文章编号：2095-2163(2020)01-0240-05 中图分类号：TP309 文献标志码：A

基于利益最大化的位置隐私保护技术研究

王宇航，张宏莉
（哈尔滨工业大学 计算机科学与技术学院，哈尔滨 150001）

摘 要： 基于位置的服务(LBS)改变了日常生活中获取信息的方式。不同类型的 LBS,例如定位、导航、兴趣点搜索和社交网络登记,已经成为几乎每个人的智能手机的基本应用。最近值得注意的 LBS 演变可能会改变 LBS 和 LPPM 的整体情况。研究将这种新颖的 LBS 定义为依赖于设备的基于位置的服务(DLBS)。DLBS 扩展了 LBS 的概念,也影响了现有的通用 LPPM 的架构和威胁模型。这种变化主要归结为服务提供商获取位置的方式的变化。属于用户和 DLBS 提供商的这两个基本权利已形成微妙的冲突需要解决。针对这种情况,本文为了克服 DLBS 中的位置隐私威胁设计了一个 DLBS 框架。提出了信用系统规则来平衡位置隐私和 DLBS 可用性,仿真结果验证了的方案的有效性。

关键词： 位置隐私保护技术；信用系统；应用

Research on Location Privacy Protection Technology based on benefit maximization

WANG Yuhang, ZHANG Hongli
(School of Computer Science and Technology, Harbin Institute of Technology, Harbin 150001, China)

【Abstract】 Location-based services (LBS) change the way in which information is obtained in everyday life. Different types of LBS, such as location, navigation, point of interest search and social network registration, have become the basic applications for almost everyone´s smartphones. The recent notable LBS evolution may change the overall situation of LBS and LPPM. The paper defines this novel LBS as a device-dependent location-based service (DLBS). DLBS extends the concept of LBS and also affects the architecture and threat models of existing generic LPPMs. This change is mainly due to changes in the way the service provider gets the location. These two fundamental rights belonging to users and DLBS providers have created subtle conflicts that need to be addressed. In response to this situation, this paper designs a DLBS framework to overcome the location privacy threat in DLBS. Credit system rules are proposed to balance location privacy and DLBS availability, and simulation results verify the effectiveness of the scheme.

【Key words】 Location Privacy Protection Technology; credit system; application

1 相关工作

最近的研究试图建立整个位置隐私保护机制。这些 LPPM 在文献[1]中得到了系统阐述。基于现有工作,则有必要对 LPPM 可以提供给该位置的隐私数量进行有效评定,并且位置隐私度量是在文献[2-5]中进行了有针对性的研究。只是对于 LBS 场景,这些研究都集中在如何安全地使用该位置。

与此同时,当下也有部分研究正致力于在位置获取场景中保留位置隐私,对此可以描述为如何安全地获得位置。诸如文献[6-8]等就给出了有效的方法来应对这种威胁。

一般而言,包括匿名、混淆、噪声添加、差异隐私和基于加密的方法在近年来均得到了深入研究和重要的实践应用部署。无论研究中采用了何种具体方法,这些研究中几乎都拥有相同的系统模型以及边界假设。在 LBS 场景中,亦无需担心 LBS 提供商可能在没有用户意识或位置的情况下获取位置信息。而且,在位置获取场景中,研究也并不考虑该如何生成位置。在研究中提出的新服务方案中,不可避免地会在用户意识之外获得该位置。

迄今为止,当今仍鲜有研究对 LBS 的发展和位置隐私挑战给予足够的重视。本文中首次定义了 DLBS 和新的隐私挑战。文中提出的方案是可以解决 DLBS 场景中位置隐私挑战的前沿研究。

2 DLBS 和新型隐私威胁

DLBS 极大地扩展了 LBS 的范围,作为一种实践中新的 LBS 形式,在本节中,首先列出了本文所指的 DLBS 的特征,对此可做阐释分述如下。

(1) DLBS 过程中涉及可本地化的服务设备,该设备将为用户服务,同时在没有用户意识的情况下自行进行本地化并与 DLBS 提供商进行通信。

(2)DLBS 设备在市区分开,随时可用。为了享

作者简介：王宇航(1987-),男,博士研究生,主要研究方向:移动互联网、信息安全；张宏莉(1973-),女,博士,教授,博士生导师,主要研究方向:并行计算、网络与信息安全、网络测量等。

