基于网格标识匹配的位置隐私保护方法

张少波[①③] 刘 琴[②] 王国军*[①④]
[①](中南大学信息科学与工程学院 长沙 410083)
[②](湖南大学信息科学与工程学院 长沙 410082)
[③](湖南科技大学计算机科学与工程学院 湘潭 411201)
[④](广州大学计算机科学与教育软件学院 广州 510006)

摘 要：在基于位置的服务中，基于可信第三方模型是当前位置隐私保护中的主要模型，但该模型存在一定的隐私泄露风险。该文提出一种基于网格标识匹配(GIM)的位置隐私保护方法，用户首先将查询区域划分为网格，并结合保序对称加密和 K 匿名技术，在匿名器形成 K 匿名，然后利用网格标识匹配返回查询结果给用户。在查询的过程中，匿名器并不知道用户的具体位置，加强了该模型中用户位置的隐私保护。同时中间匿名器仅进行简单的比较和匹配，有效缓解了匿名器的性能瓶颈问题。安全分析表明该方法能有效保护用户的位置隐私；并且通过实验验证该方法能有效减小匿名器的处理时间开销。

关键词：位置隐私；网格标识匹配；保序对称加密；K 匿名
中图分类号： TP393 **文献标识码**： A **文章编号**：1009-5896(2016)09-2173-07
DOI: 10.11999/JEIT160350

The Method of Location Privacy Protection Based on Grid Identifier Matching

ZHANG Shaobo[①③] LIU Qin[②] WANG Guojun[①④]
[①](*School of Information Science and Engineering*, *Central South University*, *Changsha* 410083, *China*)
[②](*College of Computer Science and Electronic Engineering*, *Hunan University*, *Changsha* 410082,*China*)
[③](*School of Computer Science and Engineering*, *Hunan University of Science and Technology*, *Xiangtan* 411201, *China*)
[④](*School of Computer Science and Educational Software*, *Guangzhou University*, *Guangzhou* 510006, *China*)

Abstract: The model based on fully-trusted third party is a major model for location privacy protection in location-based services, but the model has some risk of exposing privacy. In this paper, a location privacy protection method based on Grid Identifier Matching (GIM) is proposed. In this method the user first divides the query area into grid and combines the order-preserving symmetric encryption and K-anonymity mechanism. Then, the K-anonymity paradigm is formed in anonymizer. Finally, the query results are returned to users by utilizing GIM. In the query process, the anonymizer dose not have any knowlegdge about a user's real location, which can enhance the user's location privacy. Meanwhile, the anonymizer only does simple comparison and matching operations, which relieves effectively is performance bottleneck of the anonymizer. Security analysis shows that the proposed approach can effectively protect the user's location privacy. Experimental evaluations show that the proposed approach can decrease processing time overhead of the anonymizer.

Key words: Location privacy; Grid Identifier Matching (GIM); Order-preserving symmetric encryption; K-anonymity

1 引言

随着无线通信技术、智能终端设备和定位技术的发展，基于位置的服务(Location Based Service, LBS)发展迅速并获得广泛关注[1,2]。在LBS中，用户通过带有定位功能的设备可以获得当前位置，并向位置服务器发送查询，以获取用户位置附近的兴趣点(Points Of Interests, POIs)，例如寻找距离当前位置最近的宾馆、影院和加油站等，然而人们在享用LBS带来便利的同时，也面临着敏感信息泄露的风险[3]。根据用户发送的LBS查询，攻击者可能分析出特定用户的敏感信息，如家庭住址、生活习惯、

收稿日期：2016-04-12；改回日期：2016-07-18；网络出版：2016-08-09
*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)，中南大学中央高校基本科研业务费专项资金(2016zzts058)
Foundation Items: The National Natural Science Foundation of China (61472451, 61272151, 61402161), The Fundamental Research Funds for the Central Universities of Central South University (2016zzts058)

健康状况以及社会关系等[4]。同时位置服务提供商(Location Services Provider, LSP)也可能将用户的隐私信息泄露给第三方，这将给用户带来严重的安全隐私风险。因此，目前基于位置服务的位置隐私保护问题已引起学者的广泛关注，并迫切需要解决。

为减少隐私泄露的风险，国内外已提出一些位置隐私保护方法，采用的基本结构主要分为两类[5]：基于点对点的结构和基于可信第三方(Fully-Trusted Third Party, TTP)的中心服务器结构。在基于点对点的结构中，用户之间通过协作的方式形成K匿名域[6,7]或使用混淆的方式[8]向LBS发送查询，使LSP不知道用户的精确位置。在基于可信第三方的中心服务器结构中，引入了一个可信匿名器，作为移动用户和LSP之间的中间体[9–11]。该结构中用户首先将查询请求发送给匿名器，然后匿名器将用户的服务请求按用户的隐私需求形成一个包括K个用户的匿名域，并将它发送给LSP进行查询，得到查询结果集后再返回给匿名器，最后可信匿名器根据用户需求对候选结果集进行求精，并将精确结果返回给用户。但基于可信第三方的中心服务器结构存在两个问题：(1)匿名器知道用户的精确位置，如果它被攻击者攻破，将会带来严重的安全威胁。(2)匿名器承担着匿名、求精等繁重的计算任务，容易成为该结构中的性能瓶颈。

