

T/CAICI

中国通信企业协会团体标准

T/CAICI XXXX—XXXX

基于移动网络室内定位的隐私保护方法

Privacy Protection Methods for Indoor Localization Based on Mobile Networks

（征求意见稿）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX – XX – XX 发布

XXXX – XX – XX 实施

中国通信企业协会 发布

目 次

前 言 II

引 言 III

1 范围 4

2 规范性引用文件 4

3 术语和定义 4

4 隐私保护原则 5

5 室内定位的隐私保护方案性能指标 5

6 四种室内定位架构分类 6

7 分布式架构的隐私保护方法 8

8 协作式架构的隐私保护方法 8

9 集中式架构的隐私保护方法 9

10 云定位的隐私保护方法 11

11 实施要求 11

12 隐私保护的附加实施要求 12

附 录 A 13

前 言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本文件由中国通信企业协会标准化管理委员会提出并归口。

本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件起草单位：中国移动通信集团设计院有限公司、中国移动通信集团云南有限公司、中国移动通信集团终端有限公司、北京万相信息技术有限公司

本文件主要起草人：王谦、张金柱、徐金鹏、李子君、梁杨、姜书敏、梅红、夏雪玲、程凯、商俊、吴丽雯、陈露、高超云、孙磊、李德海，杨玉佳，王吉钊、朱嘉鲁，宋艳楷

本文件为中国通信企业协会首次发布。

引 言

随着智能手机的普及与室内定位技术的快速发展,用户对精准室内定位服务的需求显著增加。然而,随着室内定位服务的广泛应用,隐私安全问题也愈发突出。特别是第三方定位服务提供商所提供的服务,存在用户隐私信息泄露的潜在风险。因此,制定室内定位隐私保护的团体标准成为保障用户隐私的必要措施。

室内定位服务通常依赖定位服务商提供的基础设施和数据支持。用户通过智能手机的传感器收集位置信息,并通过信息交互和计算实现定位服务。在这一过程中,用户的位置信息和移动轨迹可能存在泄露风险,尤其是在未经适当保护的情况下,这对用户隐私构成潜在威胁。

本团体标准旨在总结当前室内定位隐私保护领域的研究进展,提供一致的技术规范和最佳实践,确保用户隐私信息在定位服务中得到充分保护。通过分析不同系统架构及其潜在威胁模型,梳理隐私保护需求,并比较各种技术方案的性能及优缺点,本标准为室内定位系统的隐私保护提供全面的指导。

本文件的发布机构提请注意,声明符合本文件时,可能涉及到相关的专利的使用。

本文件的发布机构不承担识别专利的责任。

本文件的发布机构对于该专利的真实性、有效性和范围无任何立场。

基于移动网络室内定位的隐私保护方法

1 范围

本标准规定了集中式架构、分布式架构、协作式架构和基于云的室内定位系统中的隐私保护要求和技术方法。本标准适用于各类室内定位系统及其服务提供方，旨在确保在不同架构下的用户隐私信息得到有效保护。

各类架构需满足本标准中规定的隐私保护要求，集中式架构需确保定位资源集中管理的隐私保护，分布式架构需防止节点与用户之间的隐私泄露，协作式架构需保护设备间信息交互的隐私，云架构下需确保云端托管的定位数据和用户信息的隐私保护。

本标准适用于所有提供基于移动网络室内定位服务的系统和平台。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

YD/T 4690-2024《隐私计算 多方安全计算产品安全要求和测试方法》

YD/T 4581-2023《隐私保护场景下安全多方计算技术指南》

YD/T 4361-2023《室内定位系统测试方法》

3 术语和定义

下列术语和定义适用于本文件。

3.1 同态加密技术

1) 同态加密 (Homomorphic Encryption, HE) :

是指一种允许在密文上进行计算，并在解密后得到与在明文上计算相同结果的加密技术。

$$Enc(f(m_1, m_2)) = f(Enc(m_1), Enc(m_2))$$

其中， m_1 和 m_2 表示任意明文信息， f 表示任意计算过程。

2) 部分同态加密 (Partially Homomorphic Encryption) :