收稿日期：2019-07-27

受 DLBS，用户需要靠近 DLBS 设备并将其激活。例如，使用用户的智能手机扫描设备的 QR 码。

(3)在服务期间，设备将为用户提供特殊容量，也将由用户使用。在 DLBS 期间，设备和用户的位置被视为相同。

(4)为了维护 DLBS 系统，以及 DLBS 设备上的所有权，DLBS 提供商需要了解设备的位置。这个要求(也是提供商的权利)违背了用户的位置隐私保护需求。在最基本的情况下，DLBS 提供商至少需要知道那些不在服务中的设备的位置，以便 DLBS 提供商可以确保维护 DLBS 系统。

由于上述功能，在 DLBS 场景中，传统的 LPPM 及其威胁模型正面临着挑战。研究可得剖析概述如下。

(1)传统 LBS 场景中的 LPPM 不必考虑服务提供商未经用户许可就能获得该位置的情况。但是在 DLBS 中，由于可本地化的设备，这种假设不再存在。这对那些仅考虑如何对即将发送给服务提供商的位置信息进行保存的 LPPM 来说是一个灾难性的挑战。

(2)一般而言，从法律角度来看，DLBS 提供商确实有权知道其 DLBS 设备的位置。这至少与用户方的位置隐私提议相同。这种矛盾也超出了传统 LPPM 的容量范围。需要新型 LPPM 来平衡位置隐私要求和“知情权”事实。

(3)具体地，在 DLBS 场景中，用户获取设备并激活 DLBS 的位置几乎不可能隐藏，因为 DLBS 提供商必须知道相对应的自身设备的位置。

结合前述 DLBS 功能和位置隐私挑战，在本文中，研发设计了一个全新的 DLBS 框架来应对这些问题。通常，在本文的框架中，将尊重、保护和实现位置隐私要求和来自用户与 DLBS 提供商方的位置感知要求。本次研发框架的基本原则是只鼓励 DLBS 提供商在最低满意度下询问足以维护的位置信息。最后，本文的框架具有与传统 LPPM 的兼容性，用户仍然可以使用自身的 LPPM 来保护本文研发框架上的位置隐私。在下一节中，对此拟展开研究详述。

3　基于信誉体系评价的 DLBS 位置隐私保护方法

在本文的框架中，首先需解开用户和 DLBS 提供商之间的直接通信，也在 DLBS 提供商和其配备的设备之间。此处引入了受信任的第三方代理来执行信用系统。图 1 显示了本文研发的系统架构。通常，DLBS 提供商将设备的位置广播到 TTP 代理，用户则从 TTP 代理查询可用设备。当需要位置信息时，TTP 代理就从 DLBS 提供者接收位置请求，根据其信用值决定是否满足当下需求。在用户方面，如果位置请求获得批准，就可以使用 LPPM 执行一定程度的保存，再将保存结果发送回 DLBS 提供商。研究设计内容详见如下。

