分布式结构下基于用户协作的匿名区域构建算法

吴丹丹 吕 鑫
(河海大学计算机与信息学院 南京 211100)

摘 要 随着移动终端的日益普及和通信技术的飞速发展,基于位置的服务应用愈发广泛。但用户的位置信息时常涉及个人隐私,因此如何在确保服务质量的同时防止用户隐私的泄露是当前研究的热点问题。文中提出了一种分布式结构下基于用户协作的匿名区域构建算法,该方法在设定范围内随机选取锚点,并通过逐跳广播的方式搜寻协作用户,直至满足匿名需求。在协作用户响应过程中,用户计算自身到锚点的距离,形成以锚点为圆心的匿名区域。实验结果表明,该方法可有效抵御共谋攻击和匿名中心攻击,同时能较大程度地降低平均匿名面积。

关键词 P2P,位置隐私,锚点,欧氏距离
中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2019.04.025

Location Anonymous Algorithm Based on User Collaboration under Distributed Structure

WU Dan-dan LYU Xin
(College of Computer and Information, Hohai University, Nanjing 210000, China)

Abstract With the increasing popularity of mobile terminals and the rapid development of communication technology, location-based service applications have been widely used in people's daily life. However, the users' location information is commonly privacy-related. Thus, how to preserve users' privacy while guaranteeing the service quality has become a hot issue in current research. An anonymous region constructing algorithm, through collaborating users, was proposed in this paper. The anchor is randomly selected in the designed set, and the cooperative users can be discovered by broadcasting hop-by-hop, until the anonymous demand is satisfied. During the collaboration responding process, the anchor-centered anonymous region is formed based on the distance between the user and the anchor. The experimental results show that the proposed algorithm is able to effectively resist collusion attacks and anonymous center attacks, meanwhile, the average area of anonymous region is greatly decreased.

Keywords P2P, Location privacy, Anchor, Euclidean distance

1 引言

近年来,随着智能手机、平板电脑等智能终端的飞速发展,基于位置的服务(Location-based Service,LBS)在各个领域得到了广泛应用。用户可以利用移动终端随时向LBS服务商发送位置查询请求,如"距离我最近的医院""距离我5 km里面的超市",以及应用较为广泛的滴滴打车等。但是由于在进行位置请求的过程中,用户需要提交自己的位置坐标,当LBS服务商不可信或者发生恶意攻击时,用户的位置隐私就会面临被泄露的风险,因而如何在位置服务中对位置隐私进行保护成为了一个热门的研究方向。

2 相关工作

目前针对位置隐私的研究主要分为中心式结构以及分布式结构。中心式结构的主要实现手段是在用户和LBS服务商之间增加一个可信的第三方,可信第三方通过构建匿名区域、选取假位置、位置模糊化等方法进行位置隐私保护。Cruteser[1]根据数据库中的k匿名化的方法提出了将真实用户的位置放入到一个包含$k-1$个虚假位置的用户集合中,LBS根据集合中用户的请求返回位置信息的方法。这样即便是攻击者截获了用户集合,推测出真实用户的概率也只有$1/k$。但是由于虚假位置是随机选取的,因此很有可能出现选取的位置在湖泊、高山等不可能成为用户点的特殊情况。为了解决这个问题,Niu等[2]提出了根据位置熵来选择假位置的方法,即中心服务器在进行假位置生成时根据用户所在网格的信息熵来挑选假位置。虽然生成假位置的方法快捷安全,但如果用户的匿名需求k较大,极易造成可信第三方的工作负载。当用户连续请求位置服务时,由于现有保护单次查询的假位置方案未考虑相邻位置集合间的时空关系,使攻击者能推断出假位置,降低了用户的位置隐私保护等级。针对

到稿日期:2018-06-05 返修日期:2018-10-25 本文受国家重点研发计划课题(2018YFC0407105,2016YFC0400910),国家自然科学基金面上项目(61272543),NSFC-广东联合基金重点项目(U1301252)资助。

