# 室内定位隐私保护综述

王志恒，徐彦彦
（武汉大学测绘遥感信息工程国家重点实验室，湖北 武汉 430072）

**摘 要**：智能手机的室内定位服务通常由第三方定位服务商提供，其独有的隐私泄露风险已成为制约其发展的主要因素，如何保护定位过程中用户和数据的隐私成为一个亟待解决的重要问题。对近年来室内定位隐私保护的研究进展进行综述。介绍了常用的室内定位技术，讨论了室内定位系统的不同实现架构及其威胁模型、隐私保护需求，总结了应用于室内定位隐私保护的安全技术，分类介绍了针对不同架构的室内定位隐私保护方案，全面比较和分析了不同方案的性能及其优缺点，总结并展望了未来的研究方向。

**关键词**：室内定位；隐私保护；安全协议；信息安全
**中图分类号**：TN92
**文献标志码**：A
**DOI:** 10.11959/j.issn.1000−436x.2023162

# Survey on privacy protection indoor positioning

WANG Zhiheng, XU Yanyan
State Key Laboratory of Information Engineering in Surveying Mapping and Remote Sensing, Wuhan University, Wuhan 430072, China

**Abstract:** Smartphones are usually provided with indoor positioning services by third-party positioning service providers, in which the unique privacy leakage risk has become a major factor limiting its development. How to protect the privacy of users and data in the positioning process has become an important issue to be solved. The research progress of indoor positioning privacy protection in recent years was reviewed. The commonly used indoor positioning technologies were introduced, different implementation architectures of indoor positioning systems and their threat models, privacy protection requirements were discussed, security technologies applied to indoor positioning privacy protection were summarized, indoor positioning privacy protection schemes for different architectures were classified and introduced, and the performance of different schemes and their advantages and disadvantages were comprehensively compared and analyzed, and finally future research trends were summarized and looked forward to.

**Keywords:** indoor positioning, privacy protection, security protocol, information security

## 0 引言

随着智能手机的普及和室内位置应用的快速发展，人们对高精度室内定位技术的需求日益强烈。由于卫星信号无法穿透建筑物，室内定位服务需要定位服务商提供定位设施和定位数据的支持，由用户智能手机上的传感器收集与位置相关的测量信息，并通过信息的交互计算来实现定位服务[1-2]。与直接在智能手机上接收卫星导航信号并在本地进行定位的全球导航卫星系统（GNSS, global navigation satellite system）不同，室内定位系统通过通信和交互计算实现定位的模式产生了特有的隐私泄露问题。一方面，用户的位置信息、移动轨迹等可能在交互计算的过程中泄露，从而造成与用

**收稿日期**：2023−05−18；**修回日期**：2023−08−21
**通信作者**：徐彦彦，xuyy@whu.edu.cn
**基金项目**：国家重点研发计划基金资助项目（No.2021YFB2501103）；国家自然科学基金资助项目（No.42271431）
**Foundation Items:** The National Key Research and Development Program of China (No.2021YFB2501103), The National Natural Science Foundation of China (No.42271431)

户位置相关的隐私信息泄露，如生活习惯、收入水平、健康状况、宗教信仰等，给用户带来困扰，甚至会危及生命财产安全[3]；另一方面，定位资源信息的泄露将给定位服务商带来重大的影响。定位数据库等定位资源的构建需要花费大量的时间和人力成本，其泄露会造成定位服务商经济上的巨大损失；此外，攻击者可能通过定位资源中的信息攻击定位基础设施，导致整个定位系统不可用。因此，隐私泄露已成为室内定位服务亟待解决的瓶颈问题。

国内外学者已提出了多种隐私保护的室内定位（PPIL, privacy protection indoor localization）方案。本文对近年来室内定位隐私保护的研究进展进行综述，介绍了常用的室内定位技术，分析了室内定位系统不同实现架构及其威胁模型、隐私保护需求，梳理了 PPIL 中常用的安全技术，并分类介绍了针对不同架构的各种 PPIL 方案，全面比较和分析了不同方案的性能和优缺点，最后在总结现有方案的基础上展望了未来的研究方向。

## 1　室内定位原理和安全威胁

### 1.1　室内定位技术

目前，常用的室内定位技术从原理上可以分为基于无线信号交会的定位技术、基于数据库匹配的定位技术和基于航迹推算的定位技术等[4]。

1) 基于无线信号交会的定位技术

无线信号交会技术是通过测量来自不同信源的无线信号在介质中的传播时间、接收角度和信号强度等信息，并结合信源的位置对目标点进行定位的技术。用于定位的信号源包括低功耗蓝牙、射频信号、超带宽信号、全球移动通信信号、超声波和红外线等。定位方法包括到达时间（ToA, time of arrival）、到达时间差（TDoA, time difference of arrival）、信号到达角（AoA, angle of arrival）、三角定位法等。

以三角定位法为例，其定位原理如图 1 所示。用户计算以锚点为圆心、以用户到锚点之间的测距值 $d_1,d_2,d_3$ 为半径的 3 个圆的交点作为定位结果。然而由于测量误差的存在，3 个圆可能出现多个交点或无交点的情况，此时可以将对用户的定位视为使误差平方和最小的优化问题[5]，利用最小二乘法求解定位，即将位置估计转化为下述最小二乘估计问题

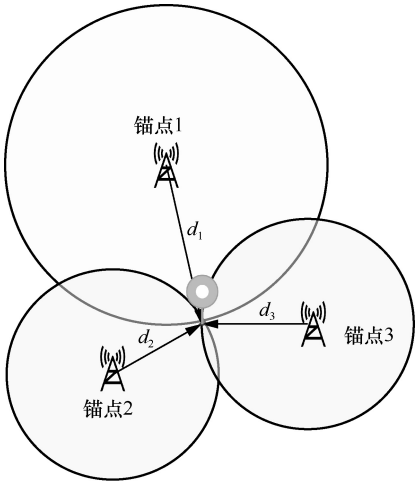


图 1　三角定位法定位原理

$$\hat{\boldsymbol{x}} = \min_{\boldsymbol{x}} \left\| 2\boldsymbol{A}\boldsymbol{x} - \boldsymbol{b} \right\|^2 \tag{1}$$

其中，$\boldsymbol{A}$ 表示锚点的位置信息，$\boldsymbol{b}$ 表示测量的距离信息，$\boldsymbol{x}$ 表示优化变量。该问题有如下形式的闭合解

$$\hat{\boldsymbol{x}} = \frac{1}{2}(\boldsymbol{A}^{\mathrm{T}}\boldsymbol{A})^{-1}\boldsymbol{A}^{\mathrm{T}}\boldsymbol{b} \tag{2}$$

通过求解式(2)即可得到用户位置的最小二乘估计结果。

2) 基于数据库匹配的定位技术

数据库匹配技术是通过测量信号特征，并与预先构建的数据库中的特征进行匹配或者相似性分析，得到位置估计的定位技术。可利用的信号特征包括地磁特征、重力场特征、Wi-Fi 的接收信号强度（RSS, received signal strength）指纹特征、信道状态信息（CSI, channel state information）特征等。基于数据库匹配的定位技术包括离线的数据库构建和训练阶段，以及在线定位阶段 2 个过程。

以 Wi-Fi 指纹定位为例，离线定位阶段，定位服务商测量定位场景中预先设定的参考点（RP, reference point）的 RSS 特征，也称为 Wi-Fi 指纹 $\boldsymbol{V}_i = [v_{i1}, v_{i2}, \cdots, v_{in}]$，同时记录参考点的坐标 $\boldsymbol{X}_i = [x_i, y_i]$，构建一个 Wi-Fi 指纹数据库 $D = \{(\boldsymbol{V}_i, \boldsymbol{X}_i) \mid i = 1,2,\cdots,m\}$。其中，$n$ 和 $m$ 分别表示 Wi-Fi 接入点（AP, access point）和参考点的数目。为了提高数据采集的效率，定位数据库以众包的方式构建。在线定位阶段，用户收集测量信息并发送至定位服务器请求定位服务。定位服务器运行确定性或概率性定位算法估计用户的位置。确定性算法如 RADAR[6]基于 Wi-Fi 指纹向量之间的欧氏距离

搜索最相似的参考点，将其位置坐标作为用户位置的估计值；概率性算法如 Horus[7]利用概率估计的方式，定位过程中利用贝叶斯推理，基于用户的测量指纹和数据库中 Wi-Fi 指纹的先验概率分布，计算出用户位于各个参考点的条件概率，从而确定用户的位置。

3) 基于航迹推算的定位技术

利用集成在移动终端设备中的惯性测量单元，如加速度计、陀螺仪和磁力计，来实时推算物体运动的速度和方向。通过对这些运动状态值进行积分，可以得到物体相对位移，从而实现对物体的定位。基于航迹推算的定位技术不需要外部信号或定位基础设施的支持，定位过程在用户设备内完成而不需要进行信息交互。且航迹推算一般只能得到相对位置关系而非绝对位置，因此较少考虑其隐私泄露问题。

### 1.2 定位系统架构和威胁模型

根据定位资源在系统中的部署方式，可以将室内定位系统分为集中式架构、分布式架构、协作式架构和基于云的架构。不同的系统架构中参与实体间信息交互和信息处理方式各异，因此威胁模型和隐私保护目标也不相同。

1) 集中式架构

在集中式架构中，定位资源信息集中部署在由定位服务商提供的服务器上。大部分基于数据库匹配的定位技术（如 Wi-Fi 指纹匹配）和隐私保护方案都基于集中式的室内定位系统架构实现。如图 2 所示，用户在定位时收集测量信息发送到定位服务商，定位服务商基于用户的测量信息和定位数据库运行定位算法，得到位置估计结果返回给用户。