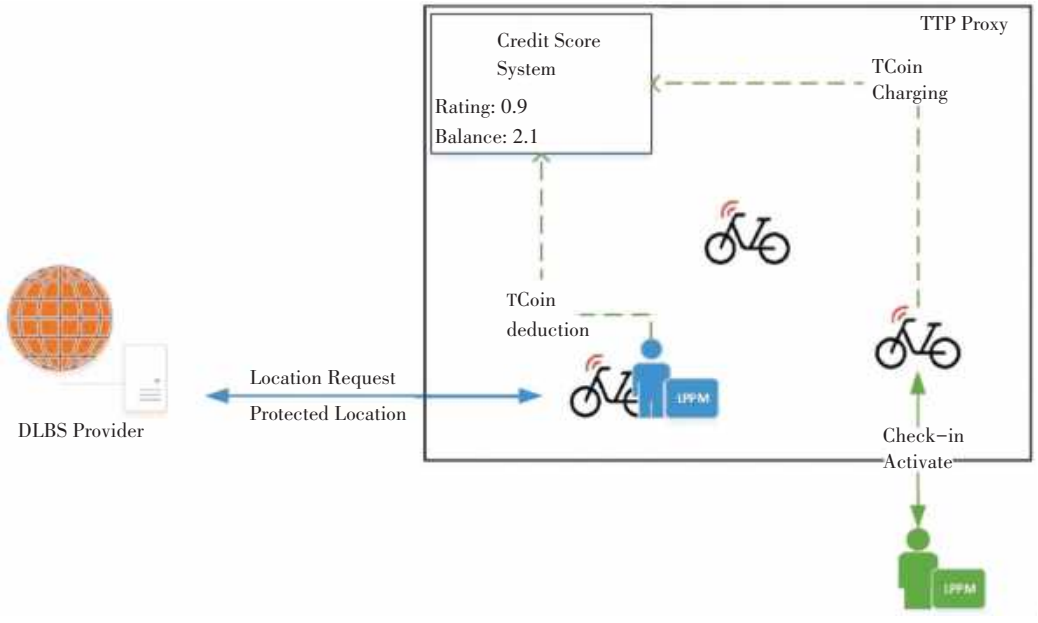

图 1　隐私保护系统架构

Fig. 1　System architecture of location privacy preservation in DLBS

3.1 基本思路

由于 DLBS 提供商在必要时有权知道其设备的位置,这就使得研究将无法假设 DLBS 提供商获取该位置的真正动机。因此,与传统的 LPPM 有所不同,在 DLBS 中,研究会将用户的位置隐私和 DLBS 系统的可用性放在规模的两边。

换句话说,本次研究允许 DLBS 提供商知道设备的位置(受 LPPM 保护),但却必须承担相应的费用。从兴趣的角度来看,DLBS 提供商必须保持规模的平衡,以使其自身的 DLBS 系统发挥应有的作用。这也意味着 DLBS 提供商不能过度抢占用户的位置隐私,但只能获得足够的适当位置信息以维持 DLBS 的操作。本次研究提出的系统假设可总述如下。

(1)用户诚实,即喜欢 DLBS,没有任何不正当的想法。且总是随身携带 DLBS 设备,并报告其所在位置,虽然由 LPPM 保存,但做如实汇报。

(2)用户的激活位置超出了本文的方案保护,如关于 DLBS 的特征所陈述的,研究将激活位置视为想要享受 DLBS 的用户支付的必要成本。本次研究希望在本文框架中保留的是 DLBS 期间的轨迹信息。

(3) DLBS 提供商不受信任,且知道所有已停用设备的位置信息,同时也有权查询激活设备的位置,如果 TTP 代理批准该用户请求,则用户必须报告其所在位置。此外,由于位置查询会损害 DLBS 系统的可用性,因此 DLBS 提供商将始终寻求位置隐私和系统可用性之间的利益最大化。

3.2 信誉评价系统

为了最小化维护 DLBS 系统的位置信息要求,DLBS 提供商仅需要知道设备的激活位置,其中用户终止 DLBS 并离开设备。DLBS 提供商将获取此位置且更新设备的状态,从而为下一轮服务做好准备。

在本文研发的框架中,设计建立了信用评分系统,用来鼓励 DLBS 提供商仅从 TTP 代理请求其设备的停用位置。研究中引入了信任硬币的概念,DLBS 提供商使用此概念来获取 TTP 代理上的位置信息。接下来,对于该系统的工作原理将做整体阐述如下。

(1)每次用户激活 DLBS 时,系统将创建一定量的 TCoin,并将其提供给 DLBS 提供商。在基本条件下,对于每次 DLBS 服务,将创建一个 TCoin、且将其提供给 DLBS。

(2)对于在线设备,DLBS 提供商必须购买设备位置。文中建议可提送至 TTP 代理,TPP 代理会告知用户这个请求。由于知情权原则,用户必须响应该请求,然而,由用户决定 DLBS 提供者可以获得的位置的精确度。