吴丹丹(1993-),女,硕士生,主要研究方向为位置隐私保护,E-mail:1024399176@qq.com;吕 鑫(1983-),男,博士生,讲师,CCF会员,主要研究方向为网络与信息安全,E-mail:lvxin.gs@163.com(通信作者)。

上述问题，文献[3]通过对生成的候选假位置进行连续合理性检查和单次隐私增强来对其进行筛选，提出了一个适用于连续请求的假位置隐私保护增强方法。现有方案在匿名区构造过程中均未考虑位置服务提供商（Location-based Service Provider，LSP）的查询区域面积，导致 LBS 查询服务质量降低。为了解决上述问题，文献[4]将用户的查询范围引入到匿名区的构造中，匿名服务器首先生成满足用户隐私保护需求的初始子匿名区，再以 LSP 的查询区域面积为判定标准进行子匿名区合并，能有效降低 LSP 的查询区域面积，从而提高 LBS 查询的服务质量。

由于中心式的服务结构对于第三方的要求较高，在整个位置请求过程中很有可能成为系统性能瓶颈，并且可信第三方一旦被攻破将会导致用户位置的直接泄露，存在较大的安全隐患。因此众多专家学者提出了分布式的位置隐私保护框架。Yiu[5] 提出了 SpaceTwist 方案，利用用户身边随机选取的兴趣点进行增量查询，该方法不需要借助于可信第三方，但无法实现 k 匿名。文献[6]在此基础上结合已有的 SpaceTwist 方法来实现用户协作，并且达到了 k 匿名效果。Perazzo[7] 指出了已有位置偏移和模糊方案中存在的缺陷，并且在此基础上提了一种偏移向量的概率分布函数。Andres 等[8] 将差分隐私与位置隐私保护相结合，设计了一种满足该特性的噪音生成机制，使得用户位置不可辨别，由此来保护隐私。由于存在关联概率攻击，文献[9]针对这些攻击方法提出了与之对应的基于广义差分隐私的隐私保护模型，基于建立的隐私保护模型设计了基于位置偏移产生关联概率不可区分的隐私保护方法。

由于位置偏移模糊化会造成服务质量下降，为解决这个问题，文献[10]提出了可信任用户协作无中心服务器的隐私保护方法，该算法由查询用户自身发送广播来与其他用户通信构建匿名区，但是这种方法存在诸多问题。针对文献[10]所提出的 P2P 算法的问题，文献[11]提出了改进算法 P2PSC，通过对获得的匿名区域进行随机扩大来规避匿名区中心攻击，但仍然无法抵御共谋攻击[12]，存在安全隐患。Manweiler 等[13] 提出陌生人之间的协作方案，主要是通过蓝牙进行通信，但系统开销较大。文献[14]采用了四叉树结构对区域用户建立索引来构建匿名区，用户首先查看所在网格内的用户数，如果不能构成 k 匿名，则查看兄弟节点中的用户数，进而再查看父节点中的用户数，以确保达到 k 匿名。但该方法形成的匿名区域中的有效面积不能确定，很有可能包括很多没有用户点的区域。文献[15]提出了个性化 k 匿名方案，将整个区域进行层次划分，形成一个自顶向下的金字塔数据结构，用户可以根据自己的需求设置不同的 k 和匿名区域大小。文献[16]在分布式结构下提出了基于网格扩增的方法，可以快速地找到 k 个用户并且有效杜绝匿名区中心攻击问题，但形成的匿名区域较大影响了服务质量，并且由于通信距离的限制使得用户之间的沟通成为障碍。

由于整个分布式匿名组中协作用户以及查询用户都是半可信的，即在提交自身的真实位置来协作构建匿名组的同时也想要获取其他用户的位置信息，所以很有可能出现查询用户或者协同用户是攻击者的情况，即为共谋攻击[12]。因此，近三年来不少专家学者将密码学与分布式位置隐私保护结合起来，文献[17]提出了基于 AV-net 和 Paillier 的群组加密、位置隐私协议 GLP，通过计算用户群组的质心位置并以质心为中心构建匿名区域来解决该问题，但并未考虑到用户运动的情况；文献[18]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，但整个算法不仅需要对用户位置进行扰动还需要进行加密、解密，时间复杂度较高。

