北京理工大學

本科生毕业设计（论文）外文翻译

外文原文题目：Enabling Strong Privacy Preservation and Accurate Task Allocation for Mobile Crowdsensing

中文翻译题目：移动群智感知实现强隐私保护和精确任务分配

基于区块链的出租车调度系统的完善

The perfection of the taxi dispatching system based on blockchain

学　　院：计算机学院

专　　业：计算机科学与技术

学生姓名：万琦玲

学　　号：1120180744

指导教师：陆慧梅

移动群智感知实现强隐私保护和精确任务分配

摘　要

移动群智感知是指一群人使用他们的移动设备，为有共同兴趣的客户合作收集有关社会事件和现象的数据。它可以降低传感器部署的成本，并通过人工智能提高数据质量。为了提高数据的可信性，服务提供商必须根据移动用户的个人特征，如移动模式、声誉等来招募移动用户，但这会导致移动用户的隐私泄露。因此，如何解决用户隐私和任务分配之间的矛盾，在移动群智感知中是一个挑战。在本文中，我们提出了 SPOON，一个强隐私保护的移动群体感知方案，支持基于移动用户的地理信息和信用点的精确任务分配。在 SPOON 中，服务提供商能够根据移动用户的位置来招募他们，并根据他们的可信程度来选择适当的传感报告，而不侵犯用户隐私。通过利用代理重新加密和 BBS+ 签名，保护传感任务，同时报告被匿名化以防隐私泄露。此外，还引入了一种保护隐私的信用管理机制，以实现分散的信任管理和移动用户的安全信用证明。最后，我们展示了 SPOON 的安全性，并证明了其在计算和通信方面的效率。

关键词：北移动群智感知、任务分配、信任管理、隐私保护

目 录

第 1 章 介绍

传感器与嵌入式计算设备的融合引发了移动群智感知的出现，即以用户为中心的移动设备，如智能手机、车载设备、可穿戴设备，用于感知、收集和处理社会事件和现象的数据。这种“感知即服务”通过为数据收集和共享打开一扇新的大门，详细阐述了我们对物理世界的认识。由于移动设备的日益普及，移动群智感知支持广泛的传感应用，从社会推荐，如餐厅推荐，停车位发现和室内平面图重建，到环境监测，如空气质量测量，噪声等级检测和大坝放水预警。借助人类智能和用户移动性，移动群智感知可以显著提高感知数据的可信度，扩大传感应用的规模，降低高质量数据收集的成本。

虽然移动群智感知让数据感知比以往任何时候都更有吸引力，但它也给移动用户带来了新的挑战，其中之一就是隐私泄露，移动群智感知让移动用户的隐私受到威胁。从周边地区收集的传感数据必然以人为中心，并与移动用户及其社交环境的某些方面有关：他们在哪里，他们要去哪里；他们经常去哪些地方，看到了什么；他们的健康状况如何，他们喜欢做什么活动。社交活动照片可能会暴露移动用户的社会关系、地点甚至政治派别。携带设备收集的空间数据可能会揭示移动用户的轨迹。例如，谷歌地图收集司机的“匿名”位置信息，用于实时生成交通地图，但仍会显示司机的驾驶路线和轨迹。此外，移动用户参与的感知任务越多，用户贡献的数据越丰富，他们的敏感信息暴露的可能性就越高。因此，保护移动用户的隐私是移动群智感知的首要安全问题。如果没有有效的隐私保护机制，就很难激励移动用户加入移动群智感知服务。此外，感知任务可能包含关于发出它们的客户的敏感信息，例如身份、位置、参考和购买意图。例如，如果 Bob 发布任务来收集附近的交通状况和噪音水平，房屋代理机构可能知道 Bob 希望在特定区域买房。为了保护客户或者移动用户的隐私，提出了几种利用匿名技术保护隐私的移动众感知方案。然而，匿名不足以保护隐私，因为移动用户可以通过旅行路线和社会关系进行追踪。根据美国一家全国性手机运营商提供的大量通话数据记录，有可能使用他们的前两个位置来唯一地识别 35% 的移动用户，使用他们的前三个位置来识别 85% 的移动用户。因此，在移动众感知中，探索强大的隐私保护机制，同时防止身份、位置和数据隐私泄露，对于客户和移动用户都具有重要意义。

一旦移动用户和客户的所有档案被完美保护，服务提供商就不可能准确地招募

移动用户来完成任务，而任务分配是移动群智感知中确保感知结果质量的关键组成部分。与传统传感网络不同，它产生的数据无法先验预测，其可信度完全取决于移动用户的智能和行为。一般来说，感知数据的质量越高，移动用户需要付出的努力和成本就越多。因此，移动用户的设置将直接影响感知数据的质量。从服务提供商的角度来看，如何根据感知任务的目标来识别正确的移动用户群以产生期望的数据是一个复杂的问题。基于地理位置和基于信誉的方法在移动众测中将任务分配给移动用户时很流行，但是这两种方法都有其固有的弱点。首先，基于信誉的任务分配机制需要一个可信的第三方 (TTP) 来执行繁重的信誉管理任务，它们容易受到信誉链接攻击，在这种攻击中，匿名移动用户可以根据他们的信誉被重新识别。其次，基于地理的任务分配方案可以基于它们的空间和时间相关性来优化用户选择，但是它们向服务提供商公开了感测任务的内容和移动用户的位置，而位置隐私是普适环境中移动用户主要关注的问题之一。总之，隐私保护和任务分配成为移动群智感知中一对矛盾对象。

为了解决这个问题，我们提出了一个强隐私保护移动群智感知方案（SPOON），支持基于位置的任务分配、分散的信任管理以及同时为移动用户和客户提供隐私保护。通过利用盲签名和随机矩阵乘法，我们充分防止移动用户和客户的个人资料（包括位置、身份和信用点）泄露隐私，而不会影响服务提供商的正常移动群智感知功能，如任务分配，数据过滤和信任管理。本文的主要贡献总结为三个方面：

- 我们设计了一种基于矩阵乘法的隐私保护位置匹配机制，允许服务提供商根据任务的感知区域和移动用户的地理位置分配感知任务。特殊的是，服务提供商可以分别基于从感测区域和用户位置生成的两个随机矩阵来确定移动用户是否在任务的感测区域。因此，服务提供商可以了解位置匹配的结果，但不了解客户感兴趣的区域和移动用户的位置。

- 通过扩展代理重加密和 BBS+ 签名，我们保护了有关移动用户和客户的敏感信息，包括他们的身份、信用点、感知任务和感知报告。具体而言，我们允许注册客户和移动用户匿名证明其参与众感知服务的能力和信任水平，并在不公开感知任务或感知报告内容的情况下安全地执行感知任务。此外，为了防止移动用户为了不公平的奖励而做出不当行为，可信的权威机构能够检测贪婪的移动用户并获得其身份。

- 我们引入了一种保护隐私的信用管理机制，在该机制中，移动用户能够证明自己的可信度，而无需暴露信用点和管理集中的服务器。特别是，它支持基于任务贡献的移动用户信用点的正面和负面更新。此外，多个服务提供商可以合作维护一个独特的信任评估系统，允许移动用户使用独特的信用点参与不同服务提供商提供的移动众感知服务。

本文的其余部分组织如下。第 2 节中我们回顾了相关工作，并在第 3 节中对系统模型、威胁模型和安全目标进行了形式化描述。在第 4 节中，我们提出了 SPOON，第 5 节中讨论了安全性。在第 6 节中，我们将讨论 SPOON 的一些扩展，并在第 7 节中评估性能。最后，我们在第 8 节中得出结论。

第 2 章 相关工作

为了实现保护隐私的移动群智测，最先进的解决方案旨在保护移动用户的位置、身份或感应数据。Christin 等人研究了移动用户的位置隐私，并提出了一种去中心化的协作机制，允许移动用户交换传感数据以保护他们的旅行路线。Wang 等人设计了一种位置聚合方法，将用户聚为一组，以实现 k-anonymity 。To 等人和 Ma 等人通过添加噪音来打破真实位置和混淆位置的相关性来保护移动用户的位置。为了保护身份隐私，提出了 AnonySense ，允许移动设备通过混合网络提供传感数据。Dimitriou 等人提出了客户隐私泄露的问题，并为移动传感设计了一个保护隐私的访问控制方案，用以保护客户的隐私。然后上述方案没有一个能够同时保护移动用户和客户的隐私。因此，Cristofaro 和 Soriente 提出了一个基于盲提取技术和基于身份的加密的隐私增强的参与式感应基础设施（PEPSI）。不幸的是，Günther 等人证明 PEPSI 容易受到移动用户和客户之间的串通攻击。为了解决这个问题，我们设计了一个新的基础设施，即基于身份的匿名加密技术。Qiu 等人提出了 SLICER，一个用于移动传感的 k-anonymity 隐私保护方案，实现了对移动用户的强隐私保护和高数据质量。然而，这些方案可能不足以保护现在的隐私，因为通过不同来源的信息组合，如旅行路线、社会关系或支付记录，有可能重新识别移动用户或顾客。为了保护传感数据，Zhou 等人扩展了一个通用的高效批处理密码系统，以支持云辅助移动众测中细粒度的多接收者多文件共享。Chen 等人引入了一个群体管理协议，以保证个人数据的差异化隐私。Rahaman 等人设计了一个基于双线图的群组签名方案，同时支持具有向后不可链接性和可开脱性的次线性撤销检查，用于匿名但可问责的众测。虽然可以保护身份、位置或数据隐私的隐私保护方案是现成的，但设计一个方案来实现强大的隐私保护是不容易的。

然而，在保护了移动用户和客户的隐私后，服务提供商很难找到合适的移动用户来完成任务。在移动众筹中已经提出了许多保护隐私的任务分配方案，可以分为三类，即基于位置的任务分配, 基于拍卖的激励和基于信誉的任务分配。Kazemi 和 Shahabi 专注于空间众包的空间任务分配，其中服务提供商根据移动用户的位置来分配任务。To 等人介绍了一个框架，以确定有效的地理广播区域，达到高任务分配率，同时保护移动用户的位置。Wang 等人提出了一种用于移动众包的个性化隐私保护的任务分配方案，该方案可以有效地分配任务，同时提供个性化的位置隐私保护。激励

