一种身份认证下交换查询的轨迹位置保护算法

李 兰[1]，张才宝[1]，奚舒舒[1]，马鸿洋[2]

[1](青岛理工大学 信息与控制工程学院，山东 青岛市 266525)

[2](青岛理工大学 理学院，山东 青岛市 266033)

E-mail：17864213324@163.com

摘 要: 用户使用基于位置服务功能的 APP 时，通常利用手机号进行登录，为了防止手机号码与用户提交的位置信息与查询内容被恶意攻击者关联起来，提出一种身份认证下交换查询的轨迹位置保护算法。用户登录时，利用第三方服务器将手机号码过滤，使服务提供商无法获得手机号；用户利用自身位置发送查询请求时，第三方服务器根据距离权重选择最佳协同用户，对用户的 *ID* 进行转换，保护用户位置隐私与查询内容。实验结果表明，与 CPP 算法相比，该算法将轨迹位置保护度提高了 2.8%，并降低了用户请求响应时间。

关键字： 基于位置服务；位置隐私保护；轨迹位置保护；身份认证；交换查询

中图分类号： TP309 **文献标识码：** A **文章编号：** 1000-1220（2020）02--

A Trajectory Position Protection Algorithm of Exchange Query Under Identity Authentication

LI Lan[1] , ZHANG Cai-bao[1] , XI Shu-shu[1] , MA Hong-yang[2]

[1](School of Information and Control Engineering, Qingdao university of technology, Qingdao 266525, China)

[2](School of Science, Qingdao university of technology, Qingdao 266033, China)

Abstract: When users use APPs based on location service functions, they usually use mobile phone numbers to log in. In order to prevent the mobile phone number and location information and query content from being linked by malicious attackers, a trajectory position protection algorithm of exchange query under identity authentication is proposed. When the user logs in, the mobile phone number is filtered by a third-party server, so that the service provider cannot obtain the mobile phone number; when the user sends a query request by using his own location, the third-party server selects the best collaborative user according to the distance weight, and converts the user's ID Protect user location privacy and query content. Experimental results show that, compared with the CPP algorithm, the algorithm improves the trajectory position protection by 2.8%, and reduces the user request response time.

Key words: Location-based service; Location privacy protection; track position protection; authentication; exchange query

1 引言

无线通信和全球定位技术的飞速发展给移动应用程序带来了新的机遇，许多嵌入基于位置服务[1-4] (Location-Based-Service,LBS)功能 的 APP 被开发出来，用户可以在陌生的环境中使用这类 APP 查询附近的酒店、超市等兴趣点[5](Point of Interest,POI)来满足自身需求，这些应用程序给日常生活提供了诸多便利[6,7]。但随着用户安全意识的提高，在享受 LBS 服务的同时，用户也时刻担心提交给位置服务提供商(Location Service Provider,LSP)(以下 LSP 与 LBS 服务器指代同一个对象)的信息被不法分子截取。用户主要考虑两个方面，第一，使用此类 APP 时需通过手机号获取验证码进行登录，此时，用户的手机号会被 LSP 获取；第二，使用时用户需要提交查询信息，并将自身位置发送给 LSP，此时，用户的查询内容和位置信息会被 LSP 获取。由于实名制度的实施，手机号码可作为用户的真实身份之一[8]，当恶意攻击者将手机号码与用户提交的查询内容和位置信息链接后，容易推断出用户的兴趣、住址等隐私[9]，因此目前的工作是如何有效解决这两个问题。

2 相关工作

目前，对于连续查询中用户的轨迹隐私保护已经引起广泛关注。Huo 等[10]提出对轨迹信息上的敏感点进行匿名化的方法，以保护轨迹隐私。Hwang 等[11]提出了一种根据用户隐私档案和环境条件形成隐藏区域的时间模糊技术，使得恶意 LBS 服务器无法重建用户轨迹。Palanisamy 等[12,13]利用混合区提供黑箱空间，截断各子轨迹所反映的相关性，降低攻击者关联整个轨迹的成功

