文章编号：2095-2163(2021)07-0156-07 中图分类号：TP391 文献标志码：A

基于连续查询的语义位置隐私保护算法

贾媛媛[1]，史志才[1,2]，方 凯[1]
（1 上海工程技术大学 电子电气工程学院，上海 201620；2 上海市信息安全综合管理技术研究重点实验室，上海 200240）

摘 要： 针对用户连续位置查询请求服务中未考虑语义信息而导致用户敏感语义泄露问题，为了实现对道路网络上客户端的查询隐私、位置隐私和语义位置隐私保护，本文提出一种离线轨迹聚类和语义位置图相结合的算法来进行隐藏用户的选择，使隐藏用户的位置具有明显的多样性和不同的语义以及多样化的服务请求，有效保护客户端的语义和位置隐私。在具有 2 个定义指标的真实地图上评估了该算法的有效性，整个连续查询道路网络服务的过程中，有很好的成功率和查询处理时间。同时与现有的其他可信第三方模型算法进行了对比分析，验证了本文算法的有效性。

关键词： 位置隐私保护；连续查询；轨迹聚类；语义位置图；语义位置隐私

Semantic location privacy protection algorithm based on continuous query

JIA Yuanyuan[1], SHI Zhicai[1,2], FANG Kai[1]
(1 School of Electronic and Electrical Engineering, Shanghai University of Engineering Science, Shanghai 201620, China;
2 Shanghai Key Laboratory of Integrated Administration Technologies for Information Security, Shanghai 200240, China)

【Abstract】 Since the user´s continuous location query request service without considering semantic information , to realize the protection of query privacy, location privacy and semantic location privacy of the client on the road network, this paper proposes an algorithm of offline trajectory clustering and semantic location map to choose hidden users, so that the hidden users´ locations have obvious diversity, different semantics and diversified service requests effectively protect the semantics and location privacy of the client. The effectiveness of the algorithm is evaluated on a real map with two defined indicators, the entire process of continuously querying road network services has a very good success rate and query processing time. At the same time, compared with other trusted third-party model algorithms, the validity of this algorithm is verified.

【Key words】 location privacy-preserving; continuous query; trajectory clustering algorithm; semantic location graph; semantic location privacy

0 引 言

位置大数据为人们的生活带来了巨大的改变，在给人们带来显著收益的同时，也带来了个人信息泄露的危险。2014 年，iPhone 用户隐私泄露事件披露出苹果公司曾私自记录每次使用 LBS（基于位置的信息服务）应用时的位置信息，从而造成用户的大量位置信息泄露[1]。因此，在用户使用 LBS 应用时，如何保护用户的个人隐私成为一个待解决的问题。

现有的隐私保护方法扩展了查询客户端的范围，一些研究者们将 $k-1$ 个其他用户也包括进来[2-4]；但在这个过程中，会将具有不同移动趋势的其他请求结果移动对象包括起来，这可能是攻击的来源。2007 年，Liu 借鉴数据发布隐私处理中的 l-差异性模型的思想，提出了位置 l - 差异性模型，以防止位置同质性攻击[5]。但最初提出的位置差异性模型忽略了用户的位置语义。直观上来讲，用户位置带有语义信息，如用户现在位于早餐店，说明用户可能在吃早餐；用户在医院，则该用户很大概率有某种疾病。为了保护用户的语义位置，Damiani 等人[6]采用了语义位置隐藏方法，该方法允许用户定义个性化的隐私配置文件，该配置文件说明了指定的敏感场所类型和每种类型所需的隐私程度。但是这种语义位置掩盖方法仅被设计为在不受限制、不受约束的空间中工作移动；但在现实环境中，移动用户大部分在道路网络上，因此可能导致隐私泄露。Lee 等人[7]提出了一种位置隐私保护技术，该技术可以保护位置语义免受对手的攻击，采用第三方可信匿名服务器，该服务器使用位置语义信息来掩盖用户的语义位置。同样，研究时只考虑了欧几里得空间，在路网限制下会导致隐私泄漏。又有一些学