是指仅支持密文域中单一运算（如加法或乘法）的同态加密技术。

示例：ElGamal 加密方案支持乘法运算。

3) 全同态加密 (Fully Homomorphic Encryption) :

是指支持在密文上进行加法和乘法运算的同态加密技术。这种技术能够在增强隐私保护的同时，增加计算和通信开销。

3.2 安全多方计算技术

1) 安全多方计算 (Secure Multiparty Computation, SMC) :

是指允许多个参与者在泄露各自私密输入的情况下进行联合计算，并获取计算结果的密码学技术。

2) 混淆电路 (Garbled Circuit, GC) :

是指通过将计算功能转换为布尔电路，并使用加密和扰动技术隐藏输入与输出之间关系的技术。

3) 不经意传输 (Oblivious Transfer, OT) :

是指一种密码学协议，发送者向接收者发送多条消息，而接收者只能接收其中一条，且发送者无法得知接收者选择了哪条消息。

3.3 差分隐私技术

- 1) 差分隐私 (Differential Privacy, DP) :
是指通过向数据添加噪声, 以防止通过分析数据集推断个别参与者私密信息的隐私保护技术。
- 2) 隐私预算 (Privacy Budget) :
是指用于控制差分隐私强度的参数, 通常以 ϵ 表示。
- 3) Laplace 机制:
是指根据拉普拉斯分布向查询结果添加噪声的技术, 用于平衡数据隐私与可用性。
- 4) 指数机制:
是指通过指数分布向非数值型查询结果添加噪声的技术, 用于保护隐私。

3.4 信息隐藏技术

- 1) 信息隐藏技术:
是指通过向数据中添加噪声以隐藏原始信息的技术, 旨在保护数据隐私。
- 2) 零和噪声机制 (Zero-Sum Noise Mechanism) :
是指通过向数据添加噪声, 并确保噪声之和为零, 从而不影响数据计算结果准确性的技术。
- 3) 随机化技术:
是指通过向数据添加随机噪声来混淆数据并保护隐私的技术, 但可能会降低数据的准确性。

4 隐私保护原则

在设计和运营室内定位系统时, 必须遵循以下隐私保护原则:

4.1 最小化数据收集原则

只允许收集系统运行所需的最少数据。应仅记录与定位相关的测量数据 (如 Wi-Fi 信号强度、BLE 信标数据), 避免收集个人身份信息 (如姓名、电话号码等)。

4.2 数据匿名化和伪装原则

必须对收集的数据进行匿名化处理, 去除可能识别用户身份的信息。应采用数据伪装技术, 如添加噪声或数据扰乱, 确保个人数据无法被还原或识别。

4.3 透明度和可控性原则

必须向用户提供清晰的隐私政策和用户协议, 解释数据的收集和处理方式。用户应有权选择是否共享位置信息, 并能够控制数据的访问和修改权限, 系统设计中应具备支持隐私设置的技术能力。

4.4 安全保障原则

必须采用加密算法 (如 AES、RSA) 确保用户数据在传输和存储过程中的安全。应实施访问控制措施, 采用身份验证和授权机制, 限制对敏感数据的访问权限, 确保仅授权人员可以访问。

4.5 服务质量与隐私权衡原则

在保护用户隐私的同时, 应保持系统的定位精度和服务质量。应通过优化定位算法和降低数据处理延迟, 尽量减少隐私保护对系统性能和用户体验的影响。

4.6 合规性与法律要求原则

系统设计和运营必须符合当地法律法规及隐私标准, 确保遵守数据保护法和用户隐私权法律。应定期审查隐私政策和系统设计, 确保其与最新的法律法规保持一致。

5 室内定位的隐私保护方案性能指标

(Privacy Protection for Indoor Localization, PPIL)方案性能指标：指在实现隐私信息保护的同时，室内定位的场景要求方案具有较高的效率和精度，因此通常适用于以下几个性能指标：

