

移动用户位置隐私保护方案研究

史敏仪, 李玲娟

(南京邮电大学 计算机学院, 江苏 南京 210003)

摘要:随着基于位置的服务(LBS)的发展,如何保证用户在使用位置服务时的隐私安全,已成为一个亟待解决的问题。文中对主流的位置隐私保护技术进行了分析和比较。在此基础上,针对移动用户的位置隐私保护,提出了一种基于中心服务器的位置隐私保护方案。该方案针对隐私保护需求的差异性,考虑区域的敏感等级,对敏感区域采用 K -匿名和假名进行保护,同时运用脚印来辅助匿名。该方案能在不降低位置服务质量的前提下,有效地保护移动用户位置隐私。

关键词:位置隐私;假数据法; K -匿名;脚印

中图分类号:TP311

文献标识码:A

文章编号:1673-629X(2014)10-0151-04

doi:10.3969/j.issn.1673-629X.2014.10.036

Study on Location Privacy Protection Scheme for Moving Objects

SHI Min-yi, LI Ling-juan

(College of Computer, Nanjing University of Posts and Telecommunications, Nanjing 210003, China)

Abstract: With the rapid development of Location-Based Service (LBS), how to ensure the users' privacy security has become an urgent problem when they use LBS. In this paper, several primary location privacy protection technologies are analyzed and compared, and a central server-based location privacy protection scheme is proposed for protecting mobile user's location privacy. This scheme considers the sensitive level of area according to different privacy protection needs, uses K -anonymity and pseudonyms to protect location privacy in sensitive areas, and applies footprint to assist anonymity. This scheme can effectively protect location privacy of moving object without reducing the quality of service.

Key words: location privacy; false data method; K -anonymity; footprint

0 引言

随着位置服务(Location Based Service, LBS)的快速发展,在享受位置服务的同时,个人的位置隐私信息泄露也成为不可忽视的问题。面向LBS的位置隐私保护成为了一个研究热点。

已有的位置隐私保护研究主要关注用户的即时位置信息,采用 K -匿名技术,当用户在连续运动时,用户每个时刻的位置都被匿名化为匿名区域。但是攻击者可以将这些区域连接起来构建出用户的轨迹,这使得用户的连续位置的隐私信息不能被有效地保护,导致用户的行为模式、生活习惯等隐私信息泄露。为此,文中的研究将同时考虑移动用户位置及轨迹隐私保护。

1 位置隐私保护技术分析

位置隐私信息由标识信息和位置信息组成^[1]。标

识信息表示用户的静态属性或特征,用来唯一标识一个用户。位置信息则描述某个个体或团体的行踪。

现有的LBS隐私保护技术大致可以分为三类:假数据法、泛化法和抑制法^[2]。

假数据法通过添加假的位置信息或者利用假的标识信息和位置信息替代真实信息来对原数据进行干扰,同时保证被干扰的数据不发生严重的失真。假数据法具有计算开销小、实现简单的优点和数据失真、移植性较差的缺点^[3]。

泛化法将位置信息泛化为对应的匿名区域,以达到隐私保护的目。最常用的泛化法是 K -匿名技术^[4],即使得一个移动用户的位置无法与其他 $K-1$ 个用户的位置相区别。一般来说, K 值越大则隐私保护效果越好,但是丢失的信息也越多。泛化法具有实现简单、移植性好、数据较真实的优点和实现最优化匿名区域开销较大、有隐私泄露风险的缺点^[5]。

收稿日期:2013-12-13

修回日期:2014-03-13

网络出版时间:2014-07-28

基金项目:国家“973”重点基础研究发展计划项目(2011CB302903)

作者简介:史敏仪(1989-),男,硕士研究生,研究方向为信息安全;李玲娟,教授,研究方向为数据挖掘、信息安全、分布式计算等。

网络出版地址: <http://www.cnki.net/kcms/detail/61.1450.TP.20140728.1230.055.html>

抑制法根据具体情况有条件地发布位置数据以实现隐私保护。抑制法通常有 2 个原则^[6]:抑制敏感/频繁访问的位置信息;抑制增大隐私泄露风险的位置信息。抑制法具有实现简单、隐私保护度较高的优点,但数据可能会严重失真。