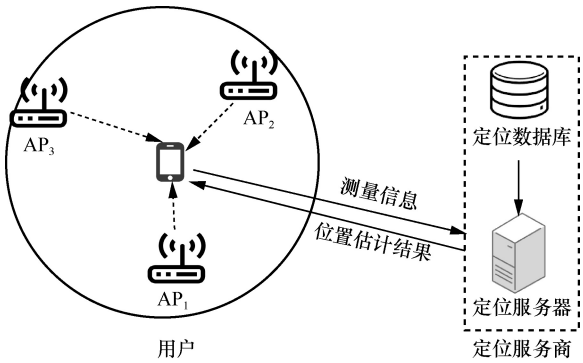


图 2 集中式室内定位系统架构

集中式室内定位系统考虑用户和定位服务商互不信任的威胁模型。其中测量信息和位置估计结果与用户位置隐私密切相关，需要防止定位服务商和外部攻击者的分析和获取；定位资源信息属于定位服务商的数据隐私，也要防止攻击者或者恶意用户利用服务器返回的信息推测出定位数据库[8]。因此，集中式室内定位系统的隐私保护目标是在用户和定位服务商互不信任的计算条件下实现定位，同时保护用户的测量信息和定位结果，并防止恶意用户对数据库资源的分析攻击。

2) 分布式架构

在分布式架构中，定位资源信息分布在多个定位基础设施（如定位锚点）中。基于无线信号交会的定位技术（如 ToA、TDoA 等）常采用分布式的系统架构，如图 3 所示。各个定位锚点维护自己的位置信息，用户需要与各个锚点交互，获得测量信息与锚点位置之间的计算结果，最终得到位置估计的结果。

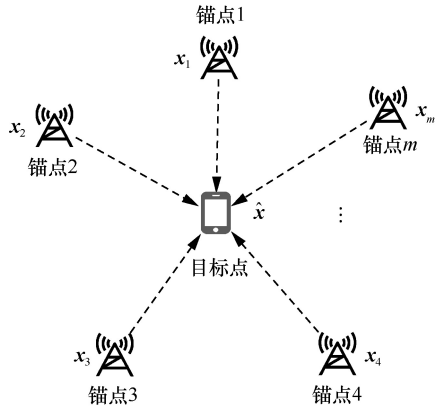


图 3 分布式室内定位系统架构

分布式室内定位系统的威胁模型考虑锚点和目标点同时为恶意实体的场景[9-10]。系统中的锚点可能利用交互过程中用户泄露的信息对用户位置进行粗略估计，甚至通过与其他锚点共谋进一步分析用户的精确位置；同时也可能存在恶意用户企图获取各个锚点的位置或其他隐私信息。因此在分布式室内定位系统中，隐私保护目标是防止交互过程中泄露双方隐私信息，需要同时保护锚点和目标点的位置隐私。

3) 协作式架构

在上述系统架构中，待定位的设备只与定位基础设施或定位服务器通信，完成定位过程。而在协作式室内定位系统架构中，待定位设备也需要与其邻居设备直接或间接通信，交换测量信息（如距离测量值）或定位资源信息（如已知的位置坐标或部

分数据库），通过设备之间相互协作实现定位[11]。例如在图 4 中，设备 1 和设备 2 都至多与 2 个锚点直接通信，此时三角定位法会产生二义性的结果，无法唯一地确定其位置。而利用两设备之间位置或距离信息的交换（图 4 中加粗箭头）可以排除二义性实现准确定位。已定位的设备可为其他未定位的设备提供协助性信息，从而实现整个系统所有用户的定位。

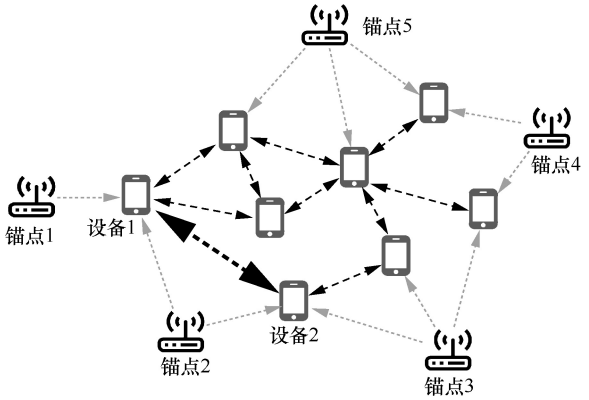


图 4　协作式室内定位系统架构

协作式室内定位系统依赖于锚点与设备，以及设备与设备之间的通信和交互计算，因此与分布式架构的威胁模型类似，协作式定位考虑锚点与用户同时为恶意实体的威胁模型，保护锚点和用户的位置隐私；此外，协作式定位还需要保护设备之间信息交互的安全性，防止位置隐私信息泄露给其他用户。

4) 基于云的架构

云定位是定位服务商将定位资源（如锚点位置信息、Wi-Fi 指纹数据库等）和定位算法外包给云服务提供商（CSP, cloud service provider），云端接收用户的测量信息并进行定位解算，向用户返回定位结果[12-13]。基于云的室内定位系统架构如图 5 所示。

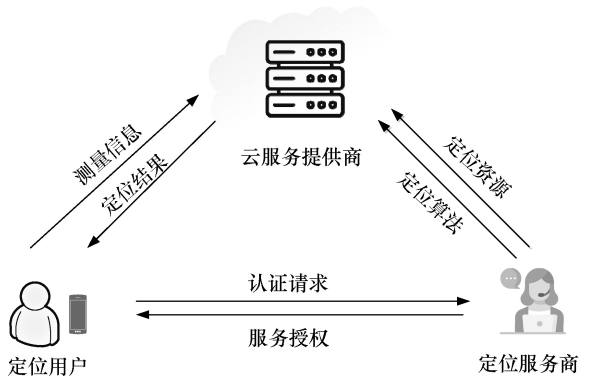


图 5　基于云的室内定位系统架构

基于云的室内定位系统考虑用户、定位服务商和 CSP 互不信任的威胁模型。其中 CSP 是“诚实而好奇”的实体，即它诚实地执行定位服务商交付的定位任务，但可能出于利益或好奇而主动地窥探定位服务商的定位资源信息以及用户的测量信息和定位结果，并且 CSP 作为开放的平台可能受到外部攻击造成数据和隐私信息的被动泄露；定位服务商既不希望云环境在定位过程中泄露其定位资源信息，同时又尽力分析和收集用户的位置信息；用户向云环境请求定位服务，同时可能存在恶意用户利用从云端返回的信息窃取云端的定位资源。基于上述威胁模型，云环境下室内定位隐私保护方案需要实现各方隐私信息的保护，防止隐私信息被除自身以外的任何实体获知。

### 1.3　PPIL 方案性能指标

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，因此通常从以下几个性能指标进行评估。

1) 隐私保护度

如前文所述，不同定位系统架构下威胁模型和隐私保护目标也各不相同，因此没有统一的隐私保护度的指标。文献[10]为分布式架构下基于无线信号交会的定位技术定义了三级隐私保护度。具有 Level-Ⅰ隐私保护度的方案中，锚点无法获知其他锚点或用户的位置，但可以根据各自掌握的信息得到目标点位置的粗略估计结果；具有 Level-Ⅱ隐私保护度的方案可以抵抗单个锚点对用户位置的粗略估计，但无法抵抗锚点之间的共谋；具有 Level-Ⅲ隐私保护度的方案可以抵抗锚点之间的共谋。该定义可应用于分布式或协作式架构下隐私保护性能的度量，但是不适于其他架构。因此本文扩展了该定义在集中式和云定位架构下的含义：如果方案可以保护用户的测量信息和定位结果，但是可能泄露定位服务商的数据库信息，则方案具备 Level-Ⅰ的隐私保护度；如果方案可以同时保护定位数据库信息，但是需要运行在定位服务商信任的服务器下，则方案具备 Level-Ⅱ的隐私保护度；如果方案在不可信的服务器下能同时保护用户的测量信息、定位结果，以及定位服务商的数据库信息，则方案具备 Level-Ⅲ的隐私保护度。基于上述隐私保护度的定义，本文对不同方案的隐私保护性能进行分析。

2) 定位精度

定位精度直接反映了隐私保护方案对室内定

位系统服务质量的影响。PPIL 对定位精度的要求不在于提升原始算法的精度，而在于尽量降低对原始定位算法的影响。在实验中，定位精度使用均方误差（RMSE, root mean square error）衡量，定义为

$$e=\sqrt{\frac{\sum_{i=1}^{N}\| \hat{\boldsymbol{x}}^{(i)}-\boldsymbol{x}^{(i)} \|^2}{N}} \tag{3}$$

其中，$\hat{\boldsymbol{x}}^{(i)}$ 表示第 $i$ 次的定位结果，$\boldsymbol{x}^{(i)}$ 表示用户当次的真实位置，$N$ 表示定位实验的次数。实验中应以原始算法的精度作为基准，从而显示隐私保护方案对精度的影响。

3) 方案开销

开销反映隐私保护技术的应用所引入的额外代价，主要包括存储、计算和通信开销。其中存储开销主要包括运行隐私保护技术所需的参数、密钥等信息，相比于现阶段计算机和云环境的存储能力，其数据量可以忽略；计算和通信开销可以通过对隐私保护算法的时间和通信复杂度进行理论分析，并通过实验定量度量。高效的 PPIL 方案应当在实现隐私保护需求的同时尽量降低开销。

## 2 关键技术

### 2.1 同态加密技术

同态加密（HE, homomorphic encryption）最早是 Rivest 等[14]于 1978 年提出的概念，它支持密文域运算，可以得到对应明文计算结果的密文，即满足

$$\mathrm{Enc}\big(f(m_1,m_2)\big)=f\big(\mathrm{Enc}(m_1),\mathrm{Enc}(m_2)\big) \tag{4}$$

其中，$m_1$ 和 $m_2$ 表示任意明文信息，$f$ 表示任意计算过程。同态加密的这一特性既可以保护数据的安全性，又使密文数据具有一定的可用性，因此在云环境下的安全计算中有广泛的应用，也适于隐私保护的室内定位场景。