收稿日期：2020-6-5 基金项目：国家自然科学基金（No. 11975132）资助；山东省高等教育科技计划项目（No. J18KZ012）资助。
作者简介：**李兰**，女，1963 年生，硕士，教授，CCF 会员(74505M)，研究方向为数据挖掘，图像处理。**张才宝**(通讯作者)，男，1995 年生，硕士研究生，研究方向为位置隐私保护。**奚舒舒**，女，1995 年生，硕士研究生，研究方向为图像处理。**马鸿洋**，男，1976 年生，博士，教授，研究方向为网络空间安全、量子信息、量子保密通信等。

概率，之后又提出将用户形成一个隐匿区域，除查询发起者外，该区域还包含其他 *k*-1 个用户，这样，对手就无法确定发起者用户。Jiang[14]等提出一种基于查询分片用户协作的位置隐私保护方法，用于解决实际应用环境中协作用户的不可信问题。还有基于原语的密码学方法[15,16]，通过对用户与 LBS 服务器的交互信息加密实现隐私保护目的，可以提供很好的安全性，但存在用户与 LBS 服务器通讯中计算开销很大的问题。

身份认证是移动用户使用 LBS 功能应用程序的基础，手机号码和姓名、住址等一样，代表着用户的真实信息，如果不法分子将用户的网络信息与真实信息关联起来，用户的隐私会遭到泄露。Wang 等[17]提出一种通过第三方平台存储个人信息的模型，为用户提供个性化信息推送服务。Gu 等[18]提出一种数字签名技术与身份认证方案，该方案结合椭圆曲线密码体制与组合式伪随机数，并使用 SVO 逻辑对该方案进行形式化分析。Wang 等[19]提出基于 PTPM(portable TPM)和无证书公钥签名算法的身份认证方案，支持用户利用任意终端设备来完成与云端的双向身份认证过程，以解决目前云环境下用户与云端之间进行身份认证时所存在的安全问题和不足。Zhou 等[20]提出可证安全的高效无证书两方认证密钥协商协议。类似于文献[19][20]主要集中在利用公钥证书进行身份认证的研究，而基于短信验证码的身份认证的安全性的研究较少。

本文提出一种身份认证下交换查询的轨迹位置保护算法。用户登录时，利用可信第三方服务器，将数据进行分割，该服务器保存用户的手机号码，LSP 保存与用户真实身份无关的数据。当用户进行查询时，根据用户的隐私需求构建候选协同用户区域，利用距离权重计算方法，选择熵最大的一个用户作为最佳协同用户(Best Collaborative User,BCU)，使双方互相交换查询内容。这样既保护了用户的真实身份，又保护了位置隐私，即使 LBS 服务器被不法分子攻击，也无法对用户进行准确识别，有效保护用户隐私安全。

3 身份认证下交换查询的轨迹位置保护算法

本节首先定义了一些基本概念，然后给出身份认证下交换查询的轨迹保护模型，本文使用的符号汇总在表 1 中。

表 1 符号汇总

Table1 Symbol summary

符号	描述
E_{U2A}	用户发送给第三方匿名服务器的查询
E_{A2S}	第三方匿名服务器发送给 LBS 服务器的查询
TelePhone	用户的电话号码
ID	用户的身份
PassWord	用户使用 *ID* 登录时的密码
ID_{B_i}	第 *i* 个查询中 BCU 的身份
R_{min}	寻找协同用户范围的最小半径
R_{max}	寻找协同用户范围的最大半径
k	区域中候选协同用户的最少数量
Q	查询内容
R	查询兴趣点的范围
K_S	对称加密密钥
PK_S	LBS 服务器公钥
SK_S	LBS 服务器私钥
PK_A	第三方服务器公钥
PK_U	用户公钥
E	查询结果
E_{S2A}	LBS 将结果发送给第三方匿名服务器
E_{A2U}	第三方匿名服务器将结果发送给用户

3.1 相关定义

定义 1（距离度量）用户 u_i 和 u_j 之间的距离度量（本文使用欧几里得距离），定义为

$$dis(u_i,u_j)=\sqrt{(x_i-x_j)^2+(y_i-y_j)^2} \tag{1}$$

其中 x，y 分别表示用户所在位置的经度和纬度。

定义 2（距离权重）用 α_i 表示查询用户 u_{real} 的候选协同用户区域内用户 u_i 的距离权重，定义为

$$\alpha_i=\frac{dis(u_{real},u_i)}{\sum_{j=1}^{k}dis(u_{real},u_j)},\ (i=1,\ldots,k) \tag{2}$$

