定位系统中的位置隐私泄露与保护

史秀纺　张文安　浙江工业大学信息工程学院

摘要：定位系统作为基于位置的服务的基础支撑系统，其位置隐私泄露问题不可忽视。本文介绍了定位系统面临的位置隐私泄露威胁，并描述了两类典型的定位系统（指纹定位系统和基于模型的定位系统）中的隐私保护机制。最后，本文针对物联网环境下的定位系统，讨论了其在隐私保护方面的未来发展方向。

1. 引言

基于位置的服务（Location Based Services, LBS）是指服务提供商根据设备所在位置向设备或者用户提供信息服务，如导航、兴趣点查询、叫车服务等。LBS 最初是用于军事领域，美国国防部利用 GPS 全球定位系统来监控和跟踪目标。后来，LBS 逐渐拓展至民用领域。1996 年，美国联邦通信委员会对应急 911 提出了定位需求，要求网络运营商能快速准确地确定拨打 911 紧急呼叫的用户的位置[1]，以便用户享受到相关的服务，如紧急救援等。近年来，随着物联网相关支撑技术（如定位技术、移动通信技术等）的快速发展，LBS 已经渗透到了日常生活的方方面面。

LBS 在给生活带来各种便利的同时，也存在隐私泄露的风险。攻击者可以在 LBS 过程中窃取用户的位置信息，并进一步挖掘用户的兴趣爱好，健康状况、作息习惯等个人隐私信息，为用户带来困扰甚至威胁用户安全。LBS 中存在多种隐私泄露途径。从图 1 所示的 LBS 基本构成来看，LBS 主要包含四部分：定位系统，移动设备（用户），通信网络和服务器（服务提供商）。定位系统为用户提供 LBS 所必需的位置信息，通信网络是用户与服务提供商之间通信的桥梁，用户向服务提供商发送请求，服务提供商根据用户的信息提供相应的服务。常见的隐私泄露方式有三种：(1) 服务提供商不可信，将用户的位置信息卖给第三方以谋取利益；(2) 在用户向服务提供商上传位置信息的过程中，攻击者通过窃听通信网络获得用户的位置信息；(3) 定位过程中的位置隐私泄露。目前 (1) (2) 中的隐私保护已受到了广泛关注，

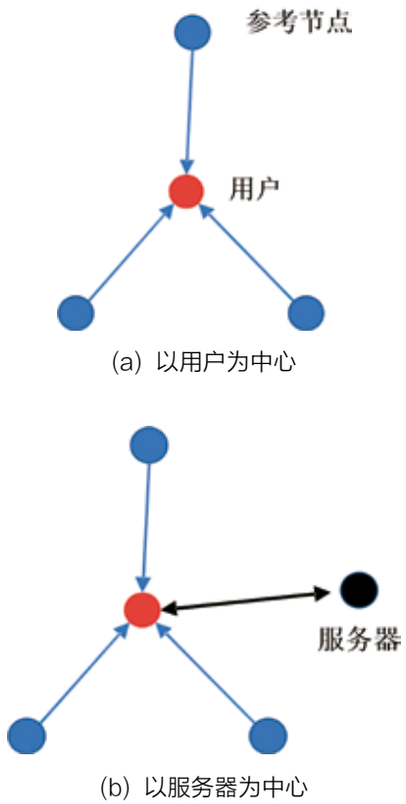
图1 LBS的基本构成

并且已有大量的解决方案。而定位系统中的隐私保护机制还不成熟。

2. 定位系统中的位置隐私威胁

定位系统中，用户获取位置信息的方式主要有两类：以用户为中心和以服务器为中心，如图2所示。在以用户为中心的定位系统中，用户接收参考节点的信号，获得量测信息，如到达时间（TOA），到达时间差（TDOA），接收信号强度（RSS）等，并根据所得信息对自己的位置进行估计。在以服务器为中心的定位系统中，用户将所得信息发送给服务器，由服务器执行位置估计算法，并将位置信息返回给用户。

两类定位系统都容易受到位置隐私泄露的威胁。在以用户为中心的定位系统中，用户的位置由自己计算，其位置信息一般不容易泄露，而参考节点的位置信息常常会暴露给用户。在定位系统中，参考节点大多是GPS卫星、蜂窝基站、WiFi接入点（AP）等，其位置一般是公开的，对隐私泄露不敏感。然而，在物联网时代，参考节点不再局限于以上设备，变得更加多样化，也可能是对位置信息敏感的其他用户或者物联网节点，在这种情况下，参考节点的位置信息保护也是不可忽视的。以服务器为中心的定位系统降低了用户端位置计算的开销，然而，用户的位置信息，甚至包括参考节点的位置信息，都暴露给了服务器。如果服务器是不可信的或者是恶意的，用户和参考节点的位置隐私安全将无法保证。



