Personal and Ubiquitous Computing manuscript No.
(will be inserted by the editor)

A Classification of Location Privacy Attacks and Approaches

Marius Wernke · Pavel Skvortsov · Frank Dürr · Kurt Rothermel

Received: date / Accepted: date

Abstract In recent years, location-based services have become very popular, mainly driven by the availability of modern mobile devices with integrated position sensors. Prominent examples are points of interest finders or geo-social networks such as Facebook Places, Qype, and Loopt. However, providing such services with private user positions may raise serious privacy concerns if these positions are not protected adequately. Therefore, location privacy concepts become mandatory to ensure the user's acceptance of location-based services.

Many different concepts and approaches for the protection of location privacy have been described in the literature. These approaches differ with respect to the protected information and their effectiveness against different attacks. The goal of this paper is to assess the applicability and effectiveness of location privacy approaches systematically. We first identify different protection goals, namely, personal information (user identity), spatial information (user position), and temporal information (identity/position + time). Secondly, we give an overview of basic principles and existing approaches to protect these privacy goals. In a third step, we classify possible attacks. Finally, we analyze existing approaches with respect to their protection goals and their ability to resist the introduced attacks.

Keywords location-based services · location privacy · protection goals · principles · adversary · attacks · classification · approaches

1 Introduction

Location-based services (LBS) currently attract millions of mobile users. Common examples include points of interest (POI) finders such as Qype [1], which

Institute of Parallel and Distributed Systems, Universität Stuttgart
Tel.: +49 711 685 88230
Fax: +49 711 685 88424
E-mail: {marius.wernke,pavel.skvorzov,frank.duerr,kurt.rothermel}@ipvs.uni-stuttgart.de

help the user to find the next POI such as bars or cinemas, and enrich the provided information, for instance, with special offers or vouchers. Other prominent examples are friend finder services such as Loopt [2], which determine all friends in the vicinity of a user, or geo-social networks such as Facebook Places [3] or Foursquare [4], where users "check-in" to bars, restaurants, etc. to share their current position with friends. Besides check-ins at individual locations, more and more users also share their complete movement trajectory, for instance, showing their last hiking trail or jogging path. Moreover, advanced navigation systems provide complete trajectory information to service providers in real-time to calculate real-time traffic information from the gathered positions.

Although these services are very popular, their usage can also raise severe privacy concerns as shown in [5, 6, 7]. For example, revealing precise user positions may allow an adversary to infer sensitive information if a user visits, for instance, a hospital or a night club. Furthermore, the revealed user data could be misused for stalking, mugging, or to determine empty homes for a burglary. Therefore, mechanisms for protecting location privacy are mandatory when using LBSs. Available location privacy approaches differ with respect to the protected information and the considered attacker model. For instance, a wide-spread approach to protect user positions is *location obfuscation* [8], which deliberately decreases the precision of a position such that attackers can only retrieve coarse-grained position information. Using this approach, a realistic attacker model has to consider the fact that an attacker is aware of a map and therefore can use map matching to increase the precision of the known position by excluding, for example, non-reachable areas from the obfuscated area. However, map matching is often not considered by existing approaches, although it poses a serious threat to location privacy.

Other examples with different privacy goals are approaches implementing the concept of *k-anonymity* [9] to protect the user identity. In general, these approaches try to find a set of k users that are indistinguishable from each other such that an attacker cannot identify a single user out of the set. These approaches are usually based on a trusted third party (TTP) component for anonymization. However, it is questionable whether the assumption of a TTP is realistic. As shown in [6], the number of reported incidents and successful attacks on different providers where private user information was leaked, lost, or stolen, is rapidly increasing. Consequently, such approaches are insecure if providers cannot be considered to be trustworthy.

In order to systematically assess the effectiveness of the different approaches protecting location privacy, we first need to know which information the user actually wants to protect, i.e., his privacy goal. Second, we need to know what kind of information is available to an attacker, in order to analyze how an attacker could use this information to infer private user information w.r.t. the defined protection goal. Although different classifications of location privacy approaches exist, they fall short of comparing the effectiveness of different approaches under different attacker models. In [10], Solanas et al. classify approaches based on the distinction between methods relying on a TTP and

TTP-free approaches. However, they do not consider different attacker models in their classification as presented in our work. This is also the case for the taxonomy of location privacy approaches presented by Barker et al. [11] and the taxonomy presented by Khoshgozaran and Shahabi in [12]. Location privacy surveys considering different attacks are presented by Bettini et al. [13] and Krumm [14]. Both provide good classifications of attacks, which are however not comprehensive (e.g., they do not include map matching) and they do not provide an analysis to show which of the presented approaches are vulnerable to which attacks.