定义 3（最佳协同用户）k 个候选协同用户中权重最大的一个称为最佳协同用户，表示为

$$\alpha_{max}=arg\max_{i\in(1,\cdots,k)}\{\alpha_i\} \tag{3}$$

3.2 系统模型

本文系统架构如图 1 所示，轨迹隐私保护模块由移动用户、第三方服务器及 LBS 服务器(LSP)组成；身份认证模块由移动用户、可信第三方服务器、LBS 服务器(LSP)及短信平台组成。

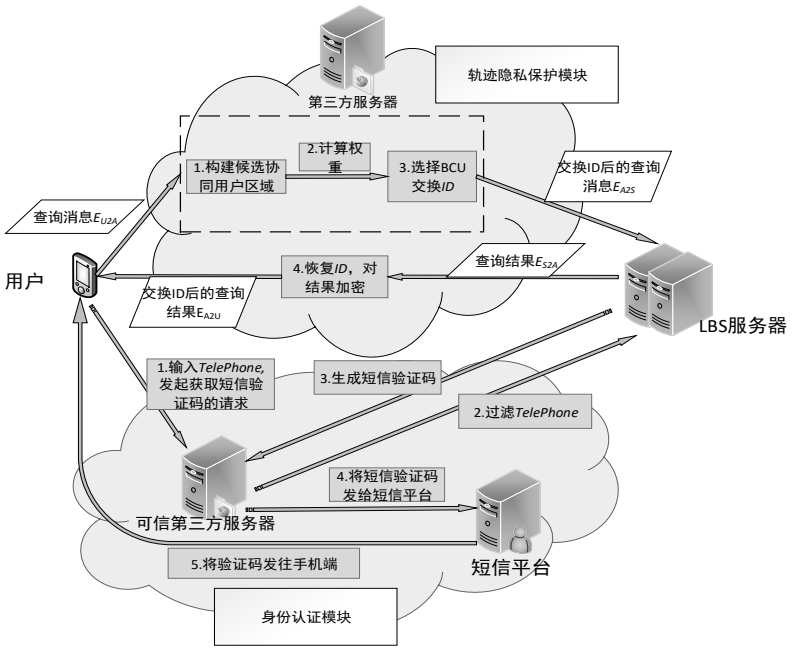

图 1 系统架构

Fig. 1 System structure

轨迹隐私保护算法中，第三方服务器根据定义 2 中的距离权重计算α_i，并选择 BCU 辅助用户进行查询，BCU 的选择如图 2 所示。

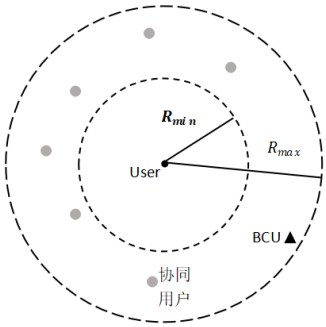

图 2 候选协同用户区域

Fig. 2 Candidate collaborative user area

3.3 移动用户身份认证

为了防止 LBS 服务器泄露用户的隐私信息，本文在移动用户与 LBS 服务器间引入可信第三方服务器，将原来存储在 LBS 服务器上的手机号码分离出来，存储在第三方服务器上，从而防止由手机号码引起的用户隐私信息的泄露。架构图如图 1 身份认证模块所示，具体步骤如下：