(a) 以用户为中心

(b) 以服务器为中心

图2 定位系统中的位置信息获取方式

3. 典型定位系统中的隐私保护机制

关于位置隐私保护，已有一些经典方法提出，如 K 匿名、差分隐私、同态加密等。在 LBS 中，这些方法一般用于保护用户位置上传过程中的隐私信息，而无法直接用于定位系统中的隐私保护。在定位系统中，一般针对其实现方式，结合现有的位置隐私保护方法进行专门的设计。

3.1 指纹定位系统中的隐私保护机制

指纹定位系统将信号在不同位置的特征作为指纹来实现定位。目前最常用的指纹特征是 WiFi 的信号强度。基于 WiFi 的指纹定位系统一般是以服务器为中心的，定位过程分为两个阶段，离线训练和在线定位。离线训练阶段，服务器在感兴趣的区域内设定足够数量的参考点，移动设备在各参考点测量其 WiFi 指纹，即接收到的周围 WiFi AP 的信号强度值，然后服务器收集各参考点的指纹信息存入指纹数据库，构建指纹地图。在线定位阶段，用户将自己当前位置测量的 WiFi 指纹发送给服务器，服务器计算用户的 WiFi 指纹与数据库中各位置的指纹之间的欧式距离，确定指纹距离最短的 k 个位置，然后根据这 k 个位置计算用户的当前位置。无论是离线训练阶段还是在线定位阶段都存在隐私泄露的风险。

3.1.1 在线定位阶段的隐私保护

在线定位阶段，用户的位置信息会暴露给服务器，若服务器是不可信的或者恶意的，其很容易对用户发起攻击或者挖掘出用户更多的隐私信息。现有研究大多关注在线定位阶段的隐私保护，其中具有代表性的工作是由 Li 等人提出的基于 Paillier 密码系统的隐私保护机制 PriWFL[2]，其工作流程如图 3 所示。加入隐私保护机制的在线定位过程由四个阶段构成：（1）预处理阶段。服务器抽取指纹数据库中的元数据（metadata）发送给用户。元数据包含两个表格，一个表格包括 WiFi 指纹的采集地点和其在数据库中的编号，另一个表格中包含 WiFi AP 信息。（2）准备阶段。用户利用 Paillier 密码系统生成一对公钥和私钥，将自己采集的 WiFi 指纹信息加密，连同公钥一起发给服务器。（3）距离计算阶段。收到用户发送的信息后，服务器利用同态加密算法在密文空间计算用户的指纹与指纹数据库中各指纹之间的欧式距离，并将加密后的计算结果返回给用户。（4）位置估计阶段。用户利用私钥对加密后的距离进行解密，确定最短的 k 个距离，然后根据元数据中的表格，确定 k 个最短距离的指纹对应的采集位置，并最终估计自己的当前位置。在 PriWFL 中，服务器获得的都是经过加密的信息，由于缺少私钥，无法破解用户的指纹信息，从而无法得到用户的位置信息。另一方面，由于用户从元数据只能获取数据库中指纹对应的位置，却无法获得指纹数据，这样指纹数据库的数据隐私也得到了保护。

针对在线定位阶段的隐私保护，除了 PriWFL，不断有新的算法提出，如 Zhao 等人提出的基于 K 匿名和差

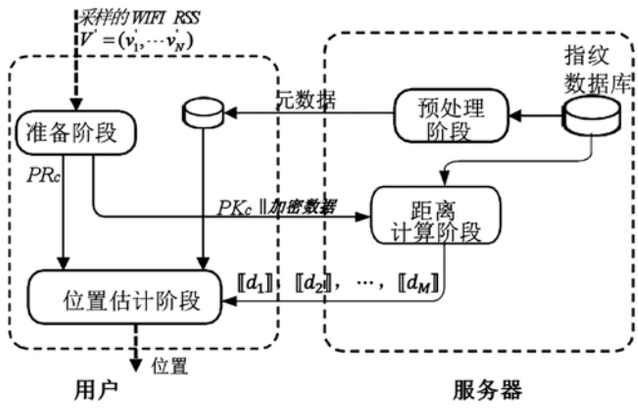


图3 PriWFL的工作流程[2]

分隐私的定位机制 P3-LOC[3]，Zhang 等人提出的基于 Paillier 密码系统隐私保护的轻量级定位机制 LWP2[4] 等。

3.1.2 离线训练阶段的隐私保护

离线训练阶段中，由于定位精度与指纹地图的精细程度紧密相关，指纹数据库的建立需要事先进行大量的现场勘测工作，另外考虑到环境中信号特征常常是动态变化的，往往需要频繁地更新指纹地图。为了减少事先现场勘测工作和地图更新成本，近年来学者提出利用群智感知的思想建立指纹数据库 [5]，进入感兴趣的区域内的移动用户（也可以叫做志愿者用户）将自己的位置和相应的指纹信息上传至服务器，大量移动用户上传的信息就构成了指纹数据库。然而，移动用户在上传指纹信息的同时又向服务器暴露了自己的位置隐私。