2 位置隐私保护系统结构分析

位置隐私保护技术多种多样,不同的技术需要不同的隐私保护系统结构。目前主流的位置隐私保护系统结构有三种,分别是独立式结构、中心服务器结构以及分布式点对点结构^[3]。

独立式结构如图 1 所示,其中的移动用户设备具有定位、计算和储存能力,可独立生成假位置或进行区域模糊化来完成隐私保护。节点将所生成的匿名区域替代真实位置发送给服务器,服务器根据匿名后的位置进行处理,将结果返回给用户,最后由用户对返回的结果进行过滤,得到需要的结果。这种结构简单、易于扩展和维护;但是在保护过程中计算开销大,对设备的计算能力和存储空间有较高的要求^[7]。此外,该结构仅对单个用户进行匿名处理,没考虑周围的用户,攻击者很容易鉴别出该用户,而且当匿名区域中用户过少时,达不到要求的匿名度。

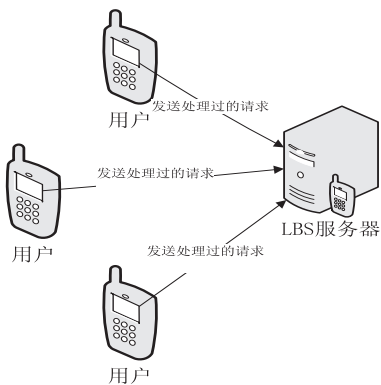


图 1 独立式结构

中心服务器结构如图 2 所示,由用户、LBS 服务器和可信任的第三方中间件(位置匿名服务器)组成。可信任的匿名服务器作为整个结构的核心,负责按照用户的隐私保护度要求,对用户的真实位置数据进行匿名处理,把处理好的请求发送到 LBS 服务器。服务器接收到 LBS 请求后,根据请求计算出一个包含众多结果的候选集合,并返回给匿名服务器。匿名服务器收到候选集合后,根据用户的真实位置信息进行筛选,最后把有效的结果发送给用户。这是目前位置隐私保护领域比较常用的一种结构,匿名保护的效率高。但是由于匿名服务器要处理大量用户频繁的匿名需求和筛选候选结果集,很容易成为系统的瓶颈,影响服务质量。另外匿名服务器往往要储存用户的真实位置信

息,一旦遭受攻击,用户隐私会泄露^[8]。

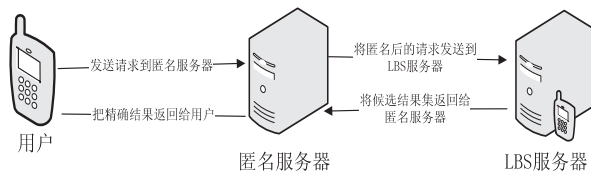


图 2 中心服务器结构

分布式点对点结构如图 3 所示,由服务器和用户群组成的匿名网络组成。该体系结构中的用户在相互信任的前提下,为了保护自身的隐私安全而互相协助。当用户 A 发送 LBS 请求时,将其 LBS 请求广播给网络中的用户,当用户数量达到用户 A 的隐私要求后,选择一个头节点 B,由 B 来构建匿名区域,并由 B 把请求发送给服务器,B 收到服务器返回的候选结果集后,把候选结果集发送给 A,最后用户 A 自己筛选出最佳结果。这种结构所具有的节点独立自主、动态和非中心化特点,以及资源和服务的独立分布特性,增强了抗攻击能力,均衡了网络负载。但是,节点间的相互信任,也导致了一旦有攻击者冒充节点混入其中,用户的隐私很可能被泄露^[9],而且匿名区域的构建和候选结果集的筛选还是在客户端完成,需要客户端具备较高的计算和存储能力。

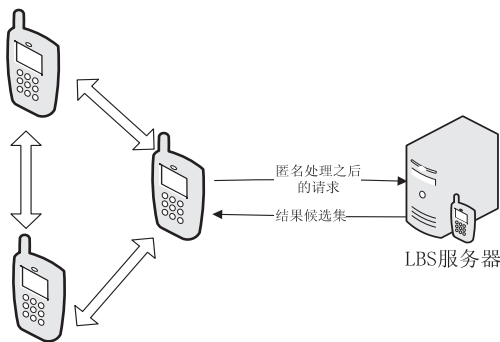


图 3 分布式点对点结构

3 一种基于中心服务器的移动用户位置隐私保护方案

Huang 等人在文献[10-11]中提出了 Silent Period 方法。Silent Period 方法把用户的运动空间分为混合区域和应用区域。当用户在混合区域运动时,不发送任何服务请求。用户在进入和离开混合区域时采用不同的假名,从而增加了把用户前后位置联系起来的难度。虽然此方法能很好地保护用户的位置隐私,但是由于用户在混合区域中没有任何通信,会损失通信时间,降低服务质量。

