基于 Wi-Fi 指纹且计算外包的室内定位隐私保护方案

张应辉[1]，张思睿[1]，赵秋霞[2]，郑晓坤[2]，曹进[3]

（1. 西安邮电大学网络空间安全学院，陕西 西安 710121；2. 青海师范大学计算机学院，青海 西宁 810016；
3. 西安电子科技大学网络与信息安全学院，陕西 西安 710126）

摘 要：为了解决室内定位中用户和服务器双方的隐私保护问题，提出了一种在使用 Paillier 加密的过程中将部分计算外包给云服务器的方案，这不仅保护了用户和定位服务器的隐私，而且避免了产生过大的计算和通信开销。该方案的主要思想是服务器先在离线阶段建立指纹数据库，在线阶段用户将 *k* 匿名算法和 Paillier 加密结合，将加密后的 Wi-Fi 指纹发送给定位服务器，服务器对接收到的 Wi-Fi 指纹和数据库指纹进行聚合处理，然后外包给云服务器进行解密和距离计算，最终得到定位结果。理论分析和实验结果表明了所提方案的安全性、有效性和实用性。

关键词：Wi-Fi 指纹；计算外包；云服务；Paillier 加密

中图分类号：TP309

文献标志码：A

DOI: 10.11959/j.issn.1000−436x.2024051

Privacy-preserving indoor localization scheme based on Wi-Fi fingerprint with outsourced computing

ZHANG Yinghui[1], ZHANG Sirui[1], ZHAO Qiuxia[2], ZHENG Xiaokun[2], CAO Jin[3]

1. School of Cyberspace Security, Xi'an University of Posts & Telecommunications, Xi'an 710121, China
2. The College of Computer, Qinghai Normal University, Xining 810016, China
3. School of Cyber Engineering, Xidian University, Xi'an 710126, China

Abstract: To solve the privacy-preserving problem of both the user and the server in indoor positioning, outsourcing part of the calculation to cloud server in the process of using Paillier encryption was considered. The scheme not only protected the privacy of the user and the positioning server, but also avoided excessive computing and communication overhead. The main idea of the scheme was that the fingerprint database in the offline stage was established by the server firstly. The *k*-anonymity algorithm was combined with Paillier encryption in the online stage by the user, and the encrypted Wi-Fi fingerprints were sent to the positioning server. An aggregation of the received Wi-Fi fingerprints and database fingerprints were performed by the server. Then they were outsourced to the cloud server for decryption and distance calculation by the positioning server. Finally, the positioning result was obtained. Theoretical analysis and experimental results show that the proposed scheme is safe, effective and practical.

Keywords: Wi-Fi fingerprint, outsourced computing, cloud service, Paillier encryption

---

收稿日期：2023−11−02；**修回日期：**2023−12−29

基金项目：国家自然科学基金资助项目（No.62072369, No.62072371）；陕西高校青年创新团队基金资助项目；陕西省特支计划青年拔尖人才支持计划基金资助项目；陕西省重点研发计划基金资助项目（No.2021ZDLGY06-02, No.2020ZDLGY08-04）；陕西省技术创新引导计划基金资助项目（No.2023-YD-CGZH-31）

Foundation Items: The National Natural Science Foundation of China (No.62072369, No.62072371), The Youth Innovation Team of Shaanxi Universities, The Shaanxi Special Support Program Youth Top-notch Talent Program, The Key Research and Development Program of Shaanxi Province (No.2021ZDLGY06-02, No.2020ZDLGY08-04), The Technology Innovation Leading Program of Shaanxi Province (No.2023-YD-CGZH-31)

0 引言

随着智能手机等移动智能设备的兴起，位置数据已经成为一种重要的资产。从传统的导航和地图应用程序到社交媒体和定向广告，位置数据被用于各种基于位置的服务中[1-4]。任何基于位置的服务的一个明显的先决条件都是定位，即获取客户端的物理位置。在户外环境中，定位主要是基于全球导航卫星系统（GNSS, global navigation satellite system），如GPS或北斗卫星导航系统。然而，GNSS卫星信号非常弱，在进行定位的过程中可能被障碍物阻挡，导致不能提供良好的定位服务，尤其是在室内环境中。因此，在室内环境中，需要其他定位技术来提供定位服务。常见的室内定位技术有基于Wi-Fi指纹的定位技术、红外线定位技术、频射识别定位技术、蓝牙定位技术、ZigBee定位技术、超宽带定位技术[5-8]等。其中，基于Wi-Fi指纹的定位技术是应用最多的，其原因是许多室内环境已经部署了广泛的Wi-Fi设备，在进行定位服务时可以使用现有的基础设施，从而降低成本。与此同时，随着室内定位服务的日益普及，人们对隐私保护有了更高的要求，所以在进行定位服务的过程中还要保护客户端的位置隐私和服务器端的数据隐私。

在基于Wi-Fi指纹的室内定位服务中，用户想要知道自己所处的位置，就要通过计算当前位置采样的接收信号强度（RSS, received signal strength）和若干个参考点的RSS之间的距离，来获取用户的位置坐标。在这个过程中，用户公开了自己的RSS，就会被不受信任的室内定位系统（IPS, indoor positioning system）或其他恶意攻击者获取，从而泄露用户的位置隐私，用户敏感的个人信息将有可能被披露并以恶意的方式使用[9-11]。与此同时，定位过程中存在恶意用户通过对IPS发送多次定位请求以获取整个指纹数据库，侵害服务器的数据隐私，对IPS造成财产的损失。因此，在进行定位服务的过程中保护用户和IPS双方的隐私是十分必要的。然而具有隐私保护的室内定位方案通常伴随着较高的计算和通信开销。针对此问题，计算外包是一种好的解决方法。