机制也被提出来，以鼓励移动用户参与群智感知任务，其中，拍卖是普遍采用的激励机制之一。Gao 等人引入了一种基于反向拍卖的激励机制，考虑到传感数据的质量，选择具有近乎最小社会成本的中标价。Zhang 等人设计了一种基于拍卖的激励机制，为用户的参与和招揽提供奖励，并消除对不诚实的移动用户的恶意价格操纵。考虑到投标隐私，Lin 等人设计了两种基于差分隐私的保留隐私的拍卖激励机制。Jin 等人整合了用户激励、数据聚合和数据扰动机制，设计了一种激励性的保留隐私的数据聚合方案，以在移动众测中产生高准确度的聚合结果。此外，基于移动用户的信誉实现任务分配也很常见。Kazemi 等人定义了信誉分数，以代表移动用户能够正确执行任务的概率，以及说明任务可以接受的信心水平。Huang 等人证明了移动用户容易受到信誉的链接攻击，并提出了一种匿名化方案和信誉管理机制，以尽量减少这种攻击的风险。Wang 等人提出了 ARTSense 来实现移动传感中无身份暴露的信任管理。ARTSense 在没有 TTP 的情况下实现了移动用户声誉的正负更新，但它仍然需要每个服务提供商的信誉数据库来支持声誉管理。Ma 等人为边缘计算增强型移动众测设计了两种保护隐私的信誉管理方案。声誉用于识别愿意参与任务的恶意移动用户，但精确的信誉会直接透露给服务提供者和其他好奇的实体。

由于上述原因，在我们的初步工作中，我们提出了一个保护隐私的移动群智感知框架，使基于轨迹的任务分配和保护移动用户和客户的隐私。在本文中，我们扩展了这项工作，以支持移动众测中基于隐私保护的信誉任务分配。具体来说，提出的 SPOON（1）为移动用户提供了强大的隐私保护；（2）保护客户的身份、感应区域和任务；（3）允许服务提供商根据移动用户的位置和信用点来分配感应任务；以及（4）在没有集中服务器的情况下支持隐私保护的信用管理。我们在表 1 中显示了 SPOON 和现有工作的理想特征的比较。

Features	Identity Privacy		Data Privacy		Location Privacy		Credit Management		
	Users	Customers	Users	Customers	Users	Customers	Credit Privacy	No TTP	Greedy User Tracing
SPOON	√	√	√	√	√	√	√	√	√
[11], [12]	√	X	X	X	X	X	X	X	X
[13]	X	√	X	√	X	√	X	X	X
[14], [18], [29]	√	X	√	X	√	X	X	X	X
[35]	√	X	√	X	√	X	X	√	√
[20], [30]	X	X	X	X	√	X	X	X	X
[24], [25]	√	√	√	X	X	X	X	X	X
[26], [27], [36], [38]	X	X	√	X	X	X	X	X	X

图 2-1 SPOON 与现有工作的比较

第 3 章 问题陈述

在这一节中，我们正式定义系统模型和威胁模型，并确定我们的设计目标。

3.1 系统模型

移动群智感知服务为客户提供了一种以人为中心的方式来收集周围环境的数据。该架构由三个实体组成：服务提供商、客户和移动用户。

服务商：服务商自行开发云服务或租用云厂商提供的云资源。他们有足够的存储和计算资源来提供移动群智感知服务。服务提供商从客户那里接收传感任务，并根据他们的位置将它们分配给移动用户。他们还收集来自移动用户的传感报告，根据移动用户的信用点选择传感报告，并为客户生成传感结果。最后，服务提供商将信用积分分配给移动用户以进行激励。

客户：客户可以是个人、公司或组织。他们需要完成数据收集任务，例如研究城市的交通拥堵、小溪的污染程度和对公共交通的满意度，但他们没有足够的能力独自完成任务。因此，他们将他们的传感任务发布给服务提供商。

移动用户：每个移动用户都有多个移动设备，例如手机、平板电脑、车辆和智能眼镜。这些移动设备部署了丰富的计算、通信和存储资源，无论走到哪里、做什么，都由其所有者随身携带。移动用户确保他们的设备有足够的电力来支持正常的功能。他们参与传感任务并利用他们的便携式设备从周围区域收集数据，并将传感数据报告给服务提供商以获得信用积分。如图 1 所示，移动群智感知系统模型有以下步骤。

1. 每个移动用户或客户都需要在可信授权机构 (TA) 注册才能访问移动众测服务。
2. 客户创建传感任务以在传感区域收集数据，并将其连同身份验证消息和奖励政策一起发送给服务提供商。
3. 服务商提供移动群智感知服务，并将收到的感知任务发布给客户。
4. 愿意进行数据收集的注册移动用户使用能够定位的移动设备（例如，通过无线接入点或 GPS）获取他们当前或未来的位置，并将他们的位置连同身份验证消息一起发送给服务提供商.

5. 服务提供商在收到移动用户的消息后，会检查移动用户是否在感应区域内，或者他们将在不久的将来在感应区域内。

6. 服务提供商招募位置与感知区域匹配的移动用户，并将感知任务发送给匹配的移动用户。

7. 移动用户根据奖励政策和执行任务的成本接受或拒绝感知任务，接受任务的移动用户感知事件或现象，收集数据，并生成感知报告。

8. 移动用户将感知报告提交给服务提供商。

9. 服务提供商选择信任度高的移动用户生成的感知报告。

10. 服务提供商将选择的传感报告转发给客户。

11. 客户阅读传感报告，评估传感报告的质量和信任度，生成反馈。

12. 客户将反馈发送给服务提供商。

13. 服务提供商根据客户的反馈计算移动用户的奖励（即信用积分）。

14. 服务提供商将积分分配给对感知区域做出贡献的移动用户。

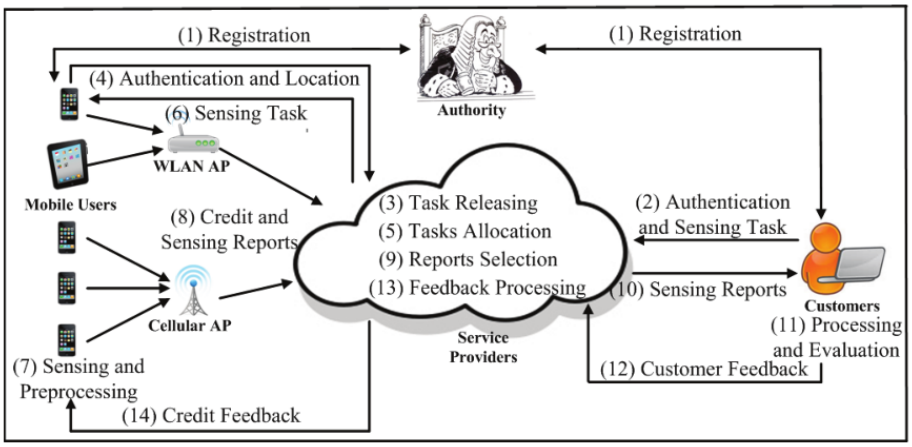


图 3-1 移动群智感知系统模型

3.2 威胁模型

服务提供商负责向客户提供移动群智感知服务，但它可能会为了增加收入而违反其隐私政策。例如，基于众包的拼车服务提供商优步（Uber）于 2017 年 1 月出于自己的目的，在未经客户许可的情况下公开了乘车预订数据。因此，服务提供者不是完全信任的，而是诚实但好奇的。一方面，服务提供商诚实地提供移动群智感知服务；另一方面，它可以学习特定移动用户的时空概率分布以及有关客户和移动用户的其他敏感信息，例如偏好、社会关系、政治派别和购买意愿。服务提供者不会与移动用户串通以损害其他移动用户的隐私，因为服务提供者和移动用户在移动群智感知中的目的不同，一旦串通公开，服务提供者的声誉将受到严重损害。

移动用户对客户和其他移动用户的隐私感兴趣。特别是，他们希望了解参与相同感知任务的其他移动用户，了解他们为之工作的客户的背景，以达到客户的期望。此外，移动用户可能是贪婪的，因此他们可能会匿名提交比允许的更多的传感报告来获得更多的信用点。此外，移动用户可能会恶意伪造、修改传感数据或传递模棱两可、有偏见的传感数据以欺骗客户。可以使用冗余或真相发现方法发现这些伪造或有偏见的数据。这些位置是从移动设备或接入点中的 GPS 可信芯片中提取的，我们假设移动用户无法修改他们的位置信息。

窃听者和黑客等外部攻击者也给移动群智感知服务带来了严重的安全威胁。攻击者有可能通过物理观察获得附近移动用户或客户的身份，这样匿名化可能不足以保证客户和移动用户的隐私保护。客户是可以完全信任的，因为他们是移动群智感知服务的主要受益者。

3.3 设计目标

为了在上述系统模型下实现强大的隐私保护移动众包感知并抵御安全威胁，SPOON 应实现以下设计目标：

- 强隐私保护：强隐私保护是指不会将移动用户的敏感信息暴露给公众，包括位置、身份、数据或信用积分。与传统的隐私保护侧重于对移动用户的位置或身份进行模糊处理相比，强大的隐私保护需要保护所有敏感信息，从位置和身份到移动群智感知中的传感数据和信用点。

1. 位置隐私保护：移动用户的位置和感知任务的感知区域不会暴露给他人。

移动用户只知道他们是否在感应区域内。

2. 数据保密性：除受委托的参与者外，任何实体都无法获得发布任务或传感报告的内容，使客户和移动用户的隐私不会泄露给他人。
3. 移动用户和客户的匿名性：客户、移动用户、服务提供商或他们的合谋无法将传感报告链接到移动用户或将传感任务链接到客户。攻击者甚至无法识别两个传感报告是由同一个移动用户生成的，还是两个传感任务是由同一个客户发出的。
4. 贪婪的用户跟踪：识别在报告周期内针对同一任务提交多个感知报告的贪婪移动用户的身份，以防止移动用户获得不公平的信用积分。
5. 隐私保护信用管理：信用积分用于记录移动用户的信任，并鼓励他们参与众感活动作为奖励。移动用户的精确信用点对好奇的实体隐藏，包括服务提供商和移动用户。