同态加密方案分为部分同态加密和全同态加密。部分同态加密可以支持密文域的加法或者乘法运算，如 RSA 加密算法、Elgamal 算法[15]和 Paillier 算法[16]等。全同态加密能够同时支持密文域上的加法和乘法，例如 Gentry[17]于 2009 年提出的基于理想格的同态加密方案，微软开发的全同态加密算法的 SEAL 库[18]等。

同态加密算法同时保证了数据的安全性和可用性，似乎是理想的隐私保护计算的工具，但是同态加密有较高的计算开销。并且由于同态加密的密文数据一般较大，即存在密文扩展效应，导致基于同态加密的方案的通信开销较大，计算和传输都有较高的负担。

### 2.2 安全多方计算技术

安全多方计算起源于百万富翁问题[14,19]，即双方在不泄露各自财产的情况下完成财富比较。经过对该问题的多次扩展[20-21]，安全多方计算是指在没有可信第三方时，参与方通过交互计算，在各自的私有输入上联合完成目标函数的计算，得到约定函数的结果。并且保证参与方无法推测出其他任意一方的输入和输出数据。主要采用的技术包括混淆电路（GC, garbled circuit）[22]、不经意传输（OT, oblivious transfer）[23]等。

混淆电路的核心技术是将两方参与的安全计算函数编译成布尔电路的形式，将真值表加密并扰乱来掩盖真实信息，从而实现电路的正常输出而又不泄露参与方的私有信息。任何安全计算函数都可转换成对应布尔电路的形式，例如加法电路、比较电路、乘法电路等，因此相较其他的安全计算方法，混淆电路具有较高的通用性。

不经意传输是一个密码学协议，最早在 1981 年被 Rabin[24]提出。在最早的 OT 协议中，发送者发送一个信息，接收者以 $\frac{1}{2}$ 的概率接收。OT 协议保证交互结束时，发送者无法判断消息是否被接收。Even 等[25]对其进行改进，提出了 1-out-2 OT 协议，即接收者可以选择 2 个秘密信息之一而无法知道另一个；发送者也无法判断接收者的选择。后续也相继提出了 1-out-$n$ 的 OT 协议[26-27]和各项提高 OT 协议效率和可用性的研究[28-29]。

目前，已有许多安全多方计算架构[30-33]实现了上述的安全协议。例如 ABY[30]架构支持 3 种秘密共享类型：基于姚氏混淆电路的 YAO 共享、基于 GMW 协议[20]的布尔共享和基于 GMW 的算术共享，提供了不同共享类型之间的转换方法，以及被动安全保证，即假定攻击者遵循安全协议，则无法从接收到的消息中获取到任何附加信息[34]。

### 2.3 差分隐私技术

差分隐私（DP, differential privacy）是一种数据共享手段，实现仅分享数据库的统计特征而不

公开具体到个人的信息。差分隐私的思想最早由Dwork[35]于 2006 年提出，随后被不断完善和扩展[36-40]。差分隐私背后的直观想法是如果随机修改数据库中的一个记录造成的影响足够小，求得的统计特征就不能被用来反推出单一记录的内容，具体定义式为

$$\Pr\left[A(T)\in S\right]\leqslant e^{\varepsilon}\Pr\left[A(T')\in S\right] \tag{5}$$

其中，$A(\cdot)$ 表示作用在数据库上的算法，$T$ 和 $T'$ 表示一对相邻数据集，即仅有一条记录不同的 2 个数据集，$\varepsilon$ 表示隐私预算，$S$ 表示输出集合。式(5)表示随机算法作用在相邻数据集上输出的结果是相似的，无法通过差分攻击获取单一记录中包含的隐私信息。

差分隐私通常是通过向数据集中添加满足一定分布的噪声来实现的，常用添加噪声的方式有 Laplace 机制和指数机制，前者常用于数值型的结果，后者适于非数值型的结果。差分隐私可以实现对隐私的定量分析和证明，但是加入的噪声会导致数据的可用性下降。因此在使用差分隐私方法实现隐私保护定位的同时，如何权衡数据的安全性和可用性是重点研究的方向。

### 2.4　信息隐藏技术

本文中的信息隐藏技术是指向数据中添加噪声从而隐藏原始信息的方法。与差分隐私技术不同的是，为使信息隐藏所添加的噪声可以在后续的计算中相互抵消，因此不影响数据的可用性，也称为“零和噪声”机制（zero-sum noise mechanism）。例如在隐私保护求和（PPS, privacy protection summation）中，节点 $i$ 持有其隐私信息 $x_i, i=1,2,\cdots,n$，其中 $n$ 是节点数目，汇聚节点需要在保护各个节点隐私信息的条件下求和。为实现这个目的，节点 $i$ 生成 $n$ 个随机数 $\left\{r_{ij}\mid i=1,2,\cdots,n, j=1,2,\cdots,n\right\}$，且满足 $\sum_{j=1}^{n} r_{ij}=0, i=1,2,\cdots,n$。然后节点 $i$ 保留其中的一个值，而将其他 $n-1$ 个值发送到另外 $n-1$ 个节点。同样地，节点 $i$ 也会接收到来自其他节点的共 $n-1$ 个随机值。节点 $i$ 将自己保留的随机值和接收到的随机值与自己的隐私信息 $x_i$ 相加发送到汇聚节点，汇聚节点将来自各个节点的数据相加实现求和。容易看到，由于汇聚节点收到的来自各个节点的数据是经过噪声保护的，各个节点的隐私信息实现了隐藏；另外，由于所添加的噪声之和为 0，因此在求和的过程中相互抵消，从而实现了隐私保护的求和。

相比于加密的方法，信息隐藏技术计算较高效，但是隐私保护强度也相对较弱。并且在添加噪声的过程中需要各个节点之间相互通信传递随机值，会产生一定的通信开销。

## 3　隐私保护室内定位方案

### 3.1　集中式架构的隐私保护方案

集中式架构下，定位服务商拥有对定位资源信息的绝对控制，因此隐私保护方案侧重于对用户位置隐私和测量信息的保护。采用的技术主要包括同态加密和安全多方计算、差分隐私、$k$ 匿名等。

1) 基于同态加密和安全多方计算的方案

通过对测量信息加密，并在密文上同态地进行计算，基于同态加密的方案可以在实现定位算法的同时，保护测量信息和定位结果的安全性。

在基于数据库匹配的定位方案中，大多数隐私保护方案是为指纹匹配法设计的，如 RADAR 定位算法。文献[41]研究了指纹收集方式对用户隐私信息威胁的可能，其结论表明用户收集测量信息应当采取被动监听的策略，以防止主动探测方式下 AP 和网络提供商对用户的记录和追踪。文献[42]设计了基于 Elgamal 的隐私保护定位方案，定位服务器利用加密的测量值同态地计算欧氏距离的密文，用户进行解密、比较和排序，得到最接近的 Wi-Fi 指纹以及对应的位置坐标，实现定位。方案进一步利用网格划分和 Wi-Fi 指纹聚类的方法提高计算效率。然而方案中用户可解密获得真实的欧氏距离，威胁定位数据库的安全，即未考虑恶意用户的数据分析攻击[8]。文献[8]介绍了基于 Paillier 的隐私保护定位方案（PriWFl）。该方案利用 AP mask 技术抵抗数据分析攻击，即在欧氏距离的同态计算时随机地丢弃一些接入点的 RSS 值并添加相同的随机噪声来掩盖真实的欧氏距离。进一步地，文献[43]在基于 Paillier 计算欧氏距离实现用户定位之后，将自身位置编码进空间布隆过滤器（SBF, spatial bloom filter），并与加密的包含感兴趣区域的空间布隆过滤器进行运算，使定位服务商能够确定用户是否出现在感兴趣区域内。文献[44]指出文献[8]中随机丢弃 Wi-Fi 接入点的做法会降低定位精度，并且揭示了该方案由于添加相同的噪声，面对恶意用户的数

据分析攻击仍然具有一定的脆弱性，会完全地泄露定位数据库的信息。同时，文献[44]也提出了 4 种实现隐私保护室内定位的方案，包括基于全同态加密的方案、基于混淆电路的方案、基于 Paillier 部分同态加密的方案和基于 GC 与 Paillier 混合的方案。然而该文仅介绍了方案的框架，并不包含具体的算法和实现。文献[45]为基于支持向量机的定位算法设计了隐私保护方案，利用部分同态加密实现了 3 种常用核函数（内积核、高斯径向基核、Sigmoid 核）的安全计算，保护了用户的位置隐私和测量数据的隐私。

通过将定位算法转换为待评估的目标函数，安全多方计算可以在实现定位计算的同时，不向对方泄露各自的隐私信息。基于文献[44]中的方案，文献[46]设计了同态加密和 GC 电路混合的方案。与 PriWFl 类似，该方案同样使用 Paillier 算法实现测量信息的加密和欧氏距离的同态计算，不同的是服务器在距离值上添加不同的噪声，因此填补了 PriWFl 在安全性上的漏洞，但是也造成用户解密后无法直接进行排序，于是用户和定位服务器之间需要评估一个 GC 电路，进行噪声消除和排序操作。该文也为外包场景设计了基于安全多方计算的方案（PILOT）[34]，该方案使用 ABY 框架[30]实现。方案中定位服务商的数据库信息被分割并安全共享到 2 个不共谋的定位服务器中，定位用户也将测量信息的份额分别发送到 2 个定位服务器。经过定位服务器的安全两方计算，得到定位结果的份额后返回给用户。用户将份额合并得到真实的定位结果。其中 2 个定位服务器会评估距离计算电路、$k$ 近邻电路和矩阵的不经意访问电路，实现基于安全两方计算的定位算法。文献[47]介绍了基于不经意传输的隐私保护 Wi-Fi 指纹定位方案，其中定位服务器根据用户提交的 AP 的 ID 信息返回部分数据库，用户在本地计算出测量指纹与该部分数据库中最接近的 $k$ 个指纹，然后运行不经意传输协议安全地从服务器中获取这 $k$ 个指纹对应的坐标值，从而实现隐私保护定位。