(3)研究定义了值为 1 的 TCoin 的精确位置,LPPM 的位置输出值取决于隐私级别的粒度。位置的精度越低,就越便宜。

(4)由于 DLBS 提供商与用户之间的一对多关系,DLBS 提供商可能在 DLBS 系统的运行时期间具有 TCoin 的余额。显然,较小的 TCoin 仍然是更值得信赖的 DLBS 提供商。因此,在本次研发的系统中,通过将 DLBS 提供商的信用评级定义为 0~1 之间的数字,1 表示 DLBS 提供商没有 TCoin 的余额,0 表示 TCoin 的余额等于或大于当前活跃用户。最后,研究进一步定义了在服务开始时创建的 TCoins 数量为 1 次 C $ TCoins。

鉴于上述信用评分系统和本文给出的系统假设,可以确保 DLBS 提供商将表现出维持其 DLBS 系统的可用性,对于合理的情况,这是在获得用户的位置隐私之前。在本文研发的系统中,理想情况是 DLBS 提供商总是花费其持有的 TCoin 在 DLBS 结束后请求精确位置。由于没有剩余的冗余 TCoin,因此在 DLBS 启动时总是会获得一个 TCoin,并且在 DLBS 结束后总是花费一个 TCoin。

在下一节中,将分析信用评分系统,以及 DLBS 提供商和用户在此类规则下的行为。基于这个信用评分系统,研究分析了本文框架的一些其它细节特征和设计,具体如下。

3.3 方法的隐私性分析

在本节中,首先分别从 DLBS 提供商和用户的角度分析本文研发的方案。然后,仿真模拟本文研发的框架并显示其对各种行为的表现。实际上,通过选择共用自行车作为模拟的原型,本文研发的框架中涉及的参数被认为是合理的。对此可做重点论述如下。

3.3.1 隐私度量

这里使用文献[1]中定义的位置隐私度量,并将用户的位置隐私量化为对手的预期错误。该指标还表明 LPPM 保存后位置的模糊程度。然后,也可以使用此值来为 DLBS 提供商定价以获取位置。

3.3.2 静默攻击

对于滥用 TCoins 并且无法负担在 DLBS 之后获得的位置,为了实际应用的目的,研究使用隐藏设备而不是让设备永远消失作为惩罚。如果 DLBS 提供商在 DLBS 后不再需要设备的位置,TTP 代理则会在足够长的时间内将该设备隐藏起来,诸如 24 h。

这将导致 DLBS 提供商的某些财务损失。

3.3.3　延迟通信

为了避免 DLBS 的去激活位置显示用户的当前位置，在本次研发方案中，当用户结束 DLBS 时，就会在 DLBS 的结束时间和 DLBS 提供商的可搜索时间之间设置时间间隔。在此延迟期后，DLBS 提供者可以将一个 TCoin 用于设备位置，如果希望在此期间内获得设备位置，则仍然需要花费额外的 TCoin。

3.3.4　隐私性

虽然必须满足来自 DLBS 提供商的设备位置请求，但是本文研发的系统对用户的位置隐私的恶意行为提供了强烈的排斥性。研发论述内容如下。

首先，如果 DLBS 提供商在 DLBS 期间花费了一定的 TCoins 请求该位置，就将无法在 DLBS 之后获得其所需的设备的位置，这意味着该属性丢失以及 DLBS 系统的可用性降低，对此 DLBS 提供商则不会接受。

其次，当 DLBS 提供商寻求 TCoins 的某些平衡并准备使用 TCoins 以获得更多的位置隐私时，将只能保持这样做的时间窗口，因为由于 TCoin 生成机制，更多的平衡意味着每个 TCoins 的收益减少。DLBS 的时间，并且为了维护 DLBS 系统，提供者每次总是需要花费一个 TCoin 来获得设备的位置。这种赤字将很快耗尽 DLBS 提供商的 TCoins。

最后，即使在 DLBS 提供商的情况下，考虑到所有可用性和好处，都非常积极地获取用户的位置，其将获得的位置信息并不比在传统 LBS 场景中得到的更好，因为用户侧的 LPPM 将控制发回的位置信息的粒度。

