移动社交网络中基于代理转发机制的轨迹隐私保护方法

张少波[①④] Md Zakirul Alam Bhuiyan[②] 刘 琴[③] 王国军*[①⑤]
[①](中南大学信息科学与工程学院 长沙 410083)
[②](天普大学计算机与信息科学系 费城 PA19122)
[③](湖南大学信息科学与工程学院 长沙 410082)
[④](湖南科技大学计算机科学与工程学院 湘潭 411201)
[⑤](广州大学计算机科学与教育软件学院 广州 510006)

摘 要：K 匿名技术是当前轨迹隐私保护的主流方法，但该方法也存在隐私泄露的风险。该文提出一种在移动社交网络中基于代理转发机制(BAFM)的轨迹隐私保护方法。该方法利用安全多方计算和内积安全计算进行隐私加密匹配，通过可信服务器在移动社交网络中找最匹配的用户做代理，然后由代理转发用户的请求到服务器进行查询，隐藏用户的真实轨迹与位置服务器的联系，有效保护用户的轨迹隐私。安全分析表明该方法能有效保护用户的轨迹隐私；同时，通过实验验证该方法相对 K 匿名更高效，能减小服务器的查询和通信开销。

关键词：移动社交网络；轨迹隐私保护；安全多方计算；内积安全计算
中图分类号：TP393 **文献标识码**：A **文章编号**：1009-5896(2016)09-2158-07
DOI: 10.11999/JEIT151136

The Method of Trajectory Privacy Preserving Based on Agent Forwarding Mechanism in Mobile Social Networks

ZHANG Shaobo[①④] Md Zakirul Alam Bhuiyan[②] LIU Qin[③]
WANG Guojun[①⑤]
[①](*School of Information Science and Engineering*, *Central South University*, *Changsha* 410083, *China*)
[②](*Department of Computer and Information Sciences*, *Temple University*, *Philadelphia*, PA19122, *USA*)
[③](*College of Computer Science and Electronic Engineering*, *Hunan University*, *Changsha* 410082, *China*)
[④](*School of Computer Science and Engineering*, *Hunan University of Science and Technology*, *Xiangtan* 411201, *China*)
[⑤](*School of Computer Science and Educational Software*, *Guangzhou University*, *Guangzhou* 510006, *China*)

Abstract: The trajectory K-anonymous is the mainstream of the current trajectory privacy protection, but the method has some defects such as privacy leakage. In this paper, a method of trajectory privacy preserving is proposed Based on Agent Forwarding Mechanism (BAFM) in mobile social networks, which uses secure multi-party computation and inner product secure computation to find the best matching user by the trusted server as the agent. The agent forwards the user's request to the server to query, which hides the correlation between user's real trajectory and the server in order to achieve user's trajectory privacy. Security analysis shows that the propose method can effectively protect the user's trajectory privacy. Experiments show that the proposed method is more effective, it reduces the overhead of server's query and communication.

Key words: Mobile social network; Trajectory privacy-preserving; Secure multi-party computation; Inner product secure computation

1 引言

随着无线通信技术和具有定位功能的个人智能终端设备的发展，基于位置的服务(Location- Based Service, LBS)发展迅速并获得广泛关注[1]。用户通过LBS可以获得用户位置附近的兴趣点(Points Of Interests, POIs)，然而人们在享用LBS服务带来便利的同时，也面临着敏感信息泄露的风险。例如：根据用户连续的LBS查询，攻击者可以分析出用户的敏感轨迹特征，如工作及家庭地址、个人生活习惯等。因此，目前基于位置服务的轨迹隐私保护问题已引起学术界和工业界的广泛关注，并迫切需要解决。为减少轨迹隐私泄露的风险，国内外学者已

收稿日期：2015-10-10；改回日期：2016-02-18；网络出版：2016-04-26
*通信作者：王国军 csgjwang@csu.edu.cn
基金项目：国家自然科学基金(61472451, 61272151, 61402161, 61502163)，中南大学中央高校基本科研业务费专项资金(2016zzts058, 2016zzts060)
Foundation Items: The National Natural Science Foundation of China (61472451, 61272151, 61402161, 61502163), The Fundamental Research Funds for the Central Universities of Central South University (2016zzts058, 2016zzts060)

提出一些轨迹隐私保护方法，主要可分为3类[2]：假轨迹方法、抑制法和泛化法。假轨迹方法通过为真实轨迹产生一些假轨迹来减少真实轨迹暴露的风险[3,4]，该方法简单并具有较小的计算开销，但数据存储容量大。抑制方法使轨迹上的敏感位置或频繁访问的位置不发布到LBS服务器[5,6]，该方法容易实现，但会丢失信息。泛化法就是泛化轨迹上的样本点到相关的匿名域，使用户的位置不能被精确地确定[7−10]，该方法能确保数据的正确性，但有很高的计算开销。