相比于上述确定性的 Wi-Fi 定位算法，基于概率模型的 Wi-Fi 定位算法也受到了研究者的关注。文献[48]为基于隐马尔可夫模型（HMM, hidden Markov model）的 Wi-Fi 定位算法设计了隐私保护方案。基于 HMM 的定位算法是将用户在连续移动过程中的位置建模为隐马尔可夫模型中的“状态”。定位服务商基于每个状态的发射概率、转移概率和用户的 Wi-Fi 指纹序列，使用维特比算法确定用户出现概率最大的路径[49]。方案基于同态加密实现了安全两方计算协议，以维特比算法作为待评估的函数，以用户测量值和 HMM 参数作为输入，向用户端输出加密后的定位结果。由于同态加密的性质，定位服务器可以直接进行密文测量值的加法和乘法运算而不需要交互；而 HMM 参数值在交互计算前进行盲化处理，从而保护定位服务商的数据隐私，实现了双方隐私信息保护下的定位计算。文献[50]设计了名为 PriHorus 的隐私保护方案，利用 Paillier 加密算法实现最大似然估计的定位过程，同时保护用户的隐私信息。

基于同态加密和安全多方计算方案的共同缺点在于方案的计算效率较低，特别是需要由用户承担大量的加密和解密计算。基于安全多方计算的方案需要大量的通信开销，例如 PILOT 中每次定位需要超过数百兆字节的通信开销[51]，实用性较低。

2) 基于差分隐私的方案

差分隐私可以应用于离线阶段（众包建库和模型训练）和在线阶段（位置估计）用户的隐私信息保护。文献[52]为 Wi-Fi 指纹数据库的众包建库过程设计了基于差分隐私的保护方案。方案利用秘密共享技术实现各个众包参与者测量信息和位置的安全收集，并且众包参与者在各自测量的 RSS 指纹和位置访问指示标识中添加满足差分隐私定义的噪声，从而防止收集者通过对收集结果的差分攻击获取参与者的隐私。文献[53]设计了基于差分隐私的定位模型训练方案，将隐私预算分散到模型训练的 3 个阶段，使整体满足 $\varepsilon$-差分隐私，保护训练过程中指纹收集者的位置隐私。文献[54]将差分隐私的定义扩展到 Wi-Fi 指纹数据中，提出了基于差分隐私的数据模糊机制，对 Wi-Fi 指纹进行泛化和特化处理。文献[55]设计了边缘环境下基于差分隐私的定位模型训练方法，用以保护训练阶段用户收集的训练样本中的隐私信息。方案利用可信的边缘服务器收集用户的训练样本进行训练，在模型的激活函数输出中添加满足差分隐私定义的噪声，从而保证中央服务器在聚合各个边缘服务器的子模型时无法从中推断出参与用户的隐私信息，保护用于训练的 Wi-Fi 指纹数据库信息。在众包建库或者模型训练过程中，加入的差分隐私噪声将会降低在线定位阶段的定位精度。

文献[56]提出了一个基于差分隐私的 Wi-Fi 指纹定位方案，其中定位服务器使用基于差分隐私的聚类算法对定位数据库进行聚类划分，使用指数机制来隐藏真实的聚类中心，从而保证攻击者无法根据聚类的输出推断出用户位置所属类别。文献[57]提出了一个范式驱动的隐私保护机制（P3-loc），适于所有满足以信息测量和定位估计组成的定位范式的定位算法。方案中用户收集到测量信息后将其分割成 $k$ 个片段，然后将其中的 $k$–1 个片段与周围的用户交换组成一个新的测量信息。用户在进行测量信息交换前会向其中添加满足差分隐私定义的噪声，从而保护各个用户真实的测量信息。定位服务器对信息片段进行重组和定位，向每个用户返回对应于所包含信息片段的多个定位结果，用户从中挑选出自己的真实位置。

基于差分隐私的 PPIL 方案具有较高的计算效率，并且可以实现隐私的定量分析和证明。但是方案需要在数据中添加满足差分隐私定义的噪声，虽然实现了隐私信息的保护，但是会提高定位误差，降低定位服务的质量。

3) 基于 $k$ 匿名的方案

基于 $k$ 匿名的隐私保护方案利用空间泛化、假名和随机化等技术，在服务器端产生 $k$ 个不可区分的定位结果，保护用户位置信息和测量信息的安全性。根据其实现方式，可以分为有匿名器的方案和无匿名器的方案。

在有匿名器的方案中，匿名器位于用户和定位服务器之间，对测量信息进行泛化、随机化或假名技术的处理，将由模糊数据得到的查询结果转换为用户需要的结果，系统结构如图 6 所示。

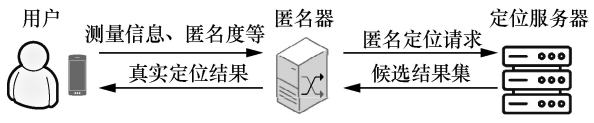


图 6　有匿名器方案的结构

匿名器利用的假名技术是将定位查询中的用户标识符使用临时的假名替代或者直接删除，断开用户和查询之间的关联，实现用户匿名的目的。文献[58]在利用匿名器向定位服务器转发定位请求信息的同时，将具有标识作用的 ID 替换为无标识作用的临时标签，从而防止定位服务器获知该定位结果对应的用户身份；定位服务器在完成定位后利用希尔伯特（Hilbert）曲线对位置坐标进行变换，防止匿名器获知用户的真实位置。同时方案使用两次非对称加密，实现 Wi-Fi 指纹在匿名器和定位服务器之间的安全传输。文献[59]利用可信的匿名器，去除用户定位请求中的 ID 信息，实现用户的匿名保护。

随机化技术会根据用户指定的匿名度，向测量信息中添加生成的哑元信息并一起发送给定位服务器，使定位服务商无法从 $k$ 个测量值和定位结果中区分，实现用户位置和测量信息的隐私保护。这种随机化的方法必须使哑元值的定位结果与真实可能的定位结果不可区分，否则将极大降低隐私保护强度。因此已有的研究重点考虑如何智能地生成哑元信息。文献[60]使用一个可信的匿名器对用户的测量信息随机化，匿名器以有向图结构存储 AP 信息，基于用户发送的 AP 集合另外生成 $k$–1 个可定位的 AP 集从而实现匿名。方案设计了 3 种可定位 AP 集的生成策略以满足不同场景对定位效率和匿名成功率的需求。类似地，文献[61]同样使用匿名器完成测量信息的匿名操作，生成 $k$–1 个测量信息哑元，不同的是该方案从用户历史提交的定位请求中构建 AP 信息的图结构，因此可以实现 AP 信息图的动态更新，提高匿名成功率。文献[62]中的匿名器利用了历史请求频率作为辅助信息，可以得到更符合真实分布的测量信息哑元。

无匿名器的方案中，测量信息的随机化等操作由移动终端独立完成，系统结构如图 7 所示。上文介绍的以范式驱动的隐私保护定位方案 P3-loc 中，用户与其邻居节点交换测量信息片段，构成一个匿名集，从而使定位结果对服务器不可区分。然而方案在只有单一用户时将失去匿名性，可以与虚拟用户构成匿名集以克服这一缺陷，即利用哑元测量值的方法。文献[63]利用高斯–马尔可夫模型对用户的移动性进行建模，生成 $k$–1 个哑元轨迹。用户端基于真实的测量值和信号的对数衰减模型，计算哑元轨迹对应的哑元测量值。文献[64]考虑了连续定位时用户的移动能力生成更合理的哑元位置和哑元测量信息，防止定位服务器的时空关联攻击。用户从最远到达边界（MAB, maximum arrival boundary）和匿名域的交集中，基于最大分散程度的原则选取 $k$–1 个哑元位置，将这些位置映射为哑元测量信息，实现用户真实的测量信息和定位结果的隐藏。文献[65]将 $k$ 匿名技术与布隆过滤器相结合，利用布隆过滤器具有一定误支持率的特点，从

测量信息中随机选择一个 AP 点，映射到布隆过滤器中。定位服务器在进行指纹匹配时可以匹配到不少于 $k$ 个包含该 AP 的参考点。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，定位服务器分析出用户真实位置的概率不超过 $\frac{1}{k}$，但是方案中向用户返回部分数据库，可能会导致定位服务商的数据隐私泄露。

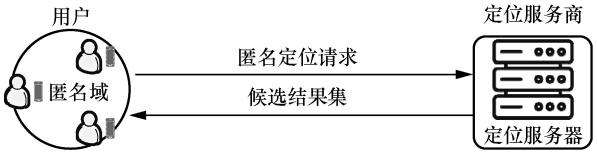


图 7 无匿名器方案的结构

$k$ 匿名技术只能提供有限的隐私保护，因此经常与其他技术结合提升系统的安全性。并且 $k$ 匿名技术需要匿名器的额外运算，例如文献[60-62]中的匿名操作；或者数据的重复计算，例如文献[63-64]中为处理单次定位请求所执行的 $k$ 次定位运算。因此在一定程度上降低了系统的效率。

表 1 总结了基于集中式架构的隐私保护方案。总体而言，基于同态加密和安全多方计算的方案具有更高的隐私保护性能，且对于精度影响较小，但是也具有更高的计算和通信代价；基于差分隐私的方案效率较高，且具有可量化的隐私保护强度，但是会显著降低定位精度；而基于 $k$ 匿名的方案则在隐私保护强度上有不足，无法抵抗拥有背景知识的攻击者，如数据关联攻击。

### 3.2 分布式架构的隐私保护方案

分布式架构的定位系统中，定位资源信息分布在定位基础设施（如定位基站、信号锚点）中，通过交互计算完成位置估计。基于分布式架构的隐私保护方案主要侧重于保护用户与分布式节点交互过程中双方的隐私信息，且不耗费太大开销。已有的研究使用信息隐藏技术实现高效的隐私保护定位，利用同态加密和安全多方计算技术增强安全性。