基金项目：上海市信息安全综合管理技术研究重点实验室开放研究课题基金（AGK2019004）。

作者简介：贾媛媛（1995-），女，硕士研究生，主要研究方向：隐私保护、网络信息安全；史志才（1964-），男，博士，教授，CCF 高级会员（No. 06601S），主要研究方向：计算机网络与信息安全、隐私保护。

收稿日期：2021-04-06

者提出多样化的服务请求[8]，从而满足 k - 匿名性和 l - 多样性隐私条件。然而，确定移动用户在线的语义位置是一个挑战，这使得绝对隐私保护的实现更具挑战性。

本文提出了一种保护用户语义位置隐私的连续查询道路网络服务隐私保护算法，贡献如下：

(1)提出一种离线聚类移动用户轨迹的算法，并使用在线导出的移动趋势来帮助选择匿名用户，提高客户端的隐私保护程度。

(2)提出一个生成语义位置图的算法，以帮助确定在线用户的语义位置，利用导出的离线轨迹聚类算法与语义位置图相结合来保护用户在路网下连续查询的语义位置隐私。

1　系统架构及相关知识

1.1　系统架构

为了避免客户端计算量过大，本文采用由移动客户端(MC)、匿名服务器(AS)和基于位置的服务器(LBS)组成的可信第三方体系结构[9]。蜂窝服务提供商为匿名服务器提供了用户的初始轨迹和服务请求(查询内容)数据库。位置和服务请求数据库可以通过客户端定期电话呼叫和 LBS 查询服务进行获取，如果没有初始数据，匿名服务器会收集几天的位置服务请求数据，在移动用户请求 LBS 的过程中，将从用户那里获得更多的位置数据。同时允许 MC 使用隐私配置文件 k，即期望匿名的用户数。

系统的核心是 AS，AS 由隐藏存储库(CR)和离线轨迹聚类引擎(TCE)组成。系统的功能可以定义为：

(1)隐藏存储库保存一些以前隐藏的结果，并使用其来生成新的隐藏区域。

(2)轨迹聚类引擎对移动用户的轨迹数据库进行聚类，结构如图 1 所示。

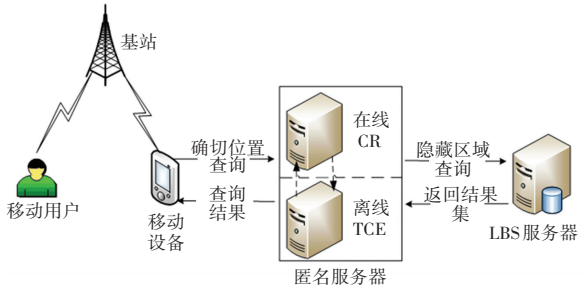


图 1　系统框架

Fig. 1　System framework

1.2　路网模型

道路网由一个有向图 $G=(V,E)$ 表示，由交叉点 $V=(n_0,n_1,\dots,n_n)$ 和定向边 $E=((S_{id},n_in_j)\mid n_i,n_j\in V)$ 表示。$Edge=(S_{id},w_0,w_1,con,n_in_j)\in e$ 表示连接实际道路网络中 2 个交叉点 n_i 和 n_j 的路段，其属性包括路段标识符 S_{id}、路段分类 w_0、交通密度 w_1 和服务请求类型 $con(sr_1,sr_2,\cdots,sr_n\in con$，其中每个 sr 是一个服务请求)。研究中将根据路段的速度限制对其进行分类。路段分为主要路段(限速< 40 km/hr)、普通路段(40 km/hr≤限速<70 km/hr)、公路(70 km/hr≤限速<100 km/hr)、高速公路(限速≥100 km/hr)，分别用 p、a、h、ex 表示。因此，路段分类 w_0 可用 p、a、h 或 ex 表示。例如，$w_0=ex$ 表示快速路分类。将用户在时间戳为 t 和坐标为 (x,y) 的路段 S 上的位置表示为 $l=(S_{id},x,y,t)$

