性的影响程度(即$\mathcal{M}_{\mathrm{o}}$发布, $\mathcal{M}_{\mathrm{r}}$的不确定性降低的程度)。

在具体应用中, 互信息指标的使用需要控制两个参数, 一是隐私保护的级别, 二是保护所引起的服务质量损失情况。该指标引入随机变量 Z 用于模拟攻击者拥有额外背景知识的情况, 并结合给定的用户初始定位可能性分布以及其移动概率分布情况, 计算了$\mathcal{M}_{\mathrm{o}}$与$\mathcal{M}_{\mathrm{r}}$间的互信息, 作为实际轨迹隐私损失的上限值。但这一指标考虑的是模糊轨迹$\mathcal{M}_{\mathrm{o}}$在已知真实轨迹$\mathcal{M}_{r}$时的后验概率与$\mathcal{M}_{\mathrm{o}}$先验概率的相对比值大小, 但忽略了$\mathcal{M}_{\mathrm{o}}$先验概率的实际大小, 因此, 当攻击者对目标用户的相关位置进行了概率分布统计之后, 该指标将不再能提供对轨迹隐私保护水平的客观量化和证明。由于这一指标所面临限制与地理不可区分性类似, 互信息被划分为差分隐私的变体。

(2) 基于攻击事实的保护效果评价指标

基于攻击事实的评价指标利用具体攻击的效果对位置隐私保护的效果构建衡量标准, 提供相对评价。当前, 能够对用户位置隐私保护方案提供相对评价的指标主要有两种: 即攻击者误差期望和熵, 下面将对这两种指标进行依次介绍。

估计误差期望(Expected Estimation Error, EE): Shokri 等人针对概率框架所提出的一种攻击评价指标。对于概率框架而言, 这些保护方法会将用户请求服务时提交的真实位置替换为模糊位置, 以此来保护用户的位置隐私; 具体而言, 保护将按照一定概率从模糊位置候选集中选择待提交的位置。在此, 攻击者将对于每一个观察到的模糊位置v_{o}构建猜测候选集, 并对猜测候选集中的每一个位置v_{g}计算其为真实位置的概率 $p(v_{\mathrm{g}}|v_{\mathrm{o}})$, 构成猜测的概率分布(即推断攻击的输出结果)。为评估这一推断结果, Shokri 等人[73]提出了三方面的指标, 依次是准确性(Accuracy)、正确性(Correctness)和确定性(Certainty)。其中, 准确性表示攻击结果的后验概率(即攻击结果的置信度), 置信度越低, 攻击效果越差, 隐私保护效果越好; 正确性表示猜测位置与真实位置的距离期望, 正确性越大, 猜测位置距离真实位置越远, 攻击效果越差, 隐私保护效果越好; 确定性表示攻击者对于猜测结果的确定程度, 用待猜测的候选位置的熵值来衡量, 熵值越大, 待猜测位置的概率分布越均匀, 攻击者的不确定性越大, 攻击效果也越差, 隐私保护效果越好。三个指标的具体计算过程表示如下:

$$\mathrm{EE}_{\mathrm{Acc}} = p(v_{\mathrm{g}}|v_{\mathrm{o}}) \tag{7}$$

$$\mathrm{EE}_{\mathrm{Cor}} = \mathrm{E}_{\chi}\, p(v_{\mathrm{g}}|v_{\mathrm{o}}) d(v_{\mathrm{r}}, v_{\mathrm{g}}) \tag{8}$$

$$\mathrm{EE}_{\mathrm{Cer}} = \mathrm{E}_{\chi}\, p(v_{\mathrm{g}}|v_{\mathrm{o}}) \log \frac{1}{p(v_{\mathrm{g}}|v_{\mathrm{o}})} \tag{9}$$

其中, v_{r}是用户 u 的真实位置, v_{o}为用户 u 提交的模糊位置, v_{g}为攻击者猜测的用户当前位置, $d(\cdot)$ 为衡量两个位置间物理距离的函数, 用测地距离表示。χ 为猜测位置候选集合, v_{g}为χ中的任一位置。

对于这三个指标而言, Shokri 等人[73]经过分析认为: 准确性和确定性并不能全面衡量攻击猜测结果的好坏——即准确性和确定性都很高时, 攻击的正确性依然存在表现不好的情况。例如, 用户在访问新地点时, 提交了以往的模糊位置, 如果依照准确性和确定性指标, 攻击者可能会猜测用户历史访问过的位置, 但该位置可能与用户真实访问的地点相距甚远, 即正确性较低。因此, Shokri 等人认为正确性对于用户隐私水平有本质影响。在具体使用中, 正确性指标可用于量化几种位置隐私保护方法的有效性, 例如扰动方法[16]和差分隐私[33], 但需要控制两个参数, 一是隐私保护的级别, 二是保护所引起的服务质量损失情况。在实际攻防中, 尽管基于攻击事实的正确性指标被明确定义为考虑了具体攻击者的保护机制, 但它仍然受到限制: 由于攻击者的背景知识复杂多样, 难以定性或定量地捕获, 因此, 嵌入在正确性定义中的背景知识很可能与实际数据不一致, 导致量化不准确。

