•网络空间安全•

DOI:10.15961/j.jsuese.201900895

本刊网刊

一种新的多用户位置隐私保护方案

汪晶晶[1,2], 韩益亮[1,2*], 陈家勇[3], 杨晓元[1,2]

(1.武警工程大学 密码工程学院, 陕西 西安 710086; 2.网络与信息安全武警部队重点实验室, 陕西 西安 710086;
3.武警工程大学 教务处, 陕西 西安 710086)

摘　要:位置服务中许多应用都需要多用户进行位置共享,但传统的刚性隐私保护策略迫使用户不得不共享自身的精确位置。为满足用户个性化的隐私保护需求,本文提出了一种新的多用户位置共享隐私保护方案。该方案利用两种位置转换模型保证用户能够灵活地自定义其不同精度的共享位置,再通过基于中国剩余定理的多秘密共享机制将不同精度的位置数据打包转换,只需一次份额分发就可实现不同共享对象恢复出不同精度的位置信息。安全性分析表明,该方案的安全性高,不依赖于位置服务器的可信度,能够抵抗单个位置服务器攻击、多个位置服务器合谋攻击以及多个用户之间的合谋攻击,在不可信环境下实现了多用户位置共享的弹性隐私保护。仿真实验分析进一步表明,该方案与同类方案相比更高效,性能平稳。当参与存储管理份额的位置服务器数量增加或需恢复更高精度位置信息时,计算通信开销不会剧增,在资源受限的网络环境中同样适用。

关键词:多用户位置共享; 弹性位置隐私保护; 多秘密共享

中图分类号:TP391　　**文献标志码**:A　　**文章编号**:2096-3246(2020)05-0178-08

A New Location Privacy Protection Scheme for Multi-users

WANG Jingjing[1,2], *HAN Yiliang*[1,2*], *CHEN Jiayong*[3], *YANG Xiaoyuan*[1,2]

(1.College of Cryptography Eng., Eng. Univ. of PAP, Xi'an 710086, China; 2.Key Lab. of Network & Info. Security of PAP, Xi'an 710086, China;
3.Office of Academic Affairs, Eng. Univ. of PAP, Xi'an 710086, China)

Abstract: Many applications in location-based services require multiple users to share location. However, the traditional rigid policy of privacy protection forces users to share and expose their precise locations. In order to meet the user's personalized needs for privacy protection, a new multi-user location sharing privacy protection scheme was proposed in this paper. Two kinds of location conversion models were used in our solution to ensure that users can flexibly customize their shared locations with different precision levels. Then all the location data with different precisions is packaged and converted through a multi-secret sharing mechanism based on the Chinese Remaining Theorem. In this mechanism, only one time shares-distribution was needed to realize different shared objects recover location information with corresponding different accuracies. In the security analysis, it is proved that the flexible location privacy protection of multi-user location sharing was realized in an untrusted net environment by our solution. It is highly secure since it does not depend on the trustability of the location provider and can resist single location server attack, collusion attacks of multiple location servers and multiple users. Furthermore, compared with the peer solutions, the simulation experiments showed that ours is more efficient and stable in performance. When the number of location servers participating in the share storage increases or the higher-precision location information is required to be reconstructed, the overheads of computation and communication will not increase dramatically. Thus, it is also applicable in the resource-constrained network environment.

Key words: multiple users location sharing; flexible location privacy protection; multi-secret sharing

收稿日期:2019 – 09 – 16

基金项目:国家自然科学基金项目(61572521); "十三五"国家密码发展基金密码理论研究项目(2017YFB0802000); 陕西省自然科学基金项目(U1636114; 2015JM6353); 武警工程大学创新团队科学基金项目(KYTD201805)

作者简介:汪晶晶(1986—),女,讲师,博士. 研究方向:应用密码学位置隐私保护. E-mail: 344505421@qq.com

* 通信联系人 E-mail: yilianghan@hotmail.com

网络出版时间:2020 – 09 – 15 11 : 33 : 48　　**网络出版地址**:https://kns.cnki.net/kcms/detail/51.1773.TB.20200914.1430.003.html

位置服务（location-based service，LBS）是一类在定位技术、地理信息系统和第三方位置服务提供商的支撑下，以用户位置信息为基础，向移动用户提供与位置相关的增值服务的总称[1–2]。近年来，LBS作为移动互联网中最重要的移动服务之一，正在全球以惊人的速度发展普及，呈现出井喷式发展态势。用户在享受更多位置服务的同时，也产生了大量位置数据信息，这些信息往往会明显或隐性地暴露用户的个人隐私信息，产生蝴蝶效应，引发更严重的个人隐私安全问题[3]。《Science》的“The end of privacy”[4]专题就曾指出，从用户的运动轨迹和位置信息，就能推理出其惯用路线、家庭工作单位地点、健康状况、生活习惯、兴趣爱好、社交关系、平时乘坐交通工具[5]等个人隐私信息。位置相关敏感信息的泄露已成为LBS中最大的隐私威胁，也给LBS在军用、民用领域的全方位普及带来了前所未有的挑战。然而，在当前移动社交网络中，LBS的应用几乎都离不开多方之间位置信息的实时共享[6]，其中因共享导致的隐私泄露问题不容忽视。因此，如何在共享的同时实现对用户的位置隐私保护，已经成为研究者关注的热点和亟待解决的问题，深入研究符合网络特点和现实需求的LBS位置隐私保护技术具有广阔的应用前景和重要的现实意义。