Therefore, the main contribution of this paper is a classification of existing location privacy approaches that takes the attacker knowledge and attacker methods into account. We present an overview of different protection goals and fundamental location privacy approaches, as well as a classification of different types of attacks according to the applied attacker knowledge. Finally, we compare existing approaches based on the identified protection goals and attacks.

The rest of the paper is structured as follows: First, we present our system model in Section 2. In Section 3, we identify different protection goals from the user's point of view. In Section 4, we give an overview of existing location privacy approaches. Then, we introduce our classification of location privacy attacks in Section 5. In Section 6, we present our classification of existing location privacy approaches. Finally, we conclude our work with a summary in Section 7.

2 System Model

Before discussing the details of protecting private position information, we introduce a common system model that matches most approaches described in the literature (cf. Figure 1). This model consists of three components, namely, *mobile user devices*, *location servers*, and *clients*.

The mobile device of a user is equipped with an integrated position sensor to determine the current user position. This device is assumed to be trusted, and it is guaranteed that no malicious software component is running on the mobile device that has access to the position sensor. This can be assured by using a mobile trusted computing approach such as [15]. Otherwise, the location privacy approaches considered in the following are not effective since the malicious software component could transmit the precise user position to an adversary.

Mobile devices send their position information to a location server (LS), which stores and manages mobile device positions on behalf of the user. The LS can either be non-trusted (cf. Figure 1a) or trusted (cf. Figure 1b). In case of a trusted LS, the LS can perform trusted computations and act, for example, as anonymizer. For instance, a trusted LS can use an internal anonymizer to implement the concept of k-anonymity (cf. Section 4.3) by using the positions of several users stored by the LS to make the user indistinguishable from $k-1$

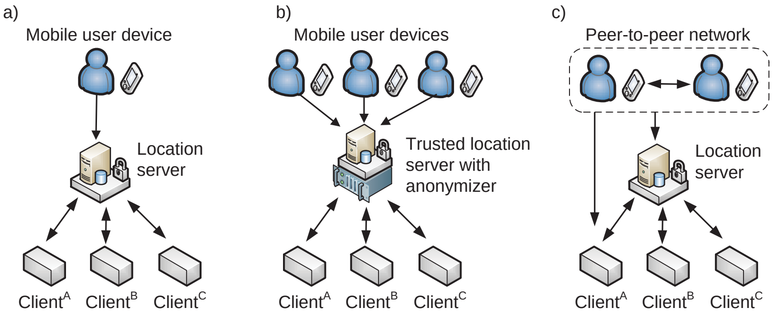

Fig. 1 System model without a TTP (a), with a trusted LS using an internal anonymizer (b), and based on a peer-to-peer network.

other users. Furthermore, the anonymizer can calculate obfuscated positions covering several users.

Clients query the LS for user positions in order to implement a certain location-based service. The LS grants clients access to the stored positions based on an access control mechanism. In practice, clients and LSs can also be integrated. However, in our description we explicitly distinguish both components.

LSs and clients can both be compromised, even if these entities are assumed to be trusted. For location privacy approaches relying on a TTP this means that a successful attack undermines the privacy approach. Therefore, we explicitly consider this kind of attack in our attack classification in Section 5. If an LS is successfully compromised by an attacker, then the attacker is aware of all the information that users provided to the LS. On the contrary, a compromised client does not necessarily have access to all the information stored at the LS but only a portion of it depending on its access rights.

Besides this pure infrastructure-based client/server model, some approaches described in the literature are combining or replacing the client/server model with peer-to-peer concepts (cf. Figure 1c). Instead of letting each user send its position directly to an LS, users are organized in a decentralized peer-to-peer network which provides user positions either to an LS or directly to clients. We also consider these peer-to-peer approaches in our location privacy classification.

3 Protection Goals

Before we discuss different approaches to protect location privacy, we have to define the different protection goals which are considered by these approaches. The attributes to be protected are the user identity, his spatial information (his position), and temporal information (time). The information provided by a user can be defined as a tuple $\langle identity, position, time \rangle$. The protection goal of the user defines which attributes of the information must be protected and which can be revealed. Next, we present some examples of different protection goals and application scenarios, before we consider the protection of the stated attributes in more detail.

3.1 Examples of Protection Goals

As an application scenario consider a user of an advanced navigation system providing real-time traffic information and points of interest information based on the current user position. Assume that the user is willing to provide anonymized position information to the navigation service provider. To this end, he protects the identity attribute using an anonymization concept. However, as shown in [16], the user's identity can also be revealed from the position information, for instance, based on the periodically visited home and work locations. Therefore, also the position attribute has to be protected.

