面向群智感知应用的基于协作的位置认证方案

田有亮[1,2,3]，田茂清[1,2]，高鸿峰[2]，何淼[4]，熊金波[1,2,5]

（1. 贵州大学公共大数据国家重点实验室，贵州 贵阳 550025；2. 贵州大学计算机科学与技术学院，贵州 贵阳 550025；
3. 贵州大学密码学与数据安全研究所，贵州 贵阳 550025；4. 女王大学电子和计算机工程学院，安大略 金士顿 ON K7L 3N6；
5. 福建师范大学计算机与网络空间安全学院，福建 福州 350117）

摘 要：群智感知利用移动设备收集与位置相关的数据，存在位置欺骗攻击的安全问题，如何保障这些敏感数据的质量成为一个挑战。针对此问题，提出了一种基于协作的位置认证方案来检测提交虚假位置的恶意用户。首先，利用携带移动设备的用户为彼此生成位置证明，利用随机数多次碰撞获取新信息的距离边界协议构造位置认证方案，保证了用户位置的不可伪造，达到提高数据质量的目的。其次，基于区域划分和信誉模型的方法选择位置证明协作者，有效防止了共谋攻击，解决了权益集中的问题。同时，基于信誉值和任务完成时效的激励机制有效提高了协作者完成任务的效率。最后，通过安全性分析和性能评估证明了所提方案的正确性和安全性，以及在计算和通信开销方面的优势。

关键词：距离边界协议；位置认证；群智感知；共谋攻击；信誉激励

中图分类号：TP309

文献标志码：A

DOI: 10.11959/j.issn.1000−436x.2022173

Cooperation-based location authentication scheme for crowdsensing applications

TIAN Youliang[1,2,3], TIAN Maoqing[1,2], GAO Hongfeng[2], HE Miao[4], XIONG Jinbo[1,2,5]

1. State Key Laboratory of Public Big Data, Guizhou University, Guiyang 550025, China
2. College of Computer Science and Technology, Guizhou University, Guiyang 550025, China
3. Institute of Cryptography & Data Security, Guizhou University, Guiyang 550025, China
4. College of Electrical and Computer Engineering, Queen's University, Kingston ON K7L 3N6, Canada
5. College of Computer and Cyber Security, Fujian Normal University, Fuzhou 350117, China

Abstract: Utilizing mobile devices to collect location-related data in crowdsensing has the security problem of a location cheating attack. How to guarantee the quality of these sensitive data has become a challenge. In response to this, a location authentication scheme was proposed based on cooperation to detect malicious users who submit false locations. Firstly, users with mobile devices were used to generate location proofs for each other, and a location verification scheme was designed based on distance bounding protocols for obtaining new information by multiple collisions of the same random number, which ensured the user's location should be unforgeable and achieved the purpose of improving the quality of collected data. In addition, a location proof cooperator select method based on region division and reputation model was proposed which effectively prevented collusion attack and solved the problem of concentration of equity. Meanwhile, the incentive mechanism based on reputation value and task completion time was designed to effectively improve the location proof cooperator efficiency of task completion. Finally, security analysis and performance evaluation indicate that the scheme has proved to be correctness and secure, and the advantages in computational cost and communication overhead.

Keywords: distance-bounding protocol, location authentication, crowdsensing, collusion attack, reputation incentive

收稿日期：2022−04−28；**修回日期：**2022−07−15

基金项目：国家重点研发计划基金资助项目（No.2021YFB3101100）；国家自然科学基金资助项目（No.U1836205）；贵州省高层次创新型人才基金资助项目（黔科合平台人才[2020]6008）；贵阳市科技计划基金资助项目（筑科合[2021]1-5，筑科合[2022]2-4）；贵州省科技计划基金资助项目（黔科合平台人才[2020]5017，黔科合支撑[2022]一般 065）

Foundation Items: The National Key Research and Development Program of China (No.2021YFB3101100), The National Natural Science Foundation of China (No.U1836205), Project of High-Level Innovative Talents of Guizhou Province (No.[2020]6008), Science and Technology Program of Guiyang (No.[2021]1-5, No.[2022]2-4), Science and Technology Program of Guizhou Province (No.[2020]5017, No.[2022]065)

0 引言

随着具备传感、计算和存储能力的移动智能终端的大量普及，出现了很多群智感知应用和服务[1]，例如，环境检测[2]、广告发布[3]、基于位置的服务[4-5]等。群智感知应用通过招募携带嵌入传感器的智能终端用户作为数据收集者，收集与特定时间和地点相关的数据，然后将数据发送给收集者进行分析。该技术被认为是一种可以用来解决现实问题（如交通预测/管理[6]）的有效方法。相对于使用固定位置传感设备收集信息的方式，群智感知应用具有部署成本低、灵活性高、移动设备数量大、覆盖范围广等优势[7]。

群智感知应用通过对多个移动智能终端收集的数据进行处理，以获得更多的有效信息。为了提高收集数据的安全性和可靠性，大多数群智感知任务请求者需要限定参与者完成任务的位置。然而，感知任务通常在不受信任的环境下由不同类型的参与者协作完成，因此保证参与者身份和位置信息的真实性在群智感知应用中占据十分重要的地位。该类应用中位置欺骗攻击会对感知结果产生严重的影响，在车辆群智感知应用中提交被车辆恶意伪造的位置信息，并上传错误位置上产生的数据，会对感知任务发布者的分析造成干扰，给经济带来严重的损失[8]。因此，验证感知任务参与者位置的真实性是很有必要的。

针对位置欺骗攻击，研究者提出了很多位置认证方案。在集中式方案中借助固定基础设施，基于请求位置验证设备的信道状态信息（CSI, channel state information）与在正确位置上相关设备返回的 CSI 之间的相似性比较，从而确定请求设备位置的合法性[9]。但该方案可能会泄露用户的身份隐私，此外，在分布式场景下，借助固定基础设施验证位置真实性增加了成本开销。因此，分布式位置验证方案被提出。大多数分布式方案都是通过提供一定的奖励或资源，激励携带移动智能终端的用户成为位置证明协作者参与位置验证任务。但这些方案采用平均化激励，没有对协作者完成任务的时间与激励关联，可能会导致协作者超时完成位置证明，最终位置验证失败，但仍能获得奖励[10-11]。此外，设计具备基本安全保证的距离边界（DB, distance bounding）协议来测量位置证明请求者与多个证人之间的距离上界，并采用先签名后加密的方法保证了参与位置验证的用户隐私不被泄露[10]。但该方案还存在一些缺陷，首先，没有考虑到随着参与位置验证用户的增加，大量的加解密运算增大了计算开销。其次，只根据信誉值大小选择用户，没有考虑到信誉值低但诚实的用户无法被选择导致权益集中化的问题。权益集中化是指部分信誉值高的用户多次被选择完成位置验证的任务，信誉值低的用户不被选择，奖励集中分发给部分用户，这在一定程度上提高了共谋的可能性。最后，该方案采用的信任模型不能很好地解决用户与位置证明请求者共谋的安全问题。目前，现存方案无法彻底解决位置证明请求者和协作者共谋问题，只能降低共谋攻击成功的可能性。因此，需要一个安全且高效的位置认证方案以解决效率和安全的挑战。

本文面向群智感知应用设计了一种基于协作的位置认证方案。为验证位置的真实性，首先，本文基于文献[12]初始化阶段生成响应值的思想，设计了既可解决隐私问题又可降低计算开销的位置验证协议，并将其集成到群智感知应用位置认证方案中。其次，将信誉值的大小和所得奖励相结合，设计了基于信誉值的激励机制，一方面可以激励更多用户接受位置证明任务，另一方面可用来提高位置证明协作者完成任务的效率。此外，接受位置证明任务的协作者需要提交押金，解决了协作者完成任务超时的问题。最后，针对如何挑选位置证明协作者这一问题，本文将采用区域划分和信誉值大小相结合的方式优化位置证明协作者的选择，该方法不仅可以抵抗共谋攻击，还解决了信誉值低但诚实的位置证明协作者一直不被选择的问题。

本文主要贡献如下。

1) 提出了群智感知应用中一种基于协作的安全高效的位置认证方案。该方案在 DB 协议中利用同一对随机数多次碰撞获取的新信息生成快速响应阶段的响应值，实现了位置的不可伪造。此外，位置验证过程不依赖大量的加解密操作，位置验证参与者不会泄露其身份隐私。因此，本文方案同时满足了隐私和效率要求。

2) 将信誉机制和激励机制相结合，解决了位置验证任务中协作者参与积极性和完成任务效率低的问题。同时，采用区域划分和信誉值大小相结合的方法优化位置协作者的选择，有效地抵抗了共谋攻击并解决了权益集中的问题。

3) 从理论上分析了本文方案的正确性和隐私性，并评估了计算开销和通信开销。与现有文献相比较，本文方案能在保证安全性和隐私性的前提下有效降低计算开销和通信开销。

1 相关工作

近年来，在群智感知领域中提出了很多方案用来提高收集数据的可靠性与隐私性。Xu 等[13]提出了一种隐私保护和可验证的数据聚合方案，实现对收集数据隐私保护的同时任务请求者可以验证收集结果的正确性。Zhang 等[14]研究了基于众包的合作频谱感知中的恶意数据注入攻击，利用外部探测器来验证数据的真实性。Peng 等[15]提出了基于质量的激励机制，以激励理性的参与者提交高质量的传感数据。Xiao 等[16]解决了多个未知任务接受者的招聘问题，目标是在有限的预算下最大限度地提高总传感质量。Wu 等[17]研究了在各种约束条件下能够实现质量最大化的任务分配机制并引起了人们的关注，然而，现有的任务分配机制未能很好地解决恶意用户参与的问题。