1 相关工作

1.1 现存工作

目前，针对室内定位中的隐私保护主要采用基于密码学的方案。Li等[12]提出了第一个通过加密测量的Wi-Fi RSS保护隐私的方案，即在用户端使用同态加密算法处理测量的Wi-Fi RSS，然后通过随机选择多个接入点（AP, access point），在服务器端处理用户的定位请求。Wang等[13]结合了同态加密和模糊逻辑来保护Wi-Fi定位的隐私。Shu等[14]利用Paillier加密系统和不经意传输构建了一个定位协议，该协议根据其他移动设备的位置来确定用户的位置。Konstantinidis等[15]在提出的隐私保护室内定位（PPIL, privacy-preserving indoor localization）方案中使用了k匿名算法，确保了在一组k个客户端中，用户的身份难以被识别。Li等[16]研究利用差分隐私向参与者的指纹数据中注入噪声，来保护位置隐私。Järvinen等[17]的方案结合了不同的安全两方计算协议，并为PPIL设计了尺寸和深度优化的电路。具体来说，构建了独立的高效电路构建块：单指令多数据，能够忽略访问低电路深度的阵列，并选择小电路尺寸的k个最近邻。Zhao等[18]提出了可信虚拟位置保护算法，通过利用合理的虚拟位置来加强虚拟技术，以抵御攻击。Hu等[19]提出了基于RSS和部分同态加密的方案PriHorus，该方案依赖于最大似然估计，而不是经典的K最近邻（KNN）算法。Li等[20]将基于位置的服务（LBS）与区块链技术相结合，提出了一种利用基于区块链的空天地一体化网络（SAGIN）系统来提高位置数据管理的安全性和信任度的方案。该方案可以在提高位置数据管理效率的同时保护用户数据隐私。Zhang等[21]提出了一种在边缘计算中使用差分隐私指纹融合半监督极限学习机进行室内定位的方案，称为Adp-FSELM，这种融合式训练模型依赖于边缘节点中的半可信聚合和大量参与者，且方案中引入多个实体。

以上方案主要存在3个问题：一是大多数方案只关注了用户侧的位置隐私，而没有考虑到IPS的数据隐私；二是定位过程中产生了很大的通信和计算开销；三是为了保护隐私，在数据中注入噪声，从而导致较大的定位误差，降低定位服务的质量。综上所述，研究隐私保护的轻量化室内定位技术是十分必要的，可以在保护隐私的同时减小通信和计算开销。

1.2 本文工作

为了解决上述问题，本文提出了一种将部分计算外包给云服务提供商（CSP, cloud service provider）的定位方案。该方案可以在减小开销的同时，保护用户和服务器的隐私。其主要思想是IPS在离

线阶段建立指纹数据库，用户在在线阶段采用 k 匿名的方法，将得到的 k 组 Wi-Fi 指纹经过 Paillier 加密后发送给 IPS，IPS 对加密的数据库指纹信息和接收到的加密数据进行聚合，然后发送给云服务提供商解密并计算距离。在此过程中，因为用户的指纹信息被 $k-1$ 组匿名信息隐藏并进行了加密，攻击者无法进行区分，所以用户的隐私得到了保护。服务器端的指纹数据库使用加密后的数据，并且位置检索阶段也是在服务器端完成，这就避免了数据的泄露。

2　预备知识

2.1　基于 Wi-Fi 指纹的室内定位

在众多室内定位的技术中，基于 Wi-Fi 指纹的室内定位是最常见且最受欢迎的。简单来说，定位的过程分为 2 个阶段：离线阶段和在线阶段。

离线阶段。IPS 建立数据库 $<i,(x_i,y_i),V_i=\{v_{i,j}\}_{j=1}^{N}>_{i=1}^{M}$，其中，$i$ 是索引，N 是接入点的数量，M 是测量点的数量，V_i 是 (x_i,y_i) 处的 Wi-Fi 指纹。

在线阶段。待定位的用户测量其 Wi-Fi 指纹 $V'=(v_1',v_2',\cdots,v_N')$，然后计算 V' 与服务器数据库中 V_i 之间的距离，得到用户的具体位置信息，完成一次定位工作。

2.2　Sφrensen 距离

本文方案使用 Sφrensen 距离计算方法。Sφrensen 距离基于 Manhattan 距离，由结果值的总和标准化得来。Sφrensen 距离计算式为

$$d_s=\frac{\sum_{i=1}^{N}|x_i-y_i|}{\sum_{i=1}^{N}(x_i+y_i)} \tag{1}$$

室内定位中常用的距离计算方法还有 Manhattan 距离、Euclidean 距离、Kumar-Hassebrook 距离等。但是 Torres-Sospedra 等[22]研究表明，这 3 种距离计算方法的成功率和准确度都不及 Sφrensen 距离，具体如表 1 所示。

表 1　4 种距离计算方法的成功率和误差

距离度量	成功率	误差/m
Manhattan	90.73%	7.06
Euclidean	92.71%	7.40
Kumar-Hassebrook	94.33%	7.00
Sφrensen	94.78%	6.86

