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

随着基于位置的服务（LBS）的流行个人隐私得到越来越多的关注，因为用户共享他们的位置和查询以获取服务。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。

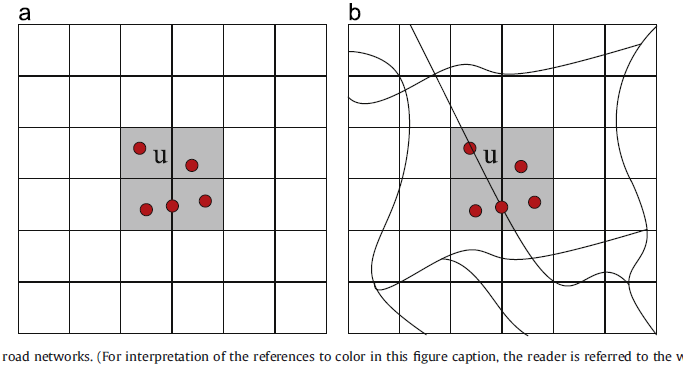
已经提出了许多为欧几里得空间设计的隐私保护技术（Samarati和Sweeney，1998; Gruteser和Grunwald，2003; Liuetal，2009），其中用户可以以随机速度在任意方向上移动。然而，用户的移动可以是 受底层路网的限制。 例如，用户应该在最大速度限制内沿某条道路行驶。将这些技术直接应用于道路网络可能导致隐私泄露。如图1（a）所示，u与4个其他用户匿名，用红色 （Bamba etal。，2008; GedikandLiu，2008; Kainisetal。，2007），并将其精确位置模糊成灰色区域。 有了这样的斗篷修补程序，实现了5匿名，攻击者只能告诉u可能在灰色地区的某个地方。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

PSNN和PSRQ技术（Kuetal。，2007）完全依赖于为欧几里德空间设计的Casper（Mokbel等人，2006）。结果，继承了欧几里德空间技术的缺点。 Kolahdouzan和Shahabi（2004）划分整个道路网络变成小的Voronoi区域用于匿名化。在Mouratidis和Yiu（2010）中，Hilbert阶用于使用k 1个邻居来匿名用户。因此，算法的有效性取决于排序。为了平衡处理成本和隐私保护，Wang和Liu（2009）提出了一个基于X-star的隐私保护框架，将邻近的查询合并为一个新建立的匿名明星（超星）。 Chow等人（2011）设计了一种有效的共享执行范式。 Bao等人（2009）提出了一种名为Pros的apeer-to-peerlocation隐私保护系统，用户与他人合作形成完全的路段集合。然而，简单地将这些技术应用于连续的基于位置的查询可能遭受攻击关联快照样品。

2.2.2 基于位置的连续查询的隐私保护

以前的研究主要集中在通过利用混合区改变用户的识别来打破位置暴露的连续性。 在Freudigeretal。（2009）中，可能的混合区位置的混合效果被用于优化混合区的位置.Mobimix（PalanisamyandLiu，2011）在混合区的布置中考虑多个因素，例如用户群的统计行为。Liu等人（2012）设计了两个启发式算法来策略性地选择混合区域位置。一般来说，尽管混合区域 - 区域保护连续查询的隐私，它们限制用户服务的领域，这对于一些用户可能是不可接受的。因此，我们的框架采用基于隐藏的机制用于连续查询隐私保护，这也考虑了路网更新。

2.3基于PIR的隐私保护

在位置隐私保护中使用依赖于加密或私人信息检索（PIR）的方法。专用信息检索（PIR）技术允许用户检索数据库的元素，而该数据库的所有者不是能够确定选择哪个元素（Chor等人，1998）。通常，基于PIR的技术不需要可信第三方。 Zhong等人（2007）引入了三种协议，即Louis，Lester和Pierre，在回答K个最近邻（KNN）查询时提供位置隐私。类似地，Papadopoulos等人（2010）使用安全的硬件辅助PIR来实现强位置隐私。 Ghinita等人（2008）提出了一种基于PIR技术支持私人位置相关查询的框架。该框架不需要可信第三方，并且可以实现用户位置快照的强大隐私。 Narayananetal。（2011）提出了各种加密支持私人接近测试的协议。它们使用从物理环境生成的“位置标签”来加强接近测试的安全性。 Li和Jung（2013）设计了一套保护隐私的位置查询协议（PLQP），以在社交网络服务（SNS）的应用场景下保护用户的位置隐私。

这种类型的技术提供了强的隐私保护。然而，它的性能，虽然通过利用特殊硬件改进，仍然在现实世界中仍然是可适用的。另一方面，仍然需要看到，是否任何基于位置的服务提供商将部署密码系统 在市场上。

2.4 隐私保护免受攻击（没翻）

3.系统模型

在本节中，我们首先制定隐私保护问题，然后介绍隐私概要和相应的隐私保护机制。 最后，我们展示实施策略。

3.1 问题的提出

我们定义了基础道路网络和隐私问题需要解决。

3.1.1基础道路网

我们认为一个由底层道路网限制的空间，其由加权有向图G =（V,E）表示; EÞ，其中顶点集合V。 Fv0; v1;乧; vNg代表路口，和边缘集合E。 fdvi; vjTj vi; vjAVg表示路段连接两个连接vi和vj。列出的顺序vivj指示从vi到vj的道路段的方向。 注意，在我们的模型中，用户运动的方向被保留。当没有混乱发生和简化时，我们不明确地提及在随后的部分中出现的图中的基础道路网络的方向。

我们使用dðvÞ表示在V中的顶点v的度数。具体来说，具有dðv= 1的顶点被称为端点顶点，中间顶点具有dðv= 2，并且段间顶点具有dðv^。 E中的每个边e与负负权重w（e）相关联，负权重w（e）表示从一个顶点到另一个顶点的边的成本。成本可以是相应道路的行驶距离，行程时间或通行费。 系统，我们在道路网络中根据行进距离和顺序顶点来权重边缘，基于此，我们定义移动方向朝向具有较大数目的顶点，否则，它是负的。在我们的工作中，假定所有移动用户驻留在边缘中。