定义 1　轨迹　由 $TR=\{t_{id},l_0,l_1,\cdots,l_n\}$ 表示的轨迹，是道路网络上用户随时间变化的位置 l_0，$l_1,\cdots,l_n$ 的时间顺序序列，由轨迹标识符 t_{id} 唯一标识。对于一个移动用户来说，对应的行程与起始位置和目的地位置形成一条轨迹。

定义 2　语义位置　语义位置是一个区域，在该区域中聚集的用户具有相似的情景信息，如年龄、性别、活动等。学校、医院、公司等都可以是语义位置[10]。

定义 3　类簇　对于给定的轨迹集 $T=\{TR_1,\dots,TR_n\}$ 在道路网络上，类簇 cw_0 是在具有相似段分类 w_0 的所有段中的所有段簇 cs_{id} 的集合。因此，类簇是 cp、ca、ch、cex，其中每个类簇通常可以表示为 cw_0。

定义 4　集群　对于给定的轨迹集 $T=\{TR_1,\dots,TR_n\}$ 在道路网络上，集群 C 是所有类簇的集合，即 $C=\{cp,ca,ch,cex\}$。因此，C 表示具有段分类 w_0 的所有类簇。

2　轨迹聚类算法及语义位置图

2.1　轨迹聚类算法

聚类算法将数据库对象分组为一组有意义的子类，所以根据用户在同一路段上的相似运动特征，离线将其轨迹聚类成子类[11]。在一个网段内的用户可以被认为是网络接近的，因此在移动中将显示一组子类特征，这些特征将反映该路段上任何在线移动对象的特征。因此，可以从离线特性中估计该对象的加入是否会在将用户伪装成在线特性之前保护客户端的隐私。根据路段 id、服务请求、流向、速度、时间、路段长度及其速度限制，将离线移动用户的轨迹聚类成沿路段的子类。利用这一先验信息，

提出了一种基于用户轨迹的轨迹聚类算法。考虑一组由 $T = \{TR_1, \ldots, TR_n\}$ 表示的一组轨迹在 *TCE* 中，检查从第一个位置 l_0 到最后一个位置 l_n 的单个轨迹 $TR_i = \{t_{id}, l_0, l_1, \cdots, l_n\}$。取轨迹中每两个连续点，例如 l_i and l_{i+1}，并使用地图匹配方法检查以获得与 2 个路段相交的道路交叉点[12]。将获得的连接节点作为新点插入正在检查的轨迹中的 l_i 和 l_{i+1} 之间。在检查给定轨迹 TR_i 中的每个点之后，TR_i 中添加的连接节点序列将作为轨迹分割点，用于沿段将轨迹分割为轨迹碎片（*tf*）。例如，在图 2 中，轨迹 *C* 具有沿段 2 和段 3 断裂的 2 个轨迹碎片。分析单个轨迹碎片所经过的时间段，并将其分为一天中的不同时间段（*tb*）。对 *T* 中的所有轨迹集重复此过程。

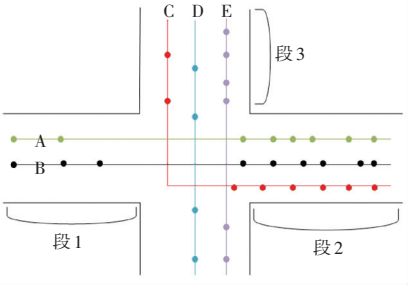


图 2 轨迹道路网沿路段分为轨迹碎片

Fig. 2 Trajectory road network segment is divided into trajectory fragments along the road