1) 基于信息隐藏的方案

通过向数据中添加零和噪声，基于信息隐藏的方案可以实现在保护隐私信息的同时不影响定位精度。文献[10]中的协议 1 和协议 2 采用了信息隐藏的思想保护用户测量信息和锚点位置信息。文献[10]的协议 1 中移动的锚点在不同的位置进行测量，并根据测量的结果和测量时锚点的位置坐标计算定位的中间结果，这些中间结果隐藏了锚点的位置和用户测量值等隐私信息。目标点将各个中间结果汇总计算得到最终的定位结果。在文献[10]的协议 2 中，各个锚点在计算的中间结果上加入可抵消的噪声，隐藏自己的位置坐标信息。目标点对各个锚点的信息求和，将噪声抵消从而实现隐私保护的定位过程。与文献[10]的协议 2 类似，文献[9]基于 PPS 为 2 个 TDoA 定位场景设计了隐私保护的定位算法，2 个场景中测量信息分别在用户端和锚点处获得。算法将 TDoA 的最小二乘估计过程分解为向量或者矩阵求和的基本形式，在各个求和的单项中添加可抵消的噪声，实现信息隐藏的同时不影响定位精度。文献[66]设计了基于近邻相减的最小二乘法的隐私保护方案，其中第 $i$ 个锚点与第 $i$+1 个锚点信息相减构建定位方程。方案利用了 PPS、隐私保护的近邻乘积求和（PPPS, privacy preserving adjacent product summation）和隐私保护的近邻差分求和（PPDS, privacy preserving adjacent difference summation）实现定位算法中对应过程的隐私保护计算，保护锚点的位置隐私信息和目标点的测量信息和定位结果。文献[67]为水下传感器网络设计了隐私保护的定位方案，方案包括基于 PPS 的计算阶段和基于隐私保护对角乘积（PPDP, privacy preserving diagonal product）计算阶段，实现了最小二乘法的安全计算。

与上述最小二乘法不同，文献[68]为分布式定位算法（DILOC）[69]设计了基于信息隐藏的隐私保护协议（PP-DILOC）。DILOC 算法基于重心坐标进行定位，即将用户位置表示为锚点坐标的线性组合，用户利用距离测量值和锚点坐标迭代更新线性组合系数实现定位。PP-DILOC 通过添加噪声值实现锚点位置坐标的隐藏，并且噪声可在迭代过程中相互抵消从而不影响定位精度。文献[70]为文献[71]中提出的分布式单锚点定位算法设计了隐私保护协议。该算法中锚点同时测量距离和角度值实现单锚点定位，并且多个锚点将定位结果发送到用户端计算均值得到更精确的结果。协议将发往用户的单锚点定位结果中加入噪声，并且在用户端均值计算过程中相互抵消，从而保护锚点的隐私信息并且不影响用户的定位精度。作者在其后来工作[72-73]中使用了相同的隐私保护方法，但是分别使用了锚点性能评估和锚点辅助设施对方案进行改进，提升了定位精度。

**表 1　　基于集中式架构的隐私保护方案**

| 安全技术 | 文献 | 方案分类 | 隐私算法 | 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 Level | | |
| 基于同态加密和安全多方计算的方案 | 文献[42] | 同态加密 | Elgamal | 受加密保护 | 无加密且易受分析攻击 | 在用户端获得 | Level- Ⅰ | 高，但是网格划分可以降低开销 | 网格划分方式降低定位精度 |
| | 文献[8] | | Paillier | 受加密保护 | 无加密且易受分析攻击 | 在用户端获得 | Level- Ⅰ | 高 | AP mask 会降低定位精度 |
| | 文献[43] | | Paillier | 受加密保护 | 无加密 | 在用户端获得，但会向服务器泄露区域信息 | Level- Ⅰ | 高 | 不影响精度 |
| | 文献[50] | | Paillier | 受加密保护 | 无加密保护 | 在用户端获得 | Level-Ⅱ | 高 | 不影响精度 |
| | 文献[45] | | Paillier | 受加密保护 | 模型无加密保护 | 密文结果 | Level-Ⅱ | 中 | 不影响精度 |
| | 文献[48] | 安全多方计算 | 以 Paillier 实现 | 受加密保护 | 受盲化处理 | 密文结果 | Level-Ⅱ | 高 | 不影响精度 |
| | 文献[34] | | ABY | 被分割保护 | 被分割保护 | 被分割保护 | Level-Ⅲ | 高 | 受量化位数影响 |
| | 文献[46] | 混合方案 | Paillier 和 ABY | 受加密保护 | 无加密，但抵抗数据分析 | 在用户端获得 | Level-Ⅱ | 高 | 不影响精度 |
| 基于差分隐私的方案 | 文献[52] | 众包建库 | 拉普拉斯机制 | 秘密共享和差分隐私保护 | — | 秘密共享和差分隐私噪声保护 | Level-Ⅱ | 高 | 降低数据库的准确性和定位精度 |
| | 文献[53,55] | 模型训练 | 拉普拉斯机制 | 差分隐私噪声 | — | 差分隐私训练模型保护 | Level-Ⅱ | 低 | 降低在模型精度和定位精度 |
| | 文献[56] | 定位过程 | 拉普拉斯机制和指数机制 | AP 模糊化 | 基于 DP 聚类和扰动保护 | 用户端获得 | Level-Ⅱ | 低 | 降低精度 |
| | 文献[57] | | 拉普拉斯机制 | 差分隐私噪声保护 | 无保护 | 匿名保护 | Level-Ⅱ | 低 | 降低精度 |
| 基于 $k$ 匿名的方案 | 文献[58] | 有匿名器 | 假名技术，身份替换 | 对称加密和匿名保护 | 无保护 | Hilbert 变换，加密和匿名 | Level-Ⅱ | 中 | 不影响精度 |
| | 文献[59] | | 假名技术，身份删除 | 匿名保护 | 无保护 | 匿名保护 | Level- Ⅰ | 低 | 不影响精度 |
| | 文献[60-62] | | 随机化技术，哑元信息生成 | 匿名保护 | 无保护 | 匿名保护 | Level-Ⅱ | 取决于匿名度 | 不影响精度 |
| | 文献[63-64] | 无匿名器 | 随机化技术，哑元信息生成 | 匿名保护 | 无保护 | 匿名保护 | Level-Ⅱ | 取决于匿名度 | 不影响精度 |
| | 文献[65] | | 随机化技术 | 受布隆过滤器保护 | 泄露部分数据库 | 匿名保护 | Level- Ⅰ | 中 | 不影响精度 |

由于未使用任何的加密算法，基于信息隐藏的 PPIL 方案具有较高的计算效率。但是信息隐藏技术需要用户与锚点之间相互通信传递随机值，将在系统中产生一定的通信开销。例如在 $m$ 个锚点的定位系统进行一次 $n$ 级矩阵的隐私保护求和，就需要在系统中产生 $m^2n^2$ 的通信开销。另外方案的安全性，特别是抵抗锚点共谋攻击的能力相对较低。文献[10]中的协议 1 以及文献[70]和文献[72]中的方案仅具有 Level-Ⅰ安全性；文献[9]中的方案和文献[10]中的协议 2 具有 Level-Ⅱ的安全性。文献[9,67]中的结论也表明方案仅具有抗部分锚点共谋攻击的能力。

2) 基于同态加密和安全多方计算的方案

一些基于分布式架构的 PPIL 方案利用了同态加密和安全多方计算等密码学技术，以实现更好的隐私保护效果。文献[10]中设计的协议 3 利用 Paillier 加密算法对目标点的距离测量值进行加密保护，锚点在加密的距离值和明文的坐标值上进行同态计算，之后由目标点解密获得定位计算中双方隐私信息的乘积项，进而实现最小二乘法。该方案被证明具有 Level-Ⅲ安全性，即可以抵抗共谋的锚点对目

标点位置的粗略估计。文献[74]将测距定位中用户位置所在的圆以多边形描述，从而将原始最小二乘估计公式中分散的敏感信息集中。这一方面避免了计算过程中敏感信息的乘法运算，降低了对加密算法同态性的要求；另一方面减少了所需加密的数量。最终使方案能够以部分同态加密算法实现最小二乘估计并且提高了性能。文献[75]介绍了基于混淆电路（GC）的三角定位协议，利用了 3 台救援车辆定位丢失的车辆，并且保护所有车辆的位置隐私。协议中设计了 2 个圆求交的 GC，分别以 2 辆车的位置坐标和测得的与丢失车辆的距离值为隐私输入，输出交点坐标。在 3 台救援车辆两两之间评估该 GC 之后，得到 3 个圆相交的三角形，丢失车辆计算该三角形的中心作为自身的位置坐标。

相比于信息隐藏方案，基于同态加密和安全多方计算的方案利用加密算法和安全协议提升方案的安全性，方案在锚点共谋攻击下仍然可以有效保护用户的位置隐私，然而降低了方案的计算效率。各个方案均不影响原始定位算法的精度，但是在安全性和效率上却有所取舍，不能同时保证或取得均衡。表 2 分析对比了基于分布式架构的隐私保护方案。

### 3.3 协作式架构的隐私保护方案

协作式定位系统中用户之间相互通信传递各自的位置和测量值等信息，具有严重的隐私泄露风险，但是隐私保护相关研究相对较少[11]。已有工作中对协作式定位中用户的隐私保护侧重于其匿名性的保持，即无法将测量信息、位置信息或定位结果链接到具体的用户身份，保护参与者的隐私。

文献[76-77]中提出 2 种基于匿名属性凭证的协议，实现了在协作式室内定位系统中保护用户隐私的目标。系统中每个用户拥有其身份的有效凭证，并通过蓝牙广播其位置信息和关于其身份凭证的证明信息，以协助其他用户定位。待定位的用户验证其他用户的凭证，并在通过验证后利用广播中的位置信息辅助自身定位。方案利用零知识证明实现匿名属性凭证的构造、展示和验证算法，使待定位的用户不需要获知信息源的身份和属性的情况下验证其合法性，且位置数据与身份凭证的证明无法链接，实现了匿名状态下位置信息的交换，保护了用户隐私。

