位置隐私保护中基于虚拟轨迹的用户协作伪装

赵耘华 白光伟 沈 航 狄海阳 李瑞瑶
(南京工业大学计算机科学与技术系 南京 210009)

摘 要 提出位置隐私保护中基于虚拟轨迹的用户协作伪装算法(VTPP)。该算法不依赖可信第三方代理,通过用户节点的自组织通信,生成节点虚拟轨迹,进行用户的协作,形成凸多边形伪装区域来保护用户的位置隐私,从而提高了位置伪装的质量和查询结果的准确性。仿真结果表明,该算法能够在不可信的环境下较好地保护位置隐私,匿名成功率较高,系统平均响应时间较短。

关键词 位置服务,用户协作,虚拟轨迹
中图法分类号 TP393 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2015.10.030

Collaborate Privacy Protection Based on Virtual Tracks in Position Privacy Protection

ZHAO Yun-hua BAI Guang-wei SHEN Hang DI Hai-yang LI Rui-yao
(Department of Computer Science and Technology, Nanjing University of Technology, Nanjing 210009, China)

Abstract This paper proposed a collaborative privacy protection based on virtual tracks(VTPP), without relying on a trusted third-party agent. Users create virtual tracks and collaborate through self-organization communication. A convex polygon cloaked area is created to protect users' location privacy, causing that the location cloaking quality and query result accuracy are improved. Our simulation results demonstrate that VTPP algorithm achieves higher cloaking success rate along with lower service response time.

Keywords Location-based service, Collaboration, Virtual track

1 引言

随着移动互联网和定位技术的不断发展,基于位置的服务(Location-based Service, LBS)得到了越来越广泛的应用。服务器在提供LBS服务时,需使用移动用户的位置信息,位置信息在服务过程中容易泄露或遭到攻击,这极大地限制了LBS应用的发展。因此,位置信息的隐私管理至关重要。

目前主要的LBS隐私保护技术分为两类[1]:基于可信第三方机构TTP(Trust Third Party)的隐私保护技术[2-5]和不基于可信第三方机构的技术[6-10]。基于TTP的隐私保护技术虽然能够提供较好的隐私保护质量,但容易成为系统性能的瓶颈和集中攻击点。本文将采取不基于TTP的用户协作方法,通过用户之间的协作形成匿名组,达到k-匿名要求进而进行位置伪装。

本文提出的基于虚拟轨迹的用户协作伪装方法,以轨迹取代点来表示用户位置,使得用户协作环境中即使存在恶意节点也很难对系统造成安全性的损害。

本文第2节研究分析典型的不基于TTP的LBS伪装算法以及其存在的隐私威胁;第3节首先定义了需要使用的符号,在此基础上,描述了VTPP的实现细节;第4节通过仿真的方法对提出的机制进行性能分析与评价;最后总结全文。

2 相关工作

目前,不基于TTP的隐私保护算法在LBS隐私保护策略中有较多的研究和应用。

Chi-Yin Chow等人提出了P2P空间匿名方法[6],用户通过相互协作形成匿名组,根据组内用户位置得出最小外接矩形,由查询发起者随机选取一个用户作为代理,向LBS服务器发出查询请求,最后将服务器返回的结果发送给发起请求的用户。该方法假设用户节点都是可信的,不考虑存在恶意节点的情况。

文献[7]提出了基于用户协作的隐私保护方法Coprivacy,通过用户相互协作,以单跳或多跳方式寻找节点形成匿名组。与P2P空间匿名方法不同的是,Coprivacy组内用户使用该组成员位置形成区域的密度中心作为锚点,并用锚点代替自己的真实位置,采用增量近邻查询返回结果,进而根据用户真实位置得到精确的近邻查询结果。使用锚点代替用户真实位置虽然避免了使用伪装区域造成的高计算代价和通信代

到稿日期:2014-09-24 返修日期:2014-12-30 本文受国家自然科学基金项目(60673185,61073197),江苏省自然科学基金项目(BK2010548),江苏省科技支撑计划(工业)项目(BE2011186),江苏省六大高峰人才基金资助项目(第八批)资助。

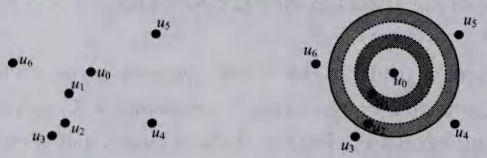
赵耘华(1990-),女,硕士生,主要研究方向为位置服务隐私保护;白光伟(1961-),男,博士,教授,博士生导师,CCF高级会员,主要研究方向为无线传感器网络、移动互联网、网络体系结构和协议、网络系统性能分析和评价、多媒体网络服务质量等,E-mail:bai@njtech.edu.cn(通信作者);沈 航(1984-),男,博士生,CCF学生会员,主要研究方向为无线网络编码、移动互联网、无线多媒体通信协议等;狄海阳(1990-),女,硕士生,主要研究方向为无线多媒体传感器网络、无线网络编码;李瑞瑶(1989-),女,硕士生,主要研究方向为无线多媒体传感器网络、无线网络QoS保障技术。

价，但查询结果准确度不高。

文献[9]提出了 Prive 方法，该方法基于分散式架构，移动用户通过自组织通信，形成了一个具有良好容错能力和负载均衡特性的覆盖网络。用户利用 P2P 技术，通过 k 匿名方法保护用户的位置信息，通过假名方法保护用户的身份信息。然而，Prive 在自组织通信过程中并未对用户位置进行保护，很容易造成位置隐私泄露。