根据路段 *id*、流向、速度（*v*）、路段长度、行程时间（*tb*）和该路段的速度限制 *vL* 对轨迹碎片进行分组，形成一组基簇。然后，计算出一个段中每个基簇上产生的交通密度 w_1 作为轨迹碎片的数量。交通密度给出一天中给定时间段内具有特定特征用户的可能数量。例如，在图 2 中，如果所有轨迹片段具有相似的特性，那么段 2 将具有 3 的交通密度，而段 1 具有 2 的密度。同一段 *id* 下的一组基簇构成一个段簇 cs_{id}。该算法根据 $b = (S_{id}, w_0, sr, v, w_1, tb, n_i n_j)$ 的段 *id* 输出一个基本簇，作为 *tb* 时该段上的用户特征组。最后，将相似道路分类 w_0 下的所有路段簇抽象表示为 cp、ca、ch、$cex \in C$ 的类簇，根据路段分类进行抽象，将有助于隐藏具有不同位置语义的用户。一组类簇构成一个 *C* 簇，具体描述如算法 1 所示。

算法 1 轨迹聚类算法

输入 <有向图 G >，< $T = TR_1, TR_2, \ldots, TR_n$ >，< $TR_i = t_{id}, l_0, l_1, \ldots, l_n$ >

0 输出 < 集群 $C = cp, ca, ch, cex$ >

1：有向图 *G* 由节点 $V(n_i, n_j \in V)$ 和边 E（$e \in E$）组成；

2：for $TR_i, i = 1 \ldots n$ do

3：检查每个 l_i 和 l_{i+1} 以获得路口节点 n_i；

4：将获得的节点作为新点插入 l_i 和 l_{i+1} 之间；

5：使用新的节点将 *TR* 分解为 *tf*；

6：为每个 *e* 分配唯一标识 S_{id}；

7：将所有 *tf* 的 *tb* 进行分类；

8：根据 S_{id}，v，vL，tb，$n_i n_j$ 和 $|n_i n_j|$ 将所有 *tf* 沿着 *e* 分组成 *b*；

9：end for

10：在每个 *b* 中评估 w_1；

11：将每个 *e* 中的所有 *b* 分组为 cs_{id}；

12：对所有 cs_{id} 分组 w_0 和 cw_0 相同；

13：将所有 cw_0 输出为 *C*

2.2 语义位置图

本节中，建立一种语义位置图的算法，以帮助选择要隐藏的用户，从而保护语义位置隐私。将语义位置隐私定义为不同时间点用户访问量，采用用户到访时间作为定义语义位置的标准。例如晚上十点，用户可能访问酒吧、但是不可能访问早餐店，这里可以采用一个时间点来标识一个语义位置。但是晚上九点，用户可能访问娱乐场所、医院等等，仅仅采用一个时间点的用户访问量是不够的，因此采用一个 24 维的向量来表示语义位置[13]。一个语义位置即如式（1）所示：

$$SL_U = \{L_0, L_1, \ldots, L_{23}\} \tag{1}$$

其中，$L_0, L_1, \ldots, L_{23}$ 分别表示某一个小时内某个语义位置的用户访问数，其中 *u* 是在 $L_0, L_1, \ldots, L_{23}$ 提供的服务类别，例如，将诊所、卫生站、医院、牙科诊所等归为“健康”类别，其中“健康”是指提供的服务类别，进行分类是为了避免用类似的服务隐藏用户位置，以增强其语义位置的 l - 多样性。每个语义位置都有一个特定的区域，比如学校有对应的区域，不在这个区域的位置，就属于别的语义位置，利用语义位置集 *SL*，采用地图匹配的方法在路网模型的各个路段上精确定位相关的位置。然后，生成一个语义位置图 *G*’ 来描述各种语义位置及其提供的服务。语义位置算法如算法 2 所示。