结合基础道路网络，发出连续查询的用户u的轨迹是连接边的序列：其中vsi和vei表示开始 节点和终端节点边缘通过u，和vei =vsðiþ1Þ。

3.1.2 问题设置

在连续的基于位置的服务中，查询具有三种状态：（1）新：新发起的查询被称为新查询。 （2）活动：先前创建但尚未终止的查询是活动查询。 （3）过期：到达其到期时间的查询终止称为过期查询。 对于新查询，移动用户以ou的形式将其发送到LBS提供商; l; Tinit; Texp; Con4，其中u是用户的标识符，l是用户的当前位置（纬度和经度），Tinit表示查询启动时间，Texp是查询到期时间，Con是查询文本，例如“通知我 最近的加油站在接下来的30分钟“。 一旦它变为活动，用户仅需要用他的标识符u来更新他的位置l，并将其发送到LBS提供商，因为提供商将保留Con直到Texp。 在查询生命周期中，LBS提供商提供服务通过用更新的位置周期性地（例如，每30秒）应答查询。

两个位置和查询内容暴露给LBS提供商，这可能是不可信的。考虑一些LBS需要用户的服务提供的确切位置，我们尝试保持用户的查询隐私。在我们的系统中，我们引入可信第三方 将用户与其他人掩蔽到隐藏的用户集Su中。 相应地，隐藏分段集合Ssg包含用户驻留在其中的分段，并且由Su中的用户发送的查询形成隐藏的查询集合Q.

3.1.3攻击模型

为了准确地解释我们的方法，我们建立了对其进行保存的攻击模型。通常，使用两个特征来表示攻击者：背景知识和攻击。 我们首先指定攻击者的背景知识，并且该秘密证明他执行的攻击以窃取隐私和伤害个人。

我们假设用户的位置和查询的答案可以不显示查询内容，即，用户发出的查询是未知的，即使他的位置泄漏。攻击者关于用户的背景知识BK被假定知道：

1. u在其查询生命期内的确切位置。

2. u的隐藏用户设置Su和相应的查询集Q为每个查询。

3.隐私保护算法。

给定所采用的隐私保护算法，用户的确切位置以及由隐私保护算法生成的隐藏的用户和查询集合，攻击者可以运行四个典型的攻击，其最频繁地并且特别地针对连续查询实现， （Chow和Mokbel，2007），重放攻击（Wang和Liu，2009）和同质性攻击（Bettini等人，2007）。 他们全部旨在找出用户和查询之间的关联。

同质性攻击是由于缺乏多样性，我们使用查询熵来度量隐藏查询集的多样性，这将在3.2节中解释。随着多样性，同质性攻击可以自然地被隐私保护算法抵制，因此，我们只考虑其他三种攻击。通常，当攻击者获得背景知识时，他试图推断一些关于用户的感兴趣的私人信息，查询内容，例如将用户的确切位置链接到特定查询并且可以访问查询内容。然而，用户被隐藏在具有隐藏的用户集合的形式的区域中，并且由母亲发送的查询被分组到隐藏的查询集合中。因此，将用户的确切位置链接到他的问题实际查询是概率性的。攻击的输出可以是对可能的攻击类别的概率分布。因此，我们定义链接能力来量化我们的框架在三种典型攻击下的漏洞能力。

定义1（可链接性）。在BK下查询q到用户u的链接能力，表示为链接½u'qjBK？，是攻击者可以推断匿名用户集合Su中的用户之间由u发出q的概率。

查询抽样攻击（Chow和Mokbel，2007）：查询抽样攻击意味着当用户位置的分布不均匀时，隐藏的用户集会彼此重叠。因此，一些用户可以隐藏成两个或更多集合，这增加将查询链接到查询发行者的概率。

查询抽样攻击可以如下形式化：假设有三个用户u1，u2，u3，分别发出查询q1，q2，q3。 包含u1和u2的Su1是u1的隐藏用户集合，而包含u2和u3的Su2是u2的。 攻击者可以推断链路½u1'q1 j BK？ ¼1，因为u1只属于Su1。

查询跟踪攻击（Chow和Mokbel，2007）：在连续查询中，用户不断地向LBS提供商报告他们的位置。 查询跟踪攻击可以将连续时间快照连接在一起以识别查询发出者，尽管他与其他用户隐藏。

假设用户u发出查询q。 在时间t1，他被隐藏到用户集合Su1中，并且相应的查询集合Q1。 因此，链接能力是链接能力。 ¼1 j Q1 j。 随着时间的流逝，生成更多的隐藏集合，表示为时间ti的Sui和Qi。 由于查询发出者必须在所有的斗篷eduserset中，攻击者链接集合并且链接能力被改变为链接。

重放攻击（Wang和Liu，2009）：在重放攻击中，我们假设攻击者具有关于隐藏算法的全部知识。 通过使用假定为查询发出者的匿名用户集中的元素重新运行隐藏算法，攻击者估计用户生成匿名集的可能性。

攻击者通过如下方式重放隐藏过程：foreach user uiASu，（1）通过将ui作为查询q的查询发出者来重新运行隐藏算法，以生成隐藏集S0ui，其中j Suj = jS0ui j; （2）计算ui发出q的概率，即（3）选择具有最大概率值的ui作为查询发行者。链接能力是链接能力。 ？ ¼n i = 0Prob½Suj ui; BK？ ？ 1 j Q j。

在本文中，我们旨在防止在查询抽样攻击，查询跟踪攻击和重放攻击下将连续的基于位置的查询链接到特定用户，即低链接能力。

3.2 隐私资料

如上所述，Su，Ssg和Q分别表示隐藏的用户集，隐藏段集合和对应的查询集。 路段是边的序列（v0 v1; v1 v2; ...; vm1 vm），其中只有v0和vm是截面顶点或端点。生成的Su，Ssg和Q应满足用户的个性化隐私 在其隐私概要中以（klocal; kglobal; llocal; lglobal; Lmax; Dismax）的形式定义的要求。 它们主要从四个方面定义隐私要求：k-匿名性，l-分集，最大长度和最大距离。

3.2.1.k-匿名

如果k可以由k个用户中的任何一个发出，则查询服从k-匿名性（Chow和Mokbel，2007）。 在我们的系统中，查询发布者至少隐藏k-1个其他不区分的用户来实现k-匿名。

klocal和klobal是k匿名的要求。 klocal确保在每个快照处用户被至少klocal？1个其他用户隐藏。 对于kglobal，其指示在连续查询中针对连续快照的隐藏集的交集中的公共用户的数量至少是全局的。 查询跟踪攻击将失败，因为查询发出者仍然不能区别于其他全球用户，即使攻击者链接sall自定义集合。对于由n个快照拍摄组成的连续查询，我们维持

