基于缓存候选结果集的轨迹隐私保护方法

张少波[1]，刘 琴[2]，李 雄[1]，王国军[3]

(1. 湖南科技大学计算机科学与工程学院 湖南 湘潭 411201；2. 湖南大学信息科学与工程学院 长沙 410082；
3. 广州大学计算机科学与教育软件学院 广州 510006)

【摘要】在基于位置服务的连续范围查询过程中，针对相交区域需要重复查询的问题，提出一种基于缓存候选结果集的轨迹隐私保护方法。该方法采用二级缓存机制，分别在用户端和匿名器中缓存用户查询得到的候选结果集，供用户移动轨迹上的后续查询点使用，以减少用户与服务器之间的交互，降低用户信息暴露给服务器的风险。同时通过基于Markov模型的移动位置预测方法进行*k*-匿名，提高缓存的命中率。安全分析表明该方法能有效保护用户的轨迹隐私。实验结果显示该方法能减小服务器的计算和通信开销。

关 键 词 缓存；*k*-匿名；基于位置服务；Markov模型；轨迹隐私
中图分类号 TP309 **文献标志码** A doi:10.3969/j.issn.1001-0548.2018.03.020

A Trajectory Privacy Preserving Method Based on Caching Candidate Result Set

ZHANG Shao-bo[1], LIU Qin[2], LI Xiong[1], and WANG Guo-jun[3]

(1. School of Computer Science and Engineering, Hunan University of Science and Technology Xiangtan Hunan 411201;
2. College of of Computer Science and Electronic Engineering, Hunan University Changsha 410082;
3. School of Computer Science and Educational Software, Guangzhou University Guangzhou 510006)

Abstract To address the intersecting region of the continuous range queries needs to repeat queries in the location-based service, this paper proposes a method of trajectory privacy protection based on caching candidate result set. The method utilizes two-level cache mechanism to cache user's candidate result set at client and anonymizer, and the next query point on the trajectory can obtain the answer from the cached data, which can reduce the interaction between the user and the server to reduce the risk of user's information exposed to the server. At the same time, we propose the k-anonymity of the mobile location prediction based on the Markov model, which can improve the hit ratio of cache and enhance the user's trajectory privacy. Security analysis shows that the method can effectively protect the user's trajectory privacy. Experiments show this method can reduce the computation and communication overhead of the server.

Key words cache; *k*-anonymity; location-based service; Markov model; trajectory privacy

目前，基于位置服务(location-based service, LBS)已广泛应用于军事、商业和民生等领域[1]。用户通过 LBS 可以获得当前位置附近的兴趣点(points of interests, POIs)，如最近的影院、医院和餐馆等[2]。根据用户连续的 LBS 查询，攻击者可能分析出特定用户轨迹的敏感信息，如家庭住址、生活习惯和健康状况等行为特征[3]。苹果手机引发的“隐私门”风波，就是通过 LBS 泄露用户的隐私。因此，LBS 中的轨迹隐私保护已成为急需解决的问题。

在连续 LBS 查询中，学者已提出一些轨迹隐私保护方法，主要分为两类结构[4]：点对点和基于可信第三方(trusted third party, TTP)的中心服务器结构。在点对点结构中，文献[5]最先提出了用户协作的点对点匿名算法。文献[6]提出了一种通过用户缓存相互合作的隐私保护方法。但在这种结构中，用户发送的查询需要进行匿名或变换处理，对终端将会产生较大开销。在基于 TTP 中心服务器结构中，引入一个可信匿名器作为移动用户和位置服务提供商(location service provider, LSP)之间的中间体，它负责对用户的查询进行泛化处理，形成一个包括 k 个用户的匿名域[7]。文献[8]首次提出在第三方服务器进行匿名的 TTP 框架。文献[9]提出了一种社交网

收稿日期：2017－01－21；修回日期：2017－11－15
基金项目：国家自然科学基金(61632009, 61402161, 61300220, 61772194)；湖南省自然科学基金(2015JJ3046)；湖南省教育厅资助科研项目(16B089)
作者简介：张少波(1979－)，男，博士，主要从事社交网络隐私保护、云计算安全方面的研究.