本文提出了分布式结构下基于用户协作的匿名区域构建算法（P2P-D），该算法从两个方面进行了改进。

1）利用网格划分，随机选取网格中心作为查询用户的锚点，将锚点作为自己的真实位置发送给协同用户。随后以锚点为圆心构建圆形匿名区域，有效规避了匿名区域的中心攻击，且无需进行加密、解密，时间复杂度较低。

2）在接收到查询用户发出的广播后，协同用户不再发送自己的真实位置，而是将自身到锚点的距离发送给查询用户，有效解决了暴露用户真实位置的隐患。

3　相关知识

3.1　系统结构

本文基于分布式用户协作体系结构进行研究，系统框架如图 1 所示。在分布式结构中，每个终端设备都具有较高的计算处理能力，移动用户相互信任、地位平等、互相协助，共同参与匿名区域构建。移动用户 A 发起查询请求时，向周围用户发送广播请求协作，当有 $k-1$ 个用户响应后根据每个响应点的位置构建匿名区域 S。随后 A 在这些移动用户内选取一个代理节点 B，由 B 将请求以及匿名区域 S 发送至 LBS 位置服务器。LBS 位置服务器完成查询处理后，将结果集返回给 B，B 再通过网络发送给 A，A 根据自己的真实位置来对返回结果进行筛选。

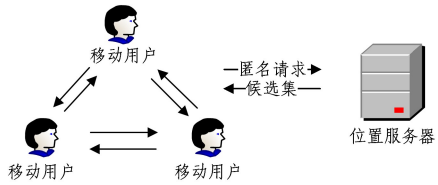

图 1　P2P 系统构架

Fig. 1　System architecture of P2P

3.2　相关定义

定义 1　用户隐私需求 P 表示用户在请求 LBS 服务时希望得到的隐私保护力度，可表示为四元组：

$$P=\{k,A_{\min},A_{\max},t_c\}$$

其中，k 表示用户希望得到的匿名度，即匿名区域中包括的最少用户数。$A_{\min}$ 和 $A_{\max}$ 为用户希望达到的匿名区域最小和最大面积，其与服务质量成反比。匿名区域是 LBS 用来对用户请求进行查询的依据，匿名区域过大会导致查询不准确，且如果用户密度较小、匿名区域过大将导致无法实现 k 匿名。t_c 表示缓存失效的时间，其与匿名区的安全性成反比。缓存失效的时间越长，则匿名区域内的点失效的可能性越大，攻击者

根据背景知识推测出用户的真实位置的可能性就越大，对隐私保护将造成一定威胁。

定义 2 用户发出的查询请求 Q 表示用户向 LBS 所请求的位置服务的具体信息，可表示为六元组：

$Q=\{ID,x,y,q,P,T\}$

其中，ID 表示识别用户的唯一标识符，x,y 表示根据查询用户所选锚点的二维坐标值，q 表示查询用户所请求的位置查询内容，P 表示查询用户所希望达到的隐私保护力度，T 表示响应用户集合。

定义 3 协同用户在接收到广播后，相应用户所发出的位置信息表示为三元组：

$L=\{ID,d,h\}$

其中，ID 为协同用户识别的唯一标识符，d 为到查询用户所选锚点的距离，h 表示接收到查询用户的广播跳数。

4 算法描述

在本文设计的算法结构中，首先将用户所在的二维平面分割成大小一致的正方形网格。用户根据自身位置来选取锚点，发送包含用户 ID、锚点位置、查询请求以及匿名用户集合的广播信息。周围的协同用户响应该请求，协同用户将其到锚点的距离发送给查询用户。在一次广播后，如果协同用户的数目大于或等于 $k-1$，则停止广播；协同用户的数目没有达到 $k-1$，则继续广播，直到协同用户的数目达到 $k-1$，并将所有响应的用户增加到匿名用户集合 T 中。

