基于位置服务中的隐私保护

孟小峰

近年来随着传感器和无线移动设备的飞速发展，随时随地获得个人位置成为可能。一方面，促进了新一类应用程序——基于位置服务的出现与发展；另一方面，个人隐私保护问题引起人们的广泛关注。由于移动环境中位置信息的特殊性，造成无法直接利用现有的关系数据库隐私保护技术。本文分析了位置隐私保护中存在的挑战问题，从系统结构、位置匿名技术和查询处理技术三方面归纳总结了现有的研究工作，并指出了未来的研究方向。

基于位置服务中的隐私保护

孟小峰
中国人民大学信息学院

报告大纲

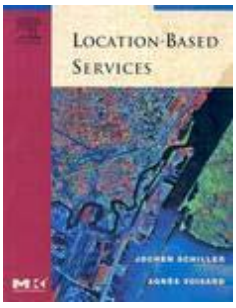
- 隐私保护问题及意义
- 隐私保护系统结构
- 隐私保护研究内容
- 隐私保护面临挑战
- 总结

基于位置服务（LBS）

基于位置服务

- Services that integrate a mobile device's location or position with other information so as to provide added value to a user

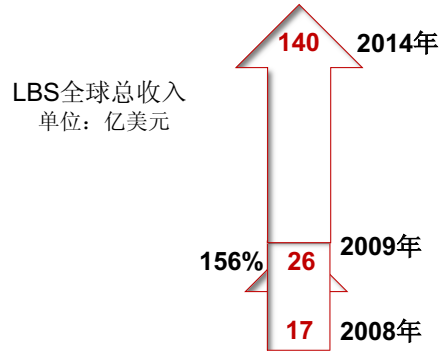
(基于位置的信息服务是将一个移动设备的**位置**或者**坐标**和其他信息整合起来，为用户提供增值服务)

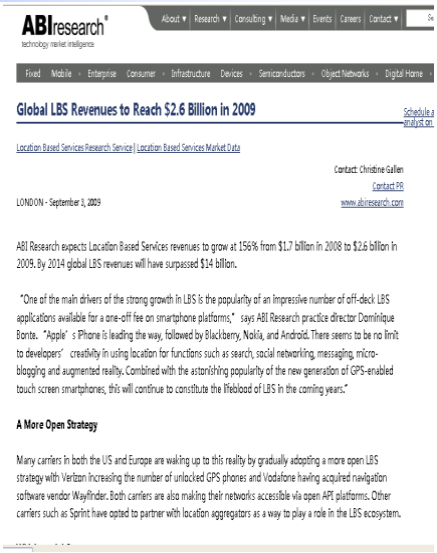


J. Schiller, Jochen, A. Voisard,Location-based Services, Elsevier Science Ltd, April 2004

基于位置服务

- 美国著名市场研究公司ABI research日前发布预测





ABIresearch
technology market intelligence

About ▾ | Research ▾ | Consulting ▾ | Media ▾ | Events | Careers | Contact ▾

Fixed · Mobile · Enterprise · Consumer · Infrastructure · Devices · Semiconductors · Object Networks · Digital Home

Global LBS Revenues to Reach $2.6 Billion in 2009

Schedule a analyst on

Location Based Services Research Service | Location Based Services Market Data

Contact: Christine Gallen
Contact PR
www.abiresearch.com

LONDON - September 3, 2009

ABI Research expects Location Based Services revenues to grow at 156% from $1.7 billion in 2008 to $2.6 billion in 2009. By 2014 global LBS revenues will have surpassed $14 billion.

"One of the main drivers of the strong growth in LBS is the popularity of an impressive number of off-deck LBS applications available for a one-off fee on smartphone platforms," says ABI Research practice director Dominique Bonte. "Apple's iPhone is leading the way, followed by Blackberry, Nokia, and Android. There seems to be no limit to developers' creativity in using location for functions such as search, social networking, messaging, micro-blogging and augmented reality. Combined with the astonishing popularity of the new generation of GPS-enabled touch screen smartphones, this will continue to constitute the lifeblood of LBS in the coming years."

A More Open Strategy

Many carriers in both the US and Europe are waking up to this reality by gradually adopting a more open LBS strategy with Verizon increasing the number of unlocked GPS phones and Vodafone having acquired navigation software vendor Wayfinder. Both carriers are also making their networks accessible via open API platforms. Other carriers such as Sprint have opted to partner with location aggregators as a way to play a role in the LBS ecosystem.