文献[10]提出的 SpaceTwist 方法是非 TTP 的无用户协作位置隐私保护算法。用户选取真实位置附近的点作为锚点，使用该锚点代替真实位置向位置服务提供商发起增量近邻查询。由于缺少用户协作，且无法达到位置 k-匿名，因此隐私保护质量不高。

目前的部分非 TTP 的用户协作伪装算法[6,7]都不考虑恶意节点对系统安全性的影响。大多数应用 P2P 技术的研究[6,7,9]在用户自组织通信阶段缺少对用户位置的保护。如图 1 所示，算法采用了自组织通信方式寻找临近查询发起者的 $k-1$ 个节点行成匿名组。用户在协作过程中完全暴露位置信息，恶意节点很容易在节点发现阶段大致定位节点的位置。



(a)用户位置　　(b)节点发现

图 1　P2P 空间伪装

图 1 中有 7 个用户 $u_0, u_1, \cdots, u_6$。其中，u_0 为查询发起者。在 P2P 空间伪装算法的单跳情况下，假设查询发起者 u_0 本身为恶意节点或被恶意节点控制，那么运行在 u_0 移动设备上的节点寻找算法会被恶意监听和干扰。u_0 广播匿名成组消息后，记录下 u_1, u_2 的响应消息到达时间，根据信道的数据包发送速率并结合一定误差，就可以估计出消息 u_1, u_2 最有可能出现的区域。在图 1(b)中，灰色区域为 u_1, u_2 出现概率最大的区域。由此可见，传统的非 TTP 空间伪装算法不能很好地解决恶意节点环境下的用户隐私保护。另外，在自组织通信阶段，用户始终保持运动状态，使用用户的准确位置参与伪装，实时性较差。

针对大多数非 TTP 位置隐私保护技术的不足，本文提出了基于虚拟轨迹的用户协作伪装算法。通过以线代点的方式，使通信节点无法获取用户的准确位置，减少了恶意节点对系统安全的危害，目的是提高安全性、实时性。

3　伪装策略

3.1　系统结构和符号定义

在研究基于虚拟轨迹的用户协作伪装算法之前，先介绍本文的系统结构，如图 2 所示；接着进行符号定义，用于机制描述。

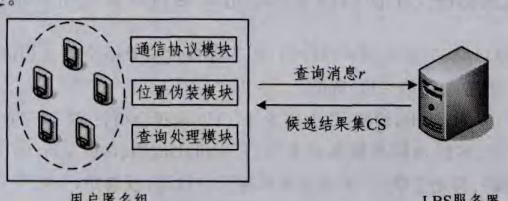


图 2　系统结构

移动客户端的主要模块有：通信协议模块、位置伪装模块和查询处理模块。通信协议模块包含 P2P 通信协议和无线互联网通信协议。用户通过 P2P 通信方式进行自组织通信，形成匿名组，再通过无线互联网向服务器发送查询请求和接收查询结果。P2P 通信一般通过无线局域网或蓝牙实现，无线互联网通信使用移动基站进行交互。位置伪装模块主要负责根据用户的隐私保护需求实现 k 匿名，形成匿名组，生成伪装区域。查询处理模块负责发送查询请求和处理查询结果集。用户请求 LBS 服务时，首先进行广播，寻找 $k-1$ 个匿名同伴，达到位置 k 匿名后，位置伪装模块根据匿名集生成伪装区域，移动客户端以伪装区域形式发送查询请求内容到服务器。LBS 服务器根据该伪装消息进行全数据库检索，并将检索后的结果返回给用户，用户再根据自己的实际位置选择最佳的查询结果。

定义 1(查询消息)　$r=\{u_{id}, p, v_{max}, \beta, k, C, G\}$：$u_{id}$ 代表提出询问请求的用户 id；$p=\{x, y\}$ 代表该消息的位置坐标；v_{max} 代表用户的最大移动速度；β 代表用户的移动方向；消息的 k 值代表用户指定的最低匿名水平，$k=1$ 表示该消息不需要匿名，$k>1$ 表示该消息将与其他至少 $k-1$ 个不同的消息一起伪装，较大的 k 值意味着更高程度的隐私；C 代表消息的文本内容；G 是用户是否入组的标识，是一个 bool 值，$G=0$ 代表用户未加入任何匿名组，$G=1$ 代表用户已入组，G 的初始值为 0。

定义 2(虚拟轨迹)　$l=\{l_{id}, \rho, \rho', k, C, G\}$：$l_{id}$ 代表提出询问请求的用户 id；$\rho=(x, y)$，$\rho'=(x', y')$ 代表该消息的轨迹端点坐标；k 代表用户指定的最低匿名水平；C 代表消息的文本内容；G 是用户是否入组的标识，同查询消息的定义。

定义 3(匿名查询消息组)　$kGROUP=\{g_{id}, k, P, R, C\}$：$g_{id}$ 表示匿名组 id；k 表示匿名组内 l 拥有的最高 k 值；P 代表匿名组内包含的轨迹集合；R 代表匿名组形成的伪装区域；C 代表消息的文本内容。

文中使用的符号如表 1 所列。

表 1　符号含义

符号	参数意义
n	通信范围
v_c	信道传播速率
α	相对位置角度
β	节点运动方向
γ	随机偏离角度
r_q	请求发起节点
r_0	响应节点
L	RWP 转移距离
R	伪装区域
A_{min}	伪装区域最小面积

3.2　RWP 移动模型介绍

随机路点移动模型(Random Waypoint(RWP) Model)[11]是移动通信网络中一个常见的节点移动模型。在 RWP 中，节点随机选择一个目标点(路点)，并以恒定的速度向路点径直移动。路点均匀分布在系统区域，节点从起始位置到下一路点的移动称为一个移动周期。节点移动到下一路点时，重新选择运动方向及运动速度。

