doi:10.11959/j.issn.1000-436x.2015167

移动互联网中的位置隐私保护研究

王宇航，张宏莉，余翔湛
(哈尔滨工业大学 计算机网络与信息安全技术研究中心，黑龙江 哈尔滨 150001)

摘 要：全面归纳了移动互联网中位置隐私保护的相关研究工作，总结了位置服务和定位服务中的威胁模型。然后，详细介绍了现有基于位置服务的隐私保护技术，分析了其在抗隐私攻击和位置隐私适用性方面的优缺点，并阐述了定位服务中位置隐私问题的本质、威胁和解决方法。最后指出了需要进一步研究的问题。
关键词：位置隐私；基于位置的服务；定位服务；移动互联网
中图分类号：TP393 **文献标识码**：A

Research on location privacy in mobile internet

WANG Yu-hang, ZHANG Hong-li, YU Xiang-zhan
(Research Center of Computer Network and Information Security Technology, Harbin Institute of Technology, Harbin 150001, China)

Abstract: The related researches on location privacy in mobile internet were surveyed comprehensively, dissertate separately from the perspective of LBS(location-based services) and location service. First the privacy protection approaches for LBS were detailed, their features in the view of privacy attacks and LBS applicability were researched. Then the essence and research boundary of location privacy in location service were demonstrated, its related research progress and policies were introduced. The future research directions are provided in the end.
Key words: location privacy; LBS; location service; mobile internet

1 引言

移动互联是指通过移动通信设备对互联网进行访问的新型互联网访问形式[1]。近年来，伴随着智能手机、平板电脑等高性能移动设备的普及，以及 3G、4G 等移动通信技术的快速发展，移动互联网的规模和普及率均在日益提升。2013 年，全球移动互联网流量较 2012 年上升 81%，截至 2014 年 5 月，25%的全球用户利用移动互联网访问网络，而该数字在 2013 年 5 月时仅为 14%，可以预见在未来，移动互联网将会成为使用互联网服务的最主要渠道[2]。

移动互联网的便携性和实时性促进了新的网络服务模式发展，基于位置的服务(LBS, location-based services)是其中重要的组成部分。当前 LBS 已经融入社交、电子商务、生活服务等多个领域，在全球范围内逐渐成为日趋普及化的服务。

移动互联网中的位置隐私保护研究需要解决 2 个问题。

1) 面向 LBS 的位置隐私保护：在用户使用 LBS 过程中，如何保护用户的位置隐私。多数情况下，LBS 提供者(SP, lBS provider)必须首先获知用户位置才能提供服务，其中不只包含地理坐标信息，通过对位置的观察和分析，能够获知大量其他隐私信息，例如用户的家庭住址、惯用路线、生活习惯等。由于 SP 的不可信性，用户将位置发送给 SP 时将面临个人隐私泄露的风险。如何在充分利用位置服务提供便利的同时，保证用户隐私安全是应用中亟待解决的问题。

收稿日期：2014-08-17；**修回日期**：2014-12-10
基金项目：国家重点基础研究发展计划(“973”计划)基金资助项目(2011CB302605)；国家自然科学基金资助项目(61173144, 61073194, 61202457)；国家科技支撑计划基金资助项目(2012BAH37B01)
Foundation Items: The National Basic Research Program of China(973 Program) (2011CB302605); The National Natural Science Foundation of China(61173144, 61073194, 61202457); The National Key Technology R&D Program(2012BAH37B01)

2) 面向定位服务的位置隐私保护：在定位服务过程中，如何保护用户的位置隐私。移动互联网环境下，研究位置隐私保护的另一个重要驱动要素，来源于位置信息采集，即定位过程中存在的安全隐患。随着定位技术趋于多样化，定位功能本身也已经成为了一种第三方服务。该过程中位置信息会被定位服务的提供者(LP, location provider)获得，因此也产生了和用户与 SP 之间类似的位置隐私问题。尽管当今的 LP 是由谷歌、微软、苹果、百度等此类国内外 IT 巨头担任，其安全防护能力与 SP 相比而言相对较高，但单凭这点无法消除移动互联网用户对自身位置隐私的顾虑，2013 年爆发的 Google 协同美国 NSA 棱镜计划利用其定位服务追踪用户位置的丑闻足以说明这一点[3]。如何保护用户在使用定位服务过程中的位置隐私同样是实际应用中亟待解决的问题。

对于问题 1)，研究者们开展了大量研究工作，汇集成了若干研究方向，其思想主要是通过对位置的泛化、模糊或掩盖等方式，降低攻击者识别用户位置的能力。这些技术从理论上能够提高位置攻击的难度，但距离实际应用仍有大量工作需要完成。对于问题 2)，当前研究界对其讨论还不够充分，长期以来，位置隐私保护问题往往被片面理解为仅仅是问题 1)，直到 2013 年才由 Damiani 等[4]指出其在移动互联网场景中存在片面性。目前还没有良好的相关技术来解决问题 2)，有待深入研究和探讨。

本文立足移动互联网视角，对当前该领域内的位置隐私保护技术和相关问题进行全面综述和讨论。

2　面向 LBS 的位置隐私保护背景知识

基于位置的服务，是一类以用户位置信息为基础，向用户提供与位置相关的实用服务的总称。SP 为用户提供服务的同时，也是位置隐私威胁的主要来源。面向 LBS 的位置隐私保护的理想目标是实现“绝对隐私”，即在不让包括 SP 在内的任何一方获得自身位置的前提下使用 LBS。然而，受限于 LBS 实现原理，“绝对隐私”的理想与 LBS 的提供前提矛盾。因此当前大多数研究的目标，围绕于实现位置的“相对隐私”保护，或称为“可控隐私”，即将位置信息以一种相对难以被攻击者识别的形式发布。这样的形式既能满足用户个性化的隐私需求，又能保证 LBS 不至于因不能获得位置而无法实现[5]。在该目标下，当前展开的工作积累了一定量的研究成果，形成了大致统一的威胁模型、若干架构模型和隐私度量标准。

2.1　威胁模型

面向 LBS 的位置隐私保护并不考虑定位过程的位置隐私，其威胁来源是 LBS 过程中涉及的角色。通过对现有技术的研究归纳，当前的威胁模型主要基于如下假设。

1)可信的移动设备。绝大多数研究工作都将用户设备视为完全可信的。“可信”有 2 层含义：首先是定位的可信，即用户通过定位获得的位置，无论其定位技术是什么以及将被如何使用，首先都能够真实地反映现实中用户在某时刻的真实位置，所不同的只是位置精度而已。其次是 LBS 请求行为的可信，用户终端没有被病毒或恶意程序等攻击手段所侵害，用户发送自身位置行为是完全自愿的。

2)不可信的 SP。现有研究几乎都将 SP 假设为不可信的或恶意的。这是因为，首先用户没有能力验证 SP 的可信性，其次即便诚实的 SP 也可能被其他恶意第三方攻击从而泄露位置隐私。事实上大多数工作都直接将 SP 本身视为最直接的恶意攻击者。

3)允许有一个可信第三方(TTP, trusted third party)集中管理用户的位置信息。大量位置隐私保护技术使用 TTP 作为用户与 SP 之间的桥梁。TTP 在不同的位置隐私保护技术中常常用来管理用户真实位置并执行一些具体的隐私保护操作。此假设广泛存在于大量位置隐私保护技术文献中，但一些文献同时也指出其合理性有待商榷[6]。

2.2　场景及架构模型

图 1 是移动互联网中，用户进行定位以及使用 LBS 的一般场景，按时间顺序可将该场景先后分为“位置信息采集”和“基于位置的信息查询”。用户在位置信息采集后，在信息查询时将位置连同 LBS 所需的其他信息发送给 SP，SP 利用这些信息为用户提供其指定的服务。面向 LBS 的位置隐私保护不关心位置来源，专注于使用户在享受 LBS 的同时避免 SP 或其他攻击者侵害其位置隐私。

当前的位置隐私保护技术所采用的架构模型大体可以分为图 1 虚线右侧所使用的 3 类。表 1 列出了这 3 种架构模型，以及按照 3 种架构模型对当前主要技术的分类。