传统的位置信息共享过程实行的是刚性的“全部或全不”隐私保护策略，无法满足用户的个性化、弹性位置隐私保护需求。为此，Marias等[7]最先提出将秘密共享技术用于位置信息的隐私保护，将用户位置信息利用随机数加密拆分成多个份额，并存放于多个STS（share the secret）服务器中，当用户发起位置服务时，位置服务器需要向每个STS服务器发出申请获得份额。虽然，该方案因引入额外的存储服务器会增加新的性能瓶颈与安全风险，也无法根据不同访问权限提供分级精度的位置共享结果，但是，其提出的多服务器秘密共享存储技术非常值得借鉴。Dürr等[8]借鉴多服务器存储的方法提出了在不可信系统中利用秘密共享策略实现位置共享隐私保护。该方案将系统假设为部分可信，基于坐标变换和空间模糊设计了位置秘密共享方法，分发有限精度的位置份额给多个位置服务器，不同精度的份额集合可重构出不同程度模糊的位置信息。但是，该方案有两个份额产生算法，较为复杂，多级别的位置信息需要多次共享，用户终端计算量较大。为了克服上述缺点，Skvortsov等[9]在开放的网络环境下，将精确位置模糊成具有不同半径的圆形区域，令攻击者从一定数量的份额中再难得到更加精确的位置信息。但是，该方案在较长时间内目标位置更新时生成的份额并不更新，仅适用于“签到”模式，且存储份额的服务器发生问题时，仍会泄露一定精度的目标位置信息。同时，Wernke等[10]提出了Pshare方案。该方案是第一个针对语义位置的多秘密共享隐私保护方案，解决了连续位置更新问题，增强了算法抵抗多种攻击的鲁棒性，并在后续研究中进行了优化和仿真[11–12]。然而，上述方案的计算量较大，当位置份额数量或参与存储份额的位置服务器增加时，其计算份额和重构位置的运算开销也会急剧增加，在移动互联网中资源受限的用户终端上并不适用。2017年，Skvortsov等[13]改变了之前文献[8–9, 11–12]方案中一直采用的“平等份额分发”模式，而预设服务器具有不同的可信级，可信度高的服务器能够存储更高精度的位置信息，反之亦然。但由于可信度高的服务器存储的是更高精度（更多数量）份额，该类服务器易变成攻击热点，且该方案直接采用一般概率信任模型[14]进行分级，需要额外维护管理一个服务器信任分级数据库。

综上所述，虽然LBS中位置共享隐私保护问题没有得到完美解决，但这些方案将位置信息转化为一系列份额分发给多个位置服务器以实现隐私保护的思想具有可借鉴性。作者针对多用户位置共享中的好友查找应用[15–16]，基于弹性位置隐私保护策略，提出了一种能够满足用户个性化需求的分级位置共享隐私保护方案。本方案不需要引入其他服务器，也不依赖于位置服务器集的可信度，利用基于中国剩余定理的门限可变多秘密共享方法弹性地满足用户不同精度位置信息的共享需求。

1　方案描述

1.1　系统模型

如图1所示，方案的系统模型主要由定位系统和位置隐私保护系统两部分组成。其中，位置隐私保护系统由查询目标Q_o、用户终端C_*（共享Q_o位置的用户）以及n个位置服务器集合（$sp_1, sp_2, \cdots, sp_n$）组成。

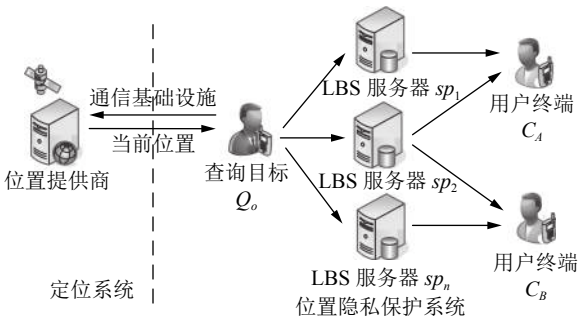

图 1　多用户位置共享隐私保护模型

Fig. 1　Model of location sharing privacy protection for multi-users

1.2 位置转换模型

用户通过两种位置转换模型可灵活地将真实位置坐标转换成不同精度的位置信息分级共享给其他用户，即自主把握共享位置的对象与精度级别，这更有利于满足实际网络环境中用户的个性化隐私需求。

1）地理位置转换模型

通常情况下，通过定位系统获得的位置经纬度坐标一般都以度（°）、分（′）、秒（″）表示，若用G表示查询目标的精确位置，则用户真实位置的地理坐标数字表示为$G=\{I_1^\circ,I_2',I_3'',J_1^\circ,J_2',J_3''\}$。用$G_{L_i}=p(G,L_i)=\{T_{i,1},T_{i,2},\cdots,T_{i,r_{L_i}}\}$表示由真实位置而来的精度级别为$L_i$的位置信息。此时，根据度、分、秒的精度级别，可将地理位置转换成：$G_{L_1}=p(G,L_1)=\{I_1^\circ,J_1^\circ\}=\{T_{1,1},T_{1,2}\}$即$L_1$精度级（精确到度）的位置坐标；$G_{L_2}=p(G,L_2)=\{I_1^\circ,I_2',J_1^\circ,J_2'\}=\{T_{2,1},T_{2,2},T_{2,3},T_{2,4}\}$即$L_2$精度级（精确到分）的位置坐标；$G_{L_3}=p(G,L_3)=\{I_1^\circ,I_2',I_3'',J_1^\circ,J_2',J_3''\}=\{T_{3,1},T_{3,2},\cdots,T_{3,6}\}$即$L_3$精度级（精确到秒）的位置坐标。$G_{L_1}$、$G_{L_2}$、$G_{L_3}$构成了$L_{\max}=3$的不同精度级别的位置信息，即为需要共享的秘密，每组的秘密个数分别为$r_1=2,r_2=4,r_3=6$。