现有感知任务大多是在位置约束下执行的，为了过滤用户提交的虚假数据，提高收集到的数据质量，Talasila 等[18]提出位置的真实性是迈向数据可靠性的第一步，并实现了对恶意用户虚假位置证明的检测。Reddy 等[19]描述了一个考虑参与者位置信息、时间可用性和行为习惯的招募方案。He 等[20]通过观察参与者当前位置和预测轨迹，提出了一种高质量的参与者招募方案，最大限度地实现了车辆众包的时空覆盖。因此，验证任务接受者位置的真实性是群智感知应用中一个重要的研究方向。

2009 年，Chandran 等[21]首次提出位置密码学的概念，并在有界检索模型（BRM, bounded retrieval model）下构建了一种位置验证协议，但由于验证者能获取证明者的具体位置，存在位置隐私泄露的风险。Yang 等[22]在文献[21]的基础上提出了一个带隐私的位置验证协议，该协议采用中心化的验证方式，并使用可信机构来验证证明者位置的正确性。然而，采用固定基础设施验证位置的灵活性较差、成本较高，不适用于物联网下大多数的应用场景。另一种位置验证技术是 DB 协议，该协议利用一个验证者度量证明者与其所在位置距离的上界[23]。现有大量文献基于 DB 协议围绕用户位置真实性和隐私性等方面进行研究。Wang 等[24]通过借助邻近移动用户基于 DB 协议为证明者生成位置证明，提出的方案可以确保位置证明的完整性和不可转让性，并设计基于熵的信任评估方法，防止用户共谋攻击。Zhu 等[25]主要通过定期更改假名的方式保护用户的隐私，但会增加计算开销和通信开销。Nosouhi 等[10]提出了一个位置证明生成与验证框架，其使用基于熵的信任模型降低了用户之间共谋攻击成功的概率，并采用先签名后加密的方法保护了用户的敏感信息，但该方案的计算开销和通信开销会随着挑选的位置证明协作者人数的增加呈线性增长。Liu 等[26]提出了一个高效的位置验证协议，但该协议致力于解决位置隐私，无法抵抗共谋攻击。Kounas 等[27]使用可信机构验证用户身份、验证者验证邻近协作者生成的位置证明，实现在验证位置真实性的同时保护用户身份隐私，抵抗了常见的攻击。但使用可信机构和验证者分离的验证方式以及密码承诺的运算增加了大量的计算开销。

在群智感知应用中引入参与者的位置信息可以帮助请求者做出招募决策，但到目前为止关于群智感知应用中参与者招募过程的位置认证和隐私保护问题的研究相对较少。因此，本文提出了一种安全高效的方法来验证感知任务参与者位置的真实性，该方法防止了参与者提交错误位置区域收集到的信息，同时很好地保护了参与者的身份隐私。

2 预备知识

2.1 DB 协议

DB 协议是实时质询–响应协议，用来确定双方距离上界。文献[12]在 DB 协议初始化阶段中使用同一对随机数多次碰撞来获取新随机数的思想生成快速响应阶段响应值。该协议的具体定义如下。

定义 1 元组 $\prod=\{\mathrm{P},\mathrm{V},\mathrm{B},\mathrm{Init},\mathrm{RBE},\mathrm{Verify}\}$ 组成 DB 协议。其中 P 和 V 表示证明者和验证者，B 表示 P 与 V 之间距离上界，该协议执行流程由初始化 Init、快速响应 RBE、验证 Verify 这 3 个阶段组成。

假设 P 和 V 共享密钥 x，协议具体执行阶段如下。

阶段 1　$\mathrm{Init}(N_{\mathrm{V}},N_{\mathrm{P}},x)\rightarrow(y)$

1) V 生成一个随机数 N_{V} 并发送给 P。

2) P 首先生成随机数 N_{P} 计算 $(a^{'},b^{'})=f(x,N_{\mathrm{V}},N_{\mathrm{P}},\mathrm{ID}_{\mathrm{P}})$，$\mathrm{ID}_{\mathrm{P}}$ 表示不变的参数（如身份标识），f 表示伪随机函数，$Z^0=a^{'}$，$Z^1=b^{'}$。其次，P 计算 $y=x\oplus h_0(a^{'},b^{'})$，$h_0$ 表示哈希函数。最后，P 将参数 (N_{P},y) 发送给 V。

3) V 接收到 (N_{P},y) 后验证 y 的正确性，如果不正确，则终止协议；否则，继续执行。

阶段 2 $\mathrm{RBE}(c_i,Z^0,Z^1)\rightarrow(r_i^{'},\Delta t_i)$

1) 该阶段重复 n 次，V 随机生成一个比特位 c_i，将 c_i 发送给 P 的同时将时钟归零，测量往返时延。

2) P 收到 V 发送的挑战值 $c_i^{'}$，计算响应值 $r_i^{'}=Z_i^{c_i^{'}}$，并发送给 V。

3) V 收到 P 发送的响应值 $r_i^{'}$，停止时钟并保存往返时延 Δt_i 和响应值 $r_i^{'}$。

阶段 3 $\mathrm{Verify}(r_i^{'},\Delta t_i)\rightarrow(\mathrm{Accept},\mathrm{Reject})$

V 通过阶段 1 生成的相关参数 $(x,N_{\mathrm{P}},N_{\mathrm{V}},\mathrm{ID}_{\mathrm{P}})$ 和 c_i 可计算正确的 r_i，并验证 $r_i^{'}=r_i$ 和 $\Delta t_i\leqslant t_{\max}$（$i=1,2,\cdots,n$）是否成立。如果 n 轮响应值和往返时延都通过验证，则输出接受 Accept；否则，输出拒绝 Reject。

2.2 位置证明

位置证明（LP, location proof）是一组用来表示用户在特定位置的数字证书，一个 LP 包括一个或多个位置证明段[28]。在本文方案中，通过收集多个位置证明段，并设定位置证明段通过的阈值来判断位置真实性。LP 定义如下。

定义 2 $\mathrm{LP}=\{\mathrm{LP}_1,\mathrm{LP}_2,\mathrm{LP}_3,\cdots,\mathrm{LP}_A\}$ 是一个证明者的位置证明段集合，验证者发布的一条数字证书 LP_j 用于表示证明者在某一特定位置。LP 由 A 个验证者生成的 LP_j 组成。

3 系统模型

3.1 整体框架

本文提出了一种安全且高效的基于协作的位置认证方案。系统模型如图 1 所示，该模型主要由信任机构（TA, trust authority）、任务请求者（TR, task requester）、边缘服务器（ES, edge server）、任务参与者（TP, task participant）、位置证明协作者（LP_C, location proof collaborator）5 类实体组成，具体说明如下。

TA 是完全受信任的一方，在该系统中，负责系统初始化和用户注册，并为不同角色用户分配相关参数。

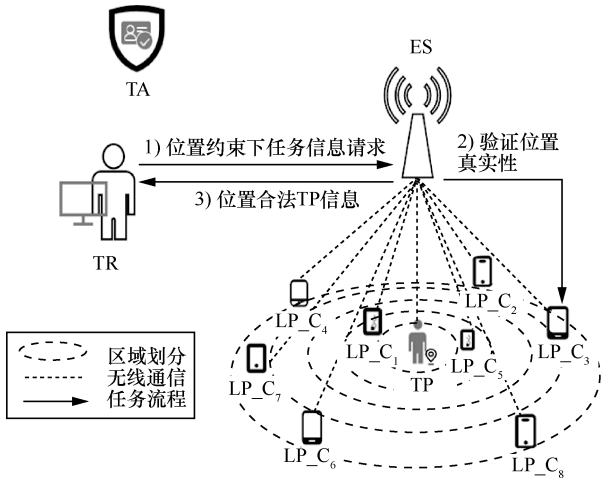


图 1 系统模型

TR 是发布感知任务的一方，该任务可能带有位置约束。

TP 是接受 TR 发布感知任务的参与者，同时，TP 也是位置证明请求者（LP_R, location proof requester），需要验证其位置真实性后才能具有被 TR 选择的机会。

ES 拥有强大的计算能力和存储能力，负责为 TR 验证 TP 位置信息是否真实，并将位置真实的 TP 信息发送给 TR。在该系统模型中也作为位置证明验证者（确保 LP_R 发送的 LP 的合法性）。本文方案中假设 ES 可信。

LP_C 需要遵循协议规范执行 LP_R 发布的位置证明任务，只有位于正确位置区域内的 LP_C 成为合法协作者，生成的 LP 才能被 ES 所接受，是半可信的。根据实际情况，LP_C 也可能成为 LP_R，本文将 LP_C 与 LP_R 称为位置证明参与者。LP_C 在注册期间将获得一个初始信誉值，该信誉值根据其行为不断更新。假设该模型下携带移动智能终端的用户具有短程通信功能。

