

增强现实中的位置隐私保护

杨 洋¹, 王汝传^{2,3}

(1. 南京广播电视大学 南京城市职业学院 信息技术系, 江苏 南京 210002;

2. 南京邮电大学 计算机学院, 江苏 南京 210003;

3. 江苏省无线传感网络高技术研究重点实验室, 江苏 南京 210003)

摘 要:随着增强现实技术和基于位置服务(LBS)技术的发展,增强现实的应用也越来越广泛,LBS是增强现实的一个重要应用,用户位置隐私的泄漏是LBS用户的重要威胁,因此对用户位置隐私的管理就显得非常重要。论文首先分析用户位置隐私保护的重要性,接着介绍用户位置隐私泄露的类型,并分析和比较目前已有的用户位置隐私保护方法的优缺点,最后提出含有集中受信任的第三方模型的用户位置隐私保护方法,该方法优化了现有的用户位置隐私保护方法,可以有效地实现用户位置隐私的保护。

关键词:基于位置服务;位置隐私;K-匿名法;假匿名法;受信任的第三方

中图分类号:TP309

文献标识码:A

文章编号:1673-629X(2012)09-0232-03

Location Privacy Protection in Augmented Reality

YANG Yang¹, WANG Ru-chuan^{2,3}

(1. Department of Information Technology, Nanjing City Vocational College, Nanjing Radio and TV University, Nanjing 210002, China;

2. College of Computer, Nanjing University of Posts and Telecommunications, Nanjing 210003, China;

3. Jiangsu High Technology Research Key Laboratory for Wireless Sensor Networks, Nanjing 210003, China)

Abstract: With the development of augmented reality technology and location based services (LBS) technology, the application of augmented reality is applied more and more widely. LBS is one of the most important applications in augmented reality. The leak of user location privacy (ULP) is a major threat to clients of LBS. So the management of ULP is very important. It analyzed the importance of ULP protection, introduced the types of ULP leak and analyzed the advantages and disadvantages of the existing ULP protecting methods. Finally put forward an improved ULP protection method with centralized trusted third party model, which would optimize the existing ULP protecting methods and effectively realize the ULP protecting.

Key words: location based service (LBS); location privacy; K-anonymity method; pseudo-anonymity method; trusted third party

0 引 言

增强现实这个概念是1990年由Thomas Caudell提出的^[1],经过许多年的技术发展,增强现实的概念也经历了多次变革和更新,现在广泛公认的增强现实概念是Ronald Azuma提出的^[2]:即虚实结合,实时交互,三维注册。可以这样理解增强现实,它是一种结合虚

拟化技术观察世界的方式,是将现实世界的真实环境和计算机产生的虚拟物体实时地结合在一起的技术,增强现实也可以与虚拟世界互动,但是其不是构建完全虚拟的环境,而是在现实环境上的补充。

基于位置服务(Location Based Services, LBS)是增强现实提供的常用服务之一,它是通过移动的无线网络或外部定位方式获取移动终端用户的位置信息,通过用户的位置信息来增加服务价值的移动服务。LBS服务含有多项内容,如紧急服务、社区和娱乐、信息和导航、跟踪和监控、移动电子商务等。在基于位置服务中,用户通过向服务端提供自己的位置信息,得到相应的查询结果^[3]。也可以收集亲朋好友现在的位置信息、紧急救助信息、老人儿童跟踪信息等,也就是所谓的定位别人。例如:在某范围内寻找手机用户当前位

收稿日期:2012-02-07;修回日期:2012-05-13

基金项目:国家自然科学基金(60973139,61170065,61171053);江苏省自然科学基金(BK2011755);江苏省科技支撑计划项目(BE2010197, BE2010198, BE2011844, BE2011189)

作者简介:杨 洋(1980-),女,江苏南京人,硕士,讲师,主要研究领域为网格计算、增强现实技术、无线传感器网络;王汝传,教授,博士生导师,主要研究方向为计算机软件、计算机网络、信息安全、移动代理和虚拟现实技术等。