熵(Entropy): 熵[15, 69]是从不确定性角度来评价用户位置隐私保护程度的指标, 它可以直接衡量攻击者对所有猜测候选位置的确定程度, 进而反映出用户位置隐私的保护效果。熵指标通常适用于两类位置隐私保护框架的衡量, 即匿名框架[69]和概率框架[15]。其中, 匿名框架具体包括基于 k-匿名性的隐匿方法、随机化方法、路径扰动方法和基于 mix-zone 区域的假名方法, 这些方法将基于匿名用户的集合, 对集合中用户的定位信息进行交换以保护其位置隐私; 为衡量位置隐私的保护效果, 该框架采用攻击事实的确定性进行定量表示。在此, 潜在攻击者将基于匿名用户的集合, 对每一个观察到的位置进行判断, 输出这一位置属于每一个匿名用户的概率p_{i}, 用来计算攻击的确定性指标(即熵), 具体计算如下:

$$H_I = -\sum_I p_{\mathrm{i}} \cdot \log p_{\mathrm{i}} \tag{10}$$

其中 I 是基于 k-匿名性原理设置的用户匿名集。

对于概率框架下的熵值而言, 具体计算公式可见式(4)。需要注意的是, 熵值可根据攻击者对猜测结果的确定程度来衡量保护框架提供隐私保护的级别,

但这一指标并不能完全刻画隐私保护的效果。具体而言, 熵值高将意味着高度的匿名性。然而, 如果所有位置之间的距离本身就很小(意味着攻击者知道用户的大致位置), 在这样的情况下即使不确定性(熵)很高, 用户的位置隐私将依然受到威胁。此外, 由于熵和攻击者误差期望都是基于具体攻击事实的隐私保护指标, 其所受到的限制也都是相同的, 都无法完全抵御基于其他背景知识的攻击。

5.1.2 抵御特定推断攻击的服务质量评价指标

本节将按照抵御特定推断攻击的分类对其所引起的服务质量损失进行依次介绍。

(1) 抵御数据解密攻击的数据加密保护方法: 这类方案在设计时往往需要考虑实际的计算代价和通信代价。其中, 通信代价往往采用基于协议/算法的分析方式获得; 实际的计算代价衡量的是从用户提交查询给服务器直到服务器将产生结果返回用户之间的 CPU 时间, 包含查询结果在返回给用户之前的压缩过程。这一指标既可以在服务器端进行统计, 也可以在用户端进行统计。

(2) 抵御重识别攻击的身份干扰保护方法: 这类方案中, 假名方法往往需要考虑 mix-zone 区域的面积大小以及mix-zone之间的分布情况, 因为mix-zone区域面积过大会影响用户查询结果精确性, 而 mix-zone 分布过于密集则会导致用户通过 mix-zone 的过程中频繁加入和退出匿名群组, 进而影响连续查询时的用户体验。此外, 假名方法和随机化方法在设计时往往都需要考虑实际的计算代价, 实际的计算代价衡量的也是从用户提交查询给服务器直到服务器将产生结果返回用户之间的 CPU 时间。

(3) 抵御位置推断攻击的位置失真保护方法: 这类方案中, 隐匿方法需要考虑保护算法的计算代价; 而扰动方法采用模糊结果替代用户的真实位置进行提交。从直观上来看, 搜索结果取决于用户提交的位置: 在采用扰动方法进行保护前, 用户提交的位置为实际位置; 在采用扰动方法进行保护后, 用户提交的位置为模糊位置。因此, 这里采用模糊位置与实际位置之间的期望距离来衡量扰动方法导致的服务失真程度。而这一指标在后续使用中也常作为通用的位置效用损失指标, 用于衡量保护引起的效用损失, 而不仅仅限于搜索服务[81]:

$$E_{\text{utility}} = \mathrm{E}||v_{\mathrm{o}} - v_{\mathrm{r}}|| \tag{11}$$

其中, v_{r}是用户 u 的真实位置, v_{o}为用户 u 提交的模糊位置。

5.2 抵御组合推断攻击的评价方法

相比于特定推断攻击, 组合推断攻击往往将具有不同背景知识、带有不同攻击目标或采用不同攻击评价指标的攻击组合在一起。对于保护效果评价指标而言, 面向特定推断攻击的隐私保护评价指标可能是一个, 也可能是多个, 例如 Shokri 等人[73]就提出了准确性、确定性和正确性这三类攻击者期望误差。而面向组合推断攻击的隐私保护评价指标可能是一个, 也可能是多个, 但多为特定推断攻击的隐私保护评价指标的简单组合。表 4 给出了这些隐私保护评价指标与组合攻击之间的联系情况。从表中可以得出, 除差分隐私类评价指标[33]可以抵御任意背景知识攻击外, 尚未发现其他可以抵御组合推断攻击的隐私评价指标。同时, 差分隐私与 k-匿名、推断误差期望的组合[51]已被证实可用于联合评估对于贝叶斯推断攻击、最优推断攻击以及长期观测攻击的抵御效果。

对于服务质量评价指标而言, 为抵御组合推断攻击可以采用缓存协作和访问控制这两种保护方法, 也由此引入了相对应的服务质量评价指标。

(1)基于协作缓存机制的保护方法: 这类方案希望尽可能减少与服务供应商之间的通信, 用缓存中的历史查询结果来替代真实查询结果, 通常使用缓存命中率[86]这一技术指标, 包括本地命中率和合作命中率。本地命中是指用户所需要查找的位置项在移动设备的本地缓存中; 合作命中是指用户所需要查找的位置项在参与协作的移动设备缓存中。

$$\mathcal{H}_{\text{local}} = \frac{\left|\mathcal{R}_{\mathrm{u}} \cap C_{\mathrm{u}}\right|}{\left|\mathcal{R}_{\mathrm{u}}\right|} \tag{12}$$

$$\mathcal{H}_{\text{collaborative}} = \frac{\left|\mathcal{R}_{\mathrm{u}} \cap \mathcal{G}_{\mathrm{u}}\right| - (C_{\mathrm{u}} \cap \mathcal{G}_{\mathrm{u}})}{\left|\mathcal{R}_{\mathrm{u}}\right|} \tag{13}$$