在本文方案中，TR 首先将带有位置约束的任务请求发送给 ES，ES 需为 TR 挑选积极参与感知任务的 TP。由于 TP 可能不诚实，收集错误位置上产生的感知数据，因此，TP 需要证明其位置的真实性后，才能被 ES 挑选并返回给 TR。为验证位置真实性，TP 成为 LP_R 发布位置证明请求任务，并提交一定的奖励用来激励拥有移动终端的用户接受位置证明任务，被 ES 选择的用户将成为合法 LP_C，LP_C 在接受该任务时缴纳押金并与 LP_R 协作完成 LP。最后，LP_R 向 ES 提交 LP 完成最终验证，ES 将向 TR 返回位置合法的 TP 信息。

3.2　攻击模型

在带位置区域限制的感知任务请求中，参与该任务的用户的目的都是为了获得奖励，恶意的用户可能会对方案产生重大的影响。攻击模型主要针对 LP_R 和 LP_C 的恶意行为展开分析。一个远离合法位置区域的 LP_R 伪造自己的位置信息参与感知任务，并成功获得感知任务请求者的奖励。一个不诚实的 LP_C 可能会与 LP_R 共谋，为 LP_R 生成虚假的 LP 以获得奖励或资源。此外，LP_C 可能会假装参与位置证明任务骗取 LP_R 支付的奖励，或完成任务超时，最终导致任务失败。

4　具体方案

本节基于本文所提出的系统模型，设计了面向群智感知应用的基于协作的位置认证方案。为了更好地描述位置证明与验证过程，将该方案分为 6 个阶段，即系统初始化阶段、注册阶段、位置证明初始化阶段、位置证明协作者选择阶段、位置证明生成阶段和位置证明验证阶段。表 1 列出了本文使用的系统参数。

表 1　系统参数

参数	含义
pk_i	实体 i 的公钥
sk_i	实体 i 的私钥
Cert_i	实体 i 的公钥证书
ID_i	实体 i 的身份标识
$\mathrm{Loc}_{\mathrm{ID}_i}$	实体 i 的位置信息
H_0, H_1	哈希函数
$E_{\mathrm{pk}_i}(m)$	使用实体 i 的公钥加密数据 m
$\mathrm{Sign}_{\mathrm{sk}_i}(m)$	使用实体 i 的私钥对数据 m 签名
$d_{\max}$	LP_R 与 LP_C$_j$ 最大合法距离
c	光速
f	伪随机函数

4.1　系统初始化阶段

TA 在初始化阶段输入安全参数 k，输出系统公开参数 $\mathrm{params}=\{q,\alpha,\mathrm{mpk}\}$，其中，$q$ 表示大素数，α 表示有限域 $\mathrm{GF}(q)$ 上的一个本原根，mpk 表示系统公钥。

4.2　注册阶段

用户向 TA 注册，TA 为用户生成公钥证书 $\mathrm{Cert}(\mathrm{pk},\mathrm{ID})$，并为不同的用户分配相关参数。TA 为 LP_C$_j$ 设置初始信誉值。ES 需生成位置证明列表 $\mathrm{LP\_List}=\{\mathrm{ID}_{\mathrm{LP\_C}_j},\mathrm{ID}_{\mathrm{LP\_R}},\mathrm{Loc},\mathrm{Score}_{\mathrm{LP\_C}_j},\mathrm{num}\}$，其中，Loc 表示位置，$\mathrm{Score}_{\mathrm{LP\_C}_j}$ 表示 LP_C$_j$ 完成位置验证最新评分，num 表示 LP_C$_j$ 协助 LP_R 完成位置验证的次数。

4.3　位置证明初始化阶段

在该阶段，LP_R 向 ES 发送位置证明请求 LP_Req，并与 ES 完成密钥协商，计算位置证明生成阶段所需相关参数，流程如图 2 所示。具体步骤如下。

Step1　LP_R 生成随机数 N_R 和秘密值 X_R，计算 $Y_R=\alpha^{X_R} \bmod q$。通过短程通信接口发布位置证明协作任务，同时向 ES 发送位置证明请求消息 $\mathrm{LP\_Req}=E_{\mathrm{pk}_{\mathrm{ES}}}(\mathrm{ID}_{\mathrm{LP\_R}}\|\mathrm{Loc}_{\mathrm{ID}_{\mathrm{LP\_R}}}\|Y_R\|N_R\|\mathrm{LP\_ID}\|c_R)$，其中，LP_ID 表示位置证明标识，$c_R$ 表示 LP_R 对位置证明请求提供的奖励。

Step2　LP_C$_j$ 在接收到 LP_R 发布的任务后，如果接受，则向 ES 发送包括押金 $c_{\mathrm{LP\_C}_j}$ 和 LP_ID 的任务接受消息 $\mathrm{Mes}^{\mathrm{LP\_C}_j\to\mathrm{ES}}=\{c_{\mathrm{LP\_C}_j},\mathrm{LP\_ID}\}$。其中，押金用来防止 LP_C$_j$ 不按规定时间完成任务，当 LP_C$_j$ 未被选择或按规定完成任务后将退还全部押金。

Step3　ES 对接收到 LP_Req 与 $\mathrm{Mes}^{\mathrm{LP\_C}_j\to\mathrm{ES}}$ 进行验证。首先，提取两条消息中的 LP_ID 验证其是否一致，若一致，ES 从 LP_Req 中提取出 Y_R，并生成随机数 N_v 和秘密值 X_v，计算 $Y_v=\alpha^{X_v} \bmod q$，$X=Y_R^{X_v} \bmod q$，可得会话密钥 X。其次，使用 LP_R 的公钥加密 Y_v、N_v，将加密后的信息 $\mathrm{Mes}^{\mathrm{ES}\to\mathrm{LP\_R}}=E_{\mathrm{pk}_{\mathrm{LP\_R}}}(Y_v\|N_v)$ 发送给 LP_R。

4.4 位置证明协作者选择阶段

若接受位置证明任务的用户数量满足预设定阈值 A_1，ES 将根据 LP_List 挑选 A 个合法的 LP_C$_j$；否则，终止协议。

ES 以 LP_R 位置为圆心、$d_{\max}$ 为半径划分多个区域。首先，根据信任模型在各个区域选择信誉值高的 LP_C$_j$ 为 LP_R 生成 LP；然后，ES 为该任务设置时间阈值 (t,T) 并发送给被挑选的 LP_C$_j$，其中，t 和 T 将 LP_C$_j$ 完成该任务的时间分成三段。如果完成时间大于 T，则拒绝支付奖励，并扣除一半押金 $c_{\mathrm{LP\_C}_j}$；如果完成时间小于 t，根据 LP_C$_j$ 完成任务的时间 $t_{\mathrm{LP\_C}_j}$ 和信誉值 $\mathrm{Rep}_{\mathrm{LP\_C}_j}$，使用式(1)

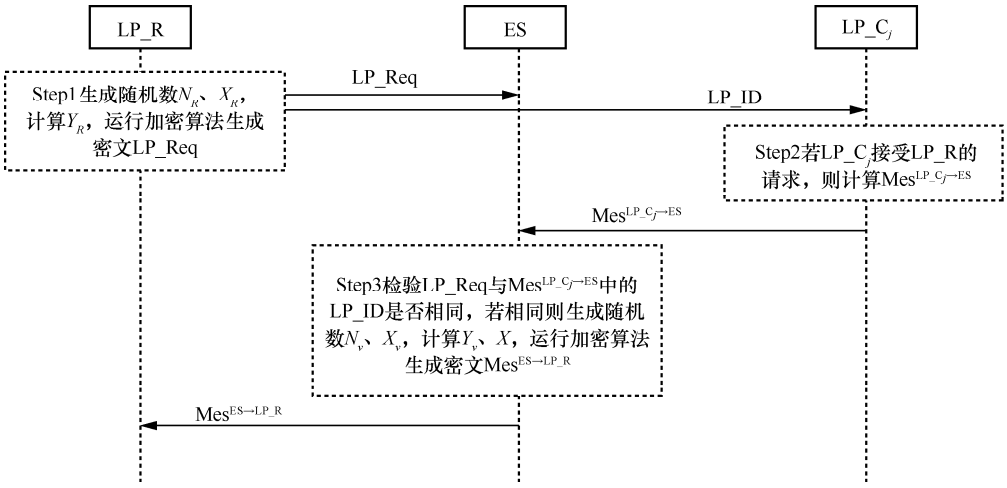


图 2 位置证明初始化流程

计算 LP_C$_j$ 应获得奖励 $\pi_{\mathrm{LP\_C}_j}$，该奖励包括 LP_C$_j$ 的押金；如果完成的时间大于 t 且小于 T，则使用式(2)计算 $\pi_{\mathrm{LP\_C}_j}$。

$$\pi_{\mathrm{LP\_C}_j}=\frac{\mathrm{Rep}_{\mathrm{LP\_C}_j}\mathrm{ps}_{\mathrm{LP\_C}_j}}{\sum_{i=1}^{A}\mathrm{Rep}_{\mathrm{LP\_C}_i}\mathrm{ps}_{\mathrm{LP\_C}_i}}c_R+c_{\mathrm{LP\_C}_j} \tag{1}$$