2）语义位置转换模型

根据通用规则，语义位置通常表示为{国家，省（州），市，区（县），乡/镇（街道），门牌号}，可根据一定数字映射关系（规则）建立语义转换数据库，将语义位置对应表示为数字。如语义位置{中国，陕西省，西安市，未央区，三桥武警路，66号}对应的数字坐标可转换为{0086, 71, 00, 86, 0010, 66}。精确位置的语义位置对应的数字坐标可表示为$G=\{s_1,s_2,\cdots,s_{L_{\max}}\}$。与地理位置转换类似，查询目标$Q_o$能够灵活地将不同精度级别的语义位置转化为不同的数字坐标。其语义位置可定义为以下精度递增的6个级别：$G_{L_1}=p(G,L_1)=\{s_1\}=\{T_{1,1}\}$表示$L_1$精度级的位置坐标，即共享的位置信息仅体现$Q_o$所在的国家；$G_{L_2}=p(G,L_2)=\{s_1,s_2\}=\{T_{2,1},T_{2,2}\}$表示$L_2$精度级（精确到省域）的位置坐标；以此类推，$G_{L_3}=p(G,L_3)=\{s_1,s_2,s_3\}=\{T_{3,1},T_{3,2},T_{3,3}\}$表示$L_3$精度级（精确到市域）的位置坐标；$G_{L_4}$表示$L_4$精度级（精确到区（县）域）的位置坐标；$G_{L_5}$表示$L_5$精度级（精确到乡（镇）街道域）的位置坐标；$G_{L_6}$表示$L_6$精度级（精确到门牌域）的位置坐标。由此，$G_{L_1},G_{L_2},\cdots,G_{L_6}$构成$L_{\max}=6$的不同精度级别的位置信息，即为需要共享的秘密，每组的秘密个数分别为$r_1=1,r_2=2,r_3=3,r_4=4,r_5=5,r_6=6$。

1.3 位置信息共享机制

本方案中位置信息共享机制将Q_o定义的$L_{\max}$个不同精度级的位置信息，并打包成一组秘密进行处理转换，采用基于中国剩余定理的多秘密共享方法[17]对位置份额进行一次分发，可使不同位置份额集重构出不同精度级别的位置信息。共享机制主要包括3个部分：系统参数初始化、秘密分发和秘密重构。

1.3.1 初始化

$G_{L_1},G_{L_2},\cdots,G_{L_{\max}}$构成$L_{\max}$组需要共享的秘密集，每组的秘密个数分别为$r_{L_1},r_{L_2},\cdots,r_{L_{\max}}$。各组秘密分别根据不同的$(t_i,n)$的门限访问进行共享，其中，$t_i$为计算$G_{L_i}$时需要的份额数量（门限值），$1\le i\le L_{\max}$，门限值满足$1\le t_1\le t_2\le\cdots\le t_{L_{\max}}$。$Q_o$在分发秘密时将门限访问结构、参与的位置服务器等信息在公告牌上发布。

1.3.2 份额生成与分发

Q_o将不同精度级别的位置信息与不同信任关系的用户共享，其中，精度级别和C_*的对应关系由Q_o自行确定发送给位置服务器。Q_o首先为每个参与的位置服务器$sp_1,sp_2,\cdots,sp_n$产生并发送一个主份额，产生过程如下：

1）查询目标选择$L_{\max}$个互不相同的素数$q_1<q_2<\cdots<q_{L_{\max}}$，满足$T_{i,j}<q_i(1\le i\le L_{\max},j=1,2,\cdots,r_{L_i})$，$n<q_1$和$r_{L_{\max}}<q_1$；若$r_{L_{\max}}>t_1$，则还要满足$r_{L_{\max}}-t_1+1+n<q_1$。

2）若$r_{L_{\max}}>t_1$，在区间$[r_{L_{\max}}-t_1+1,q_1)$上任意选择n个不同整数$x_1,x_2,\cdots,x_n$分别作为$sp_1,sp_2,\cdots,sp_n$的公开身份标志；若$r_{L_{\max}}\le t_1$，在$[1,q_1]$上任意选择n个不同整数$x_1,x_2,\cdots,x_n$作为$sp_1,sp_2,\cdots,sp_n$的公开身份标志。

3）令$a_0,a_1,\cdots,a_{r_{L_{\max}}-1}$分别为下列$r_{L_{\max}}$组恒等式的解：

$$\begin{cases}\begin{cases}a_0\equiv T_{1,1}\bmod q_1,\\a_0\equiv T_{2,1}\bmod q_2,\\\quad\vdots\\a_0\equiv T_{L_{\max},1}\bmod q_{L_{\max}};\end{cases}\quad\begin{cases}a_1\equiv T_{1,2}\bmod q_1,\\a_1\equiv T_{2,2}\bmod q_2,\\\quad\vdots\\a_1\equiv T_{L_{\max},2}\bmod q_{L_{\max}};\end{cases}\\\cdots\\\begin{cases}a_{r_{L_1}-1}\equiv T_{1,r_{L_1}}\bmod q_1,\\a_{r_{L_1}-1}\equiv T_{2,r_{L_1}}\bmod q_2,\\\quad\vdots\\a_{r_{L_1}-1}\equiv T_{L_{\max},r_{L_1}}\bmod q_{L_{\max}};\end{cases}\quad\begin{cases}a_{r_{L_1}}\equiv 0\bmod q_1,\\a_{r_{L_1}}\equiv T_{2,r_{L_1}+1}\bmod q_2,\\\quad\vdots\\a_{r_{L_1}}\equiv T_{L_{\max},r_{L_1}+1}\bmod q_{L_{\max}};\end{cases}\\\cdots\\\begin{cases}a_{r_{L_{\max}}-1}\equiv 0\bmod q_1,\\\quad\vdots\\a_{r_{L_{\max}}-1}\equiv 0\bmod q_{L_{\max}-1},\\a_{r_{L_{\max}}-1}\equiv T_{L_{\max},r_{L_{\max}}}\bmod q_{L_{\max}}\end{cases}\end{cases}\tag{1}$$

由中国剩余定理可求得式（1）的解$a_0,a_1,\cdots,a_{r_{L_{\max}}-1}$。

4）构造多项式。令$M=\prod_{i=1}^{L_{\max}}q_i$：

① 若$r_{L_{\max}}>t_1$，对于$i=1,2,\cdots,L_{\max}-1$，计算b_{t_i}，

$b_{t_i+1},\cdots,b_{t_{i+1}-1}$:

