文章编号:1671-4229(2023)04-0066-11

基于属性代理重加密的车联网隐私保护方案

周　权[a]，曾志康[a]，王科梦[b]，陈梦龙[b]
(广州大学 a. 数学与信息科学学院，b. 计算机科学与网络工程学院，广东 广州　510006)

摘　要：车联网是未来智能交通系统的核心组成部分,在人们生活中发挥着重要的作用,但其存在的诸多安全问题,时刻威胁着人们的隐私安全。为更好地保护用户的位置隐私和减少资源的消耗,文章提出了一个基于属性代理重加密的车联网隐私保护方案。该方案在基于密文策略的属性加密(CP-ABE)的基础上,为用户提供隐私保护的细粒度方式,并与其他用户进行位置服务共享,然后在代理重加密的基础上实现将基于属性加密的密文转换为基于身份加密的密文,降低了用户加密时的计算开销。与此同时,该方案还支持一定程度关键字错误的隐私保护多关键字模糊搜索。安全性分析及实验表明,该方案具有抗隐私泄露、抗共谋攻击等的优点,并有良好的性能表现。

关键词：车联网；隐私保护；CP-ABE；代理重加密；计算开销
中图分类号：TP 309　　**文献标志码**：A

Privacy protection scheme of the Internet of Vehicles based on attribute-based proxy re-encryption

ZHOU Quan[a], *ZENG Zhi-kang*[a], *WANG Ke-meng*[b], *CHEN Meng-long*[b]
(a. School of Mathematics and Information Science, b. School of Computer Science and Cyber Engineering, Guangzhou University, Guangzhou 510006, China)

Abstract: The Internet of Vehicles is the core component of future intelligent transportation system and plays an important role in people's life. However, its many security problems are a constant threat to people's privacy security. In order to better protect users' location privacy and reduce resource overhead, this paper proposes a privacy protection scheme of the Internet of Vehicles based on attribute-based proxy re-encryption. This scheme provides a fine-grained way for users to share location services with the rest of users in a privacy-preserving way based on ciphertext policy-based attribute encryption (CP-ABE). Then, it implements the conversion of attribute-based encryption ciphertext to identity-based encryption ciphertext on the basis of proxy re-encryption, which reduces the computational overhead when the users encrypt. At the same time, this scheme also supports a privacy-preserving multi-keyword fuzzy search with a certain degree of keyword error. Security analysis and experiments show that this scheme is resistant to privacy leakage, collusion attacks, etc., and performs well.

Key words: Internet of Vehicles; privacy protection; CP-ABE; proxy re-encryption; computational overhead

车联网以新一代的移动通信技术为基础,实现了车辆内部、车与车、车与人、车与路、车与服务平台的全方位网络连接[1]。它既可以通过汽车超速预警、红绿灯预警等手段提醒驾驶员安全驾驶,又可以将车载和道路信

收稿日期：2022-09-28；**修回日期**：2022-12-15
基金项目：国家重点研发计划重点专项资助项目(2021YFA1000600)；国家自然科学基金资助项目(12171114)
作者简介：周权(1971—),男,副教授,博士. E-mail：zhouqq@gzhu.edu.cn
引文格式：周权,曾志康,王科梦, 等. 基于属性代理重加密的车联网隐私保护方案[J]. 广州大学学报(自然科学版),2023,22(4):66－76.

息及时地发送到云服务器,建立智能化的交通管理系统,从而提高道路安全和交通通行效率[2-3]。尽管它给人们的生活带来了诸多便利和一些便民的应用,如拼车[4-6]、打车[7-9]、寻找停车位[10-12]和导航[13-15]等,但也存在着泄露用户隐私的安全隐患,如恶意用户可通过数据挖掘等技术对收集到的用户数据进行分析,从而得到用户的敏感信息[16-17]。

为解决上述问题,学者们提出了许多隐私安全保护方案,但由于用户身份、位置数据的隐私性和其可用资源的局限性,现有的方案面临着许多挑战。一方面,基于同态加密、安全多方计算和群签名等的隐私保护方案虽能为用户提供高质量的位置服务,即可以对用户过去、现在或将来的位置数据进行加密,并且加密后的数据仍能生成精确的位置服务,但这些方案都存在着一些不足,如基于群签名的隐私保护方案,其群组构建和群密钥管理在动态性强、可拓展性高的车联网中有一定的局限性;另一方面,基于属性的加密机制为实现车辆间的安全通信和打破一对一的加密通信模式的限制提供了新的解决方式,如 CP-ABE。具体而言,基于 CP-ABE 的隐私保护方案是面向特定用户群体的加密机制,其在面向多个用户进行加密数据共享时,不需要对同样的数据进行不同用户密钥的多次加密,即可实现高效的细粒度加密数据共享,而在密文解密时,只要用户密钥中的属性集合满足加密数据密文中的访问控制策略,即可将密文进行解密,输出有效的明文,如文献[18]。但其密文解密的计算开销随着属性数量的增加而线性增加,这对于一些计算资源有限的用户来说,会带来巨大的负担。

为使得车联网中的用户在实现高效的细粒度加密数据共享的同时,降低其密文解密的计算开销,使用代理重加密机制来进行密文转换是一种较好的方式。具体而言,代理重加密机制支持在不需要解密密钥和泄露明文信息的前提下,将一个公钥加密的密文(如 ABE 密文)转换为另一个公钥加密的密文(如 IBE 密文),这样既保证了用户数据的安全性,又能实现数据的灵活访问和共享。

针对上述问题,本文提出一个基于属性代理重加密的车联网隐私保护方案,允许在网合法用户通过发起一个服务查询来进行基于位置的服务。与传统的基于 CP-ABE 的车联网隐私保护方案不同的是,本文不需要对请求用户生成的 ABE 密文进行解密操作,亦可完成相应的细粒度数据共享,其主要原因在于本文将协同用户的访问权限,验证外包给路边单元来完成。而对于具备访问权限的协同用户来说,将由路边单元对请求用户生成的 ABE 密文重加密为可由协同用户解密的 IBE 密文。本文所提方案在保护用户隐私安全的同时,还能实现高效的细粒度数据共享和较低的密文解密计算开销,其主要贡献如下:

(1)本文通过 CP-ABE 和代理重加密机制等提出了一个基于属性代理重加密的车联网隐私保护方案,可以有效地保护用户的隐私安全。用户先泛化自己的敏感位置数据,然后进行一次 CP-ABE 操作生成位置服务查询,并发送至服务提供商完成相应的基于位置的服务。在此期间,即使某些攻击者可以通过窃听、共谋等手段获取到用户的密文信息,也无法获得相应的明文信息。

(2)高效的细粒度数据共享和较低的密文解密计算开销。每一个用户都有其独特或者大众的属性,本文在 CP-ABE 的基础上,实现了高效的细粒度数据共享,并通过代理重加密机制,将需要复杂的密文解密计算的 ABE 密文转化为高效的 IBE 密文,从而有效地降低用户解密时的计算开销。

(3)安全性分析和实验表明,本文所提方案具有较高的安全性和较低的计算开销,在密文解密上的性能表现要优于目前已有的方案。

1　相关工作

近年来,车联网中基于位置服务的隐私问题引起了人们广泛关注,而为了更好地保护用户的隐私、解决车联网中存在的位置隐私泄露问题,学者们提出了许多解决方案,其大致可分为 3 类:基于匿名的位置隐私保护、基于模糊的位置隐私保护和基于密码学的位置隐私保护。

基于匿名的位置隐私保护最早可追溯到 2002 年由 Sweeney[19] 提出的 K-匿名,但当时其主要的应用是数据库中的隐私保护。Gruteser 等[20] 在 Sweeney 的基础上,首次将 K-匿名应用到位置隐私保护中。基于匿名的位置隐私保护的主要思想是当存在某些用户需要发起基于位置的服务时,先通过生成虚拟用户的位置信息(或协同获取其余用户的位置信息)构造匿名集,然后用这个匿名集替代用户的真实位置信息提交给位置服务提供商,以此实现用户的位置隐私保护。文献[21]提出了第一个以生成虚拟用户的方式为用户生成匿名集的方案。随后,为保证虚拟用户位置信息的有效性、不确定性和分散性,文献[22]利用匿名熵和有效距离等方法对现有的虚拟用户的生成算法进行了改进,但该方案需要一个可信第三方充当匿名服务器,为用户生成相应的虚拟用户。对此,学者们提出了无需可信第三方的分布式 K-匿名位置隐私保护方案[23-27]。文献[23]提出了第一个基于分布式 K-匿名的位置隐私保护方案,然而并不