其中，$\mathrm{ps}_{\mathrm{LP\_C}_j}=\frac{\mathrm{ts}}{t_{\mathrm{LP\_C}_j}-\mathrm{ts}}$，ts 表示 ES 发送时间阈值参数给 LP_C$_j$ 的开始时间，$\mathrm{ps}_{\mathrm{LP\_C}_j}$ 表示根据 LP_C$_j$ 完成任务的时间计算得到的奖励调节因子。当 LP_C$_j$ 越早完成时 $\mathrm{ps}_{\mathrm{LP\_C}_j}$ 越大，即可获得更多 LP_R 提供的奖励 c_R，同时返还其提交的全部 $c_{\mathrm{LP\_C}_j}$。

$$\pi_{\mathrm{LP\_C}_j}=\frac{\mathrm{Rep}_{\mathrm{LP\_C}_j}\mathrm{ps}_{\mathrm{LP\_C}_j}}{\sum_{i=1}^{A}\mathrm{Rep}_{\mathrm{LP\_C}_i}\mathrm{ps}_{\mathrm{LP\_C}_i}}c_R+c_{\mathrm{LP\_C}_j}\frac{T+t-t_{\mathrm{LP\_C}_j}}{T} \tag{2}$$

其中，$\frac{T+t-t_{\mathrm{LP\_C}_j}}{T}$ 是根据 $t_{\mathrm{LP\_C}_j}$ 计算得到的押金调节因子。$t_{\mathrm{LP\_C}_j}$ 越大，押金调节因子越小，LP_C$_j$ 将被扣除更多的 $c_{\mathrm{LP\_C}_j}$。

本文通过提供奖励的方式来激励用户参与位置证明协作任务，并基于信誉值和完成任务的时间计算奖励值，提高用户完成任务的效率。

4.5 位置证明生成阶段

在该阶段，被 ES 挑选的 A 个合法 LP_C$_j$ 与 LP_R 执行安全高效的位置验证协议，流程如图 3 所示，具体步骤如下。

Step1 LP_R 解密消息 Mes$^{\mathrm{ES}\to\mathrm{LP_R}}$ 提取出 Y_v，计算会话密钥 $X=Y_v^{X_R} \bmod q$ 和长度为 $2n$ bit 的随机数 $a\|b=f(X\|\mathrm{ID}_{\mathrm{LP\_R}}\|N_v\|N_R)$，其中 a 与 b 长度为 n bit，通过短距离通信接口广播 LP_ID。

Step2 LP_C$_j$ 对接收到 LP_ID 进行验证，如果与位置证明初始化阶段收到的相同，则选择 n bit 随机数 h 送给 LP_R。

Step3 LP_R 收到 h 后，首先，根据 LP_C$_j$ 发送消息的顺序计算 $z_j=a_j\oplus h$，其中，$a_1\|b_1=H_0(a,b)$，$a_j\|b_j=H_0(a_{j-1},b_{j-1})$，$z_j$、$a_j$ 与 b_j 都表示 n bit 随机数；然后，计算 $y_j=X\oplus H_1(a_j,b_j)$；最后，发送 y_j 给 LP_C$_j$。

Step4 LP_C$_j$ 接收到 y_j 后，开始与 LP_R 执行 DB 协议，具体步骤如下。

1) LP_C$_j$ 向 LP_R 发起质询挑战，生成一个随机比特位 c_i，将 c_i 发送给 LP_R 的同时开始计时 Δt_i。

2) LP_R 接收到 c_i 后，立即计算响应值 $r_i=z_{ji}c_i+b_{ji}\overline{c_i}$，发送 r_i 给 LP_C$_j$。其中，z_{ji}、a_{ji}、b_{ji} 分别表示随机数 z_j、a_j、b_j 的第 i 位。

3) LP_C$_j$ 接收到 LP_R 的响应值 c_i 后，立即停止计时，重复步骤 1)～步骤 3) n 轮。

如果 n 轮挑战的时间 Δt_i ($i=1,2,\cdots,n$) 都满足

$\Delta t_i \leqslant \frac{2d_{\max}}{c} + t_0$，LP_C$_j$ 生成位置证明 $\mathrm{LP}_j = E_{\mathrm{pk_{ES}}}(\mathrm{Mes}_1^{\mathrm{LP\_C}_j \to \mathrm{ES}} \| \mathrm{Sign}_{\mathrm{sk}_{\mathrm{LP\_C}_j}}(\mathrm{Mes}_1^{\mathrm{LP\_C}_j \to \mathrm{ES}}))$ 并发送给 LP_R。其中，t_0 表示 LP_R 计算 r_i 的时间开销，$\mathrm{Mes}_1^{\mathrm{LP\_C}_j \to \mathrm{ES}} = r \| c \| h \| y_j \| \mathrm{ID}_{\mathrm{LP\_C}_j} \| \mathrm{Loc}' \| t_{\mathrm{LP\_C}_j}$。否则，LP_C$_j$ 发送 $\mathrm{LP}_j' = E_{\mathrm{pk_{ES}}}(\mathrm{Sign}_{\mathrm{sk}_{\mathrm{LP\_C}_j}}(\mathrm{Mes}_2^{\mathrm{LP\_C}_j \to \mathrm{ES}}) \| \mathrm{Mes}_2^{\mathrm{LP\_C}_j \to \mathrm{ES}})$ 给 LP_R，其中，信息 $\mathrm{Mes}_2^{\mathrm{LP\_C}_j \to \mathrm{ES}} = \mathrm{ID}_{\mathrm{LP\_C}_j} \| \mathrm{false} \| t_{\mathrm{LP\_C}_j}$。

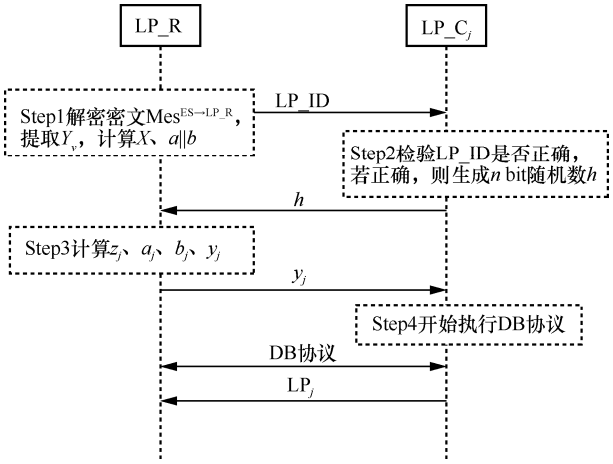


图 3　位置证明生成流程

4.6　位置证明验证阶段

LP_R 使用 ES 的公钥加密数据 $m = \{\mathrm{LP}, X\}$ 得密文 $E_{\mathrm{pk_{ES}}}(m)$，并将其发送给 ES，其中，$\mathrm{LP} = \mathrm{LP}_1 \| \mathrm{LP}_2 \| \mathrm{LP}_3 \| \cdots \| \mathrm{LP}_A$。ES 设定 K 表示接受 LP_R 位置证明通过预定义的阈值，并验证 LP_R 位置的合法性。验证过程具体步骤如下。

Step1　ES 解密 $E_{\mathrm{pk_{ES}}}(m)$ 验证 X 和 A 个位置证明的正确性。

Step2　ES 首先判断 X 是否合法，若合法，则获取 LP$_j$ 中标识 $\mathrm{ID}_{\mathrm{LP\_C}_j}$ 并判断其是否属于被挑选位置证明协作者集合，如果属于，再验证其签名是否正确，若正确则继续执行 Step3；否则，ES 拒绝 LP_C$_j$ 为 LP_R 生成的 LP$_j$。

Step3　ES 获取值 y_j，并根据位置证明初始化阶段生成的随机数 N_v 与 N_R 来计算 a_j' 与 b_j'，判断 $y_j = X \oplus H_1(a_j', b_j')$ 是否成立，如果成立，继续执行 Step4；否则，ES 拒绝 LP_C$_j$ 为 LP_R 生成的 LP$_j$。

Step4　ES 获取 LP$_j$ 中随机数 h 与 c，根据式(3)计算 r_i'，验证 n 轮质询挑战响应值 r_i 是否正确。如果存在 $r_i' \neq r_i\ (i = 1, 2, \cdots, n)$，ES 将拒绝 LP_C$_j$ 为 LP_R 生成的 LP$_j$；否则，继续执行 Step5。

$$r_i' = \begin{cases} a_{ji}' \oplus h_i, & c_i = 1 \\ b_{ji}', & c_i = 0 \end{cases} \tag{3}$$

Step5　ES 验证 $t_{\mathrm{LP\_C}_j}$ 是否小于 T，如果验证通过，合法的位置证明个数 $A_t = A_t + 1$。

重复以上步骤验证 A 个 LP$_j$。如果 $A_t \geqslant K$，ES 验证 LP_R 的位置合法，并将所有位置合法 LP_R 的信息发送给 TR。

4.7　信誉模型

为了抵抗 LP 生成过程中 LP_R 和 LP_C 之间发起的共谋攻击，本文基于 LP_R 和 LP_C 历史位置验证记录来计算其信誉值，并结合信誉值和区域划分的方法来选择 LP_C，具体步骤如下。