针对 TTP 结构存在的两个缺陷，文献[12]提出通过自定义动态网格系统，使中间第三方不知道用户的具体位置，达到保护用户位置隐私的目的。但如果用户指定的查询区域只有一个用户，LBS 服务器就会很容易指出真实的用户，暴露用户的位置隐私。针对该方法存在的缺陷，本文提出基于网格标识匹配(Grid Identifier Matching, GIM)的位置隐私保护方法，结合保序对称加密(Order-Preserving Symmetric Encryption, OPSE)和 K 匿名技术，用户首先对查询面积进行网格划分，并将能确定各用户查询区域的坐标用保序对称加密算法加密，然后发送到中间匿名器形成 K 匿名域，匿名器并不知道用户的具体位置，且它不需要完全可信，加强了对用户位置的隐私保护。同时在查询的过程中，中间匿名器仅进行简单的比较和匹配，有效缓解了匿名器的性能瓶颈问题。

2 系统模型和相关定义

2.1 系统模型

如图1所示为基于GIM的位置隐私保护模型图，系统主要由用户、匿名器和LBS服务器3类实体组成，具体工作过程为：(1)用户发送查询时，首先指定一个查询面积进行网格划分，并寻找用户附近$(K-1)$个其它用户，各用户按查询范围在网格结构上确定各自的查询区域，然后用OPSE对各确定网格查询区域的坐标进行加密，发送给匿名器；同时用户将自己指定的查询区域内的网格单元标识进行Hash并加密发送给匿名器；(2)匿名器比较用OPSE加密后的坐标大小，并根据比较结果形成包含K个用户查询区域的匿名域，然后将该匿名域发送给LSB服务器进行查询；(3)LBS服务器查询匿名域内的POIs，并将各POIs的位置以及对应的网格单元标识进行Hash并加密后返回给匿名器；(4)匿名器将各POIs位置所在的加密网格单元标识与用户需要查询区域的加密网格单元标识进行匹配，如果相等，则将该网格单元标识对应的POIs发送给用户。该方法的优点是匿名器并不知道用户的精确位置，同时它只进行简单的比较和匹配操作，加强了对用户位置的隐私保护，同时也有效缓解了匿名器的性能瓶颈问题。

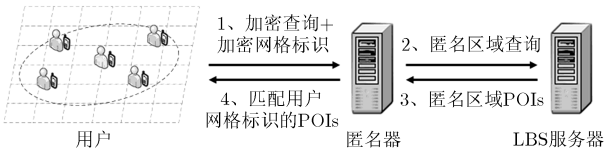


图1 基于GIM的位置隐私保护模型

2.2 保序加密

定义 1 保序加密 如果加密函数 Enc 是确定性的，那么 $\mathrm{SE}_{D,R}=(K, \mathrm{Enc}, \mathrm{Dec})$ 与明文空间 D 、密文空间 R 也是确定性的。当 $A,B\in\mathbb{N}$ 并且 $|A|\le|B|$，对于任意 $i,j\in A$，如果 $i>j$，那么 $f(i)>f(j)$，则函数 $f:A\to B$ 是保序的。对于所有 K 的输出 k，如果 $\mathrm{Enc}(K,\bullet)$ 是一个从 D 到 R 保序函数，那么确定性的加密 $\mathrm{SE}_{D,R}=(K, \mathrm{Enc}, \mathrm{Dec})$ 是保序的[13,14]。

定义2 保序对称加密 假设 $\mathrm{OPSE}=(\mathrm{KeyGen}, \mathrm{Enc}, \mathrm{Dec})$，OPSE 与明文空间 D 、密文空间 R 组成3个算法。KeyGen 是随机密钥生成算法，通过输入一个安全的参数可返回一个密钥 k；加密算法 Enc 和解密算法 Dec 是明文空间 D 和密文空间 R 的描述，用密钥 k 加密明文 m 可得到密文 c；用密钥 k 解密密文 c 可得到明文 m。并且 OPSE 保序对称加密满足不可区分选择明文攻击。假如函数 $\mathrm{LR}=(\bullet,\bullet,b)$ 表示输入 m_0,m_1 得到 $m_b, b\in\{0,1\}$，$\mathrm{OPSE}=(\mathrm{KeyGen}, \mathrm{Enc}, \mathrm{Dec})$ 是一个对称加密方案[15]。