其中, $\mathcal{R}_{\mathrm{u}}$ 是用户 u 不使用协作缓存机制时获得的检索列表, C_{u} 是用户 u 手持设备中缓存的信息, $\mathcal{G}_{\mathrm{u}}$ 为用户 u 的所有地理邻居所缓存的全部信息。

(2) 基于访问控制的保护方法: 这类方案并不需要效用指标, 因为它们几乎不会影响用户使用在线社交网络中的服务。

6 总结与展望

面向在线社交网络的用户位置隐私保护已逐渐成为当今热门研究领域之一。本文面向在线社交网络, 从特定推断攻击和组合推断攻击的角度进行了攻防技术和方法总结, 重点阐述了目前在线社交网络中攻击的组合方式及其对应的保护方案, 分析了攻防关系的发展升级现状。本文立足攻防交替升级的本质, 旨在为广大研究人员快速且较为全面地了解在线社交网络中攻防发展的现状提供综述, 为研究人员针对位置隐私从攻击和保护这

表 4 组合推断攻击的抵御方案及其效果统计表

Table 4 Statistics of defense schemes and their effects against combinatorial inference attacks

		推断攻击														位置隐私指标							服务质量指标			
	保护机制	唯密文攻击	已知明文攻击	选择明文攻击	选择密文攻击	其他解密攻击	链式攻击	重构攻击	其他重识别攻击	同质化攻击	位置依赖攻击	长期观测攻击	位置注入攻击	位置重放攻击	信息理论隐私	k-匿名性	差分隐私	互信息	估计误差期望	熵	其他隐私指标	存储代价	计算代价	通信代价	服务失真程度
(同角度)组合加密攻击的抵御方案	PTCPIR[41]					✓✓										✓								✓	✓	✓
	PPTR[57]	✓		✓											✓							✓	✓	✓	✓	✓
	[58]			✓✓								✓								✓			✓		✓
	PrivSTL[59]			✓		✓✓																	✓		✓
	[83]							✓✓✓									✓							✓	✓
(同角度)组合重识别攻击的抵御方案	[43]						✓	✓							✓	✓							✓		✓
	DFPS[56]						✓	✓								✓									✓
	MoveWithMe[60]							✓✓✓								✓							✓	✓	✓
(同角度)组合位置推断攻击的抵御方案	[8]										✓✓								✓						✓
	Eclipse[51]										✓✓	✓				✓	✓		✓				✓		✓
	[52]									✓	✓					✓			✓					✓	✓
	[54]										✓✓								✓				✓		✓
	[55]										✓			✓		✓							✓		✓
	[61]										✓✓						✓		✓						✓
	[62]									✓	✓							✓✓							✓
	[63]										✓✓							✓							✓
	[84]										✓✓✓						✓						✓		✓
双角度组合推断攻击的抵御方案	[67]	✓		✓			✓														✓		✓		✓
	CPP[36]	✓	✓				✓													✓					✓
	[85]			✓			✓													✓			✓		✓
	[69]							✓				✓								✓					✓
	MobiMix[35]							✓				✓								✓					✓
	Location-Privacy Meter[73]							✓				✓✓				✓			✓						
	[71]						✓				✓						✓						✓	✓	✓
	GCS[37]							✓					✓										✓	✓	✓
	QDER[38]							✓					✓							✓			✓	✓	✓
	CAST[39]						✓	✓			✓	✓				✓							✓	✓	
	[42]									✓				✓		✓	✓						✓		✓
	DPLP[70]							✓	✓		✓					✓	✓						✓		✓
	[53]						✓					✓				✓									✓
	DKM[72]							✓				✓		✓		✓							✓		✓
全角度组合推断攻击的抵御方案	PPGNN[74]												✓										✓	✓	✓
	[75]			✓			✓				✓												✓	✓	✓
	[76]			✓			✓				✓												✓	✓	

两个方面开展研究提供思路与方法。在“万物互联”的大数据时代背景下，用户的位置隐私问题日益凸显，亟待解决，未来对于在线社交网络用户进行位置隐私保护所面临的挑战将从以下两个方面进行总结与展望。

6.1 在线社交网络用户的位置隐私新型攻击机制

(1)基于深度学习的攻击组合机制与评价体系

当前，以 RNN(recurrent neural network)为代表的深度学习模型在时序数据的处理方面展现了优秀的性能优势，完全有可能被潜在攻击者利用来组合开展解密攻击、重识别攻击、位置推断攻击和追踪攻击，形成对在线社交网络用户更具威胁的新型攻击。由此，如何对这些基于深度学习的新型攻击建立评价体系、完善组合机制将成为未来研究的重点内容。具体而言，基于深度学习的新型攻击与基于机器学习的传统攻击之间是否形成互补关系还是替代关系；如果存在互补关系，那么基于深度学习的新型攻击与基于机器学习的传统攻击如何有效组合形成新的攻击体系。上述问题的量化研究对于全面刻画用户隐私特征和深入挖掘用户隐私本质都具有重要作用。