Step1　ES 设定位置证明信誉阈值 T_{rep}，根据 LP_C$_j$ 为位置证明请求者 LP_R$_k$ 生成 LP 的历史记录计算信誉值 $\mathrm{Rep}_{\mathrm{LP\_C}_j}$

$$\mathrm{Rep}_{\mathrm{LP\_C}_j}(\mathrm{LP\_C}_j, \mathrm{LP\_R}_k) = \frac{\mathrm{Score}_{\mathrm{LP\_C}_j} U_{\mathrm{LP\_C}_j}}{1 + \mathrm{Sum}(\mathrm{LP\_C}_j, \mathrm{LP\_R}_k)} \tag{4}$$

其中，$\mathrm{Sum}(\mathrm{LP\_C}_j, \mathrm{LP\_R}_k)$ 表示 LP_C$_j$ 与 LP_R$_k$ 协作完成位置证明的总数；$\mathrm{Score}_{\mathrm{LP\_C}_j}$ 表示 ES 对 LP_C$_j$ 过去完成位置证明任务的总评分，由式(5)计算可得；$U_{\mathrm{LP\_C}_j}$ 由式(6)计算可得。

$$\mathrm{Score}_{\mathrm{LP\_C}_j} = g + \sum_{i=1}^{N^*} s\left(2 - \frac{t_{\mathrm{LP\_C}_j}}{T}\right) \tag{5}$$

$$U_{\mathrm{LP\_C}_j} = \sum_{k=1}^{n^*} \frac{N^*}{w_k} \tag{6}$$

其中，g 表示用户在注册成为 LP_C 时的初始分数；s 表示 LP_C$_j$ 按规定时间阈值内完成位置证明任务应获得的分数；$\frac{t_{\mathrm{LP\_C}_j}}{T}$ 表示根据 $t_{\mathrm{LP\_C}_j}$ 计算得到的评分调节因子；N^* 与 n^* 分别表示 LP_C$_j$ 过去执行位置证明任务的总次数和 LP_C$_j$ 过去协助过不同 LP_R 的数量；w_k 表示 LP_C$_j$ 过去完成 LP 总数中与 LP_R$_k$ 协作的比例；$U_{\mathrm{LP\_C}_j}$ 可用来调节 LP_C$_j$ 的 $\mathrm{Score}_{\mathrm{LP\_C}_j}$，进而影响 LP_C$_j$ 的 $\mathrm{Rep}_{\mathrm{LP\_C}_j}$。

由于 LP_R 和 LP_C$_j$ 都是不受信任的实体，

LP_C$_j$ 很可能与 LP_R 共谋为其生成一个虚假的位置证明，如果 LP_C$_j$ 多次协助同一个 LP_R$_k$ 生成位置证明，将会增大它们之间发生共谋的可能性。因此，本文通过检测 LP_C$_j$ 与 LP_R$_k$ 历史位置验证记录来计算 LP_C$_j$ 的 $\mathrm{Rep}_{\mathrm{LP\_C}_j}$，并根据 $\mathrm{Rep}_{\mathrm{LP\_C}_j}$ 的大小选择 LP_C$_j$，目的是使 LP_R$_k$ 的位置证明协作任务不依赖于少部分 LP_C$_j$，提高被挑选 LP_C$_j$ 的多样性来降低共谋的可能性。从式(4)和式(6)可以看出，当一个 LP_C$_j$ 频繁协助某个 LP_R$_k$ 完成位置证明，会影响信誉模型中相关参数的大小（如 Sum（LP_C$_j$, LP_R$_k$）增大、$U_{\mathrm{LP\_C}j}$ 降低），从而使其获得较低的信誉值，在位置证明协作者选择阶段被选中的概率下降，与 LP_R$_k$ 共谋成功的可能性降低。

此外，引入 LP_C$_j$ 完成位置证明协作任务的时间 $t_{\mathrm{LP\_C}_j}$ 来计算其 $\mathrm{Rep}_{\mathrm{LP\_C}_j}$ 和 $\pi_{\mathrm{LP\_C}_j}$，目的是提高 LP_C$_j$ 完成任务的效率。由式(4)和式(5)可以看出，当 $t_{\mathrm{LP\_C}_j}$ 越小时，LP_C$_j$ 获得的 $\mathrm{Score}_{\mathrm{LP\_C}_j}$ 越高，$\mathrm{Rep}_{\mathrm{LP\_C}_j}$ 越大。又由式(1)和式(2)可知，LP_C$_j$ 所获得的 $\pi_{\mathrm{LP\_C}_j}$ 与其 $\mathrm{Rep}_{\mathrm{LP\_C}_j}$ 的大小和 $t_{\mathrm{LP\_C}_j}$ 相关联，当 $\mathrm{Rep}_{\mathrm{LP\_C}_j}$ 越大、$t_{\mathrm{LP\_C}_j}$ 越小时，LP_C$_j$ 获得的 $\pi_{\mathrm{LP\_C}_j}$ 越多。LP_C$_j$ 若想要获得更多的奖励，则会选择高效完成位置证明协作任务。

综上所述，本文将任务完成的时间和历史位置验证记录结合来计算 LP_C 的信誉值，既能抵抗 LP_R 和 LP_C 之间的共谋攻击，又能防止 LP_C 完成任务超时的不良行为。

Step2 首先，ES 以 LP_R$_k$ 所在位置为圆心，将参与位置协作的 LP_C$_j$ 数量 N 平均划分在 M 个区域内，使每个区域内 LP_C$_j$ 数量 N_i 相差不超过 1；其次，计算每个区域内信誉值大于阈值 T_{rep} 的 LP_C$_j$ 的数量 H_i，$H=H_1+H_2+H_3+\cdots+H_M$（$i=1,2,\cdots,M$），根据所需要 LP_C$_j$ 的数量 A 与接受 LP_R 位置证明通过阈值 K 来计算每个区域选择的 LP_C$_j$ 的数量 A_j 与阈值 K_j（$j=1,2,\cdots,M-1$）；最后，根据每个区域信誉值的大小选择 LP_C$_j$。

$$A_j=\left\lfloor\frac{H_jA}{H}\right\rfloor,\quad A_M=A-\sum_{j=1}^{M-1}A_j \tag{7}$$

$$K_j=\left\lfloor\frac{H_jK}{H}\right\rfloor,\quad K_M=K-\sum_{j=1}^{M-1}K_j \tag{8}$$

区域划分的方法使 LP_R 发起共谋时需保证在每个区域内不诚实的 LP_C$_j$ 被 ES 选择，且数量不小于所在区域阈值 K_i。因此，该方法不仅可以进一步抵抗共谋攻击，还可以防止信誉值低但诚实的位置证明协作者一直不被选择，解决了权益集中的问题。具体划分的个数需由 ES 根据 N 的大小来决定，本文仅对 N<30 的情况进行分析。

5 安全性分析

为了在位置验证协议中安全通信，需要保证一些基本安全需求，如用户身份隐私、抗距离欺诈、抗伪造攻击等[29]。同时，协议还需要能抵御各种恶意攻击，如共谋攻击、伪造攻击。

1) 用户身份隐私

整个位置验证协议执行期间，参与用户的身份标识 ID 都是通过 ES 的公钥加密进行通信的，因此，只有 ES 知道它们的真实身份，实现了用户在位置验证过程中的隐私性。

2) 抗距离欺诈

快速的质询挑战可以防止距离欺诈。在本文方案中，根据随机数 N_v、N_R 和会话密钥 X 生成响应值种子 $a\|b$，由该种子生成每一轮响应参数 a_j 与 b_j，随机种子 $a\|b$ 可以确保 $a_j\neq b_j$。如果一个不诚实的 LP_R 挑选 n bit 随机数 $a_j=b_j$，则可以在接受挑战位 c_i 之前发送响应值 $r_i=a_{j_i}=b_{j_i}$，导致响应值 r_i 独立于挑战值 c_i。因此，本文方案可以抵抗距离欺诈。

3) 抗伪造攻击

恶意的 LP_R 不能与非法 LP_C$_j$ 协作执行位置验证协议，伪造虚假的 LP。在本文方案中，位置证明验证阶段 ES 需要验证 LP$_j$ 是否由合法的 LP_C$_j$ 生成。此外，由于每次位置验证需生成会话密钥，ES 在位置证明验证阶段需使用会话密钥去验证 LP$_j$ 中的 y_j 值是否正确。因此，不诚实的 LP_R 试图伪造或使用其他用户的 LP 将不会成功。

4) 抗重放攻击

一个敌手伪造成一名合法的用户请求位置验证，在进行通信的过程中获取为合法 LP_R 生成的 LP，在与 ES 交互过程中重放消息 LP，以此通过位置验证。在本文方案中，即使敌手知道 LP 所属用户的身份标识 $\mathrm{ID}_{\mathrm{LP\_R}}$，也无法创建位置证明验证阶

段生成消息 m 中的会话密钥 X，因为消息 m 使用 ES 的公钥加密，敌手无法获取。因此，本文方案可以抵抗重放攻击。

5) 抗共谋攻击

在本文方案中，存在 3 种共谋攻击。

首先，不诚实 LP_R 与处于合法位置的 LP_R′ 发起共谋攻击。在该攻击中，LP_R′ 与 LP_C$_j$ 成功完成协议的前提是 LP_R′ 必须知道 LP_R 的参数 a、b、N_R 和 y，这意味着 LP_R′ 可以获取 LP_R 与 ES 的会话密钥 X，因此，LP_R′ 能在一段时间内模仿 LP_R。而理性的用户将不会选择接受这种风险，因此，LP_R 与 LP_R′ 之间的共谋将不会成功。