是所有的用户都关心自己的位置隐私,这导致发起位置服务协同的用户时常难以获得足够多的位置信息构造匿名集,对此,学者们提出了用户激励机制[24-27],通过给定相应的"奖励"激励用户积极地参与用户协同。

由 Dwork[28] 于 2006 年提出的差分隐私是常见的一种基于模糊的位置隐私保护方法,其主要思想是通过在原有数据中添加噪声,而不改变数据本身的统计学意义,以此来保护原有数据的隐私安全,但直接利用差分隐私来保护用户的位置隐私,会出现单个位置点的变动对位置数据集几何质心的影响较大、添加的噪音较大等问题,而地理不可区分性(Geo-I, Geo-Indistinguishability)[29]的出现,则解决了差分隐私在位置隐私保护中的局限性。在 Geo-I 概念提出之后,有许多基于位置混淆的隐私保护方法被提出[30-31]。文献[32]指出,现有的位置隐私保护机制在面对连续定位服务时,将难以较好地保护时空事件隐私,进而提出一个框架 PriSTE,将现有的位置隐私保护机制转化为一个保护时空事件隐私的框架。为了满足用户的个性化隐私保护需求,以支持为用户在不同位置时提供差异化隐私保护,文献[33]在合理保护用户隐私的同时,提出了一种基于差分隐私的个性化位置隐私保护方案。

基于密码学的位置隐私保护通常是利用密码算法来对用户的位置查询信息进行加密处理。在此过程中,基于传统公钥密码的数据共享一般要求数据共享者明确地知道共享数据的用户是谁,这就要求数据共享者要使用不同用户的公钥来对数据进行加密共享,这对动态性强、灵活度高的车联网来说,是难以实现的,而访问控制能保证数据只被拥有相应权限的用户使用,从而保证了数据共享者的隐私安全。

支持访问控制的隐私保护方案拓展了以往的"一对一"加、解密模式,变成了"一对多"模式。如基于属性的加密机制(ABE:由 Sahai 等[34]在 2005 年的欧密会上提出),密文与密钥都与用户的属性相关,数据共享者可以根据待共享的数据和接收者的属性信息,制定一个由属性构成的加密策略,由此而产生的密文只有属性满足加密策略的用户才能解密,进而实现了"一对多"的加、解密模式。随后,根据不同的策略和属性的匹配方式,提出了两种 ABE 方案:基于密钥策略的属性加密(KP-ABE)[35]和基于密文策略的属性加密(CP-ABE)[36]。文献[18]在多权限属性加密的基础上,提出一种新的基于位置的数据访问控制方案,实现了基于属性和位置的云存储访问控制。文献[37]提出基于车辆命名数据网络架构的访问控制方案,该方案利用代理重加密实现了访问控制、数据的保密性和非法车辆的吊销,利用匿名和基于身份的签名实现了匿名认证和数据的完整性。文献[38]提出一个支持车内应用细粒度访问车内数据的方案,从而避免了因车内应用过度获取车辆信息而造成的隐私泄露。

本文主要研究基于匿名和密码学上的车联网隐私保护方案,并提出一个可提供隐私安全和计算资源开销少的方案。

2 预备知识

2.1 访问控制

令 $\mathcal{AT}=\{A_1,\cdots,A_n\}$ 为一个属性集合,$A_i\in\mathcal{AT}$ 为属性。一个集合 $\mathbb{A}\subseteq 2^{\mathcal{AT}}$ 是单调的,当且仅当对 $\forall B,C\in 2^{\mathcal{AT}}$,若 $B\in\mathbb{A}$,$B\subseteq C$,则 $C\in\mathbb{A}$。若 $\mathbb{A}\subseteq 2^{\mathcal{AT}}\setminus\{\phi\}$ 且单调,则称 $\mathbb{A}$ 为一个访问结构。若集合 $D\in\mathbb{A}$,则称 D 为授权集,否则称为非授权集。

2.2 线性秘密共享

一个有 l 个参与方 $P_1,\cdots,P_l$ 的秘密共享方案 Π 在 $\mathbb{Z}_p$ 上是线性的,满足:

(1)每个参与方 P_k 关于秘密 s 的份额是 $\mathbb{Z}_p^n$ 中的一个 n 维向量;

(2)在 Π 中存在一个 $l\times n$ 维的共享生成矩阵 $\boldsymbol{M}$,令 ρ 表示一个从 $\{1,\cdots,l\}$ 到 $\{P_1,\cdots,P_n\}$ 的映射,即映射 ρ 将 $\boldsymbol{M}$ 中的每一行映射到一个参与方。选择一个向量 $v=(s,v_2,v_3,\cdots,v_n)^{\mathrm{T}}\in\mathbb{Z}_p^n$,则 $\mathbb{M}\cdot v$ 表示 Π 中秘密 s 的 l 个份额的向量,$s_k=\mathbb{M}_k\cdot v$ 表示参与方 $\rho(k)$ 的分享份额,其中 $v_2,\cdots,v_n\in_R\mathbb{Z}_p$,$\{\mathbb{M}_k\}$ 表示 $\mathbb{M}$ 的行向量。

若集合 $D\in\mathbb{A}$ 为授权集,令 $K=\{k\mid P_k\in D\}\subset\{1,\cdots,l\}$,则存在常数 $\{c_k\in\mathbb{Z}_p\}_{k\in K}$,使得 $\sum_{k\in K}c_k\mathbb{M}_k=(1,0,0,\cdots,0)$。

2.3 多关键字模糊搜索

文献[39]的隐私保护多关键字模糊搜索方案的形式化定义如下:$KeyGen(\lambda)$:输入安全参数 λ,输出私钥 $SK=(SK_1,SK_2,S)$ 和哈希密钥集 $\mathcal{H}K=\{k_t\}$;$Index\_Enc(SK,\mathcal{BL}_{\mathcal{E}})$:输入私钥 SK 和布隆过滤器 $\mathcal{BL}_{\mathcal{E}}$,输出索引 $Enc_{SK}(\mathcal{BL}_{\mathcal{E}})$;$Query\_Enc(SK,\mathcal{BL}_{\mathcal{P}})$:输入私钥 SK 和布隆过滤器 $\mathcal{BL}_{\mathcal{P}}$,输出陷门 $Enc_{SK}(\mathcal{BL}_{\mathcal{P}})$;$BuildIndex(\mathcal{E},SK,L)$:选择 L 个互不相关的位置敏感哈希函数 $\mathcal{H}=\{h_t\}$ 和一个伪随机函数 F;在 $\mathcal{E}$ 中提取关键字集 $W_{\mathcal{E}}$,并通过函数 $\{g_t\mid g_t=F_{k_t}\circ h_t\}$ 构造一个布隆过滤器 $\mathcal{BL}_{\mathcal{E}}$ 作为 $\mathcal{E}$ 的索引;$Trapdoor(\mathcal{P},SK)$:用同样的函数为 $\mathcal{P}$ 生成一个布隆过滤器 $\mathcal{BL}_{\mathcal{P}}$;$Search(Enc_{SK}(\mathcal{BL}_{\mathcal{E}}),Enc_{SK}(\mathcal{BL}_{\mathcal{P}}))$:输出搜索结果 $\langle Enc_{SK}(\mathcal{BL}_{\mathcal{E}}),Enc_{SK}(\mathcal{BL}_{\mathcal{P}})\rangle$。

3　方案模型

3.1　系统模型

本文方案的系统模型主要包含以下 5 个主体:可信中心(TA, Trust Authority)、路边单元(RSU, Road Side Unit)、请求用户(RU_i, Requesting User)、协同用户(CU_j, Collaborating User)和位置服务提供商(LSP, Location Service Provider)等。本文方案的系统模型如图 1 所示。

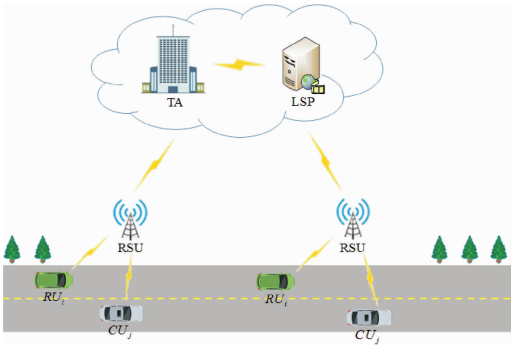

图 1　系统模型

Fig. 1　System model

(1)TA 是受信任的第三方,它初始化系统并生成系统公钥 PK、系统私钥 MSK、用户跟踪密钥 TK 和系统参数 $params$。方案中各个实体(包括 RU_i、CU_j 和 RSU)都必须向 TA 进行注册。当检测到不当行为,并且需要对其身份进行揭露时,TA 可根据其签名来揭露他的真实身份。