2.3　Paillier 加密系统

Paillier 加密方案[23]是 Paillier 于 1999 年提出的一种加法同态概率公钥密码系统。该密码系统的使用步骤及性质如下所示。

密钥生成。设 p 和 q 是 2 个随机选择的大素数，满足 $\gcd\big(pq,(p-1)(q-1)\big)=1$。计算 $n=pq$，$\lambda=\mathrm{lcm}(p-1,q-1)$，$g=n+1$。公钥 $\mathrm{PK}=(n,g)$，私钥 $\mathrm{SK}=\lambda$。

加密。选择一个随机的 $r\in Z_n$，对于明文 m，使用式(2)计算密文 c，加密操作如下

$$c=E(m)=g^m r^n \bmod n^2 \tag{2}$$

解密。密文 c 的解密操作如下

$$m=D(c)=\frac{L(c^\lambda \bmod n^2)}{L(g^\lambda \bmod n^2)}\bmod n \tag{3}$$

Paillier 加密是一种满足加法同态和数乘同态的加密方法。对于明文 m_1,m_2 和常数 c，有

$$D\big(E(m_1)E(m_2)\bmod n^2\big)=(m_1+m_2)\bmod n \tag{4}$$

$$D\big(E(m_1)^k \bmod n^2\big)=km_1 \bmod n \tag{5}$$

2.4　敌手模型

本文方案同时考虑用户端的位置隐私和 IPS 的数据隐私。从用户的角度来看，攻击者有可能是好奇的 IPS，想要通过搜集用户的位置隐私来制定相应的营销策略，也有可能是外部的攻击者，想要通过售卖用户的位置信息来牟利。因而，Wi-Fi 定位系统在提供位置服务的过程中应该确保用户的位置隐私不被泄露。攻击者一般会通过以下 2 种方式获取用户的位置隐私。

1) 攻击者直接从查询中获取用户的位置信息。

2) 攻击者获取用户 Wi-Fi RSS，推断用户的位置信息。

从 IPS 的角度来看，攻击者可能是恶意用户，想要通过多次定位请求获取数据库来牟利。因而，在提供定位服务的过程中应防止 Wi-Fi 指纹数据库的泄露。攻击者一般会通过以下 2 种方式攻击服务提供商的数据库。

1) 攻击者得到一个与 IPS 的数据库完全相同 Wi-Fi 指纹数据库。

2) 攻击者得到一个与 IPS 的数据库 D 相似且定位精度相同的 Wi-Fi 指纹数库 D'。

3 具体方案

本文方案的系统架构如图 1 所示。离线阶段，IPS 对采样点的 Wi-Fi RSS 使用 Paillier 半同态加密算法进行加密，并建立指纹数据库。在线阶段，一个待定位的用户在自己当前位置测量从不同 AP 采样到的 Wi-Fi RSS，使用 Paillier 半同态加密算法进行加密，并将加密后的真实 RSS 和虚拟 RSS（通过 k 匿名技术生成，除用户外其他人无法进行区分）发送给 IPS 进行定位请求。在接收到用户的定位请求后，IPS 对自己数据库中的加密 RSS 和接收到的 RSS 进行初步处理，然后外包给 CSP 解密并计算 Sφrensen 距离，CSP 将计算结果返回给 IPS，IPS 使用 KNN 算法进行计算并从数据库中匹配对应的物理坐标，返回给用户，用户从中找出自己的真实位置。总体上，本文方案主要包括以下 4 个阶段。本文方案中涉及的符号说明如表 2 所示。

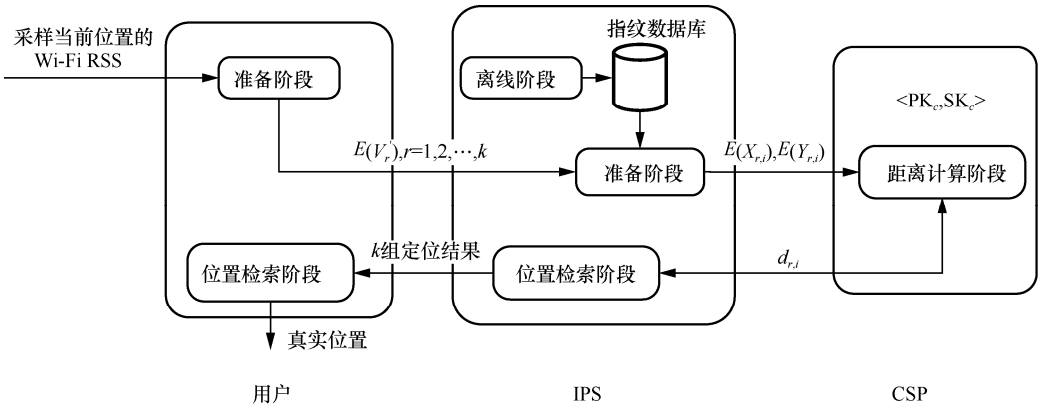

图 1 系统架构

表 2 符号说明

符号	说明
N	接入点的总数量
M	测量点的总数量
i	第 i 个测量点
j	第 j 个接入点
k	用户端发送的 k 组指纹
K	KNN 算法中的 K 个最近距离
r	用户 k 组指纹数据中的第 r 组
V_i	第 i 个测量点的 Wi-Fi 指纹
V_j	第 j 个 AP 测量到的 Wi-Fi RSS
V'	用户端测量到的 Wi-Fi 指纹
v'_j	用户第 j 个 AP 测量的 Wi-Fi RSS