目前泛化法中的K匿名是轨迹隐私保护的主流方法。如文献[11]中提出用K匿名方法保护用户的轨迹隐私。当用户发出查询时，首先寻找历史轨迹上的其它$(K-1)$个足迹点，以形成包含K个不同位置的匿名域，然后发送到服务器查询，使服务器不知道用户的精确位置，以达到保护用户轨迹隐私的目的。但该方法也存在以下隐私泄露的风险：(1)通过连接各个匿名域，攻击者可以知道用户的运动轨迹。(2)通过对比不同时间点匿名域中的用户，攻击者能指出真实用户。(3)如果匿名域太小，攻击者能识别用户的具体位置。

针对K匿名方法的不足，本文结合移动社交网络(Mobile Social Network, MSN)，提出一种MSN中基于代理转发机制(Based on Agent Forwarding Mechanism, BAFM)的轨迹隐私保护方法。通过在MSN中找到最匹配的用户做代理，建立用户信息的转发机制，隐藏用户真实轨迹与LBS服务器的联系，以实现用户的轨迹隐私保护。在MSN中，寻找与服务用户距离最远、且运动方向差异最大的用户做代理，使它们的轨迹差异最大。匹配过程中，利用安全多方计算和内积安全计算进行隐私加密，实现安全和高效的匹配。该方法中代理转发到服务器查询的用户位置是精确的，可以减少服务器的计算和通信开销。

2　系统模型和相关定义

2.1 系统模型

基于代理转发机制的轨迹隐私保护模型如图 1 所示。移动过程中服务用户需要 LBS 时，首先以当前位置为中心形成一个 MSN，该 MSN 覆盖范围内的用户分别将个人的属性信息发送到可信计算服务器，然后利用基于安全多方计算和内积安全计算进行隐私匹配，找到 MSN 中与服务用户指定属性最匹配的用户做代理。通过代理在服务用户和 LBS 服务器之间进行信息转发，使 LBS 服务器无法获得服务用户的真实身份信息，该方法能以较低的计算和通信开销保护用户的轨迹隐私，并让用户获取精确的查询结果。该模型主要由 4 类实体组成：服务用户、最匹配用户、LBS 服务器以及可信计算服务器。

服务用户　携带具有全球定位、计算存储和无线通信功能的智能终端用户，它能将不同时刻的请求信息连续发送到服务器进行查询。

最匹配用户　在 MSN 中最满足服务用户特定属性条件的用户，它的主要功能是在服务用户和 LBS 服务器之间转发查询请求信息和查询结果。

LBS 服务器　它是一个服务提供者，拥有服务数据库能为用户提供各种数据服务。LBS 服务器收到查询请求后，在数据库搜索服务用户指定的 POIs，并将它返回给服务用户。

可信计算服务器　它是建立在可信计算平台上的服务提供者，具有较强的计算能力，为用户提供各种计算服务。本模型中，可信计算服务器主要提供安全多方计算和内积安全计算，以高效计算得到最匹配值。

2.2 相关定义

定义 1　两点间的距离　二元组$(x\ ,y)$表示平面上某点位置的经纬度，假设$A(x_1\ ,y_1)$和$B(x_2\ ,y_2)$是 2 维平面的两个位置点，则它们之间的欧氏距离D_{AB}可以表示为

$$D_{AB}=\sqrt{(x_1-x_2)^2+(y_1-y_2)^2} \tag{1}$$

定义 2　轨迹　一个移动对象Q，它的运动轨迹T是在样本时间内具体的位置集，可以表示为

$$T=\left\{\mathrm{ID}_Q,\left(x_1,y_1,t_1\right),\left(x_2,y_2,t_2\right),\cdots,\left(x_n,y_n,t_n\right)\right\},\ t_1<t_2<\cdots<t_n \tag{2}$$

其中，ID_Q表示移动对象Q的轨迹标识，(x_i,y_i,t_i)表示移动对象Q在时间t_i的样本位置。

定义 3　安全多方计算协议　假设有n个参与者$P_1,P_2,\cdots,P_n$，它们通过密码学协议共同计算某个给定的函数$f(x_1,x_2,\cdots,x_n)=(y_1,y_2,\cdots,y_n)$，其中函数$f$是一个概率函数，$x_1,x_2,\cdots,x_n$分别为参与者$P_1,P_2,\cdots,P_n$的秘密输入，协议结束后，$P_1,P_2,\cdots,P_n$

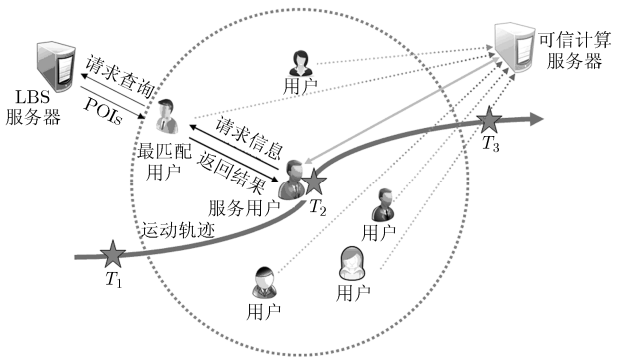


图 1　BAFM 轨迹隐私保护模型

分别得到 $y_1, y_2, \cdots, y_n$。协议要求每个参与者 P_i 除了知道 (x_i, y_i) 之外，不能得到任何信息。

定义 4 内积安全计算 假设 $\boldsymbol{X}$，$\boldsymbol{Y}$ 为实数向量空间 R^n 中的任意两个向量，$\boldsymbol{X}=(x_1,x_2,\cdots,x_n)$，$\boldsymbol{Y}=(y_1,y_2,\cdots,y_n)$，则向量 $\boldsymbol{X}$，$\boldsymbol{Y}$ 的内积为

$$\langle \boldsymbol{X},\boldsymbol{Y}\rangle = x_1y_1 + x_2y_2 + \cdots + x_ny_n \tag{3}$$

