doi:10.11959/j.issn.1000-436x.2015054

LBS 中面向协同位置隐私保护的群组最近邻查询

高胜，马建峰，姚青松，孙聪
（西安电子科技大学 计算机学院，陕西 西安 710071）

摘 要：在分析现有群组最近邻查询中位置隐私保护的基础上，提出 LBS 中一种面向位置隐私保护的群组最近邻查询方法。该方法采用分布式系统结构，克服了集中式匿名系统结构所存在通信瓶颈和攻击重点的缺陷。在此基础上根据用户群组的运动状态信息，提出使用位置随机扰动和门限秘密共享的 Paillier 密码系统来安全地计算用户群组的质心位置。于是将用户群组的最近邻查询转换为此质心的最近邻查询。与现有的相关工作相比，理论分析表明所提有关方案能够在有效抵御现有的距离交叉攻击和共谋攻击下，实现灵活的群组最近邻查询，同时耗费较低的网络资源。

关键词：分布式系统结构；群组最近邻查询；位置隐私；质心位置
中图分类号：TP309 **文献标识码**：A

Towards cooperation location privacy-preserving group nearest neighbor queries in LBS

GAO Sheng, MA Jian-feng, YAO Qing-song, SUN Cong
(School of Computer Science and Technology, Xidian University, Xi'an 710071, China)

Abstract: On the basis of analyzing the existing location privacy protections in GNN queries, a GNN queries method for location privacy protection in LBS was proposed. In this method, a distributed system structure for GNN was adopted to overcome the disadvantages of centralized anonymous system structure such as making a communication bottleneck and being a vulnerable point of attack. According to the motion status of a user group, two methods on the basis of this structure, named location random perturbation and threshold secret sharing version of Paillier cryptosystem, were used to securely compute the center location of the user group. Then these users' GNN queries had been turned into NN queries of the group center. Compared with existing related work, theoretical analysis proves that the proposal can effectively resist against the existing distance interaction attack and collusion attack and achieve flexible GNN queries, while it costs lower network resources.

Key words: distributed system architecture; group nearest neighbor query; location privacy; center location

1 引言

近年来，移动终端的发展呈现出功能强大化、种类多样化、使用大众化等特点；同时，定位技术的发展使用户能随时随地获得地理位置信息，如基于 GPS、北斗等的室外定位，基于 Wi-Fi、ZigBee 等的室内定位，这两者的配合使基于位置的服务(LBS, location-based services)进入发展的繁荣期[1]。具体而言，LBS[2]是指在地理信息系统（GIS, geographic information system）和定位技术的支撑下，终端用户利用无线通信技术向服务提供者（SP, service providers）发送位置信息及查询请求，得到所需要的服务。典型的 LBS 应用包括：兴趣点搜索，如查询距用户最近的快餐店；路线导航，如搜索距某地铁站

收稿日期：2013-09-10；**修回日期**：2013-12-05
基金项目：国家自然基金委员会-广东联合基金重点基金资助项目（U1135002）；国家自然科学基金资助项目（61303221, 61303033）；航空科学基金资助项目（2013ZC31003, 20141931001）
Foundation Items: The Key Program of NSFC-Guangdong Union Foundation (U1135002); The National Natural Science Foundation of China (61303221, 61303033); The Aviation Science Foundation of China (2013ZC31003, 20141931001)

最快捷的路线；基于位置的推荐服务，如向商场周围 100 m 范围内的用户推送商品促销信息等。

然而，SP 并没有提供保护用户位置数据的措施，甚至有些会因为利益关系将用户的位置信息和查询内容透露给攻击者。然而，位置信息的泄露极大地威胁着用户的个人隐私，例如，若用户在医院使用 LBS，则可推断出其可能存在健康问题；若用户多次出现在咖啡厅，则可推测出其有喝咖啡的习惯。近年来，国内多次发生因用户位置信息泄露而造成的犯罪事件[注1]。因此，位置隐私保护成为 LBS 广泛应用所亟需要解决的问题。

为解决位置隐私问题，Gruteser 和 Grunwald[3] 最早将数据库中 k-匿名隐私模型[4]应用到位置隐私保护。Chow 等[5]从系统结构方面总结 LBS 中位置隐私保护方案。现有的大部分位置隐私保护方案[6~10]采用具有可信匿名服务器的集中式结构，将用户的精确位置概化为满足需求的区域。显然，集中式结构中可信匿名服务器会成为通信瓶颈和攻击重点。本文采用无可信匿名服务器的分布式系统结构来克服这些缺陷。

此外，现有的方案[3,6~13]大都保护 LBS 中单个用户请求的位置隐私，对用户群组的位置隐私考虑较少，因而不适用于多个用户共同完成群组最近邻查询任务的协同计算环境[注2]。在这一场景下，群组中的用户一方面需要与其他用户交换消息来完成群组最近邻查询任务；另一方面又不愿意将自己的位置信息泄露给对方。此时，用户群组如何协同完成群组最近邻查询任务，同时保护群组中每个用户的位置隐私是要解决的主要问题，例如，如何安全地查找距离所有人都最近的地址。最直接的方法是各自将当前位置信息提供给 SP，由其完成最近邻位置查询。然而，不可信的 SP 将对用户的位置隐私造成极大的威胁。出于个人隐私考虑，群组中每个用户只将位置匿名后的区域信息发送给 SP，而不将自己的位置信息告诉 SP 或者其他用户。虽然这样能够保证群组中每个用户的位置隐私，但是由于无法得到每个用户的精确位置，因而查询结果不能保证距离所有用户都最近。