5.1 隐私保护度

隐私保护度是指根据不同定位系统架构下的威胁模型，评估方案对隐私信息的保护能力。本标准定义了以下隐私保护等级：

- Level-I：保护用户的测量信息和定位结果，可能泄露定位服务商的数据库信息。
- Level-II：保护用户的测量信息、定位结果和数据库信息，但要求在可信的服务器上运行。
- Level-III：在不可信的服务器上，保护用户的测量信息、定位结果及定位服务商的数据库信息。

5.2 定位精度

定位精度是衡量隐私保护方案对系统服务质量影响的指标。本标准评估方案对定位精度的影响，确保隐私保护不会显著降低定位准确性。定位精度计算公式为：

$$e = \sqrt{\frac{\sum_{i=1}^N \|\hat{X}^{(i)} - X^{(i)}\|^2}{N}}$$

其中， $\hat{X}^{(i)}$ 表示第*i*次的定位结果， $X^{(i)}$ 表示用户当次的真实位置，N 表示定位测试的次数。本标准以原始算法的精度为基准，评估隐私保护方案的影响。

5.3 方案开销

方案开销是指实施隐私保护技术时引入的额外代价，包括存储、计算和通信开销。本标准评估各隐私保护方案的开销，确保在满足隐私保护要求的同时，尽量降低系统的资源消耗。

6 四种室内定位架构分类

6.1 集中式架构：

集中式架构是指定位资源信息集中部署在定位服务商的服务器上，用户通过与服务器交互实现定位。该架构的隐私保护要求包括：

- 保护用户的测量信息和定位结果，防止泄露给未授权方。
- 防止恶意用户通过分析攻击数据库资源，确保系统安全。

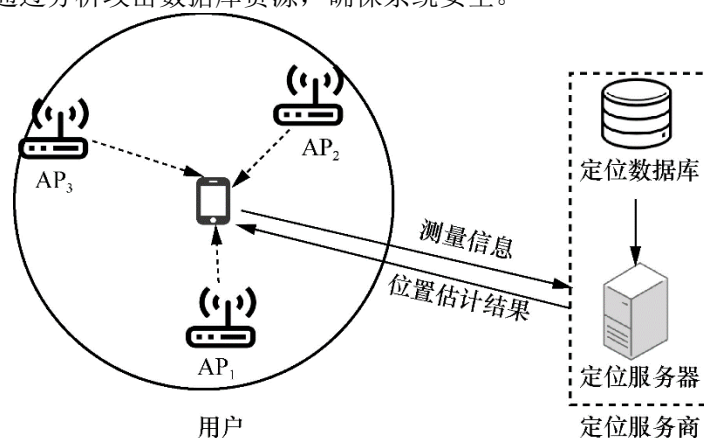


图1 集中式室内定位系统架构

6.2 分布式架构：

分布式架构是指定位资源信息分布在多个定位基础设施（如锚点）中，用户通过与锚点交互实现定位。该架构的隐私保护要求包括：

- 保护用户和锚点双方的隐私信息，防止交互过程中泄露位置数据。
- 防止恶意用户和锚点对彼此隐私信息的攻击。

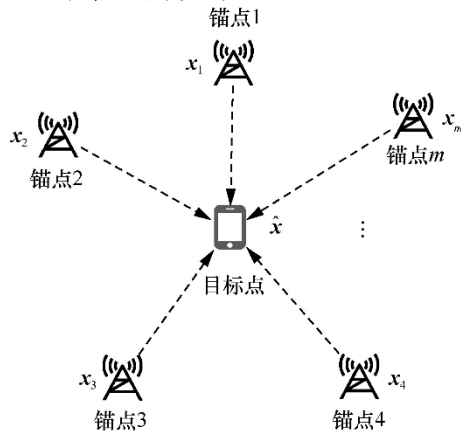


图 2 分布式室内定位系统架构

6.3 协作式架构：

协作式架构是指设备间通过直接或间接通信完成定位任务。该架构的隐私保护要求包括：

- 保护设备之间的信息交互，防止位置信息泄露给未经授权的用户。
- 确保协作过程中设备间通信的安全性。

