Deliverable WP.4 Task 4
Report on New Location Privacy Methods

Dr. Agusti Solanas

CRISES Research Group
Dept. Computer Engineering and Mathematics
Rovira i Virgili University
Av. Paisos Catalans, 26
43007 Tarragona

October 2, 2009

Contents

Abstract

The massive use of mobile devices equipped with self-location technologies such as GPS has fostered the appearance of an unprecedented number of location-based services (LBS) that are gaining importance rapidly. The location-based applications that these new technologies can bring to people are almost unlimited and their advantages paramount, however, the wide deployment of LBS can jeopardise the privacy of their users and raise social concern. Consequently, ensuring user privacy is essential to the success of those services.

This report surveys some of the most relevant techniques, which can be found in the literature, to guarantee the location privacy of LBS users. These techniques are classified according to their ability to operate with or without trusted third parties (TTP), and according to their ability to protect the privacy of users by distorting their real locations or by keeping them untouched.

Also, we summarise the main contributions that the CONSOLIDER team has achieved in this active field of research, and we sketch some ideas on the future of location privacy.

All the articles related to location privacy published by the CONSOLIDER team between 2007 and 2009 can be found in the Appendix.

Keywords: Location-based services, location privacy, vehicular area networks.

1 Introduction

Information and Communications Technologies (ICT) are the fundamental building blocks of a modern Information Society. As ICT reduce their costs and increase their ubiquity, the way our society uses them rapidly changes to become wider, more dynamic, and more efficient. A clear example of the wide penetration of ICT in our society is the use of mobile phones. In Europe, the use of mobile phones has grown dramatically to reach extraordinary levels of usage above 75% in all European countries (cf. Figure 1).

In addition to the great advances in computation that have led to more powerful and affordable computers and portable devices, the unprecedented explosion of the wireless and mobile communications market has fostered the appearance of services that allow users to retrieve, manage and share information anywhere, anytime. Some of these virtually pervasive services are fed with location information and private data from users so that they can retrieve data related to their current location. These services are called Location-Based Services (LBS). LBS provide users with highly personalised information accessible by means of a variety of mobile devices that are able to locate themselves, e.g. by using a GPS or a fixed network infrastructure with GSM [10]. Mobile devices are ubiquitous and services related to the user's current location proliferate. Examples of LBS are location-based tourist information [30], route guidance [40], emergency assistance [24], location-based advertising [21], etc.

The extensive deployment of ubiquitous technology is not without privacy drawbacks. By sending their locations, LBS users could endanger their security and privacy because, for example, an attacker could determine their location and track them. This tracking capability of attackers opens up many computer-aided crime possibilities (harassment, car theft, kidnapping, etc.). Also, if an attacker impersonates an LBS provider, the traffic patterns of LBS users could

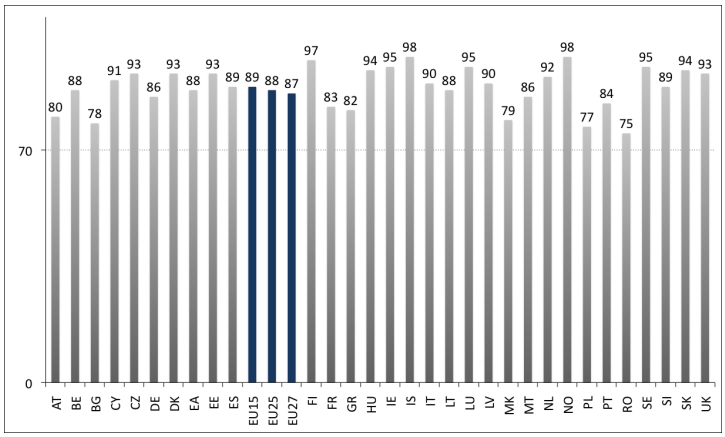


Figure 1: Percentage of use of mobile phones in Europe (source: Eurostat)

be influenced by false information, and the users' location could be compromised [20]. Moreover, there are other attacks that aim to identify users by means of the locations contained in the queries they send to service providers. Although the identities of the users are kept secret, by analysing users location and queries, attackers can disclose the real identities of the users. In those ways, attackers can obtain detailed profiles of the users and send them undesired advertisements or even harass them. Some examples of techniques/attacks used to identify users are the restricted space identification (RSI) attack and the observation identification (OI) attack. The RSI attack consists in linking locations to identities by using queries which are submitted from a restricted space (e.g. if a user submits queries from his garage in a suburban house, it is easy to link those queries to his/her real identity by looking up who lives in that house, for example by means of a phonebook). Similarly the OI attack links queries to identities by observing where users are (i.e. the attacker knows the user's location because he/she can see him) and correlating this information with the location contained in their queries [18].

Several countries have taken legal initiative to cope with privacy problems related to electronic communications. In Europe, the European directive on Data Protection and Privacy [37] agrees on a set of measures to assure the privacy of the users of telecommunications technologies such as LBS. Similarly, the Wireless Privacy Protection Act [1] does the same in the US. Unfortunately, all these measures regulate well-established business models but they can hardly be applied to the new LBS that arise in ad-hoc networks created and dismantled on the fly.

Although there are many relevant topics related to LBS (e.g profile anonymisation [3, 29], trajectories analysis [19, 36], privacy in location-based community services [25], etc.), in this report we concentrate on the methods to protect the location privacy of LBS users who send their location to an LBS provider.