其中Suiði¼1; 2; ...; n是第i个快照的隐藏用户集。

3.2.2查询l-多样性

对于隐藏的查询集Q，给定整数l，如果该集合的查询熵等于或大于logðl，则其满足查询l分集。

类似于分类不同业务的黄页公司，我们根据兴趣点（POI）（例如医院和餐馆）将查询分类为不同的类别。例如，发出查询的用户“每5分钟向我报告最近的加油站 接下来30分钟“似乎对加油站感兴趣，因此，查询涉及加油站类别。这些类别表示为C = fc1; c2; ...; cng。 假设查询类别是已知的，并且不能从这些类别推断准确的查询内容。对于特定查询q属于类别ci，查询熵H定义为

引入查询多样性以抵抗同质性攻击（Bettini等人，2007）。 类似于k匿名限制，我们有l局部多样性和l全局多样性为每个单一隐藏的查询集和所有集的交集。因此我们有



其中QðSuiÞ是用户在Sui中发出的隐藏查询的集合，Hd是熵函数。

3.2.3 最大长度

当隐藏段集合Ssg中的道路段的总长度不大于预定义的最大值时，查询满足最大长度限制。

在我们的系统中，它将Ssg中的段的总权重限制为L max，

引入L max以限制匿名集合的扩展，这可能产生具有更多候选结果的计算和通信成本。 最大长度要求在人口密度特别低的粗糙区域中尤其重要，因为它需要大的隐藏段集合以满足k-匿名性。当违反最大长度限制内的k-匿名性时，我们可以生成伪查询 与查询上下文一致（Pingley等人，2011）。 因此，用户的隐私被保留，因为攻击者不能从虚拟物中告诉真实的。 生成虚拟对象是基于位置的查询隐私保护的另一个主题，这不是本文的重点。

3.2.4 最大距离

只有当查询发出者与任何其他匿名用户之间的距离小于预定义的最大距离时，查询才满足最大距离要求，在我们的框架中表示为Dismax。然后对于每个用户uiASu，它保持

其中u是查询发行者，Disðu; ui是从u到ui的shor测试路径的长度。 它发挥重要作用，特别是当一个区域中的用户具有请求某一类别的查询的高概率时。

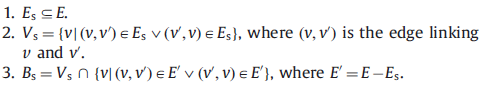
3.3 隐私保护机制

首先，我们提出了基本的概念，在我们的隐私 - 保留机制。然后，我们显示用户的资格被掩盖。

3.3.1.Snet和Snet层次

在道路网络中，由群集（或社区）概念性覆盖的部分可以表示潜在的隐藏段集合。在将空间域划分为欧几里德空间中的单元的隐私保护技术的支持下，我们从下而上递归地构建道路网络的子图 每个子图被命名为Snet，它是我们系统中的基本掩饰单位.

定义2（Snet）。 对于给定的路网图G =ðV; Enet，Snet是G的子图，表示为Sn / d'Vs; Bs; Es，其中Vs，Bs和Es分别表示在Sn中的顶点集，边界顶点集和边集合，此外：



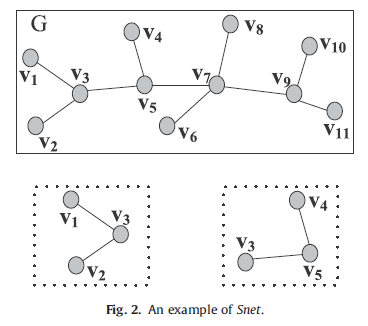
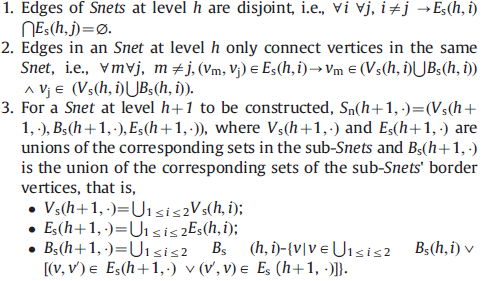


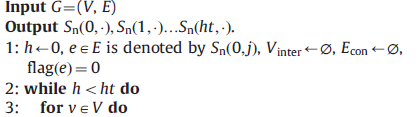
图2示出了道路网络图G（在实心框架中）的两个Snets（在虚线框中）。对于左Snet，对应的顶点集合V s是{v1; v2; v3}，边集Es包含ðv1; v3Þ和ðv2; v3，并且边界顶点集Bs是{v3}，因为边缘ðv3; v5Þ不属于边集Es。 类似地，对于正确的Snet，对应的顶点集合V0s是{v3; v4; v5}，边集E0s包含ðv3; v5Þ和ðv4; v5Þ，边界顶点集B0s isfv3; v5g因为边ðv1; v3Þ，ðv2; v3Þ和ðv5; v7不在边集E0s。 此外，由于两个Snets共享边界顶点v3，它们被称为相邻Snets。

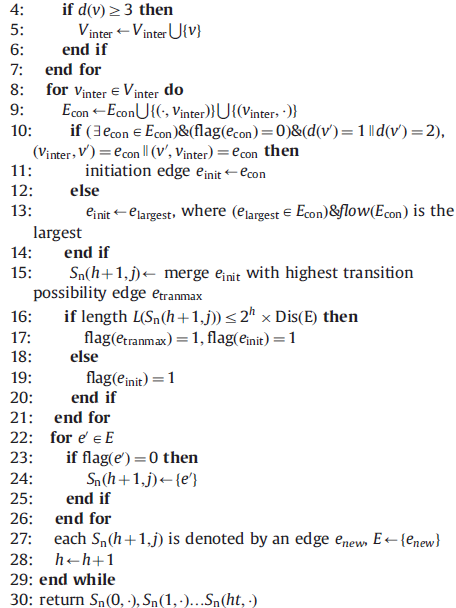
我们通过以自下而上的方式构建Snets来将基础道路网络构建成Snet层级结构，其中上层的Snets由较低级别的Snets形成。 为了简单起见，我们限制一个Snet最多由两个子Snets组成。在每个级别，道路网络被视为互连的Snets的图。 具体来说，level0的每个Snet表示路网中的一个原始段。在顶层ht只有一个Snet，它覆盖整个路由网络。