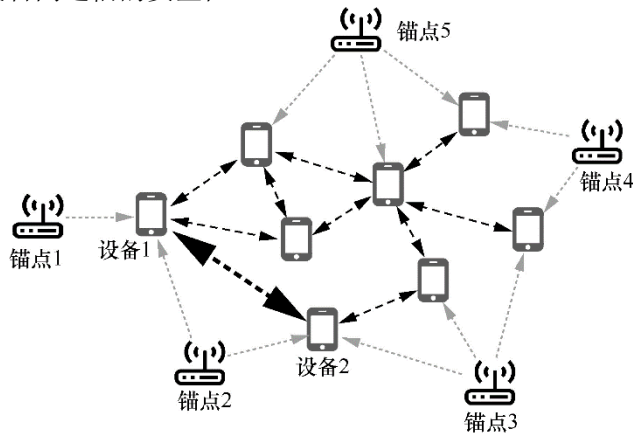


图 3 协作式室内定位系统架构

6.4 基于云的架构：

基于云的架构是指定位服务资源和算法外包给云服务提供商，用户通过云端实现定位。该架构的隐私保护要求包括：

- 保护用户、定位服务商和云服务提供商的隐私信息，防止互不信任的各方泄露数据。
- 确保定位数据和算法在云端运行时的隐私保护。

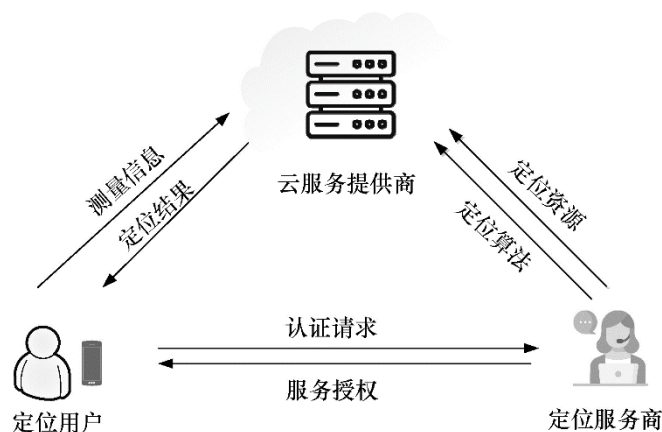


图 4 基于云的室内定位系统架构

7 分布式架构的隐私保护方法

本标准规定了分布式架构下的室内定位隐私保护方法，采用信息隐藏、同态加密和安全多方计算技术，确保在定位过程中保护用户隐私信息，同时保持定位的精度与可靠性。本标准要求至少满足 Level-II 隐私保护等级。

7.1 基于信息隐藏的隐私保护方案

- 1. 基于零和噪声的隐私保护方案：通过在计算过程中加入零和噪声，保护用户的测量信息和锚点位置信息，噪声在计算过程中抵消，不影响定位精度。
- 2. 基于隐私保护的 TDoA 近邻相减方案：该方案针对到达时间差（TDoA）定位场景，将最小二乘估计过程分解为向量或矩阵求和，并在每个求和项中添加可抵消的噪声，实现信息隐藏，同时确保不影响定位精度。
- 3. 基于近邻差分求和的隐私保护方案：通过隐私保护的近邻乘积求和（PPPS）和近邻差分求和（PPDS）技术，保护锚点位置和目标点测量信息，并在最小二乘法计算过程中实现隐私保护。
- 4. 基于 DILOC 的隐私保护定位方案：在分布式定位算法（DILOC）中，通过信息隐藏协议保护用户位置。用户利用锚点坐标和测量数据进行迭代更新，噪声在计算过程中抵消，保证定位精度，同时保护锚点位置和测量信息。

7.2 基于同态加密和安全多方计算的隐私保护方案

- 1. 基于 Paillier 加密的隐私保护方案：采用 Paillier 加密算法对目标点的距离测量值加密，锚点在加密距离值和明文坐标上执行同态计算，目标点解密后获取定位结果。该方案提供 Level-III 安全性，抵御共谋锚点攻击。
- 2. 基于多边形描述的最小二乘估计方案：将用户位置的测距定位圆描述为多边形，避免计算过程中对敏感信息的乘法运算，减少加密操作数量，利用部分同态加密算法提高性能。
- 3. 基于混淆电路的三角定位隐私保护方案：该方案通过混淆电路（GC）保护车辆位置信息，在三角定位场景中，通过车辆之间的两两圆交点计算，保护所有参与车辆的位置隐私。