1.1 Contribution and plan of the document

This document summarises the most relevant techniques proposed in the literature to protect the privacy of LBS users. The described methods are classified according to their ability to operate with and without trusted third parties (TTP) and, according to their ability to protect the privacy of users by distorting their real locations or by keeping them untouched. In addition, the main contributions that the CONSOLIDER team has made to this active field of research are summarised, and some ideas on the future of location privacy are sketched. The rest of the document is organised as follows: Section 2 describes the scenario, this is, the main actors and their basic interactions along with some notations and examples to illustrate the privacy risks that LBS users face. Section 3 provides two alternative classifications of the location privacy preserving (LPP) schemes that are later summarised in Section 4. In Section 5 we draw some conclusions and point out some future research lines. The report finishes in Section 6 with a summary of research results. The publications of the CONSOLIDER team can be found in the Appendix.

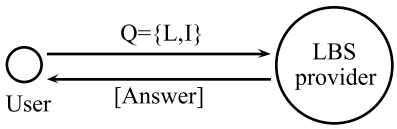


Figure 2: Simplest communication scheme between LBS users and providers

2 Scenario

All the schemes to protect the location privacy of LBS users considered in this report have two main actors in common: LBS users and LBS providers. Providers receive location information and/or personal data from users along with queries related to a wide variety of topics depending on the service provider (e.g. concierge services, emergency services, etc.).

It is assumed that users and providers have the ability to exchange information by means of a wireless communication channel, which is not necessarily secure, provided by a telecommunications company or the like. Thus, the communication channel provider and the service provider could be different entities with different degrees of trust. In the following, we simply assume the existence of communication channels between users and providers and we do not take for granted any special properties such as resiliency or security of these channels.

2.1 The simplest scheme

In the simplest form of communication between an LBS user (U) and an LBS provider (P), the former sends a simple query (Q) containing his location (L) and a request for information (I) that he wants to retrieve from P (cf. Figure 2 for a graphical representation of this simple communication scheme). Thus, a simple query Q sent from U to P can be:

$$Q = \{L, I\} = \{x_U, y_U, \text{“}Where\ is\ the\ closest\ bus\ station?\text{”}\}$$

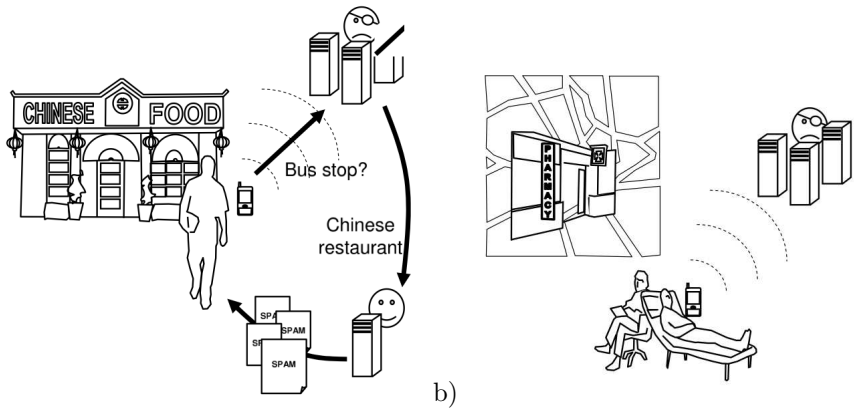
and the answer A from P can be:

$$A = \{The\ closest\ bus\ station\ to\ (x_U, y_U,)is\ located\ in\ (x_A, y_A)\}$$

or simply a set of locations sorted from the closest to the furthest:

$$A = \{(x_{A_1}, y_{A_1}), (x_{A_2}, y_{A_2}), \ldots, (x_{A_n}, y_{A_n})\}$$

Note that by sending their current locations to P, LBS users assume that P manages their data honestly and refrains from any misuse. However, LBS providers cannot always be trusted and more complex communication schemes are needed. As a result, a number of location privacy preserving (LPP) methods have been proposed.



a) b)

Figure 3: Examples of situations where privacy could be endangered. a)The consumer habits of users can be inferred. b) Personal information of users can be disclosed

2.2 Putting privacy in danger: two examples

There are many situations in which we can put our privacy in danger by freely releasing our real location information to LBS providers. Let us describe two situations in which LBS users can put their privacy in danger. In the first situation we show how to infer the consumer habits of users and, in the second, we describe how to disclose personal information from them.

2.2.1 The Chinese food fan

Consider an LBS user U who really enjoys Chinese food and he frequently visits different Chinese restaurants at lunch time. After having lunch, he has to come back home and he looks for the closest bus station to do so. Instead of carrying a timetable and a map of the public transportation system of his city, he uses an LBS that provides him with the information he needs by simply sending his current location (x_U, y_U) to the service provider P. After repeating these actions several times, P could detect that the locations he receives from U correspond to Chinese restaurants and, consequently, he can determine that U is a Chinese food fan. If P is not a honest provider, he can sell this information to a spammer who would send undesired advertisements about Chinese restaurants to U.

It is apparent that the provider has been able to infer the consumer habits of U, thus, harming his privacy. This situation is illustrated in Figure 3.a.

2.2.2 The patient

Let us consider another user U that suffers from a given disease and has to visit several doctors in different hospitals. Right after visiting the doctor, U has to go to a pharmacy to buy some medicines. Due to the fact that he is visiting several doctors and hospitals, he do not know where pharmacies are and he uses

an LBS to find out where the closest pharmacy to his current location is. To do so, he sends his current location to a provider P. P sends back the information to U and stores the query from U. After repeating these actions several times, P could determine that U visits hospitals frequently and that he is a patient because he is asking for information about pharmacies (alternatively he could have been a doctor instead of a patient). Consequently, P can conclude that U has some kind of disease. If P does not behave properly, he can send this information to insurance companies that will raise the costs of the insurance of U because he suffers from a disease.

It is clear that due to the sending of location information and queries, providers could be able to infer personal data from users (e.g. the degree of healthiness). This situation is illustrated in Figure 3.b.