2.3 安全模型

对隐私模型进行攻击时，攻击者的背景知识非常关键。根据已有的研究[12,13]，该隐私方法安全模型可分为：弱攻击者攻击模型和强攻击者攻击模型。

(1)弱攻击者攻击模型：在弱攻击者攻击模型中，攻击者具有很少关于用户的背景知识。通常攻击者通过侦听不安全的无线信道，试图得到一些信息，从中推断出用户的敏感信息，如用户的敏感位置、真实身份和兴趣爱好等。本文方法中，攻击者试图窃听服务用户与 LBS 服务器之间的通信信道，分析代理转发的信息进行攻击。

(2)强攻击者攻击模型：在强攻击者攻击模型中，攻击者能监视整个系统中特定用户的行为记录。本方法中的LBS服务器和代理可能成为潜在的强攻击者。LBS 服务器管理所有用户的 LBS 查询数据，服务提供商因利益关系，可能会泄露 LBS 服务器中敏感信息给第三方。代理在服务用户和 LBS 服务器之间转发信息，也可能会泄露转发的信息或对信息进行用户行为分析。

3 基于代理转发机制的轨迹隐私保护方法

MSN中基于代理转发机制的轨迹隐私保护方法，主要分为查找代理、代理转发和服务器查询3个过程，相关的符号描述如表1所示。

表 1 BAFM隐私保护方法中的符号描述

符号	描述	符号	描述
MSG_{U2A}	LBS 服务用户向代理发送的信息	ID_U	服务用户的身份
MSG_{A2S}	代理转发给LBS服务器的信息	ID_{p_i}	t_i 时刻代理的身份
E	非对称加密函数	L_i	t_i 时刻服务用户的位置
En	对称加密函数	Q	服务用户的查询内容
PK_S	LBS服务器的公钥	MSG	服务用户兴趣点的集合
SK_S	LBS服务器的私钥	MSG_{S2A}	LBS服务器发给代理的消息
K_S	对称加密密钥	MSG_{A2U}	代理转发给服务用户的消息
t_i	服务用户发出LBS的时间点		

服务用户 U 的请求信息定义为

$$\mathrm{MSG}_{U2A} = \left\{\mathrm{ID}_U, E_{\mathrm{PK}_S}\left(T_i, L_i, Q, K_S\right)\right\} \tag{4}$$

其中，ID_U 表示服务用户 U 的身份标识，T_i 和 L_i 表示服务用户发出 LBS 查询时的时间和位置，Q 表示服务用户需要查询的内容；E 是非对称加密函数；PK_S 是 LBS 服务器的公钥；K_S 是 LBS 服务器和服务用户的对称加密密钥，它封装在请求信息中传递给 LBS 服务器。

3.1 查找代理

在查找最匹配用户做代理的过程中，利用安全多方计算和内积安全计算进行隐私匹配，以确保用户之间属性信息的隐私[14,15]。MSN 中的用户都能获得当前的位置和运动方向，因此服务用户匹配过程中可定义两个属性：距离(D)和角度差(θ)。D 表示服务用户和被匹配用户之间的距离，$D\in[0,R]$，R 为 MSN 覆盖范围的半径；θ 表示服务用户和被匹配用户之间的运动方向角度差，$\theta\in[0, 180^\circ]$。假设 A，B 是移动对象 2 维平面的位置坐标，在时间 Δt 内能获得两个不同的权重矢量 $\boldsymbol{a}$ 和 $\boldsymbol{b}$，则 A，B 之间的角度差 θ 为

$$\theta = \arccos\left(\frac{\boldsymbol{a}\bullet\boldsymbol{b}}{|\boldsymbol{a}|\ |\boldsymbol{b}|}\right) \tag{5}$$

根据用户的两个共同属性以及它们的权重创建属性矩阵 $\boldsymbol{M}_{L\times 2}$，其中，行向量 L 表示属性的权重，列向量2表示共同属性的数目。

$$\boldsymbol{M}_{L\times 2} = \begin{bmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \\ \vdots & \vdots \\ m_{L1} & m_{L2} \end{bmatrix} \tag{6}$$