- 准确的任务分配：准确的任务分配是指招募的移动用户能够完成感知任务。这些能力包括移动用户在传感区域或将在不久的将来访问传感区域的事实，并且他们被信任以高质量地报告可用的传感数据。

1. 基于位置的任务分配：感知任务被分配给客户定义的感知区域内的移动用户，在给定区域之外的其他移动用户无法获知任务的任何信息。
2. 基于信任的报告选择：服务提供商根据移动用户的信用点选择感知报告，如果移动用户报告可信的感知数据，则将信用点奖励给移动用户。达到信用积分的平衡，意味着移动用户不可能伪造信用积分而不被发现，这样移动用户的信用积分总和应该等于奖励的信用积分加上初始积分。

第 4 章 SPOON

在这一部分中, 我们回顾了前期工作, 并提出了基于矩阵乘法、BBS+ 签名和代理重新加密的 SPOON, 它由五个阶段组成：服务设置、用户注册、Task 分配、数据报告和信用分配

4.1 前期工作

我们回顾了用于设计 SPOON 的预备知识, 包括双线性映射、BBS+ 签名和代理重新加密。

双线性映射设 (G_1, G_2, G_3) 是三个素数阶为 p 的循环群。$\hat{e} : G_1 \times G_2 \to G_t$ 为双线性配对, 具有以下性质:

- 双线性, 对于 $g \in G_1, h \in G_2, a, b \in Z_p, \hat{e}(g^a, h^b) = \hat{e}(g, h)^{ab}$
- 非退化性, 对于 $g \neq 1_{G_1}, h \neq 1_{G_2}\hat{e}, (g, h) \neq 1_{G_T}$
- 可计算性,$\hat{e}$ 是可以有效计算的
- （唯一标识）$G_1 \square G_2 \square G_T$ 中所有元素的二进制表示都是独一无二的。

如果 $G_1 \neq G_2$, 并且在任一方向上 G_1 和 G_2 之间不存在可有效计算的同态, 则 $\hat{e}$ 是 3 型双线性配对。如果 $G_1 = G_2$, 则 $\hat{e}$ 是 1 型双线性对。

BBS+ 签名。我们简要回顾了提出的具有 1 型双线性对的 BBS+ 签名, 它可用于对 ℓ-message 向量 $(m_1, ..., m_l)$ 进行签名

设 g, g_1, g_{+1} 是 G_1 的生成元。从 Zp 中随机选择 x 作为签名方案的秘密密钥, 计算对应的公钥为 y = gx。消息 (m_1, m) 上的签名是 (A,e,s), 其中 $A = (gg_1^{m_1}...g^m g_{+1}^s)^{\frac{1}{x+e}}$ 和 (e,s) 是从 Zp 中选择的随机值。

此签名可检查为：$\hat{e}(gg_1^{m_1}...g^m g_{+1}^s, g) == \hat{e}(A, yg^e)$

BBS+ 签名的安全性可简化为 q-SDH 假设, 并可用于构造一个零知识知识证明协议, 允许签名者证明消息签名对的拥有。

代理重加密。代理重加密是一种特殊的公钥加密, 具有一个理想的特性, 即半可信代理, 能够在给定代理重加密密钥的情况下, 将 Alice 的密文转换为 Bob 的密文, 而

不必看到底层的明文。由于这特性, 它已被广泛应用于数据共享场景中。代理重加密方案由 Ateniese 等人 [42] 提出,1 型双线性对的详细方案如下：

- KeyGen (•)。Alice 选择了一个随机值 $a \in Z_p$ 作为密钥 sk_a, 并计算公钥 $pk_a = g^a$。
- RKeyGen（sk_a, pk_b）。Alice 通过使用 Bob 的公钥将重新加密的密钥 $rk_{A\to B} = g^{b/a}$ 发送给一个代理来委托 Bob
- Encrypt（m,pk_a）。为了在 pk_a 下加密消息 $m \in G_T$, Alice 选择一个随机值 $k \in Z_p$ 计算 $c_a = (g^{ak}, m\hat{e}(g,g)^k)$。
- Re-Enc($c_a, rk_{A\to B}$）。代理可以通过 $rk_{A\to B}$ 将 Bob 的密文 c_a 转换为密文 c_b。从 c_a, 代理计算 $\hat{e}(g^{ak}, g^{b/a}) = \hat{e}(g,g)^{bk}$ 并得到 $c_b = (\hat{e}(g,g)^{bk}, m\hat{e}(g,g)^k)$。
- Decrypt(c_b, sK_b)。Bob 对 c_b 进行解密, 得到 $m = m\hat{e}(g,g)^k/(\hat{e}(g,g)^{bk})^{1/b}$。

4.2 SPOON 的主要思想

从直观上看, 服务提供商应该拥有移动用户的详细配置文件, 如位置、身份、信任程度等, 以提供准确的任务分配, 从而导致移动用户的隐私泄露。事实上, 服务提供商只需要知道移动用户是否有能力执行目标感知任务, 而不是拥有所有的配置文件。根据这一观测结果, 从随机矩阵乘法出发, 设计了保护隐私的位置匹配方案。具体来说, 每个移动用户的位置表示为一个矩阵 $\widetilde{L}_{m\times n}$, 该矩阵由一个矩阵 $\widetilde{M}_{m\times n}$ 随机化。任务的感知区域表示为另一个矩阵 $\widehat{L}_{m\times n}$, 并由矩阵 $\widehat{M}_{m\times n}$ 进行随机化。矩阵随机化保护了移动用户的位置和任务的感知区域, 但位置随机化后, 服务提供商很难识别出位置与任务感知区域匹配的移动用户。因此, 为了实现基于两个随机矩阵相乘的保持隐私的位置匹配, 我们构造了两个可逆随机矩阵 $\widetilde{M}_{m\times n}$ 和 $\widehat{M}_{m\times n}$。

此外, 客户对感知任务进行加密, 以防止好奇的服务提供商和不匹配的移动用户访问它们。然而, 当客户对传感任务进行加密时, 她并不知道哪些移动用户可以进行传感工作, 因此她不知道应该使用哪一个公钥。虽然代理重加密可以借助服务提供商等代理实现加密感知任务的共享, 但它会将感知任务公开给代理。为了保护感知任务, 我们将代理划分为两个实体, 即 TA 和服务提供商, 并为匹配的移动用户之间的感知任务共享设计了一个两级代理再加密方案。其中, 感知任务由 TA 和服务提供商的公钥加密, 移动用户在拥有 TA 的代理密钥和重新加密的服务提供商密文的条件下解

密感知任务。这样一来, 由于 TA 的密钥不足, 服务提供商无法获得任务, 而不匹配的移动用户无法解密任何密文, 因此什么也学不到。另外, 为了使 TA 离线,TA 的代理密钥可以在用户注册时委托给每个移动用户使用。

最后, 盲签名是一种广泛应用的移动用户身份保护方法。通过使用 BBS+ 盲签名, 移动用户生成 BBS+ 签名的零知识证明, 以使服务提供商相信自己是能够在不暴露真实身份的情况下参与众筹活动的注册用户, 根据公钥生成跟踪标签, 识别重复报告传感数据的贪心移动用户。但是, 如果移动用户是匿名的, 支持移动用户的信任管理是一个挑战。因此, 我们扩展了 BBS+ 盲签名, 将积分整合到用户的身份签名中, 实现了积分的添加操作。从而支持积分的正、负更新。具体来说, 如果移动用户提交的报告是可信的, 服务提供商将奖励用户的积分, 否则将惩罚用户的积分。服务提供商可以在奖励或惩罚积分上生成新的 BBS+ 签名, 用于信用定稿。当移动用户参与新的感知任务时, 可以向其他服务提供商证明 BBS+ 签名, 同时更新积分。现有的信任管理机制需要集中的服务器来管理积分, 与此不同的是, 每个移动用户都可以管理自己的积分, 并在必要时向服务提供商显示自己的信任级别。从而实现了唯一的信任管理, 多个服务提供商只要相互信任, 就可以共享唯一的信任管理系统。此外, 设计了积分的零知识范围证明, 以及 BBS+ 签名的零知识证明。基于范围证明, 移动用户可以让服务提供商相信, 她拥有高于所选阈值的积分。通过这样做, 服务提供商可以根据暴露的阈值从高积分的移动用户中选择感知报告, 但不知道移动用户的准确积分。

4.3 高层次的描述

我们首先提供 SPOON 的高级描述。表 2 列出了 SPOON 中常用的符号

服务设置:TA 通过定义公共参数 $(G, G_T, p, G, g_0, g_1, g_2, g_3, h, h_0, h_1, h_2, h_3, h_4, G, h, G, h, F)$ 为服务提供商引导整个移动众筹服务, 并生成其私钥对 $(, T, T_0)$。服务提供商还生成秘-公开密钥对 (β, S), 并定义一个矩阵 $L_{m\times n}$ 来表示其众感服务的地理区域。

用户注册:TA 对愿意参与移动众筹服务的移动用户和客户进行注册。它对注册人进行评估, 确定其初始信用点 P_0, 并与注册人交互生成匿名凭证 (A, e, s, B, f, t)。(A, e, s) 用于接入移动众筹服务,(B, f, t) 用于注册人的信用管理。为了实现匿名性,(A, e, s) 和 (B, f, t) 的所有权分别由注册人用零知识证明进行身份认证和信用评估。另外, 将 RK 分配给注册人对分配的传感任务进行解密。