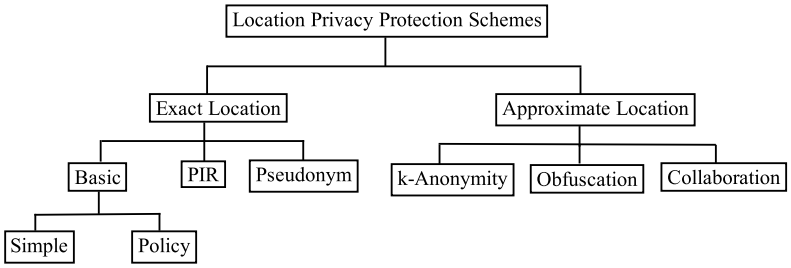


Figure 4: Exact vs Approximate location methods classification

3 Classification of location privacy protection methods

With the aim to avert some of the privacy threats that arise when LBS are used, several techniques have been proposed. Before describing these proposals, we first classify them so that they can be better put in context.

There is not a general agreement about how to classify the existing LPP methods because several criteria can be used. We propose two alternative classifications that pay attention to two different key points of LPP methods: the use of trusted third parties (TTP) and the degree of location distortion.

3.1 Exact vs. Approximate locations

The way in which LPP methods modify users real locations to prevent them from being disclosed is essential. A classification based on this criterion is shown in Figure 4.

On the one hand, we find methods that distort the location information of the users i.e. instead of sending the real location, a wider area containing the real location is sent (cf. Figure 5), or some noise is added to the real location. By doing so, it is expected that the provider will not be able to correctly infer personal information from users. Consider the example of the Chinese food fan, if the user modifies his locations in such a way that the provider cannot link them to Chinese restaurants, it becomes impossible to infer that the user is a Chinese food fan from this information.

On the other hand, other proposals keep the location information untouched and try to hide the relation between the identity of the user and his location. To do so, some methods use intermediate entities that hide the user from the provider or use temporary pseudonyms. Consider the example of the patient. If the provider is able to know that a user has some kind of disease but he is not able to link this information with a real person (i.e. name, telephone number, etc.), this information is useless and he cannot obtain any benefit from selling it (i.e. nobody will pay for it).

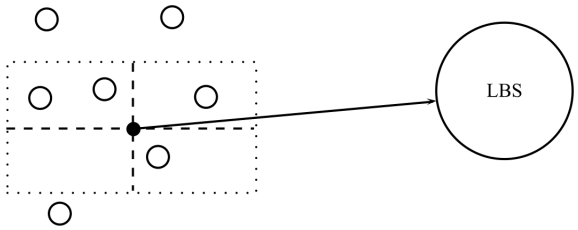


Figure 5: Users collaborate to build a cloaking area that hide their real location from the service provider

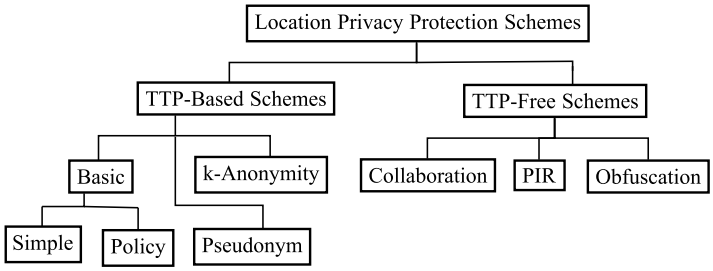


Figure 6: TTP-Based vs TTP-Free methods classification

3.2 TTP-Based vs. TTP-Free

An alternative to the above classification considers the use of trusted third parties by LPP methods. A classification based on this criterion is shown in Figure 6.

Most of the solutions proposed in the literature to address the location privacy problem are based on Trusted Third Parties (TTP), i.e. entities which fully guarantee the privacy of their users. Although this approach is widely accepted, it simply moves users' trust from LBS providers to intermediate entities. By doing so, LBS providers are no longer aware of the real locations and identities of the users; trust and, by extension, power are handed over to intermediate entities such as brokers, pseudonymisers or anonymisers. The problem is that users are not necessarily satisfied by completely trusting intermediate entities or providers, especially after the recent scandals related to the disclosure of personal data by this kind of trusted entities[1] (cf. Figure 7.left).

The main difference between the simple communication scheme and the TTP-based one is that in the latter the set of intermediate entities can be

[1]In Autumn 2007, several data privacy disasters happened in the UK connected to Her Majesty's Revenue and Customs. Two computer disks full of personal data on 25 million British individuals disappeared; HMRC also lost another disk containing pension records of 15,000 people and a laptop containing personal data on 400 people. In 2006 in the U.S, data on 26.5 million people were stolen from the home of an employee of the Department of Veterans Affairs, and queries by 658,000 users were disclosed by the AOL search engine.

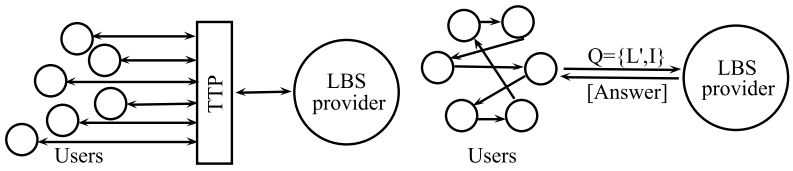


Figure 7: Illustration of the TTP-Based (left) and TTP-Free (right) schemes

expected to be smaller than the number of service providers. Therefore, intermediate entities can be well-known and the risk of trusting a dishonest entity is lessened. However, due to the above mentioned scandals, many users would prefer to trust nobody, which leads to TTP-free schemes. These represent a substantial change of paradigm (cf. Figure 7.right). Instead of trusting a third party, users collaborate to protect their privacy. Figure 6 depicts a classification of location privacy methods. The main aim of the classification is to emphasise the rigid dichotomy between these two paradigms: (i) TTP-based methods and (ii) TTP-free methods. In the following section we review some of the most relevant representatives of TTP-based and TTP-free methods.