在构建Snet时，Snðhþ1; ？在级别hþ1，有两个子Snets，Snðh; iÞ，1rir2在level h，其中Snðhþ1; ？ð¼ðVsðhþ1; ？Þ; Bsðhþ1; ÞÞ; Esðhþ1; ？必须满足以下三个条件：

定义3（过渡概率）。 从边i到j的转移概率意味着边i上的用户将移动到j的概率。 它可以通过计算用户在i中根据历史轨迹转移到j的次数来预先计算。转移概率被计算为从边缘i到边缘j的转变的计数除以从边缘i到其它边缘的转变的总数。

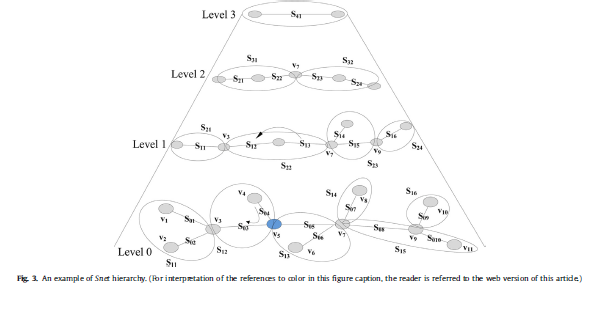
Algorithm 1. Building the Snet hierarchy.





通常，具有较大度数的顶点在路网中起更重要的作用。因此，我们选择交点和相应的边缘来开始构建过程。在所有相邻边缘中，我们给予连接到中间顶点或结束顶点的那些优先权。如果没有中间点或者端点连接，则我们选择携带最大历史用户流的边作为初始边。然后，用户最可能从初始边转移到的边（即，最高转变可能性）被选择以形成Snet。形成的Snet进一步由在较高级别的边缘表示，其通过公共边界顶点与相邻的Snets连接。递归地执行Snet构建步骤，直到基础路由网络被合并到在顶级ht的一个Snet。对于不与其他合并的边，它将自身组装为更高级别的Snet。为了平衡隐私保护和系统成本，我们将Snet中的边的最大总长度限制为值Lmax。假设基础路网的平均边长为Dis（E），我们使用2hDisðE作为在h级的Snets的最大长度限制，因为在H级的Snet中最多有2h个边。构建Snet层次结构的详细过程如算法1所示。

图3示出了建立图2中的路网的Snet层次结构的示例。我们使用边缘来表示Snet，在较低层中环绕的Snets意味着它们将被构造为上层中的透明Snet。蓝色顶点v5 被精心选择用于Snet构造过程。箭头指示从边缘dv4的过渡方向; v5T到边dv5; v3T。

在特殊情况下，层0的每个边（原始基础路由网络）构造Snet。 例如，ðv1; v3Þ表示SnetSnð0; 1Þ。 Snð1; 1Þ表示由ðv1形成的Snet; v3Þ和ðv2; v3。在Snet结构中，选择交点顶点v5。 我们选择ðv5; v4作为启动一个dge，因为它连接一个结束顶点v4。 我们将它与ðv3合并; v5Þ具有从ðv5开始的最高转移概率; 相邻边缘之间的边（共享公共边界顶点的边）。因此，我们得到SnetSnð1; 2nd at level1。类似地，SnetsSnð1; 2Þ和Snð1; 3Þ由level1的边表示，它们的相邻SnetsSnð1; 1Þ，Snð1; 4Þ和Snð1; 5通过顶点v3和v7连接。 Snet层次构造过程继续，直到整个道路网络合并成单个Snet Snd4; 1Þ在第四级。

3.3.2 隐形资格

基于Snet层次结构，我们的系统为满足预定义隐私配置文件的用户生成隐藏集。 为了满足klocal和llocal要求，我们以从下到上的方式从级别0的Snets扩展隐藏集合。当违反Lmax要求时，扩展过程终止。同时，与查询发布者的距离长于Dismax的用户 被踢出。对于kglobal和lglobal要求，我们尝试维持保持在相同Snet中的用户保持不变设置在长期。

有三个特性会影响用户将要输入的Snet以及他将来何时输入：传输行为，速度和到顶点的距离。我们使用移动趋势来描述用户进入某个Snet后的传输行为 留下前一个。在将来移动到同一个Snet的用户具有相同的移动趋势。 我们将用户的位置视为由移动方向和速度大小组成的向量，速度差用于测量用户之间的速度变化。 具有低速度差的用户更可能在未来保持靠近。 类似地，我们使用距离差来显示用户与边界顶点的距离差，它们将经过。具有低距离差的用户容易保持在相同的Snet中。 因此，在选择匿名的候选用户时，我们优选与查询相比具有类似移动趋势，低速度差和低距离差的用户发行人。

移动趋势：用户的移动趋势可以被建模为在当前Snet Sn的一组相邻Snets上的马尔可夫链。 令PSn为Sn的转移矩阵，PSn的元素pSn ij，i = 1 ... m，j = 1 ... w是从Sn的边缘i到Snet j的用户的转移概率，其中m是Sn的边缘号， n是Sn的相邻Snets的量。

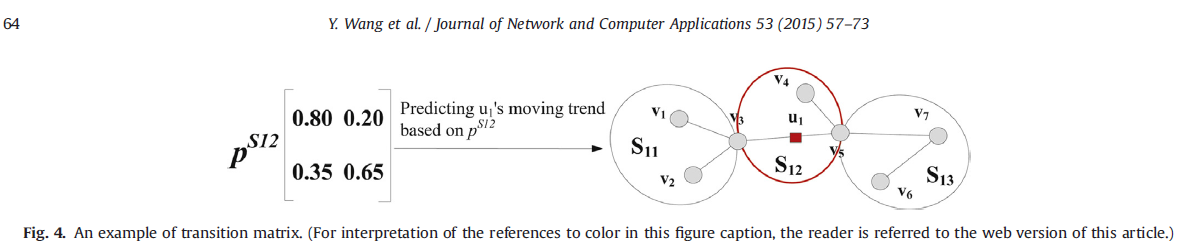


图4示出了转换矩阵的示例。ðv3的转移概率; v5关于邻居SnetsSnð1; 1Þ和Snð1; 3Þ，因此相应地，pSnð1;2Þ2 ;? 是从ðv4的转移概率; v5至Snð1; 1Þ和Snð1; 3Þ。 用红色矩形表示的用户u1沿边缘ðv5移动; v3ÞinSnð1; 2Þ。 显然，u1有较高的概率进入Snð1; 1Þ离开Snð1后; 2Þ。

