一个快速的隐私保护框架，用于连续的基于位置查询在道路网络

摘要

基于位置的服务（LBS）的流行导致个人隐私关注，因为用户共享他们的位置和查询以获得期望的服务。对于用户定期报告其位置的连续查询，攻击者通过分析其快照样本的相关性来扫描用户的隐私更多。传统的在欧几里德空间中设计的隐私保护解决方案几乎不能应用于道路网络环境，因为他们不知道网络拓扑性质。

在本文中，我们提出了一种新颖的道路网络中的连续查询隐私保护框架。我们的框架基于k-匿名和l多样性的概念。为了实现服务质量，考虑了距离限制。基于用户密度，历史轨迹和道路网络拓扑构建了Snet层次结构，以加速在匿名服务器上执行的隐藏过程。两种类型的隐藏算法，对于单用户和一批用户，被设计。安全分析表明，我们的框架是典型的攻击的鲁棒性。我们评估我们

框架从隐私保护能力，服务质量和系统性能的方面，这表明我们的框架可以提供良好的隐私保护，同时确保用户的服务质量。

1. 介绍

由于定位设备（例如，GPS）的广泛使用，基于位置的服务（LBS）近年来已经变得普遍存在。利用从这些设备获得的位置（纬度和经度），LBS应用扫描通过本地商业搜索（例如，搜索最接近用户的餐馆），电子营销（例如，发送优惠券）向用户提供高度个性化的服务到附近的潜在客户）和社交网络（例如，朋友们分享他们的被标记的照片）等。通常，用户可以向LBS提供商发送两种类型的查询：快照查询，例如“显示一英里内的酒店”以及连续查询，例如“在接下来的30分钟内每5分钟最近的加油站的信息”。 实际上，连续查询包括几个连续的快照，其被逐个用户的实时位置处理。

然而，报告位置意味着委托人值得LBS提供商，并且攻击者可以利用它来暴露位置，该位置可以位于该位置的隐私中。 用户的位置可以是敏感信息，例如健康状况和宗教信仰。特别地，这种跟踪攻击者的可能性的能力，例如车辆盗窃和抢劫。 用户不能明确地识别基于位置的服务，特别是服务敏感（例如，查询最近的癌症治疗中心）问题作为查询隐私。 显然，隐私的连续查询主题查询，因为攻击者可以通过使用空间和时间相关的隐私来实现连续查询。

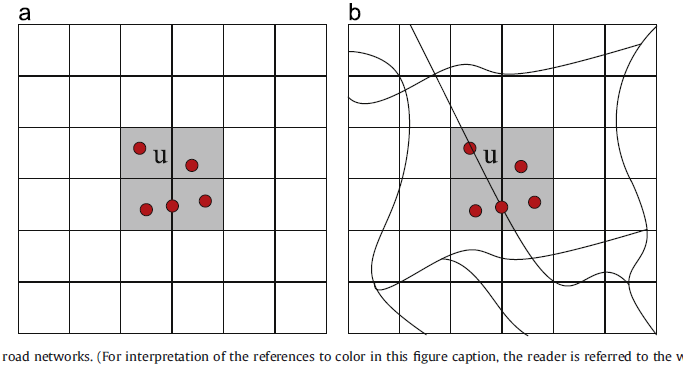
已经提出了许多为欧几里得空间设计的隐私保护技术（Samarati和Sweeney，1998; Gruteser和Grunwald，2003; Liuetal，2009），其中用户可以以随机速度在任意方向上移动。然而，用户的移动可以是 受底层路网的限制。 例如，用户应该在最大速度限制内沿某条道路行驶。将这些技术直接应用于道路网络可能导致隐私泄露。如图1（a）所示，u与4个其他用户匿名，用红色 （Bamba etal。，2008; GedikandLiu，2008; Kainisetal。，2007），并将其精确位置模糊成灰色区域。 有了这样的斗篷修补程序，实现了5匿名，攻击者只能告诉u可能在灰色地区的某个地方。图1（b）显示了同样的情况，但具有基础道路网络的知识。 由于灰色区域包含单个道路段，所以攻击者可以推断出u必须位于道路段中，并且将排除该段之外的用户。由于仅仅两个可用用户违反了匿名性，这可以使得 攻击者更容易跟踪u。通常，这种攻击不可能在实践中通过考虑基础路网而被匿名化。此外，其他道路网络属性，例如人口密度，其对隐私具有显着影响 保存，也应该关注。