文献[78]介绍的方案基于数据库匹配定位算法。系统中各个用户拥有局部数据库，由用户设备组成的定位网络将待定位用户的定位请求转发到合适的位置提供者，再将位置提供者计算的定位结果返回给请求者。方案同样保护参与者的匿名性，即网络中的任何节点（用户）无法获知定位请求者和位置提供者的身份。为了实现位置提供者的匿名，方案构建了层级的结构，将同一层级下的多个位置提供者构成一个匿名域。为了保护位置请求者的身份，方案利用了洋葱路由（ToR, the onion routing）协议[79]，将数据包使用路径节点的公钥逐层加密后发送到下一节点，路径节点进行最外层解密后继续转发，最终到达目标节点，从而保证任何节点都无法得知数据包的来源，实现了定位请求者的匿名。

### 3.4 云定位的隐私保护方案

与集中式定位架构中定位服务商对定位数据库和定位过程的绝对控制不同，云定位是将定位资源和定位算法外包到不可控的云服务提供商，拥有

**表 2 基于分布式架构的隐私保护方案对比**

| 安全技术 | 方案 | 计算开销 | 通信开销 | 隐私保护度 | 定位精度 |
|---|---|---|---|---|---|
| 信息隐藏技术 | 文献[10]中协议 1 | 低 | 低 | Level-Ⅰ | 不影响精度 |
| | 文献[10]中协议 2 | 低 | 中 | Level-Ⅱ | |
| | 文献[9] | 低 | 中 | Level-Ⅱ | |
| | 文献[66] | 低 | 中 | Level-Ⅱ | |
| | 文献[67] | 低 | 中 | Level-Ⅱ | |
| | 文献[68] | 低 | 中 | Level-Ⅱ | |
| | 文献[70,72-73] | 低 | 中 | Level-Ⅰ | |
| 同态加密技术 | 文献[74] | 高 | 高 | Level-Ⅲ | |
| | 文献[10]中协议 3 | 高 | 高 | Level-Ⅲ | |
| 安全多方计算 | 文献[75] | 高 | 高 | Level-Ⅲ | |

“诚实而好奇”的执行环境[80-82]。云环境下的室内定位方案需要额外考虑定位资源信息在云环境下的安全保护问题，这导致了传统的隐私保护方案在云定位场景下的不适用。例如从表 1 可以看出，其定位数据库信息大多处于明文和未加保护的状态，这足以满足集中式定位系统的隐私保护需求，即 Level-Ⅱ的隐私保护度，然而基于云的室内定位服务采用存储和计算任务外包的服务模式[83-87]，造成定位资源拥有者（定位服务商）和定位计算承担者（云服务提供商）的分离，并且执行定位计算的 CSP 是半可信的实体。因此适于集中式架构的隐私保护室内定位方案已不能满足云环境下隐私保护的需求。

云定位的隐私保护问题可以归纳为如何在不可信的环境下实现位置估计算法，且同时保证算法的输入（测量信息、定位数据库）和输出（定位结果）的隐私。文献[88]设计的云环境隐私保护的优化协议可以应用于云定位的场景。方案基于部分同态加密，各定位锚点将测量信息先后使用用户公钥和云端公钥进行两次加密后发送给云环境；后者在一次解密后对密文数据应用梯度下降算法，得到位置估计结果的密文。方案在云端实现定位的同时保护输入和输出信息的隐私性。然而利用同态加密在密文上迭代计算会产生巨大的计算开销。文献[89]使用随机矩阵拼接和相乘加密的方法实现了轻量级的隐私保护定位方案。方案中用户为 4 个定位锚点生成特定维度且满足特定等量关系的随机矩阵用于隐藏锚点的位置坐标和测量信息；各个锚点将隐私的坐标值和测量值与随机矩阵进行拼接并相乘后发送到云服务器，从而向服务器隐藏隐私信息；云服务器在随机矩阵上计算得到的定位结果中融合了用户设定的随机值，保护了定位结果的隐私性。方案具有较高的计算效率，但是矩阵乘法的线性性质可能降低方案的安全性。

文献[3]提出了云环境下基于内积函数加密的 TDoA 隐私保护定位方案，针对云环境下的隐私威胁设计了包含三方实体的隐私保护模型。方案将定位算法分解为向量内积的基本运算，利用内积函数加密机制实现了测量信息和定位资源信息的安全保护以及定位结果的安全计算，并结合 $k$ 匿名机制增强定位结果的安全性。方案中定位服务商在离线阶段将锚点信息利用内积函数加密后发送到云端存储；用户将在线阶段的测量信息加密后发送到云端请求定位服务；定位服务器利用解密算法得到测量向量和锚点信息之间的密文，进而得到定位结果。文献[34]设计了可以应用于外包场景（云环境）的隐私保护室内定位方案 PILOT。其中不可信的外包服务器在定位过程中只能得到定位数据库、测量信息和定位结果的份额，而无法恢复原始信息，实现了定位资源信息的保护。方案需要 2 个不共谋的服务器，这在实际环境尤其是云环境下难以满足，因此也就限制了方案在云环境下的应用。

除了在数据层加密保护，另一种实现云环境下隐私保护定位的方法是物理隔离。文献[90]利用软件防护扩展（SGX, software guard extension）在云环境下构建可信执行环境，防止定位数据的泄露，并利用 SGX 提供的远程证明机制实现用户与可信执行环境的安全连接和数据交互。表 3 总结了云环境下隐私保护定位方案的安全技术和性能评价指标。从表 3 中可以看到，这些方案同时保护测量信息、数据库信息和定位结果的安全性，即具有 Level-Ⅲ的隐私保护度，从而满足云环境下室内定位系统对隐私保护的需求。

最后，表 4 总结了各种安全技术的常用场景、隐私保护度、计算/通信开销、定位精度。从表 4 中

**表 3**　　**云环境下隐私保护定位方案的安全技术和性能评价指标**

| 文献 | 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 | | |
| 文献[88] | 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 |
| 文献[89] | 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 |
| 文献[3] | 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 |
| 文献[34] | 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 |
| 文献[90] | 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 4 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 | 可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 |

可以看到，每种技术有其不同的优缺点和性能表现，没有一种技术能解决所有的隐私问题。如何根据应用场景和隐私需求，设计满足服务需求和资源开销的隐私保护方案是这一领域重要的研究方向。

## 4 结束语

室内定位服务在为用户提供便利的同时，也具有严重的隐私泄露风险。本文回顾了近年来室内定位隐私保护的研究进展，介绍了常用的室内定位技术、实现架构及其威胁模型，总结了应用于室内定位隐私保护的安全技术，分类介绍了不同架构下隐私保护方案的流程，并分析了其隐私保护度、计算通信开销和定位精度等指标。总体来说，各种方案都在安全性、效率和精度上有所取舍，难以兼顾或者均衡。现有的研究尚未解决所有的问题，因此结合当前的研究进展，未来的研究工作可以关注如下几个方面。

1) 轨迹信息的保护。用户在连续定位过程中的测量信息、计算中间值和定位结果都具有较强时空关联性，而目前的方案考虑单次定位中隐私信息的保护，对多次定位之间的信息关联考虑不足，因此面对时空关联攻击常常具有脆弱性。该问题在基于匿名和假位置的 PPIL 方案中尤其明显，因为连续定位过程中位置的相关性可以使攻击者容易从一个匿名域的多个位置中排除不可能的结果，降低定位结果的隐私保护性能。此时，连续的时空关联攻击几乎必然导致定位结果和轨迹信息的泄露。因此需要考虑连续定位过程中时空关联信息，实现轨迹保护的室内定位。

2) 高效定位的实现。现有方案主要针对小规模的定位场景进行设计和验证，在大规模数据库上，方案的效率和可用性将急剧降低。例如基于 Wi-Fi 指纹匹配的定位方案本质上是数据检索问题，现有方案是在数据库中进行线性搜索，导致定位耗时随数据库大小线性增长。因此通过将高效的数据检索方案与隐私保护的机制相结合，可以设计高效、可扩展的隐私保护室内定位方案。但如何在隐私保护的前提下，利用有限的信息实现安全高效检索是一大挑战。

3) 云环境下的隐私保护定位方案。云定位已成为主流的趋势，但目前适于云环境下的隐私保护方案还较少。云环境下的隐私保护方案具有更加复杂的威胁模型、海量的定位资源信息、高并发的定位请求，对安全性和效率提出了更高的要求，也为方案的设计和优化带来了较大的挑战。

## 参考文献：

[1] WEI G, CONGYI H, WANYANG X, et al. Research progress and prospect of indoor navigation and positioning technology[J]. Journal of Navigation and Positioning, 2019, 7(1): 10-17.

[2] DAYU Y A N, WEI S, XUDAN W, et al. Review of development status of indoor location technology in China[J]. Journal of Navigation and Positioning, 2019, 7(4): 5-12.

[3] WANG Z, XU Y, YAN Y, et al. Privacy-preserving indoor localization based on inner product encryption in a cloud environment[J]. Knowledge-Based Systems, 2022, 239: 108005.

[4] 刘公绪, 史凌峰. 室内导航与定位技术发展综述[J]. 导航定位学报, 2018, 6(2): 7-14.
LIU G X, SHI L F. An overview about development of indoor navigation and positioning technology[J]. Journal of Navigation and Positioning, 2018, 6(2): 7-14.

[5] GILLETTE M D, SILVERMAN H F. A linear closed-form algorithm for source localization from time-differences of arrival[J]. IEEE Signal Processing Letters, 2008, 15: 1-4.

[6] BAHL P, PADMANABHAN V N. RADAR: an in-building RF-based

user location and tracking system[C]//Proceedings of Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Piscataway: IEEE Press, 2002: 775-784.