络中轨迹隐私的保护方法。文献[10]基于 TTP 结构提出一种时间混淆技术，攻击者很难重构用户的轨迹。文献[11]基于 TTP 结构和假位置思想，提出一种在路网环境的连续查询方法。文献[12]针对怎样使用激励机制而设计了两种方案来取得 K 匿名位置隐私。但在这些基于 TTP 结构的方法中，用户每次查询得到精确结果后，往往将候选结果集丢弃。在连续的 LBS 范围查询中，相邻查询点的范围总存在一定的相交区域。如果这些相交区域在后续查询点又向 LSP 查询，将会加大用户信息暴露给 LSP 的风险，也会增加 LBS 服务器的开销。

针对基于 TTP 结构存在的局限性，本文提出一种基于缓存候选结果集(cache candidate result set, CCRS)的轨迹隐私保护方法。该方法利用缓存思想，在用户端和匿名器中缓存用户每次查询得到的候选结果集，供移动轨迹上的后续查询点使用，以减少用户与 LBS 服务器之间的交互，降低用户轨迹信息暴露给 LBS 服务器的风险。

1 系统模型和相关定义

1.1 系统模型

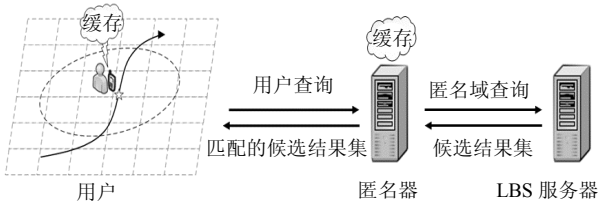

图1 基于CCRS的轨迹隐私保护模型

图1为基于CCRS的轨迹隐私保护模型，它主要包括用户、匿名器和LBS服务器3类实体，其具体工作过程为：1) 用户发送查询时，先确定查询范围内包含的各网格单元标识，并在用户端缓存中查找。如果能找到这些网格单元标识及包含的候选结果集，则返回给用户；否则将未查找到的网格单元标识发送给匿名器。2) 匿名器收到用户的这些网格单元标识后，在其缓存中查找匹配。如果匿名器缓存有这些网格单元标识及包含的候选结果集，则返回查询结果；否则基于Markov模型的移动位置预测方法，在匿名器中形成k-匿名域后再发送给LSB服务器查询。3) LBS服务器根据匿名域范围，查询各网格单元内包含的POIs，并将各网格单元标识及包含的候选结果集返回给匿名器。4) 匿名器将各网格单元标识及包含的候选结果集更新到缓存，并与用户需要查询的网格单元标识进行匹配。如果相等，则将该网格单元标识及包含的候选结果集发送给用户。5) 用户将查询匹配得到的网格单元标识及包含的候选结果集更新到缓存，并将得到的匹配候选结果集进行过滤求精，最后得到精确结果。

1.2 隐私度量

定义 1 缓存隐私度量：根据信息熵对用户位置隐私度的度量，基于缓存的隐私度量可表示为[13-14]：

$$\varphi=\frac{\sum_{g\in G_{\text{server}}} H(g)+\log_2 m^2\times\left|G_{\text{cache}}\right|}{\left|G_{\text{server}}\right|+\left|G_{\text{cache}}\right|} \tag{1}$$

式中，$\left|G_{\text{cache}}\right|$表示缓存中能找到的网格单元标识数；$\left|G_{\text{server}}\right|$表示需向LBS服务器查询的网格单元标识数；$m^2$表示网格单元数目；$H(g)$表示真实网格单元标识在查询$g$中的不确定性。在查询过程中，网格单元标识的命中率可表示为：

$$\delta=\frac{\left|G_{\text{cache}}\right|}{\left|G_{\text{server}}\right|+\left|G_{\text{cache}}\right|} \tag{2}$$