在半径为 a 的圆形系统环境中，节点在路点间的转移距离 $\tilde{l}$ 的概率密度函数[11]如式(1)所示：

$$f_L(\tilde{l})=\begin{cases}\frac{8}{\pi a}\frac{\tilde{l}}{2a}(\arccos\frac{\tilde{l}}{2a}-\frac{\tilde{l}}{2a}\sqrt{1-(\frac{\tilde{l}}{2a})^2}), & 0\leqslant\tilde{l}\leqslant 2a\\ 0, & \text{otherwise}\end{cases} \quad (1)$$

如图 3 所示，Or_0 所在直线与水平直线的夹角用 φ 表示，节点的运动方向与 Or_0 的夹角用 θ 表示，在一个运动周期内，该运动方向保持不变。节点到圆心的距离为 r，新的移动方向角度用 β 表示。节点从旧的路点移动到新的路点的运动方向 θ 的概率密度函数[11]为：

$$f_\Theta(\theta|r)=\frac{1}{2\pi}(\frac{r}{a}\cos\theta+\sqrt{1-\frac{r^2}{a^2}\sin^2\theta})^2 \quad (2)$$

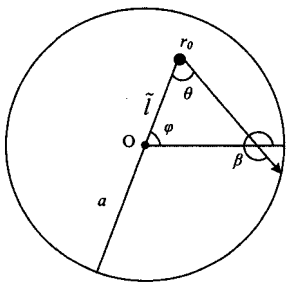


图 3　RWP 移动方向示意图

在虚拟轨迹规划阶段，用户转移距离 L 和移动角度 Θ 的概率分别如式(1)、式(2)所示。在实验仿真阶段，样本节点的分布和移动使用 RWP 移动模型生成。

3.3　虚拟轨迹规划

在 VTPP 中，虚拟轨迹的生成至关重要。在位置伪装的过程中，用户节点始终在移动，当查询请求发起节点收到响应节点的确认消息时，响应节点的位置已经发生了改变。

VTPP 中用户自组织通信的消息传输示意图如图 4 所示。r_q 广播成组消息 FORM_GROUP，接收方 r_0 持有一个计时器，将接收到 FORM_GROUP 消息的时刻记为 t_e，将准备发送确认消息的时刻记为 t_s。t_s-t_e 主要包含节点寻找下一级邻居的时间、虚拟轨迹的生成时间和其他干扰因素造成的额外时间。如果需要多跳广播，则继续寻找下一轮节点。

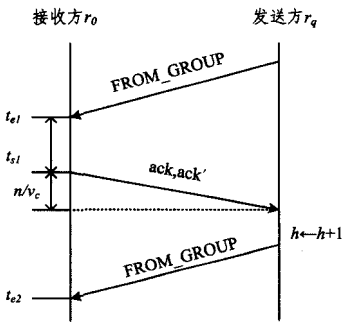


图 4　消息传输示意图

图 5 给出了 4 种具有代表性的随机运动方向的选择示意图。φ 为直线 Or_0 与 x 轴正方向的夹角；θ 为 Or_0 与新的运动方向的夹角；α 表示 r_0 相对 r_q 在二维坐标中的角度，即 r_0r_q 所在直线与 x 轴正方向的夹角；$\alpha\in[0,2\pi]$；β 表示新的运动方向与 x 轴正方向的夹角，$\beta\in[0,2\pi]$。

$$\beta=\theta+\varphi+\pi \quad (3)$$

显然，α 与 β 的值越接近(即新的运动方向与 r_0r_q 所在直线离得越近)，r_0 可能到达的位置离 r_q 越远。由于 φ,θ 取值方向的不同，由式(3)计算的 β 可能超出$[0,2\pi]$。β 在二维坐标中的实际角度为：

$$\beta=\beta-\left\lfloor\frac{\beta}{2\pi}\right\rfloor\cdot 2\pi \quad (4)$$

将 β 与 α 比较，若 $\alpha>\beta$，则用户的运动角度虚拟轨迹方向为 $\beta+\gamma$；若 $\alpha<\beta$，则用户的运动角度虚拟轨迹方向为 $\beta-\gamma$，γ 在$(0,|\alpha-\beta|]$中随机取值；若 $\alpha=\beta$，则用户的运动方向不做任何改变。图中带箭头的曲线示意运动角度的偏离方向，保证了虚拟轨迹的终点与 r_q 的距离一定大于用户实际所在位置与 r_q 的距离，即在虚拟轨迹响应 FROM_GROUP 成功时，用户真实位置不超出 r_q 的广播范围。

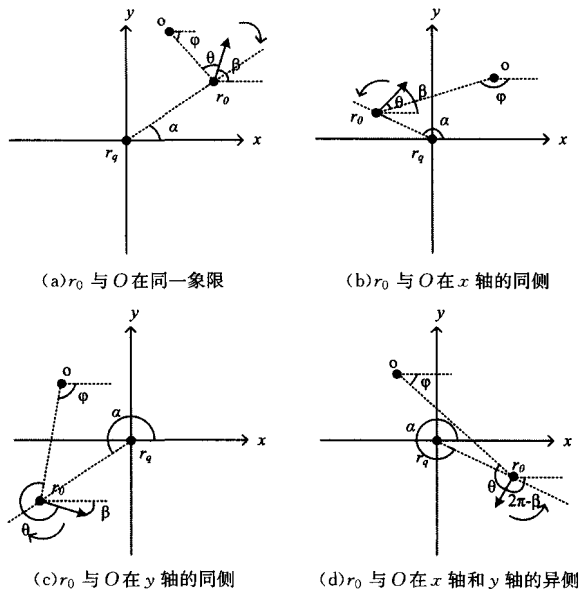


图 5　随机运动方向选择

在节点虚拟轨迹规划中，$\rho'=(x',y')$代表下一时刻的位置坐标，是虚拟轨迹的终点；$\rho=(x,y)$代表当前的位置，是虚拟轨迹的起点。r_0 首先根据自己的位置 $r_0.p$ 随机选取 γ，结合 $r_0.v_{max}$，在时间间隔(t_e,t_s)内形成一条直线 l。