(2)RU_i 是一个具备智能设备的用户。它通过智能设备向 LSP 发起位置服务查询 SQ_i,然后根据 LSP 返回的结果,自行在本地检索相关的位置服务。

(3)CU_j 是一个具备智能设备的用户,主要指响应位置服务查询 SQ_i,并生成位置服务响应 $SR_{i,j}$ 的用户。

(4)RSU:一个半可信用户,在本文方案中担任着信息传播和服务代理的职责。具体而言,在信息传播职责中,充当方案主体间信息通信的媒介;在服务代理中,为请求用户 RU_i 和协同用户 CU_j 执行代理服务。使用 RSU 的理由主要源于其能提高方案性能:RSU 是一个具备一定计算和通信能力的智能设备,可在本地处理一定的数据,从而减轻云服务器和用户的计算负担。

(5)LSP:一个有足够大的存储空间的位置服务提供商,其职责主要为存储协同用户 CU_j 的位置服务响应 $SR_{i,j}$,并响应请求用户 RU_i 的位置服务查询 SQ_i。

本文方案所用的相关符号描述如表 1 所示。

表 1　符号描述

Table 1　Symbol description

符号	描述
λ,δ,p	安全参数、素数
$\mathbb{G}_1,\mathbb{G}_2,g$	循环群、生成元
$\boldsymbol{M}_1,\boldsymbol{M}_2$	可逆矩阵
$\mathcal{H}K$	哈希密钥集
F	伪随机函数
$\mathcal{H}$	位置敏感哈希函数
e	双线性映射
H_1,H_2	哈希函数
PK,MSK	系统公钥、私钥
$TK,params$	追踪密钥、系统参数
$RU_i,CU_j(1\leqslant i,j\leqslant m)$	请求用户、协同用户
ID_i^{ru},ID_j^{cu}	RU_i,CU_j 的身份
ID_i^{rsu},ID^{ta}	RSU,TA 的身份
$pk_1^{ru},sk_1^{ru},sk^{ru}$	RU_i 的公、私钥
$pk_1^{cu},sk_1^{cu},sk^{cu}$	CU_j 的公、私钥
sk_1^{rsu}	RSU 的私钥
T_i	时间戳
$RK_{ru\to cu},RK_{cu\to ru}$	重加密密钥
P_s,P_e	起点集、终点集
$S(P_{s_i},P_{e_j})$	(P_{s_i},P_{e_j})的位置服务
$\mathcal{P}=\{P_i\in\mathcal{P}\mid P_s\cup P_e=\mathcal{P},P_s\cap P_e=\varnothing\}$	匿名集
$\mathcal{E}=\{S(P_{s_i},P_{e_j})\mid 1\leqslant i,j\leqslant m\}$	边集
$G(\mathcal{P},\mathcal{E}),(\mathbb{M},\rho)$	完全二分图、访问结构
$SQ_i,SR_{i,j}$	位置服务查询、响应
SQS	服务查询信号
$\mathcal{A}_i^{ru},\mathcal{A}_j^{cu}$	RU_i,CU_j 的属性集
RE,RE'	重加密密文
(I'_{cu},I''_{cu})	关键字索引
(S'_{ru},S''_{ru})	位置服务搜索陷门
TH_i^{ru}	搜索结果阈值
RL	撤销列表

3.2　威胁模型

本文方案的安全威胁主要来自以下 6 个部分:

(1)大部分请求用户 RU_i 是诚实可信的,会发送真实可靠的位置服务查询,但存在小部分的请求用户 RU_i 会上传虚假的位置服务查询或短时间内重复多次发起查询,从而降低系统安全性和查询效率;

(2)大部分协同用户 CU_j 是诚实可信的,会根据自己的历史经验、背景知识等生成真实可靠的位置服务响应,但存在小部分的协同用户 CU_j 会生成虚假的服务响应,从而降低服务搜索结果的正确性和查询效率;

(3)RSU 会对其他参与者的数据感兴趣,并试图在代理服务中获取到密文对应的明文信息;

(4)RSU 可与满足访问控制需求的协同用户 CU_j 进行共谋。具体而言,RSU 可以通过请求用户 RU_i 发来的重加密密钥和满足访问控制需求的协同用户 CU_j 的密钥获取有关请求用户 RU_i 的密钥的相关信息;

(5)通过窃听公共信道的信息来发起伪造攻击等手段,以获取密文所对应的明文信息;

(6)在不考虑 LSP 的存储空间是否满足方案需求的前提下,它是一个可信的用户;不考虑因物理因素造成的安全威胁。

4 位置隐私保护方案

本文方案由以下 3 个部分构成:系统初始化、用户注册协议和服务查询协议,详细描述如下。

4.1 系统初始化

TA 生成系统公钥 PK、系统私钥 MSK、用户追踪密钥 TK 和系统参数 $params$。

(1)给定一个安全参数 λ,TA 生成阶为素数 $p(p\geqslant 2^{\lambda})$的循环群$\mathbb{G}_1$, $\mathbb{G}_2$, $g\in\mathbb{G}_1$为生成元;

(2)给定另一个安全参数 δ,TA 选取可逆矩阵 $\boldsymbol{M}_1$, $\boldsymbol{M}_2\in_R\mathbb{R}^{\delta\times\delta}$,向量 $V=\{(v_1,\cdots,v_\delta)^{\mathrm{T}}\mid v_i\in_R\{0,1\}\}$,哈希密钥集$\mathcal{HK}=\{k_t\mid k_t\leftarrow\{0,1\}^{\delta},1\leqslant t\leqslant L\}$,伪随机函数 $F:\{0,1\}^*\times\{0,1\}^{\delta}\rightarrow\{0,1\}^*$ 和 L 个互不相关的位置敏感哈希函数$\mathcal{H}=\{h\mid\{0,1\}^*\rightarrow\{0,1\}^{\delta}\}$;

(3)TA 选择双线性映射 $e:\mathbb{G}_1\times\mathbb{G}_2\rightarrow\mathbb{G}_2$和哈希函数 $H_1:\{0,1\}^*\rightarrow\mathbb{Z}_p^*$,$H_2:\mathbb{G}_2\rightarrow\mathbb{G}_1$;

(4)TA 选取数 $a,\xi_1,\xi_2\in_R\mathbb{Z}_p^*$,计算 $h_1=g^{\alpha}$,$h_2=e(g,g)^{\alpha}$,$h_3=g^{\xi_1}$和 $h_4=g^{\xi_2}$;

(5)TA 生成系统公钥 $PK=(h_1,h_2,h_3,h_4)$,系统私钥 $MSK=\{\alpha,M_1,M_2,V\}$,用户的追踪密钥 $TK=(\xi_1,\xi_2)$和系统参数 $params=(\mathbb{G}_1,\mathbb{G}_2,p,e,g,PK,H_1,H_2,\mathcal{H},F)$。

4.2 用户注册协议

请求用户 RU_i、协同用户 CU_j 和 RSU 分别向 TA 进行注册,生成用户公、私钥。

(1)RU_i 选取数 $sk_1^{ru}\in_R\mathbb{Z}_p^*$,计算 $pk_1^{ru}=g^{sk_1^{ru}}$,并将(sk_1^{ru},ID_i^{ru})通过安全信道发送给 TA;

(2)TA 接收到(sk_1^{ru},ID_i^{ru})后,计算 $sk_2^{ru}=g^{H_1(\alpha\parallel T_1)+sk_1^{ru}}$,并选取数 $r,r_1\in_R\mathbb{Z}_p^*$ 和 $u,h,w\in_R\mathbb{G}_1$,计算$sk_3^{ru}=g^{\alpha}(u^{H_1(ID_i^{ru})}h)^r$,$sk_4^{ru}=g^r$,$sk_5^{ru}=g^{\alpha}w^{r_1}$和 $sk_6^{ru}=g^{r_1}$;

(3)TA 给属性集$\mathcal{AT}$中的每一个属性 A_i 都分配一个数 $t\in_R\mathbb{Z}_p^*$,然后选取数 $v\in_R\mathbb{G}_1$,计算 $sk_{i,7}^{ru}=g^{t_i}$,$sk_{i,8}^{ru}=(u^{A_i}h)^{t_i}v^{-r_1}$;

(4)TA 将$(\delta,sk^{ru},M_1,M_2,V,\mathcal{HK})$通过安全信道发送给 RU_i,其中 $sk^{ru}=(sk_2^{ru},\cdots,sk_6^{ru},\{sk_{1,7}^{ru},sk_{1,8}^{ru}\},\cdots,\{sk_{n,7}^{ru},sk_{n,8}^{ru}\})$;同样地,通过安全信道将$(\delta,sk^{cu},M_1,M_2,V,\mathcal{HK})$发送给 CU_j;