2.3 安全模型

在位置隐私保护的研究方面，目前比较典型的攻击模型主要分为两种[16]：强攻击者攻击模型和弱攻击者攻击模型。

(1)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，本方法中的匿名器和LSP都可能成为潜在的强攻击者。因为 LBS 服务器管理所有用户的 LBS 查询数据，LSP 因利益关系，可能会泄露 LBS 服务器中敏感信息给第三方。匿名器在用户和 LBS 服务器之间进行匿名和转发信息，也可能会对用户进行行为分析，并造成信息泄露。

(2)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，攻击者通过使用背景知识或其它攻击手段，试图知道其它用户更多的个人信息。本方法中，攻击者可能试图窃听用户与 LBS 服务器之间的通信信道，分析传输过程中的数据，甚至篡改查询结果发送给用户进行攻击。

3　基于网格标识匹配的位置隐私保护方法

3.1 用户加密查询

本文假定用户的查询是范围查询，例如在市区环境下用户查询自己周围 1 km 范围内的餐馆、酒店或电影院等。用户在发送查询前，首先通过带有定位功能的设备获得自己的当前位置(x_0, y_0)，然后根据自己的查询半径R，指定一个包含用户查询范围的方形查询面积。该查询面积可由左下角坐标(x_a, y_a)和右上角坐标(x_b, y_b)确定，再将该查询面积划分为大小相等的$n \times n$网格。因此，用户指定的查询面积网格结构可表示为

$$\text{structure} \leftarrow ((x_a, y_a),(x_b, y_b), n) \tag{1}$$

在自定义的网格结构中，每个网格单元的标识可以由(c, r)唯一确定，其中c表示列标识，r表示行标识，$1 \le c, r \le n$。例如：在查询面积内任选一点(x_c, y_c)，则它所在的网格单元标识(c, r)可表示为

$$(c, r) = \left(\left\lceil \frac{x_c - x_a}{(x_b - x_a)/n} \right\rceil, \left\lceil \frac{y_c - y_a}{(y_b - y_a)/n} \right\rceil \right) \tag{2}$$

用户定义好网格结构后，然后在该网格结构上以用户当前位置(x_0, y_0)为中心，形成半径为R的圆形查询范围，并将该圆形查询范围与其覆盖的相交网格单元作为查询区域，它由左下角坐标(x_{01}, y_{01})和右上角坐标(x_{02}, y_{02})确定，其中每个网格单元有唯一的标识(c_i, r_i)。然后将该查询区域内的每个网格单元标识用哈希函数$H(\cdot)$进行 Hash 得到h_i，并使用用户随机生成的密钥K_S对它们分别进行加密，形成网格单元标识加密集S_e。

$$h_i \leftarrow H\left(c_i, r_i\right) \tag{3}$$

$$\phi_i \leftarrow \mathrm{En}_{K_S}\left(h_i\right) \tag{4}$$

$$S_e \leftarrow \{\, \phi_i \,\} \tag{5}$$

为使匿名器形成 K 匿名，用户根据 K 近邻算法[17]寻找到用户附近兴趣点相同的$(K-1)$个其它用户，它们都是可信的。然后每个用户在网格结构上分别形成半径为R的圆形查询范围，并分别确定自己的查询区域。

各用户确定自己的查询区域后，用户用 OPSE 中的KeyGen生成密钥K_{OPSE}，将各用户指定查询区域的两个坐标值分别用加密算法Enc和密钥K_{OPSE}进行加密，得到K个坐标对加密后的加密坐标集R_i，$0 \le i \le (K-1)$，并形成查询区域集region。

$$R_i \leftarrow \left\{ \left(\mathrm{Enc}_{K_{\mathrm{OPSE}}}(x_{i1}), \mathrm{Enc}_{K_{\mathrm{OPSE}}}(y_{i1}) \right), \left(\mathrm{Enc}_{K_{\mathrm{OPSE}}}(x_{i2}), \mathrm{Enc}_{K_{\mathrm{OPSE}}}(y_{i2}) \right) \right\} \tag{6}$$

$$\text{region} \leftarrow \{R_i\},\ 0 \le i \le (K-1) \tag{7}$$

用户随机生成用于加密网格单元标识的密钥K_S、加密 POIs 位置的密钥K_L、完整性验证密钥K_H以及 OPSE 中的KeyGen生成密钥K_{OPSE}，共同形成一个密钥集Key，该密钥集加密后，经匿名器发送给 LBS 服务器使用。

$$\mathrm{Key} = \left\{ K_S, K_L, K_H, K_{\mathrm{OPSE}} \right\} \tag{8}$$

用户将各用户查询区域region、加密标识集S_e、查询内容POI_type、密钥集Key以及网格结构structure组成用户的请求消息$\mathrm{MSG_{U2A}}$，其中POI_type，Key和structure使用 LBS 服务器的公钥PK_S进行非对称加密。最后，用户将请求消息$\mathrm{MSG_{U2A}}$发送给匿名器。

$$\mathrm{MSG_{U2A}} = \left\{ \text{region}, S_e, E_{\mathrm{PK}_S} \left(\text{POI\_type}, \text{Key}, \text{structure} \right) \right\} \tag{9}$$