其次，恶意的 LP_C$_j$ 之间通过共谋获取诚实 LP_R 位置验证协议执行过程中生成响应值的参数，伪造 LP_R 的身份参与感知任务获得奖励。在本文协议中，新发起的位置证明请求将需要与 ES 生成新的种子 a、b，因此，不诚实的 LP_C$_j$ 获得的信息 a_j 与 b_j 在下一轮验证过程不能被使用，这种攻击将会失败。

最后，不诚实 LP_R 与 LP_C$_j$ 之间发生共谋生成虚假的 LP，因此，在本文协议中 LP_C$_j$ 的选择是 ES 根据 LP_C$_j$ 的信誉值与所在区域决定的，被不诚实的 LP_R 挑选参与共谋的 LP_C$_j$ 可能在位置证明协作者选择阶段不被 ES 所选择。本文方案在文献[10]的基础上采用了区域划分方法选择 LP_C$_j$，且本文方案 LP_R 与 LP_C$_j$ 之间共谋成功的可能性比文献[10]低。本文对真实环境做出如下假设。

首先，假设不诚实的 LP_R 与位于合法位置区域的 LP_C$_j$ 共谋，其中，A_c 是 LP_R 在合法位置区域内选择共谋的 LP_C$_j$ 的数量，N 是在合法位置范围内接受位置证明请求任务的数量（包括恶意的 LP_C$_j$）；其次，假设 K 是该位置证明请求通过的阈值，其中，A 是 ES 从接受位置证明任务 N 个参与者中挑选的数量，A_x 是 ES 挑选出 A 个参与者中与 LP_R 共谋的数量；最后，ES 以 LP_R 的位置为中心将合法区域划分为两部分，在每个区域挑选 LP_C$_j$，假设每个区域内 LP_C$_j$ 的信誉值满足信誉阈值 T_{rep}，区域 1 接受该任务的协作者数为 $N_1=\left\lfloor\frac{N}{2}\right\rfloor$，区域 2 接受该任务的协作者数为 $N_2=N-N_1$。同样，在区域 1 中选择 A_1 个协作者完成该任务，其中 $A_1=\left\lfloor\frac{A}{2}\right\rfloor$，区域 2 选择 $A_2=A-A_1$。假设在区域 1 恶意的 LP_C$_j$ 数量是 A_{c1}，区域 2 是 A_{c2}，其中 $A_c=A_{c1}+A_{c2}$，区域 1 中位置证明验证通过阈值为 $K_1=\left\lfloor\frac{K}{2}\right\rfloor$，区域 2 为 $K_2=K-K_1$，只有 2 个区域验证通过的位置证明数量都满足阈值，才能通过最终验证。

如果 $A_{c1}<K_1$ 或 $A_{c2}<K_2$，位置区域 1 或区域 2 共谋数量均小于阈值，共谋攻击将失败。

如果 $K_1\leqslant A_{c1}<A_1, K_2\leqslant A_{c2}<A_2$，由式(9)计算可得到共谋成功的可能性。

$$P_{\text{success}}=\prod_{i=1}^{2}P_i(A_{x_i}\geqslant K_i)=$$

$$\prod_{i=1}^{2}\sum_{j=K_i}^{A_{ci}}P_i(A_{x_i}=j)=\prod_{i=1}^{2}\frac{\sum_{j=K_i}^{A_{ci}}\binom{A_{ci}}{j}\binom{N_i-A_{ci}}{A_i-j}}{\binom{N_i}{A_i}} \tag{9}$$

其中，P_i（$i=1,2$）是区域 i 成功的可能性。

如果 $A_{c1}\geqslant A_1, A_{c2}\geqslant A_2$ 且 $K_1=A_1, K_2=A_2$，由式(10)计算可得共谋成功的可能性。

$$P_{\text{success}}=\prod_{i=1}^{2}P_i(A_{x_i}=K_i)=$$

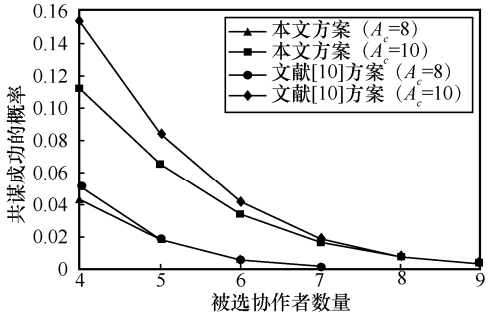
$$\prod_{i=1}^{2}\frac{\binom{A_{ci}}{A_i}}{\binom{N_i}{A_i}}=\frac{A_{ci}!(N_i-A_i)!}{N_i!(A_{ci}-A_i)!} \tag{10}$$

图 4 展示了当 A_c 不同时，随着被选协作者数量 A 的变化，LP_R 与 LP_C$_j$ 共谋成功的概率。从图 4 可以看出，本文方案共谋成功的概率低于文献[10]。因此，本文通过合理划分区域并在每个区域选择合适参数，对于抵抗 LP_R 与 LP_C$_j$ 之间的共谋提供了比文献[10]更可靠的解决方案。

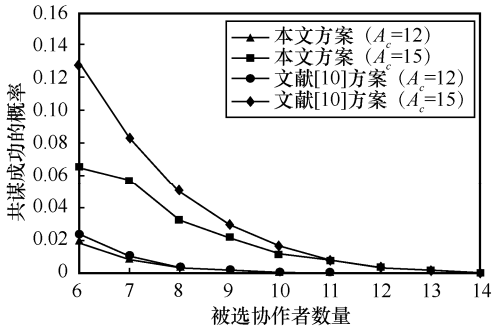
6) 抗远程劫持攻击

对于该类攻击，远离合法区域的敌手 A_0 与 ES 执行位置证明初始化阶段。A_0 想要欺骗诚实的位置证明协作者 C 为其生成 LP，但无法通过短程通信广播位置证明标识给 C。假设 A_0 可以广播信息给 C，并借助诚实的用户 P_0 来完成挑战，然而 P_0 无法获得 A_0 与 ES 生成的随机数种子 $a_{A_0}\|b_{A_0}$ 和密钥 X_{A_0}，因此无法使用正确的数据计算响应值和信息 $y_{A_0}=X_{A_0}\oplus H_1(a_{A_{0j}},b_{A_{0j}})$。如果 P_0 使用自身与 ES

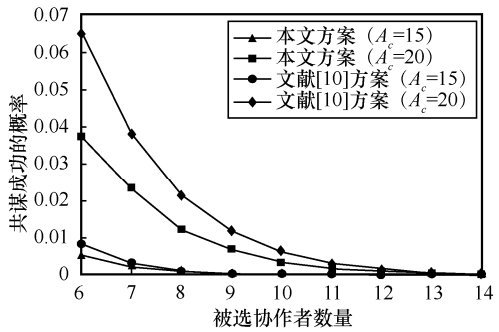
初始化生成的信息执行响应，A_0 劫持 C 为 P_0 生成的 LP 发送给 ES 进行验证，在位置证明验证阶段使用 A_0 与 ES 生成的密钥 X_{A_0} 和种子 $a_{A_0} \| b_{A_0}$ 验证 y_{A_0} 将会失败。因此，本文方案可以抵抗远程劫持攻击。



(a) N=15



(b) N=20



(c) N=30

图 4 不同参数下共谋成功的概率

6 性能分析

本文方案通过借助位置证明协作者来完成位置验证协议，协议在执行过程中需要使用多次加解密运算。因此，本节将从计算开销和通信开销 2 个方面将本文方案与文献[10]、文献[24]、文献[26]和文献[27]等相关方案进行分析比较。

6.1 计算开销分析

现有位置验证方案主要受位置验证过程中加解密影响，因此本文更侧重于通过减少位置证明过程中加解密的次数来提高验证位置真实性的效率。本节在配置为 Intel(R) Core(TM) i5-9500U 3.00 GHz 处理器、RAM 为 8 GB 的 Windows 10 系统，IDEA 2021 编译环境下通过对本文方案、文献[10]、文献[26]和文献[27]这 4 种方案中所涉及的密码学操作进行模拟，并使用 RSA 加密/签名算法、SHA1 哈希运算以及哈希承诺来评估协议时间开销。其中，哈希运算、模运算、对称加密/解密、非对称加密/解密、签名/验签以及承诺值计算是 6 种消耗最大的运算，因此，本节在实验过程中将重点评估以上 6 种计算操作。实验中所有结果均为 50 次结果的平均值。

本文方案与文献[10]、文献[26]、文献[27]在协作者数量为 1，密钥大小为 512 bit、1 024 bit、2 048 bit 时产生的计算开销如图 5 所示。从图 5 可以看出，由于文献[26]借助一个位置证明协作者参与位置验证，验证方案的实体只涉及请求者和协作者，不需要进行多次加解密计算，因此文献[26]计算开销最小，但该方案安全性较低。本文方案在密钥大小为 512 bit 时计算开销大于文献[10]，这是因为本文方案在位置证明初始化阶段需要计算会话密钥，但随着密钥大小的增大，计算开销小于文献[10]和文献[27]，因为文献[10]和文献[27]在位置证明生成与验证阶段执行了大量的加解密与承诺值计算。

