位置隐私保护技术研究进展*)

魏 琼 卢炎生
(华中科技大学计算机科学学院 武汉 430074)

摘 要 移动通信和移动定位技术的快速发展促进了一个新的研究领域——基于位置的服务(LBSs)。基于位置的数据的隐私保护已经成为基于位置的服务中的研究热点。在基于位置的服务被广泛使用的今天,位置隐私保护的重要性已经被充分地认识到。位置k-匿名[25]是最早提出的用来保护位置隐私的技术,它是在用于保护关系数据记录隐私的k-匿名方法的基础上扩展而来的。目前,关于基于位置服务中的隐私保护的研究已经取得了一定的成果。然而,在基于位置的服务中,服务的质量与用户的隐私是一对矛盾,如何更好地平衡两者之间的矛盾也是研究的重点。另一方面,对用户的隐私进行保护而引发的一系列问题将对服务器处理能力提出新的挑战,例如如何对服务器端的不确定数据进行高效的查询处理等。因此,基于位置服务中的位置隐私保护不仅仅只关注如何保护用户的隐私,还需要关注隐私保护带来的一系列相关问题。本文初步讨论了当前位置隐私保护的方法及有待解决的问题。

关键词 位置隐私,轨迹隐私,隐私模型,隐私保护,服务质量

Overview of Location Privacy Protection

WEI Qiong LU Yan-sheng
(Department of Computer, Huazhong University of Science and Technology, Wuhan 430074, China)

Abstract The explosive growth of wireless communications and mobile database techniques results in the sufficient growth of location-detection devices. We can easily obtain the locations of the mobile objects through positioning techniques which result in the sufficient development of location-based services (LBSs). Location-based services provide corresponding services to users based on the locations of the mobile users, and provide conveniences for mobile users. In location-based services system, mobile users provide their location information to the central server when they issue location-based services, and then the central server will process the query requirements. However, the system can not guarantee that the location-based server is trusted; it will disclose or misuse the location information of the users, so mobile users may suffer from some invade which could not presuppose. To protect mobile users' location privacy, the exact location information of mobile users should not be sent to the location-based server. However, the quality of the service is determined by the precision of location information of the service issuers. Hence a trade-off between location privacy and quality of services emerges. Some solutions have been proposed to deal with location privacy problem in location-based service. In this paper, we give an overview of the methods dealing with the location privacy problem and some problems that have not been resolved.

Keywords Location privacy, Trajectory privacy, Privacy model, Privacy preservation, Quality of service

1 引言

无线通信和移动数据库技术的快速发展,使得移动用户在任何时间、地点查询任意信息的设想成为现实。位置探测设备(例如便携式电话、GPS、RFID等)的快速发展引发了一个新的研究领域——基于位置服务(LBSs),例如基于位置的商店或餐厅(等)的查找、交通报告和基于位置的广告等。基于位置的服务要求用户在向基于位置的服务器提出服务请求时,必须向基于位置的服务器提供自身的位置信息,服务器根据用户提供的位置信息来处理用户提出的基于位置的查询并将查询结果返回给用户[1-3]。

基于位置的服务使得移动用户能够获取与它所在的位置相关的服务信息。移动用户通过配备移动定位装置可以在任意时刻获得自身的位置信息。当移动用户向服务器提出服务请求时,用户通过定位装置获得自己的位置信息并不断传递给基于位置的服务器,服务器根据接收到的位置信息对该用户的服务请求进行处理。由于服务器根据用户的位置信息来处理服务请求,因此用户位置信息越准确,服务器返回给用户的服务信息将越准确。在基于位置的服务中,用户的位置信息的准确性决定了LBSs的服务质量。尽管基于位置的服务和定位技术为移动用户提供了极大的方便,但基于位置的服务器需要先获取移动用户的位置信息才能对移动用户提供相应的服务,而基于位置的服务系统并不能保证服务器不泄露或非法使用用户的位置信息。因此,基于位置的服务给用户的位置隐私保护带来了极大的挑战。

在信息爆炸的今天,数据已经成为一个重要的资源,大量访问数据、共享数据和从数据中抽取信息的方法的出现使得用户也越来越关注隐私保护。用户需要在不暴露隐私信息的

*)本课题获国家"十一五"预研项目资助(513150402)。魏 琼 博士研究生,主要研究领域为隐私保护、数据库等;卢炎生 博士生导师,主要研究领域为数据库、软件工程等。