8 协作式架构的隐私保护方法

本标准规定了协作式架构下的隐私保护方案，重点在于保护用户匿名性，防止测量信息、位置信息或定位结果与特定用户身份的关联。通过匿名属性凭证和数据库匹配方案，确保参与者隐私得到有效保护。本标准要求至少满足 Level-I 隐私保护等级。

8.1 基于匿名属性凭证的隐私保护方案

在该方案中，每个用户拥有身份凭证，并通过蓝牙广播位置信息及凭证证明信息。用户验证其他用户的凭证后，利用位置信息辅助定位。通过零知识证明生成和验证凭证，确保用户无需知晓信息源身份即可验证其合法性，并保护位置信息与身份的匿名性。

8.2 基于数据库匹配的匿名定位方案

该方案基于数据库匹配定位算法，用户设备通过洋葱路由（ToR）协议转发定位请求，并将结果返回至请求者。通过匿名域的构建，确保位置提供者和定位请求者身份不被泄露。

9 集中式架构的隐私保护方法

本标准规定了在集中式架构下应用的室内定位隐私保护方法，包括同态加密和安全多方计算、差分隐私、k 匿名等技术，确保用户数据的隐私保护和定位结果的安全性。本标准至少满足 Level-II 隐私保护等级。

9.1 基于同态加密和安全多方计算的隐私保护方案

1. 基于 ElGamal 加密的欧氏距离隐私保护方案：

本方案采用 ElGamal 加密算法对测量值进行加密处理，定位服务器在密文上同态计算欧氏距离，用户解密获取距离，并进行比较和排序。此方法通过网格划分与 Wi-Fi 指纹聚类提高计算效率，但需防止用户通过解密获取的距离数据对数据库进行分析攻击。

2. 基于 Paillier 加密的隐私保护方案（PriWFI）：

该方案采用 AP mask 技术，在同态计算过程中随机丢弃部分 RSS 值并添加噪声，掩盖真实欧氏距离，防止数据分析攻击。尽管随机丢弃会略微降低定位精度，该方案仍可提供较高的隐私保护。

3. 基于安全多方计算的隐私保护方案（PILOT）：

通过 Paillier 加密和安全多方计算（SMC），在不泄露双方隐私信息的情况下实现定位计算。本方案使用 ABY 框架评估 k 近邻电路和矩阵访问电路，实现安全两方计算。

4. 基于隐马尔可夫模型的 Wi-Fi 定位方案：

本方案基于隐马尔可夫模型（HMM），使用同态加密保护位置数据，并通过维特比算法计算用户的移动状态，确保在保护双方隐私的前提下完成定位。

9.2 基于差分隐私的隐私保护方案

1. 基于差分隐私的 Wi-Fi 指纹数据库保护方案：

在 Wi-Fi 指纹数据库的众包建库过程中，采用差分隐私技术为每个参与者的测量数据添加噪声，防止通过数据库查询结果进行差分攻击，确保参与者的隐私信息不会泄露。

2. 边缘环境下的差分隐私模型训练方案：

在边缘服务器上收集用户的训练样本，并在激活函数输出中添加差分隐私噪声，确保中央服务器无法推断用户隐私信息，从而保护训练数据中的敏感信息。

3. 基于差分隐私的 Wi-Fi 指纹定位方案：

该方案采用差分隐私聚类算法对定位数据库进行划分，并使用指数机制隐藏聚类中心，防止攻击者推断用户的位置信息。

4. 范式驱动的隐私保护机制（P3-loc）：

用户将测量信息分割为多个片段，并与周围用户交换部分片段，添加差分隐私噪声以保护用户隐私。定位服务器对片段进行重组并返回多个定位结果，用户根据片段挑选出真实位置。

9.3 基于 k 匿名的隐私保护方案

本标准规定了采用空间泛化、假名和随机化技术的 k 匿名隐私保护方案，旨在保护用户位置信息和测量信息的安全性。该方案通过在服务器端生成 k 个不可区分的定位结果，确保用户隐私不被泄露。根据具体实现方式，k 匿名方案分为有匿名器和无匿名器两种架构。