离线阶段。IPS 在 M 个测量点测量 Wi-Fi RSS 值，记为 $\{V_1,V_2,\cdots,V_i,\cdots,V_M\}, i=1,2,\cdots,M$，其中 $V_i=\{v_1,\cdots,v_j,\cdots,v_N\}, j=1,2,\cdots,N$。CSP 生成一对 Paillier 密钥 $<\mathrm{PK}_c,\mathrm{SK}_c>$，其中，$\mathrm{PK}_c$ 是公钥，SK_c 是私钥，CSP 公开 PK_c。IPS 使用 PK_c 加密采样到的 RSS 值，记为 $E(v_{i,j})$。再对所有 RSS 值取负值后加密，记为 $E(-v_{i,j})$。建立指纹数据库 D，数据库中包括索引、物理位置、采样点的 RSS 值以及加密后的 RSS 值，记为 $D=<i,(x_i,y_i),\{V_i=\{v_{i,j}\},E(v_{i,j}),E(-v_{i,j})\}_{j=1}^{N}>_{i=1}^{M}$。

准备阶段。用户采样当前位置的 Wi-Fi RSS 值，记为 $V'=\{v'_1,v'_2,\cdots,v'_N\}$，其中 N 是 AP 的数量。使用 k 匿名算法，使用户的真实指纹与 $k-1$ 条匿名指纹不能被除了用户之外的所有攻击者区分。将这 k 条指纹数据使用 PK_c 进行加密后发送给 IPS，记为 $E(V'_r), r=1,2,\cdots,k$。IPS 计算

$$\begin{cases} E(x_{r,i,1})=E(v'_{r,1}-v_{i,1})=E(v'_{r,1})E(-v_{i,1}) \\ E(x_{r,i,2})=E(v'_{r,2}-v_{i,2})=E(v'_{r,2})E(-v_{i,2}) \\ \vdots \\ E(x_{r,i,N})=E(v'_{r,N}-v_{i,N})=E(v'_{r,N})E(-v_{i,N}) \end{cases} \tag{6}$$

$$E(Y_{r,i})=E\left(\sum_{j=1}^{N}(v'_{i,j}+v_{i,j})\right)=\prod_{j=1}^{N}\left(E(v'_{r,j})E(v_{i,j})\right) \tag{7}$$

其中，$r=1,2,\cdots,k$，$i=1,2,\cdots,M$。然后将 $E(X_{r,i})=\{E(x_{r,i,1}),E(x_{r,i,2}),\cdots,E(x_{r,i,j}),\cdots,E(x_{r,i,N})\}$ 和 $E(Y_{r,i})$ 发送给 CSP。

距离计算阶段。CSP 使用 SK_c 解密 $E(X_{r,i})$ 和 $E(Y_{r,i})$，得到 $X_{r,i}=\{x_{r,i,1},x_{r,i,2},\cdots,x_{r,i,N}\}$ 和 $Y_{r,i}$，然后计算

$$\begin{cases} d_{r,1}=\dfrac{\sum\limits_{j=1}^{N}\left|v'_{r,j}-v_{1,j}\right|}{\sum\limits_{j=1}^{N}(v'_{r,j}+v_{1,j})}=\dfrac{\sum\limits_{j=1}^{N}x_{r,1,j}}{Y_{r,1}} \\ d_{r,2}=\dfrac{\sum\limits_{j=1}^{N}\left|v'_{r,j}-v_{2,j}\right|}{\sum\limits_{j=1}^{N}(v'_{r,j}+v_{2,j})}=\dfrac{\sum\limits_{j=1}^{N}x_{r,2,j}}{Y_{r,2}} \\ \vdots \\ d_{r,M}=\dfrac{\sum\limits_{j=1}^{N}\left|v'_{r,j}-v_{M,j}\right|}{\sum\limits_{j=1}^{N}(v'_{r,j}+v_{M,j})}=\dfrac{\sum\limits_{j=1}^{N}x_{r,M,j}}{Y_{r,M}} \end{cases} \tag{8}$$

其中，$r=1,2,\cdots,k$。CSP 将计算结果集 $\{d_{r,1},d_{r,2},\cdots,d_{r,M}\}$ 返回给 IPS。

位置检索阶段。IPS 对收到的 k 组计算结果集 $\{d_{r,1},d_{r,2},\cdots,d_{r,M}\}$ 的每一组分别使用 KNN 算法进行处理，每组数据都找到其 K 个最近的距离，再根据索引 $\{I_1,I_2,\cdots,I_K\}$ 从数据库中匹配对应的物理坐标 $\{(x_1,y_1),(x_2,y_2),\cdots,(x_K,y_K)\}$，通过计算质心，最终得到 k 组定位结果，将其发送给用户，用户从 k 组结果中找到自己对应的位置，完成定位请求。