In a second scenario, assume that the user is willing to share his non-anonymous track. However, he does not want to reveal that he is speeding on the motorway since revealing such information may have negative impact on the user if the service provider misuses the data and provides it to the police, his insurance company, etc. In this scenario, the position and time attributes have to be protected to prevent the calculation of the maximum speed.

In order to show that the protection of each attribute combination is relevant, we list further scenarios for each combination in Table 1. To achieve the different protection goals, different location privacy approaches are required. As we will see later, no location privacy approach is suited to protect all stated protection goals at the same time. Next, we consider the protection of each attribute in more detail.

3.2 User Identity

One possible goal to ensure privacy is to hide the user's identity while the position of the anonymous mobile object is visible to clients. The identity of a user can be her name, a unique identifier, or any set of properties uniquely identifying the user. If a user publishes position information without personal information, an attacker can still try to derive the user's identity by analyzing the position information and additional context data such as the visited objects. In general, quasi-identifiers can be used to identify the user as shown in [17].

3.3 Spatial Information

Another protection goal is to provide position information of a user only with a given precision to clients. For instance, a user might want to provide precise

Table 1 Protection goal examples for protected and non-protected attributes. A "✓" states that the corresponding attribute must be protected, while a "✕" states that the attribute can be revealed.

Attributes			
ID	Pos.	Time	Example
✓	✓	✓	– Protect the information where a user lives and make it impossible to infer it from several traces
✓	✓	✕	– Protect that the user drove through a residents-only street – Protect the precise user position in a building and the user identity, while showing to the security manager that someone is still in the building such that the building cannot be locked
✓	✕	✓	– Provide traces to openstreetmap.com to model new streets without revealing the user's identity or speed – Give feedback for a restaurant without revealing the user's identity
✓	✕	✕	– Protect the user's identity when publishing jogging paths – Use an advanced navigation system for real-time congestion prediction
✕	✓	✓	– Protect a slight detour on a longer trip while the general trip should be visible – Protect the maximum velocity on a longer trip while keeping the average velocity accurate
✕	✓	✕	– Do not show that a user visits a bar while keeping friends informed of being in the inner city – Hide the fact that the user was within a hospital – Protect where the user is working
✕	✕	✓	– Share the last hiking trail with friends without revealing to be currently not at home
✕	✕	✕	– Provide precise information to a high quality friend alert service without privacy limitations – Query a points of interest service with the precise user position

position information to his friends, whereas only coarse positions with city-level granularity are provided to a location-based news feed service. In general, this goal is known as position obfuscation or cloaking [8].

We also have to consider that a user position usually carries more information than only geometric information like longitude and latitude values. Often the *semantic* of a location is defining the criticality of position information. For instance, a user might have no problem to share a precise position as long as he does not enter certain semantic locations such as a hospital, since this could be used to derive further private information like the health status of the user. Therefore, a specific goal of protecting spatial information is the protection of semantic location information. In general, this is achieved by ensuring that a position is associated with several alternative locations of different semantics. For instance, a semantic position might be protected if the user could be within a hospital *or* within one or more locations that are no hospitals [18].

3.4 Temporal Information

Temporal information defines the point in time or time period when the spatial information of the user is valid. In some scenarios, spatial information is only considered critical if it is associated with temporal information. For instance, a user might be willing to share with others where he is traveling, whereas, he does not want to reveal that he is speeding. This means that real-time updates cannot be used in this case without raising privacy concerns, whereas temporally delayed updates could be used to reach the protection goal. In such scenarios, it must be considered that even if temporal information is not explicitly stated—e.g., as a timestamp of the position update—, it can be implicitly derived. For instance, this is possible by knowing the time when the information was received by the LS and by knowing the location update algorithm that triggered the update. In general, the user might want to control the temporal resolution of his position or complete movement trajectory.

4 Privacy Approaches

After introducing possible privacy goals in the previous section, we now give an overview of existing location privacy approaches to reach these goals. There are a number of works representing the state of the art techniques to protect location privacy [14], [10], [19], [20]. Therefore, the goal of this section is to provide an overview of the fundamental principles of these approaches rather than to give a comprehensive overview of all existing approaches. We distinguish the following principles: position dummies, mix zones, k-anonymity, spatial obfuscation, coordinate transformation, encryption, and position sharing.

4.1 Position Dummies

The goal of **position dummies** is to secure a user's true position by sending multiple false positions ("dummies") to the LS together with the true position [21]. An essential advantage of this approach is that the user herself can generate dummies without any need for other TTP components. However, it is challenging to create dummies which cannot be distinguished from the true user position, in particular, if an adversary has additional context information such as a map and can track the user for longer times.