9.3.1 有匿名器方案

在有匿名器方案中，匿名器位于用户与定位服务器之间，对测量信息进行处理，包括泛化、随机化和假名化，以模糊用户信息并转换查询结果，从而确保用户的隐私保护。系统结构如图 5 所示。

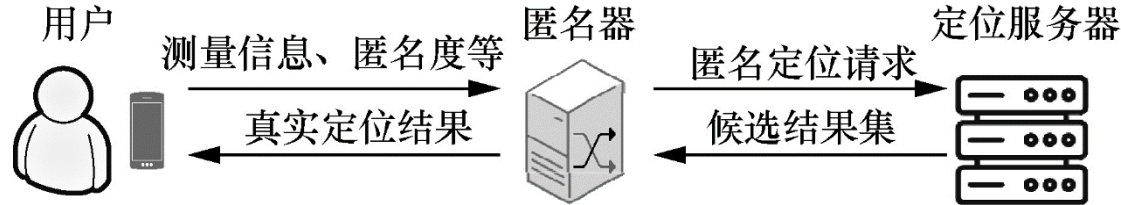


图 5 有匿名器方案的结构

1. 基于 ID 替换与希尔伯特曲线的方案

该方案通过将用户 ID 替换为临时标签，避免定位服务器获取用户身份。在定位结果返回后，服务器使用希尔伯特曲线对位置坐标进行变换，防止匿名器获得用户真实位置。同时，方案采用两次非对称加密，确保 Wi-Fi 指纹在匿名器和定位服务器之间的安全传输。

2. 基于哑元信息的随机化方案

该方案通过可信匿名器去除用户请求中的 ID 信息，并随机生成哑元信息与真实测量信息混合发送至服务器。此方法利用随机化技术，生成 k 个测量值，防止定位服务商从定位结果中推断出用户的真实位置。

3. 基于 AP 集合的匿名方案

该方案通过匿名器对用户测量信息进行随机化处理，并利用有向图结构存储 AP 信息。匿名器生成 $k-1$ 个虚假 AP 集合，与用户真实 AP 集合混合，从而完成匿名化操作。该方案通过动态更新 AP 信息图结构，提高了匿名化成功率。

9.3.2 无匿名器方案

在无匿名器方案中，用户端独立完成测量信息的随机化和匿名化处理。用户通过移动终端生成 k 个伪造轨迹或测量值，实现匿名性保护。系统结构如图 6 所示。



图 6 无匿名器方案的结构

1. 基于高斯-马尔可夫模型的轨迹生成方案

用户端利用高斯-马尔可夫模型生成 $k-1$ 个伪造轨迹，并计算对应的伪造测量值。这些虚假信息与实际测量信息一起发送至定位服务器，防止服务器推断出用户的真实位置。

2. 基于最大到达边界的哑元生成方案

用户端根据最大到达边界（MAB）和匿名域交集生成 $k-1$ 个伪造位置，并将这些伪造位置映射为虚假测量信息，从而防止定位服务器通过时空关联攻击获取用户的真实位置。

3. 基于布隆过滤器的 k 匿名方案

该方案结合 k 匿名技术与布隆过滤器，随机选择一个 AP 点并将其映射到布隆过滤器中。当定位服务器进行指纹匹配时，匹配到不少于 k 个包含该 AP 的参考点，并将这些参考点组成的部分数据库返回给用户进行精确匹配。虽然定位服务器无法确定用户的真实位置，但应避免向用户返回部分数据库可能会导致数据隐私泄露。

10 云定位的隐私保护方法

本标准规定了在云环境下实施室内定位隐私保护的技术方案，适用于云服务外包场景。为确保定位数据在云端的隐私性，云定位系统应采用部分同态加密、随机矩阵拼接和乘法、内积函数加密、安全多方计算及软件防护扩展等技术手段，保护定位资源和用户测量信息的安全性。各方案必须符合 Level-III 隐私保护度，确保云环境下的定位系统满足隐私保护要求，且在实施过程中应结合云计算资源的优化措施，确保系统性能与隐私保护的平衡。