目前，针对最近邻查询的研究工作主要集中在以下 3 个方面。1) 单个用户最近邻(NN, nearest neighbor)查询中位置隐私保护方案[6,13~15]。这类方案主要解决单个用户最近邻查询中的位置隐私问题，并不适用于群组最近邻查询中用户位置隐私的保护。2) 用户群组最近邻(GNN, group nearest neighbor)查询方案[16~18]。此类方案集中于群组最近邻的查找方法，而缺少对群组中每个用户位置隐私的考虑。3) 群组最近邻查询的隐私保护方案[19~21]。这类工作与本文的研究最为接近。Hashem 等[19]首先研究群组最近邻查询中用户位置隐私问题。他们提出首先模糊群组中每个用户的位置为相应的匿名区域；然后，SP 根据这些区域返回所有可能的位置结果集；最后，通过提出的过滤算法查找距离群组中所有用户都最近的位置。然而，此方案不能阻止共谋攻击且计算代价较大。Huang 等[20]提出在集中式和分布式 2 种模型下，利用安全多方计算框架计算使与群组中所有用户位置的距离之和最小的目标位置，即为群组的最近邻。然而，这些方案考虑的候选目标位置是预先已经确定好的，并且距离的泄露威胁着用户的位置隐私。Ashouri-Talouki 等[21]基于 AV-net 和 Paillier 加密提出群组位置隐私协议 GLP，用来计算用户群组的质心位置，同时解决 SP 和群组中部分用户共谋所带来的位置隐私问题。然而，GLP 需要通过计算 AV-net 实现位置保护并且没有考虑群组中用户的运动状态，不能实现灵活的 GNN 查询。此外，群组内部因采用广播通信方式而需要占用较多的网络资源。Solanas 等[22]总结了不同隐私水平的质心位置计算方法。然而，这些方法都不是为群组位置隐私最近邻查询而设计，并且只考虑群组中只有一个恶意用户与 SP 串谋的情况。

针对上述现有工作中的问题，本文首先引入 LBS 中面向群组最近邻查询的分布式系统结构，用来克服集中式结构所存在的缺陷。基于此结构，考虑用户群组在不同状态下的查询需求，使用位置随机扰动和基于门限秘密共享的 Paillier 密码系统来保护群组中每个用户的位置隐私，同时计算用户群组的质心位置。基于文献[21,22]，将用户群组的最近邻查询转换为对应质心的最近邻查询，同时克服这些方案所存在的缺陷。随后，SP 根据所提供的质心位置计算距离群组中所有用户最近的目标位置，并返回给该用户群组。由于不需要预先得到候选目标位置，同时考虑了用户群组的不同运动状态，故而能实现灵活的群组最近邻查询。最后理论分析在这 2 种不同质心计算方法下，本文的方案抵抗现有的

注1：http://www.zyjjw.cn/news/keji/2013-07-04/108499.html。

注2：本文将完成某项任务所构成的用户称为一群组。

距离交叉攻击和共谋攻击的能力；同时，由于用户群组通信方式不同，相比其他的方案，本文的方案耗费较低的网络资源。

2 系统结构

由于集中式匿名系统结构存在通信瓶颈和攻击重点的缺陷，一些研究集中于 P2P 匿名系统结构的隐私保护[23,24]，即通过用户协作来产生满足 k-匿名要求的区域。然而，这些工作假设用户之间是相互信任的，若任一个用户与攻击者共谋，则群组中所有用户的位置隐私均受到威胁。

基于文献[23,24]的 P2P 系统结构，本文引入 LBS 中面向群组最近邻查询的分布式系统结构，如图 1 所示。该系统主要由用户群组、证书授权中心和 SP 组成，其中，群组中的用户在 GIS 数据库和无线通信技术的协助下，利用定位系统获取有关的位置信息。

2.1 系统假设

结合实际情况，本文做如下系统假设。

1) 群组中所有用户之间互不信任，即不会把自己的真实位置发送给对方；但他们都是半可信的，即一方面按照最近邻查询要求，不会伪造错误的位置来影响查询结果，但另一方面会试图推断群组中其他用户的位置。

2) 证书授权中心为一个独立的可信第三方机构，不会泄露用户的相关信息。同时，群组中所有用户均信任证书授权中心所颁发的证书。

3) SP 是半可信的。一方面他们会返回用户群组最近邻查询的正确执行结果；另一方面他们试图推断出用户的位置信息，同时因为利益关系将用户的位置信息泄露给其他方，从而威胁到用户的个人隐私。

2.2 功能部件

1) 用户群组

协作完成最近邻查询的所有用户构成一个群组。用户持有的终端设备，如智能手机、平板电脑等都具有定位功能，能随时随地决定用户所在的位置；同时具有唯一的身份标识，如手机号码、IP 地址等，用来支持群组中用户之间的通信。因此，终端设备的接口卡应具有 2 种功能[23]：1) 支持群组的近距离通信，如 Wi-Fi、IEEE 802.11 等；2) 支持群组的远距离通信，如 GSM、3G 等。

2) 证书授权中心

证书授权中心通过给每个用户分发证书来保证群组中通信用户的合法性。任何参与该群组最近邻查询计算的用户都需要取得相应的有效证书，从而避免了恶意用户的渗入影响最终的查询结果。其中群组中用户之间相互认证的过程不在本文的研究范围之内。另外，值得注意的是证书授权中心并不参与用户匿名的过程，即其并不知道群组中用户当前的位置信息，从而保证了群组中每个用户的位置独立性。

3) SP

SP 根据用户群组的多样化需求，提供各类与位置相关的服务。SP 可采用云计算技术构建相应的服务平台，通过给用户提供可定制的接口，实现位置服务的便捷查询。另外，需要指出的是在 2.1 节系统假设中，本文已假设 SP 是半可信的。