设$j=t_i,t_i+1,\cdots,t_{i+1}-1$, $b_j=z_j\times\lambda_j\times\prod_{u=1}^{i}q_u \bmod M$, 其中, z_j为$\{1,2,\cdots,q_i-1\}$上的任意整数, λ_j为任意非零整数, 则构造一个多项式, 此多项式的阶为$(r_{L_{\max}}+t_{L_{\max}}-t_1-1)$:

$$F(x)=a_0+a_1x+\cdots+a_{r_{L_{\max}}-1}x^{r_{L_{\max}}-1}+b_{t_1}x^{r_{L_{\max}}}+\cdots+b_{t_{L_{\max}}-1}x^{r_{L_{\max}}+t_{L_{\max}}-t_1-1} \tag{2}$$

②若$r_{L_{\max}}\le t_1$, 则任意选择$(t_1-r_{L_{\max}})$个整数, 满足$1<a_{r_{L_{\max}}},a_{r_{L_{\max}}+1},\cdots,a_{t_1-1}<M$, 设$j=t_i,t_i+1,\cdots,t_{i+1}-1$, $a_j=z_j\times\lambda_j\times\prod_{u=1}^{i}q_u \bmod M$, 其中, z_j为$\{1,2,\cdots,q_i-1\}$上的任意整数, λ_j为任意非零整数, 构造如下多项式, 此多项式阶为$(t_{L_{\max}}-1)$:

$$F(x)=a_0+a_1x+\cdots+a_{t_{L_{\max}}-1}x^{t_{L_{\max}}-1} \tag{3}$$

5)计算$sp_1,sp_2,\cdots,sp_n$的主份额$S_i(1\le i\le n)$:

$$S_i=F(x_i) \bmod M \tag{4}$$

6)若$r_{L_{\max}}>t_1$, 计算公共值$d_i(1\le i\le r_{L_{\max}}-t_1)$:

$$d_i=F(i) \bmod M \tag{5}$$

7)将S_i通过安全信道传送给各参与的位置服务器sp_i, 公布$q_1,q_2,\cdots,q_{L_{\max}}$; 若$r_{L_{\max}}>t_1$, 再公布公共值$d_1,d_2,\cdots,d_{r_{L_{\max}}-t_1}$。由位置服务器存储并管理收到的份额及公共值。

1.3.3　秘密重构

Q_o自主定义不同用户对自身位置的访问权限级别并形成“好友列表”发送给位置服务器。需要共享Q_o位置时, 位置服务器运行访问控制机制(查看Q_o“好友列表”)后, 将生成的影子份额发送给该用户即可重构出对应精度级别的位置信息。

假设用户C_A要对Q_o进行好友查找, 共享其位置, Q_o确定该用户的访问权限等级为L_i级:

1)若$r_{L_{\max}}>t_1$, 由于$a_j\equiv 0 \bmod q_i(j=r_{L_i},r_{L_{i+1}},\cdots,r_{L_{\max}-1})$和$b_j\equiv 0 \bmod q_i(j=t_i,t_i+1,\cdots,t_{L_{\max}}-1)$, 则$G_{L_i}$对应的秘密多项式为:

$$F_i(x)=F(x) \bmod q_i(\in\mathbb{Z}_{q_i}[x]) \tag{6}$$

且满足$\deg(F_i(x))\le r_{L_{\max}}+t_i-t_1-1$。

t_i个位置服务器$sp_j(1\le j\le t_i)$向用户发送其生成的影子份额:

$$S_{i,j}=S_j \bmod q_i \tag{7}$$

则用户得到t_i个点$(x_1,S_{i,1}),(x_2,S_{i,2}),\cdots,(x_{t_i},S_{i,t_i})$, 再利用已公布的公共信息$d_1,d_2,\cdots,d_{r_{L_{\max}}-t_1}$, 用户可分别计算:

$$\begin{cases} d'_1\equiv d_1 \bmod q_i,\\ d'_2\equiv d_2 \bmod q_i,\\ \quad\vdots\\ d'_{r_{L_{\max}}-t_1}\equiv d_{r_{L_{\max}}-t_1} \bmod q_i \end{cases} \tag{8}$$

则用户又可得到$(r_{L_{\max}}-t_1)$个点$(1,d'_1),(2,d'_2),\cdots,(r_{L_{\max}-t_1},d'_{r_{L_{\max}}-t_1})$, 利用Lagrange插值多项式重构秘密多项式$F_i(x)$:

$$\begin{aligned} F_i(x)&=F(x) \bmod q_i=\\ &\left(\sum_{j=1}^{t_i}\left(S_{i,j}\prod_{h=1,h\ne j}^{t_i}\frac{x-x_h}{x_j-x_h}\prod_{v=1}^{r_{L_{\max}}-t_1}\frac{x-v}{x_j-v}\right)+\right.\\ &\left.\sum_{j=1}^{r_{L_{\max}}-t_1}\left(d'_j\prod_{v=1,v\ne j}^{r_{L_{\max}}-t_1}\frac{x-v}{j-v}\prod_{h=1}^{t_i}\frac{x-x_h}{j-x_h}\right)\right) \bmod q_i=\\ &a_0+a_1x+\cdots+a_{r_{L_{\max}}-1}x^{r_{L_{\max}}-1}+\\ &b_{t_1}x^{r_{L_{\max}}}+\cdots+b_{t_{L_{\max}}-1}x^{r_{L_{\max}}+t_{L_{\max}}-t_1-1} \bmod q_i=\\ &a_0+a_1x+\cdots+a_{r_{L_{\max}}-1}x^{r_{L_{\max}}-1}+\\ &b_{t_1}x^{r_{L_{\max}}}+\cdots+b_{t_i-1}x^{r_{L_{\max}}+t_i-t_1-1} \bmod q_i \end{aligned} \tag{9}$$

