文章编号:1007-5321(2017)06-0037-06 **DOI**:10.13190/j.jbupt.2017-103

路网环境下基于不经意传输的 LBS 隐私保护方法

周长利[1], 蔡绍滨[1,2], 王 田[1], 马春光[2]
(1. 华侨大学 计算机科学与技术学院, 福建 厦门 361021; 2. 哈尔滨工程大学 计算机科学与技术学院, 哈尔滨 150001)

摘要: 基于位置服务(LBS)中的隐私保护方法存在如下常见问题:重视用户端隐私保护而容易忽略 LBS 服务端的数据安全; 隐私保护强度高的方法实用效率低;隐私保护方法大多面向欧氏空间提出,无法适用路网环境,查询准确率低. 针对上述问题,基于不经意传输提出了一种 LBS 兴趣点查询服务中的隐私保护方法,在保护用户位置和查询内容隐私的同时确保 LBS 服务端数据安全,并能确保路网连续查询的效率和准确率. 性能分析及实验结果表明,新方法具有较强的安全性和良好的工作效率.

关 键 词: 基于位置的服务; 隐私保护; K 近邻查询; 服务端数据安全
中图分类号: TP311 **文献标志码**: A

LBS Privacy Preservation Scheme Based on Oblivious Transfer in Road Network Environment

ZHOU Chang-li[1], CAI Shao-bin[1,2], WANG Tian[1], MA Chun-guang[2]
(1. School of Computer Science and Technology, Huaqiao University, Fujian Xiamen 361021, China;
2. School of Computer Science and Technology, Harbin Engineering University, Harbin 150001, China)

Abstract: There are three common defects in existing location based service (LBS) privacy-preserving methods: only considering privacy preservation of the user without caring about data security of LBS server. The stronger a privacy-preserving method is, the less practical it is. Privacy-preserving methods are usually proposed based on the Euclidean space without considering actual factors in road network, and the query accuracy declines consequently. To solve the above problems, an LBS privacy-preserving scheme was proposed based on oblivious transfer with special distribution information for points of interest in road network. This scheme ensures data security of LBS server while preserving the user's location privacy and query content privacy, at the same time, it is applicable for continuous query in road network and guarantees the query efficiency and accuracy. Performance analysis and extensive experiments show that this scheme ensures strong security and works efficiently.

Key words: location-based service; privacy preservation; K nearest neighbor query; data security of server side

基于位置的服务[1]为人们提供方便的同时,需要用户提供一定的隐私数据作为获取服务的代价. 用户将个人隐私数据发送给任何实体均存在泄漏的风险. 攻击者可以通过掌握的背景知识,关联推断

收稿日期: 2017-06-07
基金项目: 国家自然科学基金项目(61472097, 61772148); 福建省自然科学基金项目(2016J05158); 福建省高校杰出青年科研人才培育计划 (MJK2015-54); 华侨大学科研基金项目(15BS412).
作者简介: 周长利(1985—), 男, 讲师, E-mail: zhouchangli666@163.com.

出用户的真实身份、兴趣爱好、生活习惯等隐私信息. 在基于位置的查询服务中,位置和查询内容隐私是两项重要的保护内容[2].

匿名框[3-4]和假位置[1,5-8]是两类经典的位置保护方法. 作为假位置的一种,锚点用来代替用户真实位置发起查询,并依据该锚点计算出实际 K 近邻兴趣点,该方法由 Yiu 等[5]首次提出,但存在未实现 k 匿名、锚点选取随机等缺陷. 孟小峰[6]及 Gong[7]等学者分别提出了改进方案,但这些方法大多面向欧氏空间设计,并且随机选取的查询锚点会带来较多数据库查询操作. Zhou 等[9]针对锚点选取方式、查询不均衡等问题提出了解决方法,但未考虑 LBS 端数据安全.

私有信息检索[1,10]是保护查询内容隐私的经典方法,能在 LBS 服务器不知晓查询内容的条件下,为用户提供查询结果. 此类技术隐私保护强度高,但存在查询处理速度慢的缺陷[4,11]. 周长利等[12]基于伪随机置换提出了一种私有信息检索协议,但仍需要借助可信中间服务器实现,存在安全风险. 杨松涛等[13]提出了一种基于不经意传输的私有信息检索协议,但是该方法基于欧氏空间设计,存在查询次数多、通信量大等问题.