前提下获得高质量服务。在基于位置的服务中，用户将自己的准确位置暴露给服务器，会严重危害到用户的位置隐私。因此，为保护用户的位置隐私，基于位置的服务器获得的并不是移动用户准确的位置信息；另一方面，服务器需要获得用户的准确位置信息才能为用户提供高质量的服务。降低移动用户位置信息的准确度将直接导致服务质量的下降，同时会增加服务器的负载。

为了保护用户的位置隐私而向服务器提供不准确或不正确的位置信息，服务器返回给用户服务信息可能会是用户完全不感兴趣的信息，这就失去了基于位置服务的本质意义。因此，平衡位置隐私保护和服务质量之间的矛盾是基于位置服务中位置隐私保护的核心问题。为了解决这一问题，已经提出了一些隐私保护方法，这些方法大致可以分为两大类：一类是保护用户的 ID 信息，使得服务器不知道服务请求者的真实 ID；另一类是保护用户的位置信息，即用户提供给服务器的不是准确位置信息而是包含用户所在位置的一块区域。

本文第 2 节介绍了关系数据记录的隐私保护方法并说明这些方法不能直接用于位置隐私的保护。第 3 节介绍了目前广泛使用的位置隐私保护方法和隐私保护的模型。第 4 节介绍位置隐私中的轨迹隐私保护。之后讨论目前位置隐私保护方法中存在的问题以及未来的研究方向。

2 关系数据的隐私保护

数据库技术的成熟发展使得大量数据以记录的形式存储在数据库中。为了从这些数据中获得有价值的信息，需要对关系数据库中的数据进行发布。另一方面，这些数据中包含大量的个人隐私信息，因此发布这些数据必须保证数据中的隐私信息不被泄露。当前对数据发布中的数据隐私保护的研究主要集中在以记录形式存储的数据发布时的隐私保护[4-6,13]，例如医院的病历数据、银行的用户交易数据等。这些方法的主要目的是不泄露个人隐私信息的前提下尽可能保留数据的可用性。关于数据发布中的隐私保护问题，已经提出了大量数据隐私保护方法[7-10,14]。

Sweeney[10]在 2002 年最先提出的 k-匿名方法是一种广泛应用于数据发布中的数据隐私保护的技术。该方法对每条记录的非敏感属性进行泛化，使得发布后的数据中的每条记录都至少不能和其他 $k-1$ 条记录区别开来[11,12]。所有非敏感属性值相同的记录的集合称为一个等价类。k-匿名方法切断了某个个体与数据库中某条具体记录之间的联系，在一定程度上保护了数据的隐私。然而该方法存在一定的缺陷，例如恶意的攻击者也可能从一张匿名表中准确地推测出某个个体的真实敏感信息，这个现象主要是因为根据 k-匿名方法得到的等价类中的敏感信息可能完全相同。同时，k-匿名方法采用泛化技术将导致原始数据中的大量信息被丢失[7]，从而严重威胁到数据分析的准确性。

为解决 k-匿名数据仍可能使得用户的敏感信息被恶意的攻击者获取这一问题，Machanavajjhala 等[8]提出了一种新的隐私保护标准——l-diversity，这种方法将原始数据分割成多个等价类，使得每个等价类中至少有 l 个不同的敏感值。因此，恶意的攻击者不可能以 100%的可能性推断出某个个体的敏感信息。文献[9]通过理论和实验证明了 l-diversity 能够提供更强的隐私保护。尽管 l-diversity 能提供更强的隐私保护，但是它仍然采用泛化技术发布原始数据，从而与 k-匿名方法存在相同的缺陷——发布的数据会丢失大量原始数据中存在的信息。因此，X. Xiao[22]在文献[8]的基础上又提出了一种新的隐私保护方法——anatomy。在对原始数据进行发布时，将原始数据的关系表分解成 ID 表（存放原始表中的非敏感属性）和敏感表（存放用户的敏感属性和一些统计信息）并发布每条记录的准确非敏感属性值。anatomy 在一定程度上抓住了数据之间的联系信息，提高了数据分析的准确性，缓解了 k-匿名方法会丢失大量原始数据间内在联系信息的问题。