4　安全性分析

将部分计算外包给云的隐私保护室内定位可以保证用户位置的安全性以及 IPS 数据的安全性。

1) 抵抗位置隐私攻击

用户将自己测量到的 Wi-Fi RSS 信息和 $k-1$ 个虚拟位置信息以不可区分的方式使用公钥 PK_c 加密后发送给 IPS。在定位过程中，假设 Paillier 加密系统是安全的，攻击者只有在拥有私钥的情况下才可以对用户发送的数据进行解密，那么用户的测量信息 Wi-Fi RSS 对于任何对手都是安全的。在位置检索阶段，恶意服务器想通过 $\{d_{r,1},d_{r,2},\cdots,d_{r,M}\}$ 和指纹数据库恢复用户的 Wi-Fi RSS，假设对于用户发送的同一组 Wi-Fi RSS，N=3，可以得到

$$d_i=\frac{\sum\limits_{j=1}^{3}v'_j-v_{i,j}}{\sum\limits_{j=1}^{3}(v'_j+v_{i,j})}=\frac{\left|v'_1-v_{i,1}\right|+\left|v'_2-v_{i,2}\right|+\left|v'_3-v_{i,3}\right|}{v'_1+v_{i,1}+v'_2+v_{i,2}+v'_3+v_{i,3}} \tag{9}$$

其中，$d_i,v_{i,1},v_{i,2},v_{i,3}$ 都是已知的，但是由于攻击者无法获得 v' 和 v 的大小关系，因此不能对用户的 Wi-Fi RSS 进行恢复。本文方案可以抵抗位置隐私攻击。

2) 抵抗数据隐私攻击

在定位的整个过程中，距离计算阶段是在 CSP 上进行的，最终 IPS 返回给用户的数据是具体的位置坐标 $<x_i,y_i>$，而不是 Wi-Fi RSS，所以恶意用户不能通过发送多次定位请求来得到 IPS 的指纹数据库。此外，IPS 外包给 CSP 进行计算的数据是加密后再经过处理的中间数据，所以即使恶意的 CSP 拥有私钥，也不能还原得到 IPS 的指纹数据库。

数据库中存储的所有测量点的物理位置都是不公开的，所以恶意用户不能通过采样这些测量点的 Wi-Fi RSS 来建立相似的指纹数据库。所以本文方案可以抵抗数据隐私攻击。

3) 抵抗 IPS 与 CSP 的合谋攻击

假设合谋攻击由恶意的 IPS 和 CSP 组成，其目的是通过获取用户的 Wi-Fi RSS 值来定位用户的具体位置。恶意的 IPS 在收到用户的定位请求后，将接收到的加密 Wi-Fi RSS 直接发送给 CSP 进行解密，CSP 返回解密结果，IPS 进行距离计算，得到用户的具体位置坐标。但在此过程中，用户通过 k 匿名算法，将自己的真实 Wi-Fi RSS 混淆在 $k-1$ 组虚拟信息中，对于除用户外任何人都是不可区分的，这意味着恶意 IPS 和 CSP 成功猜中用户 Wi-Fi RSS 的概率为 $\frac{1}{k}$。

5　性能评估

5.1　理论分析

对本文方案进行理论分析，得到各个阶段的计算和通信开销，如表 3 所示。其中，Exp 为一个模指数运算，Mul 为一个模乘法运算，L 是密文的位长。

在离线阶段，只有 IPS 会产生计算开销，因为 IPS 使用 PK_c 加密了所有测量点的 Wi-Fi 指纹 $v_{i,j}$ 以及 $-v_{i,j}$，其中 $i=1,2,\cdots,M$ 且 $j=1,2,\cdots,N$。产生的计算开销为 $O(2MN\mathrm{Exp}+4MN\mathrm{Mul})$，其中 N 是 AP 的个数，M 是采样点的个数。在准备阶段，用户首先将采样到的 Wi-Fi 指纹和 $k-1$ 组虚拟指纹进行加密，然后发送给 IPS，产生的计算开销为 $O(Nk\mathrm{Exp}+2Nk\mathrm{Mul})$。通信开销为 $O(NkL)$。IPS 对接收到的用户指纹和数据库中的指纹进行预处理，IPS 再将计算结果发送给 CSP，产生的计算开销为 $O[(3N-1)Mk\mathrm{Mul}]$，通信开销为 $O[(N+1)MkL]$。在

表 3　　**各个阶段的计算和通信开销**

阶段	计算开销			通信开销
	用户	IPS	CSP	
离线阶段	—	$O(2MN\text{Exp}+4MN\text{Mul})$	—	—
准备阶段	$O(Nk\text{Exp}+2Nk\text{Mul})$	$O[(3N-1)Mk\text{Mul}]$	—	$O(NkL)$
距离计算阶段	—	—	$O[(N+1)Mk\text{Exp}+Mk]$	—
位置检索阶段	—	—	—	—

距离计算阶段，只有 CSP 参与了计算，然后将结果返回给 IPS，因为发送的数据是明文，所以通信开销忽略不计，产生的计算开销为 $O[(N+1)Mk\text{Exp}+Mk]$。在整个定位过程中，离线阶段的计算开销是在定位请求前产生的，在分析计算和通信开销时，不进行考虑。所以在本文方案中，进行一次定位请求产生的计算开销为 $O(Nk\text{Exp}+2Nk\text{Mul})$，通信开销为 $O(NkL)$。

现有方案中，文献[12]方案和文献[24]方案同样采用了 Paillier 半同态加密算法保护定位过程中的隐私，但是本文方案具有更高的定位效率。文献[25]方案将 k-means++聚类和安全多方计算相结合，减少了使用 Paillier 半同态加密算法带来的模指数运算，从而提高了效率，但是由于使用了 k-means++聚类的方法，因此定位精度远低于本文方案。Adp-FSELM 在边缘计算中将差分隐私和机器学习相结合，在多个阶段进行了加噪处理，且需要大量参与者来训练模型，与本文方案相比，计算开销更大。