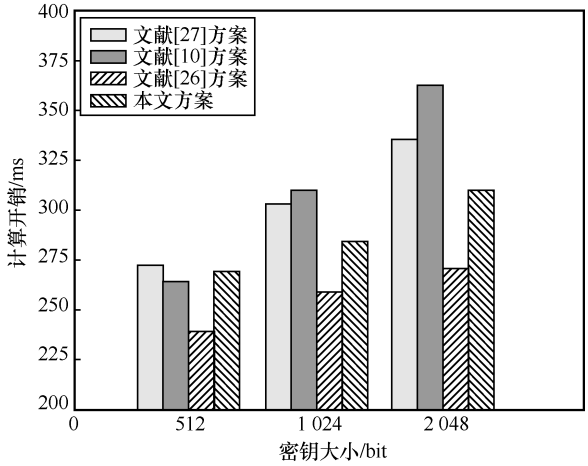
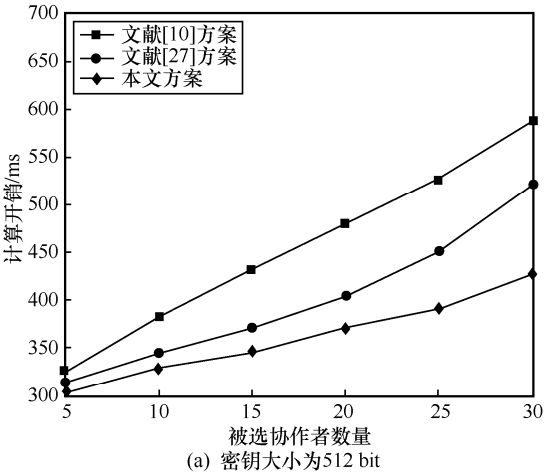


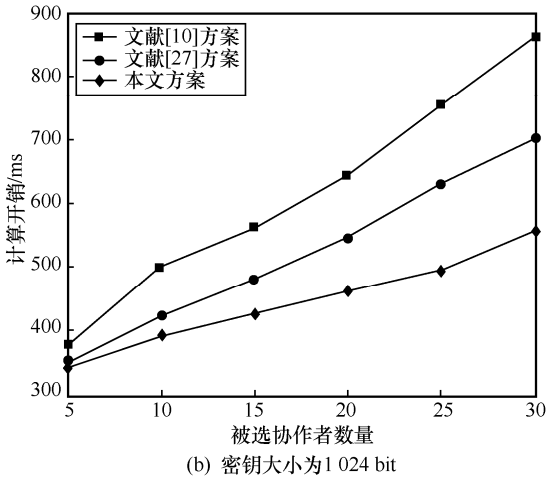
图 5 密钥大小不同时各方案计算开销比较

被选协作者数量不同时各方案计算开销比较如图 6 所示。从图 6(a)可以看出，当密钥大小为 512 bit 时，本文方案、文献[10]与文献[27]方案的计算开销会随被选协作者数量的增加而增大，但本文方案的增长率较小，文献[10]的增长率最大。因为文献[10]在位置证明生成阶段需要对每个协作者发送的签名与消息进行加密运算，在验证阶段也需要

执行对应解密和验签。而文献[27]在位置证明阶段除了需要执行加解密运算，在与协作者交互阶段还需要计算大量的承诺值，因此其消耗的时间大于本文方案。从图 6(b)可以看出，当密钥大小为 1 024 bit 时，本文方案与文献[10]、文献[27]方案随着被选协作者数量增加时计算开销差距将越来越明显。因此，本文方案使用一对随机数多次哈希获取新信息的思想来设计位置验证协议能对降低位置验证过程中的计算开销起到明显的效果。



(a) 密钥大小为512 bit



(b) 密钥大小为1 024 bit

图 6　被选协作者数量不同时各方案计算开销比较

6.2　通信开销分析

本节将通过分析文献[10]、文献[24]、文献[27]与本文方案中消息数量和传输消息的位数等参数来评估各方案的通信开销。文献[10]在位置证明初始化阶段需发送的消息分别是{Req}和{LP_ID}，在位置证明生成和验证阶段需发送消息分别为{LP_ID}、$\{h,c,r\}$、$\{E_{\text{Verifier}}(m_1 \| S_{\text{prover}}(m_1))\}$、$\{E_{\text{Verifier}}(m_2 \| S_{\text{Witness}}(m_2)\}$和$\{E_{\text{Verifier}}(\text{LP}_1 \| \text{LP}_2 \| \cdots \| \text{LP}_K \| a \| b\}$。文献[24]在位置证明生成与验证阶段需发送的消息分别为$\text{PReq}=\{C(\text{ID}_\text{P},r_p) \| L_1 \| t\}$、$\{\text{EP}_j,c,r\}$、$\text{STPC}=\{\text{EP}_1 \| \text{EP}_2 \| \cdots \| \text{EP}_A \| r_{w,1}^x \| \cdots \| r_{w,A}^x \| \text{ID}_\text{P} \| L_x \| t\}$、$\text{VReq}=\{\text{EP}_1 \| \text{EP}_2 \| \cdots \| \text{EP}_A \| \text{ID}_\text{P} \| r_p\}$、$E^{K_{\text{CA}}^-}(\cdot)$。文献[27]在位置证明生成和验证阶段需发送消息分别为$\text{PR}=\{C(\text{P},r_p) \| L_0 \| K_0 \| t_1 \| \text{CA}\}$、$\text{WP}=\{C(W_i,r_{w_i}) \| n_i\}$、$\text{hsStart}=\{\text{Start} \| \text{hS}_{\text{kp}}(\text{Start})\}$、$\text{hsC}_i=\{C_i \| \text{hS}_{\text{kw}_i}(C_i)\}$、$\text{hsR}_i=\{R_i \| \text{hS}_{\text{kp}}(R_i)\}$、$\text{hsVH}=\{\text{VH} \| \text{hS}_{\text{kp}}(\text{VH})\}$、$\text{eLPS}_i=\{c(W_i,r_{w_i}) \| E_{\text{KCA}}(\text{LPS}_i)\}$、$\text{eLIST}_i=\{C(W_i,r_{w_i}) \| E_{\text{KCA}}(\text{LIST}_i \| S_{\text{kw}_i}(\text{LIST}_i))\}$、$e\text{LPA}=\{c(P_i,r_p) \| E_{\text{KCA}}(\text{LPA} \| S_{\text{kp}}(\text{LPA}))\}$、$\text{eVS}=\{\text{CA} \| E_{\text{kCA}}(\text{VS}) \| S_{\text{kCA}}(\text{VS})\}$、$\{E_{\text{KV}}(\text{LP} \| S_{\text{kp}}(\text{LP}))\}$。本文方案在位置证明初始化阶段需要发送的消息分别为{LP_Req}、{LP_ID}、$\text{Mes}^{\text{LP_C}_j \to \text{ES}}=\{c_{\text{LP_C}_j},\text{LP_ID}\}$和$\text{Mes}^{\text{ES}\to\text{LP_R}}=E_{\text{pk}_{\text{LP_R}}}$。在位置证明生成和验证阶段需要发送消息分别为{LP_ID}、$\{h,y_i,c,r\}$、$\text{LP}_j=E_{\text{pk}_{\text{ES}}}(\text{Mes}_1^{\text{LP_C}_j\to\text{ES}} \| \text{Sign}_{\text{sk}_{\text{LP_C}_j}}(\text{Mes}_1^{\text{LP_C}_j\to\text{ES}}))$和$\{E_{\text{pk}_{\text{ES}}}(LP,X)\}$。

本文参考文献[30]通信开销的分析方法，仅考虑通信过程加解密值、承诺值、签名以及哈希值等传输位数较大的消息，并使用$|E|$、$|C|$、$|H|$和$|S|$分别表示非对称加密值、承诺值、哈希值和签名值的长度。本文方案在位置证明初始化阶段需发送 2 条非对称加密消息、位置证明生成阶段需发送 1 条非对称加密消息、位置证明验证阶段需发送 1 条非对称加密消息。由于位置证明生成阶段发送的消息数量与参与位置证明协作者的数量 A 相关，因此本文方案总的通信开销为$(A+3)|E|$，其他方案也采用相同的分析方法。表 2 是本文方案与文献[10]、文献[24]、文献[27]的通信开销对比。

表 2　　**各方案通信开销对比**

方案	通信开销/B
文献[27]	$(8A+1)\|C\|+(2A+3)\|E\|+\|S\|+6A\|H\|$
文献[24]	$3A\|E\|+A\|C\|+\|S\|$
文献[10]	$(2A+2)\|E\|$
本文方案	$(A+3)\|E\|$

本文基于一些假设值和 A 动态变化来比较各方案的通信开销，假设$|E|$和$|S|$的大小为 128 B，$|C|$和$|H|$的大小为 20 B，各方案通信开销比较如图 7

所示。从图 7 可以看出，尽管文献[10]方案交换的消息数量比本文方案少，但总的通信开销随着 A 的增加远比本文方案高，因为该方案与 A 个 LP_C_j 交互过程中使用的非对称加密运算次数远高于本文方案。文献[27]与文献[24]方案不仅非对称加密运算次数高于文献[10]与本文方案，发送的消息中还存在大量的承诺值与哈希值。因此，本文方案相较于相关方案有更低的通信开销。