式(1)可变换为：

$$\varphi=\frac{\sum_{g\in G_{\text{server}}} H(g)}{\left|G_{\text{server}}\right|+\left|G_{\text{cache}}\right|}+\delta\log_2 m^2 \tag{3}$$

可以看出，通过提高缓存命中率可增强用户的位置隐私度。

1.3 Markov模型

用户的移动轨迹可以是n阶的马尔科夫链，可表示为具有时序性的移动轨迹点序列，每个移动轨迹点p_i的所处移动位置l_i只与其前面的n个移动轨迹点$\{p_{i-n+1},p_{i-n+2},\cdots,p_{i-1},p_i\}$相关[15]：

$$\begin{aligned}\Pr(p_{i+1}l=l_{i+1}\mid p_il=l_i,p_{i-1}l=l_{i-1},\cdots,p_1l=\\ l_1)=\Pr(p_{i+1}l=l_{i+1}\mid p_il=l_i,p_{i-1}l=\\ l_{i-1},\cdots,p_{i-n+1}l=l_{i-n+1})\end{aligned} \tag{4}$$

式中，$p_il=l_i$表示第i次移动轨迹点p_i的位置是l_i。

对于前n个移动轨迹点组成的用户轨迹，可预测求解具有最大概率的移动位置：

$$\begin{aligned}\Pr(p_{i+1}l=l_p\mid p_il=l_i,p_{i-1}l=l_{i-1},\cdots,p_1l=\\ l_1)=\max_{k=1}^{n}\Pr(p_{i+1}l=l_k\mid p_il=l_i,p_{i-1}l=l_{i-1},\\ \cdots,p_{i-n+1}l=l_{i-n+1})\end{aligned} \tag{5}$$