上面提到的这些方法能为发布以记录形式存储的数据提供较好的隐私保护，但不能直接应用在位置隐私保护中，主要有三个原因：(1)这些技术主要是用来保护数据库中以记录形式存储的数据隐私，但在基于位置的服务中，不能在用户的准确位置信息存储到服务器之后进行隐私保护，必须在位置信息传递到服务器之前就进行隐私保护。(2)这些用于关系数据库中的数据隐私保护方法的目的是保护数据的隐私而不是查询。在基于位置的服务中，保护的对象是提出基于位置服务请求的用户的位置信息。例如，一个用户想要知道离他最近的 ATM 机，那么要进行隐私保护的对象是这个用户的位置信息，而不是离他最近的 ATM 机的位置信息。(3)这些方法保护的只是数据库某一时刻的状态。对于传统数据库来说，这些技术可能是有效的。因为传统数据库中的数据插入和删除的频率较慢而且这些更新都是通过明确的指令来进行的。但是对于基于位置的服务，数据和查询都在快速地变化。因此，传统的数据隐私保护方法不能适应具有动态特征的位置隐私保护的要求，需要研究出新的适应这些动态特征的隐私保护方法。

3 位置隐私保护

位置隐私保护是阻止其他个体或团体知道某个用户当前或过去的位置的能力。位置隐私信息由标识信息和位置信息组成[15]。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。

传统的位置隐私保护的方法主要是根据组成位置隐私信息的两类信息来进行分类。一类方法是向服务器提供准确的用户位置信息，以便得到高质量的服务信息，而将用户的标识信息（例如匿名、假名等）进行隐藏；另一类方法是将用户的标识信息完全暴露给服务器，而将用户位置信息进行隐藏，即将用户的位置信息模糊化后提供给服务器，以达到位置隐私保护的目的。

3.1 身份保护方法

文献[15]介绍了基于位置的服务与位置隐私之间的关系以及两类隐私保护的方法。匿名方法[24,25]关注的是将用户信息（如位置信息），与用户的真实 ID 信息分开。文献[25]中提出的位置 k-匿名技术是最早提出解决位置隐私保护问题的方法，其主要思想是使得在某个位置的用户至少有 k 个，这 k 个用户之间不能通过 ID 来相互区别。这样，即使某个用户的位置信息被恶意的攻击者获取，恶意的攻击者也不能准确地从 k 个用户中定位到该用户。假名[17]是匿名的一种特殊类型，每个用户使用一个假名来达到隐藏真实 ID 的目的。恶意的攻击者虽然可能从服务器端得到用户的准确位置信息，但不能准确地将位置信息与用户的真实 ID 信息联系起来，增加了定位某个具体用户的难度，从而达到用户的位置隐私保护的目的。Beresford 和 Stajano[19]提出了一种重要的身份保护方法——混合区域（mix zone）。该方法定义了两种类型的

区域:应用区域和混合区域。这两种类型的区域都是一个空间区域。在应用区域中,用户可以提出服务请求和接收服务信息;但在混合区域中,用户没有任何通信。这种方法的有效性在于用户使用假名。为了更好地保护用户的位置隐私,用户使用同一个假名不能超过一定的时间。例如用户在进入混合区域之前使用某一个假名,出混合区域时使用另一个不同的假名。由于用户在混合区域中没有任何通信,增加了将同一个用户前后使用的假名关联起来的难度,从而达到保护 ID 信息的目的。

尽管匿名和假名技术是隐藏用户真实 ID 信息的重要技术,但这类方法存在一定的缺陷,特别是在空间应用领域。为了从大量信息中得到用户感兴趣的信息,数据挖掘技术已经得到了充分的发展。通过成熟的数据挖掘技术可以比较容易地根据用户所在位置准确地推测出用户的标识信息,因此匿名和假名技术都会受到数据挖掘技术的威胁[18,19]。另外,匿名给身份验证和个性化带来了障碍,而在大量应用中都要求身份验证和个性化[20,21],所以在位置隐私保护研究中匿名技术并不是最好的选择。