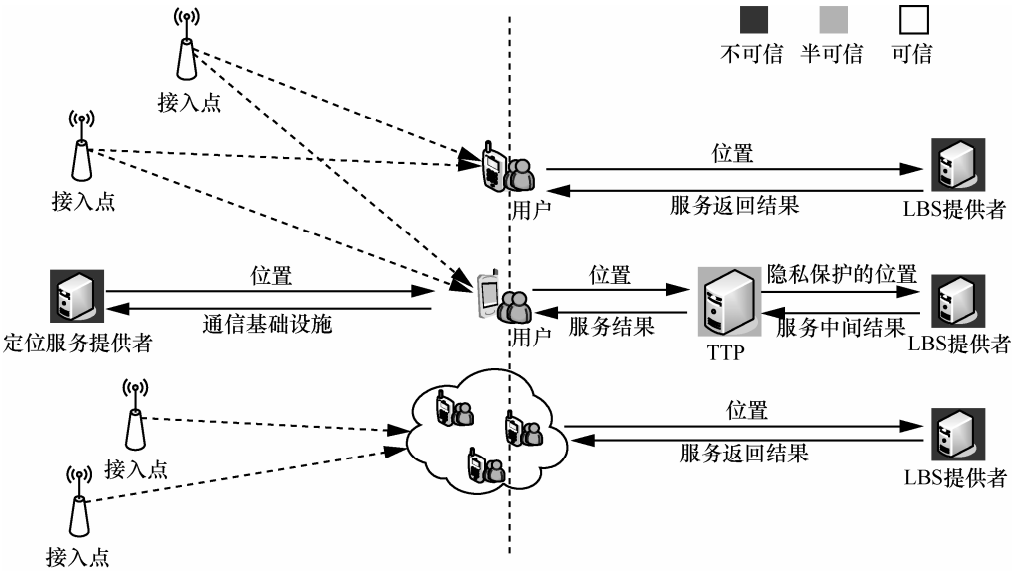


图 1 位置隐私保护的场景和架构模型

表 1 3 种架构模型

架构模型	相关文献
架构 1	文献[7~12]
架构 2	文献[13~21]
架构 3	文献[22]

架构 1：一类技术[7~12]采用了直接通信模型。在该架构下，直接在移动设备上执行具体的位置隐私保护技术，以直接通信的方式发送服务请求，接收服务结果。该架构的优点是结构简明，且服务时延短。缺点是位置隐私保护技术的实现将受到移动设备性能的限制，且 LBS 服务质量通常会降低。

架构 2：此类位置隐私保护技术中[13~22]，用户和 SP 之间由 TTP 担任通信中介。TTP 负责执行具体的位置隐私保护技术，对 SP 返回的结果进行处理。基于该模型能够实现灵活的位置隐私保护技术，但 TTP 则可能成为攻击热点，且 TTP 是否能实现理论上的“可信”也值得怀疑，同时，TTP 的效率也成为了 LBS 的瓶颈。

架构 3：如文献[22]等一些位置隐私保护技术，利用一定区域内用户自组织的 P2P 网络来执行具体的隐私保护技术，并利用 P2P 网络本身与 SP 通信。该模型避免了 TTP 带来的缺陷，同时也能继承一些在架构 2 上实现的技术。缺点则是要求用户终端必须具有 2 套无限通信设备，一套用与 SP 通信，一套用来维持 P2P 网络，且当区域内用户分布稀疏时不易构建。

2.3 保护对象和目的

保护对象包括但不仅是位置坐标本身，用户经常要将位置与其他信息一并发送给 SP。这些其他信息中有些也是位置隐私的保护对象，Wernke 等[23]将位置隐私的保护对象归纳为三元组：<*identity*, *location*, *time*>。除 *location* 为用户位置外，*identity* 是用户的唯一身份标识，*time* 是与 *location* 相关联的时间戳。一个完整的该三元组能够表达“谁，在何时，位于哪里”这样精确的位置信息。除此之外，本文认为，用户在某时刻的速度常常也会成为攻击者能够利用的信息。某些 LBS（例如，导航服务）也依赖速度信息才能够良好实现。虽然速度能够利用多次位置刷新进行间接估算，但如此其精度将受限于用户的刷新频率；另一方面，随着设备发展的进步，设备内部大多嵌有感知速度的各类传感器，意味着速度可由设备自主获得，此时，即便用户选择不频繁刷新定位，也不等价于保护了速度信息的隐私性[24]。因此，为加强完整性，本文将位置隐私保护的对象归纳为如下四元组 L

$$<identity, location, \vec{v}, time>$$

其中，$\vec{v}$ 表示用户在 *time* 时刻的速度。四元组 L 更完善地表达了面向 LBS 的位置隐私的保护对象。利用 L 可将位置隐私保护的目的表述为：使用户能够根据隐私需求，以任意的形式，对外发布自身四元组 L 中的任意元素。

2.4 隐私度量

隐私度量一方面用来量化位置隐私保护技术提供了多大程度的保护，另一方面也用来定量地表示用户需要被多大程度的提供位置隐私保护。当前并没有形成统一的隐私度量标准。各类技术汇集成了若干隐私度量，其中，较为通用的是匿名度，比

较常见的有匿名区域、泛化程度和最小半径。表 2 列出了常用隐私度量以及分别使用这些隐私度量的技术文献。

表 2　　4 种常见隐私度量

隐私度量	相关文献
匿名度	文献[12~22]
匿名区域	文献[13~17,22]
泛化程度	文献[7,8,11]
最小半径	文献[10]

匿名度首先由 Gruteser 等[13]应用于其位置隐私保护技术中，随后被多种位置隐私保护技术[7,8,11,12,14~17,21,22]采用或借鉴。利用四元组 L，匿名度为 $k(k\in N^*)$的含义可表达为：将 *identity* 匿名，将 *location* 与 $k-1$ 个其他位置混合成 k 个位置的集合，使攻击者一次从集合中辨认出真实位置的概率为 $\frac{1}{k}$。显然，k 值越大则隐私程度越高，反之亦然。匿名区域常伴随匿名度一同使用，共同表征某技术提供的隐私程度。匿名区域通常为矩形，在空间上表示一块能够覆盖匿名度为 k 的 k 个用户位置的区域。若用 δ 表示匿名区域的面积，则同时满足匿名度为 k 和匿名区域大小为 δ 的 2 个度量的技术称为实现了 k-δ 匿名。

另一些技术[7,8,11]并不对 *identity* 进行匿名保护，而仅将 *location* 泛化为 k 个不同的位置。此时，匿名度退化为“泛化程度”。例如，某用户 a 及其所在位置周边用户 b、c、d 的初始位置如图 2(a)所示，不失一般性，用<X, Y>表示二维平面坐标，图 2(b)~图 2(d)分别展示了对用户 a 使用 4-匿名、$4-\delta$ 匿名以及泛化程度为 4 后的位置表示。

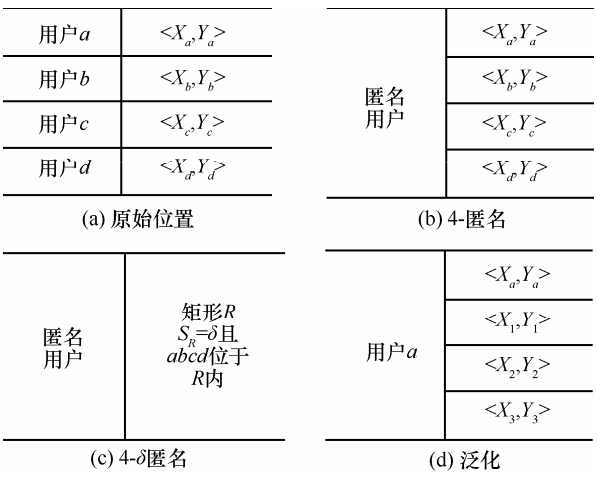


图 2　3 种隐私度量示意

最小半径适用于通过降低位置坐标精度来提高隐私程度的技术[10]中。应用该度量的位置隐私保护技术通常将位置视为一个半径为 R 的圆形区域，最小半径为 R_0 的含义即为用户发布的位置区域的面积不能小于 πR_0^2。

3　面向 LBS 的位置隐私保护技术

面向 LBS 的位置隐私保护的研究积累了一定技术成果。随着研究的推进，产生了若干个架构模型、隐私度量和技术指导思想，这些已在上一节进行了归纳，本节对当前的该类技术展开综述。给出一个对当前技术的分类，按照该分类对当前技术展开介绍，其中，重点介绍较新的和较为有代表性的技术。

表 1 和表 2 已经对当前技术按照架构模型、隐私度量 2 个角度进行了分类。本节按照各类技术对位置数据的保护方法，将当前技术分为 4 类：基于泛化法的位置隐私保护技术、基于模糊法的位置隐私保护技术、基于掩盖法的位置隐私保护技术以及基于加密法的位置隐私保护技术。下面将展开详细介绍。

3.1　基于泛化法的位置隐私保护技术

泛化法的基本思想是：将真实位置连同若干其他位置一并发送给 SP，并保证在发送的全部位置中，真实位置与其他位置是无法一次分辨的。使用泛化法技术时，SP 收到的是包含真实位置在内的位置集合，或包含多个位置的区域。泛化法使 SP 无法准确获知真实位置，从而保护了四元组中的 *location*。此外，大量泛化法技术还采取匿名手段以保护 *identity*。泛化法使用匿名度(伴有匿名区域)或泛化程度作为隐私度量。按照泛化时使用的其他位置的不同，泛化法技术可分为利用其他用户位置的泛化法技术和利用假位置的泛化法技术。