3.2 位置坐标比较

当匿名器收到用户的请求消息$\mathrm{MSG_{U2A}}$后，匿名器首先存储加密标识集S_e，然后从查询区域集region中的R_i分别得到K个用户查询区域的加密后的位置坐标，并分别对这些加密坐标值进行比较，得到K个查询区域中左下角最小的坐标值$\mathrm{Enc}_{K_{\mathrm{OPSE}}}(x_{i1})_{\min}$，$\mathrm{Enc}_{K_{\mathrm{OPSE}}}(y_{j1})_{\min}$，$i, j \in (0, K-1)$；以及$K$个查询区域右上角最大的坐标值$\mathrm{Enc}_{K_{\mathrm{OPSE}}}(x_{u2})_{\max}$，$\mathrm{Enc}_{K_{\mathrm{OPSE}}}(y_{v2})_{\max}$，$u, v \in (0, K-1)$。在比较大小的过程中，因为这些坐标值是保序加密的，匿名器没有密钥K_{OPSE}和网格结构structure，它并不知道用户的具体位置。因此，通过比较可以确定包含K个用户查询区域的K匿名区域C_region：

$$C\_\text{region}=\Big(\Big(\text{Enc}_{K_{\text{OPSE}}}\left(x_{i1}\right)_{\min},\text{Enc}_{K_{\text{OPSE}}}\left(y_{j1}\right)_{\min}\Big),\Big(\text{Enc}_{K_{\text{OPSE}}}\left(x_{u2}\right)_{\max},\text{Enc}_{K_{\text{OPSE}}}\left(y_{v2}\right)_{\max}\Big)\Big) \tag{10}$$

最后，匿名器将 C_region 与 $E_{\text{PK}_S}(\text{POI\_type, Key, structure})$ 组成新的查询请求消息 MSG_{A2S}，再转发到 LBS 服务器查询。

$$\text{MSG}_{\text{A2S}}=\Big\{C\_\text{region},E_{\text{PK}_S}\Big(\text{POI\_type, Key, structure}\Big)\Big\} \tag{11}$$

3.3 服务器查询

LBS服务器收到匿名器转发的查询请求消息 MSG_{A2S} 后，首先使用LBS服务器私钥 SK_S 解密 MSG_{A2S} 中的 $E_{\text{PK}_S}(\text{POI\_type, Key, structure})$。然后根据 structure 中 (x_a, y_a)，(x_b, y_b) 和 n 恢复用户指定的查询面积网格结构，并获得用户需要查询的兴趣点 POI_type 以及对称加密密钥集 Key。同时LBS服务器用OPSE中的解密算法 Dec 以及密钥 K_{OPSE}，解密查询区域 C_region 中的两个坐标，可以在网格结构上确定K匿名域。最后LBS服务器根据 POI_type 查询匿名域的POIs，共得到 t 个POIs。如果第 j 个POI的位置为 (x_j, y_j) $(1\le j\le t)$，则它所在的网格单元标识为 $\left(c_j, r_j\right)=\left(\left\lceil\frac{x_j-x_a}{(x_b-x_a)/n}\right\rceil,\left\lceil\frac{y_j-y_a}{(y_b-y_a)/n}\right\rceil\right)$。

LBS服务器将查询到的每个POI位置 (x_j, y_j) 所在的网格单元标识 (c_j, r_j) 使用哈希函数 $H(\bullet)$ 进行Hash得到 h_j，并将 h_j 分别进行加密得到 ϕ_j。同时对每个POI的位置 (x_j, y_j) 用密钥 K_L 进行加密可得 l_j。为防止查询得到的POIs，在匿名器转发的过程中被篡改或添加假的POIs，通过引入消息完整性验证机制，对每个POI的 ϕ_j 和 l_j 使用哈希函数 $H(\bullet)$ 进行哈希，并用密钥 K_H 进行加密得到 ψ_j，然后将它与 ϕ_j，l_j 组成查询结果集 MSG_{S2A}，返回给匿名器。

$$h_j\leftarrow H\left(c_j, r_j\right) \tag{12}$$

$$\phi_j\leftarrow \text{En}_{K_S}\left(h_j\right) \tag{13}$$

$$l_j\leftarrow \text{En}_{K_L}\left(x_j, y_j\right) \tag{14}$$

$$\psi_j\leftarrow \text{En}_{K_H}\left(H\left(\phi_j, l_j\right)\right) \tag{15}$$

$$\text{POI}_j=\left(\phi_j, l_j, \psi_j\right) \tag{16}$$

$$\text{MSG}_{\text{S2A}}=\{\text{POI}_j\},\quad 1\le j\le t \tag{17}$$

3.4 网格标识匹配

匿名器收到查询结果集 MSG_{S2A} 后，将 t 个POIs的加密标识 ϕ_j 与用户发送到匿名器保存的加密标识集 S_e 中的加密标识进行比较。如果 ϕ_j 与 S_e 中的 ϕ_i 匹配，则表示第 j 个POI是用户查询区域需要查询的POI。因此，匿名器查找每个匹配的 $\text{POI}(l_j, \psi_j)$，并将其组成用户查询区域POIs集 MSG_{A2U} 转发给用户。