式中，l_p表示用户移动的预测位置。当有n个候选移动位置时，通过计算所有移动位置l_k是目标预测位置的概率，以预测用户真实的目标位置l_p。

2 基于CCRS的轨迹隐私保护方法

图2所示为基于CCRS的轨迹隐私保护工作过程，主要分为5个步骤，下面将分别进行介绍。

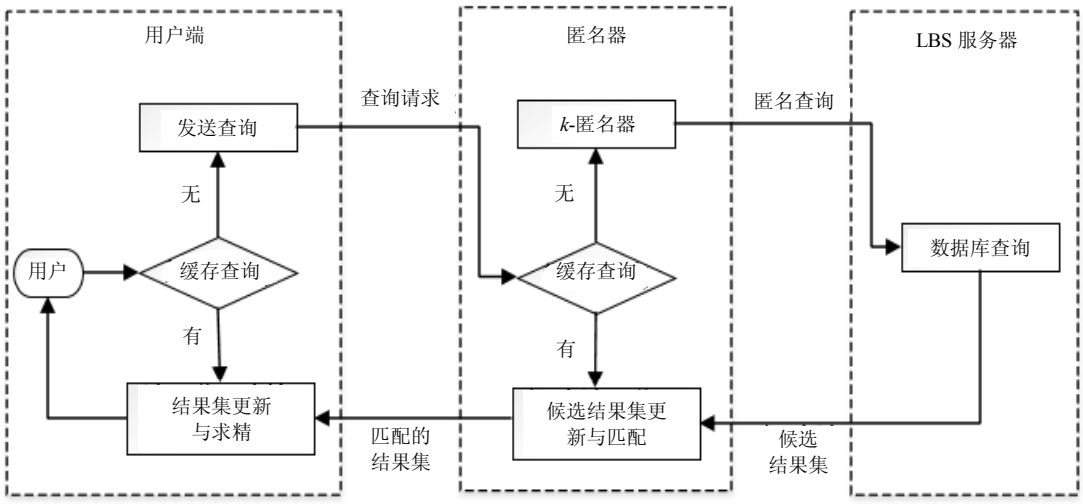

图2　基于CCRS的轨迹隐私保护工作过程

2.1　用户端缓存查询与服务请求

用户先将查询范围内网格结构定义为：

$$\text{Grids} \leftarrow ((x_1,y_1),(x_2,y_2),m\times m) \tag{6}$$

式中，(x_1,y_1)、(x_2,y_2)表示能确定用户查询范围的两个位置坐标；$m\times m$表示划分的网格数目。各网格单元都有唯一的标识(x_i,y_j)，可表示为：

$$(c_i,r_i)=\left(\left\lceil\frac{x_i-x_1}{(x_2-x_1)/m}\right\rceil,\left\lceil\frac{y_i-y_1}{(y_2-y_1)/m}\right\rceil\right) \tag{7}$$

式中，c_i、r_j分别为列、行标识，$1\leqslant i,j\leqslant m$；$(x_i,y_i)$为查询范围内的任意点。

用户根据查询半径R，确定需要查询的网格单元标识，并在用户端缓存中查找。如果能找到所有网格单元标识及包含的候选结果集，则直接对候选结果集进行求精，得到精确结果，否则将未找到的网格单元标识形成标识集I_h。

$$I_h \leftarrow \{(c_i,r_j)\} \quad 1\leqslant i,j\leqslant m \quad 1\leqslant h\leqslant n \tag{8}$$

式中，n为移动轨迹上的连续查询点次数。最后用户将需要查询的网格单元标识集I_h、随机生成的密钥K_u、用户当前位置L_h和运动方向D_h、网格结构Grids以及查询内容Content组成用户的请求消息，并使用匿名器的公钥PK_a对请求消息进行非对称加密形成MSG_{ua}发送给匿名器。

$$\text{MSG}_{ua}=E_{\text{PK}_a}(I_h,K_u,L_h,D_h,\text{Grids},\text{Content}) \tag{9}$$

2.2　匿名器缓存查询与位置匿名

当匿名器收到MSG_{ua}后，先用自己的私钥SK_a对MSG_{ua}解密，获得标识集I_h，然后在匿名器缓存中查找。如果能找到网格单元标识及包含的候选结果集，则返回给用户端。否则匿名器对未查找到的网格单元标识进行匿名处理。匿名时采用基于Markov模型的移动位置预测方法，预测用户在移动过程中的下一个查询位置。最后根据该预测位置形成匿名域，以提高下次查询的命中率。

基于Markov模型的移动位置预测主要从移动用户历史轨迹中获取一些有意义的物理位置，并通过统计概率模型来预测该用户的移动位置。本文利用文献[16]中提出的基于时间距离约束的网格聚类算法，先将用户的历史轨迹数据映射到定义的网格，获得所有停留点集合$\text{SP}=\{\text{sp}_1,\text{sp}_2,\cdots,\text{sp}_n\}$，并以sp作为输入，通过聚类方法聚集成停留区域集合$R=\{r_1,r_2,\cdots,r_N\}$，其中r_i是一个停留点sp_i的集合。然后可将用户移动轨迹表示为连续的轨迹序列$\text{Tra}=\langle r_i,\cdots,r_j\rangle$($r_i,r_j\in R$)。因此，通过输入用户每条历史轨迹序列，可获得移动对象的历史停留区域序列$\text{Tra}=\{r_1,r_2,\cdots,r_N\}$，它也可表示为状态变量序列$X=\{x_1,x_2,\cdots,x_N\}$，且每个停留区域对应一个状态。如果移动对象潜在的停留区域数目为m，则它的状态空间集合为$S=\langle s_1,s_2,\cdots,s_m\rangle$。最后用户根据这些状态，建立用户的状态转移矩阵$\mathbf{Pr}=\mathbf{Pr}(\boldsymbol{R}[i],\boldsymbol{R}[j])$。根据文献[17]基于运动趋势的移动对象预测算法，对每一个停留区域计算其移动概率，取其概率值最大的为R_p，并根据如下公式计算预测移动位置l_p：