[7] YOUSSEF M, AGRAWALA A. The Horus WLAN location determination system[C]//Proceedings of the 3rd International Conference on Mobile Systems, Applications, and Services. New York: ACM Press, 2005: 205-218.

[8] LI H, SUN L M, ZHU H J, et al. Achieving privacy preservation in Wi-Fi fingerprint-based localization[C]//Proceedings of 2014 IEEE Conference on Computer Communications. Piscataway: IEEE Press, 2014: 2337-2345.

[9] SHI X F, WU J F. To hide private position information in localization using time difference of arrival[J]. IEEE Transactions on Signal Processing, 2018, 66(18): 4946-4956.

[10] SHU T, CHEN Y Y, YANG J, et al. Multi-lateral privacy-preserving localization in pervasive environments[C]//Proceedings of 2014 IEEE Conference on Computer Communications. Piscataway: IEEE Press, 2014: 2319-2327.

[11] PASCACIO P, CASTELEYN S, TORRES-SOSPEDRA J, et al. Collaborative indoor positioning systems: a systematic review[J]. Sensors, 2021, 21(3): 1002.

[12] YANG Z, JÄRVINEN K. Modeling privacy in Wi-Fi fingerprinting indoor localization[C]//Proceedings of International Conference on Provable Security. Piscataway: IEEE Press, 2018: 329-346.

[13] ZHANG G L, ZHANG A Q, ZHAO P, et al. Lightweight privacy-preserving scheme in Wi-Fi fingerprint-based indoor localization[J]. IEEE Systems Journal, 2020, 14(3): 4638-4647.

[14] RIVEST R L, DERTOUZOS M L, ADLEMAN L. On data banks and privacy homomorphisms[J]. Foundations of secure computation, 1978, 25: 222-233.

[15] ELGAMAL T. A public key cryptosystem and a signature scheme based on discrete logarithms[J]. IEEE Transactions on Information Theory, 1985, 31(4): 469-472.

[16] PAILLIER P. Public-key cryptosystems based on composite degree residuosity classes[C]//Advances in Cryptology−EUROCRYPT ’99. Berlin: Springer, 2007: 223-238.

[17] GENTRY C. Fully homomorphic encryption using ideal lattices[C]// Proceedings of the Forty-first Annual ACM Symposium on Theory of Computing. New York: ACM Press, 2009: 169-178.

[18] MICROSOFT. Microsoft SEAL (release 4.1)[R]. 2023.

[19] YAO A C. Protocols for secure computations[C]//Proceedings of the 23rd Annual Symposium on Foundations of Computer Science. Piscataway: IEEE Press, 2008: 160-164.

[20] GOLDREICH O, MICALI S, WIGDERSON A. How to play any mental game, or a completeness theorem for protocols with honest majority[C]//Providing Sound Foundations for Cryptography: On the Work of Shafi Goldwasser and Silvio Micali. New York: ACM Press, 2019: 307-328.

[21] GOLDWASSER S. Multi party computations: past and present[C]//Proceedings of the Sixteenth Annual ACM Symposium on Principles of Distributed Computing. New York: ACM Press, 1997: 1-6.

[22] KOLESNIKOV V, SCHNEIDER T. Improved garbled circuit: free XOR gates and applications[C]//International Colloquium on Automata, Languages, and Programming. Berlin: Springer, 2008: 486-498.

[23] FIAT A, SHAMIR A. How to prove yourself: practical solutions to identification and signature problems[C]//Lecture Notes in Computer Science. Berlin: Springer, 1987: 186-194.

[24] RABIN M O. How to exchange secrets with oblivious transfer[R]. 1981.

[25] EVEN S, GOLDREICH O, LEMPEL A. A randomized protocol for signing contracts[J]. Communications of the ACM, 1985, 28(6): 637-647.

[26] NAOR M, PINKAS B. Efficient oblivious transfer protocols[C]//Proceedings of the Twelfth Annual ACM-SIAM Symposium on Discrete Algorithms. New York: ACM Press, 2001: 448-457.

[27] AIELLO B, ISHAI Y, REINGOLD O. Priced oblivious transfer: how to sell digital goods[C]//Advances in Cryptology−EUROCRYPT 2001. Berlin: Springer, 2001: 119-135.

[28] ISHAI Y, KILIAN J, NISSIM K, et al. Extending oblivious transfers efficiently[C]//Advances in Cryptology−CRYPTO 2003. Berlin: Springer, 2003: 145-161.

[29] LINDELL A Y. Efficient fully-simulatable oblivious transfer[C]// Topics in Cryptology−CT-RSA 2008. Berlin: Springer, 2008: 52-70.

[30] DEMMLER D, SCHNEIDER T, ZOHNER M. ABY - a framework for efficient mixed-protocol secure two-party computation[C]// Proceedings of 2015 Network and Distributed System Security Symposium. Reston: Internet Society, 2015: 8-11.

[31] HUANG Y, EVANS D, KATZ J, et al. Faster secure two-party computation using garbled circuits[C]//USENIX Security Symposium. Berkeley: USENIX Association, 2011: 35.

[32] LIU C, WANG X S, NAYAK K, et al. ObliVM: a programming framework for secure computation[C]//Proceedings of 2015 IEEE Symposium on Security and Privacy. Piscataway: IEEE Press, 2015: 359-376.

[33] MOOD B, GUPTA D, CARTER H, et al. Frigate: a validated, extensible, and efficient compiler and interpreter for secure computation[C]//Proceedings of 2016 IEEE European Symposium on Security and Privacy (EuroS&P). Piscataway: IEEE Press, 2016: 112-127.

[34] JÄRVINEN K, LEPPÄKOSKI H, LOHAN E S, et al. PILOT: practical privacy-preserving indoor localization using outsourcing[C]// Proceedings of 2019 IEEE European Symposium on Security and Pri-

vacy (EuroS&P). Piscataway: IEEE Press, 2019: 448-463.

[35] DWORK C. Automata, languages and programming[M]. Berlin: Springer, 2006.

[36] DWORK C, ROTH A. The algorithmic foundations of differential privacy[J]. Foundations and Trends in Theoretical Computer Science, 2013, 9(3/4): 211-407.

[37] BHASKAR R, BHOWMICK A, GOYAL V, et al. Noiseless database privacy[C]//International Conference on the Theory and Application of Cryptology and Information Security. Berlin: Springer, 2011: 215-232.

[38] DWORK C. Differential privacy: a survey of results[C]//International Conference on Theory and Applications of Models of Computation. Berlin: Springer, 2008: 1-19.

[39] DWORK C, LEI J. Differential privacy and robust statistics[C]//Proceedings of the Forty-first Annual ACM Symposium on Theory of Computing. New York: ACM Press, 2009: 371-380.

[40] DWORK C, NAOR M, REINGOLD O, et al. On the complexity of differentially private data release: efficient algorithms and hardness results[C]//Proceedings of the Forty-first Annual ACM Symposium on Theory of Computing. New York: ACM Press, 2009: 381-390.

[41] SCHAUER L, DORFMEISTER F, WIRTH F. Analyzing passive Wi-Fi fingerprinting for privacy-preserving indoor-positioning[C]// Proceedings of 2016 International Conference on Localization and GNSS (ICL-GNSS). Piscataway: IEEE Press, 2016: 1-6.

[42] 张钊, 华景煜. 基于指纹识别的室内定位中的隐私保护[J]. 南京信息工程大学学报(自然科学版), 2017, 9(5): 551-559.
ZHANG Z, HUA J Y. Privacy-preserving in fingerprinting-based indoor localization[J]. Journal of Nanjing University of Information Science & Technology (Natural Science Edition), 2017, 9(5): 551-559.

[43] ESHUN S N, PALMIERI P. A privacy-preserving protocol for indoor Wi-Fi localization[C]//Proceedings of the 16th ACM International Conference on Computing Frontiers. New York: ACM Press, 2019: 380-385.

[44] YANG Z, JÄRVINEN K. The death and rebirth of privacy-preserving Wi-Fi fingerprint localization with paillier encryption[C]//Proceedings of 2018 IEEE Conference on Computer Communications. Piscataway: IEEE Press, 2018: 1223-1231.

[45] ZHANG T, CHOW S S M, ZHOU Z, et al. Privacy-preserving Wi-Fi fingerprinting indoor localization[C]//International Workshop on Security. Cham: Springer, 2016: 215-233.

[46] NIEMINEN R, JÄRVINEN K. Practical privacy-preserving indoor localization based on secure two-party computation[J]. IEEE Transactions on Mobile Computing, 2021, 20(9): 2877-2890.

[47] SUN M X, DONG X J, WU F, et al. An efficient privacy-preserving fingerprint-based localization scheme employing oblivious transfer[C]//International Conference on Mobile Ad-Hoc and Sensor Networks. Singapore: Springer, 2018: 110-132.

[48] ZIEGELDORF J H, VIOL N, HENZE M, et al. POSTER: privacy-preserving indoor localization[J]. arXiv Preprint, arXiv: 1410.3270, 2014.

[49] VIOL N, BITSCH L J Á, WIRTZ H, et al. Hidden Markov model-based 3D path-matching using raytracing-generated Wi-Fi models[C]//Proceedings of 2012 International Conference on Indoor Positioning and Indoor Navigation (IPIN). Piscataway: IEEE Press, 2013: 1-10.

[50] HU Z H, LI Y Z, JIANG G S, et al. PriHorus: privacy-preserving RSS-based indoor positioning[C]//Proceedings of 2022 IEEE International Conference on Communications. Piscataway: IEEE Press, 2022: 5627-5632.

[51] BEETS C V D, NIEMINEN R, SCHNEIDER T. FAPRIL: towards faster privacy-preserving fingerprint-based localization[C]//Proceedings of the 19th International Conference on Security and Cryptography. Piscataway: IEEE Press, 2022: 1-10.

[52] LI S J, LI H, SUN L M. Privacy-preserving crowd sourced site survey in Wi-Fi fingerprint-based localization[J]. EURASIP Journal on Wireless Communications and Networking, 2016(1): 1-9.