(5)给定 RSU 的身份 ID_i^{rsu},TA 生成 RSU 的私钥 $sk_1^{rsu}=\alpha H_1(ID_i^{rsu})$,并将其通过安全信道发送给 RSU。

4.3 服务查询协议

本文方案的服务查询协议流程如图 2 所示:RU_i 通过 RSU 向 LSP 发起服务查询 SQ_i,LSP 对其进行合法性验证,若验证通过,则将服务查询 SQ_i' 发送给 RSU。而 RSU 则与 RU_i、CU_j 交互生成 CU_j 的重加密密文,CU_j 则据此生成相应的服务响应,并将其发送给 LSP。RU_i 向 LSP 发送一个搜索陷门,LSP 则据此返回相应的搜索结果给 RU_i。

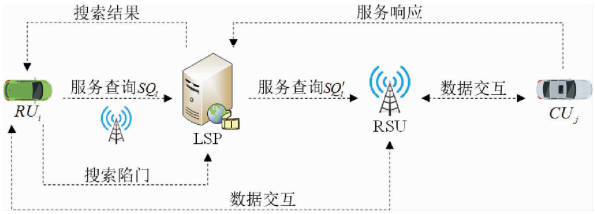

图 2 服务查询协议流程

Fig. 2 Service query protocol flow

本协议主要由以下 5 个部分组成:服务查询、查询验证、代理重加密、服务响应和服务检索,详细描述如下。

4.3.1 服务查询

请求用户 RU_i 生成位置服务查询 SQ_i,并将其通过 RSU 发送给 LSP。

(1)RU$_i$ 选取数 $r_2,r_3,r_4\in_R\mathbb{Z}_p^*$,计算 $E_1=g^{r_2}$,$E_2=g^{r_3}$,$E_3=g^{r_4}$和 $E_4=h_3^{r_2}h_4^{r_3}sk_2^{ru}$;

(2)RU_i 构造一个以匿名集$\mathcal{P}$为顶点集,所有起点为 $P_{s_i}\in P_s$、终点为 $P_{e_i}\in P_e$ 的位置服务所构成的路径为边集$\mathcal{E}$的完全二分图 $G=(\mathcal{P},\mathcal{E})$,在位置服务查询开始时,边集$\mathcal{E}$的势$|\mathcal{E}|=0$;

(3)RU_i 利用访问结构$(\mathbb{M},\rho)$对匿名集$\mathcal{P}$进行加密。具体而言,RU_i 选取数 $s,v_2,\cdots,v_n\in_R\mathbb{Z}_p$,并令其组成$\mathbb{Z}_p^n$中的一个 n 维向量$\vec{v}=(s,v_2,\cdots,v_n)^{\mathrm{T}}$;对于矩阵 $\boldsymbol{M}$ 中的每一个行向量 $\boldsymbol{M}_k$,计算$\lambda_k=\boldsymbol{M}_k\cdot\vec{v}$;

(4)RU_i 选取 l 个数 $\eta_1,\cdots,\eta_l\in_R\mathbb{Z}_p$和 $f\in_R\mathbb{G}_1$,计算

$$\begin{cases}CT_1=\mathcal{P}\cdot e(g,g)^{\alpha s},CT_2=g^s,\\ CT_3=f^s,CT_{k,1}=w^{\lambda_k}v^{\eta_k},\\ CT_{k,2}=(u^{\rho(k)}h)^{-\eta_k},CT_{k,3}=g^{\eta_k}。\end{cases}$$

并令 $CT_{\mathcal{P}}=(CT_1,CT_2,CT_3,\{CT_{k,1},\cdots,CT_{k,3}\}_{k=1}^{l})$;

(5)RU_i 计算 $L_1=H_1(\mathcal{P},E_1,\cdots,E_4,(\mathbb{M},\rho),CT_{\mathcal{P}})$,$L_2=r_4+sk_1^{ru}L_1$,并令 $\sigma_i^{ru}=\{E_1,\cdots,E_4,L_1,L_2\}$;

(6)RU_i 生成位置服务查询 $SQ_i=\{\sigma_i^{ru},CT_{\mathcal{P}},(\mathbb{M},\rho),TH_i^{ru}\}$。

4.3.2　查询验证

LSP 接收到位置服务查询 SQ_i 后,计算 $E'_3=g^{L_2}(pk_1^{ru})^{-L_1}$ 和 $L'_1=H_1(\mathcal{P},E_1,\cdots,E_4,(\mathbb{M},\rho),CT_{\mathcal{P}})$,并验证 $E'_3=E_3$ 和 $L'_1=L_1$ 是否成立。若不成立,则拒绝该查询;否则生成 $SQ'_i=\{CT_{\mathcal{P}},(\mathbb{M},\rho),TH_i^{ru}\}$,并将其发送给 RSU。

4.3.3　代理重加密

RSU 为协同用户 CU_j 生成重加密密文 RE,具体内容如下。

(1)RSU 接收到 SQ'_i 后,向周围的 CU_j 广播一个服务查询信号 SQS;

(2)CU_j 接收到 RSU 广播的服务查询信号 SQS 后,发送 $E_{ID_i^{cm}}(\mathcal{A}_j^{cm})$ 给 RSU 进行访问权限验证;

(3)RSU 计算 $D_{sk_1^{cm}}(E_{ID_i^{cm}}(\mathcal{A}_j^{cu}))=\mathcal{A}_j^{cu}$,若 CU_j 的属性集 $\mathcal{A}_j^{cu}\subseteq\mathcal{AT}$ 不满足访问结构$(\mathbb{M},\rho)$,则拒绝 CU_j 对 SQ'_i 的访问,否则定义 $K=\{k\mid\rho(k)\in A_j^{cu}\}\subset\{1,\cdots,l\}$,令常数 $\{c_k\in\mathbb{Z}_p\}_{k\in K}$,则有 $\sum_{k\in K}c_k\mathbb{M}_k=(1,0,\cdots,0)$ 和 $\sum_{k\in K}\lambda_k c_k=s$ 成立。同时,对于满足访问结构$(\mathbb{M},\rho)$的 CU_j,计算 $H_1(\mathcal{A}_j^{cu})$,并将其通过安全信道发送给 RU_i;

(4)RU_i 接收到 $H_1(\mathcal{A}_j^{cu})$ 后,选取数 $b_1,b_2\in_R\mathbb{Z}_p^*$,计算

$$RK_{ru\to cu}=\begin{pmatrix}RK_1=f^{b_1}sk_5^{ru},\\RK_2=sk_6^{ru},\\RK_3=H_2(e(g,g)^{\alpha b_2})g^{b_1}\\RK_4=(u^{H_1(\mathcal{A}_j^{cu})}h)^{b_2},\\RK_5=g^{b_2},\\\{RK_{j,1}=sk_{i,7}^{ru},RK_{i,2}=sk_{i,8}^{ru}\}_{i=1}^{|\mathcal{A}_j^{cu}|}\end{pmatrix}$$

并将 $RK_{ru\to cu}$ 通过安全信道发送给 RSU;

(5)RSU 接收到 $RK_{ru\to cu}$ 后,计算

$$B=\frac{e(CT_2,RK_1)}{\prod_{k\in K}(e(CT_{k,1},RK_2)\cdot e(CT_{k,2},RK_{\psi,1})\cdot e(CT_{k,3},RK_{\psi,2}))^{c_k}},$$

其中,ψ 是属性 $\rho(k)$ 在 $\mathcal{A}_j^{cu}$ 中的索引;

(6)RSU 生成重加密密文 $RE=(CT'_1,\cdots,CT'_5)$,并将其发送给 CU_j,其中 $CT'_1=CT_1/B$,$CT'_2=RK_3$,$CT'_3=RK_4$,$CT'_4=RK_5$ 和 $CT'_5=CT_3$。

4.3.4　服务响应

协同用户 CU_j 接收到重加密密文 RE 后,根据自己的历史经验、背景知识等生成相应的位置服务响应 $SR_{i,j}$ 和与之相关的关键字索引(I'_{cu},I''_{cu}),并将$\langle SR_{i,j},(I'_{cu},I''_{cu})\rangle$发送给 LSP 以待请求用户 RU_i 的位置服务查询。

(1)CU_j 计算

$$CT'_1\cdot e\left(\frac{CT'_2}{H_2(e(sk_3^{cu},CT'_4)/e(sk_4^{cu},CT'_3))},CT'_5\right)$$

以获得匿名集$\mathcal{P}$;

