P2P模式下基于网格扩增的位置匿名算法

王嘉慧[1] 程久军[2]
(同济大学电子与信息工程学院 上海 201804)[1]
(同济大学嵌入式系统与服务计算教育部重点实验室 上海 201804)[2]

摘 要 位置k-匿名方法是当前基于位置的服务中隐私保护领域的研究热点。典型的位置匿名算法多采用单一可信的中心匿名服务器对用户位置进行匿名,但中心服务器容易成为性能瓶颈和集中攻击点,而已有P2P模式下的位置匿名算法在安全性上较弱。针对上述问题,提出了一种P2P模式下基于网格扩增的位置匿名算法,其利用网格划分平面,通过不断翻倍扩增网格宽度寻找满足用户隐私需求的匿名区,最终完成对用户位置的匿名。同时算法在运行中能够与邻近节点分享计算所得中间结果,并对其进行缓存。实验表明,与已有算法相比,本算法可显著降低网络带宽的消耗,减少位置匿名耗时,同时能够避免匿名区中心攻击,且抗查询采样攻击的能力得到较大提升。

关键词 基于位置的服务,位置隐私,k-匿名,P2P
中图法分类号 TP309 **文献标识码** A

Spatial Cloaking Algorithm Based on Grid Expansion in P2P Mode

WANG Jia-hui[1] CHENG Jiu-jun[2]
(Department of Computer Science and Technology, Tongji University, Shanghai 201804, China)[1]
(Key Laboratory of Embedded System and Service Computing of Ministry of Education, Tongji University, Shanghai 201804, China)[2]

Abstract Location k-anonymity becomes a research focus in the privacy-preserving field of location-based service recently. Typical spatial cloaking algorithms require a centralized trusted anonymity server which could be the system bottleneck and single point of attacks, while the existing spatial cloaking algorithms in P2P (Peer to Peer) mode suffer from several attack models. A spatial cloaking algorithm based on grid expansion in P2P mode was proposed to solve this problem. It divides the space into grids and computes cloaking region by keeping trying to double the grid's width until user's privacy requirement is satisfied. Meanwhile the intermediate result is shared and cached with other peers during the running process of the algorithm. The experimental results show that the proposed algorithm reduces the consumption of network bandwidth and time cost of spatial cloaking. Moreover, it is free from center-of-cloak attack and more resistant to sample query attack in comparison with the existing algorithms.

Keywords Location-based service, Location privacy, k-Anonymity, P2P

1 引言

随着无线通信技术以及GPS等定位技术的不断成熟,基于位置的服务(Location-based Services,LBS)在交通、医疗救护、军事等各领域都得到了广泛的应用。而近几年来日益普及的智能手机也带动了大量LBS应用的出现,借助手机的定位功能,用户可以随时随地从LBS服务商处获取当前周边的各类信息。然而由于需要用户提交自己的位置坐标,当LBS服务商不可信或者发生用户数据泄漏时,用户的隐私安全将受到极大威胁。

针对这一问题,国内外已有不少研究人员提出了许多相关的方案和算法。文献[1]提出了利用虚假位置进行位置混淆的方法,用户在发出查询请求时,同时提交多个位置信息,LBS服务器则逐个返回各位置下的结果,最后用户选择自身位置对应的结果即可。文献[2]中所述的SpaceTwist方法,则利用在用户周围随机选取的一个点作为位置参数发起查询,根据返回结果与实际位置的距离,不断向LBS服务器发起增量查询,直至最后得到满意的结果。文献[3]将用户的位置用二维坐标之和以及一个泛化区间来表示,以此实现对查询发起用户位置隐私的保护。由于仅仅只是降低位置的精确度,上述3种方法仍无法避免攻击者对查询请求与查询发起人进行关联攻击。

Gruteser M等人受数据库中k匿名化方法的启发提出了位置匿名的方法来保护用户位置隐私并给出了对应的AI-CA算法[4]。不同于一般方式下用户提交位置坐标发起查询,位置匿名方法将一个平面矩形空间(即匿名区)提交给

到稿日期:2013-05-26 返修日期:2013-10-16 本文受国家科技支撑计划项目(2012BAH15F03),上海市自然科学基金项目(13ZR1443100),科技部国际合作项目(2013DFM10100),上海市科委计划项目(11JC1412800)资助。
王嘉慧(1989—),男,硕士生,主要研究方向为移动计算、信息安全等,E-mail:1131832@tongji.edu.cn;**程久军** 男,副教授,主要研究方向为移动计算、车联网等。