算法 2 语义位置图算法

输入 < 有向图 G >，< $SL = (L_0, L_1, L_2, \ldots\ldots, L_{23})$ >

输出 <语义位置图 G' > 和 < SLu >

1：有向图 *G* 由节点 $V(n_i, n_j \in V)$ 和边 E（$e \in E$）组成；

2：for $L_i, i = 1, \ldots, n$ do

3：根据 u 进行标记 L_0，L_1，L_2，.....，L_{23}

4：使得同一组 L_0，L_1，L_2，.....，L_{23} 在相同 u 下

5：将每个组输出为 SLu

6：end for

7：for L_i，$i = 1...n$ do

8：插入到 G

9：返回 G'

10：end for

3　隐私保护算法

在这一部分中，使用轨迹聚类算法和语义位置图来开发隐私保护算法。移动客户端（MC）以 $q = (q_{id}, l, t_i, tf, k, sr)$ 的形式发送新的查询 q，其中 l 是位置坐标，t_i 是查询启动时间，tf 是过期时间。服务请求是 sr，隐私配置文件 k，q_{id} 是客户端 id。当接收到新的查询 q 时，AS 确定了 q 的时间，并使用该位置来查找将其发出的段、段的分类、与 G 中的 q 相关联的语义位置 L 以及其所属的服务提供的 SL_U 的类别。

定义一个交通密度阈值 σ，低于这个阈值就不适合执行在线隐藏。$w_1 \geqslant \sigma$ 意味着会在 tb 时间段找到足够的移动用户。交通密度阈值 σ 由 AS 根据历史确定。

为了在线查找匿名 MC 的用户，TCE 搜索除包含 MC 的类簇 cw_0 以外的所有类簇，随机查找 $k-1$ 个其他类簇，并从所选类簇中选择一个时间 tb 满足 q 时间的基簇。选择的基簇必须满足设计的隐藏条件，以帮助实现采用随机段采样方法的绝对隐私保护。隐藏 C 条件：全部选定的基簇必须满足以下几方面：

（1）数量是 $k-1$。

（2）第（$k-1$）个选择的基簇 b_{k-1} 时间段 tb_{k-1} 必须满足查询 q 的时间 t 和第一个选择的基本簇 b_1 的时间 tb_1，即 $t \in tb_1$；$t \in tb_{k-1}$。

（3）任何选定的基簇交通密度满足 $w_1(b) \geqslant \sigma$，$w_1(b_1) \geqslant \sigma$，$w_1(b_{k-1}) \geqslant \sigma$。

（4）所选基簇 $sr(b_{k-1})$ 的服务请求 $sr(b_{k-1})$ 不能与 q 和第一个所选基簇 b_1 的服务请求相同，$sr(b_1) \neq sr(b_{k-1}) \neq sr(q)$。

（5）第（$k-1$）个所选基簇中，由所选段上语义位置 L 服务提供 $SL_U(b_{k-1})$ 的类别不应与 q 和第一个所选基簇 b_1 的类别相同，即 $SL_U(b_1) \neq SL_U(b_{k-1}) \neq SL_U(q)$。

（6）第（$k-1$）个选择的基簇的段分类 $cw_0(b_{k-1})$ 不应与 q 和第一个选定的基簇 b_1 相同，即 $cw_0(b_{k-1}) \neq cw_0(b_1) \neq cw_0(q)$。

当满足隐藏条件时，AS 将 $k-1$ 个其他在线用户 q' 伪装成具有 $k-1$ 个选定基本簇的特征，这些特征从其各自的段转移到 q 个隐藏区域，如果不满足这些条件那么所有查询都将被抑制。用户 id 被删除，并替换为准 id，然后将其放入隐藏区域 R_i 中，其中 i 代表具有隐藏区域标识 R_{id} 的第 i 个快照。然后将包含 k 个用户的隐藏区域 R_i 转发到 LBS。

对于连续查询 LBS，查询将由 AS 在周期内（tf-ti）周期性地发出。如果用户请求连续服务，则 AS 将请求第一个快照的连续服务的用户隐藏起来，以便在整个查询期间保持相同的隐藏用户，从而始终确保隐藏条件。此外，保留一个存储库，其中包含已隐藏的用户请求，以便在以后与同一段相关时使用。满足隐藏条件匿名集的数目用 n 表示。隐私保护算法如算法 3 所述。