[53] ZHANG X J, HE F C, CHEN Q, et al. A differentially private indoor localization scheme with fusion of Wi-Fi and bluetooth fingerprints in edge computing[J]. Neural Computing and Applications, 2022, 34(6): 4111-4132.

[54] ZHU Y J, WANG Y, LIU Q Y, et al. Wi-Fi fingerprint releasing for indoor localization based on differential privacy[C]//Proceedings of 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC). Piscataway: IEEE Press, 2018: 1-6.

[55] ZHANG X J, CHEN Q, PENG X H, et al. Differential privacy-based indoor localization privacy protection in edge computing[C]// Proceedings of 2019 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI). Piscataway: IEEE Press, 2020: 491-496.

[56] WANG Y F, HUANG M J, JIN Q, et al. DP3: a differential privacy-based privacy-preserving indoor localization mechanism[J]. IEEE Communications Letters, 2018, 22(12): 2547-2550.

[57] ZHAO P, JIANG H B, LUI J C S, et al. P3-LOC: a privacy-preserving paradigm-driven framework for indoor localization[J]. IEEE/ACM Transactions on Networking, 2018, 26(6): 2856-2869.

[58] ALIKHANI N, MOGHTADAIEE V, SAZDAR A M, et al. A privacy preserving method for crowdsourcing in indoor fingerprinting localization[C]//Proceedings of 2018 8th International Conference on Computer and Knowledge Engineering (ICCKE). Piscataway: IEEE Press, 2018: 58-62.

[59] SAZDAR A M, ALIKHANI N, GHORASHI S A, et al. Privacy preserving in indoor fingerprint localization and radio map expansion[J]. Peer-to-Peer Networking and Applications, 2021, 14(1): 121-134.

[60] 王宇航, 张宏莉, 余翔湛. KAP: 一种面向定位服务的位置隐私保护方法[J]. 通信学报, 2014, 35(11): 182-190.
WANG Y H, ZHANG H L, YU X Z. KAP: location privacy-preserving approach in location services[J]. Journal on Communications, 2014, 35(11): 182-190.

[61] HOU M, ZHANG H L, WANG Y H. OFC: an approach for protecting location privacy from location provider in location-based services[C]//Proceedings of 2018 IEEE Third International Conference on Data Science in Cyberspace (DSC). Piscataway: IEEE Press, 2018: 917-922.

[62] 金军. 基于 Wi-Fi 指纹室内定位隐私保护研究[D]. 武汉: 华中科技大学, 2017.
JIN J. Research on privacy protection of indoor location based on Wi-Fi fingerprint[D]. Wuhan: Huazhong University of Science and Technology, 2017.

[63] LI H, HE Y H, CHENG X Z, et al. A lightweight location privacy-preserving scheme for Wi-Fi fingerprint-based localization[C]//Proceedings of 2016 International Conference on Identification, Information and Knowledge in the Internet of Things (IIKI). Piscataway: IEEE Press, 2018: 525-529.

[64] ZHAO P, LIU W W, ZHANG G L, et al. Preserving privacy in Wi-Fi localization with plausible dummy locations[J]. IEEE Transactions on Vehicular Technology, 2020, 69(10): 11909-11925.

[65] KONSTANTINIDIS A, CHATZIMILIOUDIS G, ZEINALIPOUR-YAZTI D, et al. Privacy-preserving indoor localization on smartphones[J]. IEEE Transactions on Knowledge and Data Engineering, 2015, 27(11): 3042-3055.

[66] WANG G H, HE J P, SHI X F, et al. Analyzing and evaluating efficient privacy-preserving localization for pervasive computing[J]. IEEE Internet of Things Journal, 2018, 5(4): 2993-3007.

[67] ZHAO H Y, YAN J, LUO X Y, et al. Privacy preserving solution for the asynchronous localization of underwater sensor networks[J]. IEEE/CAA Journal of Automatica Sinica, 2020, 7(6): 1511-1527.

[68] SHI X F, TONG F, ZHANG W A, et al. Resilient privacy-preserving distributed localization against dishonest nodes in Internet of things[J]. IEEE Internet of Things Journal, 2020, 7(9): 9214-9223.

[69] KHAN U A, KAR S, MOURA J M F. Distributed sensor localization in random environments using minimal number of anchor nodes[J]. IEEE Transactions on Signal Processing, 2009, 57(5): 2000-2016.

[70] LI Y J, WANG G H, ZUO F. Efficient privacy preserving single anchor localization using noise-adding mechanism for Internet of things[C]//International Conference on Web Information Systems and Applications. Cham: Springer, 2021: 261-273.

[71] WANG G H, XU Y F, TONG F, et al. Modeling and analyzing single anchor localization for Internet of things[C]//Proceedings of 2019 IEEE International Conference on Communications (ICC). Piscataway: IEEE Press, 2019: 1-6.

[72] ZUO F Y, LI Y J, WANG G H, et al. Towards accurate and privacy-preserving localization using anchor quality assessment in Internet of things[J]. Future Generation Computer Systems, 2023, 148: 524-537.

[73] WANG G H, ZHANG X Y, LI Y J. Design and analysis of privacy-preserving localization assisted by reconfigurable intelligent surface for Internet of things[C]//Proceedings of the 2023 11th International Conference on Communications and Broadband Networking. New York: ACM Press, 2023: 1-7.

[74] ALANWAR A, SHOUKRY Y, CHAKRABORTY S, et al. PrOLoc: resilient localization with private observers using partial homomorphic encryption[C]//Proceedings of the 16th ACM/IEEE International Conference on Information Processing in Sensor Networks. New York: ACM Press, 2017: 41-52.

[75] HUSSAIN S U, KOUSHANFAR F. Privacy preserving localization for smart automotive systems[C]//Proceedings of the 53rd Annual Design Automation Conference. New York: ACM Press, 2016: 1-6.

[76] CASANOVA-MARQUÉS R, PASCACIO P, HAJNY J, et al. Anonymous attribute-based credentials in collaborative indoor positioning systems[C]//Proceedings of the 18th International Conference on Security and Cryptography. Piscataway: IEEE Press, 2021: 791-797.

[77] CASANOVA-MARQUÉS R, TORRES-SOSPEDRA J, HAJNY J, et al. Maximizing privacy and security of collaborative indoor positioning using zero-knowledge proofs[J]. Internet of Things, 2023, 22: 100801.

[78] SADHU V, ZONOUZ S, SRITAPAN V, et al. CollabLoc: privacy-preserving multi-modal collaborative mobile phone localization[J]. IEEE Transactions on Mobile Computing, 2021, 20(1): 104-116.

[79] DINGLEDINE R, MATHEWSON N, SYVERSON P. Tor: the second-generation onion router[C]//Proceedings of the 13th USENIX Security Symposium. Berkeley: USENIX Association, 2004: 1-17.

[80] ZAFARI F, GKELIAS A, LEUNG K K. A survey of indoor localization systems and technologies[J]. IEEE Communications Surveys & Tutorials, 2019, 21(3): 2568-2599.

[81] OBEIDAT H, SHUAIEB W, OBEIDAT O, et al. A review of indoor localization techniques and wireless technologies[J]. Wireless Personal Communications, 2021, 119(1): 289-327.

[82] CHEN R, CHEN L. Indoor positioning with smartphones: the state-of-the-art and the challenges[J]. Acta Geodaetica et Cartographica Sinica, 2017, 46(10): 1316-1326.

[83] 施闯, 章红平, 辜声峰, 等. 云定位技术及云定位服务平台[J]. 武汉大学学报(信息科学版), 2015, 40(8): 995-999.
SHI C, ZHANG H P, GU S F, et al. Technology of cloud positioning

and its platform for positioning service[J]. Geomatics and Information Science of Wuhan University, 2015, 40(8): 995-999.

[84] 张传明, 杨玲玲, 刘敏, 等. 面向海量智能终端的云定位系统设计与实现[J]. 武汉大学学报(信息科学版), 2021, 46(12): 1872-1880.
ZHANG C M, YANG L L, LIU M, et al. Design and implementation of cloud positioning system for massive intelligent terminals[J]. Geomatics and Information Science of Wuhan University, 2021, 46(12): 1872-1880.

[85] KHANH T T, NGUYEN V, PHAM X Q, et al. Wi-Fi indoor positioning and navigation: a cloudlet-based cloud computing approach[J]. Human-Centric Computing and Information Sciences, 2020, 10(1): 1-26.

[86] HAO X U, JINZHONG B E I, DEHAI L I, et al. Research on design and application of indoor location service cloud platform[J]. Journal of Navigation and Positioning, 2021, 9(5): 126-133.

[87] 刘霄, 秘金钟, 李得海, 等. 室内位置云平台关键技术研究[J]. 测绘科学, 2019, 44(6): 79-83, 144.
LIU X, BEI J Z, LI D H, et al. Research on the key technologies of indoor location cloud platform[J]. Science of Surveying and Mapping, 2019, 44(6): 79-83, 144.

[88] SHOUKRY Y, GATSIS K, ALANWAR A, et al. Privacy-aware quadratic optimization using partially homomorphic encryption[C]//Proceedings of 2016 IEEE 55th Conference on Decision and Control (CDC). Piscataway: IEEE Press, 2016: 5053-5058.

[89] LIU S S, YAN Z. Efficient privacy protection protocols for 5G-enabled positioning in industrial IoT[J]. IEEE Internet of Things Journal, 2022, 9(19): 18527-18538.

[90] YAN Z, QIAN X R, LIU S S, et al. Privacy protection in 5G positioning and location-based services based on SGX[J]. ACM Transactions on Sensor Networks, 2022, 18(3): 1-19.

## [作者简介]

**王志恒**（1996− ），男，河南汝州人，武汉大学博士生，主要研究方向为安全定位技术、云计算安全等。

**徐彦彦**（1974− ），女，河南信阳人，博士，武汉大学教授，主要研究方向为多媒体通信、云计算安全等。