Scheme / Method	TTP-Based	TTP-Free	Exact Location	Approximate Location
Simple	√		√	
Policy	√		√	
Pseudonym	√		√	
k-Anonymity	√			√
Collaboration		√		√
Obfuscation		√		√
PIR		√	√	

Table 1: Main features of the described schemes according to the classifications provided in Section 3. Although there can be variants of the main schemes that do not fit into this classification, it represents the most common features of each scheme.

4 Location Privacy Preserving methods

In this section, we describe the most relevant LPP methods proposed in the literature. We use the TTP-based vs. TTP-free classification to present these proposals in an ordered way. A brief summary of the main features of each method can be found in Table 1.

4.1 Privacy in TTP-based schemes

TTP-based schemes are very common because they are simpler than TTP-free schemes and because, in general, they offer a reasonable trade-off between efficiency, accuracy and privacy. Moreover, some of the ideas used in these schemes arose in more mature fields like e-commerce.

In the simplest communication scheme described above, users send their location information and queries directly to the LBS provider. In this scheme, whatever location privacy LBS users can get depends on the honest behaviour of the LBS provider.

In the following sections we concentrate on some TTP-based schemes that aim to protect the location privacy of the users.

4.1.1 Policy-based schemes

Policy-based schemes are one step forward in LBS privacy with respect to the simple scheme. Although the conceptual framework is the same (i.e. a user submits queries to a provider), in this case, providers adhere to a set of privacy policies known by users. Hence, if providers do not properly follow their privacy policies, users have the right to ask for a compensation and/or take legal action against providers.

Privacy policies are legal notices that contain statements defining what service providers can do with their users' personal data. Privacy policies are published by service providers, and users decide whether such policies are acceptable

to them. These policies refer to many concepts and specific languages are used to define them [31, 8]. Users reach an agreement with providers about which data are collected, what are these data used for and how they can be distributed to third parties. In this kind of schemes, privacy is understood as the ability of individuals to decide when, what, and how information about them is disclosed to others. Ideally, users can choose amongst a variety of policies. So, depending on the selected policy, users can save some money but, in return, providers can distribute/sell some of their data.

These schemes are widely used on the Internet by e.g. e-commerce sites which define their privacy policies in e.g. P3P (Platform for Privacy Preferences) [38]. They have been used for automotive telematics [14], and the Geopriv (Geographic Location/Privacy) Charter of the IETF proposes their use for LBS also [28]. A recent study on the use of policies and access control techniques can be found in [5].

4.1.2 Pseudonym-based schemes

Using pseudonyms is an alternative that aims at hiding the real identity of the users from the provider. This task is performed by intermediate entities called Pseudonymisers. Pseudonymisers are the simplest intermediate entity between LBS users and providers. They receive queries from users and, prior to forwarding them to LBS providers, they replace the real IDs of the users by fake ones (i.e. pseudonyms). In this way, the real user IDs remain hidden to the provider, but pseudonymisers must store the real IDs and their corresponding pseudonyms in order to forward the answers from the providers to the users. Clearly, users must completely trust pseudonymisers, because the latter see all the location information on the former.

The main problem of this technique is that an attacker (e.g. the LBS provider herself) can infer the real identity of the user by linking the user location with e.g. a public telephone directory (e.g. by using the aforementioned RSI or OI attacks [18]).

4.1.3 k-Anonymity-based schemes

An evolution of the previous scheme is founded on the k-Anonymity property and the entities responsible for performing such a task are called Anonymisers. Anonymisers are the most sophisticated option in TTP-based location privacy. Instead of taking care of policies or users' identifiers, anonymisers assume that communications are anonymous, i.e. LBS providers do not require an ID to answer queries[2]. Anonymisers aim to hide users true identity with respect to emitted location information. In this section we concentrate on techniques that hide the location information of users and we assume that identifier abstraction is already guaranteed.

[2]If this assumption was not made, it would be easy to track a given LBS user by simply checking the ID or the pseudonym (like in the case of pseudonymisers).

A very common way to hide the real location of the users from the LBS provider is by using the k-anonymity property. k-Anonymity is an interesting approach to face the conflict between information loss and disclosure risk, suggested by Samarati and Sweeney [26, 27, 34, 35]. Although it was designed for application in databases by the Statistical Disclosure Control (SDC) community, k-anonymity has been adapted to LBS privacy. In this context, we say that the location of a user is k-anonymous if it is indistinguishable from the location of another $k-1$ users. So, the fundamental idea behind k-anonymisers is to replace the real location of the user by cloaking areas in which at least k users are located. Anonymisers transform locations (x, y) at time t to $([x1, x2], [y1, y2], [t1, t2])$ where $([x1, x2], [y1, y2])$ is the rectangular area containing (x, y) between times $t1$ and $t2$ such that $t \in [t1, t2]$. By doing so, LBS providers cannot easily determine which of the k users in the cloaking area is really submitting the query.

Many examples of this kind of approach and other similar ones based on cloaking can be found in the literature [18, 15, 6]. One of the most recent advances in anonymisers is proposed in [16], where an extension of a previous anonymiser version [15] is proposed. The proposed anonymiser allows a user to define his personal privacy requirements, i.e. the number k of users amongst which he wants to be anonymised, and the maximum delay and location perturbation he is willing to accept. The proposal is resilient against identification attacks such as RSI and OI. However, it has some important drawbacks which, as we explain in the next section, can be avoided by TTP-free approaches: (i) the architecture relies on a TTP, so that the user must completely trust the platform mediating between him and the LBS provider; (ii) it is assumed that LBS providers are not malicious but semi-honest, which might turn out to be too much of an idealisation; and (iii) the architecture is centralised, which makes it vulnerable to Denial of Service (DoS) attacks.