$$\text{MSG}_{\text{A2U}}=\{\text{POI}(l_j, \psi_j)\},\ 1\le j\le t \tag{18}$$

3.5 用户求精结果

用户收到查询区域 POIs 集 MSG_{A2U} 后，用密钥 K_L 解密 l_j，得到 POI 的精确位置 (x_j, y_j)。然后用户需要重新计算 $H(\phi_j, l_j)$ 值并加密，以验证是否与 ψ_j 相等。如果相等，则说明该 POI 没有被篡改，它是正确的结果。最后用户计算包含在用户查询范围内的 POIs，得到精确的查询结果。

4 安全性分析

本节主要分析 GIM 位置隐私保护模型分别抵制强攻击者和弱攻击者的攻击，本模型中将 LSP 和匿名器作为强攻击者，窃听者为弱攻击者。具体分析如下。

4.1 抵制 LSP 的攻击

挑战：LSP管理所有用户的查询数据，LSP作为强攻击者想从这些数据中推断出一些用户敏感信息，从而揭露用户的精确位置。如果LSP可以确定地知道查询内容所对应用户的精确位置，那么LSP将赢得这个游戏。

定理 1 GIM 位置隐私保护方法能抵制 LSP 的推断攻击。

证明 本方案中，用户发送的查询经匿名器转发给LSP的查询请求为 MSG_{A2S}，MSG_{A2S} 中包括匿名域 C_region，兴趣点类型 POI_type，密钥集 Key 以及网格结构 structure，从这些信息中，LSP不能获得用户的精确位置。因为在查询过程中，LBS服务器根据 structure，POI_type 查询 C_region 中的每个网格的POIs，然后返回给匿名器，而LSP仅知道该用户的 POI_type，但它并不能与具体的用户关联。而且该匿名区域至少包括 K 个用户，LSP能猜到是某个用户的概率最多只有 $1/K$。因此，LSP通过这些数据不能得到用户的精确位置。 证毕

4.2 抵制匿名器的攻击

挑战：匿名器在用户和 LBS 服务器之间，负责对用户进行 K 匿名，同时对查询请求、查询结果等信息的进行转发，它作为强攻击者想从这些数据中能推断出一些用户的敏感信息，从而揭露用户的精确位置。如果匿名器可以确定地知道查询内容所对应用户的精确位置，那么匿名器将赢得这个游戏。

定理 2　GIM位置隐私保护方法能抵制匿名器的推断攻击。

证明　本方案中，用户发送查询时，通过寻找附近$(K-1)$个其它用户，分别指定查询区域发送到匿名器。匿名器得到的是用保序对称加密后能确定查询区域的坐标，它只能对它们进行大小比较，但并不知道它们具体值的含义。因此，通过在匿名器进行K匿名，匿名器并不知道用户的精确位置。用户发送给匿名器的查询请求为$\mathrm{MSG}_{\mathrm{U2A}}$，它包括region，$S_e$和$E_{\mathrm{PK}_S}(\mathrm{POI_type, Key, structure})$ 3个参数，它们都是加密的，匿名器没有密钥K_{OPSE}以及LBS服务器的私钥SK_S，它不能解密region以及$E_{\mathrm{PK}_S}(\mathrm{POI_type, Key, structure})$，所以匿名器不能从$\mathrm{MSG}_{\mathrm{U2A}}$得到有用的信息。同时匿名器收到LBS服务器返回的查询结果信息为$\mathrm{MSG}_{\mathrm{S2A}}=\{\mathrm{POI}_j\}$，而$\mathrm{POI}_j=(\phi_j,l_j,\psi_j)$，$\mathrm{MSG}_{\mathrm{S2A}}$只与POIs的位置$(x_j,y_j)$以及所在网格单元标识$(c_j,r_j)$有关，而且它们是加密的，匿名器从中得不到有用的信息。因此，从以上分析中可知，匿名器不可能得到用户的精确位置。　　证毕

4.3 抵制窃听者的攻击

挑战：弱攻击者通过侦听不安全的无线信道，试图从这些数据中能推断出一些用户的敏感信息，从而揭露用户的精确位置，甚至攻击者有意篡改用户的查询结果。如果弱攻击者知道用户的精确位置或能成功篡改用户的查询结果，那么弱攻击者将赢得这个游戏。