如果 T 中的用户数目超过 $k-1$，则保留距离最近的 $k-1$ 个。计算这 $k-1$ 个点到锚点的距离，选出最大的距离 r，构成以锚点为圆心 r 为半径的圆形匿名区域 S。将 S 和用户需求匿名面积进行比较，如果 $A_{\min}\leqslant S\leqslant A_{\max}$，返回 S 匿名算法构建成功，否则匿名算法构建失败。

构建好匿名区域后从 T 中随机挑选一个代理用户，由代理用户发送包括查询发起者在内的 k 个用户构成的匿名区域给 LBS，LBS 根据查询请求和匿名请求发送兴趣点集合，查询用户根据 LBS 返回的结果筛选出最终的查询结果。接下来主要从锚点选取和匿名区域构建两个环节进行描述。

4.1 锚点选取

首先服务器根据经纬度将用户所在的二维平面分割成大小一致的正方形网格，当查询用户 r_q 发出一个基于位置的查询请求后，查询用户首先获取自己的网格坐标（见算法 1 第 1 行），根据所在的网格中心来选取锚点，锚点的选取如图 2 所示。

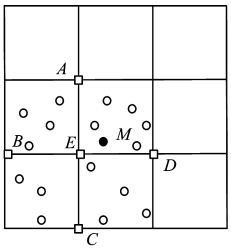

图 2 用户选取锚点的过程

Fig. 2 Process of user selecting anchor

查询用户 r_q 根据自身的网格坐标确定距离最近的网格顶点坐标，如图 2 中顶点 E（见算法 1 第 2 行）。对顶点 E 的坐标沿水平及垂直方向各进行一个网格宽度的平移，得到 4 个新的顶点坐标，如图 2 中顶点 A,B,C,D（见算法 1 第 3 行），最后查询用户从顶点集合 $\{A,B,C,D,E\}$ 中随机选取一个作为锚点（见算法 1 第 4－5 行）。

算法 1 P2P-D 算法（锚点选取）

//令查询用户为 r_q，锚点为 M，网格宽度 w_0

1. 用户所在网格坐标 $r_q.cell.x\leftarrow\left[\frac{r_q.x}{w_0}\right]\times w_0$，$r_q.cell.y\leftarrow\left[\frac{r_q.y}{w_0}\right]\times w_0$
2. 根据欧氏距离公式 $\sqrt{(x_0-x_1)^2+(y_0-y_1)^2}$ 计算两点的距离，选取距离用户最近的网格顶点 E
3. 得到候选锚点位置 $A\leftarrow(E.x,E.y+w_0)$，$B\rightarrow(E.x-w_0,E.y)$，$C\rightarrow(E.x,E.y-w_0)$，$D\rightarrow(E.x+w_0,E.y)$
4. $M\leftarrow random\{A,B,C,D,E\}$
5. return M to r_q

4.2 构建匿名区域

用户在获取锚点位置后首先检查自身的缓存记录 H，查看其是否在 t_c 时间内进行过位置服务请求，如果缓存中用户集合 T 满足此次匿名请求的需求，则直接将缓存记录作为匿名区域发送给 LBS（算法 2 第 1－第 4 行）；否则将用户广播跳数设置为 1，用户集合 T 设置为空集（算法 2 第 5－第 7 行）。在满足用户集合 T 数目小于或等于 $k-1$ 以及最近一次广播响应的用户与前一次不同的情况下，发送广播消息，其中包括锚点的坐标、用户 ID、广播跳数以及用户集合 T（算法 2 第 8－第 9 行）。响应用户 p 查看广播信息，如果此时的广播跳数为 1，则将自身到锚点的距离以广播形式发送给查询用户 r_q（算法 2 第 10－第 14 行）；否则用户集合 T 中的用户发送广播消息，将各响应节点加入到用户集合 T 中，并且将此次获取的邻近节点的信息缓存下来（算法 2 第 15－第 20 行），以便 r_q 下一次发送位置请求时快速得到结果。广播结束后查看集合 T 中的用户数目，如果大于或等于 $k-1$ 则选取其中距离锚点最近的 $k-1$ 个用户和查询用户 r_q 放入集合 S 中（算法 2 第 21－第 22 行）；否则提示用户降低匿名度 k 的大小（算法 2 第 23－第 24 行）。最后形成以锚点为圆心、以 T 中到锚点最远的距离为半径的圆形匿名区域（算法 2 第 25－第 27 行）。计算该区域的面积，如果在用户匿名需求要求内，则将最终结果返回给查询用户，否则提示用户减小最大匿名面积或增大最小匿名面积（算法 2 第 28－第 32 行）。