算法 1　虚拟轨迹规划 Virtual_track_develop

1. Input: r, n, v_c
2. Output: l
3. l. $l_{id}\leftarrow$ r. u_{id};
4. l. $\rho\leftarrow$ r. p;
5. l. k$\leftarrow$ r. k;
6. l. C$\leftarrow$ r. C;
7. $t_e\leftarrow$ the time r receive FROM_GROUP;
8. $t_s\leftarrow$ the time r finish finding other peers;
9. d$\leftarrow$ r. $v_{max}\cdot(t_s-t_e+n/v_c)$;
10. $\alpha\leftarrow$ the angle between r_q. pr. p and x-axis;
11. $\beta\leftarrow$ the angle between new direction and x-axis;
12. randomly choose $\gamma\in(0,|\alpha-\beta|)$;
13. if $\alpha>\beta$
14. $\quad\beta\leftarrow\beta+\gamma$;
15. end if
16. if $\alpha<\beta$
17. $\quad\beta\leftarrow\beta-\gamma$;
18. end if
19. x' $\leftarrow$x+d $\cdot$ cos β;
20. y' $\leftarrow$y+d $\cdot$ sin β;
21. $\rho'\leftarrow$(x', y');
22. return l$\leftarrow$\{ l_{id}, ρ, ρ', k, C, G\}

算法 1 描述了虚拟轨迹的生成规则，l 的 id 号、起点位置 ρ、匿名等级 k、查询消息文本内容 C 都与 r 的相同，G 为 0。该算法持有一个计时器，用于记录节点接收和发送消息的时间，收到消息的时刻记为 t_e，发出消息的时刻记为 t_s。r_q 的通信范围为 n，电磁波在信道上的传播速率为 v_c，估计传播时延为 n/v_c，发送时延忽略不计。由于节点一直保持移动，在接收到 FROM_GROUP 消息后，节点根据 RWP 随机选择下一个路点，生成一条轨迹 l，长度为 $r_0.v_{max}\cdot(t_s-t_e+n/v_c)$（算法 1 第 7－9 行）。接着，选取 $\gamma\in(0,|\alpha-\beta|]$，$\beta$ 的取值如式(4)，使轨迹偏离原始运动方向（算法 1 第 13－18 行），虚拟轨迹用源点坐标和终点坐标 ρ、ρ' 表示。

用户通过虚拟轨迹将自身位置模糊化，提高了位置隐私保护质量。然而虚拟轨迹的多样性也势必造成伪装区域面积的扩大，导致查询服务质量的降低。VTPP 使用凸多边形作为 k 匿名集的伪装区域，与传统的最小边界矩形和圆形伪装区域相比，凸多边形缩小了伪装区域面积，在提高位置隐私保护质量的同时，一定程度上减轻了虚拟轨迹多样性对于伪装区域大小的影响。

3.4 虚拟轨迹分组

节点通过自组织通信，形成用户匿名组。请求发起者 r_q 向全组广播一个成组请求，r_q 在跳数 h 内寻找 k 个节点轨迹 $l_1,l_2,\cdots,l_{k-1}$。当寻找到符合条件的 $k-1$ 个节点轨迹后，r_q 集中 $k-1$ 个轨迹的位置范围，形成匿名组。算法 2 描述了 r_q 寻找 $k-1$ 个伪装同伴节点的过程。

算法 2 节点寻找

```
1. Input:r_q,h,g_id
2. Output:kGROUP
3. r_q.u_id←g_id;kGROUP.g_id←g_id;
4. k'←r_q.k;
5. Virtual_track_develop(r_q,n,v_c);
6. h←1;
7. while n<k'-1;
8.   n←|P|;
9.   broadcast FORM_GROUP message with h,g_id;
10.   receive the ACK message ack and ack' from l;
11.   l.G←1
12.   add l to P';
13.   k'←highest k of P';
14.   if n<k'-1 then
15.     if P=P' then
16.     sort the track in P in increasing order of l.k;
17.       l_q←the first item of r∈S
18.     end if
19.     h←h+1;P←P';
20.   end if
21. end while
22. P=P∪{l_q},n←n+1;
23.   Cloak_area_create(P);
24. kGROUP.R←R;
25. kGROUP.k←k';
26. kGROUP.P←P;
27. kGROUP.C←l_q.C;
28. return kGROUP
```

算法 2 的输入为查询发起者 r_q、广播跳数 h 和匿名组 id 号 g_{id}，输出为匿名组 kGROUP。首先用 g_{id} 取代 r_q 的消息 id 号，这表示 r_q 已经组建了一个匿名组，并开始寻找匿名组成员，匿名组的待定伪装等级 k' 预先设置为 r_q 的 k 值（算法 2 第 3、4 行）。接着，调用虚拟轨迹规划算法生成 r_q 的虚拟轨迹 l_q。P' 表示待定轨迹集，P 表示确定轨迹集，n 表示轨迹个数。r_q 广播成组消息 FORM_GROUP，在 h 跳内，有节点接收到该消息，将准确位置伪装成虚拟轨迹，并发送确认消息 ACK 给 r_q，r_q 收集到确认消息 ack 和 ack'，若其确保轨迹两端皆在通信范围内，则将发送确认消息的轨迹 l 添加进 P'，并将匿名组 k 值设置为 P 中轨迹所拥有的最大 k 值（算法 2 第 9－13 行）。如果在 h 跳内未能找到 $k-1$ 个轨迹，则将跳数增加 1，继续广播 FORM_GROUP 寻找（算法 2 第 14－20 行）。最后，节点寻找完成，虚拟轨迹规划算法将 r_q 伪装成 l_q 并添加进匿名集 P，将 n 加 1，表示实际匿名集 P 内的轨迹个数。