定理 3　GIM位置隐私保护方法能抵制侦听者的攻击。

证明　在用户发送给LBS服务器的查询请求消息$\mathrm{MSG}_{\mathrm{U2A}}$，$\mathrm{MSG}_{\mathrm{A2S}}$中，$C\_\mathrm{region}$，region，$S_e$和$E_{\mathrm{PK}_S}(\mathrm{POI_type, Key, structure})$都是通过对称加密Enc，En和非对称加密$E$进行加密的，攻击者没有密钥，不能解密这些参数，从而得不到有用的信息。在用户查询结果返回给用户的$\mathrm{MSG}_{\mathrm{S2A}}$，$\mathrm{MSG}_{\mathrm{A2U}}$中，$\mathrm{POI}_j$中网格单元标识的哈希值加密后的$\phi_j$，POIs的位置加密后的$l_j$以及完整性验证函数$\psi_j$都是通过对称加密函数进行加密的，同样攻击者得不到密钥，也得不到有用的信息。如果攻击者在结果返回的过程中，试图篡改POIs的位置，或加入一些假POIs的位置发送给用户，使用户得到错误的查询结果。GIM方案在LBS服务器端引入消息完整性验证机制，$\psi_j \leftarrow \mathrm{En}_{K_H}(H(\phi_j,l_j))$，用户得到POIs的位置$(x_j,y_j)$后，先用$\mathrm{En}_{K_H}(H(\phi_j,l_j))$验证$\psi_j$值是否相等，如果不相等，则说明该查询结果的完整性被破坏，用户丢弃该查询结果并进行重新查询。因此，弱攻击者既不能得到用户的精确位置，也不能破坏查询结果的完整性。　　证毕

5　实验及结果分析

本节主要通过实验验证GIM方案在相关参数变化下，用户每次查询时，对平均计算时间和平均通信开销的影响；同时在匿名器的平均计算时间以及平均通信开销上，与TTP[10], ELPP[5]方法进行仿真实验比较。实验采用由Brinkhoff移动对象生成器[18]，并利用德国奥尔登堡市交通网络图作为输入生成10000个移动用户，如图2所示。实验随机选取某时刻的移动对象Tom作为实验对象，Tom寻找到邻近的其它2和3个用户的位置分布情况如图3所示。实验参数设置如表1所示。实验的硬件环境为：Intel(R)Core(TM)i5-4590CPU@3.30 GHz3.30 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 参数变化对 GIM 性能的影响

当$K=25$时，通过改变查询半径R和网格划分数目n值，分析对GIM性能的影响。由图4可知，在时间和通信开销上，查询的时间和通信开销都随着R值的增大而增大，同时n值越大，时间和通信开销就越大。因为查询半径R越大，形成的匿名域就越大，查询所需的时间和通信量就会越多。同时n

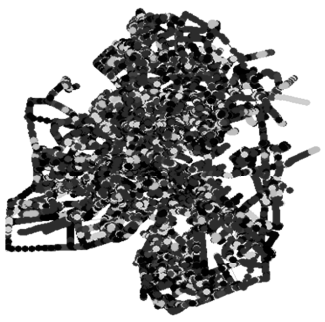
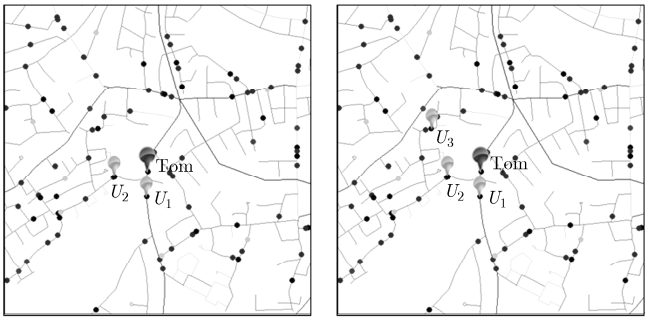


图 2　生成10000个移动用户



(a) K=3　　(b) K=4

图 3　移动用户Tom找到的邻近用户

表1 实验参数设置

参数	值(个)	参数	值(km)
用户数	10000	R	0.5~1.0
POIs	10000	(x_a, y_a)	(0, 0)
K	5~55	(x_b, y_b)	(10, 10)
n	100~300		

值越大，网格划分时网格单元粒度就越小，用户指定的查询区域覆盖的网格单元就越多，需要传输到匿名器保存的网格标识就越多。并且在查询结果返回匿名器后，网格标识匹配的时间就越长。因此 R 或 n 值越大，用户查询所需的时间和通信开销就越大。

当 $R = 0.75$ 时，通过改变匿名度 K 和网格划分数目 n 值，分析对GIM性能的影响。由图5可知，在时间和通信开销上，用户查询的时间和通信开销都随着 K 值的增大而增大，同时 n 值越大，用户查询的时间和通讯开销就越大。因为 K 值越大，K 个用户指定的查询区域形成的匿名域就越大，相应会查询到更多的POIs，系统需要更多的处理时间和通信开销。因此 K 或 n 值越大，用户查询所需的时间和通信开销就越大。