$$l_p x=\frac{\sum_{i=1}^{N} r_i x}{|R_p|} \tag{10}$$

$$l_p y=\frac{\sum_{i=1}^{N} r_i y}{|R_p|} \tag{11}$$

当获得移动用户下一个查询位置 l_p 后，匿名器根据用户需要查询的网格单元标识集 I_h 和网格结构 Grids，选择 k 个用户所在的网格单元形成匿名区域 Region。最后匿名器将匿名域 Region、网格结构 Grids 以及查询内容 Content 组成新的查询请求消息，并使用LBS服务器公钥 PK_S 对它们进行非对称加密形成 MSG_{as}，再发送给LBS服务器。

$$\mathrm{MSG}_{as} = E_{\mathrm{PK}_s}(\mathrm{Region}, \mathrm{Grids}, \mathrm{Content}) \tag{12}$$

2.3 服务器数据查询与候选结果集返回

LBS服务器收到请求消息 MSG_{as} 后，先使用自己的私钥 SK_S 解密 MSG_{as}，获得 Grids、Region 和 Content。然后LBS服务器根据 Grids 中 (x_1, y_1)、(x_2, y_2) 和 m 恢复用户指定的网格结构，并根据查询内容 Content 搜索匿名域 Region 中网格单元包含的 POIs，得到 g 个POIs。如果第 j 个POI的位置为 (x_i, y_j) $(1 \leqslant i, j \leqslant g)$，则可计算它所在的网格单元标识，并可获得每个网格单元标识 (c_z, r_t) 包含的兴趣点集。最后，LBS服务器将这些查询到的兴趣点网格集 φ_r，形成候选结果集 MSG，用匿名器的公钥 PK_a 进行加密形成消息 MSG_{sa} 返回给匿名器：

$$(c_z, r_t) = \{(x_i, y_j)\} \quad 1 \leqslant i, j \leqslant g \tag{13}$$

$$\varphi_r = \{(c_z, r_t)\} \quad 1 \leqslant r \leqslant f \tag{14}$$

$$\mathrm{MSG} = \{\varphi_r\} \quad 1 \leqslant r \leqslant f \tag{15}$$

$$\mathrm{MSG}_{sa} = E_{\mathrm{PK}_a}(\mathrm{MSG}) \tag{16}$$

2.4 匿名器缓存更新与匹配候选结果集返回

首先，匿名器解密 MSG_{sa}，得到匿名域中每个网格单元标识对应的POIs，并将它更新到匿名器缓存。匿名器更新时，根据用户当前位置 L_h 和运动方向 D_h，需替换与用户运动方向相反、且距离移动用户下一个目标预测位置 l_p 最远的POIs。然后，匿名器将查询到的网格单元标识集 φ_r 与用户需要查询区域的网格单元标识 I_h 进行匹配，找到用户需要查询的网格单元标识及对应的POIs。最后，匿名器使用用户的密钥 K_u，对查询到的网格单元标识及包含的POIs进行对称加密，并组成 MSG_{au} 返回给查询用户：

$$\mathrm{MSG}_{au} = \mathrm{En}_{K_u}(I_h, (c_z, r_t)) \quad 1 \leqslant h \leqslant n \tag{17}$$

2.5 用户端缓存更新与结果求精

用户收到 MSG_{au} 后，首先用密钥 K_u 解密 MSG_{au} 获得所需查询网格单元中的每个POI的精确位置。然后，用户将得到的网格单元标识及包含的POIs更新到用户端缓存。最后，用户计算在自己查询区域之内的POIs，得到精确查询结果。