3.2 位置信息保护方法

由于通过成熟的数据挖掘技术可以比较容易地根据用户所在位置准确地推测出用户的标识信息,匿名技术并不能提供充分的位置隐私保护。因此,另一类位置隐私保护方法得到了极大的关注。这类方法允许服务器知道用户的真实 ID 信息,而通过降低用户位置信息的准确度来达到位置隐私保护的目的。

位置隐私保护方法大致可以分为 3 类:(1)错误的或假的位置信息[26]。在这类方法中,用户发送多个不同的位置信息给服务器,这些位置信息中只有一个是该用户的准确位置,其他的都是错误的或假的位置信息。因此,即使服务器上某个用户的位置信息被恶意的攻击者获取,他也不能根据这些位置信息准确地推测该用户的准确位置。但另一方面,由于每个用户都提供多个位置信息给服务器,增加了服务器的空间开销,还增加了服务器处理服务请求的时间,同时要求移动客户端具有判断服务信息准确性的能力。(2)路标对象[27]。在这类方法中,用户发送给服务器的不是自身的准确位置信息,而是某个路标或某个重要对象的位置信息。这类方法虽然保护了用户的位置隐私,但需要用户从服务器返回的服务信息中判断哪些信息才是真正感兴趣的,增加了移动客户端的负载。(3)区域化位置信息[23-25]。这种方法的主要思想就是将用户的准确位置用一个包含该用户的准确位置的空间区域来替代。这个空间区域可以根据 k-匿名的思想来构造,例如用户提供给服务器的位置区域不仅需要包含该用户的准确位置,而且该区域至少包含 k 个移动用户。这种方法的缺点在于服务质量会大大下降,另外,由于服务器并不知道用户在该区域中的哪个位置,服务器必须确定选取该区域中的哪些位置点作为参考点进行查询处理,选取多少个参考点进行查询处理会使得返回给用户的服务信息更准确。这些增加了服务器的负载,同时也增加了服务器反应时间。

M. Duckham 和 L. kulik[23] 首次提出将 obfuscation 作为位置隐私保护的一种机制,并提出了一种根据模糊的位置信息进行查询处理仍不会降低服务质量的算法,有效地平衡了位置隐私保护与服务质量之间的矛盾。M. Duckham 和 L. kulik[16] 在文献[23]的基础上进一步说明了 obfuscation 位置隐私保护方法。Obfuscation 允许服务器知道用户的真实 ID 并通过降低用户的位置信息的准确度来达到位置隐私保护的目的;另一方面 obfuscation 不需要任何集中式的服务器作为基于位置服务的代理,因而很适合分布式环境,例如 peer-to-peer 系统。

然而,这些位置隐私保护的研究都只是集中在隐藏单个用户的位置信息。尽管这些技术在小规模的基于位置的服务中很有价值,但是在实际的基于位置的数据库服务器上的应用价值是值得怀疑的。因为这些技术缺少两个主要性能:(1)可伸缩性。在一个典型的基于位置的服务应用中,存在大量的并发用户,所以位置隐私保护技术必须具有可伸缩性。(2)查询处理。为了保护用户的位置隐私,基于位置的数据库服务器不能获取用户的准确位置信息,因此服务器必须根据用户的模糊位置信息提供高效的查询处理。这对于传统的查询处理来说是一个挑战。

Mokbel[28,29] 提出了一种能够处理大量并发用户的位置隐私保护问题的方法。该方法综合了 k-匿名和区域化位置信息两种方法的思想并引入了一个第三方——位置匿名器。在用户的准确位置信息发送给服务器之前,位置匿名器利用 k-匿名的思想将用户的准确位置信息替换成一个空间区域,使得提出服务请求的用户在该空间区域内至少不能与其他的 $k-1$ 个用户区别开来。同时在服务器端设置了一个能够处理空间区域查询的查询处理器,根据位置匿名器提供给服务器的空间区域进行查询,并将查询结果候选集返回给用户。该方法保证返回给用户的结果候选集尽可能小且包含用户真正感兴趣的信息。虽然该方法的提出在很大程度上解决了位置隐私保护存在的问题,但对用户的位置隐私进行保护的同时也对服务器端的处理能力提出了更高的要求。另一方面,提出服务请求的移动用户的位置会随时间发生变化,随着用户位置的变化服务器返回用户的服务信息也要做相应的变化,服务信息的实时性也是衡量基于位置的服务质量的一个重要标准。因此,服务器需要具有适应服务请求者位置经常发生改变及保证实时性的能力。