LBS服务器，并且确保该匿名区内至少包含 k 个用户，这样攻击者仅能以 $1/k$ 的概率将查询发起人关联到一个具体用户。鉴于该方法具有较高的安全性，当前热门的位置隐私保护技术研究均以此为基础展开。如文献[5]提出的 Capser * 系统采用四叉树结构并对区块建立索引来计算匿名区。文献[8]提出的 CliqueCloak 算法则利用图论中极大团的性质来求解匿名区，但是该方法计算量巨大，仅适用于匿名度 k 较小的情况。Panos Kalnis 等人在文献[4]中位置匿名定义的基础上，提出了位置匿名的互易性[7]，即对于一个匿名区内的所有用户，他们应当共享同一匿名区，同时作者还提出了满足该性质的 hilbertCloak 算法，该算法利用 hilbert 曲线将二维平面上的位置坐标映射到一个一维数组上，以每 k 个为一组进行划分求得匿名区。文献[6]则在研究已有位置匿名算法的基础上，提出了查询采样攻击(Sample Query Attack)，并指出只有满足互易性的 CliqueCloak 算法和 hilbertCloak 算法才能完全避免该种类型的攻击。

目前多数位置匿名方法均采用中心式结构，即在用户与LBS服务器之间建立一个可信的匿名器，通过该匿名器完成对用户位置的匿名工作。然而，由于匿名服务器需要进行大量的计算，容易使其成为系统性能瓶颈。此外由于匿名服务器掌握着所有用户的位置和查询信息，一旦其被攻击，将导致严重的后果。鉴于中心式结构的诸多不足，越来越多的研究采用无中心服务器结构的隐私保护方法。文献[10]所提出的 CoPrivacy 方法通过用户协作并结合已有的 SpaceTwist 方法[2]，在不使用匿名区的情况下达到了 k 匿名的效果。文献[11]则通过在用户查询信息转发的过程中构造一条匿名链来混淆身份信息与位置信息的对应关系，从而保护用户隐私。文献[9]提出了 P2PSC 算法，即通过 P2P 多跳通信计算匿名区，然而该方法往往会导致查询请求者最终位于匿名区的中心处，从而降低实际隐私保护的效果。文献[12]在 P2PSC 算法的基础上，通过对计算得到的匿名区进行随机扩大来规避匿名区中心攻击(center-of-cloak attack)[15]，但该方法仍无法从根本上杜绝查询发起者在匿名区内分布不随机的问题，且抗查询采样攻击的能力较弱。本文针对 P2P 模式下已有位置匿名算法在安全性上的不足，设计了一种基于网格扩增的位置匿名算法(Spatial Cloaking Algorithm Based on Grid Expansion，SCABGE)，其通过对平面空间进行网格划分并不断翻倍扩增网格的宽度来寻找符合条件的匿名区。该算法能够有效杜绝匿名区中心攻击并大大提高抗查询采样攻击的能力，借助算法中的数据缓存机制，相比 P2PSC 算法，位置匿名耗时有所降低，网络带宽消耗显著下降。

2 P2P 模式下基于网格扩增的位置匿名算法

2.1 系统结构

图 1 描述了 P2P 模式下位置隐私保护系统的结构。系统由两部分组成：移动智能终端及 LBS 服务器。用户使用移动智能终端通过与周围其他终端的协作完成匿名区的计算，然后在近邻终端节点中随机选择一节点作为代理节点，借助该代理节点经由基站使用 2G 或 3G 网络向 LBS 服务器发出位置相关的查询请求。LBS 服务器则根据用户发送的匿名区信息以及查询内容，返回满足要求的查询结果集，最后查询节点根据自身的精确位置从结果集中选取最优的部分返回给用户。

本文提出的算法用于匿名区的计算，应用于移动智能终端部分，要求其同时支持 P2P 通信和无线互联网通信两种数据传输方式。其中 P2P 方式使得查询请求终端可以通过单跳或多跳的形式与周围的其他智能终端进行自组织通信，无线互联网方式则用于向 LBS 服务器发出查询请求并取得查询结果。此外，移动智能终端还需带有无线定位功能，用以确定其精确位置。目前市场上的许多移动终端都已具备这种能力，如同时配备有 802.11b/g 模块和 GPS 定位模块的智能手机。