步骤 1：移动用户输入 *TelePhone*, 将获取短信验证码的请求发送给可信第三方服务器。

步骤 2：可信第三方服务器将 *TelePhone* 过滤,并将包含用户 *ID* 和本次会话号的请求发送给 LBS 服务器。

步骤 3：LBS 服务器通过特定算法生成短信验证码,与购买的短信平台服务权限和用户 *ID* 一起发送给可信第三方服务器。

步骤 4：可信第三方服务器将 *TelePhone* 和短信验证码发给短信平台。

步骤 5：短信平台将验证码发往用户端,用户使用验证码登录。

用户端通过验证码登录后，LSP 通过用户提交的验证码与自己生成的验证码进行比较，若相同，则验证通过。

因为可信第三方服务器没有购买短信平台服务权限，所以 LSP 需要将该服务权限发送给第三方服务器，本文通过算法 1 进行该权限的处理。

算法 1：授予访问权限

输入：ID_{LSP} ： *LSP* 的 *ID*

输出：授权结果 *Res*

1.*LSP* 通过算法产生一个随机序列 *Seq*；

2.*LSP* 利用私钥将序列 *Seq* 加密；

3.*Seq*~ = Private Key{*Seq*}；

4.*LSP* 将{*Seq*~,ID_{LSP}}发送给可信第三方服务器；

5.可信第三方服务器将{*Seq*~,ID_{LSP}}发送给短信平台；

6.短信平台根据 *LSP* 的公钥对消息进行验证：

7.*Res*=Public Key{{*Seq*~,ID_{LSP}}};

8.return *Res*

3.4 基于交换查询的轨迹位置保护算法

第三方服务器根据用户的隐私需求构建候选协同用户区，通过距离权重选择 BCU，然后将用户与 BCU 的 *ID* 转换，并发送给 LSP 进行查询，LSP 将查询结果返回给第三方服务器后，再将用户和 BCU 的 *ID* 恢复，并分别将结果发送给用户和 BCU。具体步骤如下：

步骤 1：用户将查询消息E_{U2A}发送给第三方服务器，

其中隐私需求使用第三方服务器公钥加密，查询内容和范围以及对称加密密钥使用 LBS 服务器公钥加密，第三方服务器使用私钥获得用户的隐私需求，寻找协同用户，并将距离权重最大的一个设为最佳协同用户 BCU。E_{U2A}形式如下(4)：

$$E_{U2A}=\{PK_A(ID,R_{min},R_{max},k),PK_S(R,Q,K_S)\} \quad (4)$$

步骤 2：找到 BCU 后，第三方服务器将用户的 *ID* 转换成 BCU 的伪 *ID*(ID_{B_i})，然后将ID_{B_i}与用户的查询请求共同组成查询消息，如下(5)所示：

$$E_{A2S}=\{PK_S(ID_{B_i}),PK_S(R,Q,K_S)\} \quad (5)$$

第三方服务器将用户的查询消息发送给 LBS 服务器，值得注意的是，用户的查询内容和范围使用 LBS 服务器公钥加密，所以第三方服务器无法获得。

步骤 3：LBS 服务器收到消息E_{A2S}后，进行解密，并根据用户的需求搜索 POI 并获得结果 E，最后它使用对称加密密钥加密 E，将其发送给第三方服务器。

$$E_{S2A}=\{PK_A(ID_{B_i}),K_S(E)\} \quad (6)$$

步骤 4：第三方服务器收到来自 LBS 服务器的查询结果后，首先从列表中恢复用户的 *ID*，然后利用用户公钥将提取出来的查询结果$K_S(E)$进行加密，如下(7)：

$$E_{A2U}=\{PK_U(K_S(E))\} \quad (7)$$

最后，第三方服务器将查询结果发送给用户。

步骤 5：用户从第三方服务器收到E_{A2U}后，使用私钥和对称加密密钥获得精确结果 E。在查询交换过程中，第三方服务器同样为最佳协同用户 BCU 执行步骤 1 - 4。

寻找最佳协同用户算法伪代码如算法 2：

算法 2 寻找最佳协同用户

输入：*ID*, R_{min}, R_{max}, k

输出：最佳协同用户 BCU

1.初始化队列 q，并设置|q|=k；

2.根据用户隐私需求，输入 R_{min}、R_{max} 和 k，如果用户不输入 k 值，默认 k=6，构建候选协同用户区域；

3.从候选协同用户区域中选择 k 个用户，并放入队列 q 中；

4.**if** 协同用户数量小于 *k* **then**

5. 协同用户数量不足，*k=k-1*；

6.**else**

7. **for** *i*=1 **to** *k* **do**

8. 计算距离权重α_i；

9. $\alpha_{max}=arg\ \max_{i\in(1,\cdots,k)}\{\alpha_i\}$；

10.**end if**

4 安全性分析

本文的安全性分析集中在如何保护用户的真实身份和轨迹隐私，主要针对窃听攻击、不可信 LBS 服务器及第三方服务器攻击。

4.1 窃听攻击

用户与第三方服务器之间以及第三方服务器与 LBS 服务器之间的通信过程可以被攻击者通过无线信道窃听。轨迹隐私保护模块中使用对消息加密的方式来处理窃听攻击，在无线信道中传输的所有消息都由非对称和对称密钥加密保护。