3.1.1　利用其他用户位置的泛化法技术

主要利用其他用户的位置数据实现泛化。方法是用一定面积大小的区域代替用户真实位置发送给 SP，并保证该区域中含有包括真实位置在内的多个用户位置。核心技术问题是如何获得周边其他用户的位置，以及如何对 LBS 返回结果进行处理。

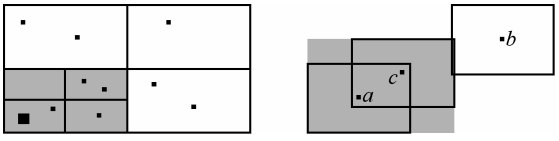
由于用户终端本身没有其他用户的位置信息，因此采用架构 2 或架构 3 实现，利用 TTP 或 P2P 络获取其他用户位置，实现泛化。以架构 2 为例，一般流程为：1) TTP 拥有区域内海量用户位置，用

户将位置信息发送至 TTP；2) TTP 利用其他用户位置实现泛化并生成匿名区域，将该区域连同服务请求发送给 SP；3) SP 将 LBS 中间结果发送给 TTP 后，TTP 再根据用户真实位置进行中间结果处理；4) TTP 将 LBS 最终结果发送给用户。

对于如何生成匿名区域，研究者们提出了多种方式。文献[13]提出了将全局区域分割成块，并利用块的组合生成匿名区域的方法。对于给定的匿名度 k，将用户所在区域均分为 4 块，计算包含真实位置的那一块中总用户数 x，若 $x>k$，则继续 4 分该块。重复该过程，直到 $x<k$ 为止，并返回该小块分割前的上一块作为匿名区域。图 3(a)展示了区域中黑色方点用户利用文献[13]的算法实现 3-匿名的过程，灰色部分为最终匿名区域。

Casper 技术[14]优化了文献[13]的方法，当找到 $x<k$ 的块之后，不立即返回其分割前大块，而首先尝试与相邻小块合并，如果合并的结果能够满足给定的匿名度 k，则返回该合并区域，否则再返回其分割前的大块。

某一时刻没有请求 LBS 的用户并不愿提供自身位置给 TTP。针对这个事实，CliqueCloak 技术[15]试图利用那些 LBS 发起者们自身的位置实现泛化。为每个 LBS 请求者的位置建立矩形框，并合并那些位置落入彼此矩形框中的用户，直至收集到给定匿名度个数的用户为止。图 3(b)中用户 a、b、c 先后发起了匿名度为 2 的 LBS 请求，TTP 则将用户 a 和用户 c 的矩形框合并成匿名区域(灰色)，用户 b 继续等待随后的其他用户位置。



(a) 文献[13]和 Casper 示意 (b) CliqueCloak 示意

图 3 基于其他用户位置的泛化法技术

文献[22]提出了基于架构 3 的泛化技术。避免了使用架构 2 所带来的安全隐患。

为应对轨迹探测攻击(见 4.1 节)，Zhang 等[16]提出互惠 k-匿名，保证在一段时间内生成的多个匿名用户集合保持不变。互惠 k-匿名增强了对轨迹探测攻击抵抗性，但因强制要求匿名集合的稳定，可能会影响匿名区域的面积，匿名区域过小则无法满足隐私程度，过大会增大 SP 的服务代价。Pan 等[17]提出的技术利用四元组 L 中的 $\vec{v}$ 来找寻更合理的匿名集，尽最大程度保持匿名集稳定，同时兼顾匿名区域大小。

3.1.2 利用假位置的泛化法技术

本类技术使用假位置实现泛化。优点是不需其他用户位置即可实现，但假位置的真实性则不如其他用户位置强。因此本类技术的核心问题是如何生成尽可能逼真的假位置。

Kido 等[7]提出了该类泛化技术，其算法采用随机方式生成假位置，也能够保证多次查询中生成的假位置带有轨迹性。

为使假位置具有真实场景下的意义，Shankar 等[8]提出 SybilQuery 技术，利用四元组 L 中的 *location* 和 $\vec{v}$ 生成高真实性的假位置。算法根据区域背景(地图、路网等)知识生成合理的起始假位置，在随后的轨迹生成中利用区域背景知识和 $\vec{v}$，生成与真实轨迹高度类似的假位置轨迹。

3.2 基于模糊法的位置隐私保护技术

通过降低位置精度来提高隐私程度。通常利用位置区域的面积(如最小半径)作为隐私度量，且不使用匿名手段。大多数模糊法技术无需额外信息的辅助，能够在用户终端直接实现，因此多使用架构 1 模型。

一种模糊法将坐标位置替换为语义位置。文献[9]利用带有语义的地标或参照物代替基于坐标的位置信息，实现模糊化。例如，图 4 中位于“中央公园”内的黑点位置所示用户，发起了查询“最近加油站”的 LBS，则该技术将黑点的坐标替换为“中央公园”并发送给 SP 进行查询。

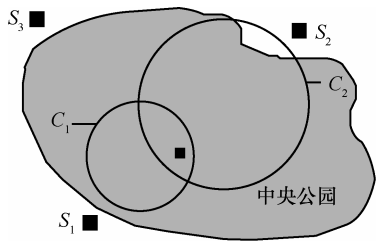


图 4 模糊法技术

文献[10]提出了用圆形区域代替用户真实位置的模糊法技术，此时，将用户初始位置本身即视为一个圆形区域（而不是坐标点），并提出 3 种模糊方法：放大、平移和缩小。利用 3 种方法中的一种或 2 种的组合，生成一个满足用户隐私度量的圆形区域。

一种模糊法技术[11]基于图模型实现地理空间的建模和模糊实现。用边带权图 $G(V,E)$对区域中用户以及兴趣点建模。点集 V 表示所有用户和所有兴趣点的集合。E 表示 V 中两点间的连通性，边的权值表示两点间路程的长度。当用户向 SP 发送位置信息时，该技术将真实位置与 V 的一个子集 O 一并发送给 SP，这相当于降低了用户位置精度，实现了模糊化。注意该技术与 k-匿名泛化不同的是：对于四元素 L 中的 *identity* 不匿名处理，且模糊集 O 中的点也不一定是用户的真实位置，还包含兴趣点。

与泛化法不同，多数模糊法技术没有能力对 LBS 返回结果进行处理，往往产生较粗糙的 LBS 结果。仍以图 4 中用户请求“最近加油站”为例，事实上 S_1 是最近加油站，当选择 C_1 作为其模糊区域时能够寻找到正确结果；但当选择了隐私程度更高的 C_2 作为模糊区域时，SP 将返回 S_2 作为结果。所以，虽然由于半径 $r_2 > r_1$，使得用户的隐私程度提高，但此时 SP 没有最好的满足用户需求。模糊法技术应解决如何在“保证 LBS 服务质量”和“满足用户隐私需求”之间寻求平衡的问题。解决该问题的一种方式是在 SP 和用户之间采用迭代问询的方法，不断征求用户是否同意降低其隐私度量，在有限次的迭代中尽可能地提高服务质量[11]。

3.3　基于掩盖法的位置隐私保护技术

指在特定或全部场景下，用户通过不对外发布位置来实现保护位置隐私的目的。掩盖法技术使 SP 无法(在特定情况或所有情况下)获得用户位置。按照在特定情况下掩盖和在所有情况下掩盖，掩盖法技术可分为 2 类：1)按需掩盖法，仅当真正有必要发布位置时，才以某种特定形式向 SP 发送一次位置，其他情况下将位置掩盖；2)完全掩盖法，彻底选择不发布位置数据，利用技术手段主动向 SP 索取所需信息。

3.3.1　按需掩盖法

Mix zones[18,19]技术是一种按需掩盖技术。Mix zones 技术将整体区域划分为 2 类：掩盖区和应用区，并规定仅当用户位于应用区时才允许其对 SP 发布位置信息；否则当用户位于掩盖区时掩盖位置。为所有用户事先赋予一个假名，且当用户进入或离开掩盖区时都更换新假名。这样，mix zones 技术就保证了仅当用户位于特定区域时 SP 才能获知其位置。例如图 5 所示，某一时刻假名分别为 A、B、C 的用户进入掩盖区后，立即停止对 SP 的位置发布。一段时间后，假名为 X、Y、Z 的用户离开掩盖区并恢复与 SP 的位置发布。SP 无法分辨$\{A, B, C\}$与$\{X, Y, Z\}$的关系，本例中理论上离开掩盖区的一个用户是进入掩盖区的某个用户的概率为 $\frac{1}{3}$。