2.3 服务流程

一个典型的 LBS 流程主要包括 3 个阶段：服务请求、服务查询和服务响应。本文通过计算用户群组质心位置来查询群组最近邻，具体过程如下。

1) 服务请求。本文形式化请求服务的用户群组为 $G=\{(P_1,L_1),(P_2,L_2),\cdots,(P_k,L_k)\}$，其中，$P_i$ 表示用户的身份标识、如手机号码等，L_i 代表用户当前的位置信息 $(i=1,2,\cdots,k)$。为保护当前用户的位置信息，群组中的用户根据各自的位置协作计算质心位置 $\overline{L}$。服务请求可形式化为：$R=(P_u,\overline{L},Q)$，其

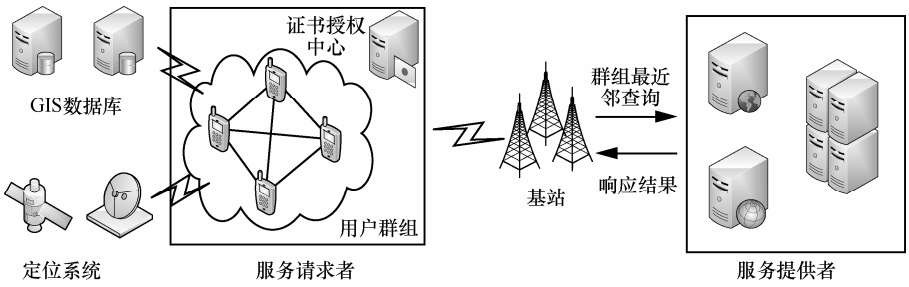

图 1 LBS 中面向群组最近邻查询的分布式系统结构

中，P_u 为用户群组与 SP 之间进行消息传递的代理用户，$\bar{L}$ 代表用户群组的质心位置，Q 表示用户群组最近邻查询请求的内容。注意，可从用户群组中随机指定一个用户作为代理用户，如 P_u。

2) 服务查询。SP 在收到服务请求 R 后，根据质心位置 $\bar{L}$，查询距离该质心位置最近的目标，并将结果返给群组中发出查询的代理用户 P_u。

3) 服务响应。群组中代理用户 P_u 在收到返回结果后，将服务查询结果分发给群组中其他的用户。

3　现有攻击模型分析

本节主要介绍现有的距离交叉攻击模型[19]和共谋攻击模型[21]。现有的具有位置隐私保护的群组最近邻计算方法[19,20]是在拥有候选目标位置 $O_1,O_2,\cdots,O_n$ 的前提下，群组中每个用户 $P_1,P_2,\cdots,P_k$ 直接根据各自当前位置计算其到目标位置 $O_1,O_2,\cdots,O_n$ 的距离，即

$$d_1=\sum_{i=1}^{k}d(P_i,O_1),\cdots,d_n=\sum_{i=1}^{k}d(P_i,O_n)$$

从而，计算使距离之和取得最小值 $d_{\min}=\min\{d_1,d_2,\cdots,d_n\}$ 的 $\bar{O}$，即为该群组最近邻的目标位置。

然而，距离的泄露易导致距离交叉攻击[19]，如图 2 所示。具体而言，尽管攻击者不知道群组中用户的具体位置，但是可通过与任意 3 个目标点位置的距离来推断出用户当前所在的位置。

如图 2 所示，尽管攻击者不知道 P_i 的位置，但是他能计算出 P_i 到各个目标位置 $O_i,i=1,2,\cdots,n$ 的距离。攻击者随机选择 3 个目标位置，如 O_1,O_2,O_3，则分别以 O_1,O_2,O_3 为圆心，以到 P_i 的距离为半径作圆，则交叉点即为 P_i 的位置。随后，Hashem 等[19]提出相应的解决方案。他们提出用区域 R_i 来模糊群组中用户 P_i 的位置，得到更新后的距离 $d'_{\max}(O_j)$ 为

$$d'_{\max}(O_j)=d_{\max}(O_j)-\mathrm{MaxDist}(R_i,O_j)+\mathrm{Dist}(P_i,O_j)$$

其中，$d_{\max}(O_j)$ 表示 O_j 到每个匿名区的最大距离之和，可计算为 $d_{\max}(O_j)=\sum_{i=1}^{n}\mathrm{MaxDist}(R_i,O_j)$，$\mathrm{MaxDist}(R_i,O_j)$ 代表 O_j 到匿名区域 R_i 的最大距离，$\mathrm{Dist}(P_i,O_j)$ 表示 P_i 到目标 O_j 的实际距离。

由于匿名区域的存在，尽管攻击者能够获得有关的计算距离，但无法通过距离交叉攻击推断出用户的实际位置。

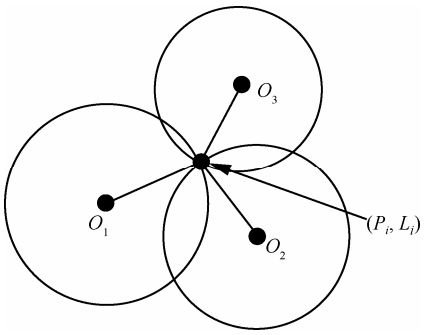

图 2　距离交叉攻击

然而，该方案不能抵御部分共谋攻击。根据文献[21]分析，因为 SP 知道上传的匿名区域的大小，则攻击者可以计算出目标位置到各个匿名区域的最大值 $\mathrm{MaxDist}(R_i,O_j)$，如图 3 中虚线所示。