$U_{i\{i\in R\}}$	Set of registered mobile users
$U_{i\{i\in \mathcal{L}\}}$	Set of mobile users in sensing area L
ST	A task issued by a customer
$task$	The detailed content of a task ST
$expires$	The expiration time of a task ST
$area$	The sensing region of a task ST
$L_{m\times n}$	A matrix to represent the service area of the service provider
$\widehat{L}_{m\times n}$	A matrix to represent the sensing area of a task ST
$\widetilde{L}_{m\times n}$	A matrix to represent the current and future locations of a user
$\widehat{M}_{m\times n}$	A random invertible matrix
$\widetilde{M}_{m\times n}$	A random invertible matrix
I	The unique identity of a registrant (mobile user or customer)
P_0	The initial credit point of a mobile user
ϵ	The trust level of a sensing report
γ	The maximum of trust level in a task ST
Q	The credit threshold chosen by a mobile user
A, e, s	The anonymous credential of a mobile user or customer
B, f, t	The anonymous credential of a mobile user with credit point P

图 4-1 常用标识符解释

任务分配: 客户生成一个感知任务 ST, 发送消息 $(c_1, c_2, c_3, expires, \widehat{N}_{n\times n}, , w, PK_2)$ 给服务提供商, 其中包括加密任务 (c_1, c_2, c_3)、过期时间过期、随机感知区 $\widehat{N}_{n\times n}$、身份证明 PK_2 等信息。后者发布 (num,$expires$, γ) 以吸引移动用户参与, 其中 num 是 ST 的标识符。移动用户 $U_{i\{i\in R\}}$ 将其位置 $\widetilde{N}_{n\times n}$ 和身份证明 PK_3 发送给服务提供商。然后, 服务提供商根据两个矩阵 ($\widehat{N}_{n\times n}$, $\widetilde{N}_{n\times n}$) 在 ST 的感知区域内找到移动用户 $U_{i\{i\in L\}}$ 的集合。由于 ($\widehat{N}_{n\times n}$, $\widetilde{N}_{n\times n}$) 是随机矩阵, 服务提供者可以通过矩阵乘法知道 U_i 是否在 ST 的感知区域, 而不知道 ST 的感知区域和 U_i 的位置。服务提供者使用 β 对 $U_{i\{i\in L\}}$ 可解密的密文 (c_1, c_2, c_3) 重新加密。最后, 服务提供商将 $(num, c_2, c_3, c_4, expires, , w)$ 发送给 $U_{i\{i\in L\}}$。

数据报告:$U_{i\{i\in L\}}$ 加密 m_i 收集数据来生成 (Di, D_i'), 并发送检测报告 (num,D_i ,D_i',C_i',X_i,$Y_i, Z_i, Q_{i,j}, SPK$) 服务提供者,C_i' 是对身份 I_i 和信用点 P_i 的承诺, 是该报告的标识符,Y_i 是 U_i 的标识符,Z_i 是标识重复报告用户的标签, Q_i 是要求的信用阈值, 以表明 U_i 具有的信用点数大于 Q_i,$_j$ 是用于报告的当前时隙, 并且 SPK 用于证明其信用点数 P_i 的所有权。服务提供商根据要求的阈值选择报告, 并将选择的报告转发给客户。对于使用双重报告标签 Z_i 向服务提供商双重报告感测报告的匿名身份用户,A 可以恢复他的身份。

信用分配: 客户评估每个报告的可信度, 并将相应的信任级别 $_i \in [-,]$ 返回给服

务提供商。后者计算授予 U_i,$_i$ 的信用点数, 并将 $(B_i, t''_i, f_i, _i, Y_i)$ 转发给 U_i, 其中 (B_i, t''_i, f_i) 是授予信用点数 $_i$ 的票证,Y_i 用于标识移动用户 U_i。一旦接收到 $(B_i, t''_i, f_i, _i, Y_i)$, U_i 更新其信用点 $P'_i = P_i + _i$, 并生成新 P'_i 的信用凭证 (B_i, f_i, t_i)。

4.4 SPOON 的细节

接下来我们将展示详细的 SPOON, 如下所示。

4.4.1 服务设置

设 (G_1, G_2, G_T) 是三个素数阶为 p 的循环群, 其中 p 是 λ 比特,e 是 3 型双线性映射。权威机构挑选随机生成器 G,$g_0, g_1, g_2, g_3 \in G_1$,$H, h_0, h_1, h_2, h_3, h_4 \in G_2$, 并分别计算 $G = \hat{e}(g, h)$ 和 $H = \hat{e}(g, h_0)$。TA 还选择了一个随机值 $G \in G_T$, 并定义了一个密码哈希函数 $H : \{0,1\}^* \rightarrow Z_p$ 和一个伪随机函数 $F : Z_p \times \{0,1\}^* \rightarrow Z_p$。公共参数 param 为 ($g_1$,$g_2$,$G_T$,p,G,$g_0$,$G_1$,$G_2$,$g_3$,H,$h_0, h_1, h_2, h_3$,$h_4$,G,H,G,H,F)。TA 随机选择 $\in Z_p$ 作为其密钥, 并计算公开密钥 $T = g \square T_0 = h$。

为了设置移动众测服务, 服务提供商随机选择其密钥 $\in Z_p$ 并计算 $S = g$ 作为其公钥。它还采用矩阵 $L_{m \times n}$ 来表示众测服务可以根据经度和纬度覆盖的地理区域。矩阵中的每个条目表示传感区域中的一个小网格, 如图 3 所示。假设安大略省的经度是从 74.40°W 到 95.15°W, 纬度是从 41.66°N 到 57.00°N, 我们可以使用 208 × 154 矩阵或更精确的 2075 × 1534 矩阵来表示安大略地区。

4.4.2 用户注册

客户或移动用户都需要在 TA 注册以获得匿名凭证, 用于参与众感服务。每个注册人在系统中都被分配了一个唯一的身份 I, 实际上可以是电话号码或邮寄地址。注册者选取三个随机值 $s', a, t' \in Z_p$ 计算 $C = g_1^{s'} g_2^a, C' = h_1^{t'} h_2^a, \widehat{A} = h_0^a$, 并将 $(I, C, C', \widehat{A})$ 发送给 TA , 以及以下零知识证明：

$$PK_1\{(s', t', a) : C = g_1^{s'} g_2^a \square C' = h_1^{t'} h_2^a \square \widehat{A} = h_0^a\}.$$

TA 首先检查证明 PK_1 以确保正确生成 $(C, C', \widehat{A})$。然后, 它根据其信用记录评估注册人的初始信用点, 假设为 P_0。之后,TA 随机选取 s″, e, t″, $f \in Z_p$ 计算 $A = (g_0 C g_1^{s''} g_3^I)^{\frac{1}{+e}}$, $B = (h_0 C' h_1^{t''} h_3^I h_4^{P_0})^{\frac{1}{+f}}$, $RK = \widehat{A}^1$, 通过安全通道返回 (A, B, s″, t″, e, f, P_0, RK) 给注册者。最后,TA 将元组 $(I, P_0, \widehat{A})$ 存储在其数据库中。

注册人计算 s = s′ + s″, t = t′ + t″ 并检查

$$\hat{e}(A, T_0 h^e) == \hat{e}(g_0 g_1^s g_2^a g_3^I, h) \tag{4-1}$$

$$\hat{e}(T g^f, B) == \hat{e}(g, h_0 h_1^t h_2^a h_3^I h_4^{P_0}) \tag{4-2}$$

注册者将（A、e、s、B、f、t、a、I、P_0、$\hat{A}$、RK）秘密存储在移动设备的只读存储器中。

4.4.3 任务分配

注册信息（$A\square e\square s\square B\square f\square t\square a\square I$、$P_0$、$\hat{A}$、$RK$）的客户有一个传感任务要分配给移动用户, 并逐个时隙请求传感数据, 其中每个时隙根据传感任务的具体要求, 范围从几分钟到几天不等。任务的语句定义为 ST = ($task$, $expires$, $area$, ,w), 表示内容（感知什么）, 过期时间（何时感知）, 感知区域（感知哪里）, 分别为最大信任级别和所需报告的数量。其他属性（例如, 感知间隔、接受条件、收益、报告期）可以在任务中说明。为保护任务内容, 客户随机选取 $k, r_1, r_2, r_3 \in Z_p$ 计算 $u = g^k$,$c_1 = S^{r1}$,$c_2 = T^{r2}$,$c_3 = (task||u)G^{r_1}H^{r_2}$。然后, 客户生成一个矩阵 $\widehat{L}_{m\times n}$ 来表示目标感应区域的面积。如图 2 所示, 对于传感区域中的每个位置, 将 $\widehat{L}_{m\times n}$ 中的相应条目设置为从 Z□p 中选择的随机值, 并将外部位置的值设置为零。为了掩蔽 $\widehat{L}_{m\times n}$ 中的感应区域, 客户从 $Z_p^{\square}$ 中选择 m × n 个随机数来生成可逆矩阵 $\widehat{M}_{m\times n}$ 并计算 $\widehat{N}_{n\times n}$ =$\widehat{L}^T_{m\times n}$ • $\widehat{M}_{m\times n}$, 其中 $\widehat{L}^T_{m\times n}$ 是矩阵 $\widehat{L}_{m\times n}$ 的转置。请注意,$\widehat{L}_{m\times n}$ 中的所有非零条目都应该是不同的, 除非攻击者仍然可以从 $\widehat{N}_{n\times n}$ 中学习感知区域。最后, 客户将 k 保密, 并将 (c_1,c_2, c_3,$expires$,$\widehat{N}_{n\times n}$, ,w) 连同以下零知识证明一起发送给服务提供商：

$$PK_2\{(A, e, s, a, I) : \hat{e}(A, T_0 h^e) == \hat{e}(g_0 g_1^s g_2^a g_3^I, h)\}. \tag{4-3}$$

服务提供商检查证明 PK_2 的有效性。如果是, 它分配一个任务标识符 num, 释放 ($num, expires,$) 并在其数据库中存储 (c_1,c_2, c_3,$expires$,$\widehat{N}_{n\times n}$, ,w) 。