由$F_i(x)$的前r_{L_i}个系数即可恢复出精度为L_i级的位置坐标$G_{L_i}=\{T_{L_i,1},T_{L_i,2},\cdots,T_{L_i,r_{L_i}}\}$, 其中:

$$\begin{cases} T_{L_i,1}=a_0 \bmod q_i,\\ T_{L_i,2}=a_1 \bmod q_i,\\ \quad\vdots\\ T_{L_i,r_{L_i}}=a_{r_{L_i}-1} \bmod q_i \end{cases} \tag{10}$$

2)若$r_{L_{\max}}\le t_1$, 则G_{L_i}对应的秘密多项式为:

$$F_i(x)=F(x) \bmod q_i(\in\mathbb{Z}_{q_i}[x]) \tag{11}$$

且满足$\deg(F_i(x))\le t_i-1$。

t_i个位置服务器$sp_j(1\le j\le t_i)$向用户发送其生成的影子份额:

$$S_{i,j}=S_j \bmod q_i \tag{12}$$

则用户可得到t_i个点$(x_1,S_{i,1}),(x_2,S_{i,2}),\cdots,(x_{t_i},S_{i,t_i})$, 利用Lagrange插值多项式重构秘密多项式:

$$\begin{aligned} F_i(x)&=F(x) \bmod q_i=\\ &\left(\sum_{j=1}^{t_i}\left(S_{i,j}\prod_{h=1,h\ne j}^{t_i}\frac{x-x_h}{x_j-x_h}\right)\right) \bmod q_i=\\ &a_0+a_1x+\cdots+a_{t_{L_{\max}}-1}x^{t_{L_{\max}}-1} \bmod q_i=\\ &a_0+a_1x+\cdots+a_{r_{L_i}-1}x^{r_{L_i}-1}+\\ &a_{r_{L_{\max}}}x^{r_{L_{\max}}}+\cdots+a_{t_i-1}x^{t_i-1} \bmod q_i \end{aligned} \tag{13}$$

利用式(10)计算得出$F_i(x)$的前r_{L_i}个系数即可恢复出精度为L_i级的位置坐标$G_{L_i}=\{T_{L_i,1},T_{L_i,2},\cdots,T_{L_i,r_{L_i}}\}$。

1.4　位置共享隐私保护方案

作者设计的多用户位置共享分级隐私保护方案的执行过程如图2所示。

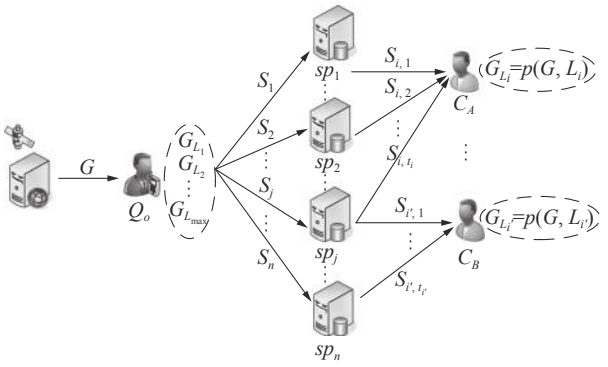

图 2 多用户位置共享隐私保护执行过程示意图

Fig. 2 Implementation of location sharing privacy protection for multi-users

Q_o通过定位系统确定自身当前的准确位置G，通过运行终端上的位置转换模型将G转换为不同精度级别的位置数字表示G_{L_i}，再利用多秘密共享份额生成算法将$G_{L_1},G_{L_2},\cdots,G_{L_{\max}}$打包生成主份额$S_i(1\le i\le n)$，分发给$sp_1,sp_2,\cdots,sp_n$存储管理。$C_A$或$C_B$对$Q_o$进行好友查找位置共享时，相应数量的位置服务器会根据Q_o“好友列表”和各自的访问权限等级提供影子份额，C_A和C_B即可重构出其对应精度级的Q_o位置共享结果。具体步骤如下：

1）Q_o通过定位系统，获取自身位置坐标G。

2）Q_o启用位置转换模型，根据自身隐私需求将位置转换为$L_{\max}$个不同精度级的位置数据，$p(G,L_i)$表示G对应的L_i精度级的位置数据：

$$\begin{cases} G_{L_1}=p(G,L_1),\\ G_{L_2}=p(G,L_2),\\ \quad\vdots\\ G_{L\max}=p(G,L_{\max}) \end{cases} \tag{14}$$

3）Q_o利用位置信息共享机制将不同精度级别的位置数字坐标作为一组秘密进行转换分割，产生秘密份额并计算主份额$S_i(1\le i\le n)$。

4）Q_o将主份额$S_i(1\le i\le n)$发送给位置服务器集中n个不同的位置服务器$sp_1,sp_2,\cdots,sp_n$，位置服务器存储管理所得主份额，且最多只能获得一个主份额；每个位置服务器执行一个访问控制机制，用户的访问权限由Q_o自行定义。

5）当C_A查询共享Q_o位置时，位置服务器会在Q_o的“好友列表”中查询其对应的访问权限等级，假设C_A被Q_o允许获得的位置精度级别为L_i，则C_A可访问t_i个位置服务器获得影子份额集。

6）被授权访问的t_i个位置服务器根据存储的份额和L_i计算其影子份额$S_{i,j}$，发送给C_A。

7）C_A收到影子份额后，执行秘密重构恢复出$G_{L_i}=p(G,L_i)$，完成好友位置查找，共享得到精度级为L_i的位置信息。

2 方案分析

2.1 安全性分析

在复杂的移动社交网络中，LBS应用中的隐私威胁主要在于不可信的sp集和其他网络用户[18]。sp可能会在利益驱动下滥用或故意泄露其存储的位置信息，其他用户会伺机窥探推测他人的位置隐私，二者往往也会因自身安全漏洞将存储的位置信息及查询结果泄露给攻击者。