另外,LBS 服务端存储的兴趣点信息也需要保护. 通常,LBS 服务器只需根据用户兴趣点查询请求为其返回对应的查询结果,不应额外泄漏其他信息,避免恶意攻击者短时间内获得服务端更多兴趣点的详细信息,并据此伪装 LBS 服务器收集用户隐私等.

针对上述问题,基于不经意传输提出了适用于路网的连续查询位置和查询内容的隐私保护方法,同时可确保 LBS 服务端的数据安全. 该方法具有较好的实用性.

1 系统架构

隐私数据具有私密性和排他性,这决定了用户不应将自身隐私数据交给任何假设可信的中心服务器来实施保护处理. 因此,采用“用户—LBS 服务器”两方实体系统架构,如图 1 所示.

用户根据 LBS 服务器公布的分块化兴趣点索引表构造不经意传输查询请求发送给 LBS 服务器,收到查询的 LBS 服务器无法确定用户的真实查询请求,进而将处理后的密文查询结果发送给用户,并且 LBS 服务器不知道用户获取的真实查询结果是

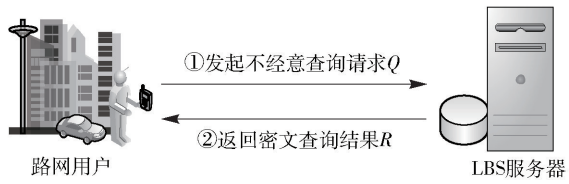

图 1 系统架构

哪个. 系统架构中存在如下假设:①LBS 服务器是半可信实体,为用户提供基于位置服务的同时对用户隐私好奇,希望深入挖掘用户深入隐私信息以满足商业利益等,同时,用户对 LBS 服务器也不可信,不应向用户泄漏过多数据库中的兴趣点分布等信息;②LBS 服务器具有较强的分析处理能力,存在勾结其他参与者关联推断用户隐私的可能,LBS 服务器和用户之间互不妥协;③通信信道不安全,存在窃听泄漏隐私的可能.

K 近邻查询请求可用 $Q=\langle u_k,\mathrm{loc},\mathrm{time},K,C\rangle$ 表示,其中:$u_k\in U$ 表示用户身份标识,为了不泄漏真实身份及抵御身份标识关联,通常使用假名 u_k' 替换并在每次查询中更换,假名之间无关联;loc 表示用户位置,为了保护用户位置隐私,采用特殊的共用锚点位置 $\mathrm{loc}_{\mathrm{anchor}}$ 替代,使用该锚点还能提高查询处理速度;time 表示查询时间戳;K 表示查询近邻兴趣点数量;C 表示查询内容,即用户感兴趣的目标兴趣点. 为了不让 LBS 服务器知晓用户的真实查询内容隐私,使用 1-out-of-n 不经意传输技术处理,提交密文查询请求内容 C'.

2 路网兴趣点组织结构

用户所处路网环境如图 2 所示,兴趣点沿路网分布,用户搜索的 K 近邻兴趣点集 $P_{u_k}^K$ 实际是从用户当前位置出发,距离自己路网距离最近的 K 个兴趣点. 该集合包含两部分,$P_{u_k}^K=P_{u_k}^X+P_{v_n}^{(K-X)}$ ($X\geqslant 0$,

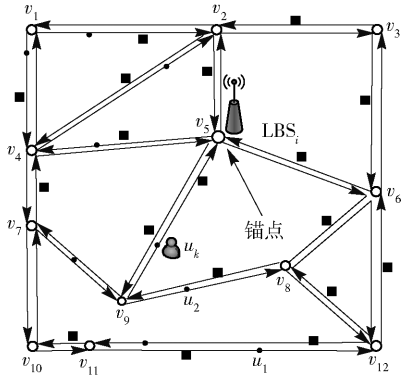

图 2 路网模型

$K>0$)，$P_{u_k}^{X}$是用户当前位置到所在路段前进方向顶点 v_n 间的 X 个目标兴趣点集合；$P_{v_n}^{(K-X)}$是从该顶点出发后的$(K-X)$个目标兴趣点集合. 用户要到达其他路段上的某个目标兴趣点，必须先到达所在路段顶点，然后以该顶点为出发点到达. 因此，以路网顶点(锚点)为基本生成元，组织路网兴趣点分布如表 1 所示.