图1

目前，已经向道路网络引入了几种隐私保护解决方案。不幸的是，在道路网工程中应用传统掩蔽算法的现有方法导致巨大的时间成本。为了避免传统方法中的这么巨大的时间成本，我们提高了检索用户被掩盖在一起的速度.另外，替代地，隐藏执行更快地处理用户的批处理，而不是一次处理单个用户。我们相信这是提出快速LBS连续查询隐私的第一个工作.即使用户的位置泄露，用户的查询隐私也被保留。网络拓扑属性被考虑，使得我们可以有效地为用户提供隐私保护，同时降低LBS提供商和隐私保护系统。我们的解决方案的主要思想是将基础的路网抽象为多个层次。抽象的edunitis表示san snet。相应地，我们提出Snet合并算法来构造Snet层次结构（参见第3.3.1节）。基于Snet层次结构，我们的框架引入了可信任的第三方来将查询发布者与其他人封装，这满足了他的特定隐私要求（见第3.2节）。从LBS提供者的角度来看，它们只能将一组用户与一组查询相关联，而不是与特定用户进行查询。

我们提出两个版本的隐私保护算法，一个分别处理每个查询，而其他处理查询的同时批处理。我们的主要贡献包括：

* + - 该框架可以抵抗通过考虑道路网络的拓扑属性打破k匿名的攻击。为了加速隐私保护过程，我们通过考虑用户的密度，历史轨迹和连接性将道路网络抽象为层次结构 的路段。
    - 整个过程分为三个阶段：初始化阶段，执行阶段和更新阶段。初始化阶段构建层次结构以便于隐藏过程。基于预先计算的层次结构，框架可以提供更有效的隐私保护服务 执行阶段。随着时间的推移，基础网络可能改变，更新阶段使我们的框架适应不同的道路条件并保持长期有效性。
    - 我们提出了基于单个用户和用户批处理的层次结构的快速隐藏算法。每个Snet被当作隐藏单元。当子Snets中的用户不能满足隐藏要求时，隐藏进程将转移到父Snet。
    - 考虑用户的移动趋势，速度差异和距离差异，以保持尽可能多的普通用户抵抗典型的攻击。攻击复原力分析和性能评估表明我们的框架可以抵御典型的攻击，并实现 很好的表现。

本文的其余部分组织如下：在第2节，我们讨论隐私保护的相关工作。我们在第3节介绍系统模型，详细的算法和框架维护显示在第4节。我们分析我们的安全性 实验和评估在第6节中给出。在第7节中，我们得出一些简短的结论。

1. 相关工作

2.1节回顾相关工作在欧几里得空间的隐私保护,2.2节调查文献在公路网络的隐私保护,2.3节解释隐私保存技术基于多党计算,和2.4节讨论隐私保护典型的攻击。

2.1 欧几里得空间的隐私保护

以前在欧几里得的工作空间根据系统架构可以分为两类：集中式隐私保护架构和分布式隐私保护架构。

2.1.1中央隐私保护体系结构

在中心化的隐私保护架构中，一个可信任的第三方涉及到模糊用户到空间区域的定位，这保证满足k-匿名性（Samarati和Sweeney，1998）的要求。基于k-匿名的想法，提出了Interval Cloak算法（Gruteser和Grunwald，2003），其将区域递归地分割为四个子区域，直到子区域中的用户小于k。 集中式架构已被应用于连续查询（Chow和Mokbel，2007; Wangetal。，2012a，b; Guhaetal。，2012）。 L2P2方案由Wangetal。（2012a）提出，允许用户为连续查询定义其动态和多样的隐私要求。 Wangetal。（2012b）提出了一个查询链接用于连续LBS查询的隐私保护算法（V-DCA），其考虑用户的移动性和加速度相似性以选择可以长期保持接近的用户。

2.1.2分布式隐私保护体系结构

在分布式架构中，用户通过协作（Domingo-Ferrer，2006）或自主地（Olumofin等人，2010; Huang和Vishwanathan，2010; Durretal。，2011）来保护他们的隐私。 Domingo-Ferrer（2006）提出了一种协同算法，其中用户广播他的扰动位置以形成具有k≥1个邻居的组。 Olumofin等（2010）结合了私人信息检索（PIR）。 Durr etal。（2011）提出了位置信息。 对于连续查询，Pingley等人（2011）基于查询上下文和运动模式生成虚拟查询。 Wangetal。（2012c）设计了一个具有几个半正式匿名服务器的分布式架构。

不幸的是，这些是为欧几里得空间设计的，并且不能解决道路网络面临的问题。在这方面，我们提出的算法不仅考虑个性化的隐私要求和移动特性，如Wangetal。（2012b），但也考虑了基础道路网络。 此外，为了提高系统效率，我们的算法可以同时掩盖用户的批处理。

2.2广域网中的隐私保护

已经提出了几种隐私保护技术来保护用户在道路网络中的隐私。基于基于位置的查询的类型，这些技术可以被分为两类：用于基于位置的快照查询的隐私保护和用于连续 基于位置的查询。

2.2.1.基于位置的快照查询的隐私保护