Huang 等人在文献[12]中针对上述问题提出了一种改进的方法—Silent Cascade。Silent Cascade 方法通过平衡用户在混合区域和应用区域中的延迟与用户需求的隐私保护度来保证在不降低服务质量的前提下满

足用户的隐私保护度要求。然而,当用户不经过其混合区域时,用户的假名没有任何变化,攻击者很容易根据用户的位置来破解用户假名,从而对用户的隐私造成侵害。

文中在不影响服务质量的前提下,为了降低用户位置隐私的泄露风险,提出一种结合假名和 K -匿名两种方法的基于中心服务器的移动用户位置隐私保护方案。

(1) 中心服务器的组成。

中心服务器即为图 2 中的匿名服务器,包含五个部分:用户信息存储、位置信息存储、假名/假用户机制、假名映射机制和位置匿名机制,如图 4 所示。

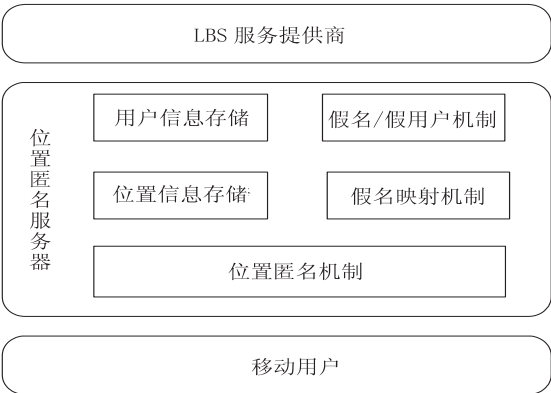


图 4 移动用户位置隐私保护中心服务器组成

其中,用户信息是指用户的基本信息,包括:个人信息、隐私安全级别、敏感区域、行进路线等。所谓敏感区域是指移动用户在运动期间不想被泄露的区域,如医院、公司等。匿名服务器把用户的运动空间划分成大小相同的区域,每个区域都有各自的编号。用户把运行路线上所经过的区域编号和敏感区域编号发送给匿名服务器。

位置信息包括用户的实时位置信息和脚印。所谓脚印是指用户在运动空间内的历史位置^[13]。当用户在其敏感区域使用位置匿名时,中心服务器把用户此时的位置信息存入数据库中,形成脚印。脚印在数据库中的表结构为 (id, location, count, time), 其中 id 为用户的假名, location 是用户的真实位置信息, count 是此位置被使用的次数, time 为存入数据库中的时间。每一个划分区域都有一个对应的脚印库,当有新的脚印生成时,加入到脚印库中。对于脚印库脚印的更新规则为:

①当新脚印的位置 (Location) 与脚印库中的位置重合时,则更新这条数据记录的时间。

②若某个脚印被 K -匿名过程所使用,其对应的 count 值加 1。

(2) 位置隐私保护的处理流程。

位置隐私保护的处理流程如图 5 所示。

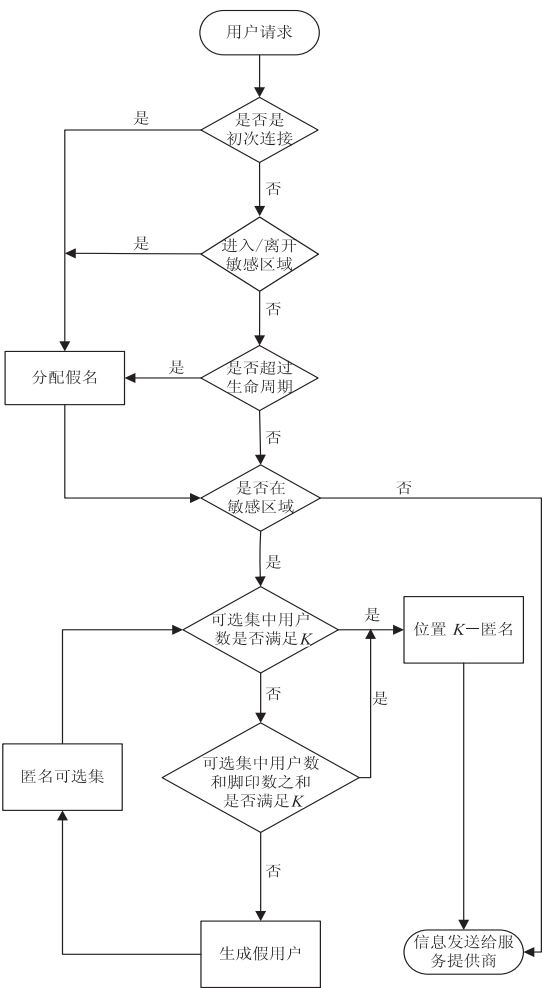


图 5 位置隐私保护的处理流程

当用户初次连接到位置匿名服务器时,系统为其分配一个假名,每个假名都具有一个有效期,当假名存在时间超过有效期时,系统为其更换假名。当用户进入/离开敏感区域时,系统为其更换假名。假名更换能很好地把用户的移动轨迹切割成轨迹片段,从而增加了攻击者还原用户轨迹的难度。这些工作由中心服务器利用假名/假用户机制中的假名功能实现。

当用户在敏感区域运动并发送请求时,由中心服务器的位置匿名机制实施 K -匿名算法来保护用户位置隐私。

K -匿名使用一个匿名可选集,文中的匿名可选集由敏感区域中将该区域作为敏感区域的移动用户和用户在该区域内的脚印组成。这样是考虑到:

①由于敏感区域是由用户自行选择的,每个用户拥有不同的敏感区域,简单地基于发送请求的用户来构建匿名区域会导致隐私泄露。例如,某一时刻 t ,在同一划分区域 A 中的四个用户 a, b, c, d 发送请求到位置匿名服务器,请求内容分别是 $Q_a\{a, L_a, C_a\}, Q_b\{b, L_b, C_b\}, Q_c\{c, L_c, C_c\}, Q_d\{d, L_d, C_d\}$ 。划分区域 A 仅对于用户 a 是敏感区域,此时用户 a 的请求匿名化为 $Q\{\{P_a, P_b, P_c, P_d\}, AR, \{C_a, C_b, C_c, C_d\}\}$,但是由于

划分区域 A 并不是用户 b,c,d 的敏感区域,用户 b,c,d 的发送到服务器的请求为 $Q_b\{P_b, L_b, C_b\}, Q_c\{P_c, L_c, C_c\}, Q_d\{P_d, L_d, C_d\}$ 。因此,服务器商很容易简化请求 Q 为 $Q\{P_a, AR, C_a\}$,这就增加了用户 a 隐私泄露的危险。

②脚印记录了用户的位置轨迹,一方面可以帮助合法用户分析用户轨迹,更好地提供位置服务;另一方面,借助脚印构造假用户,不会使假用户的位置偏离常规值,对攻击者更具迷惑性,而且只要合理选择用于 K -匿名的脚印,就不会泄露位置轨迹。

当用户在敏感区域发送请求时,如果匿名可选集满足 K -匿名要求,位置匿名服务器从该候选集中选取 $K-1$ 个用户或脚印来构建匿名区域。如果匿名可选集无法达到用户所要求的匿名度 K 时,中心服务器的假名/假用户机制中的假用户功能负责在匿名区域内随机生成一些用户以达到匿名度 K 。匿名服务器的假名映射机制保存用户真假名之间的映射关系。

4 结束语

随着移动无线技术和物联网的发展,随时随地获得个人或物品的位置信息成为可能,位置隐私保护已成为当今社会中的重要问题^[14]。文中针对位置服务中心的位置隐私保护进行研究,提出了一种基于中心服务器的移动用户位置隐私保护方案。该方案针对不同的用户隐私保护要求采用合适的保护方法。对于隐私保护度较低的区域,即非敏感区域,采用假名机制进行保护,此时不会降低位置服务质量;对于隐私保护度较高的敏感区域,则采用 K -匿名和假名进行保护。该方案利用假名机制把用户轨迹分割成具有不同假名的轨迹片段,当用户经过敏感区域之后,进一步增加了复原轨迹的难度,从而达到保护移动用户位置和轨迹隐私的目的。