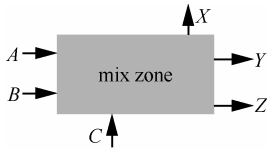


图 5　mix zones 示意

MobiMix 技术[20]在 mix zones 基础上，针对现实中能被攻击者利用的背景知识，建立更合理的掩盖区。基本思想是用不规则多边形及其组合建立掩盖区的形状，使其更适应当前场景，提高隐私程度。相对于 mix zones 技术，MobiMix 技术使攻击者无法利用四元组 L 中 $\vec{v}$ 和 *time* 特性辨识用户。

3.3.2　完全掩盖技术

2PASS[12]是基于二维 Voronoi 图模型的完全掩盖技术，基本思想是将图 1 右侧展示的一般 LBS 流程拆分为 2 步：第 1 步用户首先向 SP 请求区域内为某类兴趣点事先建立好 Voronoi 图；第 2 步用户结合自身位置和 Voronoi 图，向 SP 索要某些兴趣点的信息。由于用户与 SP 直接通信，故采用架构 1 实现。

为此，要求在 SP 处为每一类兴趣点构造并维护一个 Delaunay 三角并为每个兴趣点赋权值，权值表示兴趣点所属 Voronoi cell 的面积，这相当于维护了一个该兴趣点的 Voronoi 图。例如，某区域内点 a、b、c、d、e、f 是用户 A 周边的快餐店位置，以这些快餐店为兴趣点生成的 Voronoi 图和对应的 Delaunay 三角如图 6 所示。此时，用户 A 在当前位置查询“距离我最近的快餐店的菜单”。首先向 SP 请求该图，结合用户位置和 Voronoi 图可知，c 为距离用户 A 最近的快餐店；继而 A 向 SP 请求 c 的相关信息。

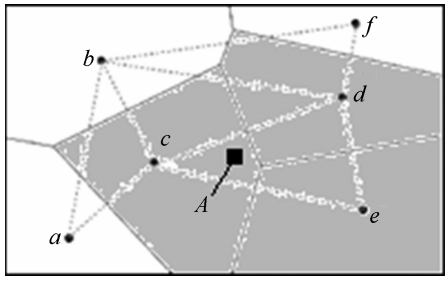


图 6　2PASS 示意

2PASS 技术利用 2 次通信，在掩盖用户位置的同时不降低服务质量获得 LBS，但其并未实现“绝对隐私”。SP 仍可以利用其最终请求的信息来推测用户当前位置。上例中 SP 根据用户的请求，可以推测用户位于 c 所在多边形中。因此仍需要用隐私度量来描述隐私程度，该技术的隐私程度可以采用泛化程度和模糊区域面积来衡量。对于泛化程度，由于根本没有将任何位置信息发送给 SP，所以可以认为是无限大的；对于模糊区域，给定区域大小 x 后，用户可以在第 2 步，向 SP 请求多个目标信息，使各个兴趣点的权值之和不小于 x，这样就满足了模糊区域要求。图 6 中用户 A 若向 SP 请求 c、d、e 3 个快餐店信息，则其模糊区域为图中灰色部分。

受移动设备性能制约，使基于架构 1 的掩盖法效率受到限制。Jang 等[21]提出了基于架构 2 的掩盖技术。该技术在 2PASS 基础上，添加 TTP 充当掩盖服务器，用户向掩盖服务器发送位置和 LBS 请求，掩盖服务器随后采取与 2PASS 中用户端相同的方式，向 SP 先后请求兴趣点索引和 LBS 信息，最后掩盖服务器将用户需要的信息发送给用户。

3.4 基于加密法的位置隐私保护技术

该类技术的基本思想是通过对位置数据进行加密或加密后拆分，来避免 SP 获得精确位置。

文献[25]提出一种基于对称加密的技术，能够实现在不暴露自身位置的前提下，当用户的某兴趣点接近该用户时对该用户进行提醒。

文献[26]提出一个基于同态加密的技术，实现了 2 个用户在彼此都不知道对方位置的前提下进行两者间距离查询的 LBS。

另一类位置加密法技术则不过于强调密文的强壮性，而是通过将一个位置数据进行加密并拆分，分布于多个 SP 中，使攻击者如果想获得用户位置数据就必须联合或攻击多个 SP 才能实现，这也从事实上降低了位置数据的隐私风险。文献[27]提出 STS 技术，将位置数据利用随机数加密并拆分，再将密文片段存放于多个 SP 中，当 SP 需要该用户位置来执行 LBS 查询时向每个密文片段持有者申请。Wernke 等[28]提出 Position Sharing 技术，将用户的精确位置拆分成若干个称为“share”的碎片，并分布存于多个 SP 中。与文献[27]中的密文片段不同的是，每个 share 单独都能表征一个比真实位置精度低的粗略位置信息，多个 share 可以进行融合，获得的 share 个数越多，则越能够精确地接近用户的原始位置。当用户发起 LBS 时，根据 LBS 的位置精度要求，SP 仅需要获取若干个 share 使之融合后的位置能够满足要求即可，而不是必须获得全部 share。

4 面向 LBS 的位置隐私保护讨论

对位置隐私保护技术的讨论，主要基于 2 个角度：技术应对于现有各类攻击时的有效性，技术面向 LBS 时的适用性。

4.1 位置隐私保护技术与面向位置隐私的攻击

在 LBS 过程中，位置隐私面临的攻击与威胁是多方面的。文献[23]总结了现存的攻击行为，按照攻击者所掌握的知识划分，主要分为如下几类。

1) 利用地域背景知识(RBA, regional background knowledge attack)

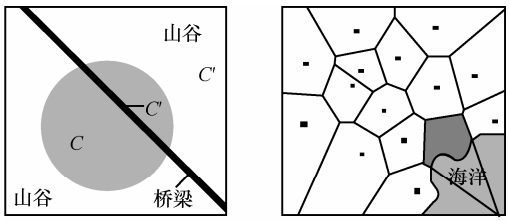
利用地域背景知识(地图、路网等)推测用户的真实位置，降低隐私程度[29]，该类攻击对不考虑地域背景知识的位置隐私保护技术具有普遍的威胁性。例如，图 7(a)和图 7(b)中，攻击者将分别使用了模糊法和 2PASS 技术后的位置叠放于相应的地图之上。前者攻击者利用地图可以将模糊区域由圆 C 缩小为区域 C'；后者真实位置所在的 Voronoi cell 覆盖了一大片不可达区域（海洋），因此其可能的位置区域就缩小了。

2) 利用用户背景知识(PBA, personal background knowledge attack)

一些情况下攻击者事先掌握了用户背景知识，例如工作单位、家庭住址等，这些知识可以用来降低隐私程度[13]。例如，用户 a 在一次 LBS 过程中利用某泛化技术已实现了 3-匿名，但若攻击者掌握了“a 是一个小学生”这样的背景知识，并且 3 个匿名用户所在的位置语义分别为警察局、酒吧和小学，则攻击者就能够以较高的概率来认定位于小学的匿名用户即为 a。

3) 利用位置四元组

一类攻击利用了四元组 L 中的要素。最大移动范围推测(MBA, max boundary attack)利用 L 中速度 v 来推算用户的可能移动最大距离[30]。图 7(c)中 C_1 和 C_2 是同一个用户利用模糊技术，先后在时刻 t_1 和 t_2 生成的模糊区域。攻击者利用 t_1 时刻的速度 $\vec{v}$，能够以 $|\vec{v}|(t_2-t_1)$ 的半径增量生成一个 t_1 至 t_2 时间段的最大可能移动区域 C_3，则 t_2 时的真实位置将极高概率的位于 C_3 与 C_2 的重叠区域，这大大缩小了原模糊法的模糊区域 C_2。



(a) RBA作用于模糊法　(b) RBA作用于2PASS

(c) MBA作用于模糊法　(d) LDA作用于泛化法

图 7　4 种攻击示例

位置分布性推测(LDA, location distribution attack)[31]利用区域内多个用户的四元组 L 中的 *location* 来推算 LBS 发起用户的 *location*，主要针对泛化法技术。当攻击者获得一个匿名区域后，首先将区域内所有用户，都假象为 LBS 发起者。随后按照当前采用的具体技术，计算这些用户各自应生成的匿名区域。显然，这些生成的匿名区域中，最接近真实匿名区域的那个用户是有最大可能的。如图 7(d)所示，攻击者掌握了多个用户的当前位置，并截获了一个 3-匿名技术所生成的匿名区域 δ。攻击者为 δ 中的用户 A、B、C 分别依据当前采用的泛化技术建立各自的匿名区域，显然用户 B 对应的匿名区域与 δ 最为吻合，则攻击者可以以较高的概率断定 B 为此次 LBS 的发起者。