LBS应用领域

- 军事和政府产业
  - 全球第一个位置系统GPS，最初主要用于军事和涉及国家重要利益的民用领域

- 紧急救援服务
  - 1996年，联邦通信委员会（FCC）颁布E-911法规要求移动运营商为手机用户提供紧急救援服务
    1999年FCC对E-911法进行修订
  - 欧洲于2003年1月1日开始实施 “US FCC”标准——建议使用E-OTD即“增强型观测时间差”技术

- 商业公司
  - 定位服务(TAGGING)、追踪服务(TRACKING)、导航服务(TRACING)等

LBS应用分类

- 面向用户 LBS
- 面向设备 LBS
- Push服务
- Pull服务

	Push服务	Pull服务
面向用户服务	当你进入某城市时接到欢迎信息	请求查找最近邻餐馆
面向设备服务	在货物追踪应用中，当货物运送偏离预计轨道时给与警报信息	请求查找卡车现在所在位置

LBS与隐私

- 欧洲委员会
  Directive 2002/58/EC 条款9
  - Location data may only be processed when it is made anonymous OR with the consent of the user for the duration necessary for the provision of a service(位置数据只有在匿名或用户同意的前提下为有效并必要的服务使用).

- Vodafone UK制定了一套隐私管理业务条例(privacy management code of practice),要求所有为Vodafone客户提供服务的第三方必须遵守

