**Location privacy in mobile networks**

Privacy: In general, the right to be free from secret surveillance and to determine whether, when, how, and to whom, one's personal or organizational information is to be revealed

Location privacy: a particular type of information privacy that we define as the ability to prevent other parties from learning the one's current or past location.

(**location privacy in pervasive computing**, 2003. )

Problem

The participants tend to share their sensor readings without apprehension as they feel more protected behind pseudonyms. This subjective feeling however leads to a false perception of security, as the use of pseudonyms does not necessarily guarantee privacy in location-based applications.

(**A survey on privacy in mobile participatory sensing applications**. 2011)

Using a long-term pseudonym for each user does not provide much privacy. Because certain region of space are strongly associated with certain identities.

(**location privacy in pervasive computing**, 2003. )

In other words, even if the participant hides his identity from the server, due to the strong correlation between people and their movement, a participant can still be identified by his location.

(**Towards preserving privacy in participatory sensing**, 2011. PerCom.)

Location-based attack (inference attack): A location-based attack is to identify a query issuer by associating the query to the query location.

(**Towards preserving privacy in participatory sensing**, 2011. PerCom.)

Target: protect users’ or participants’ identity from location-based attacks.

Categories of countermeasures (depending on hiding information—根据所要隐藏信息的类型):

1. hide user identity
2. Change the pseudonyms frequently to avoid being identified by the locations they visit. Introducing Mix Zone as a zone of several users within each other’s proximity, in which they change their pseudonyms simultaneously.

* *Location privacy in pervasive computing. 2003.*

指出仅仅使用匿名的方式无法保证用户隐私，易于遭受inference attack，其中intruder将location视为一个quasi identifier，首次提出mix zone的概念，提出两种评估位置隐私的metric：匿名集的大小和用户移动性的熵值。

* *Traffic-aware multiple mix zone placement for protecting location privacy. Infocom. 2012.*

1. Pseudonyms changing may cause service interrupt, how to make a decision to balance the privacy gain and change cost among an users’ group.

* *Personalized location privacy in mobile networks: a social group utility approach. Infocom. 2015*

提出使用game theory为移动用户是否进行匿名切换的决定过程进行建模，创新的引入社交因素作为用户切换匿名的动机/收益，在确定效益函数的基础上，分析是否存在均衡。

* *AnonySense: A System for Anonymous Opportunistic Sensing. Journal of Pervasive and Mobile Computing. 2010.*

利用ToR路由来隐藏用户的真实IP，避免暴露用户身份信息。

1. **hide user location**
2. **Dummy location**

利用冗余的假数据来掩饰自己的真实位置，用户在提交位置请求时产生多个dummy数据用以同真实位置数据的混合.

* *SpaceTwist: Managing the Trade-Offs Among Location Privacy, Query Performance, and Query Accuracy in Mobile Services. ICDE.2008*

用户提交一个假的位置请求，位置点称为anchor location，同时提交的信息包括一个demand space，这个space同时覆盖了真实位置点及其周围感兴趣的sites，通过不断的迭代比较，用户缩小demand space，同时记录在真实点附近的supply space，当前者包含于后者时，停止迭代，后者即是请求的结果。

* *PROBE: an Obfuscation System for the Protection of Sensitive Location Information in LBS.2008.*

针对的是用户所处位置未sensitive位置（如医院、军队）时如何进行隐藏，该方案首先通过离线的过程将整个map划分为多个区域，每个区域不相交，区域内部同时包含sensitive位置和不敏感位置，用户在提交位置信息的请求时使用这个区域替代真实位置，避免将自己在sensitive位置的这个信息泄露出去。

* *A game-theoretic approach for achieving k-anonymity in Location Based Services. Infocom. 2013.*

问题：

产生大量的冗余请求或错误数据；

依然存在通过位置推断发现用户真实身份的威胁；

1. **Location cloak( spatial cloak )**

Using an area cloak to obfuscate the location when submit a location-based query, the cloak should containing at least K users’ location point to provide K-anonymity on location privacy.