节点在收到广播消息 FORM_GROUP 后，发送确认消息 ACK 并协助 r_q 伪装，算法 3 给出了节点响应算法。

算法 3 节点响应算法 Node_response

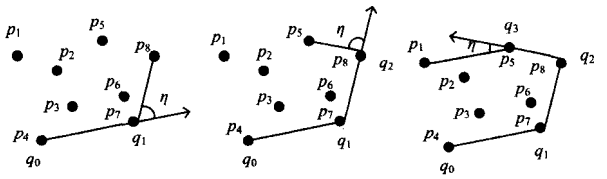
```
1. Input:FORM_GROUP,h,g_id
2. Output:P'
3. if r_0.G==0 or r_0.u_id== g_id then
4.   Virtual_track_develop(r_0,n,v_c);
5. end if
6. wait a random time τ;
7. send an ACK message ack_0 to r_q at location(x_0,y_0);
8. send an ACK message ack_0' to r_q at location(x_0',y_0');
9. r_0.u_id←g_id;
10. while h>1
11.   h←h-1;
12.   broadcast FORM_GROUP message with h,g_id;
13.   Node_response(FORM_GROUP,h,g_id);
14. end while
15. send l_0 to r_q;
```

r_0 接收到 FORM_GROUP 消息后，首先检查 $r_0.G$，如果 $r_0.G$ 的值为 1，说明 r_0 已经加入别的匿名组，则不能参与该组的伪装；如果 $r_0.G$ 的值为 0 或 r_0 的 id 已经添加该组的 g_{id}，则说明 r_0 可以参与协作伪装，于是开始执行算法 1，对 r_0 进行虚拟轨迹规划（算法 3 第 3－5 行）。接着，等待一个随机时间 $\tau\in(0s,0.1s)$，使得 r_0 发送 ACK 的时间更加具有随机性，从 l_0 的两端分别发送一个确认消息。r_0 判断 FORM_GROUP 的跳数 h，如果 $h=1$，即 r_q 对全组进行了单跳广播，当节点接收到消息时，单跳广播已经完成，接收到该消息的节点不做任何操作；如果 $h>1$，则 l_0 将 h 减 1，继续将 FORM_GROUP 消息进行广播并等待邻居节点响应，直到 h 跳广播结束。l_0 将 h 跳内收到的能够参与协作伪装的节点全部返回给 r_q。若节点响应算法为 r_q 提供了大于 $k-1$ 个轨迹，则 r_q 的匿名组形成，用户通过协作成功地形成了匿名组。

3.5 伪装区域形成

匿名组形成后，算法需要针对该匿名组形成伪装区域，才能够对 l_q 发出的查询消息进行服务。一方面，用户轨迹成组，伪装区域需要覆盖这些节点轨迹后才能够对匿名组内的用户进行伪装保护；另一方面，伪装区域的面积越小，查询服务产生的候选结果集才会越精确。如图 6 所示，VTPP 算法使用了凸多边形的伪装区域，在保护匿名组隐私的同时，生成

了面积最小的伪装区域。



(a)过程一　(b)过程二　(c)过程三

图 6　伪装区域形成示意图

由于 VTPP 中用户以虚拟轨迹方式参与伪装，模糊的用户位置意味着更大的伪装区域面积。传统的矩形伪装区域造成了较大的伪装区域冗余。为有效缩小伪装区域面积，VTPP 使用 GiftWrapping 算法生成凸多边形的伪装区域，在伪装区域中，攻击者即使知道在凸多边形的顶点处必存在一个虚拟轨迹端点，也无法准确定位用户所在的位置。

在伪装区域形成过程中，只需要使用匿名组中轨迹 l_0，$l_1, l_2, \cdots, l_{k-1}$ 的端点 $\rho_0, \rho_0', \rho_1, \rho_1', \rho_2, \rho_2', \cdots, \rho_{k-1}, \rho_{k-1}'$。为方便表示，将这些端点命名为 $p_1, p_2, \cdots, p_{2k}$。

算法 4　伪装区域形成 Cloak _area_create

1. Input:P
2. Output:R
3. q_0←the node with the smallest p. y;
4. create a line s at q_0. y parallel to the x-axis;
5. for 1≤i≤2k
6. η←the smallest angle between $\overrightarrow{q_j p_i}$ and s;
7. end for
8. q_1←p_i in $\overrightarrow{q_j p_i}$ with η;
9. j←1;e←3;
10. while q_e. x≠q_0. x and q_e. y≠q_0. y
11. for j+2≤i≤2k
12. η←the smallest angle between $\overrightarrow{q_j q_{j+1}}$ and $\overrightarrow{q_{j+1} p_i}$;
13. end for
14. q_e←p_i in $\overrightarrow{q_{j+1} p_i}$ with η;
15. add $\overrightarrow{q_j q_e}$ to E;
16. j←j+1;e←e+1;
17. end while
18. return R←the area surrounded by edges in E