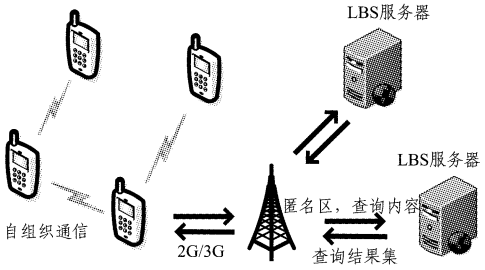


图 1 P2P 模式下位置隐私保护系统的结构

2.2 相关定义

定义 1 用户隐私需求 P 表示用户在请求 LBS 服务时希望得到的位置隐私保护的力度，可表示为 4 元组：

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

其中，k 表示匿名度，即计算所得匿名区中至少包含 k 个用户。显然，k 值越大，查询发起者被攻击者识别的概率越低，隐私保护的力度也就越强。

$A_{\min}$ 表示匿名区的最小面积。当用户处于人群密集处时，即使将匿名度设置得较高，也会得到一个面积较小的匿名区，从而降低其安全性[13]，该参数确保了计算所得的匿名区面积不会小于用户指定的值。

$A_{\max}$ 表示匿名区的最大面积。该参数用于确保在用户分布稀疏的情况下，匿名区的面积不会过大，从而导致服务质量下降。

t_c 表示缓存记录失效时间。该参数越大则越能充分利用已有的缓存数据从而加速位置匿名算法的执行时间。然而由于终端用户本身具有移动性，较大的失效时间意味着实际的匿名度可能无法得到满足，导致安全性下降。

定义 2 用户查询请求 Q 表示用户发起的查询请求，可表示为 5 元组：

$$Q=\{x,y,q,p,n\},$$

其中，x,y 表示用户位置的二维坐标值；q 表示用户向 LBS 服务器发起的查询内容；p 表示定义 1 所描述的用户隐私需求；n 表示查询结果的最大个数。

2.3 算法描述

在本文所设计的位置匿名算法中，用户所在的二维平面将被假想分割成大小一致的方形网格，初始网格宽度为 w_0，查询请求节点不断尝试翻倍扩大网格的宽度并重新分割平面，直到其所在的网格包含至少 k 个节点或网格面积超过设定的 $A_{\max}$ 值(如图 2 所示)。当最后用户所在网格中的节点数小于 k，则说明位置匿名失败，否则该网格即为待求的匿名区，随后通过选择一邻近代理节点向 LBS 服务器发起查询并根据自身坐标对结果集进行筛选得到最终的查询结果。此

外，在位置匿名算法中查询请求节点在广播匿名请求消息的同时将已得到的结果也作为参数进行广播，接收到的节点将该结果缓存至本地，以便下次自身需要位置匿名时可快速求得匿名区。整个位置匿名算法包括匿名请求发起端、匿名请求响应端及查询结果处理3部分。