LBS中的隐私泄露

- 位置隐私泄露
  - 位置，包括用户过去或现在的位置
- 查询隐私泄露
  - 查询内容，例如查询距离我最近的艾滋医院

行为模式、兴趣爱好、健康状况和政治倾向等个人隐私信息

LBS中隐私保护

- 位置隐私保护
  - 避免用户与某一精确位置匹配
- 查询隐私保护
  - 避免用户与某一敏感查询匹配

位置服务 VS 隐私保护

- 位置服务
  - 提供精确位置
- 隐私
  - 模糊用户的位置

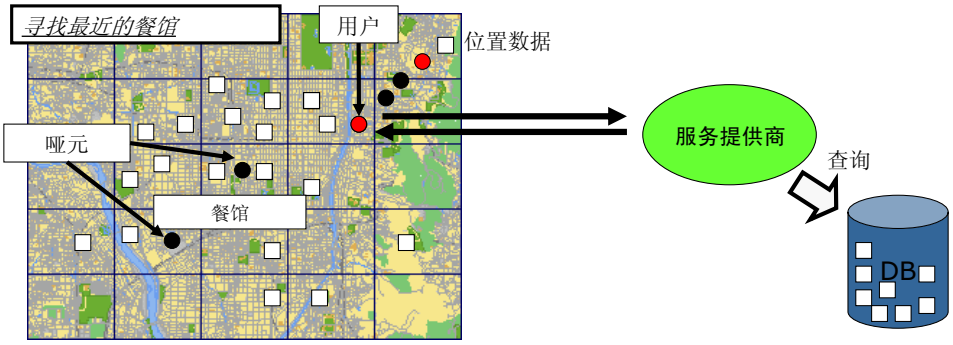
鱼与熊掌可否兼得？

隐私保护的方法

- 假位置（Dummy）
- 时空匿名（Spatio-temporal Cloaking）
- 空间加密（Space Encryption）

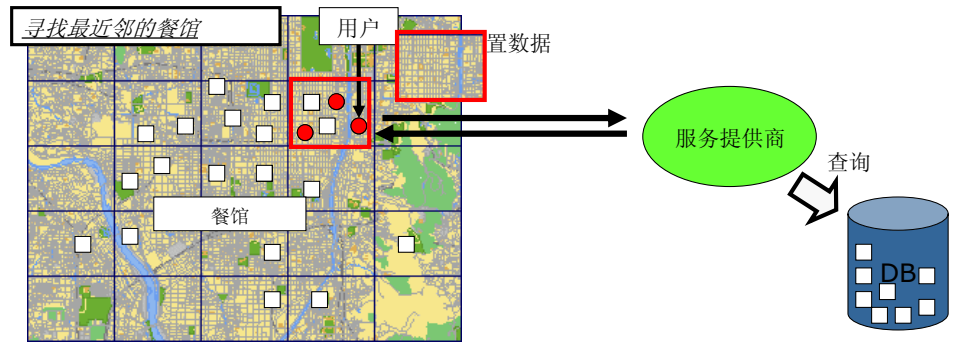
隐私保护的基本方法--假位置

- 通过制造假位置，达到以假乱真的效果



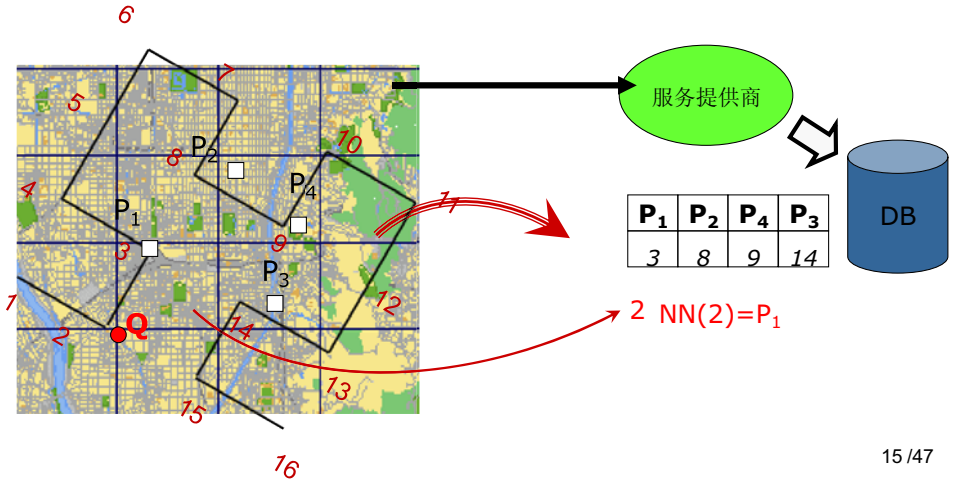
隐私保护的基本方法--时空匿名

- 将一个用户的位置通过扩展变成时空区域，达到匿名的效果



隐私保护的基本方法—空间加密

- 通过对位置加密从而达到匿名的效果



感知隐私保护的查询处理

假数据

- 移动对象数据库中的查询处理器无需作任何修改

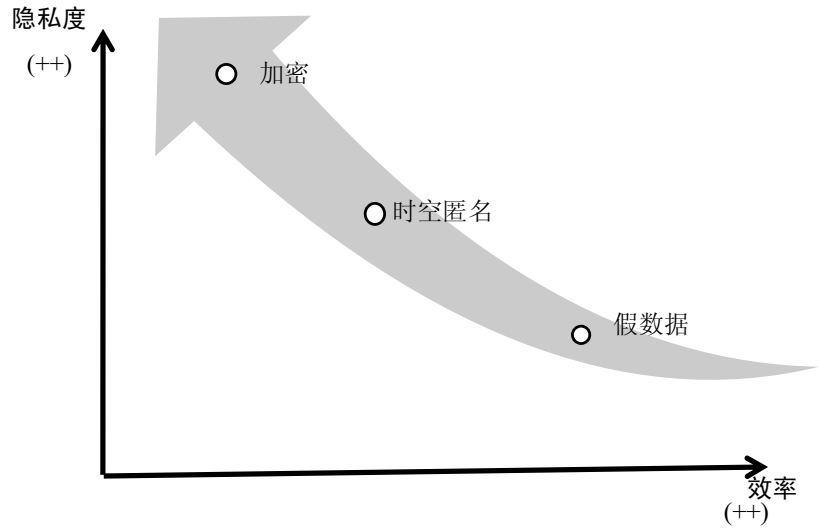
时空匿名

- 设计基于区域位置的查询处理技术；查询结果是一个包含真实结果的超集

空间加密

- 查询方法与使用的加密协议有关

隐私度与效率对比



存在的挑战

- 保护隐私与位置服务是一对矛盾
- 位置匿名的即时性
- 位置频繁更新以及位置依赖性
- 隐私需求个性化

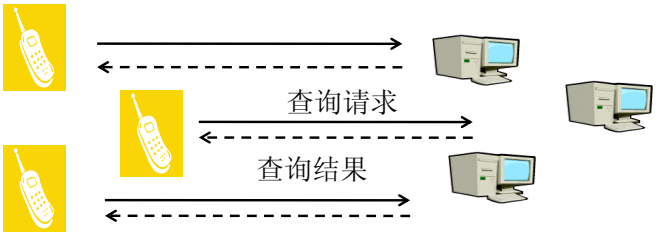
报告大纲

- 隐私保护问题及意义
- 隐私保护系统结构
- 隐私保护研究内容
- 隐私保护面临挑战
- 总结

隐私保护系统结构

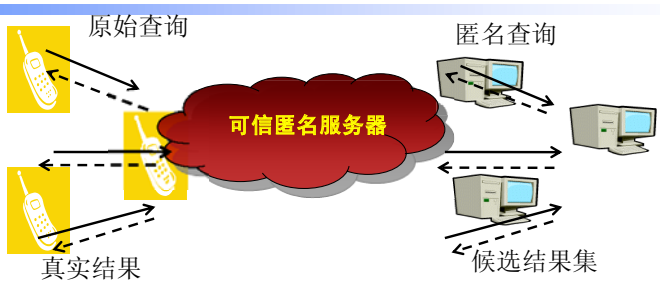
- 独立式结构
- 中心服务器结构
- 分布式结构
- 点对点结构

隐私保护系统结构-独立式结构



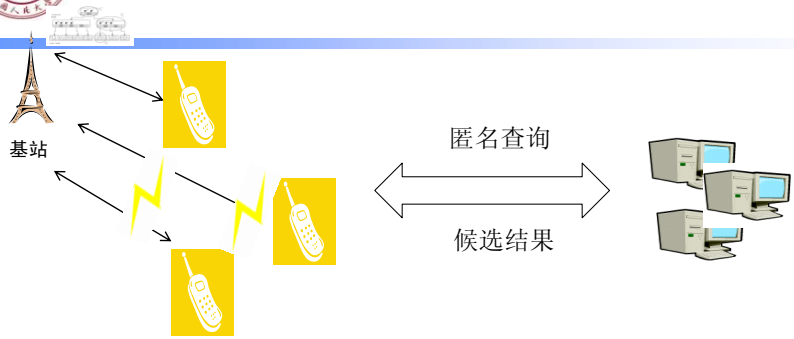
- 优点
  - 结构简单，易于配置
- 缺点
  - 增加客户端负担
  - 缺乏全局信息，隐蔽性弱