表 1 各列依次表示路网顶点坐标、邻接顶点集

表 1　LBS 端兴趣点分布表

路网顶点	邻接顶点	兴趣点类型	兴趣点记录号	$K_{\max}$近邻兴趣点集	兴趣点描述信息
v_5(anchor1)	$\{v_2, v_4, v_6, v_9\}$	School	1	$\{\text{loc}1,\text{loc}2,\cdots,\text{loc}_{K_{\max}}\}$	$\{\text{inf}\,1,\text{inf}\,2,\cdots,\text{inf}_{K_{\max}}\}$
		Super market	2	$\{\text{loc}1,\text{loc}2,\cdots,\text{loc}_{K_{\max}}\}$	$\{\text{inf}\,1,\text{inf}\,2,\cdots,\text{inf}_{K_{\max}}\}$
		Motel	3	$\{\text{loc}1,\text{loc}2,\cdots,\text{loc}_{K_{\max}}\}$	$\{\text{inf}\,1,\text{inf}\,2,\cdots,\text{inf}_{K_{\max}}\}$
		Gas station	4	$\{\text{loc}1,\text{loc}2,\cdots,\text{loc}_{K_{\max}}\}$	$\{\text{inf}\,1,\text{inf}\,2,\cdots,\text{inf}_{K_{\max}}\}$
v_8(anchor2)	$\{v_6,v_9,v_{12}\}$	School	1	$\{\text{loc}1,\text{loc}2,\cdots,\text{loc}_{K_{\max}}\}$	$\{\text{inf}\,1,\text{inf}\,2,\cdots,\text{inf}_{K_{\max}}\}$
		Bus station	2	$\{\text{loc}1,\text{loc}2,\cdots,\text{loc}_{K_{\max}}\}$	$\{\text{inf}\,1,\text{inf}\,2,\cdots,\text{inf}_{K_{\max}}\}$
		Hospital	3	$\{\text{loc}1,\text{loc}2,\cdots,\text{loc}_{K_{\max}}\}$	$\{\text{inf}\,1,\text{inf}\,2,\cdots,\text{inf}_{K_{\max}}\}$
…	…	…	…	…	…

合、兴趣点类型标号、兴趣点类型名称、$K_{\max}$个从该顶点出发按距离递增排序的同类近邻兴趣点集合和对应兴趣点详细描述信息，用户每次发起 K 近邻查询满足 $K\leqslant K_{\max}$. 索引表由表 1 的第 1 ~4 列构成，并公布给用户，用户据此构造不经意查询请求. 为了提高查询处理速度，不采用集中式数据库，而是采用分布式数据库工作模型. 将整个地图划分为若干区域，每个区域内部署一个分布式 LBS 服务.

在查询过程中，所有 LBS 用户以所在路段的顶点代替自己的真实位置发起查询，当多个不同路段用户共用同个路网顶点作为锚点发起查询时，可以实现用户位置的 k 匿名，实现用户位置隐私保护.

多个 LBS 服务器会适当存储交叉区域兴趣点信息，当用户经过重叠区域时，同样是在进入新路段后只发起 1 次新查询，获取进入新路段后的最新 K 近邻查询结果，是用户跨重叠区域后新 LBS 服务器提供的，之前查询过的兴趣点可能还在此查询结果中，但仍然是距离用户路网距离最近的 K 个兴趣点，因此查询效率和准确率不受影响.

3　基于不经意传输的隐私保护查询方法

3.1　问题描述

用户每次利用所在路段锚点 v_n 发起查询，假设 LBS 服务器的兴趣点分布表中，以该顶点为起点共有 m 种类型兴趣点 $P=\{P_1,P_2,\cdots,P_m\}$和随机生成的 m 个密钥 $\text{Key}=\{k_1,k_2,\cdots,k_m\}$. 用户希望能够得到某个类型兴趣点 $P_x\in P$ 的相关信息，但不希望 LBS 服务器知道他对此类兴趣点感兴趣. 同时，LBS 服务器也不希望用户一次获得其他兴趣点的信息.