3 安全性分析

3.1 抵制连续查询攻击

在用户初次查询时，因缓存中没有候选结果集，用户发送的查询需经过匿名器匿名后，再转发给LBS服务器查询，LBS服务器收到的查询请求为 MSG_{as}。MSG_{as} 中包括匿名域 Region、查询内容 Content 以及网格结构 Grids，从这些信息中LBS服务器不能获得用户的真实位置。经匿名后的 Region 中，它至少包含 k 个用户，LBS服务器能成功猜到是指定用户的概率只有 $1/k$。

在用户移动轨迹上后续点的查询过程中，用户可以通过缓存直接得到部分或全部查询结果。如果用户直接从缓存中取得全部结果，他将不必与LBS服务器进行交互，因此，LBS服务器不能获得用户的任何信息。否则，在缓存中没有查找到的网格单元将形成匿名域，再发送给LBS服务器查询，但该匿名域不一定包含用户的真实位置。所以，LSP通过这些连续查询数据不能获得指定的用户和真实位置，CCRS方法能抵制LSP的连续查询推断攻击。

3.2 抵制窃听者的攻击

当用户发送请求消息给匿名器时，用匿名器公钥 PK_a 对 MSG_{ua} 进行了非对称加密，侦听者没有匿名器私钥 SK_a，不能解密 MSG_{ua} 得到有用信息。当匿名器将请求消息转发给LBS服务器时，LBS的公钥 PK_s 对 MSG_{ua} 进行了非对称加密，同样侦听者没有LBS的私钥 SK_S，不能解密 MSG_{as} 得到有用信息。在候选结果返回用户的过程中，非对称加密函数 $E(\cdot)$ 和对称加密函数 $\mathrm{En}(\cdot)$ 分别对 MSG_{sa}、MSG_{au} 进行了加密，侦听者没有匿名器的私钥 SK_a 和用户密钥 K_u，不能解密 MSG_{sa} 和 MSG_{au}。因此，侦听者既不能获得任何有用的信息，更不能得到用户的精确位置，CCRS方法能抵制侦听者的攻击。

4 实验及结果分析

4.1 实验数据及环境

实验采用Brinkhoff移动对象生成器[18]，输入德国奥尔登堡市交通网络图，并生成10 000个移动对象。实验随机选取Bob的移动轨迹作为实验对象，图3为移动用户Bob的运动轨迹，表1为实验参数设置。实验运行平台为Windows 7操作系统，Intel(R) Core(TM) i5-4590处理器、4 GB内存。

图3　移动用户Bob的运动轨迹

表1　实验参数设置

参数	值	参数	值
用户数目	10 000	查询点数目 n	1～80
(x_1, y_1) /km	(0,0)	POIs	10 000
(x_2, y_2) /km	(10,10)	匿名度 k	10～50
查询半径 R /km	0.5	网格数目 m	200

4.2　缓存命中率对比

当 $n=30$ 时，对比CCRS中使用Markov与No Markov方案对两级缓存平均命中率的影响。由图4可知，通过基于Markov模型的移动位置预测进行k-匿名的CCRS比没有使用Markov模型进行k-匿名的缓存命中率要高，同时缓存命中率随着匿名度k的增大而增大。因为通过基于Markov模型移动位置预测方法，可以预测到移动用户的下一个移动点位置，然后根据该位置选择周围 k 个用户所在的网格单元作为匿名域，可以预先将下一点需要查询的网格单元提前进行查询，相对于没有Markov的方法，使用Markov的CCRS方法能提高缓存的命中率。同时匿名度越高，相应缓存中的网格单元标识及包含的候选结果集就越多，在缓存中能找到用户需要查询的网格单元标识的可能性就越大，相应的缓存命中率就高。因此，匿名度k越大，缓存命中率就越高。

