基于车流量的兴趣点查询隐私保护

晁稳，辛阳
（北京邮电大学网络空间安全学院，北京 100876）

摘要：路网环境下兴趣点查询在生活中路网环境下兴趣点查询隐私保护应用广泛，如何在保证用户位置信息安全的情况下提高用户服务质量是近年来 LBS（位置服务）领域研究重点；一方面路段在不同时间段车流量高峰不同 POI 推荐排序也应不同，同时兴趣点查询过程结合位置隐私保护算法，防止查询过程中伪服务器获取用户位置和查询内容；另一方面根据路况实际情况所能查询到的兴趣点数量也是影响服务质量的因素，根据原始路网数据组织兴趣点分布信息，并通过合并无用兴趣点路段，解决查询返回兴趣点较少问题，提高锚点匿名度。最后从兴趣点查询数量以及查询准确度和安全性方面对本文方法进行分析，通过实验验证该方法的有效性。

关键词：位置隐私保护；兴趣点存储组织结构；车流量；用户服务质量
中图分类号：TP309

Privacy protection of interest point query based on traffic flow

Chao Wen, Xin Yang
(School of Cyberspace Security, Beijing University of Posts and Telecommunications,Beijing 100876)

Abstract: Point of interest query under road network environment is widely used in life. How to improve the quality of user service under the condition of ensuring the safety of user's location information is the research focus of LBS (location-based service) field in recent years. On the one hand, the POI recommendation ranking should be different when the traffic peak is different in different time periods, and the POI query process should be combined with the location Privacy protection algorithm can prevent pseudo server from obtaining user location and query content during query process; on the other hand, the number of interest points that can be queried according to the actual situation of the road is also a factor affecting the quality of service. According to the original road network data, the distribution information of interest points is organized according to the original road network data, and the problem of fewer returned interest points is solved by merging the useless interest points, and the anchor anonymity is improved Degree. Finally, this paper analyzes the number of query points of interest, query accuracy and security, and verifies the effectiveness of the method through experiments.

Key words: location privacy protection; point of interest storage organization structure; traffic flow; user service quality

0 引言

近年来，基于位置查询隐私保护[1][2]在日常生活中得到广泛应用，目前很多查询软件会自动开放位置获取服务。用户通过提供自身所在位置来获取想要查询的兴趣点[4]，如某个用户需要查询附近位置的 K 个超市，提供自身位置信息向 LBS 服务器发送兴趣点查询请求，LBS 服务器会处理查询请求，尽可能返回满足用户需要的兴趣点信息。在兴趣点查询隐私保护过程中主要从信息隐私保护和查询兴趣点信息有效性两方面研究。

信息隐私保护又包含位置信息隐私保护和查询信息隐私保护两部分[3]，近年来信息隐私

作者简介：晁稳(1996-)，女，硕士研究生，主要研究方向:网络空间安全
通信联系人：辛阳(1977-)，男，教授、博导，主要研究方向:信息安全. E-mail: yangxin@bupt.edu.cn

保护有了很多研究，常用的位置隐私保护方法可分为构造匿名区[5]（cloaking region 简称 CR）和生成假位置等两类。构造匿名区是将位置泛化为某个区域，区域内的用户相互合作实现用户位置隐私保护；假位置方法是用户以一个或多个虚假的位置替代真实位置发起查询，具有构造灵活、易共享和易处理等优势，其中锚点技术是假位置技术的一种，锚点的选取对查询性能和查询准确性有一定影响。

兴趣点查询信息有效性也是兴趣点查询过程中最基础最重要的一点[6]，一方面要注重查询过程中隐私保护，另一方面要注重查询兴趣点的有效性，所查兴趣点是否满足用户实际查询需求,例如从兴趣点查询个数和兴趣点查询结果是否符合当前路况。

1 相关工作与技术背景

1.1 前人工作综述

兴趣点查询在先前研究中大多基于欧式空间，而现实生活中大多是基于真实路网环境的，故当前研究重点是路网环境下兴趣点查询隐私保护[7][8]。当前路网环境下兴趣点查询隐私保护重点主要包含真实路网数据组织存储方式、兴趣点组织方式、用户位置隐私保护方法、用户兴趣点查询类型、查询加密方式等等方面，着重提高查询效率、兴趣点查询准确度、用户位置隐私保护程度、查询类型隐私保护程度等。目前路网环境下兴趣点查询隐私保护[8]进行了一些研究。