假如两个属性权重能被分成 L 级，i 表示属性的权重，$i\in[1, L]$。为了抵制推导攻击，选择离服务用户最远且运动方向差异最大的用户做代理，因此

服务用户的属性矩阵 $\boldsymbol{A}_{L\times 2}$ 可定义为：$\boldsymbol{A}_{L\times 2}=\begin{bmatrix}0 & 0\\ 0 & 0\\ \vdots & \vdots\\ 1 & 1\end{bmatrix}$，其中 $m_{ij}\in \boldsymbol{A}_{L\times 2}$；当 $i=L$，$m_{Lj}=1$；$i\neq L$，$m_{ij}=0$。权重矩阵 $\boldsymbol{W}_{L\times L}$ 表示用户的个人属性偏好，其元素值 W_{ij} 由式(7)可得。

$$\left(W_{ij}\right)_{L\times L}=\begin{cases}i, & i=j\\ i-|i-j|, & i-|i-j|>1\\ 1, & i-|i-j|\le 1\end{cases} \tag{7}$$

服务用户加密过程如表2所示。

表2 服务用户加密过程

算法1 服务用户加密过程

输入：服务用户的属性矩阵 $\boldsymbol{A}_{L\times 2}$

输出：加密矩阵 $\boldsymbol{A}^{*}_{L\times 2}$

(1)随机选择两个大素数 α，β，且 $|\alpha|=256$，$\beta>3L^2\alpha^2$；

(2)任意生成两个矩阵 $\boldsymbol{P}_{L\times 2}$，$\boldsymbol{R}_{L\times 2}$，$\forall p_{ij}\in \boldsymbol{P}_{L\times 2}$，$\forall r_{ij}\in \boldsymbol{R}_{L\times 2}$，且

$$\sum_{i=1}^{L}\sum_{j=1}^{2}p_{ij}<(a-2L),\ \ \left|r_{ij}\beta\right|\approx 1024,\ 1\le i\le L,1\le j\le 2$$

(3) $\forall a_{ij}\in \boldsymbol{A}_{L\times 2},\forall a^{*}_{ij}\in \boldsymbol{A}^{*}_{L\times 2},k_i\in \boldsymbol{K}$；

(4)计算 $\begin{cases}a^{*}_{ij}=\alpha+p_{ij}+r_{ij}\beta, & a_{ij}=1\\ a^{*}_{ij}=p_{ij}+r_{ij}\beta, & a_{ij}=0\end{cases}$；

(5)可得加密矩阵 $\boldsymbol{A}^{*}_{L\times 2}$。

在匹配用户计算过程中，服务用户首先对自身属性矩阵加密，如算法1所示。通过计算得到加密矩阵 $\boldsymbol{A}^{*}_{L\times 2}$，以隐藏个人信息，再发送给可信计算服务器。同时 n 个被匹配用户将自身的属性矩阵 $\boldsymbol{B}_{L\times 2}$ 进行转置得到 $\boldsymbol{B}^{\mathrm{T}}_{L\times 2}$，并输入到可信计算服务器。然后可信计算服务器对被匹配用户 $P_i\ (1<i<n)$ 与服务用户进行匹配值计算，得到匹配值 φ_i，计算过程如算法2所示。通过该算法可信计算服务器可得到 n 个匹配值 φ_i，φ_i 值越大表示越匹配。因此服务用户选择 φ_i 值最大的被匹配用户 P_i 做为代理。

用户匹配值计算过程如表3所示。

3.2 代理转发

代理收到服务用户的转发请求后，首先从 MSG_{U2A} 中得到信息参数 ID_U，并存储在代理的文件列表中。同时将 MSG_{U2A} 中的 ID_U 换成代理的 ID_{P_i}，则代理转发的信息为 MSG_{A2S}，其中 ID_{P_i} 为 t_i 发出查询时找到的代理 ID，也是服务用户的假 ID。

表 3 用户匹配值计算

算法2 用户匹配值计算过程

输入　服务用户属性矩阵 $\boldsymbol{A}^{*}_{L\times 2}$，被匹配用户属性矩阵 $\boldsymbol{B}^{\mathrm{T}}_{L\times 2}$；

输出　匹配值 φ

(1)计算 $\boldsymbol{D}=(d_{ij})_{L\times L}=\boldsymbol{A}^{*}_{L\times 2}*\boldsymbol{B}^{\mathrm{T}}_{L\times 2}$；

(2) 转换　$\boldsymbol{T}^{*}=\left(t_{ij}-(t_{ij}\bmod\alpha^2)\right)\big/\alpha^2$，$t_{ij}=(d_{ij}+k_i)\bmod\beta$，$d_{ij}\in \boldsymbol{D}_{L\times L}$，$k_i\in K$；

(3)考虑相关权重并计算 $\boldsymbol{H}_{L\times L}=\left(h_{ij}\right)_{L\times L}=\boldsymbol{T}^{*}_{L\times L}\cdot\boldsymbol{W}_{L\times L}$；

(4)计算得到匹配值 $\varphi=\sum_{i=1}^{L}\sum_{j=1}^{L}h_{ij}$；

(5)返回 φ。

$$\mathrm{MSG}_{A2S}=\left\{\mathrm{ID}_{P_i},E_{\mathrm{PK}_S}\left(T_i,L_i,Q,K_S\right)\right\} \tag{8}$$