In [4] a similar method called PrivacyGrid is described. Although the anonymiser described in [16] and the PrivacyGrid approach are very similar, the latter seems to be more efficient due to the cloaking techniques based on grids (i.e. bottom-up, top-down and hybrid) that it uses. Moreover PrivacyGrid adds the l-diversity property to the already considered k-anonymity one. By doing so, the privacy of LBS users is improved. Although PrivacyGrid seems to improve the proposal in [16], it mainly suffers from the same shortcomings.

Current research on anonymisers focuses on improving the efficiency of the intermediaries and designing highly personalised services able to guarantee the privacy of the users.

4.2 Privacy in TTP-free schemes

Due to the shortcomings of the TTP-based schemes, other methods that do not rely on TTPs have been proposed. First, we consider the collaboration methods that aim to obtain the same results (e.g. k-anonymity, l-diversity, efficiency) than the ones based on TTP. Then, we pay attention to the methods based on the obfuscation of the real location without collaboration. Finally we point out

a new location privacy trend based on Private Information Retrieval (PIR).

4.2.1 Collaboration-based methods

In [9], the first collaborative TTP-free algorithm for location privacy in LBS is proposed. The user perturbs his location by adding zero-mean Gaussian noise to it. Then the user broadcasts his perturbed location and requests neighbours to return perturbed versions of their locations. Amongst the replies received, the user selects $k-1$ neighbours such that the group formed by the locations of these neighbours and his own perturbed location spans an area A satisfying $A_{min} < A < A_{max}$, where A_{min} is a privacy parameter (the minimum required area for cloaking) and A_{max} is an accuracy parameter (the maximum area acceptable for cloaking). Finally, the user sends to the LBS the centroid of the group of k perturbed locations including his own. Since users only exchange perturbed locations, they do not need to trust each other for privacy. On the other hand, perturbations tend to cancel out each other in the centroid, so accuracy does not degrade[3]. This method does not achieve k-anonymity because the centroid is only used by a single user to identify himself. In addition, due to the noise cancellation, users cannot use this method several times without changing their location. In [7], a similar peer-to-peer scheme for location privacy is presented. Its main idea is to generate cloaking areas as in [9]: users must find other users in their cover range and share their location information. Once this information is known, users can send their queries to LBS providers using the cloaking area instead of their real locations. The main shortcoming of this proposal is that users must trust other users because they exchange their real locations. Thus, a malicious user can easily obtain and publish the location of other users. Although we classify this technique as a TTP-free technique, it can also be understood as a distributed TTP-based scheme, where each user is a TTP.

In [32], the authors propose a method based on Gaussian noise addition to compute a fake location that is shared by k users (unlike in [9]). Thus, all k users use the same fake location and the LBS provider is unable to distinguish one user from the rest, so that their location becomes k-anonymous. This method was extended to support non-centralised communications in [33] (See Figure 8 for an illustration of centralised vs. non-centralised collaboration schemes). The proposal is based on a stack of modules that progressively increase the privacy achieved by users. The basic module is equivalent to the method described in [7] where users have to trust each other because they share their location. Once they know the locations of other users, they can compute a centroid that they use as their fake location. In order to allow users to exchange their location without trusting other peers, a second module that perturbs the location is added. This module adds Gaussian noise with zero mean to the real location of users. As explained above, the centroid of locations perturbed with zero-mean Gaussian noise is quite similar to the centroid of unperturbed locations. However, if this procedure is repeated several times with static users (i.e. users

[3]The average of k zero-mean perturbations with variance σ^2 has zero mean and variance σ^2/k.

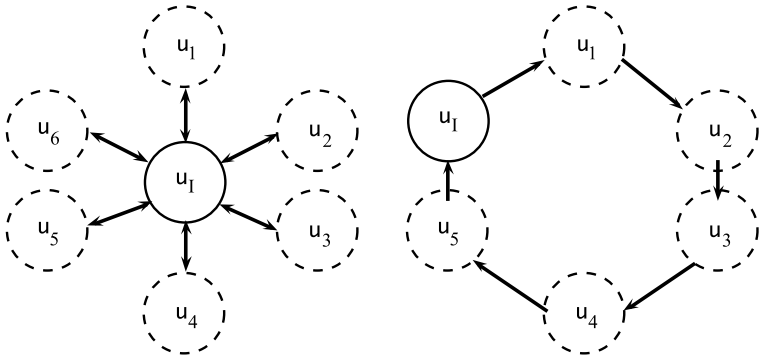


Figure 8: Illustration of the centralised TTP-Free collaboration (left) and non-centralised one (right)

that do not change their location substantially), their real location could be deduced because of the noise cancellation (this is the main problem of [9]). To prevent this, the protocol uses privacy homomorphisms [22] to guarantee that users cannot see the real locations of other users whilst still being able to compute the centroid. Finally, a module that distributes users in a chain is added to avoid denial of service attacks to the central user. At the end of the protocol users become k-anonymous and their location privacy is secured. However, the main problem of this proposal is that it cannot provide a lower bound of the location error.

4.2.2 Obfuscation-based methods

Obfuscation is a TTP-free alternative to collaboration-based methods. Obfuscation can be understood as the process of degrading the quality of information about a user's location, with the aim to protect that user's privacy [12]. Some methods like the ones described in previous sections (e.g. cloaking methods) can be understood as special kinds of obfuscation because they basically modify the location information in several ways to improve user's privacy. However, we classify them in different categories because they need TTPs and/or achieve other properties such as k-anonymity or l-diversity.