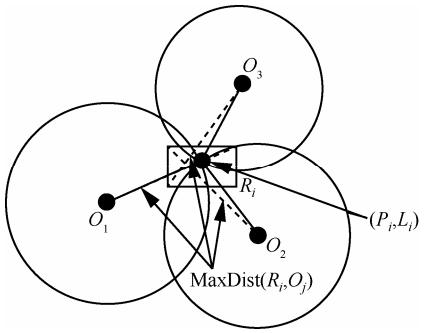

图 3　共谋攻击

假若 SP 与群组中 2 个用户 P_{i-1},P_{i+1} 共谋，则可推断出用户 P_i 的实际距离。这是因为攻击者根据 P_i 的前驱 P_{i-1} 可得到 $d_{\max}(O_j)$，根据 P_i 的后继 P_{i+1} 可得到 $d'_{\max}(O_j)$，则有

$$d(P_i,O_j)=\mathrm{MaxDist}(R_i,O_j)-[d_{\max}(O_j)-d'_{\max}(O_j)]$$

在计算出 $d(P_i,O_j)$ 之后即可发起距离交叉攻击。

4　位置隐私保护的群组最近邻(GNN)查询

针对这 2 类已有的攻击，与文献[21]一样，本文考虑通过群组的质心位置来查找用户群组的最近邻查询点，从而克服文献[19,20]中需要事先得到所有候选目标的位置，以及通过计算并比较所有候选目标位置到用户群组的距离和所带来的额外开销等缺陷。因此，在考虑群组中每个用户位置隐私的情况下，安全地计算质心位置是要解决的主要问题。

4.1　位置随机扰动的 GNN 查询

为了保护群组中用户的位置隐私，一种简单的

方案[22]即是扰动群组中每个用户的位置。文献[22]产生均值为0的高斯噪声，同时要求群组中参与计算的用户数k很大。然而，其对于数量k较少时是不适用的。本文对用户数k没有要求，利用噪声发生器产生一组特定的噪声序列(δ_i^x,δ_i^y)，用来扰动群组中用户P_i的位置(x_i,y_i)，其中，$(\frac{\sum_{i=1}^{k}\delta_i^x}{k},\frac{\sum_{i=1}^{k}\delta_i^y}{k})=(0,0)$。因此用户$P_i$扰动后的位置$L'_i$，计算如下

$$L'_i=(x'_i,y'_i)=(x_i,y_i)+(\delta_i^x,\delta_i^y)=(x_i+\delta_i^x,y_i+\delta_i^y)$$

将扰动后的位置发给用户群组中之前随机选定的一个代理用户P_u，由其计算群组质心的位置，即

$$\begin{aligned}(\bar{x},\bar{y})&=(\frac{\sum_{i=1}^{k}x'_i}{k},\frac{\sum_{i=1}^{k}y'_i}{k})\\&=(\frac{\sum_{i=1}^{k}(x_i+\delta_i^x)}{k},\frac{\sum_{i=1}^{k}(y_i+\delta_i^y)}{k})\\&=(\frac{\sum_{i=1}^{k}x_i}{k},\frac{\sum_{i=1}^{k}y_i}{k})+(\frac{\sum_{i=1}^{k}\delta_i^x}{k},\frac{\sum_{i=1}^{k}\delta_i^y}{k})\end{aligned}$$

因特定的噪声序列满足$(\frac{\sum_{i=1}^{k}\delta_i^x}{k},\frac{\sum_{i=1}^{k}\delta_i^y}{k})=(0,0)$，故由$P_u$计算出来的$(\bar{x},\bar{y})$即是质心位置，然后，SP查询距离该质心最近的目标位置即被近似成该群组的最近邻位置，将其返回给P_u，由P_u分发给群组中其他的用户。

虽然该方法能够在阻止攻击者获取群组中每个用户的实际位置的情况下，以较低的计算代价得到用户群组的质心位置。但由于存在特定的噪声序列，根据文献[22]的分析可知，若群组中用户不改变本身的位置而重复使用该方法，则扰动后的位置平均值趋向于用户的实际位置。因此，通过加噪声对于处于静止状态下用户的多次查询是无效的，攻击者较容易推断出用户的实际位置。

4.2 基于门限秘密共享的 Paillier 密码系统的 GNN 查询

为了解决上一节中用户群组静止状态下重复查询所存在的问题，在位置随机扰动的基础上，提出基于门限秘密共享的 Paillier 密码系统[25,26]来计算用户群组的质心位置。需要指出的是与文献[25,26]中利用该密码技术的目的不同，本文是用来解决 LBS 中位置隐私保护的静态群组最近邻查询问题。

1) 密钥初始化

①参数设置

随机生成 2 个大素数p,q，计算$n=pq$使得$gcd(n,\varphi(n))=1$，其中，$p=2p'+1$，$q=2q'+1$，$m=p'q'$；然后随机选择参数：$(a,b)\in Z_n^*\times Z_n^*$，$\beta\in Z_n^*$，计算$g=(1+n)^a b^n \bmod n^2$。用户群组$G$的公钥：$PK=(g,n)$，私钥：$SK=\beta m$。

② 密钥分发

基于 Shamir[27]提出的门限秘密共享方案，根据群组中参与计算的用户数k，将私钥SK按照多项式函数$f(x)=\sum_{i=0}^{k}\alpha_i x^i$，$\alpha_i\in\{0,1,\cdots,nm-1\}$进行拆分，其中，$\alpha_0=f(0)=\beta m$表示用户群组私钥。然后，将拆分后的子密钥分发给用户群组G中的每个用户，即用户$P_i\in G$得到的密钥为$s_i=f(x_i)\bmod nm$，$i=1,2,\cdots,k$。因此，当且仅当群组中参与计算的k个用户协作才能解密所加密的消息。