Location obfuscation方法中，用户在请求LBS服务时，提交假的位置信息或使用一个固定不变的位置信息。

* *Efficient algorithm for K-anonymous location privacy in participatory sensing. Infocom. 2012.*

提出一个基于位置hash的方法，为位置(x,y)计算一个cloak，cloak包含至少K个查询点，从而实现了对位置查询的K-匿名；提出基于VD（VD图，将包含若干sites的map划分为多个区域，每个区域与一个或多个sites相关）的KNN方法，为一个cloaked的area选择K个邻近点。

* *On non-cooperative location privacy: a game-theoretic analysis. CCS. 2009*

问题：

使用spatial cloak方法以及位置模糊(location obfuscation)方法可以起到隐藏用户真实位置的目的，然而由于将位置数据粗粒度化或提交了假的位置信息，所以会影响LBS服务的质量。

1. **Encryption**

* *Private Queries in Location Based Services: Anonymizers are not Necessary. In SIGMOD, 2008.*

PIR协议支持用户以密文的方式从数据库中查询返回信息，数据库服务器并不知道用户查询和反馈的信息。该类方案的核心在于：设计在密文上进行运算和检索的算法。

文献针对如何在密文上进行“find the closest POI to my location”提出一种方法：首先LBS在离线阶段将包含POI（Point of Interest）的space划分为多个区域，在收到查询请求后，server先将几个区域发送给user，user判断自己的位置在哪个区域中（不妨称为A区域），进一步使用PIR方法查询A中所有的POIs，在这个过程中，server并不知道向用户retrieve了哪个region。

针对位置数据查询的过程，可以使用密文搜索方法，即根据用户提交的关键词，与密文形式存储的数据进行特征匹配，再以密文的形式返回匹配的结果，如KNN用于返回K个与用户上传数据最邻近的点；

针对位置数据的计算，可以使用全同态加密方法。

（补充：搜索的核心是匹配，计算的核心是找到一个密文计算X可以映射为对应的明文计算Y）

**Categories of countermeasures (depending on system architecture—根据保护系统的结构):**

1. **Centralized, approaches that require a trusted server**

Relay on a trusted Central Authority or a trusted anonymizer to process queries including location information.

* *Efficient algorithm for K-anonymous location privacy in participatory sensing. Infocom. 2012.*

Location cloak和location generalization属于集中式的隐私保护范畴，这些方法要求用户提交的位置查询请求在送至服务器之前汇总至一个可信第三方，由第三方进行临近位置的加壳或者泛化处理。

问题：

集中式的方法依赖于一个集中的CA第三方进行所有用户位置信息的处理，存在以下的问题：

1) 真实环境中往往不存在一个可信的CA；

2) 这个集中式的CA会成为整个服务的瓶颈和隐私保护的软肋。

1. **Distributed, user-side approaches**

Users autonomously perform location obfuscation without a centralized 3-th party anonymizer.

* *A game-theoretic approach for achieving k-anonymity in Location Based Services. Infocom. 2013.*

Dummy location, pseudonyms changing, location perturbation都属于分布式的隐私保护策略，用户在上传数据或请求之前，**在本地**进行位置数据的处理或匿名的管理。

**Survey**

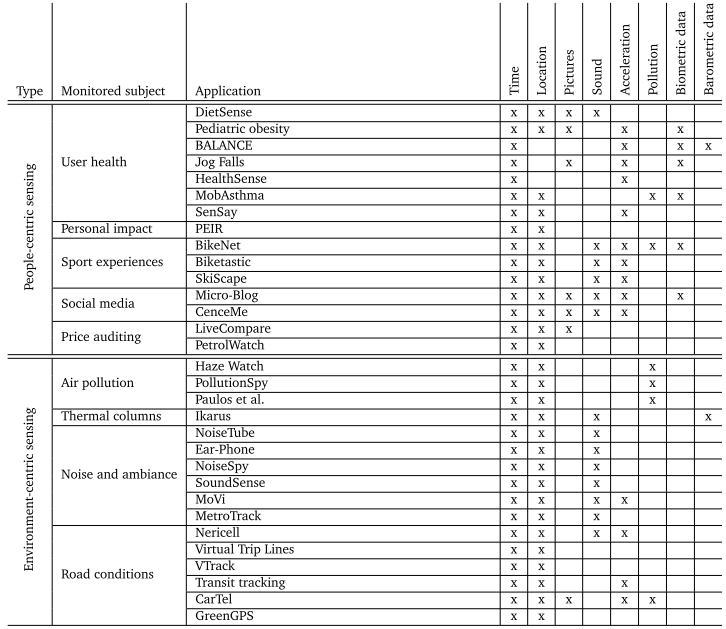
* *Private queries and trajectory anonymization: A dual perspective on location privacy. Transactions on Data Privacy. 2009.*
* *Privacy-preserving data publishing: A survey of Recent Developments. ACM Computing survey. 2009.*