已有学者关注离线训练阶段的隐私保护，如 Li 等人 [6] 提出利用同态加密和差分隐私技术在现场勘测过程中保护数据上传者的位置隐私。最近，Yin 等人提出一种基于联邦学习（Federated Learning）的分布式定位框架 FedLOC 来保护数据上传用户的位置隐私 [7]。联邦学习是由 Google 于 2016 年提出的分布式学习框架 [8]，是一种灵活且安全的合作学习框架，基本思想是利用移动用户独立进行本地训练得到的局部模型来近似一个全局的模型。在 FedLOC 框架下的指纹定位系统中，移动用户上传的不是直接测量的指纹数据，而是训练过的模型参数。图 4 展示了 FedLOC 框架下基于深度神经网络（DNN）的离线训练过程。该框架以不同位置的指纹特征（周围无线接入点的接收信号强度）为训练输入样本，以指纹特征对应的位置为训练输出样本。核心网（服务器）首先将一个全局模型参数的初始值经加密后发送给各移动用户；各移动用户基于加密的全局模型参数，利用本地获取的输入样本和输出样本，通过 DNN 训练得到局部模型参数，并将该模型参数加密后发送给核心网；核心网收到各移动用户发送的模型后，在密文空间对局部模型进行加权得到全局模型，并继续返回给移动用户；训练过程不断迭代，直至模型收敛。由于移动用户只上传了加密的训练模型参数，核心网无法推断移动用户的位置信息，从而实现了位置隐私保护。

3.2 基于模型的定位系统中的隐私保护机制

基于模型的定位系统可以是以用户为中心的，也可以是以服务器为中心的。定位过程一般也包含两个阶段，位置相关的信息收集（包括参考节点的位置信息和反映用户与参考节点之间几何位置关系的量测信息，如 TOA、TDOA、AOA 等）和位置估计。在信息收集阶段，参考节点的位置信息会泄露给用户，而在位置估计阶段，用户的位置信息又可能暴露给服务器。

Shu 等人 [9] 针对以用户为中心、基于测距的定位，设计了三个安全最小二乘估计算法以实现不同层次的隐私保护：(1) Level-I Privacy。用户和参考节点除了自己的位置，不知道其他节点的准确位置，而参考节点可以对用户的位置进行粗略估计；(2) Level-II Privacy。用户和参考节点除了自己的位置，不知道其他节点的准确位置，而参考节点可以通过与其他节点串通对未串通节点的位置进行粗略估计；(3) Level-III Privacy。用户和参考节点除了自己的位置，不知道其他节点的准确位置，参考节点即使与其他节点串通也无法估计未串通节点的位置。 在实现 Level-I Privacy 的定位算法中，每个参考节点分别在不同的位置测量其与用户的距离，参考节点不向用户直接发送位置，而是通过相互协作产生零和噪声加入到最小二乘估计的中间计算量中，并将加噪后的中间计算量发送给用户，用户根据收到的信息计算

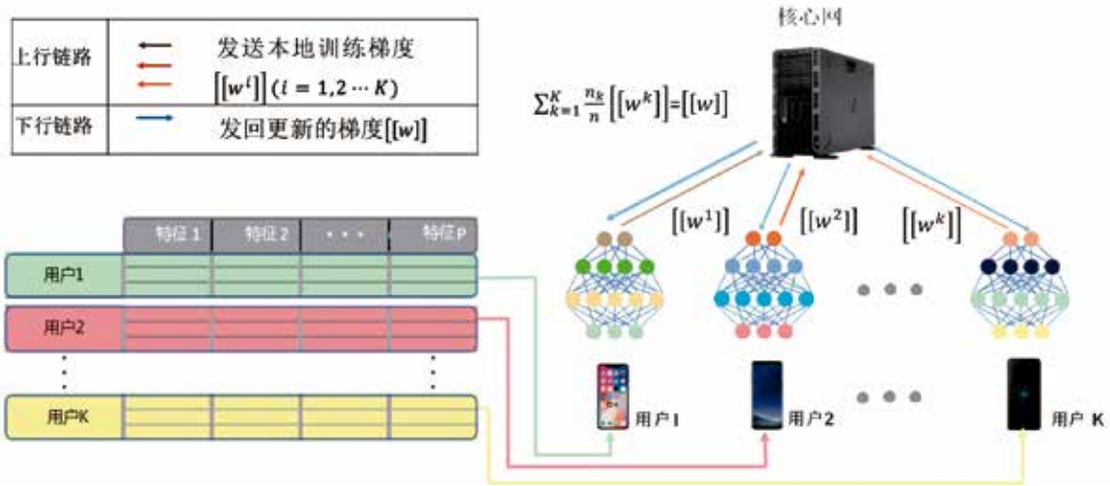


图4 FedLoc框架下基于DNN的离线训练过程[7]