隐私保护系统结构-中心服务器结构



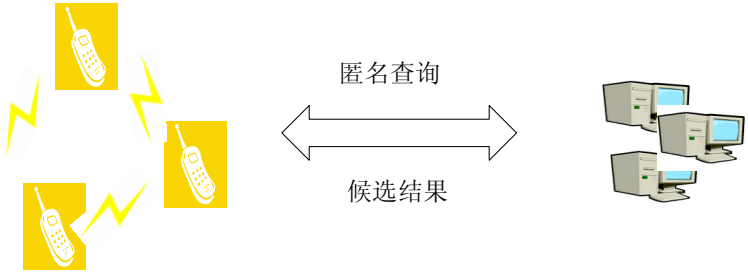
- 优点
  - 具有全局信息，隐私保护效果好
- 缺点
  - 可能成为系统瓶颈
  - 唯一攻击点

隐私保护系统结构-主从分布式结构



- 优点
  - 拥有全局信息，隐私效果好
  - 消除了系统瓶颈
- 缺点
  - 网络通讯代价高

隐私保护系统结构-移动点对点结构



- 优点
  - 拥有全局信息，隐私效果好
  - 消除唯一攻击点
- 缺点
  - 网络通讯代价高

报告大纲

- 隐私保护问题及意义
- 隐私保护系统结构
- 隐私保护研究内容
- 隐私保护面临挑战
- 总结

隐私保护研究内容

- 隐私保护方法
  - 位置隐私保护方法
  - 查询隐私保护方法
- 感知隐私的查询处理
  - 基于区域位置的查询处理技术
  - 基于加密位置的查询处理技术

隐私保护模型

- 位置 *k*-匿名
  - 当且仅当一个用户的位置与其他（*k*-1）个用户的位置无法区别时，称该用户满足*位置k-匿名*

原始查询

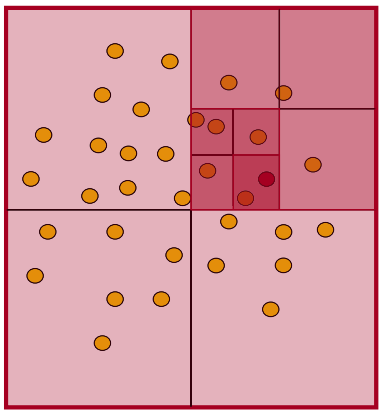
位置	查询
(1, 6)	Q_1
(1, 5)	Q_2
(2, 9)	Q_3
…	…

匿名后查询

匿名位置	查询
[(1,2)-(5, 9)]	Q_1
[(1,2)-(5, 9)]	Q_2
[(1,2)-(5, 9)]	Q_3
…	…

基于四分树的隐私保护方法 (Quadtree based Cloaking)

- 问题
  - 面对大量移动用户，如何快速高效的为移动用户寻找匿名集
- 解决方法
  - 递归式的划分空间，直至在某一子空间内的用户数小于k，则返回其上一级的子空间作为位置匿名区域

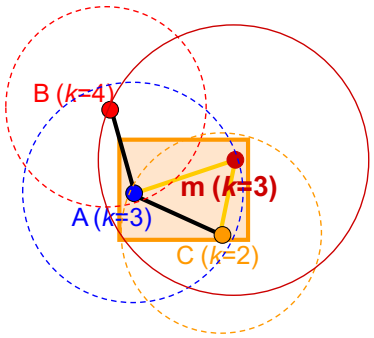


K=3

M .Gruteser,D. Grunwald. Anonymous usage of location-based services through spatial and temporal cloaking.Proceedings of the International Conference on Mobile Systems, Applications, and Services(MobiSys'03), Scan Francisco, USA, 2003:163–168.