首先选取 y 坐标最小的点作为伪装区域生成的起始点，在图 6 所示的例子中找到 p_4，记为 q_0。画一条平行于 x 轴的直线 s，显然 q_0 是凸多边形的一个顶点(算法 4 第 3、4 行)。接着，在剩下的节点 p_i 中寻找 $\overrightarrow{q_0 p_i}$ 与 s 夹角最小的点，记为 q_1(算法 4 第 5—8 行)。如图 6 所示，伪装区域形成算法找到了节点 p_7，将 p_7 记为 q_1。确定 q_1 后，继续寻找剩下的节点中与 $\overrightarrow{q_j q_{j+1}}$ 夹角最小的边 $\overrightarrow{q_{j+1} p_i}$。图 6 中算法依次找到了 p_8, p_5, p_1。将寻找到的边添加到边集 E 中。直到最后寻找到的节点与起始节点 q_0 重合(算法 4 第 10—17 行)。E 中的边所围成的区域即为所要求的凸多边形。

定理 1　已知点集 $U=\{p_1, p_2, \cdots, p_n\}$，若对于所有连续的 3 点 p_i, p_j, p_k 以及 p_h ($1\leqslant i, j, k, h\leqslant n$ 且 $h\neq j$) 均满足 $\overrightarrow{p_j p_k}$ 与 $\overrightarrow{p_i p_j}$ 的夹角小于所有 $\overrightarrow{p_j p_h}$ 与射线 $\overrightarrow{p_i p_j}$ 的夹角，则 U 所围成的区域一定是凸多边形。

证明：为方便表示，记射线正方向一端为 e。假设在一个二维坐标系内存在一个凸多边形，$p_i p_j$ 和 $p_j p_k$ 为两条相邻边，凸多边形上存在 p_0 使得 $\angle e p_j p_0 < \angle e p_j p_k$。

根据凸多边形性质，任意一边向两方无限延长成为一条直线，多边形的其余顶点均在此直线同侧。因为 $\angle e p_j p_0 < \angle e p_j p_k$，所以至少存在一点 p_0 在 $p_j p_k$ 所在直线的另一侧，与凸多边形性质矛盾，故假设不成立。

4　仿真实验与结果分析

本节针对性地设计了一系列仿真实验，对所提出的 VTPP 进行性能分析和评价。首先介绍仿真环境和参数设置，然后对仿真结果进行分析和讨论。

4.1　实验设计

本文通过仿真方法对 VTPP 的性能进行分析，并将其与 P2P 空间伪装算法进行比较。实验环境为一个 1km² 的圆形区域，实验数据由随机路点模型 RWP 生成器[7]生成，暂停时间设置为 0，100 个节点的路点转移距离概率密度函数为公式(1)，移动轨迹方向的概率密度函数为公式(2)，使用该模型产生的用户移动与实际环境接近。消息的 k 值范围为[2,10]，该匿名等级取值范围目前较流行。随机选取 k 值时，本实验分别对{5,4,3,2}和{6,7,8,9,10}使用参数为 0.6 的 Zipf 分布随机选取。基于 Zipf 分布，$k\in[5,7]$ 在源数据中个数最多，而 $k\in[2,4]$ 和 $k\in[8,10]$ 在源数据中个数相对较少，这一数据分布符合匿名水平大小的一般规律。伪装区域面积的最小限制 $A_{\min}$ 设定为面积的 0.01%，即 100 m²。设用户协作通信带宽为 1Mbps，移动用户与位置服务提供商之间使用 3G 网络通信，带宽为 2Mbps。具体实验参数如表 2 所列。

表 2　实验参数

参数名称	设置
用户数量	100
匿名等级 k	[2,10]
协作带宽	1Mbps
查询服务带宽	2Mbps
平均最大速度 v_{max}	15m/s
最小面积限制 A_{min}	100 m²

本实验衡量 VTPP 的标准包括平均匿名成功率、平均位置确定度、平均响应时间和平均伪装区域面积。其中，匿名成功率是成功匿名的用户和总用户数的比率。

用户位置确定度使用 $K(r)$ 表示，首先给出衡量混乱程度的位置熵：

$$E(r)=-\sum_{i=1}^{n} p(\tilde{l})\log_2 p(\tilde{l}) \tag{5}$$

式(5)为查询消息 r 的位置熵，$p(\tilde{l})$ 表示用户轨迹在伪装区域 R 中的概率密度分布函数，VTPP 轨迹不同时刻的概率密度分布函数由 RWP 移动模型给出。P2P 位置服从均匀分布，概率密度分布函数服从均匀分布。

$$K(r)=2^{-E(r)} \tag{6}$$

式(6)表示 VTPP 中查询消息 r 的位置确定度，$K(r)$ 值越高，确定 r 点位置的概率越大。

平均响应时间是仿真环境中得到的从用户发起查询到伪装成功的平均时间。

伪装区域面积的计算方式如下，VTPP 的凸多边形伪装区域面积为：

$$S_{convex}=\frac{1}{2}\sum_{i=1}^{n}\begin{vmatrix} x_i & x_{((i+1) \bmod (n))} \\ y_i & y_{((i+1) \bmod (n))} \end{vmatrix} \tag{7}$$

式中，x_i，y_i为凸多边形顶点在二维坐标中的位置，n表示凸多边形的顶点数。顶点的排列顺序为伪装区域形成算法生成的逆时针顺序。P2P的伪装区域为组内用户位置的最小外接矩形，其面积为：

$$S_{MBR}=(\max_{1\leqslant i\leqslant n} x_i-\min_{1\leqslant i\leqslant n} x_i)\times(\max_{1\leqslant i\leqslant n} y_i-\min_{1\leqslant i\leqslant n} y_i) \quad (8)$$