算法 3　隐私保护算法

输入　< 查询 $q = q_{id}, l, k, t_i, tf, sr$ >，< 类簇 $cw_0 = (cp, ca, ch, cex)$ >，< G' >，< SL_U >

输出　<隐藏区域>

1：for q 在 $t = t_i = i$ 发布；

2：确定 q 的 t_i，e，cw_0，L 和 SL_U；

3：在 $cw_0(b_1) \neq cw_0(q)$ 和 $t_i \in tb_1$ 的 e 中随机输出基簇（b_1）；

4：确保 $w_1(b_1) \geqslant \sigma$，$SL_U(b_1) \neq SL_U(q)$ 且 $sr(b_1) \neq sr(q)$；

5：转到 10 行；

6：for $k > 2$ do

7：使得 $w_1(b_{k-1}) \geqslant \sigma$；$cw_0(b_{k-1}) \neq cw_0(b_1) \neq cw_0(q)$；$sr(b_1) \neq sr(b_{k-1}) \neq sr(q)$；$SL_U(b_1) \neq SL_U(b_{k-1}) \neq SL_U(q)$；

8：end for；

9：if 满足 7 行条件 then

10：在各自的 e 上选择特征为 b_1 到 b_{k-1} 的在线 q'；

11：用 $k-1$ 个其他 q' 将 q 隐藏到匿名区 R_i 中；

12：用准 id 替换 q_{id}；

13：分配区域标识 R_{id}；

14：否则禁止查询；

15：end if

16：将 R_i 转发到 LBS；

17：for $t > t_i = i$ do

18：重复执行 2-17；

19: end for

4 安全性分析

本文使用轨迹聚类和语义位置图的算法能够抵御查询同质性攻击、位置同质性攻击。查询同质性攻击指的是攻击者通过当前匿名集发起的相同查询语义来推断出用户的敏感信息。为了避免查询同质性攻击,由于本文算法避免相同服务的 2 个用户在同一个匿名集中,所以攻击者推出用户的概率为 $1/k$。对于位置相似攻击,本文算法使用不同的分类来隐藏不同位置的用户,保证客户端语义位置链接到用户的概率为 $1/k$。

5 实验及结果分析

5.1 实验数据

本节主要通过实验验证用户在连续查询时与 LBS 服务器的交互情况、在相关参数变化下对本文算法性能的影响以及与 Kamenyi 等人[14]提出一种隐私保护算法 VD-DCA(Authenticated Velocity-Distance based Dynamic Cloaking Algorithm)方法进行仿真实验比较。

本文实验算法均采用 JAVA 实现,硬件平台为 Intel(R)Core(TM) i5-8265U CPU 1.80 GHz,8 GB 内存,操作系统为 Microsoft Windows10。实验数据采用真实数据:上海市的公路网络数据[15],共包括 106 867 个顶点(结点),213 734 条道路(边)并从地图上提取 20 148 个 POI,其中包括上海市 50 个不同类别的服务,作为语义位置。每隔 5 s 记录了 100 个快照。实验设置了 10 000 个发出查询请求的用户,并在上海地图上以不同的速度移动,对其分配了不同的服务请求。根据本文的分类和路段 id,对所有路段进行速度限制。