(2)CU_j 生成与匿名集 $\mathcal{P}$ 相关的位置服务 $S(P_{s_i},P_{e_i})$,并将所有位置服务构成的集合记为 $\mathcal{E}$,然后利用访问结构$(\mathbb{M}',\rho')$对$\mathcal{E}$进行加密,生成 $CT_{\mathcal{E}}=(CT''_1,CT''_2,CT''_3,\{CT''_{i,1},CT''_{i,2},CT''_{i,3}\}_{i=1}^{l})$;

(3)CU_j 生成位置服务响应 $SR_{i,j}=\{CT_{\mathcal{E}},(\mathbb{M}',\rho')\}$;

(4)CU_j 从$\mathcal{E}$中提取关键字集 $W_{\mathcal{E}}=\{w_1,w_2,\cdots\}$,并为其构造一个 δ 位的布隆过滤器$\mathcal{BL}_{\mathcal{E}}=\{(y_1,\cdots,y_\delta)^{\mathrm{T}}\mid y_\beta\in\{0,1\}\}$,开始时各个 y_β 为 0;

(5)CU_j 利用函数$\{g_t\mid g_t=F_{k_i}\circ h_t,1\leqslant t\leqslant L\}$将 $W_{\mathcal{E}}$ 中的点插入到$\mathcal{BL}_{\mathcal{E}}$,并对$\forall y_\beta\in\mathcal{BL}_{\mathcal{E}}$,若 $v_\beta\in V$ 为 1,则令 $y'_\beta=y''_\beta=y_\beta$,否则选取数 $\phi\in_R\mathbb{R}$,令 $y'_\beta=y_\beta/2+\phi$,$y''_\beta=y_\beta/2-\phi$。输出$\mathcal{BL}'_{\mathcal{E}}=\{(y'_1,\cdots,y'_\delta)^{\mathrm{T}}\mid y'_\beta\in\mathbb{R}\}$和$\mathcal{BL}''_{\mathcal{E}}=\{(y''_1,\cdots,y''_\delta)^{\mathrm{T}}\mid y''_\beta\in\mathbb{R}\}$;

(6)CU_j 计算$(I'_{cu},I''_{cu})\leftarrow(M_1^{\mathrm{T}}\cdot\mathcal{BL}'_{\mathcal{E}},M_2^{\mathrm{T}}\cdot\mathcal{BL}''_{\mathcal{E}})$,输出有关$\mathcal{E}$的关键字索引$(I'_{cu},I''_{cu})$。

4.3.5　服务检索

请求用户 RU_i 通过 RSU 向 LSP 发送一个位置服务搜索陷门(S'_{ru},S''_{ru}),并根据 LSP 返回的搜索结果进行服务检索。

(1)RU_i 从$\mathcal{P}$中提取关键字集 $W_{\mathcal{P}}=\{w'_1,w'_2,\cdots\}$,并为其构造一个 δ 位的布隆过滤器$\mathcal{BL}_{\mathcal{P}}=\{(x_1,\cdots,x_\delta)^{\mathrm{T}}\mid x_\phi\in\{0,1\}\}$,开始时各个 x_ϕ 为 0;

(2)RU_i 利用函数$\{g_t\}_{t=1}^{L}$将 $W_{\mathcal{P}}$ 中的点插入到$\mathcal{BL}_{\mathcal{P}}$,并对$\forall x_\phi\in\mathcal{BL}_{\mathcal{P}}$,若 $v_\phi\in V$ 为 0,则令 $x'_\phi=x''_\phi=x_\phi$,否则选取数 $\phi'\in_R\mathbb{R}$,令 $x'_\phi=x_\phi/2+\phi'$,$x''_\phi=x_\phi/2-\phi'$。输出$\mathcal{BL}'_{\mathcal{P}}=\{(x'_1,\cdots,x'_\delta)^{\mathrm{T}}\mid x'_\phi\in\mathbb{R}\}$和$\mathcal{BL}''_{\mathcal{P}}=\{(x''_1,\cdots,x''_\delta)^{\mathrm{T}}\mid x''_\phi\in\mathbb{R}\}$;

(3)RU_i 计算$(S'_{ru},S''_{ru})\leftarrow(M_1^{\mathrm{T}}\cdot\mathcal{BL}'_{\mathcal{P}},M_2^{\mathrm{T}}\cdot\mathcal{BL}''_{\mathcal{P}})$,输出有关$\mathcal{P}$的关键字索引$(S'_{ru},S''_{ru})$,并将其发送给 LSP;

(4)LSP 接收到(S'_{ru},S''_{ru})后,返回搜索结果$\langle sr,SR_{i,j}\rangle$至 RSU,其中 $sr=(I'_{cu})^{\mathrm{T}}\cdot S'_{ru}+(I''_{cu})^{\mathrm{T}}\cdot S''_{ru}$;

(5)RSU 接收到$\langle sr,SR_{i,j}\rangle$后,验证 $sr\geqslant TH_i^{ru}$ 是否成立。若不成立,则表明 RU_i 的位置服务查询失败,其中 TH_i^{ru} 值的高低表明 RU_i 可容忍搜索结果不精确的范围大小;

(6)RSU 验证 RU_i 的属性集 $\mathcal{A}_i^{ru} \subseteq \mathcal{AT}$ 是否满足访问结构 $(\mathbb{M}', \rho')$。若不满足,则拒绝 RU_i 对 $SR_{i,j}$ 的访问,否则执行4.3.3代理重加密中的过程,将 CU_j 生成的关于 $\mathcal{E}$ 的属性密文 $CT_{\mathcal{E}} \in SR_{i,j}$ 转化为适合 RU_i 解密的重加密密文 $RE' = (CT_1'', \cdots, CT_5'')$,并将其发送给 RU_i;

(7)RU_i 收到 RE' 后,计算

$$CT_1'' \cdot e\left(\frac{CT_2''}{H_2(e(sk_3^{ru}, CT_4'')/e(sk_4^{ru}, CT_3''))}, CT_5''\right),$$

以获得位置服务集 $\mathcal{E}$,并由此生成一个完全二分图 $G = (\mathcal{P}, \mathcal{E})$,然后在 G 中检索其所需位置服务。

5 安全性分析

5.1 抗隐私泄露

抗身份隐私泄露:用户身份除TA外,没有人可通过公开信道中的密文信息得到能确认用户身份的信息。在方案执行过程中,除用户注册部分外,需要用户将自己的身份标识通过安全信道发送给TA,其余部分均以匿名身份参与方案。

抗位置隐私泄露:用户的位置隐私仅自己能知道。由于CDH假设的安全性,即使恶意用户能窃取到相应的密文数据,也难以由此获得相应的位置信息。

5.2 抗抵赖性

若用户 $U_\gamma \in RU_i \cup CU_j$ 因存在某些恶意(如:发布虚假的位置服务查询、响应等)行为而被举报时,TA 通过计算

$$E_4/(E_1^{\xi_1}E_2^{\xi_2}) = h_3^{r_2}h_4^{r_3}sk_2^{u_\gamma}/(g^{r_2})^{\xi_1}(g^{r_3})^{\xi_2} = h_3^{r_2}h_4^{r_3}sk_2^{u_\gamma}/h_3^{r_2}h_4^{r_3} = sk_2^{u_\gamma}$$

以获得存在恶意行为的用户私钥 $sk_2^{u_\gamma}$。由于TA知道私钥 $sk_2^{u_\gamma}$ 与用户身份的对应关系,并以此来揭示存在恶意行为的用户身份,进而通过生成一个公开的撤销列表 $RL = \{sk_2^{u_\gamma} \mid \gamma \in [1, 2n]\}$,拒绝私钥 $sk_2^{u_\gamma}$ 的再次使用。

5.3 抗共谋攻击

本文方案可抵抗来自RSU和满足访问控制需求的协同用户 CU_j 的共谋攻击。

定理1 在计算 Diffie-Hellman(CDH)假设下,本文方案具有抗共谋性。

证明 给定一个安全参数 λ,随机数 $\eta \in \{0,1\}$,定义一个敌手 $\mathcal{A}$ 和挑战者 $\mathcal{C}$ 之间的游戏 $Game_{collusion}^{\mathcal{A} \leftrightarrow \mathcal{C}}(\lambda, \eta)$。若本文方案不抗共谋攻击,则敌手 $\mathcal{A}$ 能在游戏 $Game_{collusion}^{\mathcal{A} \leftrightarrow \mathcal{C}}(\lambda, \eta)$ 中获胜。

Setup $\mathcal{C}$ 运行系统初始化算法,输出系统公钥 PK、系统私钥 MSK、系统参数 $params$,并将 PK,$params$ 发送给 $\mathcal{A}$。