4) 轨迹探测(TA, trajectory attack)

该类攻击不关心某时刻精确位置，而是位置的轨迹特性[13]，对轨迹型 LBS 危害较大。对位置的连续观测是主要的攻击手段，能够威胁泛化法、模糊法和抑制法中的很多位置隐私保护技术。当攻击者获得足够多的位置后，即便每次位置刷新都能保证了一定的隐私，但仍可从中辨认出轨迹特征。图 8 展示了分别使用了某泛化法、模糊法和完全掩盖法的 3 个用户在时刻 t_1 至 t_4 内向 SP 发送的匿名区域(泛化法)、模糊区域(模糊法)和攻击者能够间接判断出的模糊区域(掩盖法)，图中的粗线即是 3 个用户的大致轨迹信息。该类攻击往往会结合区域背景知识攻击，能够使攻击者获得较高精度的轨迹信息。

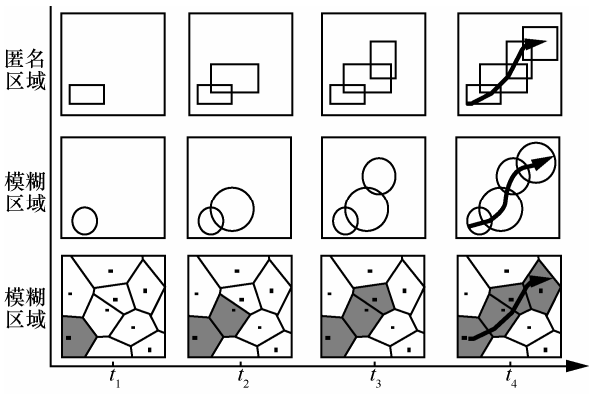


图 8　轨迹探测攻击

5) 反匿名化(AAA, anit-anonymization attack)

该攻击目的是对四元组 L 中 *identity* 的识别，以及 *identity* 和 *location* 的匹配。通常要求攻击者具备大量的位置数据和较强的计算能力，常威胁位置大数据发布时的位置隐私，但也能够在移动互联网场景下对位置隐私构成一定威胁。对于没有采用匿名化的位置隐私保护技术，攻击者可以直接将 *identity* 与 *location* 建立匹配。对于匿名化后的位置数据，攻击者可以利用连同位置发布的其他信息中，将若干用户属性（例如性别、邮政编码、生日等）合并成“准标识符”（QI, quasi-identifier）。QI 虽不能像 *identity* 那样直接匹配一个具体用户，但在大数据场景中，利用 QI 并结合某些用户背景知识能够高概率地识别匿名用户。例如文献[32]中指出，利用生日、性别、邮政编码等看似非隐私性的个人属性，预计可以正确唯一识别出全美国 87%的人口。

针对这些攻击以及当前现有的技术对攻击的有效性的研究，表 3 给出了文中提及的技术与攻击之间的有效性关系。

其中用“√”表示某技术能够抵御某类攻击，灰色区域表示某类攻击与某技术无关，最右列“TTP”表示通过攻击 TTP 来威胁位置隐私的攻击。通过对比表 3，现有问题包括如下。

1) 除文献[16,17]等外，多数技术都不能应对轨迹探测攻击，更多技术仅限于保护单次位置发布而对轨迹型 LBS 场景下的位置隐私保护考虑不够。

2) 不采用匿名手段的技术无法应对反匿名化攻击，而 4.2 节指出了在有验证 LBS 场景下无法使用匿名技术，这引入了一个矛盾。现有研究没有解决如何使位置隐私保护技术在适用于有验证 LBS 的同时又能够抵御反匿名化攻击这个问题。

3) 对于各类导致降低隐私程度攻击，现今没有

完美的解决办法，为了抵御该类攻击而往往带来了过大的查询代价(如文献[16]为应对 TA 和 MBA)或引入了更多的流程环节(如文献[12]为应对 PBA)。

4) TTP 威胁是所有采用架构 2 的技术所无法回避的威胁，如 2.2 节对当前威胁模型假设的介绍那样，现有基于架构 2 的技术，都假设一个完全可信的 TTP 并在 LBS 阶段扮演核心角色，而该假设合理性显然会受到质疑。受移动互联网设备性能限制，除模糊法等技术外，大量位置隐私保护技术无法脱离中间结构实现，目前还没有基于不可信第三方作为中间结构的位置隐私保护技术。

5) 表 3 列出各技术对于单一攻击的抵御能力有效性。但如何应对攻击者使用多种攻击手段结合的方式展开攻击，仍然少有研究。

表 3 现有技术应对攻击的有效性

位置隐私保护技术		位置隐私攻击						
		RBA	PBA	MBA	LDA	TA	AAA	TTP
泛化法	文献[13]	√		√				
	文献[14]	√		√				
	文献[15]	√			√			
	文献[22]	√			√			√
	文献[16]	√		√	√	√		
	文献[17]	√		√	√	√		
	文献[7]			√				√
	文献[8]	√		√		√		√
模糊法	文献[9]	√		√				√
	文献[10]							√
	文献[11]	√		√				√
掩盖法	文献[18,19]		√	√	√			
	文献[20]	√	√	√	√	√		
	文献[12]		√	√	√			√
	文献[21]		√	√	√			
加密法	文献[25]	√	√	√	√	√		√
	文献[26]	√	√	√	√	√		√
	文献[27]		√				√	√
	文献[28]			√		√		√

4.2 位置隐私保护技术与 LBS

对于技术优劣的评价，不仅基于其应对攻击行为时的有效性，同时也体现在其适用广度上。当前研究和其他综述类工作，还没有从 LBS 适用性的角度讨论 LBS 中的位置隐私保护技术，原因是当前还没有一个对 LBS 的合理分类。本文提出比较完备的 LBS 分类，并在此基础上讨论技术的适用性。对 LBS 的划分依托如下 3 个角度。

1) 按 LBS 是否需要用户身份验证（即 LBS 的提供是否依赖 L 中的 *identity*），可以将 LBS 分为有验证 LBS 和无验证 LBS。有验证 LBS 除 *location* 外，需要用户提供四元组 L 中的 *identity*；无验证 LBS 无需 *identity* 即可实现。

2) 按 LBS 返回的服务内容，可以将 LBS 分为社会信息 LBS 和个人信息 LBS。社会信息 LBS 的返回内容是不包含其他用户位置的社会类信息（例如基础设施信息、导航或商务信息等），可以由 SP 直接提供；个人信息 LBS 指那些在提供服务之前，首先需要 SP 请求其他用户位置的 LBS（例如 2 个用户之间的距离查询）。

3) 按 LBS 对位置的需求方式，可以将 LBS 分为单点型 LBS 和轨迹型 LBS。前者仅需要提供一次位置即可实现；后者则需要用户持续的刷新位置。

上述 3 个独立的划分角度可以将 LBS 分为 8 类，为形象化的使读者理解该分类，表 4 是针对各个种类 LBS 的举例，其中，有些是已经在现实中存在的 LBS。该分类对 LBS 提供了一个可参考的划分准则，同时对位置隐私保护技术的适用性分析建立了基础。

表 4 各类 LBS 举例

编号	LBS 分类	典型 LBS	应用
1	有验证/社会信息/单点	查看附近可以使用我的代金券的饭店	大众点评
2	有验证/社会信息/轨迹	当我预订的出租车预计 3 min 内到达时提醒我出门	快的打车
3	有验证/个人信息/单点	查看附近的好友	人人网
4	有验证/个人信息/轨迹	实时共享我的位置	微信
5	无验证/社会信息/单点	查看当前附近的加油站	百度地图
6	无验证/社会信息/轨迹	为我导航至哈尔滨工业大学	高德地图
7	无验证/个人信息/单点	查看附近的人	微信
8	无验证/个人信息/轨迹	发现附近参与玩家最多的游戏	SCVNGR

各类研究往往强调其技术应对各类攻击的有效性，但没有指明技术的 LBS 适用性。技术本身会降低 LBS 适用性，例如，从原理上考虑，泛化法技术[13]等由于使用了匿名手段，将无法适用于有验证 LBS；从代价上考虑，文献[12]提出的掩盖法，其对个人位置的 Voronoi 图建模和维护的代价将会巨大，因此很难应用个人信息 LBS。本文通过对现有技术的总结和分析，用表 5 给出了本文提及技术的