4　实验结果及分析

本次研究在 PC 上使用 Intel 8 Core 2.4 Hz CPU 和 16 GB ROM 实现了研发框架的测试仿真。1 000 个设备被发射到 100 平方公里的方形区域。研究将随机触发 DLBS 服务和不同频率的相应随机轨迹，观察输出在本节中的显示和解释。本文研发设计了架构和信用评分系统，不同类型的行为也参与了模拟。文中设定的仿真硬件环境和软件见表 1。

表 1　实验环境配置

Tab. 1　Experimental environment

CPU	内存	操作系统	开发平台	使用语言
Intel 8 Core 2.4 Hz CPUz	16 GB	Windows 10	Visual Studio 2008	C++

4.1　系统功能性

仿真测试本文提出的框架，检视其是否能够支持 DLBS 系统的顺利运行。研究得到的信用评级如图 2 所示，其中展示了 DLBS 提供商的 TCoin 余额以及当前丢失设备的百分比的模拟结果。

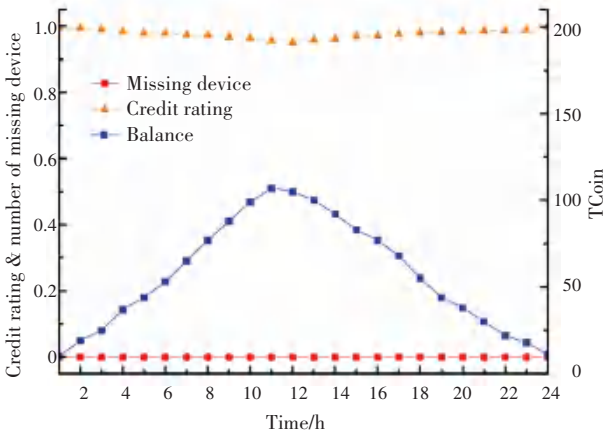

图 2　信誉评价体系运行下 DLBS 功能

Fig. 2　Runtime situation of DLBS system with the proposed credit system

研究假设一个诚实的 DLBS 提供商来衡量本文研发框架的功能。由于 DLBS 无法承受请求而丢失通信设备的数量在整个模拟中保持为 0，因此 DLBS 保持 TCoins 的合理平衡。在模拟的中期，当数字 DLBS 上升时，余额也随即上升，这即导致 DLBS 提供商的信用评级下降。然后，如后期运行结果所示，余额保持消耗，并且信用评级返回到正常水平。

4.2　监控方法

通过执行 TCoin 余额的拍摄来测试信用评分系统的监管机制。图 3 给出了前一次模拟中在相同条件下为 200 分配余额时的余额变化和得分等级。如果 DLBS 提供商通过牺牲 DLBS 系统的可用性来执行与协作者的共谋攻击，则可能在实际情况中发生平衡的拍摄。

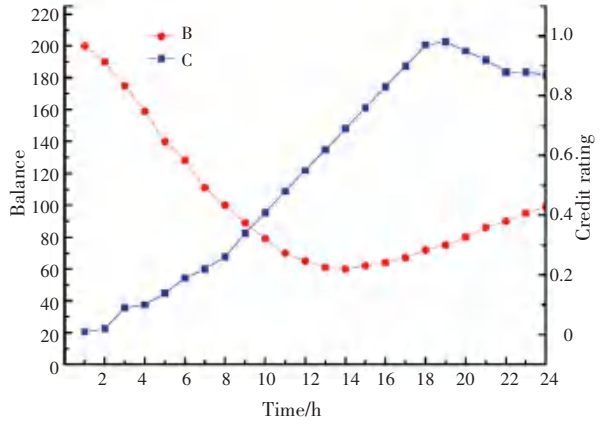

图 3　Tcoin 余额和信用值的关系

Fig. 3　Credit score vs. Tcoin balance

由图 3 可知，平衡点的上升直接将信用评级压

低到 0.03,结果是前几个小时几乎没有收入,而 TCoin 的净流出是为了获得这些收益。查询位置几乎耗尽了 8 h 的平衡。换言之,即使在这种极端情况下,DLBS 提供商执行恶意获取的时间窗口在本文研究的模拟中还不到 8 h。