速度差：两个用户的差值应考虑移动方向和幅度。 然而，只有具有相同移动趋势的用户需要检查速度差，具有相反方向的用户将被滤除。因此，在计算速度差时考虑幅度。 用户ui和uj之间的速度差VL diff被定义为

其中j vli j和j vlj j是ui和uj的速度大小。

合格的用户必须隐藏在一起的用户应该遵循速度差限制ζ：



距离差：路网距离dðu; 用户u和顶点v之间的边界权重被定义为沿着从u到v的最短路径的边权重的和。在我们的系统中，u将在进入预测的Snet时通过v。 v是公共边界节点两个相邻的Snet。 虽然有多个公共边界节点，v是最接近u的那个。 对于ui和uj，它们可以通过不同的顶点进入相同的Snet，表示为vi和vj。 然后，用户之间到它们可以经过的顶点的距离差被计算为



因此，合格的被掩盖在一起的用户应该进一步满足以下等式中的距离差限制θ：

3.4 框架实现

在本节中，我们展示了我们的隐私保护框架的系统架构。 然后讨论Snet层次结构的存储方案。

3.4.1系统架构

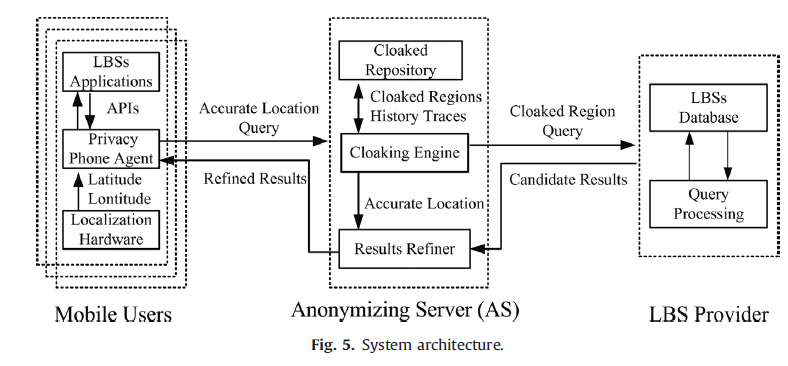
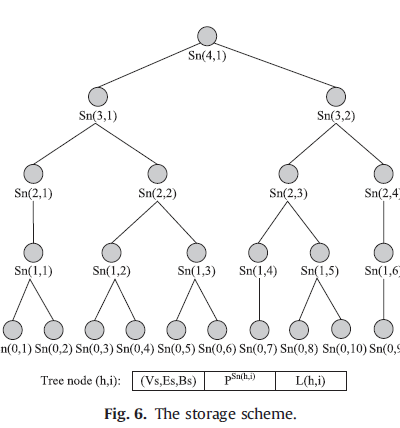


图5显示了系统架构，它由三个组件组成：移动用户，可信匿名服务器（AS）和LBS提供商。移动用户通过隐私电话向AS发送查询，形成是什么意思？ l; p; Tq; Texp; Con4，其中u; l; Tq; Texp和Con的含义与3.1.2节中的含义相同，p表示用户定义的隐私配置文件oklocal; kglobal; llocal; lglobal; Lmax; Dismax4在3.2节讨论。 l是定位设备获得的用户位置。当AS从移动用户接收到查询时，隐藏引擎利用在第4节中提出的隐藏算法来生成隐藏集合.AS将隐藏用户发出的查询发送到LBS提供商，LBS提供商将候选结果返回给AS用户并跟踪他们的位置。结果精简器基于用户的准确位置改进结果并将精化结果转发到隐私电话代理。电话代理进一步将结果传送到LBS应用。对于处于活动状态的查询，移动用户周期性地更新他的位置，直到它turn已过期。

3.4.2 Snet存储方案

因为在级别hþ1的Snet由最高级别h的两个Snets形成，所以我们使用二叉树T来存储Snet层次结构，其保持每个级别的Snets的父子关系。每个Snet由ðVs组成; Es; BsÞ保存为节点。对于每个节点，我们存储第3.3.2节中讨论的Snet的转换矩阵。 Snet中的段的总长度也被预先计算并存储在节点中。

图6示出了图1中的Snet层次结构的存储结构。 使第h级的第i个Snet为Snðh; iÞ，LðSnðh; i是Snðh中边的总长度; PSn是Snðh的转移矩阵; Þ。 对于我们的隐藏算法，隐藏的用户在同一个树节点。 换句话说，对于驻留在SnetSnð0中的查询发行者; j，与他搭档的用户将是Snð0中的用户; 在二叉树T中的一个祖先中。



4.匿名算法

我们提出了基于Snet层次结构的两种类型的隐私保护算法。第一个由算法2和3组成的是为单个用户设计的，另一个由算法4和5组成，用于一批用户。 Snet构建过程中，边缘与具有最高转移概率的边融合。因此，我们的算法将Snet作为基本隐藏单元，并以自下而上的方式检索存储Snet层次结构的二叉树。根据用户的挂钩资格在3.3.2节中，我们的算法首先在level0检索Snet，然后选择具有类似移动趋势的用户，满足我们的系统预定义的速度差和距离差限制。候选集由选择的用户形成，之后，用户将检查隐私简档。如果候选集不能满足用户的隐私简档，则算法搜索其父Snet。这些步骤继续，直到用户的隐私简档被满足，或者达到Snet层次结构的顶层。如果没有生成合格的掩码集，则相应的查询将被终止。由于发送到LBS提供商的所有查询必须通过AS ，如果它们被AS丢弃，则查询将从LBS提供者切割。因此，可以保留用户的隐私。