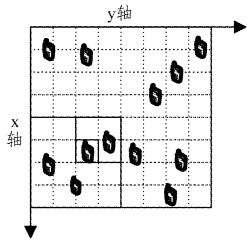


图2　网格扩增的过程

2.3.1　匿名请求发起端

查询用户 r_q 发出一个基于位置的查询请求后，位置匿名算法开始执行。首先设置广播跳数 h 为1，根据用户隐私需求中的 A_{min} 值和初始网格宽度 w_0，将当前网格宽度 w 设置为 w_0 乘以一个2的幂数，使得网格的面积在不小于 A_{min} 前提下最小。此时，r_q 所在网格左上角的 x，y 坐标可由用户当前位置的坐标除以网格宽度 w 取整再乘以 w 得到，由于该网格内的节点可能在不久前进行过位置匿名，因此先检查缓存记录 H 中该网格内的已发现节点数是否满足匿名度 k 且该条记录的时间是否在用户设定的失效时间之内，如上述两个条件均满足，则直接将该网格作为匿名区返回，否则令已发现节点集合 T 为单个元素 r_q（算法1第2－8行）。随后生成广播标识 b，该标识可根据节点的唯一性来标识与当前时间计算所得，广播 PEER_DISCOVER 节点发现消息，消息内容为参数 b、h、x、y、w 和 T（算法1第10－11行），其中将已发现节点集合 T 作为广播参数可使邻近节点得到该数据并缓存，以便未来自身需要位置匿名时可快速从缓存中得到结果。接收到各节点的响应消息后，r_q 将各响应节点返回的节点集合取并集，得到本次广播所发现的节点集合 T'（算法1第12－15行）。然后比较本次发现的节点数是否满足匿名度 k 的要求，如果 $|T|<r_q.p.k$，说明目前发现的节点数还不够多，进一步判断本次得到的节点集合 T' 与上次的结果 T 是否相同，如不同，则说明用户当前所在网格内还有潜在的节点未被发现，继续增加广播跳数 h 以发现更多的邻居节点，否则说明目前设定的网格宽度过小，需将网格宽度翻倍扩大，同时重新计算 r_q 所在网格左上角的 x，y 坐标值。此时由于当前网格已发生变化，需重新检查缓存记录中该网格的结果是否可以满足用户设定的隐私条件，如满足则返回扩大后的当前网格作为匿名区，否则需要继续广播，并用 T' 更新已发现节点集合 T（算法1第16－26行）。当 T 中的节点个数满足匿名度 k 或者网格面积超过 A_{max} 时，不再进行广播。最后比较 $|T|$ 和 $r_q.p.k$，如果 $|T|\geq r_q.p.k$，则说明位置匿名成功，匿名区即为查询用户当前所在的网格，同时缓存该结果，否则说明匿名失败，提示用户重新设置隐私需求参数（算法1第28－33行）。

算法1　SCABGE 算法：匿名请求发起端

1. //查询请求节点为 r_q
2. 设置广播跳数 h←1
3. 网格宽度 $w\leftarrow ceilingPowerOfTwo(\frac{\sqrt{r_q.p.A_{min}}}{w_0})\times w_0$
4. 节点所在网格的坐标 $x\leftarrow\lfloor\frac{r_q.x}{w}\rfloor\times w$，$y\leftarrow\lfloor\frac{r_q.y}{w}\rfloor\times w$
5. if $|H[x,y,w].T|>=r_q.p.k$ and $t_{now}-|H[x,y,w].t|<=r_q.t_c$ then
6. 返回匿名区（x，y，x+w，y+w）
7. end if
8. 已发现的节点集合 $T\leftarrow\{r_q\}$
9. while $|T|<r_q.p.k$ and $w<\sqrt{r_q.p.A_{max}}$
10. 生成广播标识 b
11. 广播节点发现消息 PEER_DISCOVER(b，h，x，y，w，T)
12. $T'\leftarrow\{r_q\}$，各响应节点返回的结果为 T_i
13. for each T_i do
14. $T'\leftarrow T'\cup T_i$
15. end for
16. if $|T'|<r_q.p.k$ then
17. if $T=T'$ then
18. $w\leftarrow 2\times w$，$x\leftarrow\lfloor\frac{r_q.x}{w}\rfloor\times w$，$y\leftarrow\lfloor\frac{r_q.y}{w}\rfloor\times w$
19. if $|H[x,y,w].T|>=r_q.p.k$ and $t_{now}-|H[x,y,w].t|<=r_q.t_c$ then
20. 返回匿名区（x，y，x+w，y+w）
21. end if
22. else then
23. h←h+1
24. end if
25. end if
26. $T\leftarrow T'$
27. end while
28. if $|T|<r_q.p.k$ then
29. 匿名失败，提示用户降低匿名度 k 或调大 A_{max}
30. end if
31. $H[x,y,w].t\leftarrow t_{now}$
32. $H[x,y,w].T\leftarrow T$
33. 返回匿名区(x，y，x+w，y+w)

2.3.2　匿名请求响应端

邻居节点 r_0 在收到查询发起节点或转发节点 r 广播的节点发现消息 m 后的处理流程如算法2所示。当 r_0 发现消息 m 重复或节点自身不在消息指示的网格内时，不对该消息作响应，直接返回（算法2第2－4行）。否则首先将消息 m 中的已发现节点集合 T 放入缓存中（算法第5－6行），继续检查消息 m 中的广播跳数 h，如果 $h=1$，则将自身加入到已发现节点集合 T 中，并将 T 返回给节点 r，否则说明接收到的节点发现消息需要进一步广播，将 h 减1后继续广播节点发现消息，消息内容为参数 $m.b$，h，$m.x$，$m.y$，$m.w$ 和 $m.T$，在接收到各节点的响应消息后，r_0 将各响应节点返回的节点集合取并集并将自身加入其中，得到已发现节点集合 T，将该结果返回给节点 r（算法2第7－18行）。