In [11] an obfuscation method based on imprecision is presented. The space is modelled as a graph where vertices are locations and edges indicate adjacency. Hence, in order to obtain an imprecise location, the user sends a set of vertices instead of the single vertex in which he is located. The LBS provider cannot distinguish which of the vertices is the real one. The article proposes negotiation algorithms that allow users to increase the QoS whilst maintaining their privacy. The main problem of this technique is that users and providers must share the graph modelling the space (cf. [13] for a comprehensive approach to imprecision in location systems). Some other recently proposed obfuscation methods can be found in [2], where the real location of LBS users is replaced by circular areas

of variable centre and radius.

SpaceTwist [39] is the most recent proposal for non-collaborative TTP-free location privacy. SpaceTwist generates an anchor (i.e. a fake point) that is used to retrieve information on the k nearest points of interest from the LBS provider. After successive queries to the LBS provider, SpaceTwist is able to determine the closest interest point to the real location whilst the LBS provider cannot derive the real location of the user. The main advantages of this method are: (i) no TTP and no collaboration are needed; (ii) the closest interest point is always found; (iii) the location of the user is hidden in a controlled area. However, due to the lack of collaboration, this method is not able to achieve the k-anonymity and/or the l-diversity properties.

4.2.3 PIR-based methods

A totally different approach to TTP-free LBS privacy is proposed in [17]. In that article, Private Information Retrieval (PIR) is used to provide LBS users with location privacy. Although the idea of using PIR techniques is promising, the proposed approach requires the LBS provider to co-operate with users by following the PIR protocol; this prevents the use of this method in real environments, where LBS providers simply answer queries containing a location or an area without any regard for location privacy. However, if this shortcoming was solved and without significant computation and efficiency penalties, using collaborative PIR amongst peers (i.e. users) could be a really promising future research line.

5 Conclusions

In this report we have emphasised the privacy problems related to the use of location-based services. After contextualising the privacy problems and the research scenario, we have proposed two different classifications of the existing LPP methods. By using the TTP-based vs TTP-free classification we have summarised the major LPP methods and we have pointed out some of their main pros and cons.

There is a clear distinction between TTP-based schemes and the TTP-free ones. Although TTP-based schemes are the most common ones, TTP-free schemes seem superior in terms of privacy due to the following shortcomings of intermediate TTPs: (i) TTPs are critical points which can be attacked; (ii) TTPs are bottlenecks; (iii) There must be many users subscribed to a TTP for the latter to be able to compute suitable cloaking regions (offering sufficient privacy and accuracy).

Despite being inferior regarding privacy, TTP-based schemes are easier to implement than collaborative-based methods because all the infrastructure required by users to circumvent the use of a TTP is not necessary. However, obfuscation-based methods are also easy to implement. We believe that there is room in the market for both approaches.

In our opinion, there are a lot of opportunities for synergy between PIR and TTP-free LBS privacy. Indeed, current PIR techniques face the (very serious) limitation of needing co-operation from the database server in following the PIR protocol. If practical PIR protocols are developed which do not need such a co-operation, it will be possible to use them for TTP-free location privacy.

Other relevant research lines that can be studied in the future are:

- Location privacy for people with cognitive disabilities that have to be monitored under some circumstances.
- Location privacy and its relation to more mature fields such as mixnets.

6 List of contributions

6.1 Articles in ISI JCR journals and LNCS

1. Q. Wu, J. Domingo-Ferrer and Ú.González Nicolás. Balanced trustworthiness, safety and privacy in vehicle-to-vehicle communications. *IEEE Transactions on Vehicular Technology.* **(to appear)**

2. V. Daza, J. Domingo-Ferrer, F. Sebé and A. Viejo. Trustworthy privacy-preserving car-generated announcements in vehicular ad hoc networks. *IEEE Transactions on Vehicular Technology*, 58(4): 1876 – 1886, 2009. ISSN: 0018-9545.

3. J. Domingo-Ferrer and Q. Wu. Safety and privacy in vehicular communications *Lecture Notes in Computer Science*, Privacy in Location Based Applications, LNCS 5599,Springer, pp. 173-189, 2009.

4. A. Solanas and A. Martínez-Ballesté. A TTP-Free Protocol for Location Privacy in Location-Based Services. *Computer Communications*, 31(6):1181 – 1191, 2008. Elsevier. ISSN: 0140-3664.

5. A. Solanas and A. Martínez-Ballesté. Privacy protection in location-based services through a public-key privacy homomorphism. *Lecture Notes in Computer Science*, 4th European PKI Workshop, EuroPKI07(4582):362 – 368, June 2007. Springer-Verlag Berlin. ISSN: 0302-9743.

6.2 Articles in non-ISI JCR journals

1. A.Solanas. Critical review of the paper: Cho E., Moon C., Im H., Baik D. "An anonymous communication model for privacy-enhanced location based service using an echo agent', CR136891, In *Computing reviews, June 2009.* ACM. ISSN: 1530-6585.

2. A.Solanas. Critical review of the book: Ning P., Du W. "Security of ad-hoc and sensor networks: book edition of Journal of Computer Security", CR136853, In *Computing reviews, May 2009.* ACM. ISSN: 1530-6585.

3. A.Solanas. Critical review of the book: Traynor P., McDaniel P., Porta T., "Security for telecommunications networks (1st ed.)", CR136416, In *Computing reviews, January 2009.* ACM. ISSN: 1530-6585.

4. A.Solanas. Critical review of the paper: Dunne C., Candebat T., Gray D. "A frequency based sighting blurring algorithm for use with location based services on the internet", CR136246, In *Computing reviews, November 2008.* ACM. ISSN: 1530-6585.