自己的位置。在实现 Level-II Privacy 的定位算法中，参考节点仅在一个位置测量其与用户的距离，然后通过参考节点之间的信息交换，对最小二乘估计的中间量进行加噪并发送给用户，用户进一步估计自己的位置。在实现 Level-III Privacy 的定位算法中，用户执行测距操作，参考节点只知道自己的位置信息，通过对最小二乘估计重新描述，利用同态加密算法在密文空间计算相关中间计算量，并最终得到用户的位置估计。借鉴以上通过传递中间计算量以实现保护位置隐私的思想，Shi 等人 [10] 又进一步为基于 TDOA 的定位系统设计了隐私保护机制。

4. 总结与展望

定位系统作为 LBS 的关键支撑系统，其隐私问题已不可忽视。本文介绍了定位系统所面临的隐私威胁和典型的定位系统所采用的隐私保护机制。虽然近几年定位系统中的隐私保护已得到一定研究，物联网技术的迅猛发展又为定位系统中的隐私保护带来了新的机遇和挑战，亟待学者进一步探索：

（1）轻量级隐私保护机制的设计：物联网中接入设备多种多样，计算和通信能力各异。现有的隐私保护机制大多采用加密机制来保护位置隐私和实现安全通信，难以适用于所有的物联网设备。为了降低用户端的开销，需要设计轻量级的隐私保护机制。

（2）隐私保护和定位性能的权衡分析与设计：现有的隐私保护机制往往以保护位置信息为主要目标而忽视了其对定位性能的影响。分析隐私保护与定位性能的内在耦合机理，并在隐私保护机制的设计中平衡二者的关系是一个重要的研究方向。

（3）基于人工智能的新型定位架构：随着物联网设备的智能化，很多物联网设备搭载了人工智能芯片用于实现必要的人工智能算法。正如前文所述，已有一些开创性工作基于人工智能方法在定位的同时实现了隐私保护，如 FedLOC。在定位系统中，利用人工智能的优势实现隐私保护将是一个新的研究方向。

参考文献

[1] https://en.wikipedia.org/wiki/Enhanced_9–1–1

[2] Li H, Sun L, Zhu H, Lu X, and Cheng X. Achieving privacy preservation in WiFi fingerprint–based localization. In Proceedings of the 33rd Annual IEEE international conference on Computer Communications (Infocom 2014). 2014. 2337–2345.

[3] Zhao P, Jiang H, Lui J, Wang C, Zeng F, Xiao F, and Li Z. P3–LOC: A Privacy–Preserving Paradigm–Driven Framework for Indoor Localization. IEEE/ACM Transactions on Networking. 2018, 26(6): 2856–2869.

[4] Zhang G, Zhang A, Zhao P, and Sun J. Lightweight Privacy–Preserving Scheme in Wi–Fi Fingerprint–Based Indoor Localization. IEEE Systems Journal, DOI: 10.1109/JSYST.2020.2977970.

[5] Yang Z, Wu C, and Liu Y. Locating in fingerprint space: wireless indoor localization with little human intervention. In Proceedings of the 18th annual international conference on Mobile computing and networking (Mobicom'12), 2012, 269–280.

[6] Li S, Li H, and Sun L, Privacy–preserving crowdsourced site survey in WiFi fingerprint–based localization. EURASIP Journal on Wireless Communications and Networking, 2016, (1): 123.

[7] Yin F, Lin Z, Xu Y, Kong Q, Li D, Theodoridis S, and Cui S, FedLoc: Federated Learning Framework for Cooperative Localization and Location Data Processing, arXiv preprint, arXiv: 2003. 0369, 2020.

[8] Konecn'y J, McMahan H, Yu X, Richt'arik P, Suresh A, and Bacon D, Federated learning: Strategies for improving communication efficiency, arXiv preprint arXiv:1610.05492, 2016.

[9] Shu T, Chen Y, and Yang J, Protecting multi–lateral localization privacy in pervasive environments, IEEE/ACM Trans on Networking, 2015, 23(5): 1688–1701.

[10] Shi X and Wu J. To Hide Private Position Information in Localization Using Time Difference of Arrival. IEEE Transactions on Signal Processing, 2018, 66(18): 4946–4956.