个性化隐私需求匿名方法 (CliqueCloak)

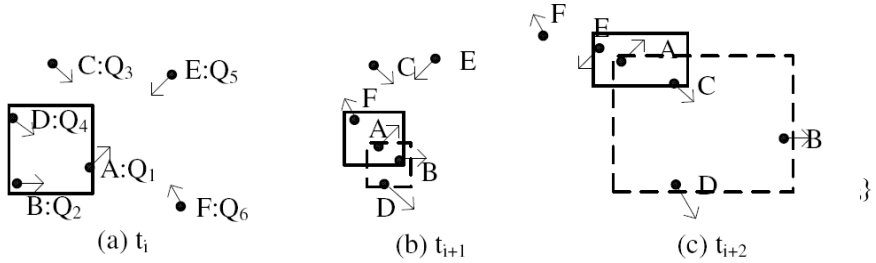
- 问题
  - 如何为每一个用户提供满足个性化隐私需求的匿名
- 解决方法
  - 利用图模型形式化的定义此问题，并把寻找匿名集转化为在图中寻找k-点团的问题



Gedik B, Liu L. Location privacy in mobile systems: a personalized anonymization model. Proceeding of the International Conference on Distributed Computing Systems(ICDCS'05), Columbus, OH, USA, 2005: 620–629

连续查询隐私保护技术（C.Chow and M. F. Mokbel,2007）

- 问题
  - 位置服务中现有的隐私保护工作均针对*snapshot*查询类型



- 解决方法
  - 连续查询的用户在最初时刻形成的匿名集在其查询有效期内均有效。

C. Chow and M. F. Mokbel. Enabling privacy continuous queries for revealed user locations. In *Proceedings of SSTD*,2007

感知查询差异性的隐私保护 (*p*-sensitive)

- 问题
  - 位置*k*-匿名只能防止用户与查询间的关联，但不能切断用户与查询内容的关联
  - 缺少语义的匿名，将产生查询隐私泄露的现象

Location	Query
[(1,2)-(5, 9)]	Hospital
[(1,2)-(5, 9)]	Clinic
[(1,2)-(5, 9)]	Hospital
[(2,5)-(4, 7)]	Gas Station
[(2,5)-(4, 7)]	Gas Station
[(2,5)-(4, 7)]	School

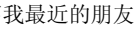
Location	Query
[(1,2)-(4, 7)]	** Club A
[(1,2)-(4, 7)]	Gas Station
[(1,2)-(4, 7)]	Gas Station
[(5,2)-(7, 9)]	Restaurant
[(5,2)-(7, 9)]	Clinic
[(5,2)-(7, 9)]	School

- 解决方法
  - 考虑查询语义
  - 一个匿名集中所包含的敏感查询不能超过p%

X.Zhen, J. Xu, and X. Meng. A Semantic Privacy-Protection Model for Location-based Services. In proceeding of MDM-PALM,2008

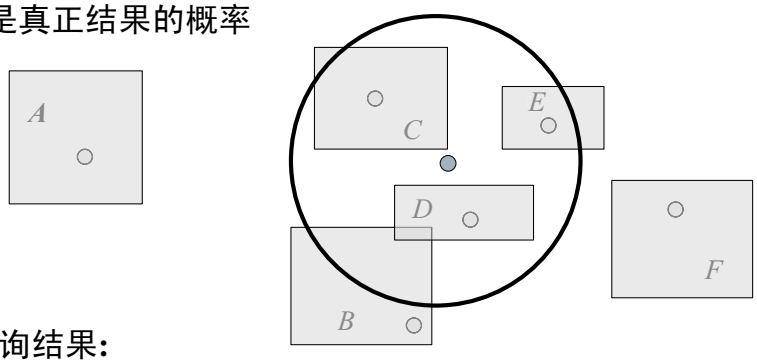
感知隐私保护的查询处理

- 如何在位置被区域匿名后提供令用户满意的服务
- 两种位置数据类型：
  - 公开位置数据．如加油站、旅馆和警车
  - 隐私位置数据．如个人位置

查询类型		被查询点	
		公开数据	隐私数据
查询点	公开数据	基于公开数据的公开查询 如：在某电影院200m内所有餐馆 	基于隐私数据的公开查询 如：某加油站500米内所有出租车 
	隐私数据	基于公开数据的隐私查询 如：距离我最近的加油站	基于隐私数据的隐私查询 如：离我最近的朋友 