算法2　SCABGE 算法：匿名请求响应端

1. //响应节点为 r_0，查询发起节点或消息转发节点为 r，节点发现消息为 m
2. if 消息 m 重复 or r_0 不在(m.x，m.y，m.x+m.w，m.y+m.w)范围内 then
3. return
4. end if

5. H[m. x,m. y,m. w]. t←t_{now}

6. H[m. x,m. y,m. w]. T←m. T

7. if m. h=1then

8. T←{r_0},向节点 r 返回结果 T

9. else

10. h←m. h−1

11. 广播节点发现消息 PEER_DISCOVER (m. b,h,m. x,m. y,m. w,m. T)

12. T←∅,各响应节点返回的结果为 T_i

13. for each T_i do

14. T←T∪T_i

15. end for

16. T←T∪{r_0}

17. 向节点 r 返回结果 T

18. end if

2.3.3 查询结果处理

算法 3 所示为查询结果处理流程。查询请求节点 r_q 从已发现节点集合 T 中随机选择一代理节点,由该节点向 LBS 服务器发出查询请求,请求内容包括匿名区信息及 r_q 的查询内容,代理节点将 LBS 服务器返回的结果集回送给查询请求节点 r_q。此时需对返回的结果集 A 进行筛选处理,建立一个以距离查询请求节点远近作为比较的大顶堆 Q_{max},将得到的各结果插入其中,当 Q_{max} 中元素超过用户设定的结果个数最大值 n 时,弹出堆顶元素即最远的那条结果。最后 Q_{max} 中的 n 个元素即为距离查询请求节点最近的 n 条查询结果。

算法 3 SCABGE 算法:查询结果处理

1. //查询请求节点为 r_q

2. r_q 从已发现节点集合 T 中随机选择一代理节点 r_a

3. r_a 向 LBS 服务器发送查询请求(x,y,x+w,y+w,r_q. q),并将得到的结果集 A 返回给 r_q

4. 建立以距离为比较的大顶堆 Q_{max}

5. for each $a_i \in A$ do

6. a_i. dist←$\sqrt{(a_i.x-r_q.x)^2+(a_i.y-r_q.y)^2}$

7. 将 a_i 插入 Q_{max}

8. if $|Q_{max}|>r_q$. n then

9. 将 Q_{max} 的堆顶元素弹出

10. end if

11. end for

12. 将 Q_{max} 内的查询结果返回给用户

3 实验与结果分析

3.1 实验环境

算法采用 C++实现,在 Intel(R) Core(TM)2 Duo E8400 处理器、2GB 内存的 Windows 7 平台上运行。移动终端的位置模拟数据由 Thomas Brinkhoff 路网数据生成器[14]将城市 Oldenburg 的交通路网中一块典型的 1000m * 1000m 区域作为输入而生成。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 1Mbps,位置查询发起间隔服从期望值为 60 秒、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。

实验分别在算法性能和安全性两方面对本文提出的 SCABGE 算法与已有的 P2PSC 算法进行比较和分析。

表 1 实验默认参数

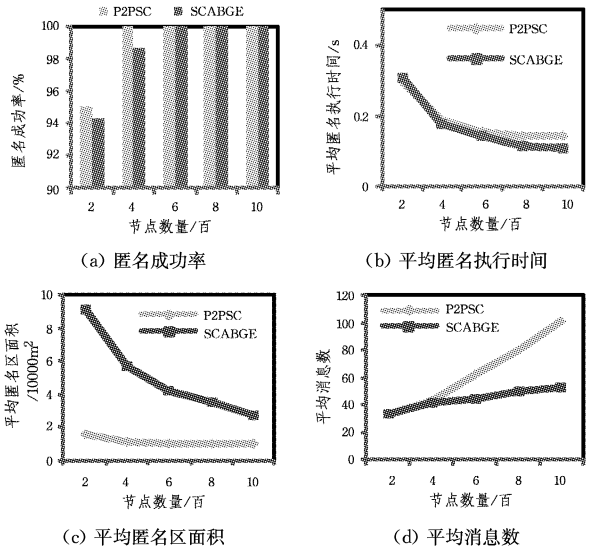
参数名称	默认值
节点信号范围	100m
匿名度 k	10
初始网格宽度 w_0	1m
匿名区最小面积 A_{min}	10000m^2
匿名区最大面积 A_{max}	1000000 m^2
缓存记录失效时间 t_c	90s