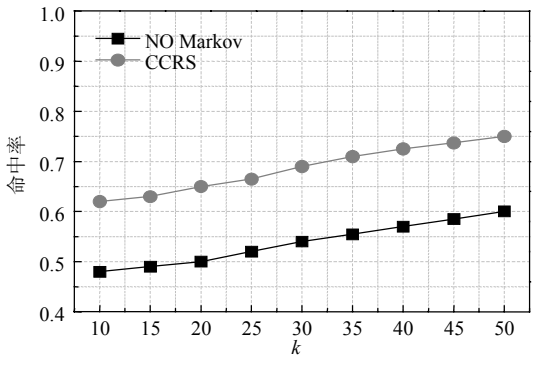

图4　缓存平均命中率对比

4.3　LBS服务器性能对比

图 5 为 LBS 服务器的性能对比图。当 $k=30$ 时，对比 CCRS 与 Gedik[9]、Hwang[10]方案对 LBS 服务器性能的影响。由图 5 可知，在 LBS 服务器时间开销和通信开销上，随着 n 的增大，CCRS 相对于 Gedik、Hwang 方案优势越大。因为 Gedik、Hwang 方案中用户发送的查询经匿名器匿名后，都需在 LBS 服务器中对整个匿名域进行查询，并将查询获得的候选结果集返回给用户。在 CCRS 方案中，用户端和匿名器使用二级缓存机制，用户发送查询时，首先在二级缓存中查询，只有在缓存中找不到需要查询的网格单元标识时，再经匿名后到 LBS 服务器中查询，这样有效减少了 LBS 服务器查询的次数和通信开销。因此，在 LBS 服务器的时间开销和通信开销上，CCRS 方案相对于 Gedik、Hwang 方案有较大的优势。

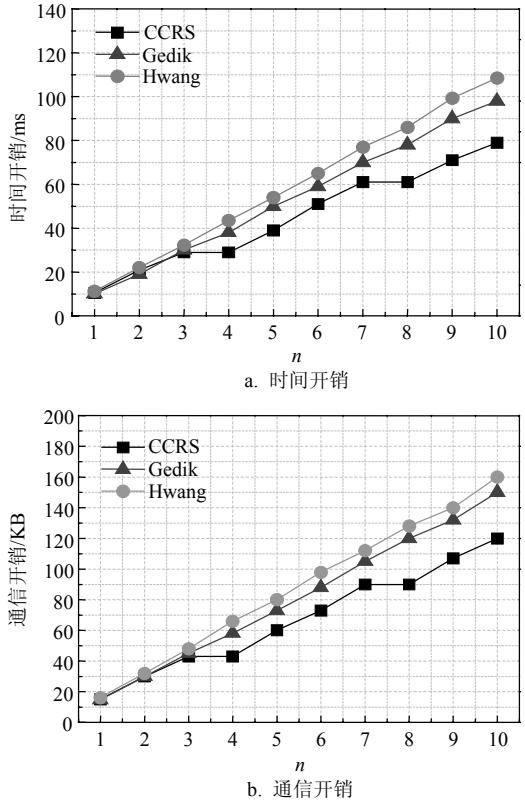

图5　LBS服务器的性能对比

5　结 束 语

本文提出了一种基于缓存候选结果集的轨迹隐私保护方法，利用缓存思想和基于 Markov 移动位置预测进行 k-匿名的技术，减少用户与 LBS 服务之间的交互，提高缓存的命中率和用户的轨迹隐私。安全分析表明该方法能抵制连续查询和侦听者的攻击。实验结果显示，与 Gedik、Hwang 方案比较，CCRS 方法能减少 LBS 服务器的开销。但 CCRS 方

法只考虑用网格单元内用户的数目形成 *k*-匿名域，因此在下一步工作中，将会考虑用户发送查询的概率形成匿名域，以进一步提高用户的位置隐私。

参 考 文 献

[1] PRIMAULT V, BOUTET A, MOKHTAR S B, et al. Adaptive location privacy with ALP[C]//Proceedings of the 35th Symposium on Reliable Distributed Systems (SRDS). New Jersey, USA: IEEE, 2016: 269-278.