算法 2 P2P-D 算法（匿名区构建）

//令查询用户为 r_q，响应用户为 p，锚点为 M

1. 读取 r_q 本地缓存内容记作 H
2. if $|H.T|\geqslant k-1$ and $t_{now}-|H.t|\leqslant t_c$
3. 返回缓存结果
4. end if
5. 已发现的节点集合 $T\leftarrow\{\varnothing\}$
6. $k\leftarrow|T|$
7. $h\leftarrow1$
8. while $|T|<k-1$ and $T_{now}\neq T_{last}$

```
9.    BroadCast PEER_DISCOVER{ID,h,M.x,M.y,T}
10.   if h=1
11.   if p 接收到相同的广播消息
12.      忽略该消息
13.   else
14.      Reply PEER_DISCOVER{ID,distance,T} to r_q
15. else
16.   for all T_i in T
17.      BroadCast PEER_DISCOVER{ID,h,M.x,M.y,T}
18.   T←T∪{响应用户 p}
19.   h←h+1
20. end while
21. if |T|≥k−1
22.   S←{r_q}∪{T 中距离 r_q 最近的 k−1 用户}
23. else
24.   匿名失败，提示用户降低匿名度 k
25. for all T_i in T
26. R←max(distance(M,T_i))
27. end for
28. acreage←π×R^2
29. if acreage∈(Area_min,Area_max)
30.   return S to r_q
31. else
32.   匿名失败，提示用户减小 Area_max或者调大 Area_min
```

5　实验与结果分析

5.1　实验环境

算法通过 Java 实现，在 Intel(R)Core(TM)i5-3210M 处理器，8GB 内存的 Windows10 平台上运行，移动终端的数据由 Thomas Brinkhoff 路网数据生成器将城市 Oldenburg 的交通路网中的一块典型的 10000 m * 10000 m 区域作为输入。

实验分别将 P2P-D 与已有的 P2PSC[9] 以及 SCABGE[14] 算法进行比较和分析。实验中模拟一个半双工的网络通信信道用于终端节点间的数据传输，带宽为 1 Mbps，位置查询发起间隔服从期望值为 60 s、标准差为 15 的正态分布，查询发起节点随机选择。如果没有具体说明，实验中使用的默认参数如表 1 所列。

表 1　实验默认参数

Table 1　Experimental parameters

参数名称	默认值
节点数	2 000
网格宽度/m	200
节点信号范围/m	200
匿名区域最大值 A_{max}/m^2	40 000
匿名区域最小值 A_{min}/m^2	4 000 000
缓存记录失效时间 t_c/s	90

5.2　结果分析

实验在不同的用户匿名需求 k 下，对 P2P-D，P2PSC[11]，SCABGE[16] 在平均匿名时间、平均匿名区域面积、平均消息数这几个方面进行比较，并针对时间复杂度与文献[18]进行了比较说明。

从图 3 中可以看出，随着用户 k 匿名需求的增加，P2PSC，SCABGE，P2P-D 这 3 个算法的平均匿名时间也随之增加。这是由于当用户匿名需求 k 增加时，构建匿名集合的协作用户数目随之增加，广播次数将有所增加，因而其平均匿名时间增加。且由图 3 可知，P2PSC 算法的平均匿名时间最少，P2P-D 算法紧随其后，SCABGE 算法的平均匿名时间最多。这是因为在 P2PSC 和 P2P-D 算法中都加入了缓存，用户会首先检查历史记录，当没有相应历史记录时才会进行广播。而 SCABGE 算法未加入缓存技术，并且由于其广播面积较大，通信范围较大，因而其匿名时间也相应变大。由于 P2P-D 算法加入了锚点选取过程，所以其匿名时间较 P2PSC 大，但从图中可以看出，两者平均匿名时间相差较小，P2P-D 算法虽然消耗了一小部分的时间成本，但其对于位置隐私的保护力度较大。