马春光[4]利用假位置思想，提出了路网环境下以交叉路口作为锚点的连续查询算法，在保护位置隐私的同时获取精确的 K 邻近查询结果；基于注入假查询和构造查询匿名组的方法，提出了抗查询内容关联攻击和抗运动模式推断攻击的轨迹隐私保护方法，并在分析中给出了位置隐私保护和查询服务质量平衡方法的讨论. 性能分析及实验表明，该方法能够在连续查询中提供较强的位置隐私保护，并具有良好的实效性和均衡的数据通信量。

R. Paulet [10]提出了两个实用的 PIR 方案，路网兴趣点信息采用网格结构存储，用户只能在专用网格中检索适当的块。此块使用上一阶段获得的对称密钥进行解密，用户只能使用上一阶段获取的加密密钥解密 PIR 获取的数据块。重新设计了密码结构，添加了一个正式的安全模型。

梁慧超[11]提出针对路网环境下兴趣点查询的隐私保护方法, 该方法充分考虑到路网的历史查询频率以及匿名路段之间的相互性问题, 使得生成的假位置频率相近、位置分散, 能够抵御重放攻击和推断攻击. 本文提出的假位置生成算法在熵值、方差、平均路径距离上都具有显著优势。

周长利[12]等针对路网兴趣点查询效率提出了以路网顶点为中心的兴趣点组织存储方式，基于 Paillier 密码系统实现保护查询内容隐私的 K 近邻兴趣点，通过兴趣点秘密检索方法，不需要引入可信的中间实体，高效的提升了查询效率和位置安全性。

朱治顺[13]等针对利用匿名框实现的兴趣点查询效率低，提出了基于单一兴趣点 Voronoi 图划分和四叉树层次化组织的 KNN 查询方法，降低了查询兴趣点次数，同时注入虚假查询保护了用户的真实查询内容隐私等。

结合前人工作，本文研究内容如下：

(1) 针对在路网结构中可能存在兴趣点查询不足、查询效率不高问题，提出以路网顶点为中心近似邻接顶点兴趣点组织结构。该兴趣点组织结构尽可能隐藏无用邻接节点，过滤掉

无用邻接点在网络中传输，提高查询效率和兴趣点查询数量，这种兴趣点组织方式也增加了锚点用户的安全性。

(2) 针对用户位置信息和查询内容可能被其他伪 LSP 服务器获取造成用户隐私泄露问题，提出利用锚点和加密算法保护用户敏感信息，结合上述兴趣点组织结构，扩大选择该锚点用户数量，增强位置隐私性；并结合路网环境中不同时段道路交通拥堵情况，提出基于车流量的路网兴趣点近邻查询方法，提高兴趣点查询准确性。

1.2 技术背景

1.2.1 Elgamal 公钥密码系统

Elgamal 公钥密码体制具有良好的数学基础，它是一种基于有限域上离散对数问题的公钥密码体制，它的安全性基础是离散对数求解的困难性。Elgamal 公钥密码体系分为密钥生成、加密、解密等三部分。Elgamal 加解密流程图如图 1 所示。

- 密钥生成过程：用户利用生成元 g 产生一个 q 阶循环群 G，从{1,…q-1}中随机选择一个 x

$$h = g^x \tag{1}$$

则(G,q,g,h)将作为公钥，而 x 作为私钥，私钥保密。

- 加密过程：服务器根据用户的公钥（G,q,g,h）对发送消息进行加密工作。首先从{1,…q-1}中随机选择一个 y，计算 $c_1=g^y$,计算共享秘密 $s=h^y$, 发送方把他要发送的秘密消息 m 映射为 G 上的一个元素 m’,计算 $c_2=m'*S$,最终计算的密文公式为：

$$(c_1, c_2) = (g^x, m' * h^y) = (g^x, m' * (g^x)^y) \tag{2}$$

最终将密文发送给接受方。

- 解密过程：利用私钥对密文(c_1,c_2)解密，计算共享秘密 $s=c_1^x$,并计算 m’，进而映射回信息 m,其中 s-1 是 s 在群 G 上的逆元。解密公式计算如下：