6.3 Articles in proceedings with ISBN

1. Pablo A. Pérez-Martínes and A. Solanas. Location Privacy Through Users' Collaboration: A Distributed Pseudonymizer. In *Proceedings of the Third International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies. UBICOMM 2009*, pages —-. Sliema, Malta, 11 - 16 October, 2009. **(to appear)**

2. D. Rebollo-Monedero, J. Forn and M. Soriano. Private Location-Based Information Retrieval via k-Anonymous Clustering. In *Proceedings of CNIT Tyrrhenian International Workshop on Digital Communications* pages —-. Pula, Italy, 2 - 4 September, 2009. **(to appear)**

3. D. Rebollo-Monedero, J. Forn, L. Subirats, A. Solanas and A. Martínez-Ballesté. A collaborative protocol for private retrieval of location-based information. In *Proceedings of the IADIS International Conference e-Society*. Barcelona, Spain, 25 - 28 February, 2009.

4. A. Solanas, J. Domingo-Ferrer and A. Martínez-Ballesté. Location Privacy in Location-Based Services: Beyond TTP-based Schemes In *Proceedings of the 1st International Workshop on Privacy in Location-Based Applications (PILBA)*, pages 12–23. ISSN: 1613-0073. Mlaga, Spain, October 9, 2008. `http://sunsite.informatik.rwth-aachen.de/Publications/CEUR-WS/Vol-397/`

5. M. Gheorghitas, A. Solanas and J. Forné. Location Privacy in Chain-Based Protocols for Location-Based Services. In *The Third International Conference on Digital Telecommunications*, pages 64 – 69, Bucarest, Romania, June 29 - July 5, 2008.

6. J. Domingo-Ferrer Location privacy via unlinkability: an alternative to cloaking and perturbation. In *PAIS '08: Proceedings of the 2008 international workshop on Privacy and anonymity in information society*, pages 1 – 2 Nantes, France, March 29, 2008.

References

[1] 108th Congress. H.R. 71: The wireless privacy protection act. In *United States House of Representatives*, 2003-4. `http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_bills&docid=f:h71ih.txt.pdf`.

[2] C. A. Ardagna, M. Cremonini, E. Damiani, S. De Capitani di Vimercati, and P. Samarati. Location privacy protection through obfuscation-based techniques. In S. Baker and G.J. Ahn, editors, *Data and Applications Security*, volume 4602 of *LNCS*, pages 47 – 60. IFIP, 2007.

[3] Vijayalakshmi Atluri and Heechang Shin. Efficient security policy enforcement in a location based service environment. In S. Baker and G.J. Ahn, editors, *Data and Applications Security*, volume 4602 of *LNCS*, pages 61–76. IFIP, Springer Berlin / Heidelberg, 2007.

[4] Bhuvan Bamba, Ling Liu, Peter Pesti, and Ting Wang. Supporting anonymous location queries in mobile environments with privacygrid. In *International World Wide Web Conference WWW*, pages 237–246, 2008.

[5] Lujo Bauer, Lorrie Faith Cranor, Robert W. Reeder, Michael K. Reiter, and Kami Vaniea. A user study of policy creation in a flexible access-control system. In Mary Czerwinski, Arnold M. Lund, and Desney S. Tan, editors, *Proceedings of the 2008 Conference on Human Factors in Computing Systems*, pages 543–552. ACM, 2008.

[6] R. Cheng, Y. Zhang, E. Bertino, and S. Prabhakar. Preserving user location privacy in mobile data management infrastructures. In *6th Workshop on Privacy Enhancing Technologies (PET)*, volume 4258 of *Lecture Notes in Computer Science*, pages 393 – 412. Springer Berlin / Heidelberg, 2006.

[7] ChiYin Chow, Mohamed F. Mokbel, and Xuan Liu. A peer-to-peer spatial cloaking algorithm for anonymous location-based services. In *GIS '06: Proceedings of the 14th annual ACM international symposium on Advances in geographic information systems*, pages 171–178, Arlington, Virginia, USA, November 2006. ACM.

[8] Lorrie Faith Cranor. P3P: Making privacy policies more useful. *IEEE Security & Privacy*, 1(6):50–55, 2003.

[9] Josep Domingo-Ferrer. Microaggregation for database and location privacy. In Opher Etzion, Tsvi Kuflik, and Amihai Motro, editors, *Next Generation Information Technologies and Systems-NGITS*, volume 4032 of *LNCS*, pages 106–116. Springer Berlin / Heidelberg, 2006.

[10] Christopher Drane, Malcolm Macnaughtan, and Craig Scott. Positioning GSM telephones. *IEEE Communications Magazine*, 36(4):46 – 54 , 59, April 1998.

[11] Matt Duckham and Lars Kulit. A formal model of obfuscation and negotiation for location privacy. In *Pervasive Computing*, volume 3468 of *LNCS*, pages 152–170. Springer Berlin / Heidelberg, 2005.

[12] Matt Duckham and Lars Kulit. *Dynamic and Mobile GIS: Investigating Changes in Space and Time*, chapter Location Privacy and Location-Aware Computing, pages 35–52. Number 3. CRC Press, 2007.

[13] Matt Duckham, K. Mason, J. Stell, and M. Worboys. A formal approach to imperfection in geographic information. *Computers, Environment and Urban Systems*, 25(1):89–103, 2001.

[14] Sastry Duri, Marco Gruteser, Xuan Liu, Paul Moskowitz, Ronald Perez, Moninder Singh, and Jung-Mu Tang. Framework for security and privacy in automotive telematics. In *Proceedings of the 2nd international workshop on Mobile commerce*, pages 25 – 32. ACM Press New York, NY, USA, 2002.

[15] Bugra Gedik and Ling Liu. A customizable k-anonymity model for protecting location privacy. In *Proceedings of the IEEE International conference on Distributed Computing Systems (ICDS'05)*, pages 620 – 629, 2005.

[16] Bugra Gedik and Ling Liu. Protecting location privacy with personalized k-anonymity: Architecture and algorithms. *IEEE Transactions on Mobile Computing*, 7(1):1 – 18, January 2008.