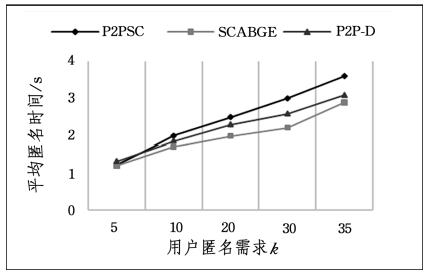

图 3　平均匿名时间

Fig. 3　Average anonymizing time

从图 4 中可以看出，随着用户 k 匿名需求的增加，P2PSC，SCABGE，P2P-D 这 3 个算法的平均消息数也随之增加。与平均匿名时间相似，当用户匿名需求 k 增加时，由于广播次数增加，导致平均消息数增加。且从图中可以看出，SCABGE 算法的平均消息数最多。这是因为在 P2PSC 和 P2P-D 算法中都加入了缓存，用户会首先检查历史记录，当没有相应历史记录时才会进行广播。而 SCABGE 算法未加入缓存技术，并且由于其广播面积较大，通信范围较大，用户数目较多，因而其平均消息数也相应变大。而 P2PSC 和 P2P-D 算法则是根据用户集合中的用户数目逐跳广播以满足用户匿名需求，因此平均消息数较 SCABGE 小。

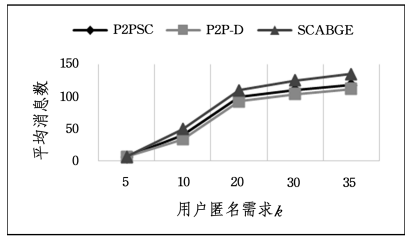

图 4　平均消息数

Fig. 4　Average number of message

从图 5 中可以看出，随着用户 k 匿名需求的增加，P2PSC，SCABGE，P2P-D 这 3 个算法的平均匿名面积也随之增加。且从图中可以看出，P2P-D 算法的平均匿名面积最小，SCABGE 算法形成的面积最大。从各自构建匿名区域的方

式可以看出，SCABGE 算法是基于网格扩增的，并且其扩增的速度较快，所以构建的匿名区域面积较大。而 P2PSC 和 P2P-D 算法都是基于用户的位置以及协作用户的分布情况，由用户向外逐渐扩增最终形成匿名面积。由于 P2PSC 算法在构建匿名区域时需要进行匿名中心平移，并在新匿名中心的基础上扩增形成新的匿名区域，因此 P2P-D 算法所形成的匿名区域面积最小。

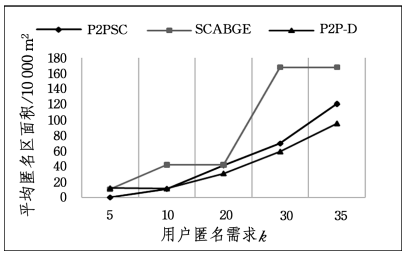

图 5 平均匿名面积

Fig. 5 Average anonymizing area

文献[18]主要解决了构建匿名组时存在的共谋攻击问题，本文在时间复杂度较低的情况下，同样可以避免共谋攻击。文献[18]主要通过加入高斯噪声对每个位置进行扰动，并且以质心位置来代替用户真实位置。而本文通过锚点同样可以有效规避共谋攻击的问题，且只需求取锚点位置而无需进行其他计算。文献[18]中还需对用户的位置进行 Paillier 门限加密、解密，从而需要对位置信息进行大量的取模计算，时间杂度较高。经过分析，本文可以在时间复杂度较低的情况下有效规避共谋攻击。