(2) 基于多源异质数据融合的位置隐私组合攻击

大数据时代背景下，在线社交网络数据呈现多源异质的发展态势，传统的简单组合方式已经无法完全适应，而基于多源异质数据融合的位置隐私攻击组合方式亟待发展。一方面，多源的在线社交网络更为全面地记录了用户的线上线下访问经历，为位置隐私攻击提供了更多行为特征，但与此同时，同一用户在不同在线社交网络中的行为模式不尽相同，如何构建有效的数据融合框架与融合算法是这一领域研究人员未来关注的重点；另一方面，在线社交网络中的位置信息往往蕴含在多种异质数据当中，包括经纬度、文本、图像、IP 地址、Wi-Fi 信号等，这些位置信息互为补充，为用户位置隐私提供了层次化立体描述，如何对这些异质数据进行语义融合与对齐也是研究的热点之一。

(3) 结合开源模型自身安全性的组合攻击

大模型时代背景下，越来越多的机器学习模型、深度学习模型和大模型趋于开源化，基于开源模型二次开发形成的保护模型是否能够杜绝训练数据泄露将成为一个重要的研究领域。具体而言，这些开源保护模型能否抵御由成员推断攻击或/和数据提取攻击的引入造成的新型组合攻击，将成为未来用户位置隐私保护的新重点。

6.2 在线社交网络用户的位置隐私完善防御方法

(1) 完善混合保护的组合方案与评价体系

在抵御潜在的组合推断攻击时，传统单一的保护方案所能发挥的作用毕竟有限，混合保护方案的研究将成为目前需要关注的方向之一。在传统保护用户位置隐私的方案中，对于位置隐私保护度评价体系和服务质量保障体系的量化探索仍然不足，这势必也会影响混合保护方案的构建效果。此外，不同保护方案可能会引入不同的潜在攻击，因此，保护方案在混合之后是否会引入新型潜在攻击也是值得关注的问题。在面向在线社交网络组合推断攻击构建混合保护的过程中，对于保护质量构建评价体系、对于服务质量构建保障体系、对于保护方法探索组合方案都是需要充分考虑的问题。

(2) 基于深度学习的位置隐私保护模型压缩技术

在大数据环境下，为抵御基于深度学习的位置隐私潜在攻击，可以利用深度学习技术构建相应的位置隐私保护模型。但这些模型在部署和更新过程中的优化问题也是目前研究学者需要关注的方向之一。为响应绿色低碳节约型社会的建设号召，资源节约型模型的构建值得深入探索，所以对于模型压缩技术也值得进一步研究。

(3) 基于多源异质数据融合的位置隐私组合保护

当前，基于多源异质的在线社交网络数据，攻击者往往可以利用多数据源的融合获取更为精准的用户位置隐私，对在线社交网络用户的位置隐私造成了更为严重的安全隐患，这一方面也是需要解决的安全问题之一。在面向多源异质数据构建位置隐私保护模型的过程中，不同数据源适用的保护方法可能不尽相同，如何在有效融合数据的基础上进一步有效组合位置隐私保护方法、构建组合保护框架也是未来的重点研究方向之一。

参考文献

[1] Chen J M, Zhang W D. Review of Point of Interest Recommendation Systems in Location-Based Social Networks[J]. *Journal of Frontiers of Computer Science & Technology*, 2022, 16(7): 1462-1478.
(陈江美, 张文德. 基于位置社交网络的兴趣点推荐系统研究综述[J]. *计算机科学与探索*, 2022, 16(7): 1462-1478.)

[2] Jiang H B, Li J, Zhao P, et al. Location Privacy-Preserving Mechanisms in Location-Based Services: A Comprehensive Survey[J]. *ACM Computing Surveys*, 2022, 54(1): 1-36.

[3] Wu X T, Ji G L, Dou W C, et al. Game Theory for Mobile Location Privacy[C]. *The 2nd ACM International Symposium on Blockchain and Secure Critical Infrastructure*, 2020: 106-116.

[4] Piao Y, Cui X H. Review on User Privacy Inference and Protection in Social Networks[J]. *Computer Engineering and Applications*, 2020, 56(19): 1-12.
(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[J]. *计算机工程与应用*, 2020, 56(19): 1-12.)

[5] Li W X, Wu H, Li C S. Survey of Semantics-Based Location Privacy Protection[J]. *Journal of Computer Applications*, 2023, 43(11): 3472-3483.
(李雯萱, 吴昊, 李昌松. 基于语义的位置隐私保护综述[J]. *计算机应用*, 2023, 43(11): 3472-3483.)

[6] Cao H L, Tang H N, Wang F, et al. Survey on Trajectory Representation Learning Techniques[J]. *Journal of Software*, 2021, 32(5): 1461-1479.
(曹翰林, 唐海娜, 王飞, 等. 轨迹表示学习技术研究进展[J]. *软件学报*, 2021, 32(5): 1461-1479.)

[7] Solanas A. Handbook of mobile data privacy[J]. *Computing reviews*, 2019, 60(10):366-366.

[8] He X F, Jin R C, Dai H Y. Leveraging Spatial Diversity for Privacy-Aware Location-Based Services in Mobile Networks[J]. *IEEE Transactions on Information Forensics and Security*, 2018, 13(6): 1524-1534.