式(8)取匿名集中x，y的最大和最小值计算MBR伪装区域面积。

平均匿名成功率越高，算法的性能越好；平均用户位置确定度越低，伪装保护质量越高；平均响应时间越短，算法的效率越高；在保证伪装质量的前提下，平均伪装区域面积越小，LBS在提供询问查询服务时的系统开销越小，查询结果越精确。

4.2 结果分析

本实验首先测试了VTPP的平均匿名成功率，然后给出了平均用户位置确定度及平均响应时间，最后给出了平均伪装区域面积并将其与P2P算法进行了比较。

图7给出k在不同取值的情况下，VTPP和P2P的平均匿名成功率结果。

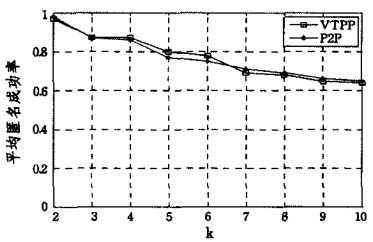


图7 平均匿名成功率

两种伪装算法的平均匿名成功率随k值的增加而下降，这是因为k值低的查询请求比k值高的消息更容易寻找到$k-1$个伪装同伴，伪装难度相对较低。从图7中可以看出，k值在[2,10]范围内时，VTPP和P2P的匿名成功率比较接近。这说明在比较大的范围内，VTPP所使用的虚拟轨迹长度未对算法的匿名成功率造成影响，即虚拟轨迹在提高了用户伪装质量的情况下，不牺牲匿名成功率。

图8给出了k在不同取值的情况下，VTPP和P2P的平均用户位置确定度结果。

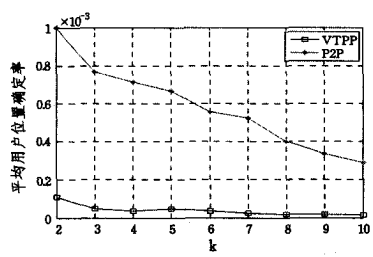


图8 平均用户位置确定度

从图8可以看出，随着k值增加，两种算法的用户位置确定度都有明显下降，这是因为k值越高，用户对于安全性的需求越高，需要寻找更多的伪装同伴，产生的伪装区域面积越大，用户在伪装区域内位置的确定度就越低。同时，VTPP的用户的位置确定度比P2P低很多，这是因为在VTPP中，用户在相互协作时的位置是模糊的，如果系统受到恶意攻击，必须先定位用户的虚拟轨迹位置，再确定用户准确位置坐标；而P2P只用伪装区域来保护用户位置，位置确定度较高。

图9给出了VTPP和P2P算法处理查询消息的平均响应时间。从图中可以看出，P2P平均响应时间明显长于VTPP算法，这是由于VTPP在进行多跳广播无法找到$k-1$个轨迹时，对匿名组内的用户根据k值进行了排序，k值小的查询请求先服务，保证了安全需求低的用户不用等待过长的时间，可以在较短时间内寻找到伪装同伴，得到服务后仍协助高k值的用户的伪装，不会滞后高k值用户的伪装。而P2P算法在无法寻找到$k-1$个伪装同伴时选择暂停查询请求的处理，这导致用户为寻找伪装同伴或配合伪装同伴消耗了大量时间，伪装的响应时间变长。

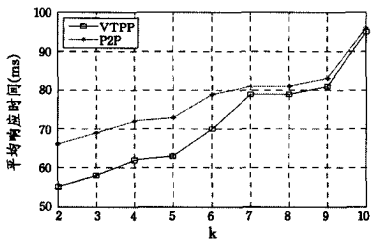


图9 平均系统响应时间

图10给出了VTPP和P2P的平均伪装区域面积。VTPP和P2P的平均伪装区域面积都与k值成正比，同时，在用户分布密度相同的情况下，VTPP的平均伪装区域面积小于P2P。产生这种差异的原因是VTPP使用凸多边形有效地缩小了伪装区域的面积，这有利于查询结果精准度的提高。当k值较小时，VTPP和P2P的伪装区域面积相差不大，而随着k值的增加，伪装区域面积有了较大的差异。这是因为在k值较小的情况下，匿名组内的轨迹个数较少，轨迹之间距离较近，凸多边形与矩形伪装区域的面积相差不明显；而随着k值增加，匿名集中的轨迹个数变多，范围变大时，凸多边形比矩形明显具有更小的面积。

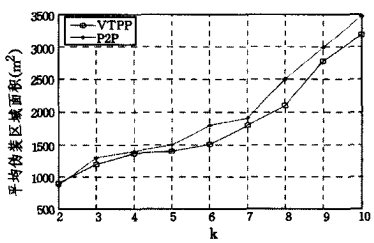


图10 平均伪装区域面积

结束语 本文提出位置隐私保护中基于虚拟轨迹的用户协作伪装算法VTPP。该算法不依赖可信第三方机构，通过用户的相互协作实现k匿名，形成匿名组。这种做法避免了依赖第三方机构而造成的安全威胁。VTPP给出了发送方和接收方两端的节点寻找和节点响应算法。节点寻找和节点响应算法清晰地表现出了用户之间协作形成匿名组的过程。虚拟轨迹规划算法给出了用户通过轨迹将自身准确位置模糊化的方法。最后形成凸多边形的伪装区域来保护用户位置隐私。VTPP为用户提供了虚拟轨迹和伪装区域的双重保护，通过k-匿名保护了用户的位置信息，通过虚拟轨迹确保了在不可信环境下的用户位置隐私不被攻击和泄露，同时提高了查询服务的实时性。凸多边形的伪装区域在保证较好地伪装质量的同时，缩小了伪装区域面积，提高了查询结果的准确性。仿真结果表明，该算法能够在不可信环境下较好地保护位置隐私，匿名成功率较高，系统平均响应时间较短，平均用