当具有 (A_i, e_i, s_i, B_i,f_i,t_i,a_i, I_i,P_i,$\widehat{A}_i$,RKi) 的移动用户 $U_i i \in R$ 愿意参与众感活动时, 它首先选择一个随机值 $\in Z_p$ 来计算 $= h$。然后,U_i 根据其当前位置和将要访问的地方生成一个矩阵 $\widetilde{L}_{m\times n}$。对于 U_i 将到达的每个位置, $\widetilde{L}_{m\times n}$ 中的相应条目设置为

从 $Z_p^{\square}$ 中选择的随机值, 其余条目设置为零。$\widetilde{L}_{m\times n}$ 的非零条目应该不同。为了保护这些位置信息, 它还通过从 $Z_p^{\square}$ 中选取 m × n 个随机值生成一个随机可逆矩阵 $\widetilde{M}_{m\times n}$, 并计算 $\widetilde{N}_{n\times n}$= $\widetilde{M}_{m\times n}^{T}$ • $\widetilde{L}_{m\times n}$。最后,$U_i$ 将 ν 秘密保存, 并将 (μ, $\widetilde{N}_{n\times n}$) 连同以下零知识证明一起发送给服务提供者：

$$PK_3\{(A_i, e_i, s_i, a_i, I_i) : \hat{e}(A_i, T_0 h^{e_i}) == \hat{e}(g_0 g_1^{s_i} g_2^{a_i} g_3^{I_i}, h)\}. \tag{4-4}$$

如果 PK_3 无效, 服务提供者返回失败。否则, 对于每个未过期的任务, 它使用 $\widehat{N}_{n\times n}$ 计算 $N_{n\times n}$ = $\widetilde{N}_{n\times n}$ • $\widehat{N}_{n\times n}$ 并检查 $N_{n\times n}$ 是否为零矩阵。如果 $N_{n\times n}$ 是非零矩阵, 这意味着 U_i 可以匹配 ST , 则服务提供者计算 $c_4 = \hat{e}(c_1,)^{\frac{1}{}}$ 并释放 (num, c_2,c_3,c_4,$expires$,, w) 。如果没有匹配 U_i 的任务, 则服务提供者响应失败。

当 U_i 得到 (num,c_2,c_3,c_4, $expires$,, w) 时, 用 (, a_i) 作为 $task||u$=$c_3 c_4^{-\frac{1}{}} \hat{e}(c_2, RK_i)^{\frac{-1}{a_i}}$ 解密 (c_2,c_3, c_4)。然后,U_i 对任务进行评估, 根据收益和成本决定参与或放弃该任务。如果任务 ST 被接受,U_i 开始根据任务中的细节进行感知工作。$task||u$ 的正确性阐述如下：

$$\begin{aligned} c_3 c_4^{\frac{-1}{}} \hat{e}(c_2, RK_i)^{\frac{-1}{a_i}} &= c_3 \hat{e}(c_1,)^{-\frac{1}{}} \hat{e}(c_2, RK_i)^{\frac{-1}{a_i}} \\ &= (task||u) GRr_1 H^{r_2} \hat{e}(S^{r_1}, h)^{-\frac{1}{}} \hat{e}(T^{r2}, h_0^{\frac{a_i}{}})^{-\frac{1}{a_i}} \\ &= (task||u) G^{r_1} H^{r_2} G^{-r_1} H^{-r_2} \\ &= task||u. \end{aligned} \tag{4-5}$$

4.4.4 报告数据

U_i 对数据 $m_i \in G_T$ 进行采集和预处理, 并定期向客户提交感知报告, 包括采集时间、感知位置和详细内容。报告期由客户定义, 我们假设当前时段为 $_j$。为了阻止来自 m_i 的攻击,U_i 使用 u 将 m_i 加密为 $D_i = u^{r_i}, D_i'$= $m_i G^{ri}$, 其中 r_i 是从 Z_p 中随机选择的值。然后,U_i 随机选取 $t'_i \in Z_p$ 计算 C'_i =$h_1^{t'_i} h_2^{a_i} h_3^{I_i} h_4^{P_i}$ 。接下来,U_i 计算 X_i = $H(num||m_i||_j)$,$v_i = F_{a_i}(num||I||_j)$,$Y_i = H^{v_i}$ 和 $Z_i = \hat{e}(g, \widehat{A}_i) G^{X_i v_i}$。最后,$U_i$ 选择一个信用阈值 Q_i 并将报告（num,D_i,D'_i,C'_i,X_i,Y_i,Z_i,Q_i,$_j$）连同以下零知识证明一起发送给服务提供商：

$$SPK\begin{cases}(B_i, f_i, t_i, t'_i, a_i, I_i, P_i, v_i):\\ \hat{e}(Tg^{f_i}, B_i) == \hat{e}(g, h_0 h_1^{t_i} h_2^{a_i} h_3^{I_i} hP_{i4})\square\\ C'_i = h_1^{t'_i} h_2^{a_i} h_3^{I_i} h_4^{P_i}\square\\ P_i > Q_i\square\\ Y_i = H^{v_i}\square\\ Z_i = \hat{e}(g, \widehat{A}) G^{X_i v_i}\end{cases} = (num) \tag{4-6}$$

如果 SPK 无效,服务提供者返回失败；否则,服务提供者检查是否有另一个报告（num,$\widetilde{D}_i$,$\widetilde{D'}_i$,$\widetilde{C}_i$,$\widetilde{X}_i$,Y_i,$\widetilde{Z}_i$,$\widetilde{Q}_i$）与新收到的报告（num,D_i,D'_i,C'_i, X_i, Y_i,Z_i,Q_i). 如果是,则服务提供商计算并发送 $W = (\frac{\widetilde{Z}_i^{X_i}}{Z_i^{X_i}})^{\frac{1}{X_i - \widetilde{X}_i}}$ 给 TA,TA 可以利用数据库中的 $\widehat{A}_i$ 检查 W = $\hat{e}$(g, $\widehat{A}_i$) 找到移动用户的身份 I_i。这样, 贪婪的移动用户的身份被 TA 恢复, 如果它在一个报告时隙中提交了两个不同的感知报告。然后, 根据移动用户声称的阈值, 服务提供商选择具有前 w 个阈值的 w 个报告, 并将它们发布给客户。请注意, 未选择报告的移动用户可以在下一个报告时隙 $_j + 1$ 增加他们的阈值。

当客户检索报告时, 它可以使用存储的 k 作为 $m_i = D'_i \hat{e}(D_i, h)^{\frac{1}{k}}$ 逐一解密它们。

4.4.5 信用分配

客户获得感知结果后, 对每份报告的可信度进行评估, 并将相应的信任等级响应给服务商。m_i 的信任级别定义为 $_i \in [-,]$。如果 $_i$ 为正, 则 m_i 是可信的, 否则,m_i 是不可思议的。

服务提供者收到信任等级后, 随机选取 t''_i ,$f_i \in Z_p$ 计算 $_i = INT(_iQ_i)$, $B_i = (h_0 h_1^{t''_i} C'_i h_4^i)^{\frac{1}{+f_i}}$, 并释放 (B_i, t''_i , f_i,$_i$,Y_i) 对于 U_i, 其中 $INT(x)$ 是最接近的整数函数。

U_i 从服务提供者处检索 (B_i, t''_i , f_i,$_i$,Y_i) , 计算 t_i =t'_i+t''_i , $P'_i = P_i + _i$ 并检查是否 $\hat{e}(Sg^{f_i}$,$B_i)$=$\hat{e}(g, h_0 h_1^{t_i} h_2^{a_i} h_3^{I_i} h_4^{P'_i})$。如果是, 则 U_i 使用新的元组 (B_i, f_i, t_i, P'_i) 替换之前的元组并将它们与 (A_i,e_i, s_i, a_i, T_i,$\widehat{A}_i$, RK_i) 一起存储。同时,U_i 将 P'_i 存储在只读存储器中, 可用于在未来的众测活动中显示信用积分。此外, 由于 (B_i, f_i, t_i, P'_i) 由 U_i 管理,U_i 能够证明 (B_i, f_i, t_i) 跨服务提供商的所有权。在参与不同服务商提供的移动众测服务期间, 可以累积不同服务商授予的信用积分,U_i 可以向多个服务商证明她拥有的信用积分。

第 5 章 安全性分析

在本节中，我们展示了 SPOON 满足 3.3 中定义的五个安全目标：位置隐私、匿名性、数据机密性、信用平衡和贪婪用户跟踪。

5.1 位置隐私

任务的感知区域表示为矩阵 $\widehat{L}_{m\times n}$，由随机矩阵 $\widehat{M}_{m\times n}$ 随机化生成 $\widehat{N}_{n\times n}$。移动用户的位置也被变换为 $\widetilde{N}_{n\times n}$。从 $\widehat{N}_{n\times n}$ 和 $\widetilde{N}_{n\times n}$ 两个矩阵中，服务提供者无法获知有关移动用户的位置或任务的感知区域的任何信息。可逆矩阵 $\widetilde{M}_{m\times n}$ 和 $\widehat{M}_{m\times n}$ 分别相乘，$\widetilde{L}_{m\times n}$ 的秩等于 $\widetilde{N}_{n\times n}$，$\widehat{L}_{m\times n}$ 的秩等于 $\widehat{N}_{n\times n}$。服务提供商计算 $N_{n\times n} = \widetilde{N}_{n\times n} \bullet \widehat{N}_{n\times n} = \widetilde{M}^{T}_{m\times n} \bullet \widetilde{L}_{m\times n} \bullet \widehat{L}^{T}_{m\times n} \bullet \widehat{M}_{m\times n}$。因此，$N_{n\times n}$ 的秩等于 $\widetilde{L}^{T}_{m\times n} \bullet \widehat{L}_{m\times n}$ 的秩。如果 $N_{n\times n}$ 的 rank 为 0，即 $N_{n\times n}$ 是零矩阵，则 $\widetilde{L}_{m\times n}$ 和 $\widehat{L}_{m\times n}$ 中具有相同索引的两个条目之一必须为 0，表示任务的感知区域之间没有重叠和移动用户的位置。否则，任务的感知区域和移动用户的位置之间会有一些重叠。如果存在一个重叠网格，其对应的条目分别为 $\widehat{L}_{m\times n}$ 中的 $\widehat{L}_{i\times j}$ 和 $\widetilde{L}_{m\times n}$ 中的 $\widetilde{L}_{i\times j}$，则 $\widehat{N}_{n\times n}$ 的 j 行和 $\widehat{N}_{n\times n}$ 的 j 列中的条目非零 n. 因此，服务提供者能够知道感测区域的 j 列上有一些重叠的位置，但是它无法区分与 m 个位置重叠的位置。此外，$\widehat{N}_{n\times n} \bullet \widetilde{N}_{n\times n}$ 或 $\widetilde{N}_{n\times n} \bullet \widehat{N}_{n\times n}$ 不能向服务提供商提供更多信息。如果重叠的网格不止一个，结果是相同的。因此，移动用户的感应区域或位置不会暴露给服务提供商或其他实体。