5.2　时间开销

本节实验使用 UJIndoorLoc 开源数据库[26]来评估方案的性能。UJIndoorLoc 数据库是一个基于 WLAN 指纹识别的多建筑和多层定位数据库，涵盖了海梅一世大学的三座建筑，每座建筑有 4 层或 5 层，近 11 万平方米。数据库由 20 多个不同的用户和 20 个安卓设备创建，包括 25 条训练记录和 19 937 条测试记录。用于采样 RSS 的 AP 数量为 520 个，信号强度的缺失值为 100。每条记录给出了用户实际的位置坐标、用户所在楼层、用户所在建筑物等。本文方案选用 UJIndoorLoc 数据库中某一层的数据，选择 AP 的数量为 40 个，测量点的数量为 1 000 个。

根据本文方案进行仿真实验并计算平均时间开销，将其与文献[12]方案和文献[24]方案的平均时间开销进行分析对比并绘制折线。由图 2 和图 3 可以看出，3 种方案的平均时间开销随着 AP 的数量 N 以及测量点的数量 M 的增加而增大。导致这种结果的原因是 AP 数量增加，用户测量到的 Wi-Fi RSS 和 IPS 测量点采样到的 Wi-Fi RSS 就会增加，双方参与计算的数据量增大，需要进行同态加解密的明文增加，就会耗费更多的时间进行处理。本文方案将解密计算外包给 CSP 进行处理，平均时间开销明显比文献[12]方案和文献[24]方案低。

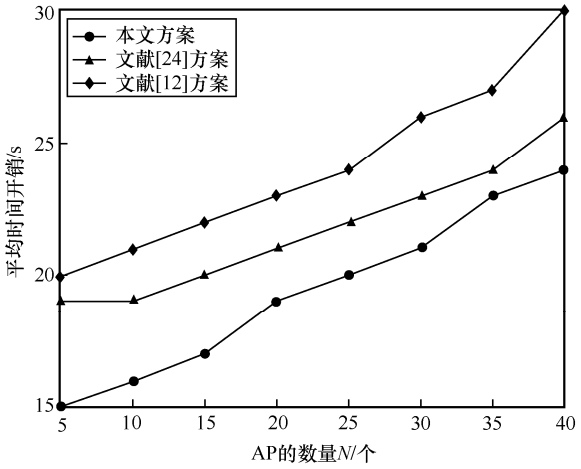

图 2　平均时间开销与 AP 的数量 N 的关系

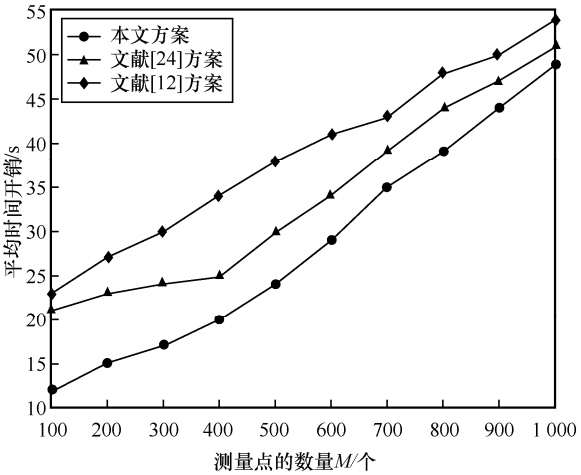

图 3　平均时间开销与测量点的数量 M 的关系

在本文方案中，为了保护用户的位置隐私，采用了 k 匿名方法。对于 k 值的不同选择，本文方案

的时间开销也会不同。平均时间开销随 k 值的变化如图 4 所示。由图 4 可知，定位的平均时间开销随 k 值的增大而增加，两者呈近似线性关系。

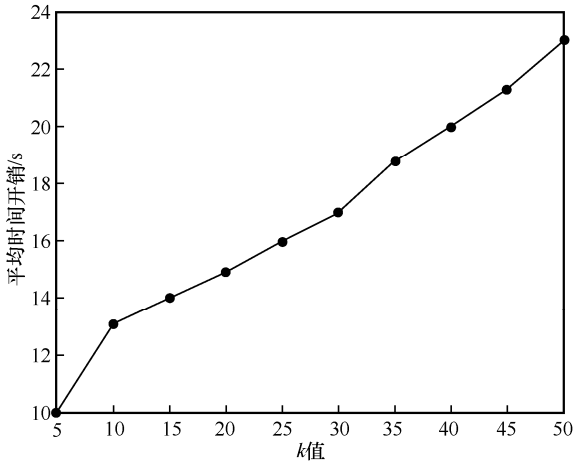

图 4 平均时间开销随 k 值的变化

5.3 通信开销

通信开销主要产生于用户进行定位请求时向IPS发送加密数据阶段，本文实验用带宽成本衡量通信开销，具体结果如图 5 和图 6 所示。由图 5 和图 6 可知，通信开销都是随着 AP 的数量的增加而增大，这是因为 AP 的数量越多，测量到的 Wi-Fi RSS 就越多，用户需要发送所有 AP 测量到的数据给 IPS，通信开销就会增加。此外，因为在本文方案和文献[24]方案中，用户发送给 IPS 的加密数据与 AP 的数量 N 有关，与测量点的数量 M 无关，所以本文方案和文献[24]方案的通信开销远小于文献[12]方案。而且在本文方案中，IPS 返回给用户的是解密后的明文数据，相比于密文数据，大小可以忽略不计，所以本文方案通信开销也优于文献[24]方案。