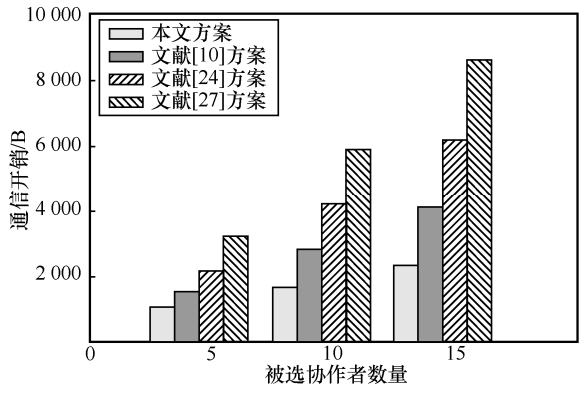


图 7 各方案通信开销比较

7 结束语

本文重点关注群智感知应用中任务参与者位置真实性和隐私性的问题，设计了一种安全且高效的基于协作的位置认证方案。该方案在位置验证协议中利用同一对随机数多次碰撞获取新信息的方法，有效解决了恐怖主义欺诈，保证了位置的不可伪造，减少了位置证明参与者执行该协议时的计算开销，并基于各方完全信任的实体 ES 收集位置证明参与者的信息，保护了位置证明参与者的位置隐私。此外，为了提高位置证明协作者完成任务的积极性与效率，提出了基于信誉的激励机制和交付押金的策略；为了解决位置证明请求者和协作者共谋问题，提出了基于信誉值与区域划分的方法选择位置证明协作者；为了提高基于信誉模型的可靠性，将位置证明协作者历史完成任务的记录与完成任务评分有效结合。最后，仿真结果表明，本文方案相较于现有方案具有更好的安全性和效率。

参考文献：

[1] WANG D X, HUANG C H, SHEN X Y, et al. A general location-authentication based secure participant recruitment scheme for vehicular crowdsensing[J]. Computer Networks, 2020, 171: 107152.

[2] MAISONNEUVE N, STEVENS M, NIESSEN M E, et al. NoiseTube: measuring and mapping noise pollution with mobile phones[C]//Information Technologies in Environmental Engineering. Berlin: Springer, 2009: 215-228.

[3] CAI J L Z, YAN M Y, LI Y S. Using crowdsourced data in location-based social networks to explore influence maximization[C]//Proceedings of the 35th Annual IEEE International Conference on Computer Communications. Piscataway: IEEE Press, 2016: 1-9.

[4] ASUQUO P, CRUICKSHANK H, MORLEY J, et al. Security and privacy in location-based services for vehicular and mobile communications: an overview, challenges, and countermeasures[J]. IEEE Internet of Things Journal, 2018, 5(6): 4778-4802.

[5] GUPTA R, RAO U P. An exploration to location based service and its privacy preserving techniques: a survey[J]. Wireless Personal Communications, 2017, 96(2): 1973-2007.

[6] CHERIAN J, LUO J, GUO H L, et al. ParkGauge: gauging the occupancy of parking garages with crowdsensed parking characteristics[C]//Proceedings of 2016 17th IEEE International Conference on Mobile Data Management. Piscataway: IEEE Press, 2016: 92-101.

[7] GONG W, ZHANG B X, LI C. Location-based online task assignment and path planning for mobile crowdsensing[J]. IEEE Transactions on Vehicular Technology, 2019, 68(2): 1772-1783.

[8] HE W B, LIU X, REN M. Location cheating: a security challenge to location-based social network services[C]//Proceedings of 2011 31st International Conference on Distributed Computing Systems. Piscataway: IEEE Press, 2011: 740-749.

[9] CHEN Y L, WANG X J, YANG Y L, et al. Location-aware Wi-Fi authentication scheme using smart contract[J]. Sensors, 2020, 20(4): 1062.

[10] NOSOUHI M R, SOOD K, YU S, et al. PASPORT: a secure and private location proof generation and verification framework[J]. IEEE Transactions on Computational Social Systems, 2020, 7(2): 293-307.

[11] ZHU Z C, CAO G H. APPLAUS: a privacy-preserving location proof updating system for location-based services[C]//Proceedings of IEEE INFOCOM. Piscataway: IEEE Press, 2011: 1889-1897.

[12] MITROKOTSA A, PERIS-LOPEZ P, DIMITRAKAKIS C, et al. On selecting the nonce length in distance-bounding protocols[J]. The Computer Journal, 2013, 56(10): 1216-1227.

[13] XU G W, LI H W, TAN C, et al. Achieving efficient and privacy-preserving truth discovery in crowd sensing systems[J]. Computers & Security, 2017, 69: 114-126.

[14] ZHANG R, ZHANG J X, ZHANG Y C, et al. Secure crowdsourcing-based cooperative pectrum sensing[C]//Proceedings of IEEE INFOCOM. Piscataway: IEEE Press, 2013: 2526-2534.

[15] PENG D, WU F, CHEN G H. Pay as how well you do: a quality based incentive mechanism for crowdsensing[C]//Proceedings of the 16th ACM International Symposium on Mobile Ad Hoc Networking and Computing. New York: ACM Press, 2015: 177-186.

[16] XIAO M J, AN B Y, WANG J, et al. CMAB-based reverse auction for unknown worker recruitment in mobile crowdsensing[J]. IEEE Transactions on Mobile Computing, 2021, 21(10): 3502-3518.

[17] WU X C, SUN Y E, DU Y, et al. An anti-malicious task allocation mechanism in crowdsensing systems[J]. Future Generation Computer

Systems, 2022, 127: 347-361.

[18] TALASILA M, CURTMOLA R, BORCEA C. Mobile crowd sensing[M]. Boca Raton: CRC Press, 2015.

[19] REDDY S, ESTRIN D, SRIVASTAVA M. Recruitment framework for participatory sensing data collections[C]//International Conference on Pervasive Computing. Berlin: Springer, 2010: 138-155.

[20] HE Z J, CAO J N, LIU X F. High quality participant recruitment in vehicle-based crowdsourcing using predictable mobility[C]//Proceedings of 2015 IEEE Conference on Computer Communications. Piscataway: IEEE Press, 2015: 2542-2550.

[21] CHANDRAN N, GOYAL V, MORIARTY R, et al. Position based cryptography[C]//Annual International Cryptology Conference. Berlin: Springer, 2009: 391-407.

[22] YANG R P, XU Q L, AU M H, et al. Position based cryptography with location privacy: a step for fog computing[J]. Future Generation Computer Systems, 2018, 78: 799-806.

[23] BRANDS S, CHAUM D. Distance-bounding protocols[C]//Workshop on the Theory and Application of of Cryptographic Techniques. Berlin: Springer, 1993: 344-359.

[24] WANG X L, PANDE A, ZHU J D, et al. STAMP: enabling privacy-preserving location proofs for mobile users[J]. IEEE/ACM Transactions on Networking, 2016, 24(6): 3276-3289.

[25] ZHU Z C, CAO G H. Toward privacy preserving and collusion resistance in a location proof updating system[J]. IEEE Transactions on Mobile Computing, 2013, 12(1): 51-64.

[26] LIU S S, YAN Z, KANTOLA R. Privacy-preserving D2D cooperative location verification[C]//Proceedings of 2021 IEEE Global Communications Conference. Piscataway: IEEE Press, 2021: 1-6.

[27] KOUNAS D, VOUTYRAS O, PALAIOKRASSAS G, et al. QuietPlace: an ultrasound-based proof of location protocol with strong identities[J]. Applied System Innovation, 2020, 3(2): 19.

[28] GAMBS S, KILLIJIAN M O, ROY M, et al. PROPS: a PRivacy-preserving location proof system[C]//Proceedings of 2014 IEEE 33rd International Symposium on Reliable Distributed Systems. Piscataway: IEEE Press, 2014: 1-10.

[29] DESMEDT Y. Major security problems with the ‘unforgeable’(feige)-fiat-shamir proofs of identity and how to overcome them[C]//Proceedings of SECURICOM. [S.l.:s.n.], 1988: 15-17.

[30] BAGGA P, DAS A K, WAZID M, et al. On the design of mutual authentication and key agreement protocol in Internet of vehicles-enabled intelligent transportation system[J]. IEEE Transactions on Vehicular Technology, 2021, 70(2): 1736-1751.

[作者简介]

田有亮（1982– ），男，贵州六盘水人，博士，贵州大学教授、博士生导师，主要研究方向为算法博弈论、密码学与安全协议、大数据安全与隐私保护、区块链与电子货币等。

田茂清（1996– ），女，贵州册亨人，贵州大学硕士生，主要研究方向为位置密码学、隐私保护技术等。

高鸿峰（1975– ），男，贵州遵义人，贵州大学副教授、硕士生导师，主要研究方向为网络与信息安全。

何淼（1988– ），男，四川成都人，女王大学博士生，主要研究方向为信号处理、应用密码学和信息安全等。

熊金波（1981– ），男，湖南益阳人，博士，福建师范大学教授、博士生导师，主要研究方向为安全深度学习、移动群智感知、隐私保护技术等。