当用户向第三方服务器发送查询消息时，隐私需求使用第三方服务器公钥加密为$PK_A(ID,R_{min},R_{max},k)$，查询内容、范围和对称加密密钥使用 LBS 服务器公钥加密为 $PK_S(R,Q,K_S)$，然后将 $E_{U2A}=\{PK_A(ID,R_{min},R_{max},k),PK_S(R,Q,K_S)\}$发送给第三方服务器，在此过程中，攻击者没有第三方服务器和 LBS 服务器的私钥，即使窃听到消息，也无法得到任何信息。同样，当第三方服务器将 *ID* 转换后的查询请求$E_{A2S}=\{PK_S(ID_{B_i}),PK_S(R,Q,K_S)\}$发送给 LBS 服务器时，攻击者无法获得任何信息，因此用户的敏感信息得到有效保护。

返回查询结果时，$E_{S2A}=\{PK_A(ID_{B_i}),K_S(E)\}$使用第三方服务器公钥和对称加密密钥加密，$E_{A2U}=\{PK_U(K_S(E))\}$使用用户的公钥加密，攻击者没有第三方服务器私钥、对称加密密钥和用户的私钥，因此，他们获取有用信息的概率可以忽略不计。通过以上分析，可以看到我们的方案可以有效抵抗窃听者的攻击，使攻击者无法获得用户的真实身份、查询位置和查询内容。

4.2 不可信 LBS 服务器

LSP 管理用户的所有查询信息，当 LSP 不是受信任时，可以通过这些数据推断敏感信息，包括用户的真实身份和移动轨迹。

本文的方案中，因为手机号码存储在可信第三方平台，而不是 LBS 服务器，所以，即使攻击者通过 LBS 服务器获得了用户信息，也无法和真实信息联系起来，有效保护用户的身份。并且在轨迹隐私保护模块中，第三方服务器在用户和 BCU 之间交换查询，在这个过程中，用户的身份*ID*在第 i 个查询中被 BCU 的ID_{B_i}替换，并且 LBS 服务器中的查询信息存储记录被链接到 BCU 的ID_{B_i}。由于每个查询点的 BCU 不同，LSP 无法推断他们之间的关系，也无法从任意 BCU 的ID_{B_i}中识别用户的真实轨迹。因此，LSP 能够推断用户真实身份或其轨迹的概率可以忽略不计。

4.3 第三方服务器攻击

身份认证模块中，假设 Bob 通过第三方服务器得到了 Alice 的信息{*TelePhone,ID*}。Bob 企图使用 Alice 的“*TelePhone* +短信验证码”进行登录，由于 Bob 没有 Alice 的手机，无法获得短信验证码，因此登录失败；同理，如果 Bob 用 Alice 的“*ID*+*PassWord*”进行登录，由于 Bob 无法获知 Alice 的 *PassWord*，同样登录失败。

轨迹隐私保护模块中，Bob 通过第三方服务器得到了 Alice 的查询消息$E_{U2A}=\{PK_A(ID,R_{min},R_{max},k),PK_S(R,Q,K_S)\}$，即使 Bob 使用第三方服务器私钥获得了 Alice 的 *ID*，但因为缺少 LBS 服务器私钥SK_S，无法解密 Alice 的

查询内容和范围；同样，假设 Bob 通过第三方服务器得到 Alice 的查询结果$E_{S2A}=\{PK_A(ID_{B_i}),K_S(E)\}$，由于 Bob 没有对称加密密钥$K_S$，无法解密查询结果$E$，因此 Bob 无法获得关于 Alice 的有效信息。

5 实验仿真

5.1 实验环境

实验环境为 2.4GHz 的双核 CPU，8GB 内存，操作系统是 Windows10。在身份认证模块中，本文在 MySQL（线程池中的 20 个线程）上模拟通信时间；轨迹隐私保护模块中，算法采用 Python 编程语言实现，在 Thomas Brinkhoff[21]上进行仿真实验，在 Oldenburg 交通路网中取大约 4km*4km 区域位置数据，其中 20 个 POIs 是随机生成的，用户数量由参数控制。