[17] Gabriel Ghinita, Panos Kalnis, Ali Khoshgozaran, Cyrus Shahabi, and KianLee Tan. Private queries in location based services: Anonymizers are not necessary. In *SIGMOD '08: Proceedings of the 2008 ACM SIGMOD international conference on Management of data*, pages 121 – 132. Vancouver, BC, Canada, ACM, June 2008.

[18] Marco Gruteser and Dirk Grunwald. Anonymous usage of location-based services through spatial and temporal cloaking. In *Proceesings of MobiSys 2003: The First International Conference on Mobile Systems, Applications, and Services.*, pages 31 – 42, San Francisco, CA, USA, May 2003. USENIX Association, ACM, Sigmobile, ACM.

[19] Baik Hoh and Marco Gruteser. Protecting location privacy through path confusion. In *Proceedings of the First International Conceference on Security and Privacy for Emerging Areas in Communications Networks*, pages 194–205, 2005.

[20] Paul A. Karger and Yair Frankel. Security and privacy threats to ITS. In *The Second World Congress on Intelligent Transport Systems*, volume 5, pages 2452 – 2458, Yokohama, Japan., November 1995.

[21] Bernhard Kölmel and Spiros Alexakis. Location based advertising. In *The First International Conference on Mobile Business*, Athens, Greece, 2002.

[22] T. Okamoto and S. Uchiyama. A new public-key cryptosystem as secure as factoring. In *Advances in Cryptology EUROCRYPT'98*, volume 1403 of *Lecture Notes in Computer Science*, page 308. Springer Berlin / Heidelberg, 1998.

[23] Linda Pareschi, Daniele Riboni, and Claudio Bettini. Protecting users' anonymity in pervasive computing environments. In *Sixth Annual IEEE International Conference on Pervasive Computing and Communication (PERCOM'08)*, pages 11–19. IEEE Computer Society, 2008.

[24] Jeffrey H. Reed, Kevin J. Krizman, Brian D. Woerner, and Theodore S. Rappaport. An overview of the challenges and progress in meeting the E-911 requirement for location privacy. *IEEE Communications Magazine*, 36(4):30 – 37, April 1998.

[25] Peter Ruppel, Georg Treu, Axel Küpper, and Claudia Linnhoff-Popien. Anonymous user tracking for location-based community services. In M. Hazas, J. Krumm, and T. Strang, editors, *Second International Workshop on Location- and Context-Awareness*, volume 3987 of *LNCS*, pages 116 – 133. Springer Berlin / Heidelberg, 2006.

[26] P. Samarati. Protecting respondents' identities in microdata release. *IEEE Transactions on Knowledge and Data Engineering*, 13(6):1010–1027, 2001.

[27] P. Samarati and L. Sweeney. Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression. Technical report, SRI International, 1998.

[28] H. Schulzrinne, H. Tschofenig, J. Morris, J. Cuellar, and J. Polk. Geolocation policy. Technical report, Internet Engineering Task Force, June 2008. `http://www.ietf.org/internet-drafts/draft-ietf-geopriv-policy-17.txt`.

[29] Heechang Shin, Vijayalakshmi Atluri, and Jaideep Vaidya. A profile anonymization model for privacy in a personalized location based service environment. In *9th International Conference on Mobile Data Management. MDM'08*, pages 73–80, 2008.

[30] Todd Simcock, Stephen Peter Hillenbrand, and Bruce H. Thomas. Developing a location based tourist guide application. In Chris Johnson, Paul Montague, and Chris Steketee, editors, *ACSW Frontiers '03: Proceedings of the Australasian information security workshop conference on ACSW frontiers 2003*, volume 21 of *CRPIT*, pages 177–183, Darlinghurst, Australia, February 2003. Australian Computer Society, Inc.

[31] Einar Snekkenes. Concepts for personal location privacy policies. In *ACM Conference on Electronic Commerce*, pages 48–57, 2001.

[32] A. Solanas and A. Martínez-Ballesté. Privacy protection in location-based services through a public-key privacy homomorphism. In *Fourth European PKI Workshop: theory and practice*, Lecture Notes in Computer Science, pages 362 – 368. Springer Berlin / Heidelberg, 2007. Palma de Mallorca, Spain.

[33] Agusti Solanas and Antoni Martínez-Ballesté. A TTP-free protocol for location privacy in location-based services. *Computer Communications*, 31(6):1181–1191, April 2008.

[34] L. Sweeney. Achieving k-anonymity privacy protection using generalization and suppression. *International Journal of Uncertainty, Fuzziness and Knowledge Based Systems*, 10(5):571–588, 2002.

[35] L. Sweeney. k-anonimity: A model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge Based Systems*, 10(5):557–570, 2002.

[36] Manolis Terrovitis and Nikos Mamoulis. Privacy preservation in the publication of trajectories. In *9th International Conference on Mobile Data Management. MDM'08*, pages 65–72, 2008.

[37] The European Parliament and the Council. Directive 2002/58/EC on privacy and electronic communications. *Official Journal of the European Communities*, 201:37 – 47, July 2002.

[38] W3C. Platform for privacy preferences (P3P) project. Webpage, October 2007. `http://www.w3.org/P3P/`.

[39] Man Lung Yiu, Christian S. Jensen, Xuegang Huang, and Hua Lu. Spacetwist: Managing the trade-offs among location privacy, query performance, and query accuracy in mobile services. In *IEEE 24th International Conference on Data Engineering ICDE'08*, pages 366–375, 2008.

[40] KyongSoo Yoo, Dongjoo Park, and ByeongYong Rhee. Development of a location-based dynamic route guidance system of korea highway corporation. In Keiichi Satoh, editor, *Proceedings of the Eastern Asia Society for Transportation Studies*, volume 5, pages 1449 – 1463, Bangkok, 2005. Eastern Asia Society for Transportation Studies.

A Appendix: CONSOLIDER Team Publications on Location Privacy