LBS 适用性。

表 5　　现有技术对各类 LBS 的适用性

位置隐私保护技术		LBS 分类							
		1	2	3	4	5	6	7	8
泛化法	文献[13]					√	√	√	√
	文献[14]					√	√	√	√
	文献[15]					√	√	√	√
	文献[22]					√	√	√	√
	文献[16]					√	√	√	√
	文献[17]					√	√	√	√
	文献[7]	√	√			√	√		
	文献[8]	√	√			√	√		
模糊法	文献[9]	√	√	√	√	√	√	√	√
	文献[10]	√	√	√	√	√	√	√	√
	文献[11]	√	√	√	√	√	√	√	√
掩盖法	文献[18,19]					√	√	√	√
	文献[20]					√	√	√	√
	文献[12]	√	√			√	√		
	文献[21]	√	√			√	√		
加密法	文献[25]			√	√			√	√
	文献[26]			√	√			√	√
	文献[27]	√	√	√	√	√	√	√	√
	文献[28]	√	√	√	√	√	√	√	√

对比表 4，现有问题概述如下。

1) 对于泛化法技术，现有工作投入了大量研究，是目前最为受关注的方法。但由于现有该类技术大量采用匿名化手段使其无法适用于有验证 LBS，严重影响该类技术的普适性，目前尚无有效解决该问题的技术出现。

2) 对于模糊法技术，其适用性较为广泛，但其不足主要体现在对 LBS 服务质量的严重降低上，文献[11]提出了几种控制服务质量降低程度的办法，但这些办法均代价过大或难以满足需求。

3) 掩盖法对位置的(彻底的或按需的)抑制使其牺牲了一定的 LBS 适用性，例如用户在 mix zones 技术设置的掩盖区中无法与 SP 刷新位置，这在现实中是不实际的。2PASS 中使用的 Voronoi 图对社会信息建模时复杂度尚可接收，但若对实时个人位置信息建立 Voronoi 图的话则会面临其更新过于频繁的问题，这导致其难以适用于个人信息类 LBS。

4) 加密法是传统数据加密技术在位置隐私保护上的延伸，但由于传统加密本身与 LBS 实现前提有矛盾，导致其适用性较低。文献[26]试图利用同态加密技术使 LBS 基于密文即可实现，但其还仅限于个人信息 LBS 一类，仍没有解决如何将传统密法应用于社会信息 LBS 的问题。以文献[27,28]为代表的密文片段方法则具有较强的普适性。表 5 列出了各类技术对 LBS 的适用性，是从一个侧面去比较当前技术的特性，而不是对当前技术优劣的绝对定论。例如，模糊法技术能够适用于全部类型的 LBS，但并不说明该类技术是当前最理想的技术，事实上，模糊法技术所面临的很多攻击行为至今都没有得到很好的解决。因此为了更好地理解当前技术发展现状，还需要对位置隐私保护技术与当前的攻击手段进行匹配和比较。

5　面向定位服务的位置隐私保护

定位服务的一般原理是：移动设备将感知到的周边通信基础设施标识发送给 LP，设施包括 WLAN 接入点、GSM/CDMA 基站等[3]，而 LP 则拥有海量的通信基础设施的地理位置数据。结合该数据和设备发送的接入点信息即可得出用户的当前位置。移动互联网中位置隐私保护研究的至今大部分工作，都围绕面向 LBS 展开。然而，另一个同等重要的问题是在定位过程中保护用户的位置隐私[4]。考虑如下场景：小明在其手机上同时使用了 Google 定位服务[34]和 Google 地图，并使用“查看附近的快餐店”LBS。此时 Google 将同时扮演 SP 和 LP 2 个角色，显然，即使小明在“查看附近快餐店”时使用了良好的面向 LBS 的位置隐私保护技术，其位置仍会被 Google 在定位服务过程中获得[35]。因此，解决移动互联网下的位置隐私保护问题，必须要同时解决 2 类位置隐私保护问题。本节对面向定位服务的位置隐私保护展开综述和讨论。

5.1　移动互联网定位技术及隐私威胁

图 1 中虚线左侧是移动互联网中定位阶段的一般场景。当前存在多种定位技术，这些技术按照位置隐私的角度，可划分为 2 类[4]。

1) 基于终端的定位技术。利用自身移动设备直接进行定位的技术，主要指卫星定位技术，例如 GPS 定位。其优点是能够在全球范围内覆盖，定位精度较高，且无需第三方参与，安全性较强；缺点

是在室内或某些城际区域内无法定位或精度受限，而且该技术对移动终端的能耗较大。此外，近年来卫星定位技术本身的隐私性也常常受到质疑。

2) 基于 LP 的定位技术，即第三方定位服务。用户从 LP 处获得自身位置，现有技术主要有手机基站定位、WLAN 热点定位[36,37]等。近年来也出现了复合型定位技术[38]，复合型定位服务结合了卫星、通信基站和 WLAN 热点等多种技术，为用户提供更优质的定位服务。该类技术有较强的区域适应性，在室内和城际环境下能够良好定位，且能耗较低；但面临着来自第三方 LP 或其他恶意攻击者的位置隐私威胁。

基于终端的定位技术虽然存在自身的隐私问题，但不在定位服务的位置隐私保护问题范畴内。本文专注于研究移动互联网中基于 LP 的定位技术下存在的位置隐私问题。有关卫星定位位置隐私保护详细内容参见文献[39]。

在基于 LP 的定位技术中，一类威胁模型即如图 1 虚线左侧所示，此时 LP 是威胁来源。使用定位服务的用户一方面希望获得自身位置，另一方面不希望自身位置被 LP 获得。另一类威胁来自 LP 以外的攻击者，称为位置欺诈(location-spoofing attack)[40]。如图 9 所示，攻击者首先获取了用户所在位置周边的各类接入点信息，通过伪装这些接入点并向 LP 请求位置，来获取目标用户的位置。

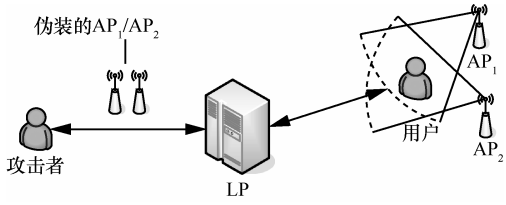


图 9　位置欺诈示意

5.2　现有技术和方法

对定位服务中的位置隐私保护技术的研究仍处于起步阶段，现有的主要技术和方法有：基于隐私政策的位置隐私保护和位置欺诈防御技术。

一种隐私政策是基于二元选择的用户协议。当用户开启其移动设备的定位服务时，可以选择同意或拒绝 LP 采集用户周边的各类接入点信息，用户必须明确地同意 LP 采集其相关数据后，LP 才能够进行数据采集，这从一定程度上保护了用户的位置隐私，图 10 是安卓系统下百度定位服务[41]的请求提示。

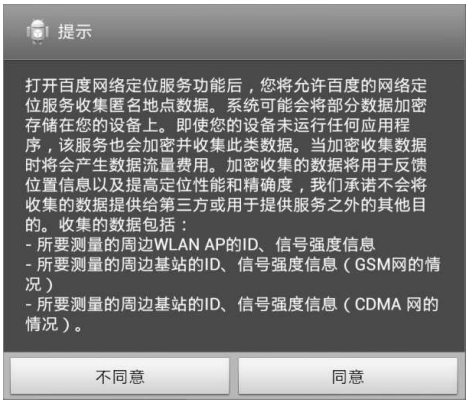


图 10　百度定位服务的隐私政策

另一种隐私政策考虑到用户可能不愿意其所拥有的接入点资源(通常是 WiFi 接入点)被 LP 采集到其地理数据库中的情况。2011 年，Google 发布了删除并不再采集那些不愿被收录入数据库 WiFi 接入点的隐私保护政策[42]。只要用户将其拥有的接入点 SSID 加后缀“*_nomap*”，Google 就会删除或停止采集其位置。该政策从一定程度上缓解了用户的位置隐私威胁，同时也对位置欺诈有一定的防御作用。

针对位置欺诈攻击，2014 年，Peng 等[43]提出了一个面向位置欺诈的位置隐私保护技术。利用空间和时间概率模型，评测移动设备在真实场景下接收 RSS 的概率特性，并以此分辨真实用户的位置请求和攻击者发送的虚假位置请求。

6　未来研究方向

通过本文的综述和研究可知，移动互联网中的位置隐私保护仍需继续深入研究。本节分别对 2 类位置隐私保护给出未来研究方向的建议。

6.1　面向 LBS 的位置隐私保护未来研究方向

第一，4.1 节和 4.2 节从位置隐私攻击和 LBS 适用性 2 个角度，总结了当前研究现状并指出了现存问题。未来应结合表 3 和表 5，对各类技术展开进一步研究，使其获得更多的 LBS 适用性和更强的攻击抵御能力。

第二，建立统一化位置隐私度量。使基于不同技术思想的各类位置隐私保护技术能够在统一的量化指标下进行比较和分析。文献[10,44]分别试图用统一化的度量，但目前为止还没有其他技术使用其度量。本文建议未来完成这个目标可以分为 2 个步骤：1)结合表 5，为各类 LBS 建立各自的隐私度量，以评估各个技术在该类型 LBS 下的表现；2)参照 3 个 LBS 划分角度，对建立起的各类度量进行