Queries 为响应 $\mathcal{A}$ 的询问,$\mathcal{C}$ 维持列表 L_1、L_2、L_3、L_4、L_5,其中 L_1、L_2 分别用于跟踪 $\mathcal{A}$ 的哈希询问 H_1、H_2,L_3、L_4 分别用于跟踪 $\mathcal{A}$ 关于 RU_i、CU_j 的密钥提取询问,L_5 用于跟踪 $\mathcal{A}$ 关于 RU_i 到 CU_j 的重加密密钥提取询问,开始时各列表 L_1、L_2、L_3、L_4、L_5 都为空。

H_1-Query 当 $\mathcal{C}$ 收到 $\mathcal{A}$ 对 RU_i 的 H_1-*Query* 后,验证 $ID_i^{ru} \overset{?}{\in} \{ID_i^{ru}\}_{i=1}^n$。若 $ID_i^{ru} \in \{ID_i^{ru}\}_{i=1}^n$,则计算 $H_1(ID_i^{ru})$,添加 $(ID_i^{ru}, H_1(ID_i^{ru}))$ 到 L_1 中,并将 $H_1(ID_i^{ru})$ 发送给 $\mathcal{A}$。反之,若 $ID_i^{ru} \notin \{ID_i^{ru}\}_{i=1}^n$,则选取数 $z_1 \in_R \mathbb{Z}_p^*$,其中 $z_1 \neq H_1(ID_i^{ru})$,添加 $(\perp, z_1, ID_i^{ru})$ 到 L_1 中,并将 z_1 发送给 $\mathcal{A}$。同样地,当 $\mathcal{C}$ 收到 $\mathcal{A}$ 对 CU_j 的 H_1-Query,执行上述过程进行响应。

H_2-Query 当 $\mathcal{C}$ 收到 $\mathcal{A}$ 的关于 RU_i 的 H_2-*Query* 后,验证 $ID_i^{ru} \overset{?}{\in} L_1$。若 $ID_i^{cu} \notin L_1$,则发送"$\perp$"给 $\mathcal{A}$。反之,若 $ID_i^{cu} \in L_1$,则选取数 $z_2 \in_R \mathbb{Z}_p^*$,计算 $H_2(e(g,g)^{\alpha z_2})$,并添加 $(\perp, z_2, H_2(e(g,g)^{\alpha z_2}), ID_i^{ru})$ 到 L_2 中,然后将 $H_2(e(g,g)^{\alpha z_2})$ 发送给 $\mathcal{A}$。同样地,当 $\mathcal{C}$ 收到 $\mathcal{A}$ 的关于 CU_j 的 H_2-Query,执行上述过程进行响应。

***RU_i* 的密钥提取询问** 当 $\mathcal{C}$ 收到 $\mathcal{A}$ 对 RU_i 的密钥提取询问后,验证 $ID_i^{ru} \overset{?}{\in} L_1$。若 $ID_i^{ru} \notin L_1$,则发送"$\perp$"给 $\mathcal{A}$。反之,若 $ID_i^{ru} \in L_1$,

(1)选取数 $z_3 \in_R \mathbb{Z}_p^*$,计算 $sk_5^{ru} = g^{\alpha} w^{z_3}$,$sk_6^{ru} = g^{z_3}$;

(2)对 RU_i 的属性集 $\{A_i\}_{i=1}^n$ 中的每一个 A_i 都分配一个随机数 $t_i \in_R \mathbb{Z}_p^*$,计算 $sk_{i,7}^{ru} = g^{t_i}$,$sk_{i,8}^{ru} = (u^{A_i}h)^{t_i} v^{-z_3}$;

(3)输出 $sk^{ru} = (sk_5^{ru}, sk_6^{ru}, \{sk_{i,7}^{ru}, sk_{i,8}^{ru}\}_{i=1}^n)$。

将 $(\perp, z_3, A, sk^{ru}, ID_i^{ru})$ 添加到 L_3 中,并发送 sk^{ru} 给 $\mathcal{A}$。

***CU_j* 的密钥提取询问** 当 $\mathcal{C}$ 收到 $\mathcal{A}$ 对 CU_j 的密钥提取询问后,验证 $ID_j^{cu} \overset{?}{\in} L_1$。若 $ID_j^{cu} \notin L_1$,则发送"$\perp$"给 $\mathcal{A}$。反之,若 $ID_j^{cu} \in L_1$,

(1)选取数 $z_4 \in_R \mathbb{Z}_p^*$,计算 $sk_3^{cu} = g^{\alpha}(u^{H_1(ID_j^{cu})}h)^{z_4}$,$sk_4^{cu} = g^{z_4}$;

(2)输出 $sk^{cu} = (sk_3^{cu}, sk_4^{cu})$。

将 $(\perp, z_4, sk^{cu}, ID_j^{cu})$ 添加到 L_4 中,并将 sk^{cu} 发送给 $\mathcal{A}$。

***RU_i* 到 *CU_j* 的重加密密钥提取询问** 当 $\mathcal{C}$ 收到 $\mathcal{A}$ 关于 RU_i 到 CU_j 的重加密密钥提取询问后,验证 $ID_i^{ru} \in L_3$ 和 $ID_j^{cu} \in L_4$ 是否都成立。若存在一个不成立,则发送"$\perp$"给 $\mathcal{A}$。否则选取数 $z_5, z_6 \in_R \mathbb{Z}_p^*$,计算

$$RK_{ru\to cu}=\begin{pmatrix} RK_1=sk_5^{ru}\cdot f^{z_5},\\ RK_2=sk_6^{ru},\\ RK_3=H_2(e(g,g)^{\alpha z_6})\cdot g^{z_5},\\ RK_4=(u^{H_1(ID_j^{cu})}h)^{z_6},\\ RK_5=g^{z_6},\\ \{RK_{i,1}=sk_{i,7}^{ru},RK_{i,2}=sk_{i,8}^{ru}\}_{i=1}^{n} \end{pmatrix},$$

并添加$(\perp,z_5,z_6,RK_{ru\to cu},ID_i^{ru},ID_j^{cu})$到 L_5 中,然后将 $RK_{ru\to cu}$发送给$\mathcal{A}$。

挑战阶段　$\mathcal{A}$发送两个挑战者身份 RU_i^*,CU_j^* 给 $\mathcal{C}$,然后$\mathcal{A}$在 L_5 中查询是否存在与 $ID_i^{ru^*},ID_j^{cu^*}$ 相关的元组。若不存在,则挑战失败,否则随机选取一个 $\eta\in\{0,1\}$,生成 RU_i^* 的密钥 $sk_\eta^{ru^*}$、CU_j^* 的密钥 $sk_\eta^{cu^*}$ 和 RU_i^* 到 CU_j^* 的重加密密钥 $RK_{ru^*\to cu^*}^{\eta}$,最后将$(sk_\eta^{cu^*},RK_{ru^*\to cu^*}^{\eta})$发送给 $\mathcal{A}$。

猜测阶段　$\mathcal{A}$生成一个对 RU_i^* 的密钥 $sk_\eta^{ru^*}$ 的猜测 $\eta'\in\{0,1\}$,若 $sk_{\eta'}^{ru^*}=sk_\eta^{ru^*}$,则$\mathcal{A}$在游戏 $Game_{collusion}^{\mathcal{A}\leftrightarrow\mathcal{C}}(\lambda,\eta)$中获胜,即 C 能解决 CDH 困难问题,这与 CDH 是困难问题相矛盾,故本文方案能抵抗共谋攻击。

6　性能分析

6.1　实验环境

本文实验均在运行 Ubuntu 20.04.3 LTS 64 位操作系统的电脑(Intel® Core™ i5-3470S CPU @ 2.90 GHz × 2,3.8 GiB 内存)上使用 Python 进行,相关实验配置:循环群$\mathcal{G}_1$和$\mathcal{G}_2$都为 1024-bit,安全参数 λ、δ 都为 160-bit,使用的算法库有 pypbc、cryptography 和 hashlib 等。

6.2　计算开销

图 3 ~ 图 8 分别表示本文方案与文献[10 - 11,14,18,40 - 42]在用户注册、签名、签名验证、属性加密、代理重加密和解密上的计算开销对比。

在用户注册阶段,本文方案与文献[40 - 41]中的用户都要对自己的属性集进行注册,生成相应的密钥,即密钥生成过程中所需的计算开销与其属性数量呈线性相关。与文献[40]相比,由于本文在此阶段未使用计算开销较大的双线性运算,故本文方案的计算开销要明显地小于文献[40],约降低了 79.59%,但与文献[41]相比,则提高了约 2.9 倍,这主要是因为本文方案在指数运算上的开销要大于文献[41]的方案,结果如图 3 所示。

在签名阶段,由于本文只涉及简单的指数和哈希运算等,故与文献[10 - 11,14,41]相比,本文方案有较少的计算开销,但与文献[40]相比,其计算开销则提高了约 3.4 倍,这是因为本文方案在签名时需要运行 5 次指数运算,而文献[40]仅需运行 1 次指数运算,结果如图 4 所示。