5.2 仿真结果分析

5.2.1 身份认证中时间效率分析

实验时从数据库表中采集了所有用户登录时请求记录数总和 n 的值，当 n 分别为 600,800,1000,1200 时，处理每一次请求所花费的时间(ms)，x 轴表示实验重复次数。

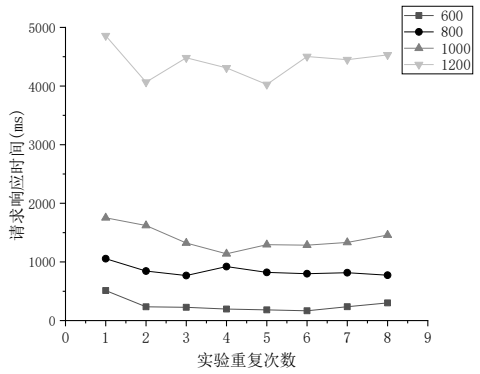

图 3 请求记录数与响应时间关系

Fig. 3 Relationship between number of request records and response time

由图 3 可以看出，第一次实验时的请求响应时间比后面 7 次响应时间大，这是因为系统初始化后需要重新连接数据库。

将图 3 中 n 分别为 600,800,1000,1200 时的 8 次模拟数据取平均值得到图 4。

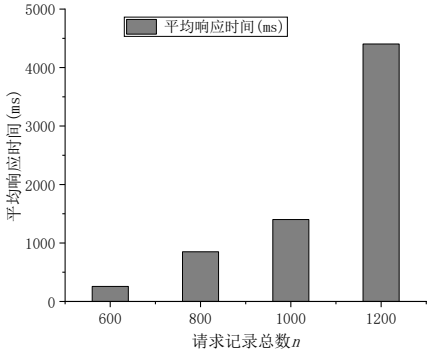

图 4 不同 n 值下的平均响应时间

Fig. 4 Average response time at different values of n

由图 4 可以看出，当请求记录数量达到 1200 时，系统平均响应时间未达到 5000ms，即 5s，现在短信平台响应时间普遍在 5s 以内，所以总响应时间可以保持在 10s 以内，而短信验证码的有效时间为 60s，所以此身份认证方案在实际应用中是可行的，既保护了用户的隐私信息，又能较好的为用户提供服务。

5.2.2 基于交换查询的轨迹隐私保护算法分析

为了验证轨迹隐私保护算法的有效性，本文将在请求响应时间和用户轨迹位置保护程度两方面与 CPP 算法[22]进行比较，为了增加说服力，两种算法中用户的R_{min}与R_{max}均相同。

系统响应时间指用户的请求通过某算法进行处理后发送给 LSP，并收到从 LBS 服务器返回的第一个 POI 的这段时间。

由图 5 可以看出，两种算法的系统响应时间随 k 值的增大而增加。当 k 很小时，用户可以很快寻找到协同用户或者生成匿名区域，但当 k 值增加到一定程度时，系统响应时间明显增加，这是因为 k 值越大，用户搜索其他 k-1 个用户的时间越久。图 5 中明显看出，本文基于交换查询的轨迹隐私保护算法的响应时间比 CPP 算法短，因为在找到协同用户后，系统只需要分别计算协同用户的权重即可，而 CPP 算法需要根据约束条件生成匿名区，增加了响应时长。

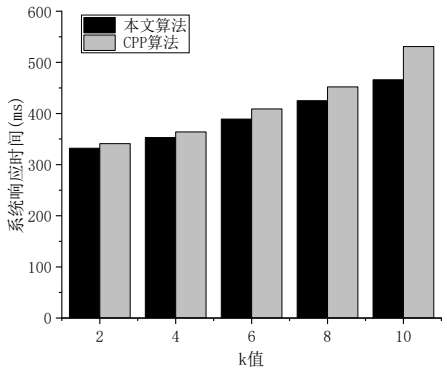

图 5 系统响应时间与 k 值的关系

Fig. 5 Relationship between system response time and k value

在可接受的系统响应时间下，用户轨迹位置保护程度是衡量算法优劣的的重要指标。图 6 为本文基于交换查询的轨迹隐私保护算法与 CPP 算法在用户轨迹位置保护程度上的对比。