5.2 数据保密

我们的目标是确保只有位置与感知区域匹配的移动用户才有能力解密相应的感知任务。在 SPOON 中，攻击者可能是服务提供商、无与伦比的移动用户和外部攻击者。为了抵抗这些对手，任务保护包括两个阶段。第一阶段，感知任务由客户在 TA 和服务提供商的公钥下进行加密；在第二种情况下，服务提供商使用其密钥对密文进行部分解密，然后为匹配的移动用户重新加密结果。因此，我们在以下两个过程中证明了任务机密性：

- 首先，第一阶段密文不应该对服务提供商或移动用户完全解密。具体来说，给定第一阶段密文 (c_1^*,c_2^*,c_3^*) 和两个明文 ($task_1||u_1, task_2||u_2$)，如果对手能够区分 ($task_1||u_1, task_2||u_2$) 是 (c_1^*, c_2^*,c_3^*) 的明文，我们展示了如何构建一个模拟器 S 来

解决 q-DBDHI 问题。给定简化的 q−DBDHI 元组 g, $T_1 = g^{z_1}$, $T_2 = g^{z_2} \in G_1$, h $\in G_2$, Q $\in G_T$ ，模拟器 S 的目标是通过与对手的交互来确定 Q = $\hat{e}$(g, h) $\frac{z_1}{z_2}$。S 设置 T = T_1。拥有服务提供者的密钥 β 的攻击者可以向模拟器 S 查询任何选择的消息任务 ||u 以获得相应的密文。然后，S 选择两条消息 $(task_1||u_1, task_2||u_2)$ 和一个随机位 b ∈ 0, 1 来计算挑战 $(c_1^*, c_2^*, c_3^*) = (S^{r2}, T_2, (task_b||u_b)QH^{r_2})$，其中 r_2 是从 z_p 中选择的随机值，并将 $(task_1||u_1, task_2||u_2)$ 与 (c_1^*, c_2^*, c_3^*) 一起返回给对手 3）。最后，攻击者返回 $\hat{b} \in 0, 1$ 给 S。如果 $\hat{b}$ = b，S 可以将简化的 q−DBDHI 问题解决为 Q == $\frac{c_3^*}{(task_b||u_b)\hat{e}(c_1^*, h_0)^{/frac-1}}$ 。针对拥有 α 的对手的任务机密性也依赖于简化的 q−DBDHI 问题，给定 h, $T_1 = g^{z_1}$, $T_2 = g^{z_2} \in G_1$, $h_0 \in G_2$, Q $\in G_T$ ，模拟器 S 的目标是确定是否 Q = $\hat{e}$(g, h_0) $\frac{z_1}{z_2}$ 通过与对手的交互。证明与上述相同，不同之处在于挑战是 $(c_1^* = T_2, c_2^* = T_1^{r1}, c_3^* = (task_b||u_b)QG^{r1})$，其中 r_1 是从 Z_p。最后，S 可以将简化的 q−DBDHI 问题解决为 Q == $\frac{c_3^*}{(task_b||u_b)\hat{e}(c_2^*, h)^{-1}}$ 。

- 其次，感知任务只能由匹配的移动用户从第二阶段密文中恢复。为了防止不匹配的移动用户学习感知任务的内容，服务提供商使用代理重加密方案使用临时公钥 μ 对感知任务进行加密。因此，第二阶段密文的安全性也可以简化为 q-DBDHI 假设。

为了保证传感报告的机密性，每个移动用户采用代理重加密方案在临时公钥 $u = g^k$ 下加密 m_i，它与传感任务一起分发给移动用户。解密密钥 k 由客户秘密保存。因此，m_i 的保密性直接取决于代理重加密方案的语义安全性，可以简化为简化的 q-DBDHI 假设 [42]。

5.3 匿名性

移动用户的匿名性是通过游戏定义的，在该游戏中，在所有其他交互都由对手指定的极端条件下，对手无法将诚实的移动用户从两个中区分开来。我们证明移动用户的身份得到了适当的保留，除非 DDH 假设不成立。具体来说，如果存在一个可以从两个具有挑战性的身份中识别出诚实的移动用户的对手 A，我们将展示如何构建一个模拟器 S 来解决 DDH 问题的一个实例。也就是说，给定一个元组 $T_1, T_2, T_3, T_4 \in G_T$ ，S 可以判断是否存在 (z_1, z_2)，使得 $T_2 = T_1^{z_1}$, $T_3 = T_2^{z_1}$, $T_4 = T_1^{z_1 z_2}$ 。S 生成 (param, S, T)，选择两个身份 (I_0, g^{a_0}), (I_1, g^{a_1}), 满足 $a_0, a_1 \in z_p$，并将它们发送给 A。S 代表用户 I_0 和 I_1 在 TA 注册。然后 S 在以下交互中与 A 交互：

- S 作为 I_0 诚实地提交位置信息。对于 I_1，在第 j 个查询中，S 随机选择 $_j \in G_2$ 并模拟零知识证明 PK_3 来证明其与 A 交互的身份。

- S 诚实地代表 I_0 报告数据。对于 I_1，S 设置 H = T_1，G = T_2。对于第 j 个查询，S 随机选择 X_j,$v_j \in z_p$ 并计算 $Y_j = T_1^{v_j}$, $Z_j = \hat{e}(g, h_0^{a_1}) T_2^{X_j v_j}$ 。S 模拟零知识证明 SPK 并向 A 发送 (X_j, Y_j, Z_j, SPK) 以及随机传感报告。

S 选择一个随机位 b □ 0, 1。如果 b = 0，S 诚实地报告作为 I_0 的数据。如果 b = 1 且 S 随机选择 $X_1 \in z_p$ 并计算 G = T_2,$Y_1 = T_3$,$Z_1 = \hat{e}(g, h_0^{a_1}) T_4^{X_1}$ 。然后，S 模拟 SPK 和传感报告，并将它们发送给 A。很容易看出，如果 $\log_{T_1} T_4 = log_{T_1} T_2 log_{T_1} T_3$，则模拟是完美的；否则，它不包含有关 I_0 和 I_1 的信息。

最后，A 返回 $\hat{b}$。如果 $\hat{b}$ = b，S 可以确认存在 (z_1, z_2)，使得 $T_2 = T_1^{z_1}$, $T_3 = T_2^{z_1}$, $T_4 = T_1^{z_1 z_2}$ 。因此，S 解决了 DDH 问题。

在客户匿名证明中，模拟器 S 模拟签名（A，e，s）PK_2 的零知识证明的副本，与攻击者 A 进行交互。由于 S 可以完美模拟 PK_2，因此攻击者无法获得客户的任何身份信息，使得 A 无法区分一个诚实的客户和两个。因此，客户的匿名性可以得到充分保证。

5.4 信用额度

信用余额意味着没有人可以拥有超过初始信用点加上服务提供商授予的信用点的信用点。这是从安全角度对信用管理最重要的要求。假设 P_0 是初始信用积分，$_j$ 是第 j 个查询中从服务提供商那里获得的积分。如果攻击者 A 最多进行 $\hat{R}$ 报告查询，并且拥有最终信用点 P_f ，其中 $P_f > P_0 + \sum_{j=1}^{\hat{R}} {}_j$，而服务提供者不识别双重报告，则必须存在模拟器 S 进行伪造攻击底层 BBS+ 签名。

首先，我们假设零知识证明 PK_1 、PK_2、PK_3 和 SPK 是可靠的。即存在提取算法 ξ_{χ_1}、ξ_{χ_2}、ξ_{χ_3} 和 ξ_{χ_5} 分别获取零知识证明的见证人

然后，我们展示了与 A 交互的模拟器 S。S 生成公共参数 param、公钥 (T, S) 和密钥 (α, β)，并被允许访问签名预言机 SO 以获得 BBS+ 输入的签名。S 发送 (param, S, T) 到 A 并与 A 交互如下：

- A 随机选择 C □ $G_1, C', \widehat{A} \in G_2$，生成证明 PK_1 并将它们发送给 S。S 使用 ξ_{χ_1} 从 PK_1 中提取见证 (s′, t′, a)，然后选择一个随机信用点 P_0 并查询签名预言机

SO 以获得 (A, e, s) 和 (B, f, t)。最后 S 计算 s″ = s − s′, t″ = t − t′ 和 $RK = \widehat{A}^{\frac{1}{}}$，并返回 (A, e, s″, B, f, t″, P_0, RK) 到 A。

- 对于第 j 个查询，A 选择一个随机 $C'_j \in G_2$ 并与 S 执行 SPK。S 利用 $\xi\chi_s$ 提取见证 (B_j,f_j,t_j, t'_j,a_j,I_j,P_j,v_j)。如果 (B_j,f_j,t_j) 不是 SO 的输出，则它是 BBS+ 签名的伪造。否则，S 查询 SO 以获得输入 (a_j, $P_j + {}_j$, I_j) 上的签名 (B_j,f_j,t_j)。S 接收 (B_j,f_j,t_j)，计算 $t''_j = t_j$ - t'_j，并将 (B_j,f_j,t''_j) 返回给 A。
-