[2] YI X, PAULET R, BERTINO E, et al. Practical approximate *k* nearest neighbor queries with location and query privacy [J]. IEEE Transactions on Knowledge and Data Engineering, 2016, 28(6): 1546-1559.

[3] 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.
ZHANG Xue-jun, GUI Xiao-lin, WU Zhong-dong. Privacy preservation for location-based services: a survey[J]. Journal of Software, 2015, 26(9): 2373-2395.

[4] 张少波, 刘琴, 王国军. 基于网格标识匹配的位置隐私保护方法[J]. 电子与信息学报, 2016, 38(9): 2173-2179.
ZHANG Shao-bo, LIU Qin, WANG Guo-jun. The method of location privacy protection based on grid identifier matching[J]. Journal of Electronics & Information Technology, 2016, 38(9): 2173-2179.

[5] CHOW C Y, MOKBEL M F, LIU Xuan. A peer-to-peer spatial cloaking algorithm for anonymous location-based service[C]//Proceedings of the 14th Annual ACM International Symposium on Advances in Geographic Information Systems. New York, USA: ACM, 2006: 171-178.

[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.

[7] CORSER G P, FU H R, BANIHANI A. Evaluating location privacy in vehicular communications and applications[J]. IEEE Transactions on Intelligent Transportation Systems, 2016, 17(9): 2658-2667.

[8] GEDIK B, LIU L. Protecting location privacy with personalized *k*-anonymous: Architecture and algorithms[J]. IEEE Transaction on Mobile Computing, 2008, 7(1): 1-18.

[9] 霍峥, 孟小峰, 黄毅. PrivateChechIn: 一种移动社交网络中的轨迹隐私保护方法与进展[J]. 计算机学报, 2013, 36(4): 716-726.
HUO Zheng, MENG Xiao-feng, Huang Yi. PrivateChechIn: Trajectory privacy-preserving for chech-in services in MSNS[J]. Chinese journal of computers, 2013, 36(4): 716-726.

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

[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.
ZHOU Chang-li, MA Chun-guang, YANG Song-tao. Location privacy-preserving method for LBS continuous KNN query in road networks[J]. Journal of Computer Research and Development, 2015, 52(11): 2628-2644.

[12] ZHANG Y, TONG W, ZHONG S. On designing satisfaction-ratio-aware truthful incentive mechanisms for *k*-anonymity location privacy[J]. IEEE Transactions on Information Forensics and Security, 2016, 11(11): 2528-2541.

[13] NIU B, LI Q, ZHU X, et al. Enhancing privacy through caching in location-based services[C]//Proceeding of the IEEE INFOCOM 2015. New Jersey, USA: IEEE, 2015: 1017-1025.

[14] XIAO C, CHEN Z, WANG X, et al. DeCache: a decentralized two-level cache for mobile location privacy protection[C]//Proceedings of the Sixth International Conference on Ubiquitous and Future Networks(ICUFN). New Jersey, USA: IEEE, 2014: 81-86.

[15] CHEN M, LIU Y, YU X. NLPMM: a next location predictor with Markov modeling[C]//Proceeding of the 18th Pacific-Asia Conference on Knowledge Discovery and Data Mining. New York, USA: Springer, 2014: 186-197.

[16] ZHENG V, ZHENG Y, XIE X, et al. Collaborative location and activity recommendations with GPS history data[C]// Proceeding of the 19th International Conference on World Wide Web. New York, USA: ACM, 2010: 1029-1038.

[17] 李雯, 夏士雄, 刘峰, 等. 基于运动趋势的移动对象位置预测[J]. 通信学报, 2014, 35(2): 46-53.
LI Wen, XIA Shi-xiong, LIU Feng, et al. Location prediction algorithm based on movement tendency[J]. Journal of Communications, 2014, 35(2): 46-53.

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

编 辑 叶 芳