基于隐私数据的公开查询

- “某加油站500米内所有出租车”
- 将所有与查询范围相交的匿名区域都作为候选集。
- 根据匿名框与矩形框的重叠区域面积大小表示查询结果是真正结果的概率



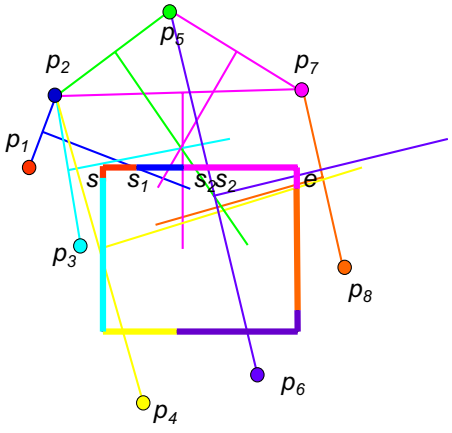
查询结果：

- (B, 50%), (C, 90%), (D,1), (E,60%)

O. Wolfson, P.A. Sistla, S. Chamberlain, and Y. Yesha, Updating and Querying Databases that Track Mobile Units, Distributed and Parallel Databases, vol. 7, no. 3, pp. 257-387, 1999.

基于公开数据的隐私查询

- “距离我最近的加油站”
- 查找匿名区域中任意一个位置的最近邻
  - 查找匿名框所覆盖的对象
  - 查找基于每一条边上的任意点的最近邻
  - 二者的并作为最终的查询结果返回



H. Hu, D. Lee: Range Nearest-Neighbor Query. IEEE Trans. Knowl. Data Eng. 18(1): 78-91 ,2006

报告大纲

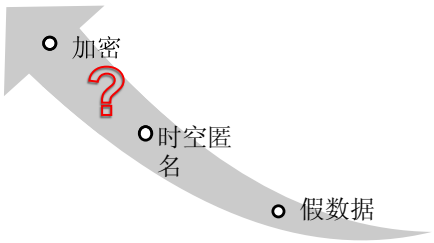
- 隐私保护问题及意义
- 隐私保护系统结构
- 隐私保护研究内容
- 隐私保护面临挑战
- 总结

隐私保护技术面临的问题

- 多技术混合的隐私保护
- 移动对象轨迹的隐私保护
- 室内位置隐私保护

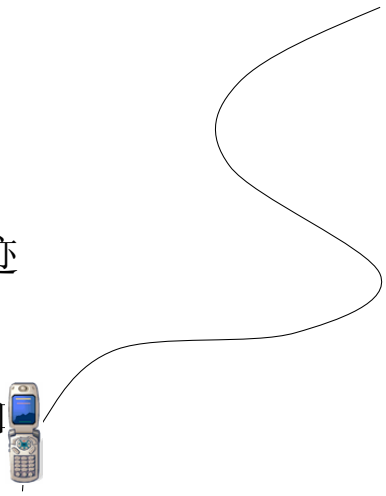
多技术混合的隐私保护

- 问题
  - 加密安全但查询代价高，时空匿名高效但不够安全
- 研究结合加密算法高隐私保护度，空间匿名算法的高效率的混合匿名模型和算法
- 研究基于混合匿名的感知隐私的查询处理算法