最后，假设 A 执行 $\hat{R}$ 查询。如果 A 能够证明，$P_f > P_0$+$\sum_{j=1}^{\hat{R}} {}_j$ 则 A 获胜。但是，如果 $P_f > P_0$+$\sum_{j=1}^{\hat{R}} {}_j$，则 A 一定是进行了伪造的 BBS+ 签名或重复报告了数据。虽然 BBS+ 签名在 q-SDH 假设下是安全的，但 A 不能伪造 BBS+ 签名，除非 q-SDH 假设不成立。如果 A 重复上报传感数据，则必须在同一时隙内生成另一个 eZi，该 eZi 与前一个 Zi 不相等。由于零知识证明协议的健全性，$Z_i = \hat{e}(g, \widehat{A}_i)G^{X_i v_i}$ 是伴随 X_i 和 Y_i 识别的特定报告的唯一有效 Z_i。由于 X_i 在两个报告中应该不同，只要证明有效，就会得到 $\hat{e}(g, \widehat{A}_i)$。我们假设证明 SPK 是正确的。因此，A 的双重报告的成功概率可以忽略不计。因此，如果 q-SDH 假设成立，则获得 $P_f > P_0$+$\sum_{j=1}^{\hat{R}} {}_j$ 的概率可以忽略不计。

5.5 贪婪的用户追踪

贪婪用户追踪包括两个目标，即防止诽谤和隐藏。诽谤预防是指攻击者不能诽谤诚实的移动用户，而隐藏预防是指贪婪的用户必须被 TA 识别。对于诽谤，攻击者会发布一些报告记录，这些记录可以链接到诚实的移动用户提交的其他报告。由于证明 SPK 是可靠的，因此攻击者无法计算出诚实移动用户的跟踪信息。因此，没有攻击者能够诽谤诚实的移动用户。在隐藏方面，攻击者需要在不被追踪的情况下生成不同的追踪信息。但是，如果伪随机函数 F 正确，贪婪的移动用户就不可能计算 Zi。

综上所述，SPOON 实现了位置隐私保护、感知数据保密、移动用户和客户匿名、信用平衡和贪婪用户追踪。

第 6 章 扩展

在本节中，我们提出了一种评估感知报告信任级别的方法和一种新的隐私保护位置匹配机制，以实现移动人群感知的通信高效任务分配。

6.1 信任度评估

服务商上传 w 个感知报告给客户，客户评估每份报告的信任度，将信用点分配给移动用户。由于数据源的各种智能，传感报告具有明显的可信度。此外，一些移动用户可能会伪造传感数据或提供模棱两可、有偏见的数据，以通过作弊获得信用积分。因此，我们提出一个公平的信任评估机制如下：

- 客户生成感知区域内与网格相关的感知数据权重 $_{z\{z\in L\}} \in (0, 1]$，使得 $\sum_{\{z\in L\}}^{z} = 1$，并将 w 个感知报告分成 |L| 组，其中 |L| 表示传感区域的网格数，如果一个传感报告中的数据是从多个网格中收集的，则该报告同时在与这些网格关联的组中。

- 对于组 z □ L 中的每个传感报告，客户计算相似度 V_i,z。如果传感报告与同一组中的其他报告显着不同（例如，相反的结果），则其相似度设置为负值 $V_i,z \in [-, 0]$。否则，客户为报告设置正相似度 $V_i,z \in (0,]$。

- 对于组 z □ L 中的每个传感报告，客户计算 $_{i,z} = V_{i,z}Q_i$ 和 $Exp_z = \sum_{i\in Z} i,z$，其中 Z 表示组 z 中的传感报告集合。然后，客户将传感报告的信任级别设置为 $_i,z = (\frac{i,z}{Exp_z})_z$。

- 如果报告仅包含从一个网格收集的数据，则其信任级别为 $_i = _{i,z}$；否则，信任级别被设置为所有网格的信任级别的平均值，其中 mi 被收集为 $_i = AVE_z(_{i,z})$。

6.2 效率提升的任务分配

在 SPOON 中，我们使用矩阵 $\widehat{L}_{m\times n}$ 和 $\widetilde{L}_{m\times n}$ 分别表示任务的感知区域和移动用户的位置。为了防止攻击者获取位置信息，利用 $\widehat{M}_{m\times n}$、$\widetilde{M}_{m\times n}$ 来随机化 $\widehat{L}_{m\times n}$、$\widetilde{L}_{m\times n}$。虽然这种方法计算效率高，并且实现了位置保护，但服务提供者必须在服务建立阶段定义其服务区域，并且在任务分配阶段的通信开销有点大，因为客户和移动用户

都需要传输矩阵 $\widehat{N}_{n\times n}$，$\widetilde{N}_{n\times n}$ 给服务提供商。为了降低通信成本，我们通过采用 BGN 加密 [45] 提出了一种高效的通信位置匹配机制。

在服务设置阶段，除了生成参数和公开密钥对（α，T，T_0），TA 设置 BGN 加密。它选择两个随机 λ 位素数 q_1, q_2，设置 n = q_1q_2，并生成两个满足双线性映射 $\tilde{e}: G_1 \times G_1 \rightarrow G_2$ 的 n 阶双线性群 G_1, G_2。它还选择一个随机生成器 l □ G_1 来计算 $l_1 = l^{q_2}$。因此，TA 的公钥为 (n, G_1, G_2, l, l_1, T)，秘密密钥为 (α, q_1)。

当具有 (A, e, s, B, f, t, a, I, P, $\widehat{A}$, RK) 的客户有感知任务 ST = ($task$, $expires$, $area$,,w) 要分配给移动用户，按照 4.4.3 中给出的步骤，它生成（c_1，c_2，c_3，u，PK_2）。感应区域面积定义为一个圆，由圆心 L_c = (L_{cx}, L_{cy}) 和半径 R 唯一标识，其中 L_{cx} 为经度，L_{cy} 为纬度。如图 3 所示，假设移动用户 U1 的地理位置为 L_{u_1}。如果 L_{u_1} 和 L_c 之间的距离小于 R，则 U_1 位于感应区域；否则，它超出了众包感知区域。为了保护传感区域，客户选择三个随机值 r'_x、r'_y、r'_r □ Z_n 并计算 $C_x = l^{L_{cx}} l_1^{r'_x}$ □$C_y = l^{L_{cy}} l_1^{r'_y}$ 和 $C_R = l^R l_1^{r'_r}$ 。客户发送 (c_1,c_2, c_3, $expires$, PK_2, C_x,C_y,C_R,,w) 给服务提供商，后者如 4.4.3 所述释放任务 ST。

如果一个移动用户 U_i 想要执行传感任务，它会选择一个随机的 ν □z_p 来计算 $= h$。然后，U_i 从 GPS 设备或接入点检索位置信息 $L_{u_i} = (L_{ix}, L_{iy})$，并使用 TA 的公钥对其进行加密，如下所示：选取随机值 r''_x，$r''_y \in$ Zn 计算 $U_x = l^{L_{ix}} l_1^{r''_x}$ ，$U_y = l^{L_{iy}} l_1^{r''_y}$。最后，$U_i$ 生成 PK_3 并将 (,U_x,U_y, PK_3) 发送给服务提供者。

服务提供者收到 (μ, U_x,U_y, PK_3) 后，首先判断感知任务的感知区域是否覆盖了 U_i 的位置。对于每个未过期的任务，服务提供者计算 $X' = \tilde{e}(\frac{C_x}{U_x}, \frac{C_x}{U_x}), Y' = \tilde{e}(\frac{C_y}{U_y}, \frac{C_y}{U_y})$ 和 $Z' = X'Y'$，然后将 Z' 发送给 TA 每个任务都使用 (C_R, num)。TA 解密 Z' 和 C_R 分别恢复 d_i 和 R，并检查 d_i<R 找到匹配的感知任务集合，并将任务编号 num 返回给服务提供者。然后，服务提供者生成 c_4 并为 U_i 释放 (num,c_2, c_3, c4, $expires$,)。最后，U_i 获得感知任务并收集数据。

基于 BGN 加密设计了位置匹配机制，利用同态性计算圆心到移动用户位置的距离。这种机制的安全性可以简化为 BGN 加密方案的语义安全性。此外，需要客户发送 (C_x, C_y,C_R)，移动用户需要发送 (U_x,U_y) 到运营中心，比 $\widehat{N}_{n\times n}$ 和 $\widetilde{N}_{n\times n}$ 短。

第 7 章 效果评估

在本节中，我们评估 SPOON 在计算和通信开销方面的性能，并分析信用管理的隐私率和准确率。

7.1 计算开销

计算开销是指我们提出的 SPOON 对系统中每个实体的执行时间。计算开销可以用耗时的密码操作数来表示，包括 G_T 中的点乘、点加法、双线性映射和指数运算，因为其他操作的运行时间，例如 G_T 中的乘法、加法、乘法和逆运算与这四个操作相比，Z_p 中的操作可以忽略不计。此外，由于双线性映射是密码计算中最耗时的操作，我们利用预处理技术来减少每个实体的计算负担。具体来说，TA 在服务设置阶段预先计算了双线性映射 $Ei_{i=0}^{3}, F, Fi_{i=0}^{4}$，如附录 A 所示，在用户注册中预先计算了双线性映射$\hat{e}$(g, $\widehat{A}_i$)Ni=0 阶段，其中 N 是注册者的数量。移动用户 U_i 也可以在用户注册阶段预先计算 e(g, $\widehat{A}_i$)。表三分别显示了每个实体在 SPOON 的每个阶段执行的操作数.