当代理收到结果信息 MSG_{S2A} 时，首先从文件列表中恢复服务用户的 ID_U，然后再转发结果信息给服务用户。从代理转发到服务用户的结果信息 MSG_{A2U} 为

$$\mathrm{MSG}_{A2U}=\{\mathrm{ID}_U,\mathrm{En}_{K_S}(\mathrm{MSG})\} \tag{9}$$

服务用户获得结果信息 MSG_{A2U} 后，使用密钥 K_S 解密 $\mathrm{En}_{K_S}(\mathrm{MSG})$ 得到查询结果 MSG。

3.3 服务器查询

LBS服务器收到代理转发的信息 MSG_{A2S} 后，首先使用服务器的私钥 SK_S 解密 MSG_{A2S} 中的 $E_{\mathrm{PK}_S}(T_i,L_i,Q,K_S)$，从中获得服务用户需要查询的位置 L_i 和查询内容 Q 等信息，然后服务器根据这些参数用 K 最近邻(K-Nearest Neighbor, KNN)搜索算法，在数据库中进行搜索，可得到查询结果 MSG。

$$\mathrm{MSG}=\left\{\text{set of POIs}\right\} \tag{10}$$

LBS服务器搜索出查询结果 MSG 后，用对称加密函数 En 以及从 $E_{\mathrm{PK}_S}(T_i,L_i,Q,K_S)$ 获得的密钥 K_S 加密查询结果 MSG，得到 $\mathrm{En}_{K_S}(\mathrm{MSG})$，并将 $\mathrm{En}_{K_S}(\mathrm{MSG})$ 与代理 ID_{P_i} 组成结果信息 MSG_{S2A} 返回给代理。

$$\mathrm{MSG}_{S2A}=\left\{\mathrm{ID}_{P_i},\mathrm{En}_{K_S}(\mathrm{MSG})\right\} \tag{11}$$

4 安全性分析

抵制强攻击者攻击　当LBS服务器成为强攻击者时，BAFM方法中的服务用户以代理 ID_{P_i} 在LBS服务器进行查询，LBS服务器记录的是与代理 ID_{P_i} 相关的行为信息。同时在服务用户移动的过程中，找到的代理 ID_{P_i} 是动态变化的，且代理之间没有关联性。因此，LBS服务器不能通过任意的代理身份 ID_{P_i} 识别出用户的真实身份 ID_U。当代理成为强攻击者时，代理转发的 $E_{\mathrm{PK}_S}(T_i,L_i,Q,K_S)$，$\mathrm{En}_{K_S}(\mathrm{MSG})$ 是使用非对称加密 E 和对称加密 En 加密的，代理没有

密钥SK_S或K_S，它将不能解密转发的信息MSG_{A2S}与MSG_{A2U}，因此，代理不可能通过转发的信息泄露服务用户的轨迹隐私。由上述可知，BAFM方法能有效抵制强攻击者的攻击。

抵制弱攻击者攻击 当攻击者窃听服务用户与代理之间的消息MSG_{U2A}和MSG_{A2U}时，攻击者只能从$\{\mathrm{ID}_U, E_{\mathrm{PK}_S}(T_i, L_i, Q, K_S)\}$，$\{\mathrm{ID}_U, \mathrm{En}_{K_S}(\mathrm{MSG})\}$得到服务用户的身份$\mathrm{ID}_U$，因为其它信息通过非对称加密$E$和对称加密En进行了加密，攻击者没有私钥$\mathrm{SK}_S$和密钥$K_S$，不能解密获得有效信息。当攻击者窃听代理与LBS服务器之间的信息MSG_{A2S}和MSG_{S2A}时，同样攻击者从$\{\mathrm{ID}_{P_i}, E_{\mathrm{PK}_S}(T_i, L_i, Q, K_S)\}$，$\left\{\mathrm{ID}_{P_i}, \mathrm{En}_{K_S}(\mathrm{MSG})\right\}$中只能得到代理身份$\mathrm{ID}_{P_i}$。即使攻击者同时得到$\mathrm{ID}_U$和$\mathrm{ID}_{P_i}$，它也不能与具体的查询信息相关联，因此该方法能有效抵制弱攻击者的攻击，攻击者不能识别出用户的轨迹。

5 实验及结果分析

实验主要从查找最匹配用户和服务器查询两方面分析该方法的性能，并与K匿名算法进行仿真实验比较。实验采用的数据集是由Brinkhoff轨迹生成器[16]生成，实验利用德国奥尔登堡市交通网络图(区域为23.57 km×26.92 km)作为输入，生成1000条移动轨迹。查询对象集数据是随机分布的，实验随机选取移动对象Tom的移动轨迹作为实验对象，Tom在不同时刻移动的轨迹如图2所示。实验参数设置如表4所示。实验的硬件环境为：Intel(R) Core(TM) i5-4590 CPU @3.30 GHz 3.30 GHz, 4.00 GB内存，操作系统为Microsoft Windows 7，采用MyEclipse 开发平台，以Java编程语言实现。