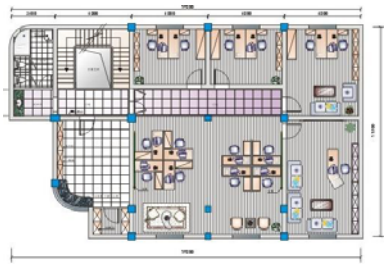
移动轨迹的隐私保护

- 问题
  - 轨迹发布而产生的隐私泄露
- 研究基于时空匿名的轨迹匿名模型和算法
- 研究在线轨迹匿名模型和算法



室内位置隐私

- 问题
  - 室内安装无限传感器收集用户位置用于安全控制、资源管理等
  - 室内提出的查询多位密度查询或聚类查询



- 研究基于室内位置隐私的攻击模型、匿名模型、匿名算法和查询处理算法

可能的解决方法

报告大纲

- 隐私保护问题及意义
- 隐私保护系统结构
- 隐私保护研究内容
- 隐私保护面临挑战
- 总结

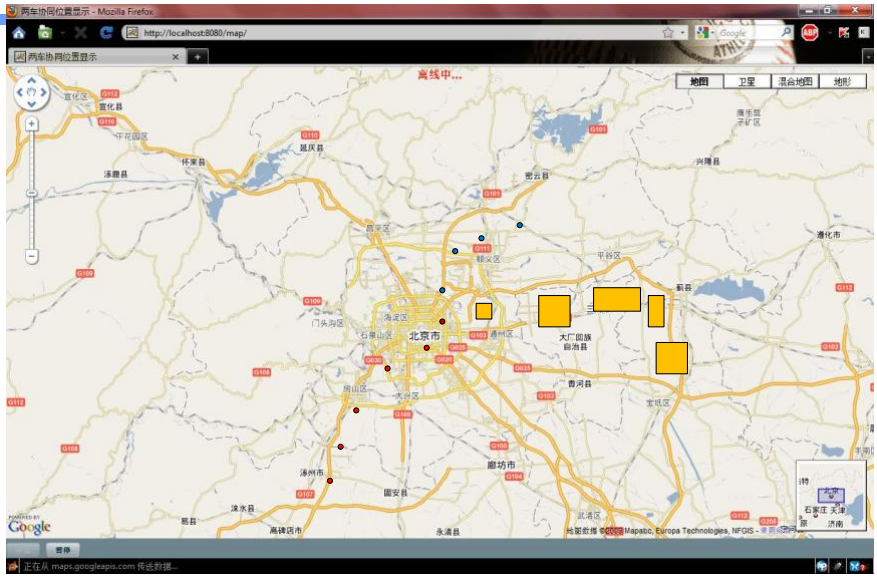
在研课题-隐私保护技术

- 国家863计划重点项目

“普适计算基础软硬件关键技术及系统”项目中“隐私保护技术”课题

- 研究目标
  - 在普适计算以人为中心的理念下，针对个人信息隐私、位置隐私和查询隐私等问题从模型、算法和评价等方面展开研究，开发可配置的分级隐私保护模块，为构建相应示范应用提供支持

在研课题-隐私保护技术



在研课题-隐私保护技术

- 系统界面

参考文献

- O. Abul, F. Bonchi, and M. Nanni, Never Walk Alone: Uncertainty for Anonymity in Moving Objects Databases, In *Proc. of International Conference on Data Engineering (ICDE'08), pp.376–385, 2008.*
- B. Bamba and L. Liu, Supporting Anonymous Location Queries in Mobile Environments with PrivacyGrid, In *Proc. of International Conference on World Wide Web (WWW'08), 2008.*
- K. Bharath, G. Ghinita, and P. Kalnis .Privacy-Preserving Publication of User Locations in the Proximity of Sensitive Sites, *In Proceedings of International Conference on Scientific and Statistical Database Management (SSDBM)* , July 2008
- C. Bettini, X. S. Wang, and S. Jajodia, Protecting privacy against locationbased personal identification, In *Proc. of the VLDB Workshop on Secure Data Management (SDM'05), pp.185–199, 2005.*
- C. Chow and M. Mokbel. Privacy in Location-based Services: A System Architecture Perspective. *The SIGSPATIAL Special Newsletters, SIGSPATIAL Special,* Vol. 1, No. 2, pages 23-27, July 2009.
- C. Chow, M. F. Mokbel, and T. He, Tinycasper: a privacy-preserving aggregate location monitoring system in wireless sensor networks. In proceedings of SIGMOD08(demo), Pages 1307-1310 , Vancouver, Canada ,2008
- C. Chow and M. F. Mokbel, Enabling Privacy Continuous Queries for Revealed User Locations, In *Proc. of the International Symposium on Advances in Spatial and Temporal Databases (SSTD'07), 2007.*
- Chi-Yin Chow, Mohamed F. Mokbel, and Xuan Liu. A Peer-to-Peer Spatial Cloaking Algorithm for Anonymous Location-based Services. *In Proceedings of the ACM Symposium on Advances in Geographic Information Systems, ACM GIS,* Arlington, VA, November 2006:171-178
- R. Cheng, Y. Zhang, E. Bertino, and S. Prabhakar, Preserving User Location Privacy in Mobile Data Management Infrastructures, In *Proc. of Privacy Enhancing Technology Workshop (PET'06), 2006.*
- J. Du, J. Xu, X. Tang, and H. Hu. iPDA: Enabling Privacy-Preserving Location-based Services. In *Proc. of the International Conference on Mobile Data Management (MDM'07), 2007.*
- Electronic Frontier Foundation, *http://www.eff.org/issues/privacy*, December 01,2009
- G. Ghinita ,Understanding the Privacy-Efficiency Trade-off in Location-Based Queries*, ACM SIGSPATIAL GIS Workshop on Security and Privacy in GIS and LBS (SPRINGL), November 2008*
- *G.* Ghinita, Private Queries and Trajectory Anonymization: a Dual Perspective on Location Privacy*, Transactions on Data Privacy (TDP) 2009*