3.2 结果分析

3.2.1 算法性能

实验比较在不同节点数量下 SCABGE 算法与 P2PSC 算法在匿名成功率、平均匿名执行时间、平均匿名区面积和平均消息数上的变化情况。其中匿名成功率说明位置匿名算法对用户查询请求的响应能力,平均匿名执行时间则表明了位置匿名的延时情况,而平均匿名区面积越小则查询节点从 LBS 服务器获得的查询结果质量将越高。平均消息数则反映了位置匿名过程中对网络带宽及各节点 CPU 资源的消耗程度,其值越低,算法越好。

如图 3 所示,随着节点数量的增加,两种算法的匿名成功率均逐步提升并达到 100%,而平均匿名执行时间和平均匿名区面积则逐步下降。由于 SCABGE 算法制约了匿名区的扩大方式,使其最终所得的匿名区面积相比 P2PSC 算法偏大,从而会导致最后得到的查询结果精确度有一定降低,但随着节点数的增加,两者的差距已逐渐缩小。而在平均消息数方面,由于采用了缓存机制使得 SCABGE 算法所需的消息广播次数要少于 P2PSC 算法,同时通过直接从缓存中得到结果加快了位置匿名执行时间,使得 SCABGE 算法的平均匿名执行时间也要优于 P2PSC 算法,且随着节点数量的增加优势愈加明显。



(a) 匿名成功率 (b) 平均匿名执行时间

(c) 平均匿名区面积 (d) 平均消息数

图 3 两种算法在不同节点数下的性能变化

3.2.2 算法安全性

(1)抗匿名区中心攻击 实验中将各查询对应的匿名区由中心向外划分成 5 个面积相等的区域,如图 4 所示,统计查询节点在各区域内的出现几率,从而比较 SCABGE 算法与 P2PSC 算法抗匿名区中心攻击的能力。图 5 所示为平面节点数量为 400 时的实验结果,本文提出的 SCABGE 算法对应查询节点在各等面积区域内出现的几率基本相同,均在 20%左右,说明查询节点在所求得匿名区内的分布较随机,所以能

够完全杜绝匿名区中心攻击。而 P2PSC 算法对应的查询节点在匿名区内的出现几率则由匿名区中心处向外快速下降，在第 1 个区域即匿名区面积 1/5 的中心处，查询节点出现的几率已经大于 80%，使得攻击者很容易缩小用户可能出现的范围，导致实际匿名度无法达到用户设定的隐私需求，从而大大降低位置匿名的安全性。

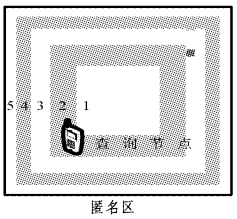


图 4　实验中对匿名区的划分

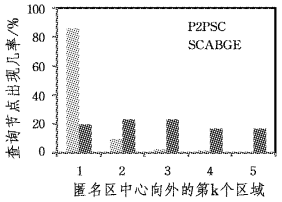


图 5　查询节点在匿名区内的分布

(2)抗查询采样攻击　由于在 P2P 模式下单个节点不能完全掌握平面上所有节点的位置信息，故无法做到完全满足互易性，即无法避免查询采样攻击。但如果对于匿名区内的大多数节点，它们共享同一个匿名区，则攻击者成功进行查询采样攻击的可能性就可大大降低。实验中通过分析匿名区的平均共享比考察算法抗查询采样攻击的能力，其计算公式为：

$$\overline{R}=\frac{\sum_{i=1}^{N}\frac{s_i}{t_i}}{N} \tag{1}$$

式中，N 表示查询总数；t_i 表示第 i 次查询对应所得匿名区内的节点个数；s_i 表示 t_i 个节点中与查询请求节点共享该匿名区的节点个数。如图 6 所示，随着节点数量的增加，SCABGE 算法的匿名区平均共享比逐步提高，当节点数量达到 400 时，其匿名区平均共享比已接近 80%，而对应的 P2PSC 算法则始终保持在较低水平，故 SCABGE 算法抗查询采样攻击的能力大大优于 P2PSC 算法。