采用位置信息保护方法来实现用户的位置隐私保护,使得存储在服务器上的用户的位置信息都是不准确的数据。如何对这些数据进行快速准确的查询,是位置隐私保护领域的另一个重要问题。因为在基于位置的服务系统中,不仅需要对用户的位置信息提供隐私保护,还需要为用户提供准确高效的服务。文献[44]首次提出了为基于不确定的数据的查询提供概率结果的概念并将这个概念应用到移动数据库中的范围查询(range query)。Cheng 等人在文献[42,43]中提出了在移动数据库模型中为基于不确定数据的最近邻居查询提供概率结果的问题,扩展了概率结果的概念,使得它可以应用到多种查询中。这些应用于不准确数据上的查询处理技术将进一步促进位置隐私保护技术的发展。

3.3 隐私模型

在过去的 10 年,为了保证从客户端发往服务器的数据的隐私安全,已经提出了多种体系结构。

安全团体通信[30,31] 将通信组织在多个团体之间进行。在这种通信方式下,每个团体只知道一部分数据,并不知道其他团体的真实数据。即使某个团体的数据被泄露或被非法使用,也不会导致所有的数据被泄露或被非法使用,从而在一定程度上保证了数据的安全性。然而,这种结构的计算量太大,导致它不能直接应用到数据库问题中。

最小信息共享模型[32] 利用加密/解密技术来执行连接和

交互操作。然而，计算代价太大，且不能为其他查询提供服务，使得这种模型不能应用于实时应用。在移动通信结构中，引入一个不可信任的第三方[33]的主要思想是通过从多个数据源收集安全信息，然后利用第三方来执行查询。虽然这个模型在某种程度上能保证数据的隐私，但由于第三方是不可信任的，它可能会泄露从各个数据源上收集到的信息，从而危害到数据的隐私。目前最通用的模型是在现有的通信结构中引入一个可信任的第三方[34,35]。这种模型主要是利用一个可以被用户信任的第三方来充当用户和数据库服务器之间的中间层，这个模型被广泛应用在位置隐私技术中[19,24,25]。它也被广泛应用到其他领域，例如用来保护 internet 上用户隐私的 anonymizer[36]、用户可信任的第三方 PayPal[37]系统等。

然而，这些利用可信任的第三方模型的商业产品并没有用来保护位置信息的。文献[28,29]利用这种模型作为大量连续移动的用户与基于位置的数据库服务器之间的接口，文中提到的位置匿名器即该模型中的第三方。通过这个可信任的第三方来对用户的位置信息进行区域化和对用户进行匿名处理来达到位置隐私保护的目的。实验表明，这种模型可以为基于位置的服务提供更好的位置隐私保护。

4 轨迹隐私保护

上面分析的位置隐私保护的方法保护的是用户某一个时刻的位置信息，而这些方法都假设用户发送到服务器的请求信息是不会被截取的。因此，这些方法不能直接用来保护用户的多个连续位置信息。而在基于位置的服务中，如何避免用户的位置被追踪也相当重要，因为当用户向服务器提出服务请求时，用户需要向服务器发送请求信息。如果发送的信息在传递到服务器之前就被恶意的攻击者截取，那么恶意的攻击者就会获得用户的位置信息。当该用户再次提出服务请求时，请求信息同样也可能被再次截取。通过连续的截取某个用户的位置信息，恶意的攻击者可以将该用户在不同时刻的位置信息连接起来，最终得到该用户在这段时间内的运动轨迹。一旦得到用户的运动轨迹，恶意的攻击者就能根据用户的运动轨迹来推测用户的行为模式等，严重威胁了用户的隐私。因此，在基于位置的服务中，如何保护用户的轨迹隐私也是一个值得研究的问题。