$$c_2 * s^{-1} = m' * h^y * (g^{xy})^{-1} = m' * g^{xy} * g^{-xy} = m' \tag{3}$$

至此可以得到发送方所发送的明文信息。

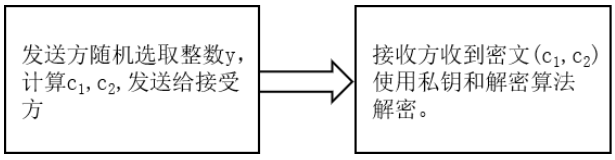

图 1 Elgamal 加解密步骤

Fig. 1 ElGamal encryption and decryption steps

1.2.2 锚点技术

锚点技术原理是通过假位置点代替真实的查询发起位置进行查询。通过锚点选择方案选取某个锚点作为假位置发送给位置服务器，并收到位置服务器返回的关于该锚点的查询结果。通过分析所选锚点、查询发起者真实位置以及查询结果间的空间几何关系，确认目标查询结果。当前使用锚点代替真实位置仍然存在一些不足，如有效锚点选择困难。锚点的选择将在很大程度上影响查询结果的准确性，带来不必要的开销。

1.2.3 路网局部模型

当前所有兴趣点查询基于真实路网环境，真实路网局部模型如图 2 所示；路网有向图组成由边和顶点组成，表示为 digraph={V,E}，V 表示顶点集合，E 表示有向边集合，V_n 表示路网顶点，$\overrightarrow{v_n v_m}$表示从顶点 V_n 到顶点 V_m 的路网有向边，反之亦然；pi 表示路段 V_n 到 V_m 上的兴趣点，ui 表示路段 V_n 到 V_m 上的用户。箭头代表用户在路段中的行驶方向。

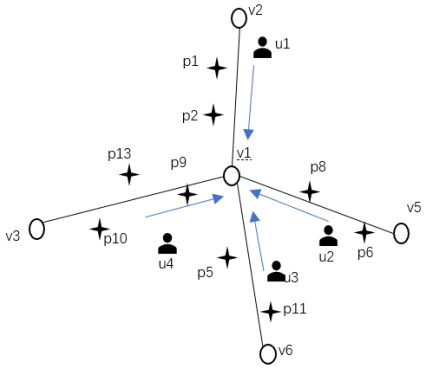

图 2 路网局部模型

Fig. 2 Local model of road network

2 基于车流量的兴趣点查询隐私保护

2.1 查询隐私保护流程概述

如图 3 所示，本文基于 Elgamal 加密的兴趣点加密查询流程如下:

①首先依据位置隐私保护中锚点技术，根据用户所在路段选取路段末端顶点 V_e 为锚点，使用 Elgamal 加密技术对查询类型加密。最终用户运行算法 1，生成查询五元组 Q=<U_k, V_e,Time, C ,K>，其中参数依次代表用户假名、锚点、查询时间、兴趣点加密信息、查询兴趣点个数等。

②LBS 服务器收到查询请求后运行算法 2，查询数据库中锚点对应兴趣点，返回密文查询结果。

③用户查询 redis 缓存中一次查询过程中当前道路结点车流量统计数据，速度较快。

④redis 缓存服务器返回用户查询结果。

⑤结合算法 1、2，用户执行算法 3 获取基于车流量兴趣点精确查询结果。

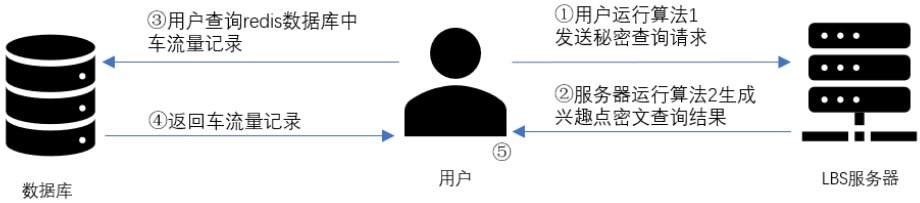

图 3 兴趣点查询流程图

Fig. 3 Interest point query flow chart

2.2 路网兴趣点组织结构

兴趣点的组织结构直接影响路网环境中兴趣点的组织效率，周长利等人[12]提出了一种以路网顶点组织存储兴趣点信息的存储结构，通过直达顶点结构定义，根据距离组织排序兴

趣点，提升兴趣点查询请求的处理效率。由于路网顶点和邻接节点之间路段中可能不存在兴趣点信息，在查询时会增加不必要的查询量，导致网络通讯量大，平均返回兴趣点数量较少影响服务质量，故通过剪枝操作尽可能将零兴趣点直达顶点合并，进而尽可能的增加兴趣点个数，同时减除兴趣点类型一列，统一用类型编号代替，提高查询内容的隐私性。