3.2　1-out-of-*n* 不经意传输隐私保护查询方法

不经意传输可以解决上述问题，但通常情况下不经意传输需要 1 次处理较多兴趣点信息，并多次通信，且存在路网适用性差的问题. 为此，基于上述路网兴趣点组织方式，提出一种满足路网 K 近邻查询的不经意传输方法，在保护用户位置和查询内容隐私实现秘密检索的同时，进一步提高查询效率.

假设 q 为大素数，Z 为 q 阶群，a、b 为 Z 的生成元，Z_q 为 q 的最小剩余集，(a,b,Z)对用户和 LBS 服务器公开. 查询过程如表 2 所示.

表 2　不经意传输方法

用户	LBS 服务器
	←服务器公布索引表
$r\in Z_q,\beta=a^r b^x \bmod q$	
依据索引生成查询请求 $\xrightarrow{Q}$	
	$k_i\in Z_q, 1\leqslant i\leqslant n$
	$s_i=a^{h_i}\bmod q$
	$t_i=k_i(\beta/b^i)^{h_i}\bmod q$
	$\text{ST}=\{(s_1,t_1),(s_2,t_2),\cdots,(s_m,t_m)\}$
	$E_p=\{E_{k_1}(P_1),E_{k_2}(P_2),\cdots,E_{k_m}(P_m)\}$
	$\xleftarrow{ST,E_p}$ 返回查询结果
$k_x=(t_x/(s_x)^r)\bmod q$	
$P_x=D_{k_x}(E_{k_x}(P_x))$	

LBS 服务器公布所负责区域内兴趣点索引信息，用户确定自己所在路段 $u_k\in\overrightarrow{v_m v_n}$，并依据该索引

构造不经意查询请求,步骤如下.

步骤1 用户希望得到索引表中的某个类型标号为 x 的兴趣点 $P_x \in P$ 的信息,其生成随机数 $r \in Z_q$,计算 $\beta = a^r b^x \bmod q$,并将原有的查询请求 $Q = \langle u_k, \mathrm{loc}, \mathrm{time}, K, C\rangle$ 改造成不经意传输查询请求为 $Q = \langle u'_k, \boldsymbol{v}_n, \mathrm{time}, K, \beta\rangle$ 发送给 LBS 服务器,该查询不直接提供用户真实位置和查询内容,分别以用户所在路网锚点 $\boldsymbol{v}_n$ 和1个依据目标兴趣点 P_x 生成的密文符号 β 代替,这样就生成了1个用保护户位置和查询内容的查询请求.

步骤2 LBS 服务器随机生成的 m 个密钥 $\mathrm{Key} = \{k_1, k_2, \cdots, k_m\}$ 满足 $k_i \in Z_q, 1 \leqslant i \leqslant n$,并计算 $\mathrm{ST} = \{(s_1, t_1), (s_2, t_2), \cdots, (s_m, t_m)\}$,其中:

$$h_i \in Z_q,\ 1 \leqslant i \leqslant n,\ s_i = a^{h_i} \bmod q,$$

$$t_i = k_i\,(\beta / b^i)^{h_i} \bmod q$$

同时 LBS 服务器使用 $\mathrm{Key} = \{k_1, k_2, \cdots, k_m\}$ 加密,以顶点 $\boldsymbol{v}_n$ 为生成元的各类型兴趣点数据 $E_p = \{E_{k_1}(P_1), E_{k_2}(P_2), \cdots, E_{k_m}(P_m)\}$,最终将 $\{\mathrm{ST}, E_p\}$ 发送给用户.

步骤3 用户计算密钥 $k_x = (t_x / (s_x)^r) \bmod q$,进而得出目标兴趣点 $P_x = D_{k_x}(E_{k_x}(P_x))$.

LBS 服务器返回给用户额外的密文兴趣点查询结果,用户仅能够对其中的目标兴趣点解密,确保了 LBS 服务器不过多释放信息. 在构造查询请求时,$P_i \in P$ 是以 $\boldsymbol{v}_n$ 为出发点的某一类兴趣点信息,这种分布式数据库和以路网顶点为生成元的兴趣点组织结构确保了仅对部分兴趣点处理,避免了不经意传输中需要处理大量额外兴趣点信息的问题.