置处几公里范围内的饭店、宾馆、电影院、图书馆等的名称和地址。

早期的增强现实系统采用头戴式显示器作为融合显示设备,这在一定程度上限制了用户的活动范围,不能用于户外环境。随着移动设备和网络技术的迅速发展,增强现实技术在移动终端上的应用已涉及很多领域,如游戏、社交网络、电子商务和个人医疗保健等方面。

增强现实的应用正随着增强现实技术及 LBS 技术的发展而逐渐广泛,如果不采取相应的安全保护措施,无限制的发展这些技术,也将带来显著的威胁,对 LBS 用户的一个重要威胁就是用户位置隐私的泄露^[4]。

用户位置隐私是一种特殊的信息隐私,其仍然属于信息隐私的范畴。信息隐私是指个人或机构定义的在某段时间、某个地点、以某种方式与别人共享信息;而位置隐私是指尽可能地阻止攻击者以某种方式获取用户的位置信息。在 LBS 中,敏感属性数据可以是相关用户的时间信息和空间信息,服务请求的内容涉及很多方面,如卫生保健信息、财产信息等,可以是推断出的用户的旅行模式、爱好和兴趣及其他个人隐私信息;用户位置隐私威胁是指攻击者在没有得到授权的情形下,通过某种方式,如定位技术、窃取位置信息传输信道技术等,非法获取用户原始的位置数据,从而推断出与位置数据有关的个人隐私信息。

1 用户位置隐私泄露的类型

LBS 能够获取用户所在位置相关的信息,而 LBS 并不能保证服务器不泄露或不滥用用户的位置信息。所以,用户位置隐私的泄露是 LBS 应用的重要威胁。攻击者可以使用用户位置信息或相关的时空推理攻击来推测用户的隐私信息、私生活细节等,因此用户的隐私可能在多个方面都受到威胁。假设 LBS 提供商是半诚实的、非恶意的、不值得信赖的,这就构成了两种攻击类型。

1.1 受限空间识别

如果攻击者知道特定用户 A 住在特定区域 P,并且发现所有的来自 P 区域的服务请求都来自同一个用户 ID,那么攻击者可以推断请求服务的用户可能就是 A。通过这些信息,攻击者可以通过简单连接点的方式来跟踪用户^[5]。这种攻击被称为受限空间识别^[6]。

例如,某宾馆某个房间的客户在房间里发送了一条消息,那么就可以通过这条消息中确切的位置坐标信息 (x, y) ,并利用外部相关的知识来确定该房间的客户。攻击者便可推断出该用户发送了哪些其他服务请求。

1.2 观察识别

另一种攻击方法是通过服务请求信息和接收的定位信息来显示用户标识。如果 LBS 提供商收到报告,用户 M 准备在某段时间访问某一地点,并且发现所有的该地点在这个时间段的服务请求均由同一个用户发出,那么攻击者就可以推断出请求服务的用户就是 M。这种攻击被称为观察识别^[6]。

例如,某用户如果在前一个消息中泄露了其位置信息和标识,那么该用户如果仍然在同一个位置发送消息,即使将后面的这些消息匿名,攻击者依然可以通过消息中的位置信息来推断和识别出后面这些消息的来源。

2 现有的位置隐私保护方法及缺陷

为有效地保护用户位置隐私信息,许多研究人员在服务质量和隐私保护之间寻求一个平衡点,即在最少暴露位置隐私信息的情况下,同时获取质量最优最好的服务。也就是说,要实现匿名的位置服务,那么用户在请求服务时,应该既能匿名的使用网络服务又能隐藏自己的位置信息和标识。

目前,基于位置服务的位置隐私保护方法有假位置法、假匿名法、K-匿名法和个性化 K-匿名法四种,下面针对它们的优缺点进行分析。

2.1 假位置法

第一种方法是通过发布假位置^[7]达到混淆视听的效果。当用户提出服务请求时,将真实的位置和假位置一起发送给服务提供商,攻击者无法辨别哪个是真实的或哪个是虚假的位置,用户的位置隐私通过报告假位置从而得到保护。但这种保护方法有一定的缺陷,其隐私保护程度不是固定不变的,随着假位置和真实位置之间的距离变化,隐私保护程度和服务质量也在变化。当假位置距离真实位置较远时,服务质量差,但其隐私保护程度较高;当两者之间的距离较近时,服务质量好,但其隐私保护程度则低。