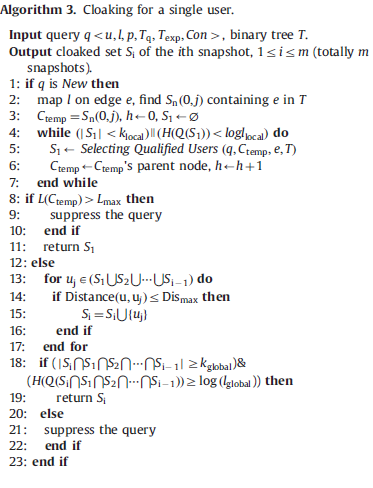
与单个用户的第一类算法相比，第二类旨在提高我们的隐私保护框架的效率。其针对一批用户同时生成匿名集以减少匿名时间。此外，用户的隐私 因为可以通过在用户之间共享隐藏的集来抵制查询抽样攻击。

4.1 单个用户的算法

当用户序列到达时，算法2在Snet中找到某个级别的合格用户，以形成每个用户的候选掩饰集合。算法3为单个用户生成匿名集合 。

算法2 选择合格的用户。

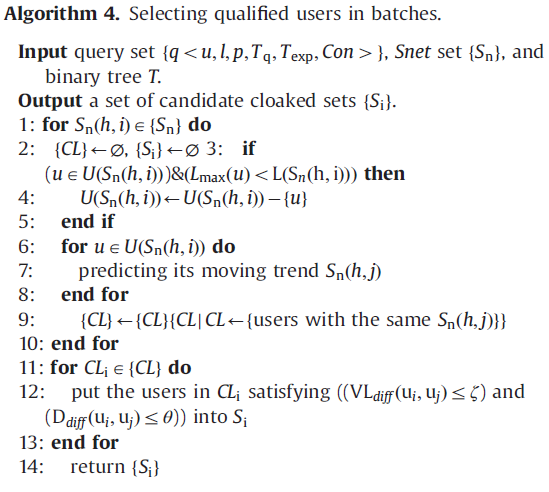
当选择每个级别的合格用户时，算法2首先预测用户u在离开原始用户时将移入的Snet（步骤1）。然后，它预测与u保持在同一Snet中的用户的移动趋势， 与u相同的移动趋势（步骤2-6）。 在挑出的所有用户中，只有那些满足速度差和距离差限制的用户将被选择作为合格匿名用户（步骤7-11）。



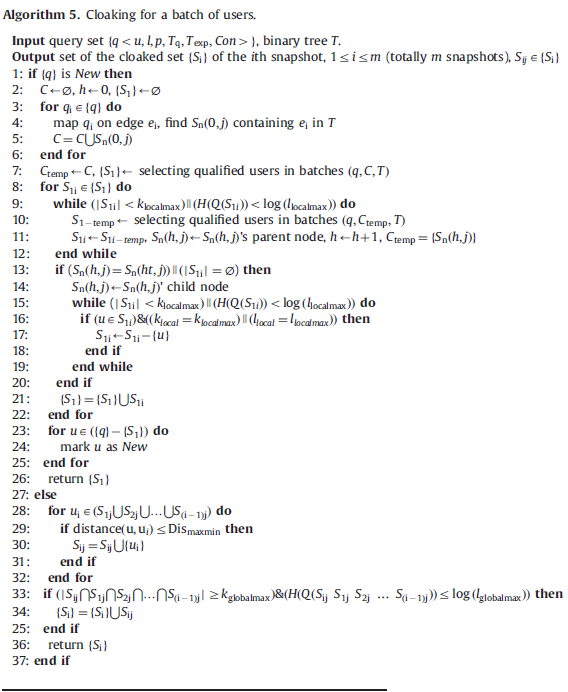
如算法3所示，用户u以ou，l，p，Tq，Texp，Con4的形式发送查询。 当从用户u的新状态接收到查询q时，ASmaps l进入路网。 算法3处理包含边e的S（0，j），其中u驻留作为初始掩盖集（步骤2）。 S（0，j）是二叉树T中的叶节点。算法遍历二叉树，直到满足u的k-匿名和l分集要求（步骤3-7）。 当隐藏集合中的边缘的总长度大于Lmax时，算法停止（步骤8-10）。如果查询处于活动状态，则该算法检查先前i-1个隐藏集合中的公共用户，添加满足 到掩蔽集合的距离限制（步骤13-17）。 还检查kglobal和lglobal多样性要求（步骤18-22）。

4.2 .一批用户的算法

由于多个查询可以同时到达AS，所以对于每个相应用户的隐藏是有效的。根据互惠原则，我们提出了一种由算法4和5组成的优化算法，该算法一次为一批用户生成隐藏集。另一方面，单个用户的算法容易受到查询抽样攻击。因此，我们引入k分享方法来抵抗这种攻击。在我们的系统中，生成的隐藏集由其中的所有用户共享。因此，在生成隐藏集对其中的所有用户有资格的同时，我们确保所有隐藏的用户的最严格的隐私要求，即klocalmax，kglobalmax，llocalmax， lglobalmax，Lmaxmin，Dismaxmin。 klocalmax，kglobalmax，llocalmax和lglobalmax指示由候选掩饰集中的用户定义的klocal，k全局，llocal，lglobal的最大值，Lmaxmin和Dismaxmin代表用户定义的Lmax和Dismax限制的最小值。当不能满足最严格的隐私要求时，请求这样的要求的用户应该从候选遮掩集中踢出。与用于单个用户的第一类型的算法类似，用于一批用户的第二类型的算法包括：两部分：算法4选择合格用户，算法5为一批用户生成匿名集。



对于未匿名用户，算法4删除用户u违反其Lmax限制（步骤2.4）。 然后预测所有用户的移动趋势，并将它们以相同的移动趋势聚集在一起（步骤5.8）。 对于每个聚类用户集，选择跟随速度差和距离差限制的那些作为合格用户（步骤10.12）。



算法5将所有用户映射到路网，在二叉树中找到相应的Snets（步骤3.6）。 它重复选择合格用户，直到满足Snet中所有用户的klocalmax和llocalmax值（步骤9.12）。当隐藏集中没有候选者或遍历步骤超出顶级时，我们使用klocalmax或klocalmax抑制用户， llocalmax要求，并向后遍历一级（步骤13.20）。 隐藏集合由驻留在其中的所有用户共享。对于以下快照，对于每个隐藏集合，我们检查驻留在先前i-1隐藏集合中的所有用户的最大距离限制（步骤28.32） 还将检查kglobal和lglobal要求（步骤33.35）。