[9] Hua J Y, Tong W, Xu F Y, et al. A Geo-Indistinguishable Location Perturbation Mechanism for Location-Based Services Supporting Frequent Queries[J]. *IEEE Transactions on Information Forensics and Security*, 2018, 13(5): 1155-1168.

[10] Li W, Zhang Y X, Gu D W, et al. Ciphertext-Only Fault Analysis on the MANTIS Lightweight Cipher[J]. *Acta Electronica Sinica*, 2022, 50(4): 967-976.
(李玮, 张雨希, 谷大武, 等. 轻量级密码 MANTIS 的唯密文故障分析[J]. *电子学报*, 2022, 50(4): 967-976.)

[11] Matsui M. Linear Cryptanalysis Method for DES Cipher[M]. Advances in Cryptology — EUROCRYPT '93. Berlin, HeidelbergSpringer1994: 386-397.

[12] Yuan K, Cheng Z W, Yang L W, et al. Research on Timed-Release Encryption System Based on Multiple Time Servers[J]. *Journal of Electronics & Information Technology*, 2022, 44(12): 4319-4327.
(袁科, 程自伟, 杨龙威, 等. 基于多时间服务器的时控性加密体制研究[J]. *电子与信息学报*, 2022, 44(12): 4319-4327.)

[13] Chen R M, Wang Y, Huang X Y. RCCA-Secure Public-Key Encryption Based on SM2[J]. *Scientia Sinica* (*Informationis*), 2023, 53(2): 266-281.
(陈荣茂, 王毅, 黄欣沂. 国密 SM2 加密算法的 RCCA 安全设计[J]. *中国科学: 信息科学*, 2023, 53(2): 266-281.)

[14] Zhao G F, Wu H, Wang S S, et al. A Location Privacy and Query Privacy Joint Protection Scheme for POI Query in Vehicular Networks[J]. *Journal of Electronics & Information Technology*, 2024, 46(1): 155-164.
(赵国锋, 吴昊, 王杉杉, 等. 车联网 POI 查询中的位置隐私和查询隐私联合保护机制[J]. *电子与信息学报*, 2024, 46(1): 155-164.)

[15] Shokri R, Theodorakopoulos G, Danezis G, et al. Quantifying Location Privacy: The Case of Sporadic Location Exposure[M]. Privacy Enhancing Technologies. Berlin, HeidelbergSpringer2011: 57-76.

[16] Xu C, Ding Y Y, Chen C, et al. Personalized Location Privacy Protection for Location-Based Services in Vehicular Networks[J]. *IEEE Transactions on Intelligent Transportation Systems*, 2023, 24(1): 1163-1177.

[17] Son J, Kim D, Bhuiyan M Z A, et al. Privacy Enhanced Location Sharing for Mobile Online Social Networks[J]. *IEEE Transactions on Sustainable Computing*, 2020, 5(2): 279-290.

[18] Lin T L, Chang H Y, Li S L. A Location Privacy Attack Based on the Location Sharing Mechanism with Erroneous Distance in Geosocial Networks[J]. *Sensors*, 2020, 20(3): 918.

[19] Polakis I, Argyros G, Petsios T, et al. Where's Wally? : Precise User Discovery Attacks in Location Proximity Services[C]. *The 22nd ACM SIGSAC Conference on Computer and Communications Security*, 2015: 817-828.

[20] Li M Y, Zhu H J, Gao Z Y, et al. All Your Location Are Belong to Us: Breaking Mobile Social Networks for Automated User Location Tracking[C]. *The 15th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, 2014: 43-52.

[21] Stern J P. A New and Efficient All-or-Nothing Disclosure of Secrets Protocol[M]. Advances in Cryptology — ASIACRYPT'98. Berlin, Heidelberg: Springer, 1998: 357-371.

[22] Li R, Liu A X, Xu H L, et al. Adaptive Secure Nearest Neighbor Query Processing over Encrypted Data[J]. *IEEE Transactions on Dependable and Secure Computing*, 2022, 19(1): 91-106.

[23] Zhou Y W, Wang Z L, Qiao Z R, et al. After-the-Fact Leakage Resilience in Identity-Based Encryption[J]. *Science in China* (*Information Sciences*), 2023, 53(3): 454-469.
(周彦伟, 王兆隆, 乔子芮, 等. 身份基加密机制的挑战后泄露容忍性[J]. *中国科学(信息科学)*, 2023, 53(3): 454-469.)

[24] Wei J H, Li J Y, Lin Y P, et al. LDP-Based Social Content Protection for Trending Topic Recommendation[J]. *IEEE Internet of Things Journal*, 2021, 8(6): 4353-4372.

[25] Sweeney L. k-Anonymity: A Model for Protecting Privacy[J]. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 2002, 10(5): 557-570.

[26] Rao J, Gao S, Kang Y, et al. LSTM-TrajGAN: A Deep Learning Approach to Trajectory Privacy Protection[C]. *11th International Conference on Geographic Information Science*, 2020:1-17.

[27] Ren Q, Tian F, Lu X Y, et al. A Reconstruction Attack Scheme on Secure Outsourced Spatial Dataset in Vehicular Ad-Hoc Networks[J]. *Security and Communication Networks*, 2021, 2021: 5317062.

[28] Machanavajjhala A, Gehrke J, Kifer D. ℓ-density: Privacy beyond k-anonymity[C]. *Proceedings of the International Conference on Data Engineering*, 2006.