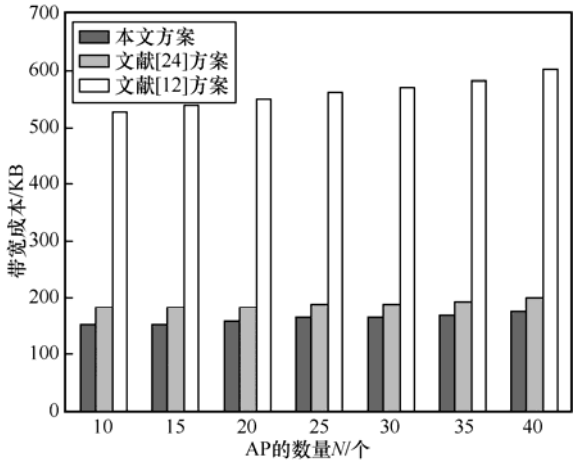

图 5　带宽成本与 AP 的数量 N 的关系

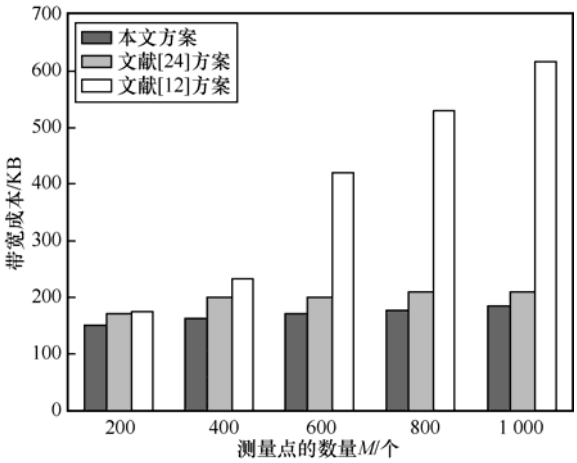

图 6 带宽成本与测量点的数量 M 的关系

5.4 定位误差

在室内定位中，经常通过定位误差的累积分布函数（CDF, cumulative distribution function）来量化定位精度，通常取 CDF=0.5 时对应的误差距离作为本文方案的定位误差。图 7 对 3 种方案进行了比较，本文方案中近 50%的定位误差小于 3.5 m，与文献[12]方案和文献[24]方案相比，比文献[12]方案定位误差减小了 18.42%，比文献[24]方案减小了 3.13%，因为本文方案使用的 Sφrensen 距离计算方法的成功率和定位误差优于室内定位中常用的 Euclidean 距离计算方法，且方案中的指纹数据没有进行加噪处理。

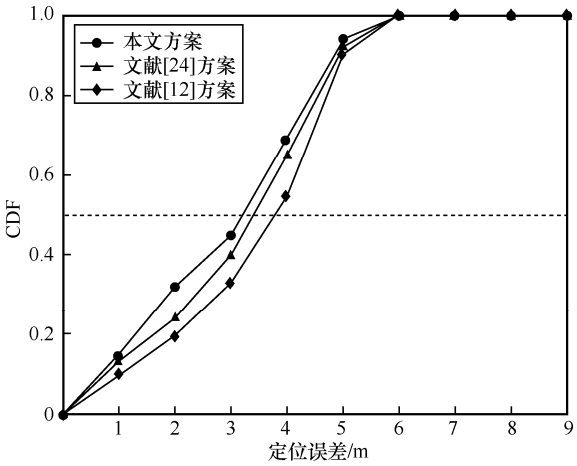

图 7　定位误差

如图 8 所示，通过比较在不同数据集大小的情况下本文方案与文献[25]方案的定位误差可以看出，本文方案的定位误差远小于文献[25]方案，误差降低了近 50%，且数据集越大，定位误差越小。对于数据集大小的选择，可以根据具体的实际情况，平衡效率和误差来选择最合适的大小。

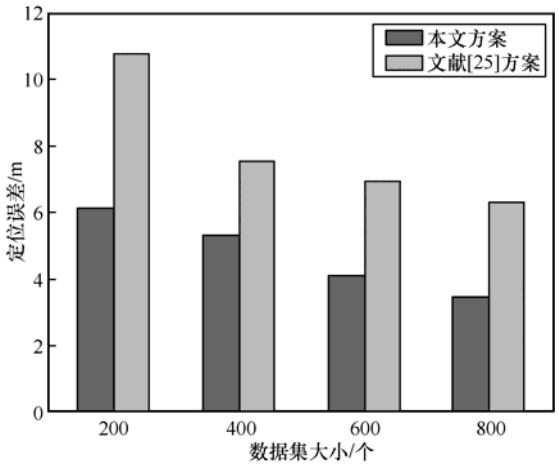

图 8 定位误差和数据集大小关系

6 结束语

本文提出了一种将部分计算外包给云的隐私保护方案，该方案既可以保护用户端位置的隐私，也可以保护服务器端的数据库隐私。将部分计算外包给云，减少了定位过程中 IPS 的计算和通信开销。相比于常用的 Euclidean 距离算法，使用 Sφrensen 距离算法提高了定位的成功率，减小了定位误差，可以给用户提供更好的定位服务。研究结果证明了本文方案的有效性、实用性和安全性。

参考文献：

[1] 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.