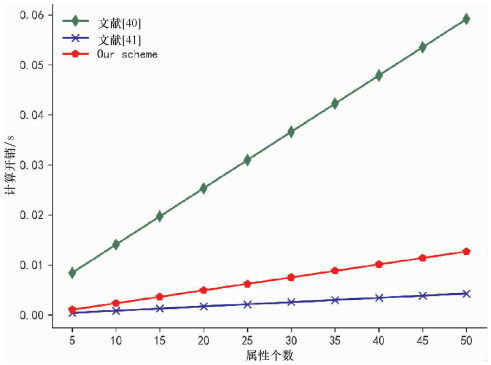

图 3　用户注册的计算开销

Fig. 3　Computational overhead of user registration

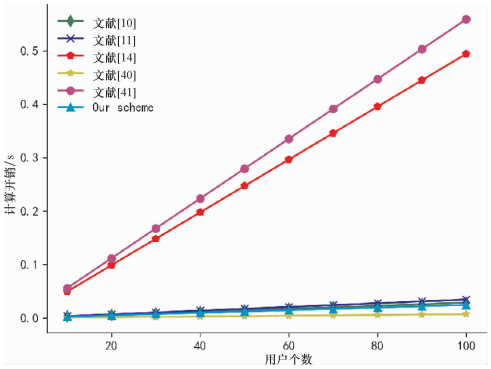

图 4　签名的计算开销

Fig. 4　Computational overhead of signatures

在签名验证阶段,由于本文方案仅涉及计算开销较少的指数和哈希运算,而未使用双线性运算,故在用户数量为[10,100]时,本文方案与文献[10 - 11,14,40 - 41]在签名验证上的平均计算开销分别约为 0.006 4 s、0.786 2 s、0.787 8 s、0.777 6 s、0.259 2 s 和 3.590 2 s,其计算成本最少降低了约 97.53%,最多降低了约 99.82%,结果如图 5 所示。

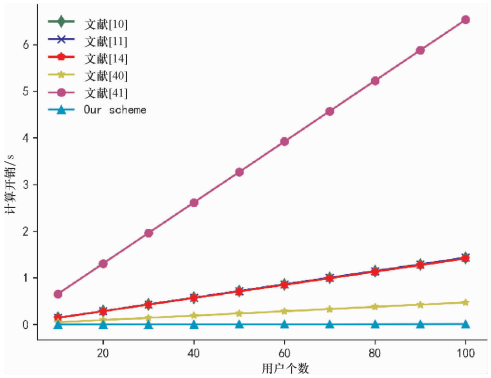

图 5　签名验证的计算开销

Fig. 5　Computational overhead of signature verification

在属性加密阶段,文献[40]中属性加密的密文生成与共享生成矩阵的维数有关(密文生成的计算开销与共享生成矩阵的维数呈线性相关),这使得其属性加密的计算开销要远远的大于本文方案和文献[41]。在属性数量为[5,50]时,本文方案与文献[40-41]在属性加密上的平均计算开销分别约为 0.010 7 s、0.167 3 s 和 0.009 6 s。与文献[40]相比,本文方案在属性加密上的计算开销降低了约 93.60%,而与文献[41]相比,则提高了约 1.1 倍,这是因为本文方案在指数运算上的开销要大于文献[41]的方案,结果如图 6 所示。

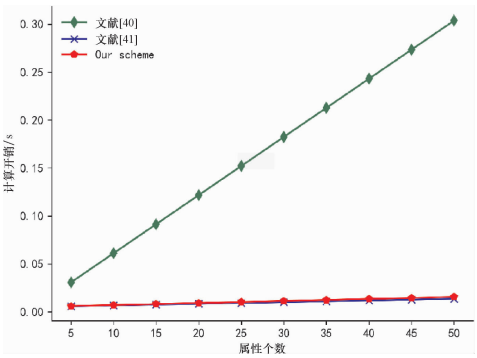

图 6 属性加密的计算开销

Fig. 6 Computational overhead of attribute encryption

在代理重加密阶段,为减少用户关于属性密文的解密开销,利用代理重加密技术,将属性加密密文转换为基于身份加密密文。在此过程中,不占用用户的计算开销,从而达到降低用户在密文解密上的计算开销的目标,但提高了其在代理重加密阶段的计算开销,结果如图 7 所示。在属性数量为[5,50]时,本文方案与文献[40-41]在代理重加密上的平均计算开销分别为 0.391 1 s、0.477 2 s 和 0.008 4 s。

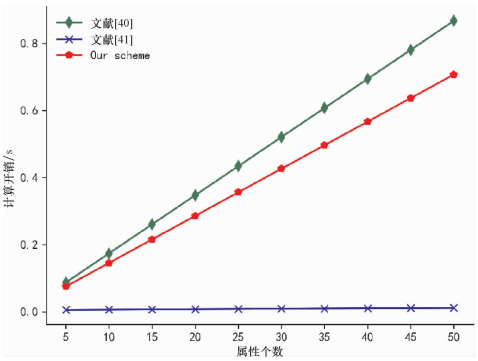

图 7 代理重加密的计算开销

Fig. 7 Computational overhead of proxy re-encryption

在解密阶段,由于经过代理重加密阶段的处理,使得处理后的密文转换为基于身份加密的密文,从而与用户的属性数量无关,故本方案在解密阶段的计算开销,均要优于文献[18,40-42],且不随属性数量的变化而变化,结果如图 8 所示。

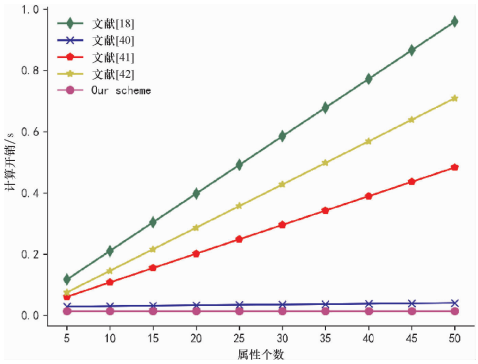

图 8 解密的计算开销

Fig. 8 Computational overhead of decryption

6.3 通信开销

本节主要对用户生成的服务查询所需要的通信开销进行分析。将本方案与文献[22]进行比较,其主要原因在于它们都是关注用户位置隐私的方案,都需要用户发起服务查询来进行基于位置的服务。对比结果如图 9 所示。

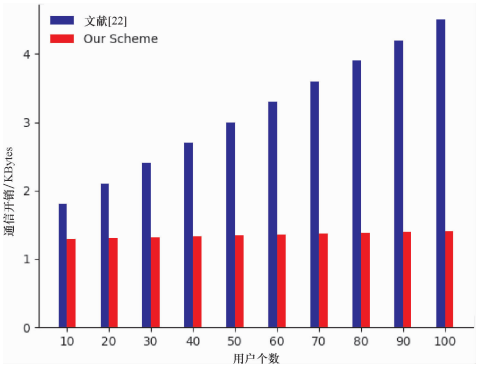

图 9 通信开销的对比

Fig. 9 Comparison of communication overhead

由图 9 可知,在用户数量为[10,100]时,本文方案在服务查询上的通信开销明显优于文献[22]。这是因为文献[22]的服务查询以用户的匿名集为主体,并直接对其进行传输,从而导致了较大的通信开销。而本文以属性密文的形式进行传输,虽然其通信开销在一定程度上受用户数量的影响,但与文献[22]相比,本文方案仍具有明显的优势。

7 总 结

本文提出了一个基于属性代理重加密的车联网隐私保护方案。该方案在 CP-ABE 的基础上,为用户提供

了隐私保护的细粒度方式与其余用户进行位置服务共享,弥补了“一对一”的位置服务共享方式难以在动态性强、可拓展性高的车联网中运用的不足;与此同时,本文以 RSU 作为一个半可信的代理用户,将基于属性加密的密文转换为基于身份加密的密文,降低了用户在密文解密上的计算开销,使得一些资源受限的用户也能在该方案中有较好的性能表现;最后,本文方案对于多关键字加密搜索上有一定的容错率,即在一定程度上支持关键字错误的多关键字模糊搜索。安全性和性能分析表明,本文所提方案具有较高的安全性和计算性能。

虽然本文为保护车联网中用户的位置隐私做出了一定的贡献,但存在以下不足:①与所提方案相比,本文方案在用户注册、签名、属性加密和代理重加密上仍需要较大的计算开销;②当有大批量数据存在时,如何实现精准且快速的实现服务检索,并在区块链中实现安全的数据存储;③随着移动通信技术的发展,如何提高本文方案在传输速度和传输延迟等方面的要求,从而更加地贴合实际应用。未来将针对以上不足,进一步优化方案。

参考文献:

[1] Chan T K, Cheng S. Review of autonomous intelligent vehicles for urban driving and parking[J]. Electronics, 2021, 10(9): 1-14.