[29] Song B, Yan X Y, Tan S Y, et al. Human Mobility Models Reveal the Underlying Mechanism of Seasonal Movements across China[J]. *International Journal of Modern Physics C*, 2022, 33(4): 2250054.

[30] Theodorakopoulos G, Shokri R, Troncoso C, et al. Prolonging the Hide-and-Seek Game: Optimal Trajectory Privacy for Location-Based Services[C]. *The 13th Workshop on Privacy in the Electronic Society*, 2014: 73-82.

[31] Zhu L H, Hong H B, Xie M D. A Novel Protection Method of Continuous Location Sharing Based on Local Differential Privacy and Conditional Random Field[C]. *Algorithms and Architectures for Parallel Processing*, 2022: 710-725.

[32] Zhang J D, Chow C Y. Enabling Probabilistic Differential Privacy Protection for Location Recommendations[J]. *IEEE Transactions on Services Computing*, 2021, 14(2): 426-440.

[33] Bordenabe N E, Chatzikokolakis K, Palamidessi C. Optimal Geo-Indistinguishable Mechanisms for Location Privacy[C]. *The 2014 ACM SIGSAC Conference on Computer and Communications Security*, 2014: 251-262.

[34] Shi X J, Zhang J R, Gong Y. Intelligent pseudo-location recommendation for protecting personal location privacy[C]. *IEEE International Conference on Artificial Intelligence and Computer Applications*, IEEE, 2021:172-176.

[35] Palanisamy B, Liu L. Attack-Resilient Mix-Zones over Road Networks: Architecture and Algorithms[J]. *IEEE Transactions on Mobile Computing*, 2015, 14(3): 495-508.

[36] Zhang S B, Liu Q, Wang G J. A Caching-Based Privacy-Preserving Scheme for Continuous Location-Based Services[M]. Security, Privacy and Anonymity in Computation, Communication and Storage. ChamSpringer International Publishing, 2016: 73-82.

[37] Nisha N S, Natgunanathan I, Gao S, et al. A Novel Privacy Protection Scheme for Location-Based Services Using Collaborative Caching[J]. *Computer Networks*, 2022, 213: 109107.

[38] Zhu H T, Zhang L, Feng W M, et al. A Users Collaborative Scheme for Location and Query Privacy[C]. *2016 IEEE 22nd International Conference on Parallel and Distributed Systems*, 2016: 383-390.

[39] Gupta R, Rao U P. Achieving Location Privacy through CAST in Location Based Services[J]. *Journal of Communications and Networks*, 2017, 19(3): 239-249.

[40] Han X, Huang H L, Wang L Y. F-PAD: Private Attribute Disclosure Risk Estimation in Online Social Networks[J]. *IEEE Transactions on Dependable and Secure Computing*, 2019, 16(6): 1054-1069.

[41] Zhang J, Li C W, Wang B T. A Performance Tunable CPIR-Based Privacy Protection Method for Location Based Service[J]. *Information Sciences*, 2022, 589: 440-458.

[42] Li Y H, Cao X, Yuan Y, et al. PrivSem: Protecting Location Privacy Using Semantic and Differential Privacy[J]. *World Wide Web*, 2019, 22(6): 2407-2436.

[43] Chow C Y, Mokbel M F, Bao J, et al. Query-Aware Location Anonymization for Road Networks[J]. *GeoInformatica*, 2011, 15(3): 571-607.

[44] Ghinita G, Kalnis P, Khoshgozaran A, et al. Private Queries in Location Based Services: Anonymizers Are Not Necessary[C]. *The 2008 ACM SIGMOD International Conference on Management of Data*, 2008: 121-132.

[45] Khoshgozaran A, Shahabi C. Private Information Retrieval Techniques for Enabling Location Privacy in Location-Based Services[M]. Privacy in Location-Based Applications: Research Issues and Emerging Trends. Berlin, Heidelberg: Springer, 2009: 59-83.

[46] Ding J C, Yu N H, Lin X Z, et al. Bitcoin-Based Payment Protocol for Private Information Retrieval[J]. *Journal of Cyber Security*, 2019, 4(6): 1-9.
(丁佳晨, 俞能海, 林宪正, 等. 基于比特币的私有信息检索支付协议[J]. *信息安全学报*, 2019, 4(6): 1-9.)

[47] Perifanis V, Drosatos G, Stamatelatos G, et al. FedPOIRec: Privacy-Preserving Federated Poi Recommendation with Social Influence[J]. *Information Sciences*, 2023, 623: 767-790.

[48] Li Y X, Zhou F C, Xu Z F. Privacy-Preserving K-Nearest-Neighbor Search over Mobile Social Network[J]. *Chinese Journal of Computers*, 2021, 44(7): 1481-1500.
(李宇溪, 周福才, 徐紫枫. 支持 K-近邻搜索的移动社交网络隐私保护方案[J]. *计算机学报*, 2021, 44(7): 1481-1500.)

[49] Baracaldo N, Palanisamy B, Joshi J. G-SIR: An Insider Attack Resilient Geo-Social Access Control Framework[J]. *IEEE Transactions on Dependable and Secure Computing*, 2019, 16(1): 84-98.

[50] Li W H, Li C, Geng Y L. APS: Attribute-Aware Privacy-Preserving Scheme in Location-Based Services[J]. *Information Sciences*, 2020, 527: 460-476.

[51] Niu B, Chen Y H, Wang Z B, et al. Eclipse: Preserving Differential Location Privacy Against Long-Term Observation Attacks[J]. *IEEE Transactions on Mobile Computing*, 2022, 21(1): 125-138.