整体路网兴趣点组织结构如表 2 所示,其中第一行分别是路网顶点(路网用户根据自身位置选择的路网锚点)；近似邻接顶点即大部分为锚点的直接邻接节点，但为了提高查询效率和兴趣点查询数量，对直达邻接节点没有兴趣点的顶点进一步合并到下一顶点作为邻接节点；兴趣点编号是所查询的兴趣点比如学校、商店对应的编号，这样的存储结构不仅可以节省空间，简化查询，同时可以通过定期变化编号兴趣点名称对应关系，保证查询兴趣点类型的隐私; K_{max} 近邻兴趣点集是对所有邻接点上的兴趣点集合根据距离远近排序，每种类型的兴趣点最多有 K 个，并且每个兴趣点都带有路段末端顶点，供后续基于单位时间内车流量状况调整兴趣点序列情况，返回更符合用户需求的兴趣点信息。

表 2　路网兴趣点组织结构

Tab. 2　Organization structure of interest points in road network

路网顶点	近似邻接顶点	兴趣点编号	Kmax 兴趣点集
V_1	$\{V_5,V_8,V_9,V_{11}\}$	5	$\{dis_1V,dis_2V,\ldots\ldots,disk_{max}V\}$
		6	$\{dis_1V,dis_2V,\ldots\ldots,disk_{max}V\}$
		8	$\{dis_1V,dis_2V,\ldots\ldots,disk_{max}V\}$
		11	$\{dis_1V,dis_2V,\ldots\ldots,disk_{max}V\}$
V_2	$\{V_5,V_6,V_7,V_9\}$	23	$\{dis_1V,dis_2V,\ldots\ldots,disk_{max}V\}$
		26	$\{dis_1V,dis_2V,\ldots\ldots,disk_{max}V\}$
		28	$\{dis_1V,dis_2V,\ldots\ldots,disk_{max}V\}$
…	…	…	…

另外利用 redis 缓存记录在用户查询到获取到查询结果这段时间中，该锚点邻接路段上查询次数。使用分布式 redis 缓存每个邻接顶点查询次数，用单次查询时间段相邻顶点的查询次数代替路网兴趣点路段的车流量；用户查询次数越多，代表当前路段车流量越大，越可能会造成因车流量过大造成的兴趣点查询排序不准确。单次查询结束后开始前将表中顶点查询数量清 0，如表 3 中锚点 V_1 的邻接顶点 V_5 在当前用户单次查询过程中有 Num_i 个用户查询到该顶点。

表 3　路段顶点车流量统计表

Tab. 3　Statistical table of peak traffic flow

POI 路段顶点编号	单次查询车流量 Number
V_5	Num_5
V_8	Num_8
V_9	Num_9
V_{11}	Num_{11}

2.3　基于车流量的兴趣点查询隐私保护

基于车流量的路网兴趣点查询隐私保护流程可以概括为用户加密查询请求生成、服务器端处理加密查询请求并返回、统计数据判断路网顶点车流量、结合车流量精确兴趣点查询顺序。基于车流量的兴趣点查询隐私保护算法流程图如图 4 所示。