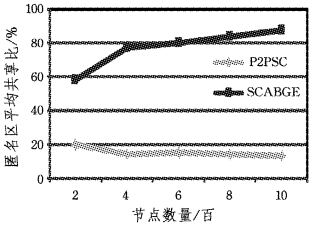


图 6　匿名区平均共享比

结束语　传统的位置隐私保护方法多采用中心式结构，需要在用户与 LBS 服务器之间建立一个可信的匿名服务器，然而大量的用户匿名请求往往使匿名服务器产生性能瓶颈且单一服务器的安全性无法保障。本文提出了一种 P2P 模式下基于网格扩增的位置匿名算法，它利用网格划分平面并通过用户间的协作完成匿名区的求解。实验显示，与已有的 P2PSC 算法对比，本文提出的算法在安全性上得到了较大提高，能够完全杜绝匿名区中心攻击，由于缓存机制的引入使得位置匿名执行时间得以降低，对网络带宽的消耗也显著减少。由于限制了匿名区的扩增方式，使得本算法在匿名成功率、匿名区面积等服务质量指标上相比已有算法有所下降，未来工作可考虑在保障安全性的前提下，进一步提高算法在服务质量上的性能。

参 考 文 献

[1] Hong J I, Landay J A. An architecture for privacy-sensitive ubiquitous computing[C]//Proceedings of the 2nd international conference on Mobile systems, applications, and services. New York: ACM, 2004: 177-189

[2] 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[C]//IEEE 24th International Conference on Data Engineering. Cancun: ICDE, 2008: 366-375

[3] 胡磊，王佳俊，倪巍伟. 一种基于坐标和的保护位置隐私近邻查询方法[J]. 计算机科学，2012，39(8)：173-177

[4] Gruteser M, Grunwald D. Anonymous Usage of Location-based Services through Spatial and Temporal Cloaking[C]//Proceedings of the 1st international conference on Mobile systems, applications and services. New York: ACM, 2003: 31-42

[5] Chow C Y, Mokbel M F, Aref W G. Casper * : Query processing for location services without compromising privacy[J]. ACM Transactions on Database Systems, 2009, 34(4): 24-48

[6] Chow C Y, Mokbel M F. Enabling private continuous queries for revealed user locations[C]//Proceedings of the 10th international conference on Advances in spatial and temporal databases. Berlin Heidelberg: Springer-Verlag, 2007: 258-273

[7] Kalnis P, Ghinita G, Mouratidis K, et al. Preventing Location-Based Identity Inference in Anonymous Spatial Queries[J]. IEEE Transactions on Knowledge and Data Engineering, 2007, 19(12): 1719-1733

[8] Gedik B, Liu L. Location Privacy in Mobile Systems: A Personalized Anonymization Model[C]//Proceedings of the 25th IEEE International Conference on Distributed Computing Systems. Washington: IEEE, 2005: 620-629

[9] Chow C Y, Mokbel M F, Liu X. A Peer-to-Peer Spatial Cloaking Algorithm for Anonymous Location-based Services[C]//Proceedings of the 14th annual ACM international symposium on Advances in geographic information systems. New York: ACM, 2006: 171-178

[10] 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

[11] 徐建，黄孝喜，郭鸣，等. 动态 P2P 网络中基于匿名链的位置隐私保护[J]. 浙江大学学报：工学版，2012，46(4)：712-718

[12] Chow C Y, Mokbel M F, Liu X. Spatial Cloaking for Anonymous Location-based Services in Mobile Peer-to-Peer Environment[J]. Geoinformatica, 2011, 15(2): 351-380

[13] Xue M, Kalnis P, Pung H K. Location Diversity: Enhanced Privacy Protection in Location Based Services[C]//Proceedings of the 4th International Symposium on Location and Context Awareness. Berlin Heidelberg: Springer-Verlag, 2009: 70-87

[14] Brinkhoff T. A framework for generating network based moving objects[J]. Geoinformatica, 2000, 6(2): 153-180

[15] Ghinita G, Kalnis P, Skiadopoulos S. MobiHide: A Mobilea Peer-to-Peer System for Anonymous Location-Based Queries[C]// Location Diversity: Enhanced Privacy Protection in Location Based Services. Berlin Heidelberg: Springer-Verlag, 2007: 221-238