[52] Xia X Y, Bai Z H, Li J, et al. A Location Cloaking Algorithm Based on Dummy and Stackelberg Game[J]. *Chinese Journal of Computers*, 2019, 42(10): 2216-2232.
(夏兴有, 白志宏, 李婕, 等. 基于假位置和 Stackelberg 博弈的位置匿名算法[J]. *计算机学报*, 2019, 42(10): 2216-2232.)

[53] Wu Z D, Li G L, Shen S G, et al. Constructing Dummy Query Sequences to Protect Location Privacy and Query Privacy in Location-Based Services[J]. *World Wide Web*, 2021, 24(1): 25-49.

[54] Ghoshal P, Dhaka M, Sairam A S. On the Effectiveness of Differential Privacy to Continuous Queries[J]. *Service Oriented Computing and Applications*, 2024, 18(4): 381-395.

[55] Liang H C, Wang B, Cui N N, et al. Privacy Preserving Method for Point-of-Interest Query on Road Network[J]. *Journal of Software*, 2018, 29(3): 703-720.
(梁慧超, 王斌, 崔宁宁, 等. 路网环境下兴趣点查询的隐私保护方法[J]. *软件学报*, 2018, 29(3): 703-720.)

[56] Hakeem A, Curtmola R, Ding X N, et al. DFPS: A Distributed Mobile System for Free Parking Assignment[J]. *IEEE Transactions on Mobile Computing*, 2022, 21(12): 4279-4295.

[57] Zhang C, Zhu L H, Xu C, et al. Location Privacy-Preserving Task Recommendation with Geometric Range Query in Mobile Crowdsensing[J]. *IEEE Transactions on Mobile Computing*, 2022, 21(12): 4410-4425.

[58] Zhu X J, Ayday E, Vitenberg R. A Privacy-Preserving Framework for Outsourcing Location-Based Services to the Cloud[J]. *IEEE Transactions on Dependable and Secure Computing*, 2021, 18(1): 384-399.

[59] Huang Q L, Du J B, Yan G Y, et al. Privacy-Preserving Spatio-Temporal Keyword Search for Outsourced Location-Based Services[J]. *IEEE Transactions on Services Computing*, 2022, 15(6): 3443-3456.

[60] Kang J, Steiert D, Lin D, et al. MoveWithMe: Location Privacy Preservation for Smartphone Users[J]. *IEEE Transactions on Information Forensics and Security*, 2020, 15: 711-724.

[61] Hong S, Duan L J, Huang J W. Protecting Location Privacy by Multiquery: A Dynamic Bayesian Game Theoretic Approach[J]. *IEEE Transactions on Information Forensics and Security*, 2022, 17: 2569-2584.

[62] Zheng Z R, Li Z T, Jiang H B, et al. Semantic-Aware Privacy-Preserving Online Location Trajectory Data Sharing[J]. *IEEE Transactions on Information Forensics and Security*, 2022, 17: 2256-2271.

[63] Min M H, Yang S, Xu J H, et al. Intelligent Semantic Location Privacy Protection Method for Location Based Services in Three-Dimensional Spaces[J]. *Journal of Electronics & Information Technology*, 2024, 46(6): 2627-2637.
(闵明慧, 杨爽, 胥俊怀, 等. 三维空间位置服务中智能语义位置隐私保护方法[J]. *电子与信息学报*, 2024, 46(6): 2627-2637.)

[64] Chakraborty S, Shen C, Raghavan K R, et al. ipShield: a framework for enforcing context-aware privacy[C]. *Usenix Conference on Networked*

Systems Design & Implementation, 2014: 143-156.

[65] Xiao C Y, Chen Z, Wang X, et al. DeCache: A Decentralized Two-Level Cache for Mobile Location Privacy Protection[C]. *2014 Sixth International Conference on Ubiquitous and Future Networks*, 2014: 81-86.

[66] Shokri R, Theodorakopoulos G, Papadimitratos P, et al. Hiding in the Mobile Crowd: LocationPrivacy through Collaboration[J]. *IEEE Transactions on Dependable and Secure Computing*, 2014, 11(3): 266-279.

[67] Liu Y J, Wu W Y, Flokas L, et al. Enabling SQL-Based Training Data Debugging for Federated Learning[J]. *Proceedings of the VLDB Endowment*, 2021, 15(3): 388-400.

[68]Cuellar J. R., Morris J. B., Mulligan D. K., et al. Geopriv reqs[EB]. IETF Internet draft, 2003.

[69] Palanisamy B, Liu L. Effective Mix-Zone Anonymization Techniques for Mobile Travelers[J]. *GeoInformatica*, 2014, 18(1): 135-164.

[70] Wei J H, Lin Y P, Yao X, et al. Differential Privacy-Based Location Protection in Spatial Crowdsourcing[J]. *IEEE Transactions on Services Computing*, 2022, 15(1): 45-58.

[71] Chen S T, Li W H, Yao Y Z, et al. Location Privacy Protection Method Based on Lightweight K-Anonymity Incremental Nearest Neighbor Algorithm[J]. *Chinese Journal of Network and Information Security*, 2023, 9(3): 60-72.
(陈赛特, 李卫海, 姚远志, 等. 轻量级 K 匿名增量近邻查询位置隐私保护算法[J]. *网络与信息安全学报*, 2023, 9(3): 60-72.)