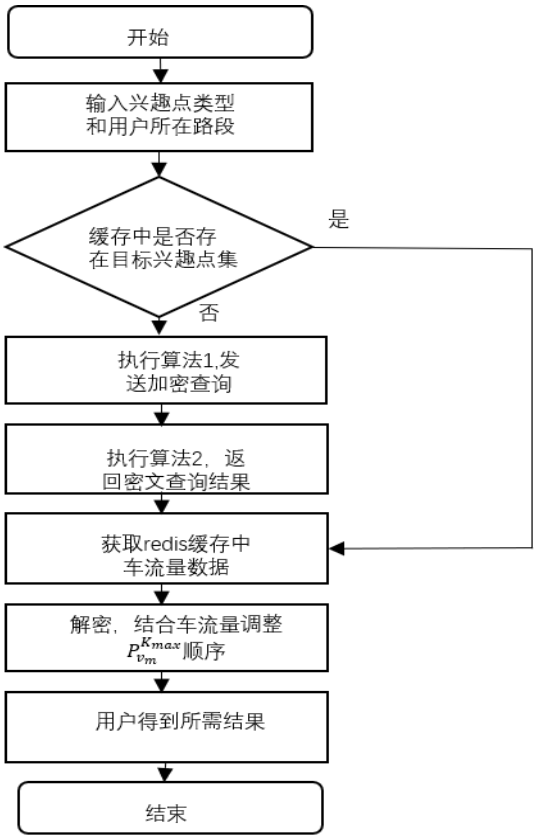

图 4　基于车流量兴趣点查询隐私保护算法流程图

Fig. 4　privacy protection algorithm based on traffic flow POI query

(1)加密查询请求生成和处理

LBS 服务器以路网顶点为中心存储邻接顶点，对路网上兴趣点类型进行编号，按照每一类兴趣点距离远近进行排序存储。这种存储方式大大简化了 LBS 查询兴趣点的复杂度。当用户输入需要查询的兴趣点之后，选择锚点代替用户真实位置，对目标兴趣点类型进行加密，确保用户位置和查询兴趣点信息不被第三方伪 LBS 服务器获取。

算法 1．用户加密查询请求生成算法.

1. 输入：用户目标兴趣点类型 t（学校、超市等），用户想要查询的兴趣点数量的最大值 K。
2. 输出：用户查询请求 Q。
3. 确定用户所在位置即开始节点 V_S、末端节点 V_e。
4. 用户获取 redis 键值对初始化为 0,并将 V_e 对应的 Number 值加一存储。
5. 根据查询兴趣点类型 t 对应兴趣点编号 POI_i。
6. 随机选取生成元 g,生成 q 阶循环群 G，从 G 中选取 x。
7. 依据公式(1)生成 Elgamal 算法的公私钥对 PK=(G,q,g,h)，SK=x。
8. 将 POI_i 依据公式(2)得到密文查询内容 C;
9. 选取所在路段末端节点 V_e 作为锚点,选取假名 U_k，最终生成查询请求 Q=<U_k,V_e,Time,C,K>。

算法 1 中用户查询过程中末端节点 V_e 的 Number 值增一，意义在于该末端节点 V_e 可能是另一用户访问的邻接节点，通过计算 Number 的方式更好的统计所查询兴趣点路段上的车流量。另通过对兴趣点编号 POI_i 进行加密，确保查询内容即使被截获攻击者也无法通过获取的密文得知用户查询的兴趣点类型；使用路段末端锚点代替真实位置也一定程度的保护了

用户的位置隐私。当查询发送到 LBS 服务器后,LBS 需要对查询内容解密，然后查找数据库中存储结构，获取兴趣点相关数据，结合车流量等影响因素对兴趣点顺序做出调整；服务器处理过程如算法 2 所示：

算法 2：LBS 服务器端查询处理请求；

1．输入：用户查询请求 Q=<U_k,V_e,Time,C,K>、LBS 服务器端路网顶点兴趣点存储表 Table。

2．输出：密文查询结果 R。

3．依据公式(3)对查询内容进行解密获取查询兴趣点类型 POI_i，和用户锚点 V_e。

4．根据锚点 V_e 从兴趣点存储表中提取对应的兴趣点编号为 POI_i 的前 K 个兴趣点集合，不足 K 个兴趣点返回符合要求的所有兴趣点。

5．依据公式(2)对兴趣点集合进行加密传输。

6．返回密文查询结果 R 给用户。

(2)基于车流量兴趣点查询隐私保护结果生成

兴趣点查询精确性查询过程即要保证位置隐私又要确保查询结果符合用户实际需求。为了实现用户位置隐私保护效率和实用性，如图 2 所示，路网用户 ui∈$\overrightarrow{v_n v_m}$，选取路段末端顶点 V_m 作为锚点代替用户真实位置发起查询，如此路网结构中可能有不同路段多个用户选取顶点 V_1 作为锚点，达到了用户位置隐私保护效果。如果在该道路上存在连续查询的情况，同一路段选择锚点相同，连续查询内容也相同，可直接获取结果，节省了连续查询的时间。兴趣点查询推荐中只根据距离推荐兴趣点太过单一，考虑兴趣点推荐中路况的影响非常有必要，当车流量过大造成拥堵时，只按距离远近进行兴趣点信息推荐非常不符合用户实际需求，路况拥堵情况即使距离较近的兴趣点也会花费非常多时间，给用户行程安排造成影响，故在考虑兴趣点查询结果时，需将车流量影响考虑在内。在本文中当车流量达到一定数值 $Tracffic_K$(不同城市不同路段 $Tracffic_K$ 值可能不同)时，代表当前路段车流量较大，造成拥堵的可能性较大，此次查询结果就需按照车流量拥堵情况调整兴趣点推荐顺序返回给用户.路网环境基于车流量兴趣点查询隐私保护算法如下：