2.2 假匿名法

假匿名法是另一种位置隐私保护方法^[8],是匿名法的一种特殊类型。首先将服务请求提交给匿名服务器,隐藏真实的可以标识用户的 ID,换成假 ID,每一个用户都使用一个假 ID 来达到隐藏真实 ID 的目的。此时,攻击者就算从服务器端得到用户的准确位置信息,他还不能准确地关联用户位置信息与其真实 ID 身份信息,那么就无法确定该服务请求是由哪个用户提出的,从而有效地实现了用户的位置隐私保护。但该方法也有其缺点,由于服务器会记录所有的服务请求的信息和用户相应的 IP 地址,所以仍然可能导致位置隐私泄露。

2.3 K-匿名法

还有一种位置隐私保护的方法叫做 K-匿名法,它是最早提出解决位置隐私保护问题的方法,其通过概括和隐藏技术,使用基于四分树的算法来实现时间和空间的模糊,在向 LBS 提供商提交前,先删除个人信息内容,发布较低精度的数据,使得各条记录至少与数据表中其他 K-1 条记录具有完全相同的准标识符属性值^[9]。由于 K-匿名法对某个个体与数据表中某条具体记录之间的关联性进行了分离,因此有效地降低了攻击所导致的隐私泄露程度。但这种方法的局限性是对于敏感属性数据的泄露问题没有相应的保护机制^[10],所有的移动用户使用同一个 K 值,不能满足个性化隐私保护定制的需求,而且由于使用了泛化技术,该技术将导致丢失原始数据中的大量信息,因此,可能会严重威胁数据分析的准确性。

2.4 个性化 K-匿名法

在位置隐私保护中,不同的用户有不同的位置 K-匿名需求,针对 K-匿名法的局限性,由 Gedik and Liu^[5]首先提出了个性化 K-匿名法。个性化 K-匿名法是改进的 K-匿名法,在这种方法中,每位用户可以自行定义其所需的匿名等级,根据匿名等级设置相应的位置隐私策略,并通过分类树的节点来定义隐私保护程度,此时有着相同 K 值的移动用户信息可能被一起匿名化。这种方法的缺点在于当 K 值增高时,模糊的信息量就会减少,匿名化信息的比例会逐渐下降。

3 优化现有的位置隐私保护方法

上述四种位置隐私保护方法有着各自的优点和不足,需要对现有的位置隐私保护方法进行优化。

3.1 实现隐私保护的模型

LBS 中实现隐私保护的模型主要有以下三种。第一种是非协作模型^[11],使用如假匿名、虚拟人物和标识物体等技术来实现隐藏用户的位置信息,其设计简单,但易于受到攻击。第二种模型是对等协作模型^[11],为实现隐私保护,多个用户尝试协作,通过分布式处理来计算或隐藏其位置。第三种是集中受信任的第三方模型^[11],此时用户位置匿名化、服务请求的位置匿名化和将结果反馈给用户都是由受信任的第三方来实现,相当于在用户和 LBS 提供商之间架构了一座通讯桥梁,如图 1 所示。该模型与其他两种模型相比,在实现隐私保护方面比较有效。

3.2 改进的位置隐私保护方法

由于现有的位置隐私保护方法各有局限性,结合 K-匿名法和假匿名法的优点,并引入集中受信任的第三方模型^[11]来实现隐私保护,此时,用户和 LBS 提供商之间的通讯由集中受信任的第三方完成^[12]。