[72] Zhang S B, Mao X J, Choo K R, et al. A Trajectory Privacy-Preserving Scheme Based on a Dual-K Mechanism for Continuous Location-Based Services[J]. *Information Sciences*, 2020, 527: 406-419.

[73] Shokri R, Theodorakopoulos G, Le Boudec J Y, et al. Quantifying Location Privacy[C]. *2011 IEEE Symposium on Security and Privacy*, 2011: 247-262.

[74] Wu Y C, Wang K, Guo R Y, et al. Enhanced Privacy Preserving Group Nearest Neighbor Search[J]. *IEEE Transactions on Knowledge and Data Engineering*, 2021, 33(2): 459-473.

[75] Zhou C L, Chen Y H, Tian H, et al. Location Privacy and Query Privacy Preserving Method for K-Nearest Neighbor Query in Road Networks[J]. *Journal of Software*, 2020, 31(2): 471-492.
(周长利, 陈永红, 田晖, 等. 保护位置隐私和查询内容隐私的路网 K 近邻查询方法[J]. *软件学报*, 2020, 31(2): 471-492.)

[76] Liu Y, Du Y M, Tian J. Privacy Protection Algorithm for Cloud Obstacle Shortest Path Navigation Based on Homomorphic Encryption[J]. *Application Research of Computers*, 2021, 38(6): 1859-1864.
(刘义, 杜云明, 田静. 基于同态加密的云环境障碍最短路径导航的隐私保护算法[J]. *计算机应用研究*, 2021, 38(6): 1859-1864.)

[77] Hu H B, Xu J L, On S T, et al. Privacy-Aware Location Data Publishing[J]. *ACM Transactions on Database Systems*, 2010, 35(3): 1-42.

[78] Cicek A E, Nergiz M E, Saygin Y. Ensuring Location Diversity in Privacy-Preserving Spatio-Temporal Data Publishing[J]. *The VLDB Journal*, 2014, 23(4): 609-625.

[79] Li N H, Li T C, Venkatasubramanian S. T-Closeness: Privacy beyond K-Anonymity and L-Diversity[C]. *2007 IEEE 23rd International Conference on Data Engineering*, 2007: 106-115.

[80] Cao Y, Xiao Y H, Xiong L, et al. Protecting Spatiotemporal Event Privacy in Continuous Location-Based Services[J]. *IEEE Transactions on Knowledge and Data Engineering*, 2021, 33(8): 3141-3154.

[81] Oya S, Troncoso C, Pérez-González F. Back to the Drawing Board: Revisiting the Design of Optimal Location Privacy-Preserving Mechanisms[C]. *The 2017 ACM SIGSAC Conference on Computer and Communications Security*, 2017: 1959-1972.

[82] Zhang W J, Li M, Tandon R, et al. Online Location Trace Privacy: An Information Theoretic Approach[J]. *IEEE Transactions on Information Forensics and Security*, 2019, 14(1): 235-250.

[83] Li Z T, Ding B L, Zhang C, et al. Federated Matrix Factorization with Privacy Guarantee[J]. *Proceedings of the VLDB Endowment*, 2021, 15(4): 900-913.

[84] Cao Y, Yoshikawa M, Xiao Y H, et al. Quantifying Differential Privacy in Continuous Data Release under Temporal Correlations[J]. *IEEE Transactions on Knowledge and Data Engineering*, 2019, 31(7): 1281-1295.

[85] Tian J, Du Y M, Li S, et al. Paillier Homomorphic Encryption Based Location Privacy Protection Scheme for Crowdsensing Task Distribution[J]. *Journal of Frontiers of Computer Science & Technology*, 2022, 16(6): 1327-1333.
(田静, 杜云明, 李帅, 等. Paillier 加密的隐私保护群智感知任务发布算法[J]. *计算机科学与探索*, 2022, 16(6): 1327-1333.)

[86] Niu B, Li Q H, Zhu X Y, et al. Enhancing Privacy through Caching in Location-Based Services[C]. *2015 IEEE Conference on Computer Communications*, 2015: 1017-1025.

马卓 于 2021 年在东南大学网络空间安全专业获得博士学位。现任江苏警官学院计算机信息与网络安全系讲师, CCF 会员, 主要研究领域为隐私保护、社会计算。
E-mail: mazhuo@jspi.edu.cn.

胥帅 于 2020 年在东南大学计算机科学与技术专业获得博士学位, 现任南京航空航天大学计算机科学与技术学院讲师, CCF 会员, 主要研究领域为智慧城市、移动社交网络、时空数据管理与挖掘。
E-mail: xushuai7@nuaa.edu.cn

曹玖新 于西安交通大学计算机系统结构专业获得博士学位，现任东南大学网络空间安全学院副院长、教授，CCF 高级会员，主要研究领域为大数据智能处理与内容安全、社会计算。E-mail: jx.cao@seu.edu.cn

王群 于南京理工大学计算机应用技术专业获得博士学位，现任江苏警官学院计算机信息与网络安全系主任、教授，CCF 高级会员，主要研究领域为网络空间安全，计算机体系结构与协议。E-mail: wagnqun@jspi.edu.cn

夏玲玲 于 2017 年在南京邮电大学信息安全专业获得博士学位，现任江苏警官学院计算机信息与网络安全系网络安全与执法教研室主任、副教授，主要研究领域为网络空间安全，数据挖掘。E-mail: xialingling@jspi.edu.cn