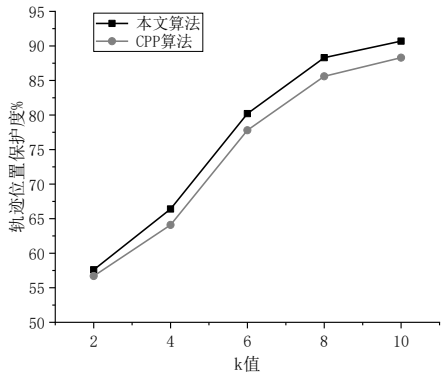

图 6 轨迹位置保护度与 k 值的关系

Fig. 6 Relationship between protection degree of track position and k value

由图 6 可以看出，当 k 值较小时，两种算法由于无法构建良好的辅助区域，在用户轨迹保护程度上接近，随着 k 值增加，本文基于交换查询的轨迹隐私保护算法明显可以达到更好的保护效果。这是因为 k 值增加到一定程度时，可以从众多协同用户中选择距离权重最大的一个作为 BCU，且最佳协同用户是动态变化的，攻击者无法将用户在各个时刻上的位置联系起来，因此 k 值越大，本文基于交换查询的轨迹隐私保护算法对用户的轨迹保护程度越高。

6 结束语

为了更好地保护用户的真实身份、位置信息与查询内容，防止恶意攻击者通过 LSP 将用户的这些信息联系起来，提出一种身份认证下交换查询的轨迹位置保护算法。用户登录时利用第三方服务器将手机号码过滤，使 LSP 无法获得用户的手机号码；当用户向 LSP 提交位置信息和查询请求时，利用 BCU 与用户进行交换查询，使 LSP 无法关联用户的查询请求与 *ID*。最后通过仿真实验，验证了该算法在保护用户身份与轨迹隐私方面的有效性。从不同方面考虑协同用户的选择是本课题将继续研究的内容。

References:

[1] Al-Dhubhani R, Cazalas J M. An adaptive geo-indistinguishability mechanism for continuous LBS queries[J]. Wireless Networks, 2017, 24(5):1-19.

[2] YUAN Jian, WANG Di, GAO Xi-long, et al. Privacy Protection Model for Anonymous Group LBS Trajectory Based on Differential Privacy[J]. Journal of Chinese Computer Systems,2019,40(02):341-347.

[3] PENG Tao, LIU Qin, WANG Guo-jun. Enhanced Location Privacy Preserving Scheme in Location-Based Services[J]. Systems Journal, IEEE,2017,11(1):219-230.

[4] HU De-min, ZHAN Han. Predictable Differential Disturbance User Trajectory Privacy Protection Method[J]. Journal of Chinese Computer Systems, 2019,40(06):1286-1290.

[5] Zhu J , Wang C , Guo X , et al. Friend and POI recommendation based on social trust cluster in location-based social networks[J]. EURASIP Journal on Wireless Communications and Networking, 2019, 89(2019).

[6] Ni L , Tian F , Ni Q , et al. An anonymous entropy-based location privacy protection scheme in mobile social networks[J]. EURASIP Journal on Wireless Communications and Networking, 2019, 93(2019).

[7] ZHANG Lei,LI Jing,YANG Song-tao,et al. A novel attributes anonymity scheme in continuous query[J]. Wireless Personal Communications,2018,101(2):943-961.

[8] ZHENG Fang, WEI Jian-Qin,LI Ping-Zhen.Research on privacy protection method in mobile identity authentication[J]. Network Security Technology and Application, 2018, 216(12):84-87.

[9] SUN Yan-ming,CHEN Min,HU Long,et al. ASA: Against statistical attacks for privacy-aware users in Location Based Service[J]. Future Generation Computer Systems,2016,70(70):48-58.

[10] Huo, Zheng et al. “You Can Walk Alone: Trajectory Privacy-Preserving through Significant Stays Protection.”[C].International conference on database systems for advanced applications;DASFAA 2012.2012.