5.3 安全性分析

5.3.1 抵御共谋攻击

共谋攻击即为假设匿名组中出现攻击者或者 LBS 和匿名组中同时存在攻击者的情况，因为匿名组内的用户也是半可信的，群组里的用户在协作别人完成匿名请求的同时也想要获取别人的位置信息。而 P2PSC 构建的为矩形匿名区域，因而需要查询用户知道协作用户的精确坐标才能构建匿名区域。但是查询用户本身很有可能就是攻击者，只要攻击者假装成查询用户发送广播，那么就能轻易获取协同用户的身份信息以及真实位置，显然整个位置匿名就失败了。同时，SCABGE 是在 P2PSC 的基础上为了防御匿名中心攻击而采取网格扩增的方式来尽量规避查询用户就在匿名中心的风险，同样地，该算法也不能抵御共谋攻击。P2P-D 算法则是在协作用户响应查询用户时，不再发送自己的具体位置，而是将到锚点的距离作为自身的位置信息发送给查询用户。这样即便查询用户是攻击者也无法知道协作用户的具体位置，从而有效地解决了共谋攻击的问题。并且由于查询用户本身发送的是锚点位置，所以即便协作用户中有攻击者也无法获取查询用户的精确位置。

5.3.2 抵御匿名中心攻击

根据文献[16]可知，在描述抗匿名中心攻击时，我们首先将匿名区域从里到外划分为 5 个面积相等的区域，如图 6、图 7 所示，统计查询节点在各区域中出现的概率，从而分析算法在抗匿名中心攻击的能力。

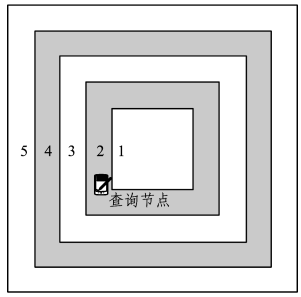

图 6 P2PSC 匿名区划分

Fig. 6 Anonymity partitioning of P2PSC

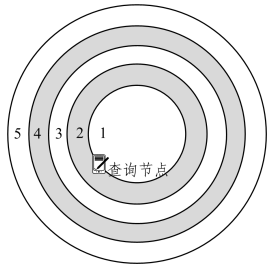

图 7 P2P-D 匿名区划分

Fig. 7 Anonymity partitioning of P2P-D

从算法原理角度分析可知，P2PSC 根据查询用户的精确位置进行广播，所以极易造成绝大多数协作用户出现在查询用户的周围的情况。本文提出的 P2P-D 算法由于锚点选取的随机性，所以协同用户出现在各个区域的概率相同。从图 8 的实验结果可以看出，P2P-D 算法中查询节点出现在靠近匿名中心各个区域的概率接近，而 P2PSC 算法中查询节点则有较大的可能出现在距离匿名中心 1/5 处，由此可见 P2P-D 不仅可以有效的抵御共谋攻击，还可以很好地解决匿名中心攻击的问题。

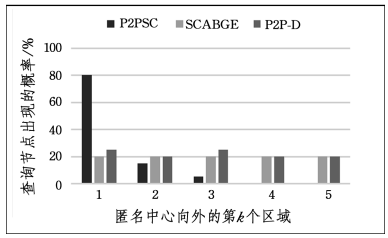

图 8 查询节点在匿名区中的分布

Fig. 8 Distribution of query nodes in anonymous area

结束语 原有的 P2P 模式绝大多数是基于用户精确位置来实现的，本文描述了其存在的问题，即无法抵御共谋攻击并且存在匿名中心攻击问题。为了改善这些问题，本文提出了一种基于距离的改进方法，不仅能规避匿名中心攻击，而且能有效规避共谋攻击的问题。大量的实验证明，P2P-D 算法具有很好的效果，在确保满足用户 k 匿名需求的同时也可以保证用户的位置安全，是对 P2P 方法的一次良好的改进，具有很好的现实意义。

参 考 文 献

[1] GRUTESER M, GRUNWALD D. Anonymous usage of location-based services through spatial and temporal cloaking[C]// 1st ACM International Conference on Mobile Systems, Applica-

tions，and Services. SanFrancisco，United States，2003：31-42.