2) 位置加密

随机选择$r_i\in Z_n^*$，利用 Paillier 加密函数$E(\cdot)$来加密群组中k个用户，利用 4.1 节中位置随机扰动方法所得到各自的位置信息$L'_i=(x'_i,y'_i)$,$1\leqslant i\leqslant k$，即

$$c_i=E_{PK}(L'_i)=g^{L'_i}r_i^n \bmod n^2,\ i=1,2,\cdots,k$$

注意，由于用户之间是相互独立的，群组中所有用户的加密过程可以并行处理，则有

$$\begin{aligned}c_i&=(E_{PK}(x'_i),E_{PK}(y'_i))\\&=(g^{x'_i}r_i^n \bmod n^2,g^{y'_i}r_i^n \bmod n^2),i=1,2,\cdots,k\end{aligned}$$

然后，将加密后的结果发给群组中的用户代理P_u，P_u在收到所有加密的位置后，计算位置和密文

$$\begin{aligned}C&=\prod_{i=1}^{k}c_i=(\prod_{i=1}^{k}E_{PK}(x'_i),\prod_{i=1}^{k}E_{PK}(y'_i))\\&=(g^{\sum_{i=1}^{k}x'_i}\prod_{i=1}^{k}r_i^n \bmod n^2,g^{\sum_{i=1}^{k}y'_i}\prod_{i=1}^{k}r_i^n \bmod n^2)\end{aligned}$$

将计算结果C发给群组中相应的用户。

3) 解密及质心位置计算

在群组中的用户收到P_u发来的C后，由于需要该k个用户的全部私钥才能解密密文信息，而每个用户并不知道其他用户的私钥，因此只能用各自私钥s_i解密其中的部分密文，即

$$w_i=C^{2k!s_i} \bmod n^2,\ i=1,2,\cdots,k$$

然后，将w_i返回给P_u，P_u根据收到的信息可分别恢复出所对应的两位置坐标和的明文信息$SL=(SL_x,SL_y)=(\sum_{i=1}^{k}x'_i,\sum_{i=1}^{k}y'_i)$，两坐标和的计

算方法相同，SL'表示SL_x或SL_y，如下

$$SL' = L(\prod_{i=1}^{k} w_i^{2\mu_{0,i}}) \times \frac{1}{4(k!)^2 L(g^{\beta m})} \bmod n$$

其中，$L(u) = \frac{u-1}{n}$，$\mu_{0,i} = k! \prod_{j=1 \wedge j \neq i}^{k} \frac{j}{j-i} \in Z$。

具体解密正确性证明见定理 1。在计算出$SL = (\sum_{i=1}^{k} x'_i, \sum_{i=1}^{k} y'_i)$后，由第 4.1 节可知质心位置为$\overline{L} = (\overline{x}, \overline{y}) = \frac{SL}{k} = (\frac{\sum_{i=1}^{k} x'_i}{k}, \frac{\sum_{i=1}^{k} y'_i}{k})$，从而可根据此质心位置查询用户群组最近邻的位置。

5　安全性和特性分析

本节首先基于文献[25,26,29]从正确性以及抗伪造密钥攻击 2 个方面证明本文方案的有效性；然后，针对已有的攻击模型，理论分析本文方案所具有的隐私保护特性；最后，通过对比分析本文方案与相关方案[19,21,22]的有关特性来说明本文方案的优势。

5.1　有效性分析

显然，基于位置随机扰动方案能正确得到用户群组质心的位置，从而实现 GNN 查询。因此，本文利用文献[25,26]中对门限秘密共享 Paillier 密码系统的正确性证明来说明群组中随机指定的用户代理P_u能够获得用户群组的质心位置，从而实现 GNN 查询。

定理 1　使用门限秘密共享的 Paillier 密码系统，P_u能够得到用户群组的质心位置，实现 GNN 查询。

证明　由拉格朗日插值函数，群组中参与计算的k个用户利用自己的子密钥可计算多项式

$$f(x) = \sum_{i=1}^{k} f(i) \prod_{j=1 \wedge j \neq i}^{k} \frac{x-j}{i-j} \bmod nm$$

从而有

$$\beta m = f(0) = \sum_{i=1}^{k} f(i) \prod_{j=1 \wedge j \neq i}^{k} \frac{j}{j-i}$$
$$= \frac{1}{k!} \sum_{i=1}^{k} \mu_{0,i} f(i) \bmod nm$$

由于群组中每个用户P_i只有部分密钥s_i，其解密密文得到$w_i = C^{2k!s_i}$，从而

$$\prod_{i=1}^{k} w_i^{2\mu_{0,i}} = \prod_{i=1}^{k} C^{4k!\mu_{0,i}s_i} = \prod_{i=1}^{k} C^{4k!\mu_{0,i}f(i)}$$
$$= C^{4k!\sum_{i=1}^{k}\mu_{0,i}f(i)} = C^{4(k!)^2\beta m} \bmod n^2$$

为方便起见，只考虑验证位置坐标和中的一个明文$SL_x = \sum_{i=1}^{k} x'_i$的解密过程。对于$SL_y = \sum_{i=1}^{k} y'_i$解密的证明过程类似。由加密过程得到的密文有

$$C^{4(k!)^2\beta m} = (g^{SL_x} \prod_{i=1}^{k} r_i^n)^{4(k!)^2\beta m}$$
$$= (1+n)^{4aSL_x(k!)^2\beta m} (b^{SL_x} \prod_{i=1}^{k} r_i)^{4(k!)^2\beta mn} \bmod n^2$$