引 理 本方案能够实现对Q_o位置共享的分级隐私保护，并能抵抗：1）对单个位置服务器的攻击；2）数量少于t_1的多个位置服务器合谋攻击；3）用户（L_i级）与数量少于t_{i+1}的多个位置服务器合谋攻击；4）L_i级用户之间、L_i级与L_{i+1}级用户之间的合谋攻击。

证明：

1）方案的正确性、可行性、有效性在文献[19]中利用多项式形式的中国剩余定理及数论中插值多项式唯一性定理已被详细证明，在此不再赘述。

2）对于任何访问结构，都存在实现该访问结构上完备的秘密共享方案[20]，即满足任意授权子集都可以很容易地恢复出秘密，但任意的非授权子集都得不到关于秘密的任何信息。当$r_{L_{\max}}>t_1$时，G_{L_i}对应的秘密多项式阶为$\deg(F_i(x))\le r_{L_{\max}}+t_i-t_1-1$，至少需要$(r_{L_{\max}}+t_i-t_1)$个点才能计算出$F_i(x)$，而事先在发送主份额阶段公布了$(r_{L_{\max}}-t_1)$个点$d_1,d_2,\cdots,d_{r_{L_{\max}}-t_1}$的值。至少还需要$t_i$个位置服务器的影子份额才能确定$F_i(x)$以获得$G_{L_i}$，少于$t_i$个位置服务器的影子份额则无法确定$F_i(x)$，也得不到关于所共享的多组秘密的任何信息，即满足Shamir门限方案安全性特点；同理，当$r_{L_{\max}}\le t_1$时，G_{L_i}对应的秘密多项式阶为$\deg(F_i(x))\le t_i-1$，因此，至少需要t_i个位置服务器的影子份额才能确定$F_i(x)$以获得G_{L_i}，而少于t_i个位置服务器的影子份额无法确定$F_i(x)$，也得不到关于所共享的多组秘密的任何信息，这也满足Shamir门限方案安全性特点。因此，本方案同Shamir的门限方案一样是安全完备的。能够抵抗单个服务器攻击或低于最小门限值个数t_1的服务器合谋攻击，位置服务器也无法通过其所掌握的份额对位置信息进行有用的推测。

3）用户与多个位置服务器的合谋攻击实质上是多个位置服务器合谋攻击的特殊情况[12]。本方案中，即使对应位置精度级L_i的用户联合门限访问结构的授权子集中t_i个位置服务器的主份额计算出G_{L_1}，$G_{L_2},\cdots,G_{L_{i-1}}$，也并不影响系统的安全性，这相当于本身可获得更高精度位置结果的用户自然也能够获知精度更低的位置结果。因此，本方案能够抵抗用户与授权子集中t_i个位置服务器的合谋攻击；进一步地，

除了$sp_1, sp_2, \cdots, sp_{t_i}$与用户合谋外，还需要属于$t_{i+1}$门限访问结构的授权子集中至少$(t_{i+1}-t_i)$个服务器与用户合谋，提供其计算出的影子份额才能重构出更高精度的位置结果$G_{L_{i+1}}$，这正说明本方案具有灵活分级隐私保护属性，即当更多服务器提供份额时能够提高重构位置信息的精度。综上所述，本方案能够抵抗L_i级用户与少于t_{i+1}个数量的位置服务器合谋攻击。

4）假设用户C_A、C_B及C_C合谋，C_A和C_B都可计算出G_{L_i}，C_C可计算出$G_{L_{i+1}}$。显然，由于C_A和C_B都能够利用t_i个不同的份额计算确定出G_{L_i}的多项式$F_i(x)$，但根据$F_i(x)$的唯一确定性，即使用多于t_i个属于同一级别G_{L_i}的影子份额，也只能确定出同一个多项式$F_i(x)$，仍然只能得到G_{L_i}。由于本方案中各精度级的位置信息的多项式是相互独立生成且具有唯一性，不会因合谋后份额增加得到关于$F_{i+1}(x)$及G_{L_i+1}的任何有用信息，C_A与C_B合谋也不会得到新的关于G_{L_i+1}的有用信息。即使不与C_A合谋，C_C本身也能够计算出G_{L_i+1}，C_A提供其拥有的影子份额也不会带来关于G_{L_i+2}及其相应多项式$F_{i+2}(x)$的任何有用信息。

本方案与文献[11–13]方案在是否需要可信sp集、应用对象范围、位置份额、抵抗攻击类型等方面的对比见表1。如表1所示，与同类方案相比，本方案可同时实现地理和语义位置共享的分级隐私保护、抵抗多种常见攻击，安全性高且不依赖于sp集的可信度。

表 1　同类方案对比

Tab. 1　Comparison of similar schemes

方案	sp集可信度	应用对象	位置份额	抵抗攻击类型
文献[11]	部分可信	地理位置	有限精度位置	无
文献[12]	部分可信	地理位置	有限精度位置	无
文献[13]	不可信	地理位置和语义位置	无意义	单个服务器攻击、用户合谋攻击、服务器合谋攻击
本方案	不可信	地理位置和语义位置	无意义	单个服务器攻击、用户合谋攻击、服务器合谋攻击

2.2　性能分析

本方案的运算主要分为3部分：Q_o端主要完成自身不同精度级别的位置坐标转换和利用基于中国剩余定理生成主份额的计算，位置服务器端主要负责生成影子份额的计算，C_*端主要通过拉格朗日插值公式计算重构出其对应级别的位置信息。下面以第1.2节中地理位置坐标为仿真对象，其中，G_{L_1}、G_{L_2}、G_{L_3}构成了$L_{\max}=3$组不同精度级别的位置信息，每组的秘密个数分别为$r_1=2$，$r_2=4$，$r_3=6$，分别对Q_o、位置服务器和C_*的终端进行仿真实验。实验环境是：64 bit的Windows 10操作系统，CPU为4210M的Intel core i5，内存为12 GB DDR3L，运行平台为Python 3.5，运行软件为PyCharm2018.2。