参考文献:

- [1] 王彩梅,郭亚军,郭艳华. 位置服务中用户轨迹的隐私度量[J]. 软件学报,2012,23(2):352-360.
- [2] Gruteser M, Grunwald D. Anonymous usage of location ba-
- (上接第 143 页)
- [9] 范勇,兰景英,李绘卓. 软件测试技术[M]. 西安:西安电子科技大学出版社,2009.
- [10] Tamura Y, Yamada S. A software testing-management tool for distributed development environment[C]//Proc of ICIM 2004. [s.l.]:[s.n.],2004.
- [11] 高慧英. 软件测试管理及其工程应用[J]. 计算机与数字工程,2007,35(1):147-149.
- [12] 李亚伟,严宏君. 软件测试过程管理工具的设计与实现


sed services through spatial and temporal cloaking[C]//Proc of first international conference on mobile systems, applications, and services. San Francisco, California, USA: ACM, 2003:31-42.

- [3] Luper D, Cameron D, Miller J A, et al. Spatial and temporal target association through semantic analysis and GPS data mining[C]//Proceedings of IKE 2007. Las Vegas, USA: [s.n.],2007:251-257.
- [4] 贾金营,张凤荔. 位置隐私保护技术综述[J]. 计算机应用研究,2013,30(3):641-646.
- [5] Abul O, Bonchi F, Nanni M. Never walk alone: uncertainty for anonymity in moving objects databases[C]//Proceedings of ICDE 2008. Cancun, Mexico: [s.n.],2008:376-385.
- [6] 霍峥,孟小峰. 轨迹隐私保护技术研究[J]. 计算机学报,2011,34(10):1820-1830.
- [7] 司超. 基于 Casper 的位置隐私保护模型与算法研究[D]. 广州:华南理工大学,2012.
- [8] 徐娜,王红,黄雯. 移动社会性软件中的位置隐私研究[J]. 计算机工程与设计,2010,31(17):3781-3784.
- [9] 陈浏,冯云霞,戴国骏. LBS 中基于移动终端的连续查询用户轨迹隐匿方法[J]. 计算机应用研究,2011,28(12):4653-4656.
- [10] Huang Leping, Matsuura K, Yamane H, et al. Enhancing wireless location privacy using silent period[C]//Proceedings of the IEEE wireless communications and networking conference. [s.l.]:IEEE,2005:1187-1192.
- [11] Huang Leping, Yamane H, Matsuura K, et al. Towards modeling wireless location privacy[C]//Proceedings of the workshop on privacy enhancing technologies. Dubrovnik (Cavtat), Croatia: [s.n.],2005:59-77.
- [12] Huang Leping, Yamane L, Matsuura K, et al. Silent cascade: enhancing location privacy without communication QoS degradation[C]//Proceedings of the 3rd international conference on security in pervasive computing. [s.l.]:[s.n.],2006:165-180.
- [13] Xu T, Cai Y. Exploring historical location data for anonymity preservation in location-based services[C]//Proceedings of INFOCOM 2008. Phoenix:IEEE,2008.
- [14] 吴婷婷,李玲娟. 面向 RFID 的位置隐私保护算法研究[J]. 计算机技术与发展,2013,23(1):157-160.
- [J]. 计算机技术与发展,2013,23(3):56-60.
- [13] 樊庆林,吴建国. 提高软件测试效率的方法研究[J]. 计算机技术与发展,2006,16(10):52-54.
- [14] Salima T M S U, Askarunisha A, Ramaraj N. Enhancing the efficiency of regression testing through intelligent agents[C]//Proceedings of the international conference on computational intelligence and multimedia applications. Sivakasi: IEEE,2007:103-108.

移动用户位置隐私保护方案研究

作者：[史敏仪](#)，[李玲娟](#)，[SHI Min-yi](#)，[LI Ling-juan](#)

作者单位：[南京邮电大学 计算机学院, 江苏 南京, 210003](#)

刊名：[计算机技术与发展](#)

英文刊名：[Computer Technology and Development](#)

年，卷(期)：2014(10)

本文链接：http://d.g.wanfangdata.com.cn/Periodical_wjfz201410037.aspx