轨迹隐私保护是用户阻止其他团体或个人通过长时间观察某个用户后获得该用户的一组位置信息的能力。文献[19,40]首次提出了如何避免用户的位置信息被追踪的问题。轨迹隐私保护的主要目的是避免恶意的攻击者追踪用户的行为。因此，当用户在敏感区域内运动时，必须有能力来隐藏他/她的位置信息。文献[38,39]提出的 silent period 方法通过在邻近的用户之间构造 mix-zone[19]，从而通过降低用户的两个或多个位置信息之间的可连接性来避免恶意的攻击者得到用户的运动轨迹。silent period 的主要思想是假设在 mix-zone 中有多个用户，当用户在 mix-zone 中运动时，不发送任何服务请求信息，也不接收任何服务信息。用户在进入 mix-zone 前后使用不同的 ID，从而增加了将一个用户的两个连续位置信息连接起来的难度。

实验表明，silent period 方法能够较好地保护用户的轨迹隐私，但是损失了通信的时隙，因为用户在 mix-zone 中运动时没有任何通信。典型的通信应用对于最大通信时隙和最小带宽都有严格的要求。如果将通信的时隙分配给轨迹隐私保护，将导致通信质量的下降。因此，这种方法不适用于轨迹隐私保护和通信质量之间存在冲突的应用。Huang 等人在 silent period 的基础上又提出了一种改进的方法——silent cascade[41]。silent cascade 在时间和空间两个方面来对用户进行匿名处理，通过平衡用户在 mix-zone 中的延迟与用户的匿名程度，使得恶意的攻击者不能将任何用户的两个或多个位置信息连接起来，同时也不会降低用户对服务质量的要求。另外，作者还提出了一个基于 mix 网络的模型，利用这个模型能够得到一个最佳的 silent cascade 结构，从而能对用户的轨迹隐私提供更强的保护。

目前，对于移动用户的轨迹隐私的保护的研究还处于起步阶段，已有的方法主要集中在切断用户的两个或多个位置的可连接性，通过增加连接用户多个位置的难度来达到轨迹隐私保护的目的。一旦用户的位置信息被连接起来，将会对用户的隐私造成极大的威胁。这是因为在目前的轨迹隐私保护方法中，恶意的攻击者得到的一定是移动用户正确的轨迹信息。如果攻击者获取的不是移动用户正确的轨迹信息，那么即使他得到了，也不能正确地推测出移动用户的行为模式或是对移动用户进行某种攻击。因此，使得攻击者不能获取移动用户正确的轨迹将是轨迹隐私保护技术的另一个研究方向。

5 存在的问题和发展趋势

上面介绍了近年来位置隐私保护技术的主要研究成果。但目前仍有以下几个方面的问题有待解决：

(1)这些研究并没有考虑移动用户之间的交互。在移动环境中，移动用户的移动并不是独立于其他移动对象的。因此，在位置隐私保护技术研究中考虑移动用户之间的交互是目前还没有解决的问题。例如，根据移动用户之间的交互模式将移动用户分成不同的组，随着时间的变化，这些组里面的移动对象也会发生变化。对这些不断变化的移动对象组的集体运动模式进行建模处理，是当前研究所没有解决的一个重要问题。

(2)当前移动对象运动轨迹的隐私保护研究也只是建立在一般的运动模式上。因此，仍需要研究能够为不同运动模式的移动对象提供足够轨迹隐私保护的轨迹隐私保护技术。

(3)位置隐私保护不仅要阻止非法获取用户的位置信息，还要保证不能滥用合法获取的移动对象的位置信息。因此，如何保证移动对象的位置信息不被滥用，也是一个有待解决的问题。

位置隐私保护将导致存储在基于位置的服务系统中的数据库服务器上的数据都是不准确的。随着位置隐私保护技术和其他相关技术的发展，目前已经呈现以下几方面的发展趋势：

(1)概率查询。由于用户不断关注自身的隐私问题，大量数据库服务器端存储的将是经过隐私处理后的不精确的数据。传统的查询处理技术已经不能很好地处理这类数据的查询。目前，已经有一些研究者开始研究不精确数据上的查询处理问题。其中包括非精确数据上的最近邻居查询、非精确数据上的反最近邻居查询和连续概率查询等。

(2)优化问题。概率查询返回给用户的并不是唯一的查询结果，通常情况下返回给用户的是查询结果的候选集，客户端必须对候选集进行评估，以便获取用户最感兴趣或是最符合查询条件的查询结果。这就存在一个评估代价优化的问题。概率查询质量的评价标准也是一个值得研究的问题。例如，如何评价一个概率查询返回给用户的查询结果候选集是