根据文献[26,28]中有关的分析结论：$\forall l \in Z_{n^2}^*$，有$l^{n\lambda} = 1 \bmod n^2$，其中，$\lambda = lcm(p-1, q-1)$。本文中因$b \in Z_n^*, r_i \in Z_n^*$，则可令$l = b^{SL_x} \prod_{i=1}^{k} r_i$，同时$\lambda = lcm(p-1, q-1) = 2p'q' = 2m$，故有

$$l^{n\lambda} = (b^{SL_x} \prod_{i=1}^{k} r_i)^{2mn} = 1 \bmod n^2$$

从而有

$$L(\prod_{i=1}^{k} w_i^{2\mu_{0,i}}) = L(C^{4(k!)^2\beta m}) = L((1+n)^{4aSL_x(k!)^2\beta m})$$
$$= L(1 + 4an(k!)^2 \beta m.SL_x \bmod n^2)$$
$$= 4a(k!)^2 \beta m SL_x \bmod n$$

同理可得：$L(g^{\beta m}) = a\beta m \bmod n$。则由解密函数可验证：$SL_x = L(\prod_{i=1}^{k} w_i^{2\mu_{0,i}}) \frac{1}{4(k!)^2 L(g^{\beta m})} \bmod n$。

对于解密SL_y的证明过程是类似的，本文不再重复。在计算出$SL = (SL_x, SL_y) = (\sum_{i=1}^{k} x'_i, \sum_{i=1}^{k} y'_i)$后，根据 4.1 节中位置随机扰动的分析过程，则可以求得用户群组的质心位置$\overline{L}$，从而实现 GNN 查询。

此外，为了防止群组中的用户伪造解密密钥影响查询结果，需要在不暴露用户私钥的情况下证明用户群组中仅拥有此私钥的用户才能正确解密部分密文。该验证过程由可信第三方机构（如证书授权中心）来完成。本文基于零知识证明[29]来证明该结论，先形式化定义如下。

定理 2　在不泄露用户P_i所拥有的私钥s_i的情况下，可证明w_i仅能由P_i的真实私钥s_i解密获得，其中$i = 1, 2, \cdots, k$。

证明　用户P_i用其分配的密钥s_i解密得到的密文为：$w_i = C^{2k!s_i} \bmod n^2$。因为$u = C^{2k!}$是已知的，则转化为要证明$w_i = u^{s_i} \bmod n^2$。

群组中证明者P_i随机选择$e \in Z_n^*$，计算承诺$u^e \bmod n^2$，将其发送给验证者，如证书授权中心。验证者随后发送挑战$d \in Z_n^*$给证明者P_i。证明者P_i计算并发送$h = e + s_i d$给验证者。最后验证者验证$u^h \bmod n^2 \stackrel{?}{=} u^e u^{s_i d} \bmod n^2$是否成立。若成立，则证

明 w_i 是由群组中用户 P_i 的真实密钥 s_i 解密的；反之，则不成立。

5.2 隐私性分析

本文中的位置随机扰动和基于门限秘密共享的 Paillier 密码系统均通过扰动群组中每个用户的实际位置来计算用户群组的质心位置。一方面避免了预先通过区域查询得到候选目标位置所带来的额外开销；另一方面阻止了因泄露目标位置与用户实际位置的距离而导致的距离交叉攻击。因此，本节主要分析用户群组在不同运动状态下，该 2 种方案抵御共谋攻击的能力。

在此之前，先明确 SP 与群组中用户共谋的数量 k'。与文献[21]类似，本文考虑 SP 与群组中的用户部分共谋的情况，即 $1 \leqslant k' < k-1$。

定理 3 在 GNN 查询中，位置随机扰动方法不能抵御静态用户群组下的共谋攻击，但是能够抵御动态用户群组下的共谋攻击。

证明 在位置随机扰动的方法中，群组中的用户均将扰动后的位置数据发送给随机选择的代理用户 P_u。用户之间的计算过程是相互独立的。在静态用户群组查询的情况下，即群组中的用户不改变当前的位置，由 4.1 节中分析可知[22]，该方法不能阻止重复查询所带来的用户位置泄露。此时 SP 与用户群组中代理用户 P_u 共谋，则可以获得用户群组中其他用户的位置信息。因此，在这种情况下不能抵御共谋攻击。

在动态用户群组查询的情况下，即群组中的用户每次请求都改变当前的位置，则能阻止重复查询所带来的用户位置泄露。当 SP 与群组中 k' 个用户共谋，得到 k' 个用户的位置坐标和。然而，由于 $k-k' \geqslant 2$，则仅能得到至少包含 2 个扰动用户的位置坐标和，因而无法推断 $k-k'$ 个用户的实际位置，因此，在动态用户群组下，位置随机扰动方法能够抵抗共谋攻击。

定理 4 在 GNN 查询中，门限秘密共享的 Paillier 密码系统能抵御 2 种状态下的共谋攻击。

证明 门限秘密共享的 Paillier 密码系统是用来解决静态用户群组下重复查询所导致的位置隐私泄露问题。因为该方案构建在位置随机扰动的基础上，故而能抵御动态用户群组下的共谋攻击。在静态用户群组查询的情况下，该方案群组中每个用户仅仅得到证书授权中心分发给自己的子密钥信息，无法知道群组中其他用户的密钥，因此发给群组的用户代理 P_u 的数据都是用各自子密钥加密后的位置信息。一方面，即使 SP 与群组中 k' 个用户共谋，因其无法得到其他 $k-k'$ 的子密钥，故而无法推断出他们的位置；另一方面，SP 能得到群组中 k 个用户扰动后的位置之和。虽然其能得到共谋 k' 个用户的位置，但是由于 $k-k' \geqslant 2$，则其仅能得到至少包含 2 个用户的扰动位置之和，故而也无法推断出他们的位置。综上，该方案能抵御不同运动状态下用户群组的共谋攻击。