**Privacy in mobile crowdsensing**

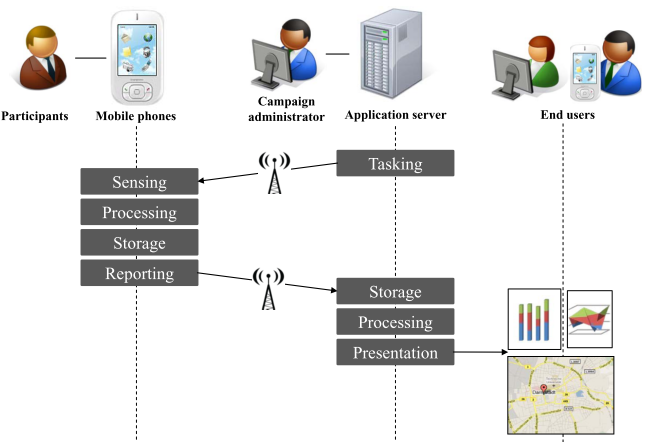
**MCS应用总结：**

以人为中心的感知，people-centric sensing，收集的主要是关于用户自身的数据，例如健康数据（diet），运动数据（bike，sport）；

以环境为中心的感知，利用用户的移动设备进行周围环境相关数据的采集，与以人为中心的感知相比，该类应用采集的数据往往变现为团体规模形式，而非个人为标签。



**MCS应用中的参与实体和他们的具体工作**：参与人、应用服务器和第三方使用者。



MCS中收集数据中潜在的隐私问题（注意，这在LBS服务中是不存在的，因为LBS只提交位置，不提交数据，MCS的数据中可能包含用户的健康状况信息、用户的身份识别信息（声音等生物指纹））。The collected data can be used to extract or infer sensitive information about a user’s “private life, habits, act and relations”- the basic privacy information defined by [The Right to Privacy].

保证数据可用的重要性。Contributed sensor data are vital to any MCS application, and their deficiency endangers the success of MCS systems.

定义：Privacy in MCS is the guarantee that participants maintain control over the release of their sensitive information. This includes the protection of information that can be inferred from both the sensor readings themselves as well as from the interaction of the users with the participatory sensing system.

**数据揭露用户隐私的实例**

Unobtrusive User-Authentication on Mobile Phones using Biometric Gait Recognition. 2010.

文章指出随着智能手机的普及和移动应用的发展，智能手机已不再仅仅是一个通信设备，包括邮件、文档、金融信息在内的诸多敏感信息都存储在手机上，所以对手机的接入认证是至关重要的。大部分手机提供PIN方式的接入认证技术，用户需要在每次进入手机之前输入PIN码，not very user friendly，已有的调查显示，仅有66%的用户选择使用这种模式，需要频繁的输入密码是妨碍使用的主要原因。

文中提出使用用户的步伐识别进行接入认证，这一生物信息可以在unobtrusive的情况下采集得到，所以处于移动状态下的用户可以不用输入任何信息即进入手机。

从另一方面看，如果在MCS应用中将accelerator的数据上传，将暴露用户隐私。

Towards preserving privacy in participatory sensing. Percom, 2011.

利用spatial cloak进行位置隐藏和隐私保护。

Towards Privacy-Sensitive Participatory Sensing. Percom, 2014.

利用tessellation和microaggregation进行位置隐藏和隐私保护。

上述工作都是利用spatial cloak的方法，需要引入可信第三方计算cloak或用于替代的位置点，同时，具有精度上的开销。。。

可否借鉴LBS隐私保护中的匿名切换策略。。。