实验仿真结果中，n变化时的计算时间对数坐标见图3。如图3所示，各位置服务器及Q_o、C_*端的计算开销小，Q_o端计算开销保持在10^{-4}～10^{-3} s级之间，C_*端计算开销保持在10^{-1}～1 s级之间，位置服务器端计算开销保持在10～10^{-4} s级之间。且C_*端、各服务器的计算时间并未因n增加而剧增，Q_o的计算时间发生了10^{-3} s级的线性变化。

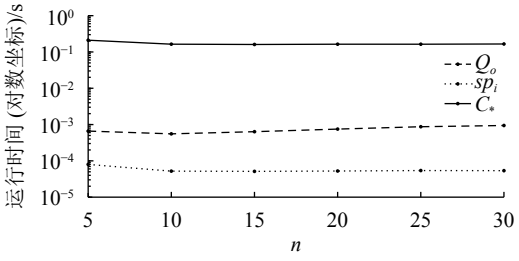

图 3　n变化时的计算时间

Fig. 3　Computation time of changing n

t_3变化时的计算时间对数坐标见图4。如图4所示，最高精度位置信息恢复门限值t_3 $(t_3 \ge t_2 \ge t_1)$增加时，各位置服务器及Q_o端的计算时间并未因t_3增加而显著增加，C_*端的计算时间发生了秒级增加。

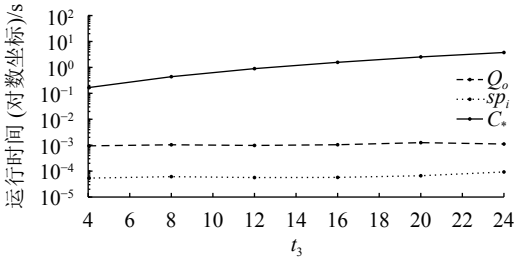

图 4　t_3变化时的计算时间

Fig. 4　Computation time of changing t_3

t_1变化时的计算时间对数坐标见图5。如图5所示，最低精度位置信息恢复门限值t_1 $(t_3 \ge t_2 \ge t_1)$增加，Q_o端、各位置服务器及C_*端的计算时间均未显著增加。

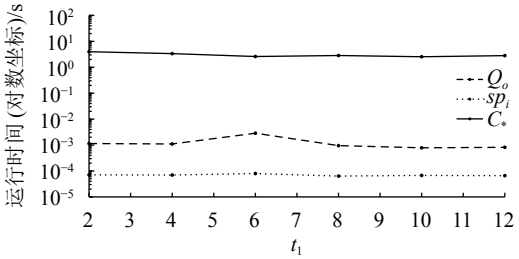

图 5　t_1变化时计算时间

Fig. 5　Computation time of changing t_1

t_2变化时的计算时间对数坐标见图6。如图6所示，当中间精度位置信息恢复门限值t_2增加时，Q_o端、各位置服务器的计算时间并未显著增加，C_*端计算时间发生了秒级增加。

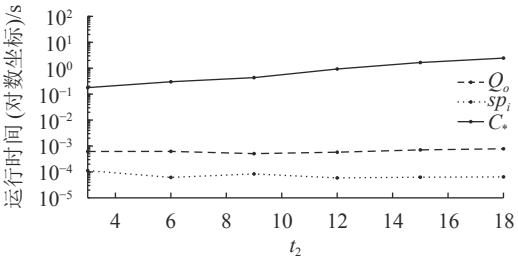

图 6 t_2变化时计算时间

Fig. 6 Computation time of changing t_2

本方案与文献[11–13]方案在运行时间上的对比见表2。如表2所示，即使在加入对大素数的素性判定与选取运算、未采用中国剩余定理快速算法的最坏情况下，本方案的效率相对于同类方案的效率仍然更高，实现简单，计算量小，性能更加稳定。

表 2 运行时间对比

Tab. 2 Comparison of running time

方案	运行时间/s（n=5～15）	时间量级
文献[11]算法1	0.21～8.65	10^{-1}～10 s级
文献[11]算法2	32.60～2 273.00	≫ 1 s级
文献[12]算法	0.17～0.74	10^{-1}～1 s级
文献[13]算法	0.12～0.69	10^{-1}～1 s级
本方案	0.16～0.21	10^{-1}～1 s级

这主要是由于本方案将多个不同精度级别的位置信息打包成一个整体，在(t_i,n)的门限访问结构上分别共享$L_{\max}$组不同精度位置信息$G_{L_1},G_{L_2},\cdots,G_{L_{\max}}$，分发过程只需通过中国剩余定理构造一个$(r_{L_{\max}}+t_{L_{\max}}-t_1-1)$阶（$r_{L_{\max}}\le t_1$时）或$(t_{L_{\max}}-1)$阶（$r_{L_{\max}}>t_1$时）拉格朗日多项式，即仅需要一个逻辑步骤和一次秘密分发过程，就可共享$L_{\max}$组不同精度的位置信息。而其他方案中共享多组位置信息就需要进行多次秘密分发、重复计算量大的情况，相比而言，本方案计算量更小。Q_o端的计算复杂度为$o(r_{L_{\max}}\log r_{L_{\max}})$，$L_i$级用户端的计算复杂度为$o\left((r_{L_{\max}}+t_i-t_1-1)^2\right)$（$r_{L_{\max}}>t_1$时）或$o\left((t_i-1)^2\right)$（$r_{L_{\max}}\le t_1$时），服务器端的计算量为$t_i$次整数取模运算。并且，只要参数值在合理范围内变大时，本方案增加的计算开销可忽略不计，即不会发生剧增。实质上，基于中国剩余定理的同余类秘密共享门限方案早已被证明比Shamir的方案更加高效[21]，因此，本方案比同类Shamir方案更高效。

若一定时间内Q_o位置变化不大，仅仅是$G_{L_{\max}}$发生变化而其他更低精度的数字坐标不变时，更新份额仅需对式（1）中最后几组同余方程组进行重新求解即可，而不需要重新执行整个秘密共享份额生成算法，进一步节省了计算量，提高了方案效率。此外，本方案的公共信息量仅为$L_{\max}$或$(r_{L_{\max}}-t_1+L_{\max})$个，在同类方案中信息量较小。