融合，最终实现位置隐私度量统一化。

第三，当前技术没有实现位置的“绝对隐私”保护，未来应研究支持绝对隐私的技术。现有技术如文献[45]将隐私信息检索技术应用于领域中，能够实现绝对隐私但仅适用于特殊 LBS 场景，未来应研究具有普适性的绝对隐私技术。

最后，随着网络和设备性能的发展，未来应对现有的问题假设和架构模型进行重新思考。本文认为其中应着重研究的问题主要有：1)研究基于更多不可信假设的保护技术，包括不可信中间件和不可信用户终端；2)研究基于高性能移动设备的保护技术。现有技术往往不对移动设备的性能抱有太大期望，但随着网络和硬件性能的提高，未来可以实现不借助架构 2 或架构 3 的复杂保护技术。

6.2　面向定位服务的位置隐私保护未来研究方向

针对此类位置隐私保护，本文提出未来技术研究方向有：降低定位频率、完善隐私政策以及若干技术方向。

第一，降低定位频率。通过降低定位频率可以减少位置隐私泄露风险。未来应研究如何在不影响 LBS 使用的前提下减少定位次数。一种方法是利用设备（不包括 GPS）自主获得位置，将定位服务变为赋予初始位置，以及误差偏移修正的手段。在此方面，文献[46]提出的 WheelLoc 技术利用设备普遍内嵌的移动传感器，能够实现精度 40 m 的自定位，但将其应用于移动互联网中仍有问题需要解决，未来应深入进行该方向的研究。另一种方法是请求一部分 LP 用以计算位置的接入点数据到自身设备中，再在移动设备上自行计算位置。这类似于 3.3 节介绍的完全掩盖法。在此思想上有所实现的是 Intel 的 POLS[47]技术，但其主要问题是无法与当前的商业模式融合。未来应将该思想纳入研究视野。

第二，完善隐私政策。当前隐私政策单一，往往仅限于用户对服务条款的二元选择（是或否）。未来应研究较为完善的位置隐私政策，包括采集频度政策、粒度控制政策、匿名政策等多种隐私保护政策。2013 年 Damiani 等[4]提出如图 11 所示的位置隐私政策管理架构模型。在用户与 LP 之间添加 TTP 作为定位请求管理器，相关隐私政策由专门的政策管理器管理。请求管理器将相关隐私政策和用户的隐私需求，向 LP 安全的请求位置信息。

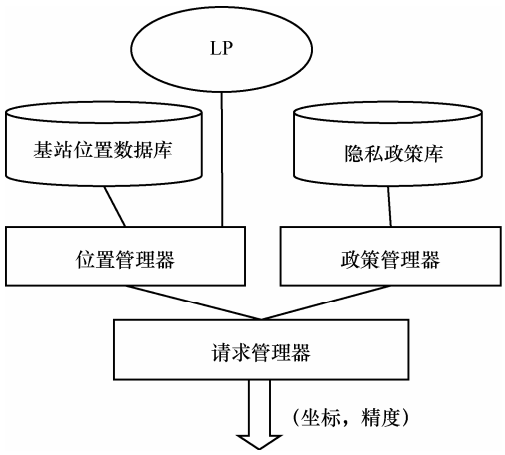
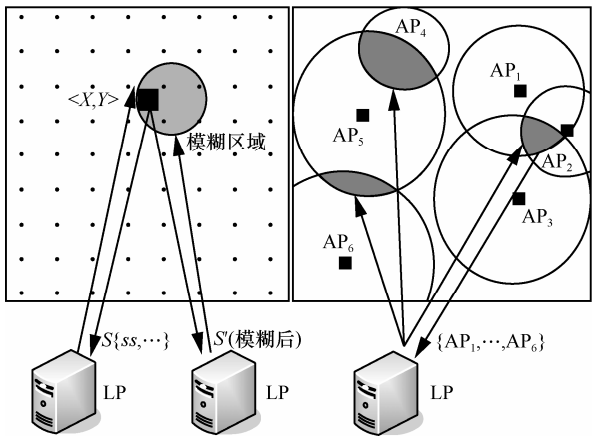


图 11　定位服务中的隐私政策架构

第三，研究面向定位服务的位置隐私保护技术，对此本文给出 2 个未来研究建议。首先对 “定位模糊化”技术展开研究。借鉴模糊法思想，使 LP 仅能将用户定位于较粗粒度水平的区域内，从而达到保护用户位置隐私的目的。以基于 WLAN（IEEE 802.11）的指纹定位法[48]为例，设采集的指纹 RSS 值为：S:{ss_1, ss_2,⋯, ss_n}，改变 S 中的参数后，值为：S':{ss_1', ss_2',⋯, ss_n'}，并保证 S' 仍具有查询意义。未来技术应使 LP 对 S' 的查询结果，能产生可控的位置模糊化，并返回给用户。图 12(a)展示了该思想。



(a) 定位模糊化　　(b) 定位泛化

图 12　2 种研究思想示意

其次是“定位泛化”技术，参考泛化法思想，使 LP 在一次定位过程中仅能将用户定位于若干无法分辨的位置之中。此技术可以利用冗余 AP 信息实现。即用户在定位时，除发送当前的周边 AP 数据外，还发送若干“干扰”AP 数据，这些干扰数据可以利用移动设备本身存储的历史 AP 信息（绝大部分智能移动设备都支持该特性）充当；随后 LP

在定位过程中，会查询出若干个位置，一并发送给用户。此时，即实现了泛化。图 12(b)以 WLAN 定位中的三角定位原理为例，展示了该思想。

最后本文指出，面向定位服务的位置隐私保护的研究，应考虑与当前定位服务的商业模式相融合。LP 与 SP 不同，当前的 LP 均是世界大型 IT 巨头，其商业模式是研究者不得不考虑的问题，如果一个位置隐私保护技术与LP的商业模式无法融合，那其也失去了应用意义(如文献[47])。

7　结束语

移动互联网时代的来临，使基于位置的服务成为人们最为常用的信息服务类型，未来也势必进一步改变人类的生活方式。在移动互联网中，如何保护用户的位置隐私，是移动互联网能够进一步普及和发展的重要安全保证。当前的各类相关研究向我们展示了位置隐私保护的可行性，以及技术上的不断进步。本文较为全面地介绍和分析了移动互联网中位置隐私保护的一般概念、保护技术、攻击技术，并对当前研究中的关键技术进行了对比，讨论了各类保护技术的适用性和攻击抵御能力，指出了未来应着重解决的问题和若干研究方向。相信随着位置隐私保护技术的不断完善和进步，移动互联网将能够更加深入地融入人类生活的各个领域。

参考文献：

[1] KIM H, KIM J, LEE Y, *et al*. An empirical study of the use contexts and usability problems in mobile Internet[A]. Proceedings of the 35th Hawaii International Conference on System Sciences (HICSS 2002)[C]. Hawaii, 2002.

[2] Internet trends 2014[EB/OL]. http://www.kpcb.com/internet-trends, 2014.

[3] The Unital States' global surveillance recond[EB/OL]. http://news.xinhuanet.com/201- 4-05/26/c_1110865223.htm, 2014.

[4] DAMIANI M L, CUIJPERS C. Privacy challenges in third-party location services[A]. IEEE 14th International Conference on Mobile Data Management(MDM 2013)[C]. Milan, Italy, 2013.

[5] DUCKHAM M, KULIK L. Location Privacy and Location-Aware Computing[M]. FL: CRC Press, 2006.

[6] 周傲英, 杨彬, 金澈清, 等. 基于位置的服务：架构与进展[J]. 计算机学报,2011,34(7): 1155-1171.
ZHOU A Y, YANG B, JIN C Q, *et al*. Location-based services: architecture and progress[J]. Chinese Journal of Computers, 2011, 34(7): 1155-1171.

[7] KIDO H, YANAGISAWA Y, SATOH T. An anonymous communication technique using dummies for location-based services[A]. Proceedings of the International Conference on Pervasive Services(ICPS 2005)[C]. Santorini, Greece, 2005. 88-97.

[8] SHANKAR P, GANAPATHY V, IFTODE L. Privately querying location-based services with sybilQuery[A]. Proceedings of the 11th International Conference on Ubiquitous Computing(UBICOMP 2009)[C]. 2009. 31-40.

[9] HONG J I, LANDAY J A. An architecture for privacy-sensitive ubiquitous computing[A]. Proceedings of the 2nd International Conference on Mobile Systems, Applications, and Services(MOBISYS 2004)[C]. Boston, Massachusetts, USA, 2004. 177-189.