[2] Liu Z, Weng J, Ma J, et al. TCEMD: A trust cascading-based emergency message dissemination model in VANETs[J]. IEEE Internet of Things Journal, 2020, 7(5): 4028-4048.

[3] Yoo H, Kim D. ROFF: RObust and fast forwarding in vehicular Ad-Hoc networks[J]. IEEE Transactions on Mobile Computing, 2015, 14(7):1490-1502.

[4] Ni J, Zhang K, Lin X, et al. IEEE International Conference on Communications (ICC), May 22-27, 2016[C]. Piscataway: IEEE, 2016.

[5] Baza M, Lasla N, Mahmoud M, et al. B-Ride: Ride sharing with privacy-preservation, trust and fair payment atop public blockchain[J]. IEEE Transactions on Network Science and Engineering, 2021, 8(2): 1214-1229.

[6] Nabil M, Sherif A, Mahmoud M, et al. Efficient and privacy-preserving ridesharing organization for transferable and non-transferable services[J]. IEEE Transactions on Dependable and Secure Computing, 2021, 18(3): 1291-1306.

[7] Zhao Q, Zuo C, Pellegrino G, et al. Network and Distributed System Security Symposium (NDSS), February 24-27, 2019[C]. San Diego:The Internet Society,2019.

[8] Yu H, Shu J, Jia X, et al. lpRide: Lightweight and privacy-preserving ride matching over road networks in online ride hailing systems[J]. IEEE Transactions on Vehicular Technology, 2019, 68(11):10418-10428.

[9] Yu H, Zhang H, Yu X, et al. PGRide: Privacy-preserving group ridesharing matching in online ride hailing services[J]. IEEE Internet of Things Journal, 2021, 8(7): 5722-5735.

[10] Zhu L, Meng L, Zhang Z, et al. ASAP: An anonymous smart-parking and payment scheme in vehicular networks[J]. IEEE Transactions on Dependable and Secure Computing, 2020, 17(4): 703-715.

[11] Zhang Y, Zhang L, Kang B, et al. 2021 IEEE Wireless Communications and Networking Conference (WCNC), March 29-April 1, 2021[C]. Piscataway: IEEE, 2021.

[12] Wang L, Lin X, Zima E, et al. Towards airbnb-like privacy-enhanced private parking spot sharing based on blockchain[J]. IEEE Transactions on Vehicular Technology, 2020, 69(3): 2411-2423.

[13] Baruah B, Dhal S. 2019 IEEE Region 10 Symposium (TENSYMP), June 7-9, 2019[C]. Kolkata, India: IEEE, 2019.

[14] Li M, Chen Y, Zheng S, et al. Privacy-preserving navigation supporting similar queries in vehicular networks[J]. IEEE Transactions on Dependable and Secure Computing, 2022, 19(2): 1133-1148.

[15] Wang L L, Liu G Z, Sun L J. A secure and privacy-preserving navigation scheme using spatial crowdsourcing in Fog-Based VANETs[J]. Sensors, 2017, 17(4):1-15.

[16] Jiang S, Zhu X, Wang L. An efficient anonymous batch authentication scheme based on HMAC for VANETs[J]. IEEE Transactions on Intelligent Transportation Systems, 2016, 17(8):2193-2204.

[17] Hoh B, Gruteser M. First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05), September 5-9, 2005[C]. Piscataway: IEEE, 2005.

[18] Jiang M, Wang H, Zhang W, et al. Location-based data access control scheme for internet of vehicles[J]. Computers & Electrical Engineering, 2020, 86(14): 1-9.

[19] Sweeney L. K-Anonymity: A model for protecting privacy[J]. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 2002, 10(5):557-570.

[20] Gruteser M, Grunwald D. Proceedings of the First International Conference on Mobile Systems, Applications, and Services (MobiSys 2003), May 5-8, 2003[C]. San Francisco: ACM, 2003.
[21] Kido H, Yanagisawa Y, Satoh T. ICPS '05. Proceedings. International Conference on Pervasive Services, July 11-14, 2005 [C]. Picataway: IEEE, 2005.
[22] Xu X, Chen H, Xie L. A location privacy preservation method based on dummy locations in internet of vehicles[J]. Applied Sciences, 2021, 11(10):1-15.
[23] Chow C Y, Mokbel M F, Liu X. GIS '06: Proceedings of the 14th Annual ACM International Symposium on Advances in Geographic Information Systems, November 10-11, 2006[C]. New York: ACM, 2006.
[24] Alamer A, Basudan S. An efficient truthfulness privacy-preserving tendering framework for vehicular fog computing[J]. Engineering Applications of Artificial Intelligence, 2020, 91(5):1-11.
[25] Ahsan Kazmi S, Dang T N, Yaqoob I, et al. A novel contract theory-based incentive mechanism for cooperative task-offloading in electrical vehicular networks[J]. IEEE Transactions on Intelligent Transportation Systems, 2022, 23(7):8380-8395.
[26] Zhang M, Zhou J, Cong P, et al. LIAS: A lightweight incentive authentication scheme for forensic services in IoV[J]. IEEE Transactions on Automation Science and Engineering, 2023,20(2):805-820.
[27] Yassine A, Hossain M S, Muhammad G, et al. Cloudlet-based intelligent auctioning agents for truthful autonomous electric vehicles energy crowdsourcing[J]. IEEE Transactions on Vehicular Technology, 2020, 69(5):5457-5466.
[28] Bugliesi M, Preneel B, Sassone V, et al. Automata, Languages and Programming. ICALP 2006. Lecture Notes in Computer Science, July 10-14, 2006[C]. Berlin: Springer, 2006.
[29] Andrés M E, Bordenabe N E, Chatzikokolakis K, et al. In Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security (CCS '13), November 4-8, 2013[C]. New York: ACM, 2013.
[30] Qiu C, Squicciarini A, Pang C, et al. Location privacy protection in vehicle-based spatial crowdsourcing via geo-indistinguishability[J]. IEEE Transactions on Mobile Computing, 2022, 21(7): 2436-2450.
[31] Niu B, Chen Y, Wang Z, et al. Eclipse: Preserving differential location privacy against long-term observation attacks[J]. IEEE Transactions on Mobile Computing, 2022, 21(1): 125-138.
[32] Cao Y, Xiao Y, Xiong L, et al. Protecting spatiotemporal event privacy in continuous location-based services[J]. IEEE Transactions on Knowledge and Data Engineering, 2021, 33(8): 3141-3154.
[33] Xu C, Luo L, Ding Y, et al. Personalized location privacy protection for location-based services in vehicular networks[J]. IEEE Wireless Communications Letters, 2020, 9(10): 1633-1637.
[34] Sahai A, Waters B. Annual International Conference on the Theory and Applications of Cryptographic Techniques, EUROCRYPT 2005: Advances in Cryptology-EUROCRYPT 2005, May 22-26, 2005[C]. Berlin: Springer, 2005.
[35] Goyal V, Pandey O, Sahai A, et al. Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS '06), October 30-November 3, 2006[C]. New York: ACM, 2006.
[36] Bethencourt J, Sahai A, Waters B. 2007 IEEE Symposium on Security and Privacy (SP'07), May 20-23, 2007[C]. Piscataway: IEEE, 2007.
[37] Jiang S, Liu J, Wang L, et al. ESAC: An efficient and secure access control scheme in vehicular named data networking [J]. IEEE Transactions on Vehicular Technology, 2020, 69(9): 10252-10263.
[38] Cui J, Chen X, Zhang J, et al. Toward achieving fine-grained access control of data in connected and autonomous vehicles [J]. IEEE Internet of Things Journal, 2021, 8(10): 7925-7937.
[39] Wang B, Yu S, Lou W, et al. IEEE INFOCOM 2014 - IEEE Conference on Computer Communications, April 27-May 2, 2014[C]. Piscatawy: IEEE, 2014.
[40] Cui J, Li B, Zhong H, et al. A practical and efficient bidirectional access-control scheme for cloud-edge data sharing[J]. IEEE Transactions on Parallel and Distributed Systems, 2022, 33(2): 476-488.
[41] Han J, Chen L, Susilo W, et al. Fine-grained information flow control using attributes[J]. Information Sciences, 2019, 484:167-182.
[42] Han Q, Zhang Y, Li H. Efficient and robust attribute-based encryption supporting access policy hiding in internet of things [J]. Future Generation Computer Systems, 2018, 83: 269-277.

【责任编辑: 周 全】