10.1 基于同态加密的隐私保护方案

为解决云定位中的隐私保护问题，本方案采用部分同态加密技术。测量信息首先使用用户公钥和云端公钥进行双重加密，云端接收密文后解密一次，应用梯度下降算法计算定位结果，并输出加密后的结果。应采取优化措施，降低同态加密的迭代计算带来的计算开销，尤其是在大规模定位请求的场景中，确保系统性能和效率。

10.2 基于随机矩阵拼接和乘法的轻量级隐私保护方案

本方案通过定位锚点生成随机矩阵，将隐私坐标值与测量值拼接后进行矩阵相乘，并将结果发送至云服务器。云服务器在随机矩阵上进行计算，最终得到定位结果。该方案通过随机矩阵的拼接与相乘操作，隐藏了用户和锚点的位置信息。应注意矩阵乘法的线性性质可能带来的安全风险，需结合其他安全机制增强系统的整体安全性。

10.3 基于内积函数加密的 TDoA 隐私保护方案

本方案利用内积函数加密技术保护云环境下的测量信息和锚点数据。定位算法分解为向量内积运算，云服务器在加密的测量信息和锚点信息上计算定位结果，同时结合 k 匿名技术增强隐私保护。用户和服务商在测量和存储阶段分别对信息进行加密处理，确保数据在传输和存储中的安全性。

10.4 基于安全多方计算的隐私保护方案（PILOT）

本方案适用于云环境的外包场景，采用安全多方计算技术，保证云端服务器仅获取定位数据库、测量信息和定位结果的部分份额，无法恢复原始信息。通过两个不共谋的服务器进行计算，保护定位资源信息的隐私。在实际应用中，依赖多个不共谋服务器的方案应制定配合方案。

10.5 基于软件防护扩展（SGX）的隐私保护方案

本方案为云环境下提供了更高的隐私保护，并确保计算结果的可信性。本方案通过 SGX 技术在云端构建可信执行环境，确保定位数据的隐私安全。SGX 技术通过在处理器内部创建物理隔离的安全环境，防止外部访问代码和数据，并结合远程证明机制确保用户与可信执行环境之间的安全通信。用户可验证所连接环境的合法性，并保证应用程序的安全性。

11 实施要求

在实施定位隐私保护方法时，必须遵循以下关键要求，以确保方案的有效性和可行性。不同隐私保护技术具有各自的优缺点和适用场景，实施时应根据具体需求进行适当选择和权衡。

11.1 分布式架构的隐私保护要求

1) 基于信息隐藏的方案

该方案具有较高的计算效率，但需要用户与锚点之间进行随机值的通信，导致显著的通信开销。例如，在 m 个锚点的系统中进行一次 n 级矩阵的隐私保护求和，通信开销为 m^2n^2 。此外，该方案在抵抗锚点共谋攻击时安全性较低。应在实际应用中结合安全需求考虑使用该方案。

2) 基于同态加密和安全多方计算的方案

该方案通过加密算法和安全协议提升隐私保护安全性，能够有效抵御锚点共谋攻击。尽管不会影响定位算法的精度，但可能会降低计算效率。实施时，应根据具体应用场景，权衡安全性与效率，选择合

适的加密和计算方案。

11.2 集中式架构的隐私保护要求

1. 基于同态加密和安全多方计算的方案

该方案提供较高的隐私保护性能，对定位精度影响较小，但需要承担较大的加密和解密计算开销，以及更高的通信代价。实施时，应优化加密和计算流程，减少性能损耗，确保系统运行效率。

2. 基于差分隐私的方案

该方案具有较高的计算效率，并能够实现隐私保护的定量分析和证明。为保证隐私信息的安全，需在数据中添加噪声，但这些噪声可能导致定位误差增大，影响定位服务质量。实施时，应在隐私保护和定位精度之间找到平衡。