[10] ARDAGNA C A, CREMONINI M, DAMIANI E. Location privacy protection through obfuscation-based techniques[A]. Proceedings of the 21st Annual IFIP WG 11.3 Working Conference on Data and Applications Security[C]. 2007. 47-60.

[11] DUCKHAM M, KULIK L. A formal model of obfuscation and negotiation for location privacy[A]. Proceedings of the 3rd International Conference on Pervasive Computing(PERVASIVE 2005)[C]. Munich, Germany, 2005. 152-170.

[12] HU H B, XU J L. 2PASS bandwidth-optimized location cloaking for anonymous location-based services[J]. IEEE Transactions on Parallel and Distributed Systems, 2010, 21(10): 1458-1472.

[13] GRUTESER M, GRUNWALD D. Anonymous usage of location-based services through spatial and temporal cloaking[A]. Proceedings of the 1st International Conference on Mobile Systems, Applications and Services (MOBISYS 2003)[C]. San Francisco, California, 2003. 31-42.

[14] MOKBEL M F, CHOW C Y, AREF W G. The new casper: query processing for location services without compromising privacy[A]. International Conference on Very Large Data Bases (VLDB 2006)[C]. Seoul, South Korea, 2006. 763-774.

[15] GEDIK B, LIU L. Location privacy in mobile systems: a personalized anonymization model[A]. Proceedings of the 25th IEEE International Conference on Distributed Computing Systems (ICDCS 2005)[C]. Columbus, OH, USA, 2005. 620-629.

[16] ZHANG C Y, HUANG Y. Cloaking locations for anonymous location based services: a hybrid approach[J]. Geoinformatica, 2009, 13(2): 159-182.

[17] PAN X, MENG X F, XU J L. Distortion-based anonymity for continuous queries in location-based mobile services[A]. Proceedings of the ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems(GIS 2009)[C]. Seattle, Washington, 2009. 256-265.

[18] BERESFORD A R, STAJANO F. Location privacy in pervasive computing[J]. IEEE Pervasive Computing, 2003, 2(1): 46-55.

[19] BERESFORD A R, STAJANO F. Mix zones: user privacy in location-aware services[A]. Proceedings of the 2nd IEEE Annual Conference on Pervasive Computing and Communications Workshops[C]. 2004. 127-131.

[20] PALANISAMYB, LIU L. MobiMix: protecting location privacy with mix-zones over road networks[A]. IEEE 27th International Conference on Data Engineering (ICDE 2011)[C]. 2011. 494-505.

[21] JANG M Y, CHANG J W. A new cloaking method based on weighted adjacency graph for preserving user location privacy in LBS[J]. Computer Science and its Applications, 2012, 203: 129-138.

[22] GHINITA G, KALNIS P, SKIADOPOULOS S. Mobihide: a mobile peer to peer system for anonymous location-based queries[A]. Proceedings of the 10th International Conference on Advances in Spatial and Temporal Databases (SSTD 2007)[C]. Boston, MA, USA, 2007. 221-238.

[23] WERNKE M, SKVORTSOV P, DURR F, *et al*. A classification of location privacy attacks and approaches[J]. Personal and Ubiquitous Computing, 2012, 18(1): 163-175.

[24] CHOW C Y, MOKBEL M F. Trajectory privacy in location-based services and data publication[J]. SIGKDD Explorations, 2011, 13(1): 19-29.

[25] MASCETTI S, FRENI D, BETTINI C, *et al*. Privacy in geo-social networks: proximity notification with untrusted service providers and curious buddies[J]. The VLDB Journal, 2011, 20(4): 541-566.

[26] LI X Y, JUNG T. Search me if you can: privacy-preserving location query service[A]. Proceedings of the INFOCOM 2013[C]. Turin, Italy, 2013. 2760-2768.

[27] MARIAS G F, DELAKOURIDIS C, KAZATZOPOULOS L, *et al*. Location privacy through secret sharing techniques[A]. Sixth IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks(WOWMOM 2005)[C]. Taormina, Italy, 2005. 614-620.

[28] WERNKE M, DURR F, ROTHERMEL K. PShare: position sharing for location privacy based on multi-secret sharing[A]. Proceedings of the 10th IEEE International Conference on Pervasive Computing and Communications (PERCOM 2012)[C]. Lugano, Switzerland, 2012. 153-161.

[29] KRUMM J. Inference attacks on location tracks[A]. Proceedings of the 5th International Conference on Pervasive Computing (PERVASIVE 2007)[C]. Toronto, Canada, 2007. 127-143.

[30] GHINITA G, DAMIANI M L, SILVESTRI C, *et al*. Preventing velocity-based linkage attacks in location-aware applications[A]. Proceedings of the 17th ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems (GIS 2009)[C]. Seattle, Washington, USA, 2009. 246-255.

[31] MOKBEL M F. Privacy in location-based services: state of the art and research directions[A]. Proceedings of the 8th International Conference on Mobile Data Management(MDM 2007)[C]. Mannheim, Germany, 2007. 228.

[32] MACHANAVAJJHALA A, KIFER D, GEHRKE J, *et al*. L-diversity: privacy beyond *k*-anonymity[J]. ACM Transactions on Knowledge Discovery from Data, 2007, 1(1): 3.

[33] TSAI J Y, KELLEY P G, CRANOR L F, *et al*. Location-sharing technologies: privacy risks and controls[A]. TPRC 2009[C]. 2009.

[34] Location API[EB/OL]. http://developer.android.com/google/play-services/location.html.

[35] Privacy policiey[EB/OL]. http://www.google.com/intl/en/policies/privacy/#infosecurity.

[36] LAMARCA A, HIGHTOWER J, SMITH I, *et al*. Self-mapping in 802.11 location systems[A]. Proceedings of the 7th International Conference on Ubiqutous Computing(UBICOMP 2005)[C]. Tokyo, Japan, 2005. 87-104.

[37] LATEGAHN J, KUENEMUND F, ROEHRIG C. Mobile robot localization using WLAN, odometry and gyroscope data[J]. International Journal of Computing, 2010, 9(1): 22-30.

[38] FICCO M, PALMIERI F, CASTIGLIONE A. Hybrid indoor and outdoor location services for new generation mobile terminals[J]. Personal and Ubiquitous Computing, 2014, 18(2): 271-285.

[39] KUHN M G. An asymmetric security mechanism for navigation signals[A]. Proceedings of the 6th International Conference on Information Hiding(IH 2004)[C]. Toronto, Canada, 2004. 239-252.

[40] TIPPENHAUER N O, RASMUSSEN K B, POPPER C, *et al*. Attacks on public WLAN-based positioning systems[A]. Proceedings of the 7th International Conference on Mobile Systems, Applications, and Services(MOBISYS 2009)[C]. Kraków, Poland, 2009. 29-40.

[41] Android location SDK[EB/OL].http://developer.baidu.com/map/ geosd-k.htm.

[42] Configure access points with google location services[EB/OL]. https://support.google.com/maps.

[43] PENG Z T, KAJI K, KAWAGUCHI N. Privacy protection in WiFi-based location estimation[A]. Seventh International Conference on Mobile Computing and Ubiquitous Networking(ICMU 2014)[C]. Singapore, 2014. 62-67.

[44] 王璐,孟小峰.位置大数据隐私保护研究综述[J].软件学报，2014, 25(4): 693-712.
WANG L, MENG X F. Location privacy preservation in big data era: a survey[J]. Journal of Software, 2014, 25(4): 693-712.

[45] GHINITA G, KALNIS P, KHOSHGOZARAN A, *et al*. Private queries in location based services: anonymizers are not necessary[A]. Proceedings of the ACM SIGMOD International Conference on Management of Data (SIGMOD 2008)[C]. Vancouver, Canada, 2008. 121-132.

[46] WANG H, WANG Z Y, SHEN G B, *et al*. Wheelloc: enabling continuous location service on mobile phone for outdoor scenarios[A]. Proceedings of the INFOCOM 2013[C]. Turin, Italy, 2013. 2733-2741.

[47] About POLS[EB/OL]. http://pols.sourceforge.net/.

[48] LI B H, QUADER I J, DEMPSTER A G. On outdoor positioning with WiFi[J]. Journal of Global Positioning Systems, 2008, 7(1): 18-26.

作者简介：

王宇航（1987-），男，黑龙江哈尔滨人，哈尔滨工业大学博士生，主要研究方向为移动互联网和信息安全。

张宏莉（1973-），女，吉林榆树人，哈尔滨工业大学教授、博士生导师，主要研究方向为网络与信息安全、网络测量与建模、网络计算、并行处理等。

余翔湛（1973-），男，黑龙江哈尔滨人，哈尔滨工业大学教授，主要研究方向为网络容灾和信息安全。