[11] Hwang, R.-H.,Hsueh, Y.-L.,Chung, H.-W.. A Novel Time-Obfuscated Algorithm for Trajectory Privacy Protection[J]. Services Computing, IEEE Transactions on,2014,7(2):126-139.

[12] Palanisamy B , Liu L , Lee K , et al. Anonymizing continuous queries with delay-tolerant mix-zones over road networks[J]. Distributed & Parallel Databases, 2014, 32(1):91-118.

[13] Balaji Palanisamy,Ling Liu. Attack-Resilient Mix-zones over Road Networks: Architecture and Algorithms[J]. IEEE Transactions on Mobile Computing,2015,14(3):495-508.

[14] JIANG Jie, FU Chao-yi. Location Privacy Protection Method Based on Query Fragment and User Collaboration [J]. Journal of Chinese Computer Systems, 2019, 40(05):25-30.

[15] Zheng X, Cai Z, Li J, et al. Location-privacy-aware review publication mechanism for local business service systems[C]//IEEE INFOCOM 2017-IEEE Conference

on Computer Communications. IEEE, 2017: 1-9.

[16] Zheng X, Cai Z, Li Y. Data linkage in smart internet of things systems: a consideration from a privacy perspective[J].IEEE Communications Magazine, 2018, 56(9): 55-61.

[17] WANG Fu, KANG Jian.Research on the Personal Information PushBased on the Trusted Third Party in the Institutions of Library and Information[J]. Library and Information Service, 2015,59(3):85-89.

[18] GU Zhao-jun,LIU Dong-nan. ECC Identity Authentication Scheme Between Aircraft and Passenger Boarding Bridges[J]. Journal of Chinese Computer Systems, 2019, 040(001):98-103.

[19] WANG Zhong-Hua, HAN Zhen, LIU Ji-Qiang, ZHANG Da-Wei, et al. ID Authentication Scheme Based on PTPM and Certificateless Public Key Cryptography in Cloud Environment[J]. Journal of Software, 2016, 27(6): 1523-1537.

[20] ZHOU Yan-Wei,YANG Bo,ZHANG Wen-Zheng. An Improved Two-Party Authenticated Certificateless Key Agreement Protocol [J]. Journal of Computer,2017,40(05):1181-1191.

[21] ZHANG Shao-bo, WANG Guo-jun, LIU Qin, et al. A trajectory privacy-preserving scheme based on query exchange in mobile social networks[J]. Soft Computing,2018,22(18):6121-6133.

[22] HU De-min,ZHENG Xia. k-anonymous privacy protection algorithm for user trajectory protection based on continuous query[J]. Application Research of Computers,2017,34(11):3421-3423+3427.

附中文参考文献：

[2] 袁健,王迪,高喜龙, 等.基于差分隐私的匿名组 LBS 轨迹隐私保护模型[J].小型微型计算机系统,2019,40(02):341-347.

[4] 胡德敏,詹涵.可预测的差分扰动用户轨迹隐私保护方法[J].小型微型计算机系统,2019,40(06):1286-1290.

[8] 郑芳, 魏建琴, 李平珍. 移动身份认证中的隐私保护方法的研究[J]. 网络安全技术与应用, 2018, 216(12):84-87.

[14] 江颉, 傅超仪. 基于查询分片用户协作的位置隐私保护方法[J]. 小型微型计算机系统, 2019, 40(05):25-30.

[17] 王福,康健.基于可信第三方的图书情报机构个性化信息推送研究[J].图书情报工作,2015,59(03):85-89.

[18] 顾兆军, 刘东楠. 一种面向廊桥 AP 的 ECC 身份认证方案[J]. 小型微型计算机系统, 2019, 040(001):98-103.

[19] 王中华,韩臻,刘吉强,张大伟，等.云环境下基于 PTPM 和无证书公钥的身份认证方案[J].软件学报,2016,27(06):1523-1537.

[20] 周彦伟,杨波,张文政.一种改进的无证书两方认证密钥协商协议[J].计算机学报,2017,40(05):1181-1191.

[22] 胡德敏,郑霞.基于连续查询的用户轨迹 k-匿名隐私保护算法[J].计算机应用研究,2017,34(11):3421-3423+3427.