[2] NIU B，et al. Achieving k-anonymity in privacy-aware location-based services[C]// 33th IEEE International Conference on Computer Communications. Toronto，Canada，2014：754-762.

[3] LIU H，LI X H. Privacy enhancing method for dummy-based privacy protection with continuous location-based service queries[J]. Journal on Communications，2016，37(7)：140-150. (in Chinese)
刘海，李兴华. 连续服务请求下基于假位置的用户隐私增强方法[J]. 通信学报，2016，37(7)：140-150.

[4] PEI Z X，LI X H，LIU H. Anonymizing region construction scheme based on query range in location-based service privacy protection[J]. Journal on Communications，2017，38(9)：125-132. (in Chinese)
裴卓雄，李兴华，刘海. 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(9)：125-132.

[5] YIU M L，JENSEN C S，MØLLER J，et al. Design and analysis of aranking approach to private location-based services[J]. ACM Transactionson Database Systems，2011，36(2)：1-42.

[6] HUANG Y，HUO Z，MENG X F. CoPrivacy：A Collaborative Location Privacy-Preserving Method without Cloaking Region [J]. Chinese Journal of Computers，2011，34(10)：1976-1985. (in Chinese)
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.

[7] PERAZZO P. A uniformity-based approach to location privacy [J]. Computer Communications，2015，64(1)：21-32.

[8] ANDRES M E，BORDENABE N E，et al. Geo-indistinguishability：differential privacy for location-based systems[C]// 20th ACM Conference on Computer and Communications Security (CCS'13). Berlin，Germany，2013：901-914.

[9] ZHANG L，MA C G. Correlation probability indistinguishable location privacy protection algorithm[J]. Journal on Communications，2017，38(8)：37-49. (in Chinese)
张磊，马春光. 关联概率不可区分的位置隐私保护方法[J]. 通信学报，2017，38(8)：37-49.

[10] CHOW C Y，MOKBEL M F，LIU X. A peer-to-peer spatial cloaking algorithm for anonymous location-based services[C]// 14th ACM International Symposium on Advances in Geographic information Systems(ACM-GIS'06). Arlington，USA，2006：171-178.

[11] CHOW C Y，MOKBEL M F，LIU X. Spatial cloaking for anonymous location-based services in mobile peer-to-peer environments[J]. GeoInformatica，2011，15(2)：351-380.

[12] ASHOUR-TALOUKIM：a cryptographic approach for group location privacy[J]. Computer Communications，2012，35(12)：1527-1533.

[13] MANWEILER J，SCUDELLARI R，COX L P. SMILE：encounter-based trust for mobile social services[C]// 16th ACM Conference on Computer and Communications Security(CCS'09). Chicago，United States，2009：246-255.

[14] CRUTESER M，GRUNWALD D. Anonymous usage of location-based services through spatial and temporal cloaking[C]// Proceedings of the 1st International Conference on Mobile System，Applications and Services，ACM，2003：31-42.

[15] CHOW C Y，MOKBEL M F. Casper*：query processing for location services without compromising privacy[J]. ACM Transactionson Database Systems，2009，34(4)：1-48.

[16] WANG J H，CHENG J J. Spatial Cloaking Algorithm Based on Grid Expansion in P2P Mode[J]. Computer Science，2014，4(41)：90-94. (in Chinese)
王嘉慧，程久军. P2P 模式下基于网格扩增的位置匿名算法[J]. 计算机科学，2014，4(41)：90-94.

[17] 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.

[18] GAO S，MA J F. Towards cooperation location privacy-preservinggroup nearest neighbor queries in LBS[J]. Journal on Communications，2015，36(3)：146-154. (in Chinese)
高胜，马建峰. LBS 中面向协同位置隐私保护的群组最近邻查询[J]. 通信学报，2015，36(3)：146-154.