4.3 框架维护

为了保持我们框架的长期有效性，我们在更新用户的历史轨迹和改变路网工作结构的情况下讨论维护策略。

4.3.1.用户的历史轨迹更新

4.3.2.道路网络结构更新

5.攻击恢复力分析

在本节中，我们分析所提出的算法对查询抽样攻击，查询跟踪攻击和重放攻击的恢复能力。

5.1 单个用户的算法

重放攻击：在重放攻击下（第3.1.3节），攻击者重复运行算法以生成具有输入u的S0i。可以看出，包含u。 链接能力可以关于所有S0i以最大概率12iif识别查询发布者。 然而，这实际上是不可能的。 隐藏集中的用户在速度差和距离差限制内共享相同的预测移动趋势，即隐藏集中的所有用户倾向于驻留在附近的路段中，即

查询抽样攻击：在查询抽样攻击（3.1.3节）下，攻击者观察隐藏集样本S1; S2; ...; Si与相应的查询集Q1; Q2; ...; Qi。 因此，链路能力可以被计算为： ¼1

查询跟踪攻击：通过考虑查询跟踪攻击的特性（第3.1.3节），我们介绍了kglobal和lglobal的原理。 普通用户的数量应该至少是全球的，并且公共查询集的熵不应小于logðlglobal。 因此，识别特定用户的查询的概率，即，可链接性链接，至少是1jQ1j，最多是1lglobal。

此外，攻击者可以组合重放攻击，查询抽样攻击和查询跟踪攻击来推断用户的查询内容。结果，链接性改变为链接。 ？ 其中Qi t表示在时间t包含u的查询集合Q，n是快照的数量，m是包含u的集合的数量。 因此，对特定用户的链接性是链接 ¼1 jPnt¼1Pm

示例1.我们假设系统中有五个用户。 他们的隐私资料部分列在表1中。 在表2中示出了隐藏的用户集合Si及其对应于快照i的每个用户的查询集合Qi。 在表2中，qj表示与类别cj有关的查询。

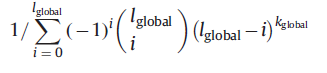
Table1

Table 2

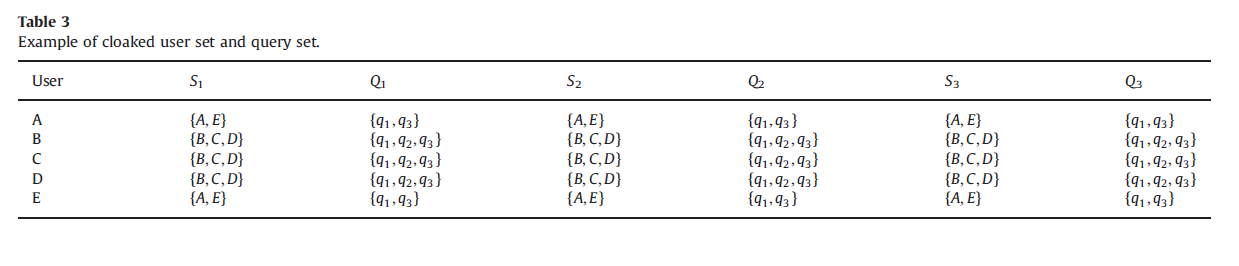
我们假设攻击者观察到一个隐藏的用户集样本{A; E}和对应的查询集样本{q1; q3}，但攻击者不知道该集合是谁生成的，也不知道查询和用户之间的关系。攻击者分别用A和E作为输入运行算法，得到相同的隐藏结果。然而，他仍然不知道查询发出者。 BK？计算为j f; E gj j fA; Eg j。 1，sois Prob.Sj E; BK。因此，重放攻击的链接能力是链接？ 。 Prob.Sj A; BK？ Prob.Sj A; BK？tProb.Sj E; BK？ ？ 12。 14。这是因为攻击者不能确保A是发布者，并且不知道A0s queryis q1。在查询抽样攻击下，如果攻击者观察到A在{A; E}，{A; B; D}在第一个快照，他可以推断A0s查询必须在{q1; q3}，概率为1/2。对于查询跟踪攻击，如果攻击者知道B0s隐藏用户集和隐藏查询集在snapshot1,2和3期间，他可以推断B0s查询的概率为1 = jQ1 \ Q2 \ Q3j .1 = 3。

5.2 一批用户的算法

由于为其中的所有用户生成隐藏集，一批用户的算法可以有效防御重放攻击和查询抽样攻击。因此，我们仅分析其对查询跟踪攻击的弹性（第3.1.3节）。 类似地，识别特定用户的查询的概率，即，可链接性链接 最多为1个lglobal。所有用户和查询之间的关联至少具有P lglobali = 0 - 1＆Sigma; i lglobal i lglobal？i？ ？kglobal种类的任务。 因此，概率



示例2.假设有五个相同的用户，如表1所示。 他们的隐藏用户集合Si和快照i的相应查询集Qi在表3中列出。 如果攻击者知道用户A0的隐藏用户集和查询集在snapshot1,2and3期间，他可以推断A0s查询的概率为1 = jQ1 \ Q2 \ Q3j = 1 = 2。



6.实验和评价

在本节中，我们评估我们提出的算法的有效性。由于根据我们的知识，路网中的连续查询没有隐私保护方法，我们将与另一个名为V-DCA的算法进行比较（Wangetal。，2012b） 为欧几里德空间。 V-DCA是一种连续查询隐私保护方法，在隐藏时考虑用户的速度和加速度特征。 然而，它不采取底层路由网考虑，更不用说建立网络层次结构以便于隐藏过程。 提出评价标准和度量，随后是实验设置描述。然后详细讨论评价结果。

6.1.评估标准和指标

我们从三个方面评估算法：隐私保护能力，服务质量和性能。编码算法为满足其隐私简档的用户生成隐藏集。 预定义的参数，例如kglobal和klocal，是用户的隐私要求。然而，算法的有效性取决于伪装集合的实际实现值。 因此，我们使用真实的归档值作为度量来评估我们的框架。相应地，我们将这些值表示为Klocal，Kglobal，Llocal，Lglobal，Len和Dis。