我们还进行了一项实验，以显示每个实体执行提议的 SPOON 的时间成本。TA 和服务商的操作是在一台 Intel Core i5-4200U CPU 的笔记本上进行的，主频 2.29GHz，内存 4.00GB。操作系统为 64 位 Windows 10，C++ 编译器为 Visual Studio 2008。客户和移动用户的操作在华为 MT2-L01 智能手机上运行，CPU 为麒麟 910，内存为 1250M。操作系统为 Android 4.2.2，工具集为 Android NDK r8d。我们使用 MIRACL 库 5.6.1 来实现基于数论的密码学方法。R-ATE 配对用于实现类型 3 双线性配对。Barreto-Naehrig 曲线，即 Fp-256BN，E : y2 = x3 + 3 在 F_p 上定义。z 是一个整数，因此 n = $36z^4$ + $36z^3$ + $18z^2$ + $6z$ + 1，p = $36z^4$+ $36z^3$ + $24z^2$+ $6z$ + 1 是素数并且 #E(F_p) = n。嵌入度 k = 12 是 $n|p^4-1$ 的最小正整数。$E[n] \subsetneq E(F_{p^{12}})$，其中 E(n) 表示 E 上所有 n−torsion 点的集合。令 G_1 = E(F_p)，G_2 是 E(n) 的迹 0 阶 n 子群，G_T 是 $F_{p^{12}}^{*}$ 的 n 阶子群。p 是大约 256 位的大素数。(g, g_0, g_1, g_2, g_3), $(h, h_0, h_1, h_2, h_3, h_4)$ 和 G 分别从 G_1、G_2 和 G_T 中随机选择。H 是 SHA-256，F 是通过 AES-256 模拟的。表 3 显示了 SPOON 每个阶段的每个实体在对应设备上实现的时间成本。每个实体的运行时间小于 300ms。因此，我们的 SPOON 部署在移动设备上是相当高效的。

Phase	User Registration		Task Allocation			Data Reporting			Credit Assignment	
	Authority	User	Customer	Provider	User	Customer	Provider	User	Provider	User
Point Multiplication	16	19	11	12	9	0	19	25	3	5
Point Addition	12	13	5	8	5	0	14	16	3	5
Bilinear Map	0	4	1	1	2	1	5	2	0	2
Exponentiation in $\mathbb{G}_T$	0	0	6	15	8	1	19	15	0	0
Running Time (ms)	48.361	289.246	97.943	51.925	152.547	55.144	132.398	201.034	9.755	132.288

图 7-1 SPOON 的计算开销

7.2 通信开销

通信开销是指 TA、服务提供商、移动用户和客户之间交换的数据数量。请注意，仅考虑 IP 数据包的数据（即有效负载），数据包头和尾不计入通信开销，因为如果确定了数据包的数量，它们是固定的。记录 SPOON 中任意两个实体之间交换的数据的二进制长度。公共参数设置与实验相同，即 |p|=256 位，|q|=1024 位。在用户注册阶段，注册者，无论是客户还是移动用户，向 TA 发送注册请求（I，C，C'，$\widehat{A}$，PK_1），即 $|I|+2176$ 位，其中 $|I|$ 是标识的二进制长度，TA 返回 $(A, B, s'', t'', e, f, P_0, R_K)$ 给注册者，其二进制长度为 $|P_0|+2176$ 位，其中 $|P_0|$ 是信用点的二进制长度。在任务分配中，客户上传 (c_1,c_2,c_3,$expires$, $\widehat{N}_{n\times n}$,,w, PK_2)，移动用户发送 (, $\widetilde{N}_{n\times n}$, PK_3) 给服务商，即 $4512+160n^2+|\square\square|+||+|w|$ 位和 $2976+160n^2$ 位，分别。服务提供者响应 (num,c_2, c_3, c_4, $expires$, γ)，即 2560 + $|num|$ + | 过期 | + || 位，匹配的移动用户或假，1 位，不匹配的用户。移动用户获取感知数据后，生成感知报告（num，D_i，D'_i，C'_i，X_i，Y_i，Z_i，Q_i，$_j$，SPK）给服务商，即 8864+$|num|$ + $|P_0|$ + $|_j|$ 位。如果移动用户重复提交数据，服务提供方需要向 TA 发送 1024 比特的 W，然后发送 w 个感知报告（num，D_i，D'_i，Y_i,Q_i，$_j$），二进制长度为 w□ (2560 + $|num|$ + $|P_0|$ + $|_j|$)，给客户。最后，客户为每个报告返回 (1024 + ||)-bit ($_i, Y_i$) 给服务提供商，服务提供商将 $(B_i, t''_i, f_{i,i}, Y_i)$ 发送给每个移动用户，即 1856 + $|P_0|$ 二进制位。

7.3 信用分析

为了防止信用点泄露给其他实体，每个移动用户都声明了一个阈值 Q_i，该阈值被证明小于其确切的信用点 P_i，以便云提供商可以根据声明的阈值选择传感报告。这样，无论是云提供商还是客户都无法获知移动用户的准确信用点。不幸的是，这种方法降低了报告选择的准确性，因为云提供商可能会选择移动用户的感知报告，其阈值大于其他人的，而信用点则具有相反的趋势。另一方面，客户可能更喜欢移动

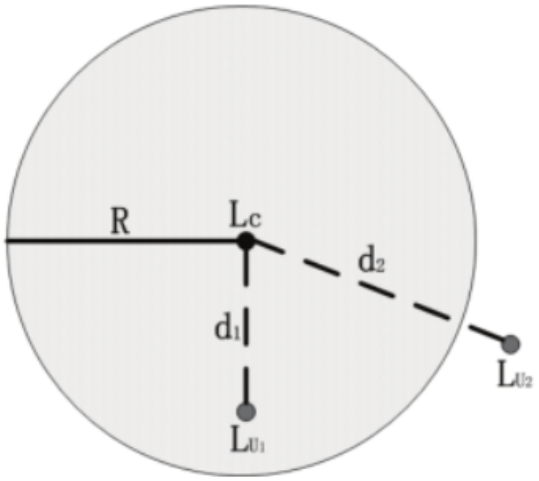
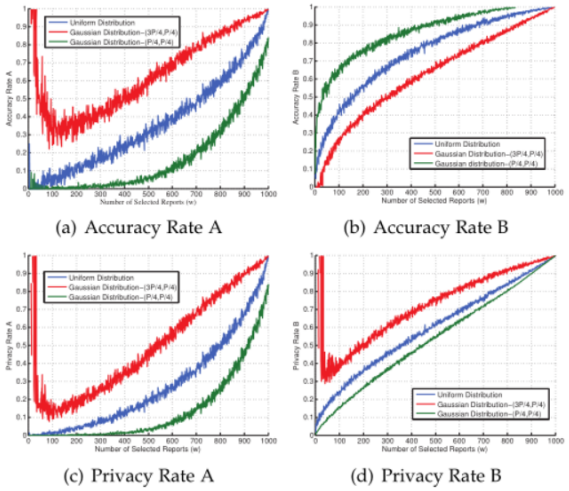


图 7-2 感知圆和位置

用户选择与其信用点相近的阈值，同时牺牲了移动用户的隐私。因此，似乎无法调和隐私和准确性之间的矛盾，因为它们具有相反的趋势。

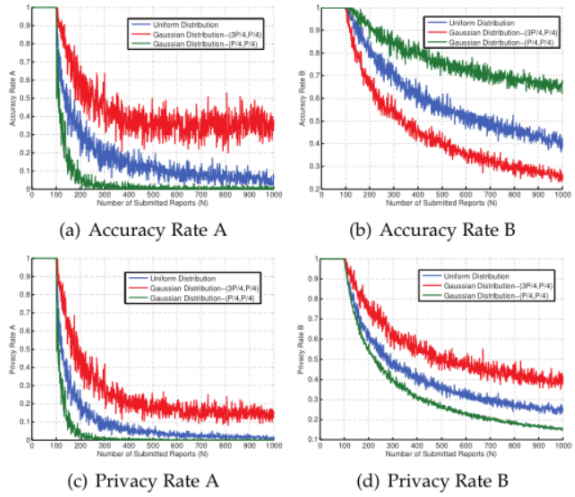
为了平衡这种权衡，为移动用户找到合理的策略来确定阈值至关重要。我们定义了四个参数来评估信用声明中的隐私和准确性。具体而言，准确率 A 表示所选报告中给定阈值的最大概率可以拥有感测报告中的 top-w 信用点。准确率 B 表示传感报告中的给定信用点大于所选报告中的最小阈值的最大概率。隐私率 A 是指给定的传感报告，其信用点大于所选报告中阈值的最小值，在所有传感报告中具有 top-w 信用点的概率。隐私率 B 是指服务提供商选择给定传感报告的概率，其信用点大于所选报告中阈值的最小值。为了确定阈值选择策略如何影响定义的隐私和准确率，我们在 Matlab 上模拟移动用户的信用点，并使用不同的阈值选择策略来计算准确率和隐私率。仿真结果如图 4 和图 5 所示。我们在图 4 中设置移动用户数为 1000，在图 5 中设置选择报告数为 100。我们比较了三种阈值选择策略，第一个是基于均匀分布；二是基于高斯分布，均值为移动用户信用积分数的四分之三，标准差为四分之一；最后一个是基于高斯分布，其中均值和标准差是学分数的四分之一。在三种策略中，第二种策略实现了最高的准确性，第三种策略实现了对信用点的最佳隐私保护。



(a) Accuracy Rate A (b) Accuracy Rate B

(c) Privacy Rate A (d) Privacy Rate B

图 7-3 N=1000 准确率和隐私率



(a) Accuracy Rate A (b) Accuracy Rate B

(c) Privacy Rate A (d) Privacy Rate B

图 7-4 w=100 准确率和隐私率

结　论

在本文中，我们提出了一种具有信用管理的强大的隐私保护移动群智感知方案，以支持移动用户的隐私保护和客户的任务分配。服务提供者可以根据任务的感知区域和移动用户的地理位置，选择移动用户进行感知任务完成，并根据移动用户的信用点选择感知报告。在任务分配和报告选择过程中，为移动用户和客户保留了包括身份、位置、信用点、传感任务和传感报告在内的敏感信息。此外，不需要可信第三方来实现对移动用户的信用管理。最后，我们展示了所提出方案在安全性和效率方面的优势。它使服务提供商能够构建安全高效的移动众测服务，为客户提供准确的任务分配和信任管理。在未来的工作中，我们将在移动众感中设计一个隐私保护的上下文感知任务分配框架。