[2] SZYC K, NIKODEM M, ZDUNEK M. Bluetooth low energy indoor localization for large industrial areas and limited infrastructure[J]. Ad Hoc Networks, 2023, 139: 103024.

[3] HAYWARD S J, LOPIK K V, HINDE C, et al. A survey of indoor location technologies, techniques and applications in industry[J]. Internet of Things, 2022, 20: 100608.

[4] LI S H, HEDLEY M, BENGSTON K, et al. Passive localization of standard WiFi devices[J]. IEEE Systems Journal, 2019, 13(4): 3929-3932.

[5] SUGANO M, KAWAZOE T, OHTA Y, et al. Indoor localization system using RSSI measurement of wireless sensor network based on ZigBee standard[J]. Wireless and Optical Communications, 2006, 538: 1-6.

[6] ABBAS M, ELHAMSHARY M, RIZK H, et al. WiDeep: WiFi-based accurate and robust indoor localization system using deep learning[C]//Proceedings of the 2019 IEEE International Conference on Pervasive Computing and Communications. Piscataway: IEEE Press, 2019: 1-10.

[7] KHELIFI F, BRADAI A, BENSLIMANE A, et al. A survey of localization systems in Internet of things[J]. Mobile Networks and Applications, 2019, 24(3): 761-785.

[8] ZWIRELLO L, SCHIPPER T, HARTER M, et al. UWB localization system for indoor applications: concept, realization and analysis[J]. Journal of Electrical and Computer Engineering, 2012, 2012: 4.

[9] HIGUCHI T, MARTIN P, CHAKRABORTY S, et al. AnonyCast: privacy-preserving location distribution for anonymous crowd tracking systems[C]//Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing. New York: ACM Press, 2015: 1119-1130.

[10] LI L, LIU J Q, CHENG L C, et al. CreditCoin: a privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles[J]. IEEE Transactions on Intelligent Transportation Systems, 2018, 19(7): 2204-2220.

[11] ARMENGOL P, TOBKES R, AKKAYA K, et al. Efficient privacy-preserving fingerprint-based indoor localization using crowdsourcing[C]//Proceedings of the 2015 IEEE 12th International Conference on Mobile Ad Hoc and Sensor Systems. Piscataway: IEEE Press, 2015: 549-554.

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

[13] WANG X S, LIU Y, SHI Z Q, et al. A privacy-preserving fuzzy localization scheme with CSI fingerprint[C]//Proceedings of the 2015 IEEE Global Communications Conference (GLOBECOM). Piscataway: IEEE Press, 2015: 1-6.

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

[15] 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.

[16] LI S J, LI H, SUN L M. Privacy-preserving crowdsourced site survey in WiFi fingerprint-based localization[J]. EURASIP Journal on Wireless Communications and Networking, 2016, 2016(1): 123.

[17] JÄRVINEN K, LEPPÄKOSKI H, LOHAN E S, et al. PILOT: practical privacy-preserving indoor localization using outsourcing[C]//Proceedings of the 2019 IEEE European Symposium on Security and Privacy (EuroS&P). Piscataway: IEEE Press, 2019: 448-463.

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

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

[20] LI B H, LIANG R C, ZHOU W, et al. LBS meets blockchain: an efficient method with security preserving trust in SAGIN[J]. IEEE Internet of Things Journal, 2022, 9(8): 5932-5942.

[21] ZHANG X J, HE F C, CHEN Q, et al. A differentially private indoor

localization scheme with fusion of WiFi and bluetooth fingerprints in edge computing[J]. Neural Computing and Applications, 2022, 34(6): 4111-4132.

[22] TORRES-SOSPEDRA J, MONTOLIU R, TRILLES S, et al. Comprehensive analysis of distance and similarity measures for Wi-Fi fingerprinting indoor positioning systems[J]. Expert Systems with Applications, 2015, 42(23): 9263-9278.

[23] PAILLIER P. Public-key cryptosystems based on composite degree residuosity classes[C]//International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 1999: 223-238.

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

[25] YANG X, LUO Y C, XU M, et al. Privacy-preserving WiFi fingerprint localization based on spatial linear correlation[C]//International Conference on Wireless Algorithms, Systems, and Applications. Berlin: Springer, 2022: 401-412.

[26] TORRES-SOSPEDRA J, MONTOLIU R, MARTÍNEZ-USÓ A, et al. UJIIndoorLoc: a new multi-building and multi-floor database for WLAN fingerprint-based indoor localization problems[C]//Proceedings of the 2014 International Conference on Indoor Positioning and Indoor Navigation (IPIN). Piscataway: IEEE Press, 2014: 261-270.

[作者简介]

张应辉（1985− ），男，陕西西安人，博士，西安邮电大学教授，主要研究方向为公钥加密、云安全和无线网络安全。

张思睿（1999− ），女，陕西延安人，西安邮电大学硕士生，主要研究方向为室内定位安全和云安全。

赵秋霞（1987− ），女，山西平陆人，青海师范大学博士生，主要研究方向为现代密码学技术和云安全。

郑晓坤（1995− ），男，山西临汾人，青海师范大学博士生，主要研究方向为密码学和云安全。

曹进（1985− ），男，陕西西安人，博士，西安电子科技大学教授，主要研究方向为5G、6G、天地一体化网络安全。