算法 3.基于车流量兴趣点查询隐私保护精确查询结果计算算法

1. 输入：查询兴趣点类型 t，用户 ui∈$\overrightarrow{v_n v_m}$当前所在路段的两个端点 V_n,V_m。
2. 输出：用户兴趣点精确查询结果。
3. if 缓存中不存在以 V_m 为锚点的目标兴趣点查询结果。
4. 调用算法 1，以 V_m 为锚点发起目标兴趣点 K 近邻查询，获取目标兴趣点集合。
5. else 直接从缓存中获取目标兴趣点内容。
6. end if
7. 获取当前所在路段末端顶点 V_m 和用户兴趣点。
8. 调用算法 1，发送加密查询请求。
9. 调用算法 2，服务器端处理查询请求，返回密文查询结果。
10. 依据公式（3）对兴趣点集合进行解密得到。
11. 获取 redis 缓存中相应顶点兴趣点路段车流量统计表如表 2 所示。
12. for 每个顶点 V_i∈AVS_{Vm}(V_m 的邻接顶点集合)。
13. if Num_{Vi}>$Tracffic_K$
14. 将末端顶点为 V_i 路段上的兴趣点的优先级降到最低，调整集合$P_{v_m}^{K_{max}}$顺序。

15. end if
16. end for

17. 返回精确 K 近邻查询结果集$P_{v_m}^{K_{max}}$。

18. End

算法 3 第 3-6 行主要是用户在相同路段发起二次查询时提高查询效率，查询缓存中是否存在目标兴趣点结果集，提高查询效率，节约查询成本。第 8-9 行主要调用算法 1 和 2 发起用户端兴趣点加密查询和服务器端查询处理得到相应 K 近邻目标兴趣点集合。第 11-17 是对路网路段车流量统计判断是否拥堵，相应调整相关路段兴趣点推荐优先级，进而返回路网兴趣点集合$P_{v_m}^{K_{max}}$，进而生成兴趣点精确查询结果。

3 实验及分析

基于上一节论文研究内容讨论，本节主要讨论在 K 值、用户发起查询数量等影响因素下，在 California 路网数据集，基于本文所提供方法，验证在兴趣点查询数量、兴趣点查询准确率以及安全性等方面效率，与其他同类方法进行对比实验。

3.1 实验环境配置

本文中的算法实验均使用 java 语言实现，所有实验均在 windows10 操作系统中完成，运行硬件环境为 Intel Core i7 八核处理器，内存大小为 8GB，路网地图采用 California 州路网结构数据集。由于该路网结构数据集相对简洁，更易处理，本文所有实验均在该路网数据集上进行，California 路网数据集统计数据见表 4 所示。

表 4 California 州路网数据集统计数据

Tab. 4 California road network data set statistics

统计名称	对应数量
边数量	21694
路网顶点数量	21047
POI 种类	62
POI 数量	87635

另外本文需要模拟路网移动对象发起路网兴趣点查询，以便 redis 分布式缓存数据库记录路网路段记录车流量。本文采用 Thomas Brinkhoff 路网生成器[14]生成一定数量移动对象。移动对象随机分布在路网结构上。为保证查询效率，减少查询时间，需保证实验网络通讯带宽大于等于 3Mbps。另路网兴趣点类型索引文件占据存储空间为 4.00KB。

3.2 POI 查询数量

在以路网顶点为锚点发起兴趣点查询过程[12]中，以直接邻接顶点所在道路组织兴趣点，返回兴趣点查询，对于某些道路上无兴趣点等情况，导致整体以该顶点为锚点组织的兴趣点个数较少，当用户查询兴趣点个数 K 不断增大时，会出现查询兴趣点数量较少等情况，不能够满足用户的需求等情况。本文通过合并无兴趣点直接邻接节点，以路网锚点近似邻接节点方式组织兴趣点，尽可能的使近似邻接节点路段上都存在兴趣点，相对而言以锚点发起兴趣点查询更容易满足用户兴趣点查询个数 K 值；满足 K 值查询比率，即在一定数量的查询