4 安全性分析

从 LBS 服务器的数据安全和用户隐私两方面做安全性分析.

4.1 LBS 服务器数据安全

由不经意传输方式可知,LBS 服务器每次返回的查询结果中,用户依据式(1)计算得出密钥 k_x,

$$k_x = \frac{t_x}{(s_x)^r} \bmod q = \frac{k_x\,(a^r b^x / b^x)^{h_x}}{(a^{h_x})^r} \bmod q \quad (1)$$

由于 x 是用户确定的,而 b^i 中的整数 i 与其密文查询结果的位置无对应关系,而无法计算出其他密钥 k_i,用户仅能解密其中一个自己感兴趣的目标兴趣点 $E_{k_x}(P_x)$. 其他兴趣点内容均是经过加密处理的密文结果 $E_{k_i}(P_i)$,用户因无法计算出密钥而难以解密,所以每次查询不会泄漏数据库的其他内容.

4.2 用户隐私安全

用户每次查询都会选择不同的随机数 $r \in Z_q$,所以,连续查询中同类型兴趣点查询也会生成不同的密文查询符号 β,这个过程类似一次一密,随机数 r 的长度选择可以进一步提高破解难度. 因此,很难通过猜解密钥方式破解用户的查询内容.

在返回的 m 个密文查询结果中,由于 LBS 服务器每个密文结果的生成处理方式相同,所以其确定其中某个兴趣点为用户查询的目标兴趣点的概率为 $p(x) = 1/m$,m 越大,LBS 服务器的不确定性越高. 在连续查询中的某个单次查询的信息熵为

$$H(Q) = \sum_{i=1} p(x) \mathrm{lb} \frac{1}{p(x)} = \mathrm{lb}m \quad (2)$$

用户在连续查询过程中,由于查询请求 $Q = \langle u'_k, \boldsymbol{v}_n, \mathrm{time}, K, \beta\rangle$ 中无明显数据关联项,即 u'_k 为每次查询更换的新假名,假名之间无关联;$\boldsymbol{v}_n$ 代替用户真实位置,多个路段用户共用该锚点可实现位置无关联;β 是查询内容的密文替代符号,相互无关联. 这样连续查询中的 n 个单次查询之间相互独立,因此联合信息熵如式(3)所示. 此时信息熵值最大,这意味着对于攻击者来说不确定性最高,达到保护用户位置和查询内容隐私的目标.

$$H(Q_1, Q_2, \cdots, Q_n) = \sum_{i=1}^{n} H(Q_i) = n\mathrm{lb}m \quad (3)$$

综上,笔者充分考虑了路网兴趣点分布的特点,构造了不经意传输查询请求,既可以保护用户端的位置隐私和查询内容隐私,还能够保护 LBS 服务器端的数据安全,具有较高的查询效率和准确性.

5 实验

实验在 Windonws 7 云平台上利用 JAVA 语言实现. 地图采用美国国家地质勘探局提供的地理数据集,采用 Thomas Brinkhoff 路网移动节点数据生成器生成用户位置数据,设置用户向 LBS 更新位置数据频率 f,采用剪枝的办法控制平均路段长度 S. 通信带宽为 3 Mbit/s,每次查询返回单个数据包为 1 500 byte,每个兴趣点描述信息设置为 300 byte,除去 40 byte 的包头,包含兴趣点个数约为 $(1\,500 - 40)/300 \approx 5$ 个, 参数配置如表3所示.

5.1 查询准确率

查询准确率是指用户获得准确查询结果占全部查询的比率. 笔者采用路网兴趣点组织结构,相比

欧氏空间查询方法，确保了查询准确性. 在查询准确率方面与两种经典方法 Cloaking Region[5]、SpaceTwist[6]进行比较的结果如图 3 所示.