5.2 实验结果分析

本文从成功率、查询处理时间对算法的性能进行评估。对此拟做研究分述如下。

(1)成功率。定义为活动查询期间内成功隐藏快照的数量 n 与所有隐藏区域数之比。成功率是衡量一个位置隐私保护算法的有效性的指标,成功率越大,说明隐私保护度越好[16]。其数学公式可写为:

$$successrate(s)=\frac{n}{C_{all}}\times 100\% \tag{2}$$

(2)查询处理时间。查询处理时间是算法查找 $k-1$ 其他用户所需的时间。对于由 n 个快照组成的活动周期的连续查询,平均隐藏时间 T_{avg} 可以计算为;

$$T_{avg}=\frac{\sum_{i=1}^{n}TR_i}{n} \tag{3}$$

平均隐藏时间越短,说明算法越高效。其中,TR_i 是查询在区域 R 中的隐藏时间。

5.2.1 参数变化对性能的影响

通过对 k 个用户和 l 个不同段($k-l$)值的隐藏区域的快照查询,研究了本文的定义度量效果。快照数与查询处理时间如图3所示。从图3可以看出,第一个快照的处理时间很长,这是因为处理需要很多时间来满足初始隐藏条件。从最初的快照到前十个快照,查询处理时间急剧减少,减少原因可能是隐藏用户在初始查询时请求连续服务,因为会涉及相同的用户,所需时间则会较少。从第 10 个快照到第 20 个快照的处理时间略有增加,这可能是由于用户更改了路段,因此需要进行一些处理。此后,处理时间缓慢减少,这种趋势可能是由于引入了存储库查询,从而减少了处理时间。一般来说,即使 $k-l$ 值增加,查询处理时间也会随着快照的增加而减少。

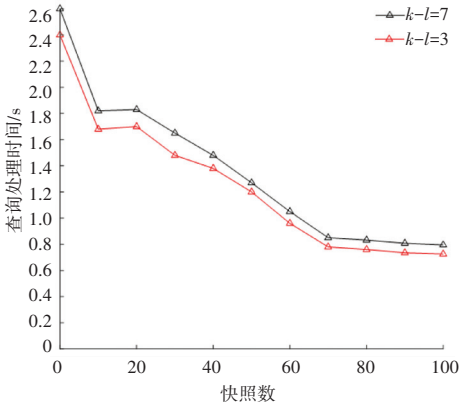


图 3 快照数与查询处理时间

Fig. 3 Snapshots and query processing time

快照数与成功率的关系曲线如图 4 所示。从图 4 可以看出,前 10 个快照的匿名化成功率几乎保持不变,这是因为用户在 t_i 时查询一直隐藏,因此大多数快照都符合隐藏原则。在第 10 个快照到第 20 个快照之间,成功率急剧下降,这是由于移动对象改变了具有不同分类和不同语义位置的片段,因此大多数快照无法满足隐藏条件。此后,由于逐渐引入存储库查询,成功率稳步提高,因此大多数查询都满足隐藏条件。当 $k-l$ 增加时,也出现类似的趋势。一

般情况下，本文算法在评估的 100 个快照中，每个快照的平均成功率高达为 87.8%。

5.2.2　匿名器的性能对比

本节主要从匿名的查询处理时间和匿名成功率两方面将本文方法与 Kamenyi 等人[14]提出的隐私保护算法 VD-DCA 方法进行仿真实验比较，移动客户端将其隐私配置文件设置为 $k-l=3$。

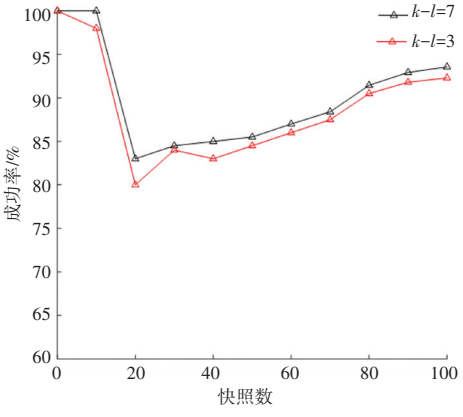
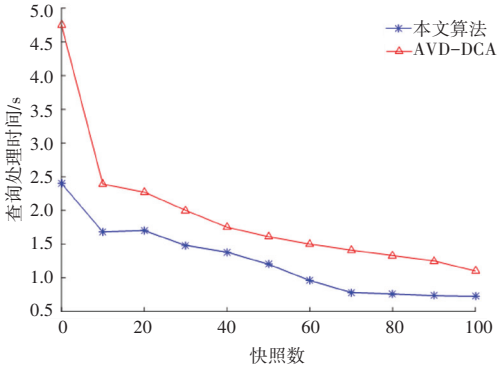