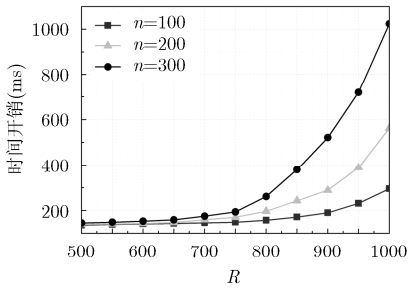
5.2 匿名器性能对比

当 R=750 , $n = 200$ 时，通过改变匿名度 K，对比GIM与TTP, ELPP方法对匿名器性能的影响。由图6(a)可知，在匿名器的时间开销上，随着 K 值增大，GIM相对于TTP, ELPP方法的优势就越大。在TTP和ELPP中，匿名器既要进行K匿名，又要对候选查询结果集进行求精，而GIM中匿名器仅进行简单的比较和匹配，它将候选结果集的求精放在用户端。因此，在匿名器的时间开销上，GIM方法相对于TTP, ELPP方法有很大的优势。

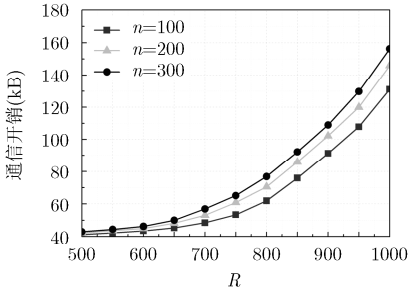
由图6(b)可知，在匿名器通信开销上，TTP和ELPP相对于GIM有一定优势。因为在用户发送查询请求消息给匿名器的过程中，TTP中发送的是用户的精确位置，ELPP中发送的是经过转换的位置信息，而GIM方法发送的是K个能确定用户指定查询区域的坐标加密集、加密网格单元标识集和用户端生成的对称密钥集等信息。同时在匿名器返回结果消息给用户的过程中，TTP和ELPP方法中匿名器返回的是精确结果，而GIM方法返回的候选结果集，在用户端需耗费一定的开销对结果集求精。因此，在匿名器的通信开销上，GIM方法有一定的劣势，但它能更好保护用户的位置隐私。

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。针对TTP结构模型存在的缺陷，本文提出一种基于网格标识匹配的位置隐私保护方法。该方法利用网格思想，结合保序对称加密和K匿名技术，加强用户的位置隐私保护，且匿名器不清楚用户的具体位置。安全分

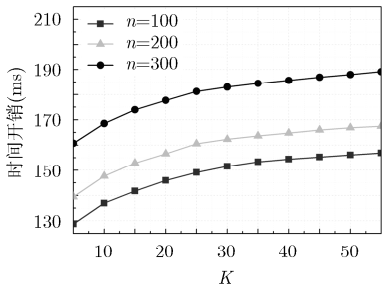


(a)时间开销

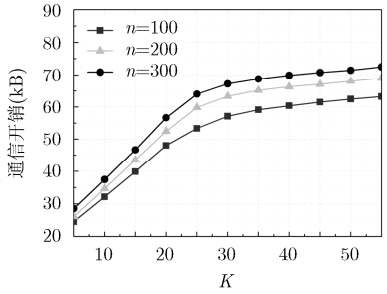


(b)通信开销

图 4 网格单元粒度及查询范围半径变化对性能的影响

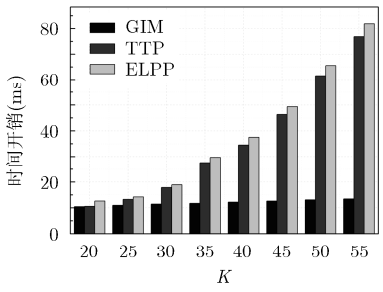


(a)时间开销

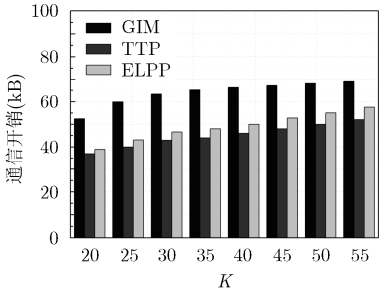


(b)通信开销

图 5 网格单元粒度及匿名度变化对性能的影响



(a)时间开销



(b)通信开销

图 6 匿名器性能对比

析表明该方法能抵制 LSP、匿名器和窃听者的隐私攻击。同时通过实验验证该方法在匿名器上具有较低的查询计算开销，有效缓解了匿名器的性能瓶颈问题。当然该方法也有待改进的地方，例如查询结果集的求精和寻找其它 $(K-1)$ 个用户由用户端完成，增加了用户端的计算开销，因此在下一步工作中，我们尝试在匿名器上通过用户历史记录形成 K 匿名，在适当增加匿名器开销的情况下，减少用户端的开销。

参 考 文 献

[1] LU Rongxing, LIN Xiaodong, LIANG Xiaohui, *et al.* A dynamic privacypreserving 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] YU Rong, KANG Jiawen, HUANG Xumin, *et al.* MixGroup: accumulative pseudonym exchanging for location privacy enhancement in vehicular social networks[J]. *IEEE Transactions on Dependable and Secure Computing*, 2016, 13(1): 93–105. doi: 10.1109/TDSC.2015.2399291.