中 K 值不断增大，兴趣点查询个数能够满足 K 值的查询占整个查询次数的比例。不同存储结构中 K 值查询比率如图 5 所示。

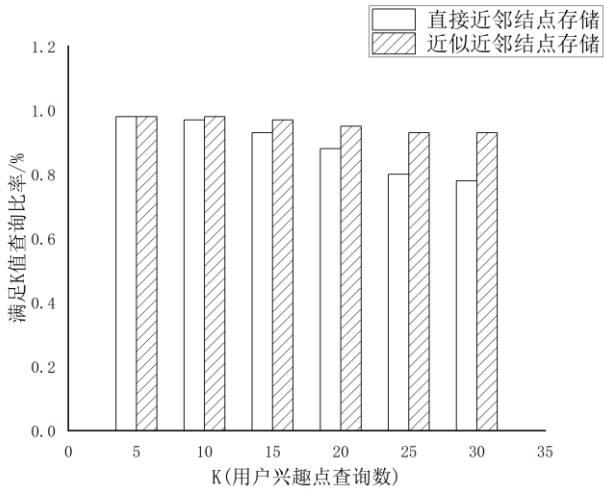

图 5　满足 K 值查询比率（K 值变化）

Fig. 2　Satisfy K value query ratio (k value change)

在图 5 中当用户查询兴趣点 K 值较小时，采用锚点直接近邻节点和锚点近似近邻节点存储方式,在固定次数兴趣点查询基本都能满足用户兴趣点 K 值查询需求，故用户兴趣点查询 K 值准确率较高。随着 K 值增大，采用直接近邻节点存储兴趣点方式，由于兴趣点存储个数不能满足用户兴趣点查询个数，兴趣点 K 值查询准确率明显下降。而采用近似邻接节点存储兴趣点，将无兴趣点邻接顶点替换为存在兴趣点的下一路网顶点，增加了锚点对应的兴趣点个数，故随着 K 值增大，在固定次数兴趣点查询基本都能满足用户兴趣点 K 值查询需求。以本文所提出的锚点对应兴趣点存储方法，较好的解决了兴趣点查询不足的缺陷。

3.3　查询准确率

本文将兴趣点道路拥挤情况考虑在内，提出符合用户需求的基于车流量的兴趣点查询隐私保护方案，而不是单一的考虑距离用户最近兴趣点。本文提出的兴趣点隐私保护方案更符合用户实际需求。在一定数量的用户查询过程中，本文用户满意度使用兴趣点查询准确率表示，兴趣点查询准确率，即在用户查询数量可变情况下，兴趣点查询结果符合当前路况的用户查询次数占总次数查询的比例。兴趣点查询准确率对比如图 6 所示。

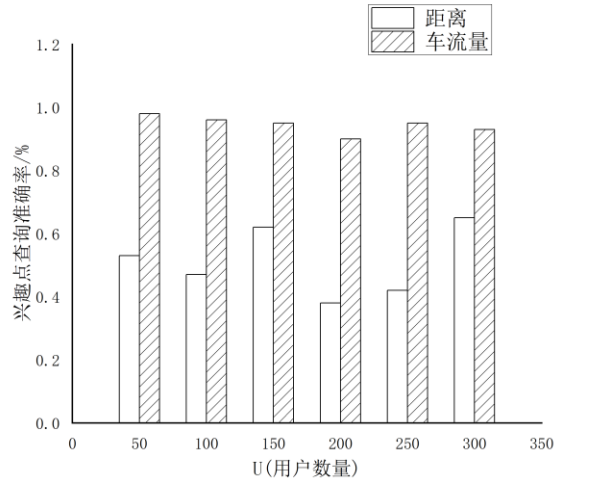

图 6　POI 查询准确率（U 值变化）

Fig. 6　POI query accuracy (U value change)

实验结果表明，在相同路网环境下，本文所提出的考虑基于车流量的兴趣点查询结果更符合用户兴趣点实际需求，为用户带来较好的用户体验。相比只考虑距离兴趣点查询方案，本方案有更好的查询效果。

3.4　安全性分析

本文采用锚点技术代替用户真实位置发起查询，选择该锚点发起查询的用户数量越多，攻击者根据锚点查询推断出用户真实位置的概率会越低，相应用户位置隐私保护安全性会更高。通过平均锚点隐匿度来表示用户查询的安全性，平均锚点隐匿度是在一定数量的用户查询中，平均每个锚点对应的用户查询数量。平均锚点隐匿度越高代表安全性越高。本文提出方法与锚点-直接近邻顶点存储方法进行对比实验。平均锚点隐匿度对比如图 7 所示。