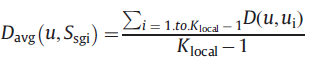
6.1.1隐私保护能力

对于连续查询，隐私级别取决于公共用户及其对所有隐藏集的查询。我们使用隐私来衡量连续查询中用户的隐私级别，可以计算为隐私 ¼Kglobal？ Lglobal

更高的隐私意味着更好的隐私保护。类似地，我们使用成功隐藏的快照n的数量来测量算法的维护。更好的隐私保护方法可以为用户提供更长的服务，即更大的n。

6.1.2服务质量

我们评估服务质量与伪装片段集合中的用户的平均距离Ssg作为查询答案在更小的隐藏区域内更准确。因此，较小的距离值表示更好的服务质量。单用户，平均距离Davgðu; 第i个快照的隐藏段集合Ssgi的SsgiÞ被计算为



其中u是查询发行者，ui表示在Ssgi中用u隐藏的用户i。 n个连续快照的平均距离为



同时，对于一批用户，平均距离



其中U是用户集，ui表示居住在U中的用户i。n个连续快照的平均距离是



6.1.3.性能

我们从两个角度评估我们的框架的性能方面：隐蔽成功率和掩蔽时间

1. 隐藏成功率：成功隐藏的用户的百分比：



其中S是成功隐藏用户的集合，U是所有查询发布者的集合。更高的隐蔽成功率对应于更好的性能。

1. 隐藏时间：我们使用ti表示快照i的隐藏时间。 对于良好执行的隐私保护机制，掩蔽时间应该足够短以实现愉快的用户体验。

6.2 实验设置

我们使用Thomas Brink hoff基于网络的移动物体发生器（Brinkhoff，2002）在Olden burg.2000移动用户的路线图上生成沿着道路网络以中等速度移动50个快照。用户的隐私要求作为klocal和llocal，在一定范围内随机设置。例如，klocal和llocal的默认范围是2-5。 第3.2节中提到的最大距离限制在1公里到6公里之间。 我们的实验中使用的参数列在表4中。 的如果在以下实验中没有具体描述，则使用默认值。

模拟实验使用具有Dual Dore 2 .13GHz CPU，4GB RAM存储器和Windows7？32最终操作系统的PC来进行。 我们用Cþþ实现算法。 对于所有图形，SINGLE表示针对单个用户的所提出的隐藏算法，相应地，Batch是针对一批用户的。 我们重复运行每个实验10次，取平均值作为评估结果。标准偏差误差可以忽略不计。

6.3 评价结果

图7显示了V-DCA和我们提出的两种类型的算法的隐私保护能力。 图7（a）表明，当距离超过4km时，我们的算法的性能优于V-DCA。具体来说，SINGLE的隐私保持常数，直到距离限制超过4公里，而Batch的隐私线性增长，并在其中执行最好的。 图7（b）显示V-DCA和SINGLE的隐私随着klocal和llocal的改变（称为本地隐私）而保持几乎稳定，而Batch的隐私保持增加并且保持远高于V-DCA和SINGLE。 如图所示。 如图7（c）所示，随着时间的推移，即快照数量增加，BATCH的私密性在三种算法中保持最高。

结果如图1所示。 7表明BATCH在三种算法中提供最好的隐私保护。通常，SINGLE执行比V-DCA更好。

图8示出了所有三个算法随着距离限制的增长或者本地隐私值（即，klocal和llocal）的增加而为更多快照拍摄提供隐私保护。 。如图8（a）所示，当距离限制超过3km时，V-DCA执行严格的距离限制并保持相对较少数量的快照。 SINGLE由于考虑了用户的移动趋势和距离关系，性能优于V-DCA。 BATCH更容易受距离限制的影响，因为它需要平衡隐蔽区域中的隐私要求，用户的速度和用户之间的距离。它执行最好的，可以实现近50快照与更宽松的距离限制。图8（b）表明，本地隐私几乎不影响SINGLE或BATCH的主要持久性。即使当地隐私非常低，他们表现相当不错。当本地隐私大于4时，V-DCA可以成功隐藏50个快照。这是因为更多的用户被隐藏了第一快照，并且是被选择到以下快照的隐藏集合中的候选。 8表明较宽的距离限制和较高的本地隐私有利于查询的维护。然而，保持的快照的数量缓慢增长，而距离限制和本地隐私大大增加。

我们使用平均距离来测量服务质量。 如图9所示，BATCH具有比其他两个更大的平均距离，因为它考虑所有用户而不是隐藏区域中的中心用户提供有效的掩蔽功能。考虑到隐藏过程中的移动趋势和距离差异，SINGLE可以提供更好的质量 的服务比长期的V-DCA。 这三种算法可以有效地选择在以下快照中保持在一起的用户，因为他们考虑用户的运动特征。此外，所有他们执行相当稳定与距离限制，本地隐私和快照数字的变化。 7和8，可以告诉我们，我们提出的算法在隐私和服务质量之间有良好的平衡。

图10评估了受距离限制和本地隐私影响的成功率。显然，在相同的距离限制和本地隐私要求下，SINGLE和BATCH可以获得比V-DCA更高的成功率，因为它们考虑了基础路由网络属性。 此外，由于该区域内所有用户的隐藏集的有效性，BATCH执行最好。我们提出的算法从长远来看可以维持比V-DCA更多的用户。特别地，BATCH可以成功地匿名约45％的用户 七到第50快照。

图11显示了使用这三种算法的每个用户的平均隐藏时间。可以看出，SINGLE占用了V-DCA占用的十分之一的时间，并且BATCH仅占用SINGLE占用的时间的二十分之一，除了第一 快照。 主要原因是SINGLE和BATCH基于Snet层次结构，这提高了检索用户被掩盖在一起的速度。此外，BATCH掩盖用户的批准，而不是一次一个用户，因此，它是更有效率。

从所有的评估结果，我们可以得出结论，我们的提出的算法可以实现更好的隐私保护V-DCA同时保持服务质量和提高成功率。由于建立Snet的启动过程可以减少伪装时间。

7.结论

在本文中，我们提出了一种快速连续的LBS查询隐私保护框架在路网中。如上所述，框架考虑了路网的拓扑属性提供隐私保护机制单用户和一批用户。分析和实验结果表明我们的算法可以抵抗典型的攻击在路网中有效保护用户的隐私隐私。