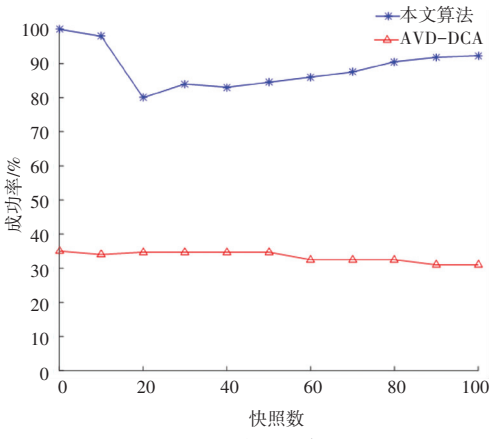
图 4　快照数与成功率

Fig. 4　Number of snapshots and success rate

匿名器的性能对比如图 5 所示。由图 5 可知，在匿名器的查询处理时间和匿名成功率上，随着快照数增大，本文算法在所有快照值下的性能都优于 VD-DCA。因为 VD-DCA 算法是基于用户的安全特性、速度上的相似性以及采用基于最小生成树的掩蔽机制保护用户隐私。然而，采用基于最小生成树的掩蔽机制会增加掩蔽时间，从而影响系统性能。所以在单个匿名器的查询处理时间和成功率上，本文方法相对于 Kamenyi 等人[14]的 VD-DCA 方法有很大优势。



（a）查询处理时间



（b）匿名成功率

图 5　匿名器的性能对比

Fig. 5　Anonymizer performance comparison

6　结束语

本文通过离线轨迹聚类算法和语义位置图来保护用户当前绝对隐私，同时在真实地图上评估算法的有效性，在整个连续查询道路网络服务的过程中，一定查询处理时间内取得较高的匿名成功率。然而，为了确保这些技术开发能够有效地工作，必须制定有利于保护用户隐私的政策。政策发展与技术考虑同样重要，以便做出必要改变适应技术进步，因此在下一步工作中将会考虑制定隐私保护政策。

参考文献

[1] 李志鹏. 位置隐私保护技术的研究[D]. 哈尔滨：哈尔滨理工大学，2018.

[2] PINGLEY A, ZHANG Nan, FU Xinwen, et al. Protection of query privacy for continuous location based services[C]//2011 Proceedings IEEE INFOCOM. Shanghai, China：IEEE, 2011：1710-1718.

[3] 穆良，程良伦. 基于k-匿名位置隐私保护的自适应学习模型[J]. 计算机工程与应用，2017，53(18)：89-94，101.

[4] TRIPATHY B K, MITRA A. An algorithm to achieve k-anonymity and l-diversity anonymisation in social networks[C]// 2012 Fourth International Conference on Computational Aspects of Social Networks. Sao Carlos, Brazil：IEEE，2012：126-131.

[5] PAN Xiao, CHEN Weihang, WU Lei, et al. Protecting personalized privacy against sensitivity homogeneity attacks over road networks in mobile services[J]. Frontiers of Computer Science，2016, 10(2)：370-386.

[6] DAMIANI M L, SILVESTRI C, BERTINO E. Fine-grained cloaking of sensitive positions in location-sharing applications[J]. IEEE Pervasive Computing, 2011, 10(4)：64-72.

[7] LEE B, OH J, YU H, et al. Protecting location privacy using location semantics[C]//Proceedings of the 17th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. San Diego, California, USA：ACM，2011：1289-1297.

[8] 曹敏姿，张琳琳，毕雪华，等. 个性化(α，l)-多样性 k-匿名隐私保护模型[J]. 计算机科学，2018，45(11)：180-186.

（下转第 165 页）