[3] NIU Ben, LI Qinghua, ZHU Xiaoyan, *et al.* Enhancing privacy through caching in location-based services[C]. 2015 IEEE Conference on Computer Communication(INFOCOM), Hong Kong, China, 2015: 1017–1025. doi: 10.1109/INFOCOM.2015.7218474

[4] 张学军, 桂小林, 伍忠东. 位置服务隐私保护研究综述[J]. 软件学报, 2015, 26(9): 2373–2395. doi: 10.13328/j.cnki.jos.004857.
ZHANG Xuejun, GUI Xiaolin, and WU Zhongdong. Privacy preservation for location-based services: a survey[J]. *Journal of Software*, 2015, 26(9): 2373–2395. doi: 10.13328/j.cnki.jos.004857.

[5] PENG Tao, LIU Qin, and WANG Guojun. Enhanced location privacy preserving scheme in location-based services [J]. *IEEE Systems Journal*, 2014: 1–12. doi: 10.1109/JSYST.2014.2354235.

[6] SHOKRI R, THEODORAKOPOULOS G, PAPADIMITRATOS P, *et al.* Hiding in the mobile crowd: location privacy through collaboration[J]. *IEEE Transactions on Dependable and Secure Computing*, 2014, 11(3): 266–279. doi: 10.1109/TDSC.2013.57.

[7] CHOW C Y, MOKBEL M F, and LIU X. Spatial cloaking for anonymous location-based services in mobile peer-to-peer environments[J]. *GeoInformatica*, 2011, 15(2): 351–380. doi: 10.1007/s10707-009-0099-y.

[8] ARDAGNA C A, CREMONINI M, VIMERCATI S D C, *et al.* An obfuscation-based approach for protecting location privacy[J]. *IEEE Transactions on Dependable and Secure Computing*, 2011, 8(1): 13–27. doi: 10.1109/TDSC.2009.25.

[9] 彭志宇, 李善平. 移动环境下LBS位置隐私保护[J]. 电子与信息学报, 2011, 33(5): 1211–1216. doi: 10.3724/SP.J.1146.2010.01050.
PENG Zhiyu and LI Shanping. Protecting location privacy in location-based services in mobile environments[J]. *Journal of Electronics & Information Technology,* 2011, 33(5): 1211–1216. doi: 10.3724/SP.J.1146. 2010.01050.

[10] GEDIK B and LIU L. Protecting location privacy with personalized k-anonymous: architecture and algorithms[J]. *IEEE Transactions on Mobile Computing*, 2008, 7(1): 1–18. doi: 10.1109/TMC.2007.1062.

[11] 周长利, 马春光, 杨松涛. 路网环境下保护LBS位置隐私的连续KNN查询方法[J]. 计算机研究与发展, 2015, 52(11): 2628–2644. doi: 10.7544/issn1000-1239.2015.20140523.
ZHOU Changli, Ma Chunguang, and YANG Songtao. Location privacy-preserving method for LBS continuous KNN query in road networks[J]. *Journal of Computer Research and Development*, 2015, 52(11): 2628–2644. doi: 10.7544/ issn1000-1239.2015.20140523.

[12] SCHLEGEL R, CHOW C Y, HUANG Q, *et al.* User-defined privacy grid system for continuous location-based services[J]. *IEEE Transactions on Mobile Computing*, 2015, 14(10): 2158–2172. doi: 10.1109/TMC.2015.2388488.

[13] AGRAWAL R, KIERNAN J, SRIKANT R, *et al.* Order preserving encryption for numeric data[C]. Proceedings of the 2004 ACM SIGMOD International Conference on Management of Data, Paris, France, 2004: 563–574.

[14] POPA R A, LI F H, and ZELDOVICH N. An ideal-security protocol for order-preserving encoding[C]. 2013 IEEE Symposium on Security and Privacy (SP), Berkeley, California, 2013: 463–477. doi: 10.1109/SP.2013.38.

[15] AHMADIAN M, PAYA A, and MARINESCU D C. Security of applications involving multiple organizations and order preserving encryption in hybrid cloudenvironments[C]. 2014 IEEE International Parallel & Distributed Processing Symposium Workshops (IPDPSW), Phoenix, Azerbaijan, 2014: 894–903. doi: 10.1109/IPDPSW.2014.102.

[16] 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.

[17] MCNAMES J. A fast nearest-neighbor algorithm based on a principal axis search tree[J]. *IEEE Transactions on Pattern Analysis and Machine Intelligence,* 2001, 23(9): 964–976. doi: 10.1109/34.955110.

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

张少波：　男，1979 年生，讲师，博士生，研究方向为隐私保护和云计算安全.

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

王国军：　男，1970 年生，教授，博士生导师，研究方向为系统安全、隐私保护、可信计算和大数据安全.