最优的等。

结束语 本文综述了关于基于位置服务中的位置隐私保护方法和技术，总结了位置隐私问题的研究方法以及这些方法存在的问题。另外，讨论了基于位置服务中的另一个重要问题——轨迹隐私保护的相关研究。随着无线通信和移动技术的进一步发展与完善，用户将对基于位置的服务质量提出更高的要求，同时对自身的隐私问题也会更加地关注，这将给基于位置服务下的位置隐私研究带来新的挑战。已有的这些技术(例如匿名通信等)将不能很好地解决移动环境下用户的轨迹隐私保护问题，需要提出更好的用于轨迹隐私保护的方法与技术。因此，位置隐私保护将是一个综合性很强的新兴研究领域。

参 考 文 献

[1] Jensen C S. Database Aspects of Location-based Services. In Location-Based Services, Morgan Kaufmann, 2004: 115-148

[2] Mokbel M F, Aref W G. PLACE: A Scalable Location-aware Database Server for Spatio-temporal Data Streams. In IEEE Data Engineering, Bulletin, 2005: 3-10

[3] Wolfson O, Cao H, Lin H, et al. Management of Dynamic Location Information in DOMINO. In EDBT, 2002

[4] Agrawal R, Jr R J B, Faloutsos C, et al. Auditing Compliance with a Hippocratic Database // Proceedings of the International Conference on Very Large Data Bases. VLDB, 2004: 516-527

[5] Agrawal R, Kiernan J, Srikant R, et al. Hippocratic Databases // Proceedings of the International Conference on Very Large Data Bases. VLDB, 2002: 143-154

[6] Agrawal R, Srikant R. Privacy-Preserving Data Mining // Proceedings of the ACM International Conference on Management of Data. SIGMOD, 2000: 439-450

[7] Xiao X, Tao Y. Anatomy: simple and effective privacy preservation // Proceedings of the International Conference on Very Large Data Bases. VLDB, 2006

[8] Machanavajjhala A, Gehrke J, Kifer D. l-diversity: Privacy beyond k-anonymity // Proceedings of the International Conference on Data Engineering. ICDE, 2006

[9] Xiao X, Tao Y. Personalized privacy preservation // Proceedings of the ACM International Conference on management of Data. SIGMOD, 2006

[10] Sweeney L. k - anonymity: a model for protecting privacy. Intl. Journal on Uncertainly, Fuzziness and Knowledge-based Systems, 2002

[11] Sweeney L. Achieving k-anonymity Privacy Protection Using Generalization and Suppression. International Journal on Uncertainty, Fuzziness and Knowledge-based Systems, 2002: 571-588

[12] LeFevre K, DeWitt D, Ramakrishnan R. Mondrian Multidimensional K-Anonymity // Proceedings of the International Conference on Data Engineering. ICDE, 2006

[13] Lefevre K, Agrawal R, Ercegovac V, et al. Limiting Disclosure in Hippocratic Databases // Proceedings of the International Conference on Very Large Data Bases. VLDB, 2004: 108-119

[14] Jr R J B, Agrawal R. Data Privacy through Optimal k-Anonymization // Proceedings of the International Conference on Data Engineering. ICDE, 2005: 217-228

[15] Baugh J P, JinHua G. Location Privacy in Mobile Computing Environments. In UIC. 2006: 936-945

[16] Duckham M, Kulik L. Simulation of Obfuscation and Negotiation for Location Privacy. In COSIT, 2005: 31-48

[17] Pfitamann A, Kohntopp M. Anonymity, unobservability, and pseudonymity—a proposal for terminology // Federrath H, ed. Designing Privacy Enhancing Technologies. volume 2009 of Lecture Notes in Computer Science. Springer, 2001: 1-9

[18] Duri S, Gruteser M, Liu X, et al. Framework for security and privacy in automotive telematics // Proc. 2nd International Workshop on Mobile Commerce. ACM Press, 2002: 25-32

[19] Beresford A R, Stajano F. Location privacy in pervasive computing. IEEE Pervasive Computing, 2003: 46-55

[20] Hong J I, Landay J A. An architecture for privacy- sensitive ubiquitous computing // Proc. 2nd International Conference on Mobile Systems, Applications, and Services. ACM Press, 2004: 177-189