5.1 寻找最匹配用户

MSN中有K个用户，当L=15，$j=2$时，通过改变K值分析它对查找最匹配用户的影响。由图3，图4可知，在时间和通信开销上，找到最匹配用户所需的时间和通信开销随着K值的增大而增大。因为用户数目越多，通过安全多方计算进行隐私匹配找到最匹配用户花费的时间就越多，同时可信服务器需要与更多的用户进行通信。因此，K值越大，找到最匹配用户所需的时间和通信开销就越多。

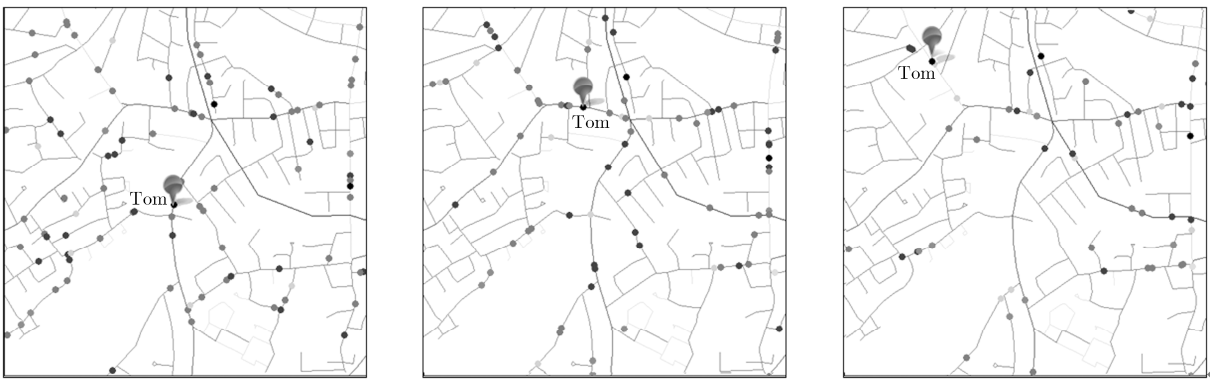
表 4 实验参数设置

参数	数值
移动对象	1000
移动速度	中速
属性数目j	2
POIs	500~1500
用户数K	10~100
属性权重L	3~30

当$j=2$，$K=20$时，通过改变其L值来分析对查找最匹配用户的影响。由图5，图6可知，找到最匹配用户所需的时间和通信开销都随着L值的增大而增大。因为L值越大，构成矩阵中行的数目就越多，需要处理的数据量就越多，用户需匹配的信息也就越多。因此，L值越大，找到最匹配用户所需的时间和通信开销就越多。

5.2 在 LBS 服务器查询时的性能对比

在POIs=500且其它参数不变的情况下，将BAFM方法与文献[17]，文献[18]中Iclique, L2P2匿名方法进行比较，对比3种方法随K值变化对LBS服务器性能的影响。由图7，图8可知，在LBS服务器处理时间和通信开销上，Iclique, L2P2匿名方法随着K值的增大而增大，而BAFM方法基本保持不变。这是因为K值越大，Iclique, L2P2匿名方法形成的匿名域就越大，LBS服务器需要查询的POIs就越多，所需的处理时间和通信开销就越多。BAFM方法发送到服务器查询的位置是精确的，因此查询时间和通信开销不会随着K值的增大而增大。