表 3　实验默认参数配置

参数名	取值范围	默认值
全局移动用户总数 U/万个	$5 \leqslant U \leqslant 30$	15
近邻兴趣点查询数 K/个	$5 \leqslant K \leqslant 25$	10
区域内兴趣点总数/万个	$2.5 \leqslant m \leqslant 10$	10
平均路段长度 S/m	$200 \leqslant S \leqslant 2\,000$	1 000
用户位置更新频率 f/(次·s^{-1})	$5 \leqslant f \leqslant 30$	15

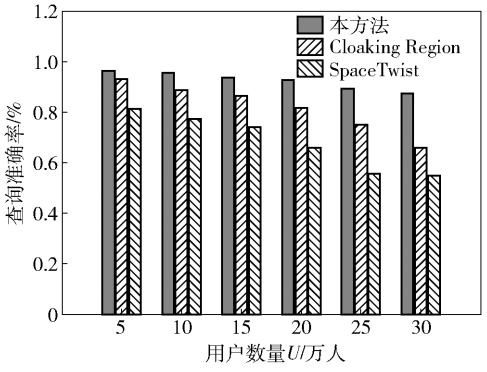

图 3　查询准确率比较(U 变化)

随着用户数量的增长，新方法的查询准确率略有下降但相对稳定，下降的主要原因是用户数量增多带来少量查询请求被丢弃造成的. Cloaking Region 方法由于采用了同态加密实现隐私保护查询，服务器处理速度显著下降，造成查询准确率随之下降. 而 SpaceTwist 方法由于返回多余兴趣点较多，在用户数量增长时，查询准确率下降迅速.

5.2　平均处理时间

路段长度是本方法中影响查询次数的重要因素之一，如图 4 所示，随着用户数量的增长，平均路段长度 S 增大会使得查询次数减少，使得平均处理时间有所降低. 因此可以采用路网图剪枝的方法去掉一些较短路段，提高处理速度.

笔者还将本方法与上述经典隐私保护方法在平均处理时间方面进行了比较，如图 5 所示. 随着用户数量的增加，本方法与 SpaceTwist 方法的平均处理时间保持稳定，主要是由于处理方法相对简单，而 Cloaking Region 方法由于采用同态加密技术生成密文查询结果，但处理时间长是其缺陷.

5.3　平均数据通信量

数据通信量主要是来自返回查询兴趣点的描述信息. 当移动用户位置不断变化而频繁发起查询时，如图 6 所示，Cloaking Region 方法处理速度较慢，较多数据包被丢弃，带来了重复数据包量的增加. 本方法查询采用固定锚点，用户仅进入新路段时用前方顶点发起一次查询，不因用户位置变化而不断发起连续查询，可保持通信量基本平稳. SpaceTwist 方法虽然也采用锚点，但是锚点是随机选取的，重复使用率不高，面对大量用户时存在数据包丢弃率增高问题，进而带来平均数据包量增加.

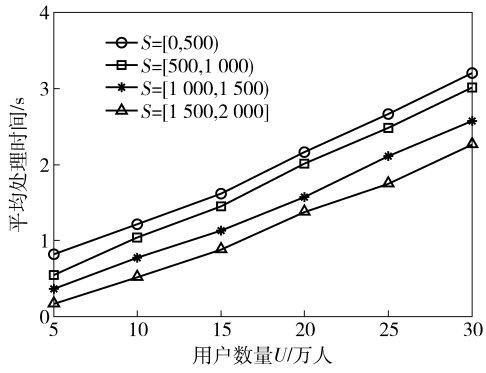

图 4　平均处理时间(U 和 S 变化)

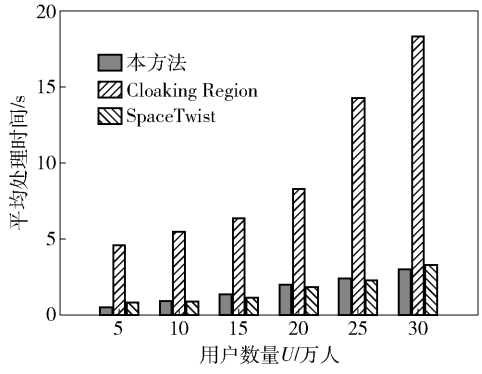

图 5　平均处理时间比较(U 变化)

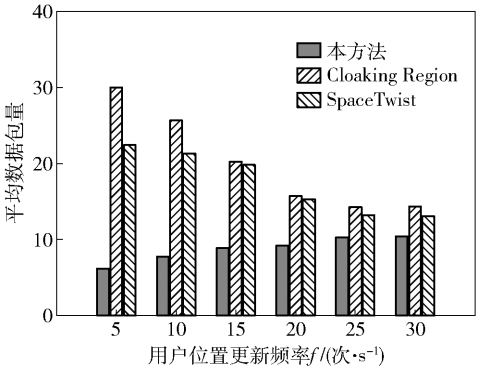

图 6　平均数据包通信量(f 变化)