5.3 特性对比分析

本节从理论分析角度对比本文的方案与相关方案[19,21,22]的有关特点，如表 1 所示。

考虑群组中 k 个用户参与位置隐私保护的 GNN 计算过程。在计算方法上，文献[19,20]均采用距离和计算 GNN，他们都需要预先得到候选目标的位置。本文以文献[19]作为实例来比较，群组中 k 个用户分别发送匿名区域计算请求，然后 SP 根据匿名区域返回 n 个候选目标位置集合，故查询点个数为用户群组中参与计算的用户数 k，结果集为 $O(n)$。因为采用环形单播方式计算用户群组与候选结果集的距离之和来过滤得到 GNN，因此占用的网络资源较低。

相比文献[19,20]，文献[21,22]及本文都考虑如何安全计算用户群组质心的位置。尽管文献[22]并不用于 GNN 查询，但总结了不同隐私级别的质心位置的计算方法。本文考虑与文献[22]中位置隐私水平最高的随机链式质心位置计算方法做比较。由于通过计算用户群组质心位置将 GNN 查询转化为质心的 NN 查询，故查询点个数只有质心点 1 个，

表 1 特性比较

方案	计算方法	通信方式	网络资源	用户状态	查询点个数	结果集大小	共谋用户个数 k'
文献[19]	距离和	环形单播	低	没有考虑	k	$O(n)$	$k'=0$
文献[21]	质心	群组广播	高	没有考虑	1	$O(1)$	$1 \leqslant k' < k-1$
文献[22]	质心	环形单播	低	静态/动态	1	$O(1)$	$k'=1$
本文	质心	星型单播	低	静态/动态	1	$O(1)$	$1 \leqslant k' < k-1$

返回的结果集为 $O(1)$。然而，由于群组内部不同的计算方式使得通信耗费不同的网络资源。文献[21]中基于 AV-net 和 Paillier 加密技术所提出的 GLP 协议包括 AV-net 值计算和用户群组质心位置计算 2 个过程。尽管不需要预先得到候选结果集，但是需要预先计算 AV-net 值。同时，在计算过程中群组中每个用户都需要给其他用户广播相应的消息，相比文献[19,22]及本文的单播通信方式需要占用较多的网络资源。此外，文献[21]与本文方案都是从密码学角度分析多用户共谋攻击。相比而言，本文采用了不同的方法计算用户群组的质心位置，同时分析了用户群组在不同运动状态下抵御共谋攻击的能力。由于群组中用户位置的计算过程是相互独立，本文所采用的星型拓扑结构相比环形结构[22]能高度并发处理加解密过程，减少系统等待时延。

此外，文献[19]并没有考虑共谋攻击问题，即共谋用户数量 $k'=0$；而文献[22]仅考虑某个代理用户与 SP 之间的共谋情况，即 $k'=1$。这些方案都不能阻止 SP 与群组中多个用户共谋所带来的位置隐私问题。文献[21]指出在选定特定共谋对象的情况下，如用户 P_i 的前驱 P_{i-1} 与后继 P_{i+1}，文献[19]所提出的方案不能保护 P_i 的位置隐私。文献[21]和本文都考虑的是 SP 与群组中多个但不是全部用户共谋的情况，即 $1\leqslant k'<k-1$。如文献[21]通过群组中每个用户用各自的参数计算 AV-net 值来匿名相应的位置信息，同时抵御共谋攻击。而考虑到计算代价及用户群组的不同运动状态，本文通过位置随机扰动和门限秘密共享的 Paillier 密码系统来抵抗 SP 与群组中多个用户之间的共谋攻击。

6　结束语

本文研究 LBS 中面向用户协同位置隐私保护的群组最近邻查询。考虑到 LBS 中集中式匿名系统结构所存在的缺陷，首先引入了 LBS 中面向群组最近邻查询的分布式系统结构。基于此结构，通过用户协作计算用户群组的质心位置坐标，将用户群组最近邻查询转换为相应质心位置的最近邻查询。考虑到计算复杂性和用户群组的运动状态信息，提出了利用位置随机扰动和基于门限秘密共享的 Paillier 密码系统来安全地计算用户群组的质心位置。针对现有的 2 类攻击，理论分析本文的 2 种用户群组隐私保护方案在不同状态下所具有的位置隐私保护能力。分析表明，相比已有的工作，本文的方案更加灵活，同时具有更好的计算性能。未来的工作将集中于开发集成这 2 种方案的 LBS 应用原型系统。

参考文献：

[1] 周傲英，杨彬，金澈清等. 基于位置的服务：架构与进展[J]. 计算机学报, 2011, 34(7): 1155-1171.
ZHOU A Y, YANG B, JIN C Q, *et al*. Location-based services: architecture and progress[J]. Chinese Journal of Computers, 2011, 34(7): 1155-1171.

[2] VIRRANTAUS K, MARKKULA J, GARMASH A, *et al*. Developing GIS-supported location-based services[A]. WISE[C]. Kyoto, 2001. 66-75.

[3] GRUTESTER M, GRUNWALD D. Anonymous usage of location-based services through spatial and temporal cloaking[A]. MobiSys[C]. USA, 2003. 31-42.