[21] Langheinrich M. Privacy by dedign—principles of privacy-aware ubiquitous systems // Abowd G D, Brumitt B, Shafer S, eds. Ubicomp 2001: Ubiquitous Computing, volume 2201 of Lecture Notes in Computer Science, Springer. 2001: 273-291

[22] Xiao X, Tao Y. Anatomy: simple and effective privacy preservation // Proceedings of the International Conference on Very Large Data Bases. VLDB, 2006

[23] Duckham M, Kulil L. A formal model of obfuscation and negotiation for location privacy. Pervasive, 2005

[24] Gedik B, Liu L. A Customizable k-Anonymity Model for Protecting Location Privacy. ICDCS, 2005

[25] Gruteser M, Grunwald D. Anonymous Usage of Location-based Services Through Spatial and Temporal Cloaking. // Processing of the International Conference on Mobile Systems, Applications, and Services. MobiSys 2003: 163-168

[26] Kido H, Yanagisawa Y, Satoh T. An Anonymous Communication Technique Using Dummies for Location-based Service // processing of IEEE International Conference on Pervasive Services. 2005: 88-97

[27] Hong J I, Landy J A. An Architecture for Privacy-Sensitive Ubiquitous Computing // Processing of the International Conference on Mobile Systems, Applications, and Services. MobiSys, 2004: 177-189

[28] Mokbel M F. Towards Privacy-aware Location-based Database Services // Proceedings of the 22nd International Conference on Data Engineering Workshops. 2006

[29] Mokbel M F, Chow Chi-Yin, Aref W G. The New Casper: Query Processing for Location Services Without Compromising Privacy // Proceedings of the International Conference on Very Large Data Bases. VLDB, 2006: 763-774

[30] Du W, Atallah M J. Secure Multi-party Computation Problems and Their Applications: A Review and Open Problems // Proceeding of the New Security Paradigms Workshop. 2001

[31] Haas L M, Miller R J, Niswonger B, et al. Transforming Heterogeneous Data with Database Middleware: Beyond Integration. IEEE Data Engineering Bulletin, 1999: 31-36

[32] Agrawal R, Evfimievski A V, Srikant R. Information Sharing Across Private Databases // Proceedings of the ACM International Conference on Management of Data. SIGMOD, 2003: 86-97

[33] Emekci F, Agrawal D, Abbadi A E, et al. Privacy Preserving Query Processing using Third Parties // Proceedings of the International Conference on Data Engineering. ICDE, 2006

[34] Aggarwal G, Bawa M, Ganesan P, et al. Vision Paper: Enabling Privacy for the Paranoids // Proceedings of the International Conference on Very Large Data Bases. VLDB, 2004: 708-719

[35] Jefferies N, Mitchell C J, Walker M. A Proposed Architecture for Trusted Third Party Services // Proceedings of the International Conference on Cryptography: Policy and Algorithms. London, UK, 1995: 98-104,

[36] Anonymous surfing. http://www.anonymizer.com

[37] Paypal. http://www.paypal.com/

[38] Huang L, Matsuura K, Yamane H, et al. Enhancing wireless location privacy using silent period // IEEE Wireless Communications and Networking Conference. NL, U.S., 2005

[39] Huang L, Matsuura K, Yamane H, et al. Towards modeling wireless location privacy // Privacy Enhancing Technology. Cavtat, Croatia, 2005

[40] Grutester M, Liu X. Protecting Privacy in Continuous Location-tracking Applications. IEEE Security and Privacy, 2004: 28-34

[41] Huang L, Matsuura K, Yamane H, et al. Silent Cascade: Enhancing Location Privacy Without Communication QoS Degradation. SPC, 2006: 165-180

[42] Cheng R, Kalashnikov D V, Prabhakar S. Evaluating probabilistic queries over imprecise data. Technical Report TR 02-020. Department of Computer Science, Purdue University, October 2002

[43] Cheng R, Prabhakar S, Kalashnikov D V. Querying imprecise data in moving object environments // Proc. of the 19th IEEE Intl. Conf. on Data Engineering. India, 2003

[44] Wolfson O, Sistla P, Chamberlain S, et al. Updating and querying databases that track mobile units. Distributed and Parallel Databases, 1999, 7(3)