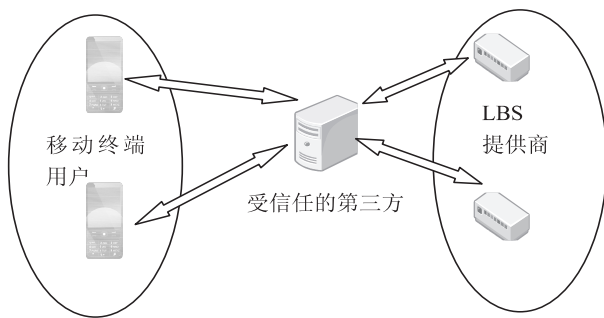


图 1 集中受信任的第三方模型

当 K 值在规定范围内,受信任的第三方首先将发送来的信息匿名化,并将产生的 K-匿名化信息传送给 LBS 提供商;如果 K 值的增高超过了一个界限,大多数或者可能所有的信息均使用假 ID 实现匿名化,此时用户位置匿名化、服务请求的位置匿名化和将结果反馈给用户都是由受信任的第三方来实现,用户 ID 被假随机 ID 取代,假随机 ID 将被存储于受信任的第三方的列表中,同时存储的还有原始 ID 及用户其他的细节信息。当同一个用户在不同的时间请求服务时,会将这些假 ID 分配给该用户,所有的这些假 ID 和原始用户 ID 一起存储于列表中。所以,无论在何时何地,当 LBS 提供商处理或响应服务请求时,受信任的第三方将检查假 ID 对应的列表中的原始用户 ID,然后将所有的原始值放回原处并将结果返回给移动终端用户。

3.3 改进后的位置隐私保护方法的优点和不足

将 K-匿名法和假匿名法结合使用,引入集中受信任的第三方,用户和 LBS 提供商之间的通讯由受信任的第三方完成,从而实现位置隐私保护,可以将绝大多数发送的信息进行匿名化,该模型也允许用户自定义 K 值,即使没有其他的 K-1 移动终端用户,信息也不会被忽略。

改进后的位置隐私保护方法也有不足之处,其不足之处在于引入的集中受信任的第三方,使用集中受信任的第三方模型的瓶颈是当其接受服务请求的数量超过它能够存储和处理的服务请求数量时,此时,匿名化的信息数量会有轻度下降。这是该模型的缺陷,但是与其他模型相比,其在位置隐私保护方面仍是非常有效的。

4 结束语

位置隐私保护是增强现实技术中最值得关注的內容之一,也是发展增强现实应用需要解决的关键问题之一。增强现实技术和无线传感器网络在不断发展,人类对个人隐私信息的重视和保护程度将随之提高,对位置隐私保护的研究必将成为增强现实技术研究领域中的热点问题。文中回顾和总结了近年来在位置隐

(下转第 238 页)

通过分析可以看出,传统的软件授权通常和机器物理属性绑定,这种方法不适用于虚拟环境下的软件授权。最好的办法是将软件授权和机器的物理属性解除绑定,指定其他合理的软件授权标准。这样既能避免虚拟机复制和虚拟机迁移引发的授权问题,还能更好地发挥桌面虚拟化和应用虚拟化移动性的优势。

5 结束语

软件保护技术在保护软件版权方面扮演着举足轻重的作用,是软件授权不可或缺的一部分。软件行业开始从传统的光盘套装、一次性授权付费,向在线托管、租赁使用、按需付费型转变。虚拟化技术的应用改变了软件的运行环境,给软件授权带来了新的问题,理想的授权方案既要保证发挥新技术的优势,又要保证软件授权的合理性。

SaaS 这种创新的商业模式不但能够保证软件的安全性,还能满足软件行业新的发展需求,它解除了软件授权和本地机器的绑定,在很大程度上可以解决虚拟化环境下软件授权的问题。只要能够解决 SaaS 模式下软件技术架构和数据在服务器端存储的安全性问题,SaaS 将会给软件行业带来一次新的创新。

参考文献:

- [1] 周建林. 软件保护技术与设计[D]. 武汉:华中科技大学

++++++
(上接第 234 页)

私保护领域的主要方法,并提出改进的位置隐私保护方法。目前,还没有一个十分完善的增强现实中的位置隐私保护方法,还需进一步对相关问题的研究。

参考文献:

- [1] Hollerer T H,Feiner S K. Mobile augmented reality[M]. [s. l.]:Taylor and Francis Books Ltd,2004.
- [2] Wikipedia. Augmented reality[EB/OL]. 2009. http://en.wikipedia.org/wiki/Augmented_reality.
- [3] 彭志宇,李善平. 移动环境下 LBS 位置隐私保护[J]. 电子与信息学报,2011,33(5):1211-1216.
- [4] Mokbel M F,Chow C Y,Aref W G. The newCasper:query processing for location services without compromising privacy [C]//Proceedings of the International Conference on Very Large Data Bases. New York:[s. n.],2006:763-774.
- [5] Gedik B,Liu L. Protecting location privacy with personalized k-anonymity:architecture and algorithms[J]. IEEE Trans. on Mobile Computing,2008,9(1):1-17.
- [6] Gruteser M,Grunwald D. Anonymous usage of location based services through spatial and temporal cloaking[C]//Proc. of

学,2009.

- [2] 魏光村,孙忠林,徐燕妮. 软件加密技术研究[J]. 福建电脑,2006(9):44-45.
- [3] 宋 扬,李立新,周雁舟,等. 软件防篡改技术研究[J]. 计算机安全,2009(1):34-37.
- [4] 杨建龙,王建民,李德毅. 软件水印技术及其新进展 [J]. 计算机工程,2007,33(17):168-175.
- [5] 高 兵,林果园,唐久涛. 基于代码迷惑的软件保护[J]. 电脑知识与技术,2011,7(1):118-128.
- [6] 月光博客. 从软件授权到软件保护[EB/OL]. (2010-11-20) [2011-07-10]. <http://www.williamlong.info/archives/2416.html>.
- [7] Bhardwaj S,Jain L,Jain S. An approach for investigation perspective of cloud software-as-a-service (SaaS)[J]. International Journal of Computer Applications,2010,10(2):40-43.
- [8] Pijanowski K. Understanding Public Clouds:IaaS, Paas, & SaaS[EB/OL]. (2009-05-31) [2011-07-31]. <http://www.keithpij.com/Home/tabid/36/EntryID/27/Default.aspx>.
- [9] 耿 冰,于修理. SaaS 与传统软件比较研究[J]. 沈阳师范大学学报(自然科学版),2009,27(1):84-86.
- [10] 巍 巍. SaaS 模式—中国软件企业面临的机遇和挑战[J]. 工业技术经济,2008,27(7):48-51.
- [11] 彭 荣. SaaS 模式下多租户系统架构及关键技术研究[D]. 大连:大连海事大学,2010.
- [12] 《虚拟化与云计算》小组. 虚拟化与云计算[M]. 北京:电子工业出版社,2009:27-55.

ACM Int'l Conf. on Mobile Systems. [s. l.]:[s. n.],2003.

- [7] Kido H,Yanagisawa Y,Satoh T. Protection of location privacy using dummies for location-based services[C]//Proc. of the 25th International Conference on Distributed Computing Systems(ICPS'05). [s. l.]:[s. n.],2005.
- [8] 潘 晓,肖 珍,孟小峰. 位置隐私研究综述[J]. 计算机科学与探索,2007,1(3):268-281.
- [9] 王平水,马钦娟. 隐私保护 K-匿名算法研究[J]. 计算机工程与应用,2011,47(28):117-119.
- [10] Machanavajjhala A,Gehrke J,Kifer D,et al. L-diversity:privacy beyond k-anonymity [C]//Proceedings of the 22nd ICDE. Atlanta,USA:ACM,2006:24-35.
- [11] Mohaisen A,Hong D,Nyang D. Privacy in location based services:primitives toward the solution[C]//Fourth Int'l Conf on Networked Computing and Advanced Information Management. [s. l.]:[s. n.],2008.
- [12] Aryan A,Singh S. Securing Location Privacy in Augmented Reality[C]//2010 5th International Conference on Industrial and Information Systems. [s. l.]:[s. n.],2010.