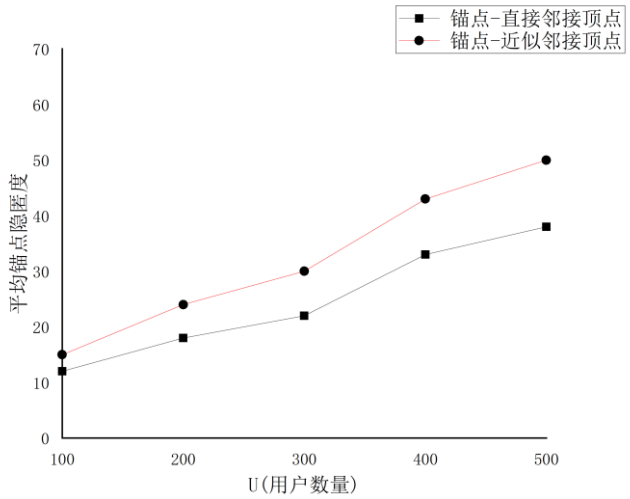

图 7　平均锚点隐匿度（U 值变化）

Fig. 7　Average anchor concealment (U value change)

实验表明本文选择锚点代替用户真实位置，根据当前路网顶点存储结构，存在两段道路上用户都选择当前锚点代替真实位置情况，达到更广范围的位置隐私保护效果。本文基于 Elgamal 公钥密码算法加密，该算法基于数学难题很难破解。由上用户位置隐私和查询内容隐私很难被除 LBS 服务器之外的第三方设备获取，保证了用户兴趣点查询隐私保护有效性。

4　结论

本文给出了基于锚点-近似邻接顶点兴趣点存储方式，改善兴趣点查询不足等情况；在该存储方式下提出基于车流量的兴趣点查询隐私保护，以一次查询过程中近似邻接顶点被访问次数来代表当前兴趣点所在路段的车流量，反映了道路拥挤情况，根据当前道路情况适当调整兴趣点推荐顺序。使用锚点和加密算法确保了在查询过程中用户安全性问题。实验数据表明本文提出的存储方式兴趣点查询数量有所提高，兴趣点查询方案具有更好的效果，用户隐私安全性得到保障。未来研究方向可以向锚点选取研究方向倾斜，为用户提供更加安全、高效的兴趣点查询。

[参考文献] (References)

[1] 张学军,桂小林,伍忠东.位置服务隐私保护研究综述[J].软件学报,2015,26(09):2373-2395.
[2] 贾金营,张凤荔.位置隐私保护技术综述[J].计算机应用研究,2013,30(03):641-646.
[3] 吴振刚,孙惠平,关志,陈钟.连续空间查询的位置隐私保护综述[J].计算机应用研究,2015,32(02):321-325+342.
[4] 周长利,马春光,李增鹏.一种保护用户隐私的路网兴趣点 KNN 查询方法[J].计算机应用研究,2016,33(01):262-265.
[5] 裴卓雄,李兴华,刘海,雷凯跃,马建峰,李晖.LBS 隐私保护中基于查询范围的匿名区构造方案[J].通信学报,2017,38(09):125-132.
[6] [6]Zhou C, Wang T, Jiang W, et al. Practical k nearest neighbor query scheme with two-party guarantees in road networks[C]//2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE). IEEE, 2018: 1316-1321.
[7] Kuang L, He S, Fan Y, et al. T-SR: a location privacy protection algorithm based on POI query[J]. IEEE Access, 2019, 7: 59491-59503
[8] Yang S, Tang S, Zhang X. Privacy-preserving k nearest neighbor query with authentication on road networks[J]. Journal of Parallel and Distributed Computing, 2019, 134: 25-36.
[9] 倪巍伟,陈萧.保护位置隐私近邻查询中隐私偏好问题研究[J].软件学报,2016,27(07):1805-1821.
[10] Paulet R, Kaosar M G, Yi X, et al. Privacy-preserving and content-protecting location based queries[J]. IEEE transactions on knowledge and data engineering, 2013, 26(5): 1200-1210.
[11] 梁慧超,王斌,崔宁宁,杨凯,杨晓春.路网环境下兴趣点查询的隐私保护方法[J].软件学报,2018,29(03):703-720.
[12] 周长利,陈永红,田晖,蔡绍滨.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(02):471-492.
[13] 朱顺痣,黄亮,周长利,马樱.一种基于兴趣点分布的匿名框 KNN 查询方法[J].电子学报,2016,44(10):2423-2431.