[4] SWEENEY L. *k*-anonymity: a model for protecting privacy[J]. Journal of Uncertainty Fuzziness and Knowledge Based Systems, 2002, 10(5): 557-570.

[5] CHOW C Y, MOKBEL M F. Privacy in location-based services: a system architecture perspective[J]. SIGSPATIAL Special, 2009, 1(2): 23-27.

[6] MOKBEL M F, CHOW C Y, AREF W G. The new Casper: query processing for location services without compromising privacy[A]. VLDB[C]. Seoul Korea, 2006.763-774.

[7] XIAO Z, MENG X, XU J. Quality aware privacy protection for location-based services[A]. DASFAA[C]. Thailand, 2007.434-446.

[8] GEDIK B, LIU L. Protecting location privacy with personalized *k*-anonymity: architecture and algorithms[J]. IEEE Transactions on Mobile Computing, 2008, 7(1): 1-18.

[9] BAMBA B, LIU L, PESTI P, *et al*. Supporting anonymous location queries in mobile environments with privacygrid[A]. WWW[C]. Beijing, China, 2008.237-246.

[10] WANG Y, XU D, HE X, *et al*. L2P2: location-aware location privacy protection for location-based services[A]. INFOCOM[C]. Orlando, FL, USA, 2012.1996-2004.

[11] SHOKRI R, THEODORAKOPOULOS G, TRONCOSO C, *et al*. .Protecting location privacy: optimal strategy against localization attacks[A]. CCS[C]. North Carolina, USA, 2012.617-627.

[12] GAO S, MA J F, SHI W S, *et al*. LTPPM: a location and trajectory privacy protection mechanism in participatory sensing[J]. Wireless Communications and Mobile Computing, 2015,15(1): 155-169.

[13] GHINITA G, KALNIS P, KHOSHGOZARAN A, *et al*. Private queries in location based services: anonymizers are not necessary[A]. ACM SIGMOD[C]. Vancouver, BC, Canada, 2008, 121-132.

[14] YIU M L, JENSEN C S, HUANG X, *et al*. SpaceTwist: managing the trade-offs among location privacy, query performance, and query accuracy in mobile services[A]. ICDE[C]. Mexico, 2008, 366-375.

[15] HASHEM T, KULIK, L. Don't trust anyone: privacy protection for location-based services[J]. Pervasive and Mobile Computing, 2011, 7(1): 44-59.

[16] PAPADIAS D, SHEN Q, TAO Y, *et al*. Group nearest neighbor queries[A]. ICDE[C]. MA, USA, 2004. 301-312.

[17] PAPADIAS D, TAO Y, MOURATIDIS K, *et al*. Aggregate nearest neighbor queries in spatial databases[J]. ACM Transactions on Data-

base Systems, 2005, 30(2): 529-576.

[18] LIAN X, L CHEN, LIAN X, *et al*. Probabilistic group nearest neighbor queries in uncertain databases[J]. IEEE Transactions on Knowledge and Data Engineering, 2008, 20(6): 809-824.

[19] HASHEM T, KULIK L, ZHANG R. Privacy preserving group nearest neighbor queries[A]. EDBT[C]. Lausanne, 2010. 489-500.

[20] HUANG Y, VISHWANATHAN R. Privacy preserving group nearest neighbour queries in location-based services using cryptographic techniques[A]. GLOBECOM[C]. Miami, FL, 2010.1-5.

[21] ASHOURI-TALOUKI M, BARAANI-DASTJERDI A, SELCUK A A. GLP: a cryptographic approach for group location privacy[J]. Computer Communications, 2012,35(12): 1527-1533.

[22] SOLANAS A, MARTINEZ-BALLESTE A. A TTP-free protocol for location privacy in location-based services[J]. Computer Communications, 2008, 31(6): 1181-1191.

[23] CHOW C Y, MOKBEL M F, LIU X. A peer-to-peer spatial cloaking algorithm for anonymous location-based service[A]. SIGSPATIAL GIS[C]. New York, NY, USA, 2006.171-178.

[24] CHE Y, YANG Q, HONG X. A dual-active spatial cloaking algorithm for location privacy preserving in mobile peer-to-peer networks [A]. WCNC[C]. Paris, France, 2012.2098-2102.

[25] FOUQUE P A, POUPARD G, STERN J. Sharing decryption in the context of voting or lotteries[A]. FC[C]. London, 2001.90-104.

[26] 雷浩等. 面向有差异群体的联合决策方案[J]. 电子学报, 2005, 33(8): 1523-1528.
LEI H, *et al*. A joint decision-making scheme for groups with members having different superiorities[J]. Chinese Journal of Electronics, 2005, 33(8): 1523-1528.

[27] SHAMIR A. How to share a secret [J]. Communications of the ACM, 1979, 22(11): 612-613.

[28] PAILLIER P. Public-key cryptosystems based on composite degree residuosity classes[A]. EUROCRYPT[C]. Prague, 1999.223-238.

[29] DAMGARD I, FAZIO N, NICOLOSI A. Non-interactive zero-knowledge from homomorphic encryption[A]. TCC[C]. New York, NY, USA, 2006.41-59.

作者简介：

高胜（1987-），男，湖北黄冈人，西安电子科技大学博士生，主要研究方向为移动感知计算、基于位置的服务、位置和轨迹隐私等。

马建峰（1963-），男，陕西西安人，博士，西安电子科技大学教授、博士生导师，主要研究方向为网络与信息安全等。

姚青松（1982-），男，湖北松滋人，博士，西安电子科技大学讲师，主要研究方向为网络安全、隐私保护。

孙聪（1982-），男，陕西兴平人，博士，西安电子科技大学副教授，主要研究方向为信息流安全。