4.3 隐私攻击

研究中,进一步考虑 DLBS 提供商愿意牺牲 DLBS 可用性并且倾向于探知用户位置隐私的情况。在前一个模拟案例中,研究认为 DLBS 将使用 TCoins 来请求额外的位置信息,并且用户将使用基本的混淆 LPPM 来保护其位置隐私。这种行为的结果则如图 4 所示。

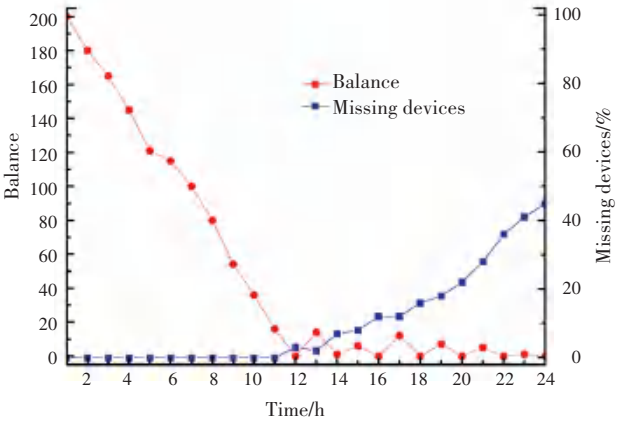

图 4 恶意跟踪行为下信誉体系变化

Fig. 4 Balance and missing devices when performing the malicious tailing

当 DLBS 提供商花费额外的 TCoin 来请求设备的位置时,余额很快接近于零,同时需要在稍后的时间获得服务设备的位置数。通过分析运行结果可知,丢失设备的百分比开始增加,在本次的模拟中,在最后一个时期中有 45% 的 DLBS 设备丢失,这对于恶意行为来说将是灾难性的结果。

5 结束语

在本文中,研究定义了一种新型的基于位置的服务,该服务命名了与设备相关的基于位置的服务。对于 DLBS,传统的 LPPM 因倾覆系统模型而无效。然后,基于信用评分系统和代理架构,本文设计了一个全新的 DLBS 框架,可以有效地保护位置隐私。研究中平衡了位置隐私与 DLBS 系统的可用性,这却可能导致位置隐私的恶意行为将受到对 DLBS 系统可用性的损害。仿真结果表明,本次研发的框架可以在真实环境中有效保护位置隐私。

参考文献

[1] 中国互联网信息中心.CNNIC 发布第 36 次中国互联网络发展状况统计报告[EB/OL]. [2015-07-23].http://www.cac.gov.cn/2015-07/23/c_1116018119.htm.

[2] JUNGLAS I A, WATSON R T. Location-based services[J]. Communications of the ACM, 2008, 51(3): 65-69.

[3] PORTMAN E A, GAILEY M L, HOLMES C S, et al. Location-based services: U.S.,6,944,447[P]. 2005-09-13.

[4] STEENSTRA J, GANTMAN A, TAYLOR K S, et al. Location based service (LBS) system and method for targeted advertising: U.S., EP20050810276[P]. 2007-06-27.

[5] VERVERIDIS C, POLYZOS G. Mobile marketing using a location based service [C]// Proceedings of the First International Conference on Mobile Business. Athens, Greece: Prentice-Hall, 2002.

[6] MOHAPATRA D, SUMA S B. Survey of location based wireless services[C]// Proceedings of IEEE International Conference on Personal Wireless Communications. New Delhi, Inida: IEEE, 2005:358-362.

[7] ALVAREZ J, DO P K, PIERCE J M, et al. Tiered on-demand location-based service and infrastructure: U.S., 11/016163[P]. 2007-02-27.

[8] FUJIMOTO J, HOTTA S, SAWADA K, et al. Hybrid positioning system combining spatially continuous and discrete information for indoor location-based service[C]// Proceedings of the first IEEE International Conference on Ubiquitous Positioning, Indoor Navigation, and Location Based Service (UPINLBS). Helsinki, Finland:IEEE, 2012: 1-6.