户位置确定度较低，平均伪装区域面积较小，能够更好地适用于现实环境。

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 service: Architecture and Progress [J]. Chinese Journal of Computers, 2011, 34(7): 1155-1171

[2] Xu J, Tang X, Hu H, et al. Privacy-conscious location-based queries in mobile environments [J]. IEEE Transactions on Parallel and Distributed Systems, 2010, 21(3): 313-326

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

[4] Mokbel M F, Chow C Y, Aref W G. The new Casper: query processing for location services without compromising privacy[C]// Proceedings of the 32nd International Conference on Very Large Data Bases. 2006: 763-774

[5] 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

[6] Chow C, Mokbel M F, Liu X. A peer-to-peer spatial cloaking algorithm for anonymous location-based services [C] // Proceedings of the Annual ACM International Symposium on Advances in Geographic Information Systems (GIS'06). Virginia, USA, 2006: 171-178

[7] 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
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

[8] Solanas A, Martínez-Ballesté A. A TTP-free protocol for location privacy in location-based services[J]. Computer Communications, 2008, 31(6): 1181-1191

[9] Ghinita G, Kalnis P, Skiadopoulos S. PRIVE′: anonymous location based queries in distributed mobile systems[C]// Proceedings of the Sixteenth International World Wide Web Conference (May 2007). Alberta, Canada, 2007: 371-380

[10] 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]// Proceedings of the IEEE International Conference on Data Engineering (ICDE'08). Cancun, Mexico, 2008: 366-375

[11] Bettstetter C, Hartenstein H, Pérez-Costa X. Stochastic properties of the random waypoint mobility model[J]. Wireless Networks, 2004, 10(5): 555-567

[12] Campos C A V, de Moraes L F M. A markovian model representation of individual mobility scenarios in ad hoc networks and its evaluation[J]. EURASIP Journal on Wireless Communications and Networking, 2007, 1(3)

[13] Camp T, Boleng J, Davies V. A survey of mobility models for ad hoc network research[J]. Wireless Communications and Mobile Computing, 2002, 2(5): 483-502

(上接第 131 页)

[4] Wang Fu-sheng, Liu Shao-rong, Liu Pei-ya. Complex RFID Event Processing[J]. The VLDB Journal, 2009, 18(4): 913-931

[5] 徐传飞，林树宽，乔建忠，等. 高密度 RFID 事件流上的复杂事件检测[J]. 东北大学学报(自然科学版)，2012，33(5)：627-631
Xu C F, Lin S K, Qiao J Z, et al. Complex event detection on high-density RFID event streams [J]. Journal of Northeastern University (Natural Science), 2012, 33(5): 627-631

[6] Wu E, Diao Y, Rizvi S. High-performance complex event processing over streams [C]// Proceedings of ACM Conference on Management of Data. Chicago, 2006: 407-418

[7] Demers A J, Gehrke J, Panda B, et al. Cayuga: A general purpose event monitoring system [C]// Proceedings of the 3rd Biennial Conference on Innovative Data Systems Research. California, 2007: 412-422

[8] Li M, Liu M, Ding L P, et al. Event stream processing with out-of-order data arrival [C]// Proceeding of the 27th International Conference on Distributed Computing Systems Workshops. Toronto, 2007: 67-74

[9] Brito A, Fetzer C, Sturzrehm H, et al. Speculative out-of-order event processing with software transaction memory[C]// DEBS 2008. New York: ACM, 2008

[10] Li C W, Gu Y, Yu G, et al. Aggressive Complex Event Processing with Confidence over Out-of-Order Streams [J]. Journal of Computer Science and Technology, 2011, 26(4): 685-696

[11] 王中强. RFID 复杂事件实时查询处理及其优化策略[D]. 武汉：华中科技大学，2011
Wang Z Q. Real-time query processing and optimizing strategy for RFID complex events [D]. Wuhan: Huazhong University of Science and Technology, 2011

[12] 叶蔚，黄雨，赵文，等. 基于 Petri 网的 RFID 中间件中复合事件检测研究[J]. 电子学报，2008，36(12A)：1-8
Ye Wei, Huang Yu, Zhao Wei, et al. Research on Composite Event Detection in RFID Middleware Based on Colored Petri Net [J]. Acta Electronica Sinica, 2008, 36(12A): 1-8

[13] 曹原，刘英博，肖利，等. 状态监测数据流时间乱序问题建模与研究[J]. 计算机集成制造系统，2013，19(12)：2960-2967
Cao Yuan, Liu Ying-bo, Xiao Li, et al. Modeling on time out-of-order problem of condition monitoring data stream [J]. Computer Integrated Manufacturing Systems, 2013, 19(12): 2960-2967

[14] 刘海龙，李战怀. 基于 ENFA 的乱序 RFID 复杂事件检测算法[J]. 华中科技大学学报(自然科学版)，2010，38(1)：25-30
Liu Hai-long, Li Zhan-huai. Out-of-order RFID complex event detecting algorithm based on ENFA [J]. Journal of Huazhong University of Science and Technology (Nature Science Edition), 2010, 38(1): 25-30

[15] 马宝林，孙济洲，于策. 基于混合时间-事件驱动的信任值更新机制[J]. 计算机应用，2006，26(10)：2289-2291
Ma Bao-lin, Sun Ji-zhou, Yu Ce. Trust value updating mechanism based on mixed time-event [J]. Journal of Computer Applications, 2006, 26(10): 2289-2291