(a) t_1时刻的位置 (b) t_2时刻的位置 (c) t_3时刻的位置

图 2 移动对象Tom的移动轨迹

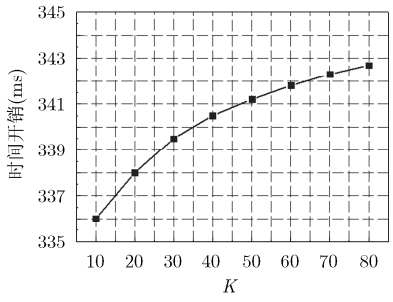


图3 K 值变化下的时间开销

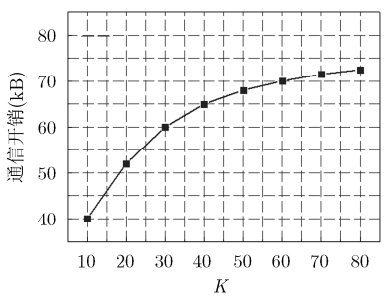


图4 K 值变化下的通信开销

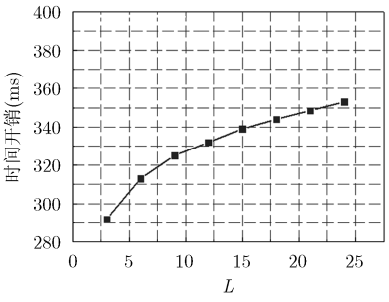


图5 L 值变化下的执行时间

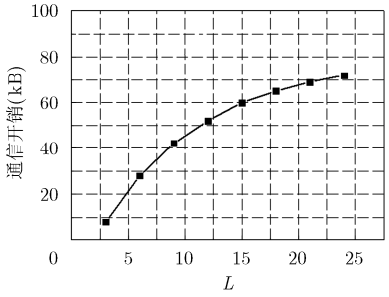


图 6 L 值变化下的通信开销

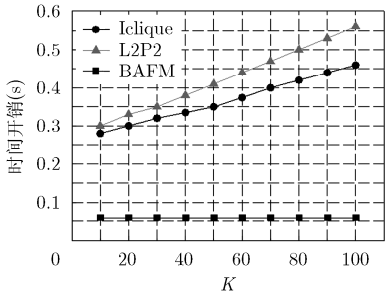


图 7 K 值变化下的时间开销对比

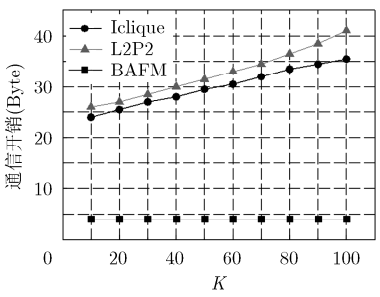


图 8 K 值变化下的通信开销对比

在其它参数不变的情况下，通过改变 K 值和设定不同的POIs值，对比BAFM方法对LBS服务器性能的影响。由图9，图10可知，在LBS服务器的时间和通信开销不会随着 K 值的增大而变化，但POIs值越大，在LBS服务器端所需的时间和通信开销就越大。因为BAFM方法中服务用户发送到LBS服务器查询的位置始终是精确的，不会随着 K 值而变化。因此，通过该实验进一步说明，在LBS服务器的时间和通信开销上，BAFM方法与 K 值无关。

6　结束语

基于位置服务的快速发展，位置隐私问题已成为当前隐私保护方向的一个研究热点。本文提出一种基于MSN代理转发机制的轨迹隐私保护方法，通过代理转发信息到LBS服务器查询，隐藏用户真实轨迹和LBS服务器的关联，保证用户的轨迹隐私。该方法利用安全多方计算和内积计算进行隐私匹配，在MSN中找到最匹配的用户做代理，在保证用户之间隐私的情况下，提高查询最匹配用户的效率。安全分析表明该方法能抵制弱敌手和强敌手攻击模型的隐私攻击。同时，通过对比实验验证该方法在服务器具有较低的计算和通信开销。当然该方法还有待改进的地方，例如，在MSN中代理转发查询信息时，只是假定用户遵守相互转发机制，因此在下一步工作中，我们尝试使用转发激励机制，激发MSN中的用户相互转发信息。

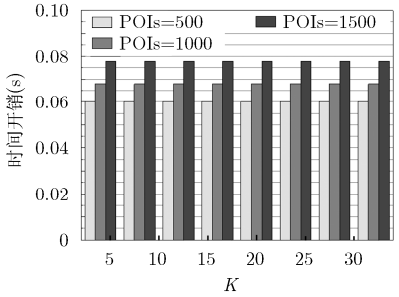


图 9 POIs 值变化下的时间开销对比

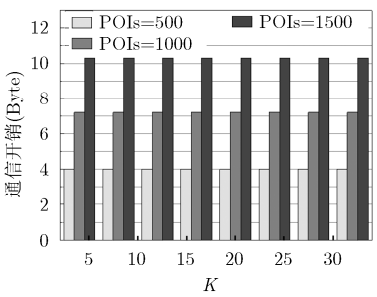


图 10 POIs 值变化下的通信开销对比

参 考 文 献

[1] LU Rongxing, LIN Xiaodong, LIANG Xiaohui, *et al.* A dynamic privacy preserving key management scheme for location-based services in vanets[J]. *IEEE Transactions on Intelligent Transportation Systems*, 2012, 13(1): 127–139. doi: 10.1109/TITS.2011.2164068.

[2] 霍峥, 孟小峰, 黄毅. PrivateCheckIn: 一种移动社交网络中的轨迹隐私保护方法[J]. 计算机学报, 2013, 36(4): 716–726. doi: 10.3724/SP.J.1016.2013.00716.
HUO Zheng, MENG Xiaofeng, and HUANG Yi. PrivateCheckIn: Trajectory privacy-preserving for check-in services in MSNS[J]. *Chinese Journal of Computers*, 2013, 36(4): 716–726. doi: 10.3724/SP.J.1016.2013.00716.

[3] LEI P R, PENG W C, SU I J, *et al*. Dummy-based schemes for protecting movement trajectories[J]. *Journal of Information Science and Engineering*, 2012, 28(2): 335–350.

[4] YOU T H, PENG W C, and LEE W C. Protecting moving trajectories with dummies[C]. Proceedings of the 8th International Conference on Mobile Data Management, Mannheim, Germany, 2007: 278–282. doi: 10.1109/MDM. 2007.58.

[5] TERROVITIS M and MAMOULIS N. Privacy preservation in the publication of trajectories[C]. Proceedings of the 9th International Conference on Mobile Data Management, Beijing, 2008: 65–72. doi: 10.1109/MDM. 2008.29.