参考文献

- G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K. Tan,Private queries in location based services: anonymizers are not necessary*, In Proc. of SIGMOD'08,* Vancouver, Canada, 2008.
- *G.* Ghinita, P. Kalnis and S. Skiadopoulos, MobiHide: A Mobile Peer-to-Peer System for Anonymous Location-Based Queries, *In Proceedings of International Symposium on Spatial and Temporal Databases (SSTD*), July 2007
- G. Ghinita, M. L. Damiani, and C. Silvestri, Preventing Velocity-based Linkage Attacks in Location-Aware Applications, In *Proc. of the ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems 2009 (ACM GIS'09), 2009.*
- M. Gruteser. and D. Grunwald, Anonymous Usage of Location-based Services Through Spatial and Temporal Cloaking, In *Proc. of the International Conference on Mobile Systems, Applications, and Services (MobiSys'03), pp.163–168, 2003.*
- G. Gidofalvi, X. Huang, and T. B. Pedersen, Privacy-preserving Data Mining on Moving Objects Trajectories, *In Proc. of the International Conference on Mobile Data Management (MDM'07*), 2007.
- B. Gedik and L. Liu, Location Privacy in Mobile Systems: A Personalized Anonymization Model, *In Proc. of the International Conference on Distributed Computing Systems (ICDCS'05),* 2005.
- Gabriel Ghinita, Panos Kalnis, and Spiros Skiadopoulos. PRIVE: Anonymous Location based Queries in Distributed Mobile Systems. *In Proceedings of International Conference on World Wide Web, WWW*, pages 1–10, 2007.
- Gabriel Ghinita, Panos Kalnis, and Spiros Skiadopoulos. MOBIHIDE: A Mobile Peer-to-Peer System for Anonymous Location-Based Queries. *In Proceedings of the International Symposium on Advances in Spatial and Temporal Databases, SSTD*, 2007.
- GPS and Privacy Rights, The New Yorks Times, http://www.nytimes.com/2009/11/23/opinion/23mon3.html?_r=1, November 22, 2009
- H. Hu and J. Xu, Non-exposure Location Anonymity, *In Proc. Of ICDE'09*, 2009.
- http://wiki.media-culture.org.au/index.php/GPS_-_Privacy_Issues,29 Oct 2004
- Hu, H., Xu, J., Du, J., Ng, J.K.Y.: Privacy-Aware Location Publishing for Moving Clients. Technical report, Hong Kong Baptist University (2007) http://www.comp.hkbu.edu.hk/~haibo/privacy join.pdf.

参考文献

- H. Hu and D. Lee, Range Nearest-neighbor Query, *IEEE Transactions on Knowledge and Data Engineering (TKDE),* vol.18, no.1, pp.843–854, 2006.
- H. Kido, Y. Yanagisawa, and T. Satoh,"Protection of location privacy using dummies for location-based services," *Proc.the 25th International Conference on Distributed Computing Systems(ICPS'05)*, 2005.
- H. Lu, C. S. Jensen, and M. L. Yiu, "A3D : anonymity area aware, dummy-based location privacy in mobile services," *Proc. 7th International ACM Workshop on Data Engineering for Wireless and Mobile Access(MobiDE'08*), 2008.
- L. Liu, From Data Privacy to Location Privacy: Models & Algorithms, *In VLDB07* ,2007.
- S. Mascetti, C. Bettini, X. S. Wang, D. Freni, and S. Jajodia, Preserving Anonymity in Location-based Services When Requests from the Same Issuer May be Correlated, *TR*, University of Milan, Italy, 2007.
- M. F. Mokbel, C. Y. Chow, and W. G. Aref, The New Casper: Query Processing for Location Services without Compromising Privacy, *In Proc. of the 32nd International Conference on Very Large Data Bases (VLDB'06),* 2006.
- M. F. Mokbel. Privacy in Location-Based Services: State of Art and research directions. In *MDM07*, 2007.
- X. Pan, X. Meng, J. Xu: Distortion-based Anonymity for Continuous Query in Location-Based Mobile Services. *In the proceedings of the 17th ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems (ACM SIGSPATIAL GIS 2009)*, November 4-6, 2009, Seattle, Washington.
- X. Pan, J. Xu, X. Meng: Protecting Location Privacy against Location-Dependent Attack in Mobile Services. *In Proceedings of the ACM 17th Conference on Information and Knowledge Management(CIKM2008)*, page 1475-1476, Napa Valley, California, October 26-30, 2008.
- L. Sweeney, K-anonymity: A Model for Protecting Privacy, International Journal on Uncertainty, *Fuzziness and Knowledge-based Systems*, vol.10, no. 5, pp.557–570, 2002.
- H. Shin, V. Atluri, and J. Vaidya, A Profile Anonymization Model for Privacy in a Personalized Location Based Service Environment, *In Proc. of the 9th International Conference on Mobile Data Management (MDM'08*), 2008.
- T. Xu and Y. Cai, Location Anonymity in Continuous Location-based Services, *In Proc. of GIS'07*, 2007.
- J. Xu, X. Tang, H. Hu, and J. Du, Privacy-Conscious Location-Based Queries in Mobile Environments, *IEEE Transactions on Parallel and Distributed Systems (TPDS),* accepted to appear, 2009.