3. 基于 k 匿名的隐私保护方案

k 匿名方案必须通过空间泛化、假名和随机化等技术，生成 k 个不可区分的定位结果，以确保用户隐私。匿名器可以位于用户与服务器之间，或由用户独立完成匿名化操作。

- 有匿名器方案：匿名器应使用假名技术替换用户标识符，并对测量信息进行泛化处理，确保定位查询与用户身份之间无法建立关联。

- 无匿名器方案：用户终端应生成 k-1 个虚假的伪造信息，以混淆真实位置，防止时空关联攻击。

k 匿名技术的实施要求：

- 应优化 k 匿名算法，减少匿名操作带来的计算和处理延迟。

- 必须避免重复计算，减少系统负担，确保在隐私保护效果和系统性能之间的平衡。

12 隐私保护的附加实施要求

在实施室内定位隐私保护方案时，必须特别关注以下几个方面，以确保系统能够满足用户需求并提供高水平的隐私保护。

12.1 轨迹信息的保护

定位服务在收集用户的移动轨迹信息时，这些信息可能被用于推断用户的行为模式和日常习惯。因此，连续定位过程中可能暴露用户的行为模式。为确保用户的轨迹信息在多次定位中不被泄露或推断，必须开发新算法和机制，防止时空关联攻击。应采取有效的保护措施，以增强系统的隐私保护能力。

12.2 高效定位的实现

隐私保护方案不仅必须确保用户隐私的安全性，还必须保证定位服务的准确性和效率。为此，应采用优化的定位算法和数据索引结构，以减少定位计算和数据检索的时间复杂度。应引入预处理和缓存机制，提升系统响应速度及并发处理能力，以满足高效定位服务的需求。

12.3 云环境下的隐私保护定位

随着定位服务逐步向云环境迁移，云环境下的隐私保护问题日益重要。在设计云环境下的隐私保护方案时，必须充分考虑云计算平台的安全性和可信度，并采取必要的安全措施防止数据泄露和恶意攻击。此外，应针对云环境的高并发和分布式计算特性，优化定位算法和通信协议，确保云环境中的定位服务高效、安全地运行。

附 录 A

提供了相关技术细节、实施示例等额外信息，以帮助理解和应用本标准内容。

云环境下隐私保护定位方案的安全技术和性能评价指标							
安全技术	定位算法	隐私保护度				计算/通信开销	定位精度
		测量信息	数据库信息	定位结果	总体		
同态加密	无线信号交会	加密保护	加密保护	加密保护	Level-III	高	不影响精度
随机矩阵拼接和乘法	无线信号交会	受随机矩阵隐藏保护	受随机矩阵隐藏保护	受随机矩阵隐藏保护	Level-III	低	不影响精度
内积函数加密	无线信号交会	加密保护	加密保护	k匿名保护	Level-III	取决于k值	不影响精度
安全多方计算	数据库匹配定位	数据分割保护	数据分割保护	数据分割保护	Level-III	高	受方案中量化位数影响
软件防护扩展	无线信号交会	远程证明机制保护	物理隔离	远程证明机制保护	Level-III	低	不影响精度

表 1 云环境下隐私保护定位方案的安全技术和性能评价指标

各种安全技术的常用场景、隐私保护度、计算/通信开销和定位精度				
安全技术	常用场景	隐私保护度	计算/通信开销	定位精度
同态加密和安全多方计算	集中式定位架构	高，但通常不保护数据库信息	高，随数据库线性增长	不影响定位精度
差分隐私	集中式定位架构	量化的隐私保护强度	低	显著降低定位精度
k匿名	集中式定位架构	取决于匿名度和匿名机制	中，取决于匿名度	不影响定位精度
信息隐藏	分布式定位架构	低，无法抵抗共谋攻击	低	不影响定位精度
零知识证明、安全路由等	协作式定位架构	高，保护参与用户的匿名性	高	不影响定位精度
内积函数加密、矩阵乘法加密、物理隔离等	云定位架构	高，同时包含测量信息、数据库信息和定位结果	中	不影响定位精度

表 2 各种安全技术的常用场景、隐私保护度、计算/通信开销和定位精度