[6] 赵婧, 张渊, 李兴华, 等. 基于轨迹频率抑制的轨迹隐私保护方法[J]. 计算机学报, 2014, 37(10): 2096–2106. doi: 10.3724/SP.J.1016.2014.02096.
ZHAO Jing, ZHANG Yuan, LI Xinghua, *et al*. A trajectory privacy protection approach via trajectory frequency suppression[J]. *Chinese Journal of Computers,* 2014, 37(10): 2096–2106. doi: 10.3724/SP.J.1016.2014.02096.

[7] HWANG R H, HSUEH Y L, and CHUNG H W. A novel time-obfuscated algorithm for trajectory privacy protection[J]. *IEEE Transactions on Services Computing*, 2014, 7(2): 126–139. doi: 10.1109/TSC.2013.55.

[8] 朱怀杰, 王佳英, 王斌, 等. 障碍空间中保持位置隐私的最近邻查询方法[J]. 计算机研究与发展, 2014, 51(1): 115–125. doi: 10.7544/issn1000-1239.2014.20130694.
ZHU Huaijie, WANG Jiaying, WANG Bin, *et al*. Location privacy preserving obstructed nearest neighbor queries[J]. *Journal of Computer Research and Development*, 2014, 51(1): 115–125. doi: 10.7544/issn1000-1239.2014.20130694.

[9] 杨静, 张冰, 张健沛, 等. 基于图划分的个性化轨迹隐私保护方法[J]. 通信学报, 2015, 36(3): 1–11. doi: 10.11959/j.issn.1000-436x.2015053.
YANG Jing, ZHANG Bing, ZHANG Jianpei, *et al*. Personalized trajectory privacy preserving method based on graph partition[J]. *Journal on Communications*, 2015, 36(3): 1–11. doi: 10.11959/j.issn.1000-436x.2015053.

[10] 王超, 杨静, 张健沛. 基于轨迹位置形状相似性的隐私保护算法[J]. 通信学报, 2015, 36(2): 144–157. doi: 10.11959/j.issn.1000-436x.2015043.
WANG Chao, YANG Jing, and ZHANG Jianpei. Privacy preserving algorithm based on trajectory location and shape similarity[J]. *Journal on Communications*, 2015, 36(2): 144–157. doi: 10.11959/j.issn.1000-436x.2015043.

[11] XU T and CAI Y. Exploring historical location data for anonymity preservation in location-based services[C]. Proceedings of the 27th International Conference on Computer Communications(INFOCOM 2008), Toronto, Canada, 2008: 547–555. doi: 10.1109/INFOCOM.2008.103.

[12] GAO Sheng, MA Jianfeng, SHI Weisong, *et al*. TrPF: a trajectory privacy-preserving framework for participatory sensing[J]. *IEEE Transactions on Information Forensics and Security*, 2013, 8(6): 874–887. doi: 10.1109/TIFS.2013. 2252618.

[13] NIU Ben, ZHU Xiaoyan, CHI Haotian, *et al*. 3PLUS: privacy-preserving pseudo-location updating system in location-based services[C]. 2013 IEEE Wireless Communications and Networking Conference, Shanghai, China, 2013: 4564–4569. doi: 10.1109/WCNC.2013.6555314.

[14] GENKIN D, ISHAI Y, and POLYCHRONIADOU A. Efficient multi-party computation: from passive to active security via secure SIMD circuits[C]. Proceedings of the 35th Annual Cryptology Conference, Santa Barbara, USA, 2015: 721–741. doi: 10.1007/978-3-662-48000-7-35.

[15] ZHU Xiaoyan, LIU Jie, JIANG Shunrong, *et al*. Efficient weight-based private matching for proximity-based mobile social networks[C]. 2014 IEEE International Conference on Communications, Sydney, Australia, 2014: 4114–4119. doi: 10.1109/ICC.2014.6883965.

[16] BRINKHOFF T. Generating traffic data[J]. *Bulletin of the Technical Committee Data Engineering*, 2003, 26(2): 19–25.

[17] PAN Xiao, XU Jianliang, and MENG Xiaofeng. Protecting location privacy against location-dependent attacks in mobile services[J]. *IEEE Transactions on Knowledge and Data Engineering*, 2012, 24(8): 1506–1519. doi: 10.1109/TKDE. 2011.105.

[18] WANG Yu, XU Dingbang, HE Xiao, *et al*. L2p2: Location-aware location privacy protection for location-based services[C]. Proceedings IEEE INFOCOM, Orlando, Florida USA, 2012: 1996–2004. doi: 10.1109/INFOCOM.2012. 6195577.

张少波： 男，1979 年生，博士生，讲师，研究方向为云安全、隐私保护.

Md Zakirul Alam Bhuiyan： 男，1983 年生，博士，助理教授，研究方向为云计算、数据挖掘和隐私保护.

刘 琴： 女，1982 年生，博士，助理教授，研究方向为云计算、大数据和隐私保护.

王国军： 男，1970 年生，博士生导师，教授，研究方向为可信计算、大数据安全和隐私保护.