6　结束语

本文针对用户连续查询中的 LBS 端数据安全

问题和用户端隐私保护问题,基于不经意传输技术,提出了一种能够保证两方数据和隐私安全的 K 近邻兴趣点查询方法,不仅实现了对两方敏感信息的保护,还提高了查询效率和准确率. 实验分析表明,本方法具有较高的查询成功率,平均处理时间相对同态加密处理实现的 PIR 更为高效,适用于频繁位置变换的路网连续查询.

参考文献:

[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, 9: 2373-2395.
Zhang Xuejun, Gui Xiaolin, Wu Zhongdong. Privacy preservation for location-based services: a survey[J]. Journal of Software, 2015, 9: 2373-2395.

[2] Ni W, Gu M, Chen X. Location privacy-preserving k nearest neighbor query under user's preference [J]. Knowledge-Based Systems, 2016, 103: 19-27.

[3] Pan X, Xu J, Meng X. Protecting location privacy against location-dependent attacks in mobile services [J]. Knowledge and Data Engineering, IEEE Transactions on, 2012, 24(8): 1506-1519.

[4] Yi X, Paulet R, Bertino E, et al. Practical approximate k nearest neighbor queries with location and query privacy [J]. IEEE Transactions on Knowledge and Data Engineering, 2016, 28(6): 1546-1559.

[5] Man Lung Yiu, Jensen C S, Xuegang Huang, et al SpaceTwist: Managing the trade-offs among Location Privacy, Query Performance, and Query accuracy in mobile services[C]//2008 IEEE 24th International Conference on Data Engineering. (ICDE 2008). Mexico: IEEE Press, 2008: 366-375.

[6] 黄毅, 霍峥, 孟小峰. CoPrivacy: 一种用户协作无匿名区域的位置隐私保护方法[J]. 计算机学报, 2011, 34(10): 1976-1985.
Hang Yi, Huo Zheng, Meng Xiaofeng. CoPrivacy: A collaborative location privacy-preserving method without cloaking region [J]. Chinese Journal of Computers, 2011, 34(10): 1976-1985.

[7] Gong Z, Sun G Z, Xie X. Protecting privacy in location-based services using k-anonymity without cloaked region [C]//2010 Eleventh International Conference on Mobile Data Management (MDM 2010). Kansas City: IEEE Press, 2010: 366-371.

[8] Niu B, Zhang Z, Li X, et al. Privacy-area aware dummy generation algorithms for Location-Based Services[C]// 2014 IEEE International Conference on Communications (ICC 2014). Sydney: IEEE Press, 2014: 957-962.

[9] Zhou C, Ma C, Yang S, et al. A location privacy preserving method based on sensitive diversity for LBS[C]// 2014 IFIP International Conference on Network and Parallel Computing (NPC 2014). Berlin Heidelberg: Springer Press, 2014: 409-422.

[10] Ghinita G. Privacy for location-based services [J]. Synthesis Lectures on Information Security, Privacy, & Trust, 2013, 4(1): 1-85.

[11] Yi X, Paulet R, Bertino E, et al. Practical k nearest neighbor queries with location privacy[C]//2008 IEEE 30th International Conference on Data Engineering (ICDE 2014). Chicago: IEEE Press, 2014: 640-651.

[12] 周长利, 田晖, 马春光, 等. 路网环境下基于伪随机置换的 LBS 隐私保护方法研究[J]. 通信学报, 2017(6): 19-29.
Zhou Changli, Tian Hui, Ma Chunguang, et al. Research on LBS privacy preservation based on pseudorandom permutation in road network [J]. Journal on Communications, 2017(6): 19-29.

[13] 杨松涛, 马春光, 周长利. NCoP: 无用户协作的 LBS 隐私保护方法[J]. 北京邮电大学学报, 2014, 37(6): 86-90.
Yang Songtao, Ma Chunguang, Zhou Changli. NCoP: A non-Cooperative location privacy-preserving method [J]. Journal of Beijing University of Posts and Telecommunications, 2014, 37(6): 86-90.