3 结 论

相对于传统“全部或全不”的刚性位置隐私保护策略，弹性的分级隐私保护策略更加符合移动互联网中用户的个性化需求。本方案通过地理和语义位置转换模型保证用户能够灵活地自定义其共享位置的精度级别及可访问对象，并利用基于中国剩余定理的门限可变多秘密共享方法，将定义的多精度级的位置信息作为整体打包转换分割，实现了一次份额分发就能使不同共享对象重构出不同精度的位置信息，在不可信环境下完成了多用户位置共享的弹性隐私保护。仿真实验分析进一步表明，本方案计算复杂度低，通信开销小，鲁棒性好，与同类方案相比更为高效，即使在网络资源受限的环境中和计算能力受限的用户终端上也同样适用。此外，本方案除可应用于好友查找等基于位置共享的社交服务场景外，也可扩展使用至军队信息化层级指挥作战系统，在基于位置共享的群组协同作战领域有着广阔的应用前景。

参考文献：

[1] Wang Yuhang,Zhang Hongli,Yu Xiangzhan.Research on location privacy in mobile Internet[J].Journal on Communications,2015,36(9):230–243.[王宇航,张宏莉,余翔湛.移动互联网中的位置隐私保护研究[J].通信学报,2015,36(9):230–243.]

[2] Lee B,Oh J,Yu H,et al.Protecting location privacy using location semantics[C]//Proceedings of the 17th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD'11).New York:ACM,2011:1289–1297.DOI:10.1145/2020408.2020602

[3] Kalnis P,Ghinita G,Mouratidis K,et al.Preventing location-based identity inference in anonymous spatial queries[J].IEEE Transactions on Knowledge and Data Engineering,2007,19(12):1719–1733.

[4] Enserink M,Chin G.The end of privacy[J].Science,2015,347(6221):490–491.

[5] Xiong Xingxing,Liu Shubo,Li Dan,et al.Private electric vehicle charging location aggregation based on local differential privacy[J].Advanced Engineering Sciences,2019,51(2):137–143.[熊星星,刘树波,李丹,等.基于局部差分隐私的电动汽车充电位置隐私汇聚[J].工程科学与技术,2019,51(2):137–143.]

[6] Li J,Yan Hongyang,Liu Zheli,et al.Location-sharing systems with enhanced privacy in mobile online social networks[J].IEEE Systems Journal,2017,11(2):439–448.

[7] Marias G F,Delakouridis C,Kazatzopoulos L,et al.Location

privacy through secret sharing techniques[C]//Proceedings of the Sixth IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks.Taormina-Giardini Naxos:IEEE,2005:614–620.

[8] Dürr F,Skvortsov P,Rothermel K.Position sharing for location privacy in non-trusted systems[C]//Proceedings of the 2011 IEEE International Conference on Pervasive Computing and Communications (PerCom).Seattle:IEEE,2011:189–196.

[9] Skvortsov P,Dürr F,Rothermel K.Map-aware position sharing for location privacy in non-trusted systems[M]//Pervasive Computing.Berlin:Springer,2012:388–405.

[10] Wernke M,Dürr F,Rothermel K.PShare:Position sharing for location privacy based on multi-secret sharing[C]//Proceedings of the 2012 IEEE International Conference on Pervasive Computing and Communications.Lugano:IEEE,2012:153–161.

[11] Wernke M,Dürr F,Rothermel K.Efficient position sharing for location privacy using binary space partitioning[M]//Mobile and Ubiquitous Systems:Computing,Networking,and Services.Berlin:Springer,2013:263–275.

[12] Wernke M,Dürr F,Rothermel K.PShare:Ensuring location privacy in non-trusted systems through multi-secret sharing[J].Pervasive and Mobile Computing,2013,9(3):339–352.

[13] Skvortsov P,Schembera B,Dürr F,et al.Optimized secure position sharing with non-trusted servers[EB/OL].(2017–02–27)[2019–09–01].https://arxiv.org/abs/1702.08377.

[14] Kinateder M,Baschny E,Rothermel K.Towards a generic trust model—Comparison of various trust update algorithms[M]//Trust Management.Berlin:Springer,2005:177–192.

[15] Sadilek A,Kautz H,Bigham J P.Finding your friends and following them to where you are[C]//Proceedings of the Fifth ACM International Conference on Web Search and Data Mining (WSDM'12).New York:ACM,2012:723–732.

[16] Strassman M.2-Case study:Development of the find friend application[M]//Location-based Services.Holland:Elsevier,2004:27–39.

[17] Li Huixian.Study on theory and application of multi-secret sharing[D].Dalian:Dalian University of Technology,2006:44–50.[李慧贤.多秘密共享理论及其应用研究[D].大连:大连理工大学,2006:44–50.]

[18] Tyagi A,Sreenath N.A comparative study on privacy preserving techniques for location based services[J].British Journal of Mathematics & Computer Science,2015,10(4):1–25.

[19] Chan Chaowen,Chang C C.A scheme for threshold multi-secret sharing[J].Applied Mathematics and Computation,2005,166(1):1–14.

[20] Benaloh J,Leichter J.Generalized secret sharing and monotone functions[M]//Advances in Cryptology — CRYPTO'88.New York:Springer,1990:27–35.

[21] Asmuth C,Bloom J.A modular approach to key safeguarding[J].IEEE Transactions on Information Theory,1983,29(2):208–210.

（编辑　赵　婧）

引用格式：Wang Jingjing,Han Yiliang,Chen Jiayong,et al.A new location privacy protection scheme for multi-users[J].Advanced Engineering Sciences,2020,52(5):178–185.[汪晶晶,韩益亮,陈家勇,等.一种新的多用户位置隐私保护方案[J].工程科学与技术,2020,52(5):178–185.]