An advanced method to generate dummies is presented in the *SybilQuery* approach proposed by Shankar et al. [22]. The approach assumes that the user has a database of historic traffic which allows him to create additional dummy positions that cannot be distinguished from the real user position.

4.2 Mix Zones

The idea of the **mix zones** approach proposed by Beresford et al. [23] is to define areas called mix zones, where all user positions must be hidden such that the user position is not known within these zones. This is achieved by not sending any position updates within a zone. If a user enters a mix zone, the user identity is mixed with all other users in the zone by changing pseudonyms to protect user identities. Thus, an attacker cannot correlate different pseudonyms of the users even by tracing the entry and exit points of a mix zone.

The *MobiMix* approach proposed by Palanisamy and Liu [24] applies the mix zone concept to road networks. They take into account various context information that can be used by an attacker to derive detailed trajectories such as geometrical and temporal constraints.

4.3 k-Anonymity

k-anonymity is a wide-spread general privacy concept not restricted to location privacy. It provides the guarantee that in a set of k objects (in our case, mobile users) the target object is indistinguishable from the other $k-1$ objects. Thus, the probability to identify the target user is $1/k$.

The concept of k-anonymity for location privacy was introduced by Gruteser and Grunwald [25]. The idea of their approach is that a user reports an obfuscation area to a client containing his position and the positions of $k-1$ other users instead of his precise position that is protected by a pseudonym. Here, the LS acts as trusted anonymizer to calculate the set of k users and the obfuscation area based on its known user positions. As an example consider that Alice is currently located at home and queries a location-based service for the nearest cardiology clinic. Without using anonymization, this query could reveal to the client implementing the service that Alice has health problems. By using k-anonymity, Alice would be indistinguishable from at least $k-1$ other users, such that the client could not link the request to Alice. Therefore, it is required that all k users of the calculated anonymization set sent to the client share the same obfuscation area such that the client cannot link the issued position to the home location of Alice.

Many other approaches make use of the k-anonymity concept to provide location privacy. Mokbel et al. [26] calculate the obfuscation area of the k users in their *Casper* framework based on the user defined values of k and an area value A_{min} indicating that the user wants to hide his location within an area size of at least A_{min}. Gedik et al. proposed the *CliqueCloak* approach [27, 28] which performs spatial and temporal cloaking to calculate the k-anonymity set.

A user can define individual upper limits for both the obfuscation area size and time periods associated with positions in order to preserve an acceptable quality of service. The approach uses temporal cloaking by delaying updates such that the required number of k users are determined within the user defined time interval and the maximum obfuscation area.

The basic concept of k-anonymity has been extended by various approaches to increase privacy protection. The most prominent extensions are *strong k-anonymity*, *l-diversity*, *t-closeness*, *p-sensitivity*, and *historical-k-anonymity*.

Zhang et al. [29] guarantee *strong k-anonymity* by ensuring that the calculated cluster of k users remains the same over several queries (so-called reciprocity of k-clusters). Therefore, attacks that intersect several k-clusters of different queries cannot easily identify a user. Another approach to achieve reciprocity of k-clusters is proposed by Ghinita et al. [30]. In [31], Talukder and Ahamed propose to use *adaptive nearest neighborhood cloaking* to achieve this property.

The idea of location *l-diversity* presented by Bamba et al. [32] is that the location of the user is unidentifiable from a set of l different physical locations such as churches, clinics, bars, etc. To this end, the approach guarantees that the position of the k-cluster members are not just different, but are also located distant enough from each other. Otherwise, an attacker would know the target user location with low imprecision if all user positions belong to the same semantic location.

The concept of *t-closeness* proposed by Li et al. [33] extends the l-diversity concept. Here, parameter t represents the distance between an attribute's distribution within the selected cluster of k users and the same attribute's distribution over the total set of user; this distance should not be smaller than a certain threshold t.

Domingo-Ferrer et al. proposed the concept of *p-sensitivity* to improve k-anonymity guarantees [34]. The idea of p-sensitivity is to guarantee that within a k-cluster each group of confidential key attributes has at least p distinct values for each confidential attribute within the same group. Otherwise, the key attributes could be disclosed by the corresponding attributes of the group. As a simple example consider the case that all members of a k-cluster have cancer. In this case, an attacker knows for sure that the target user also has this disease.

The k-anonymity guarantee can also be improved by taking into account the temporal component of the user's location information. Mascetti et al. described an approach called *historical k-anonymity* to provide k-anonymity guarantees for moving objects [35]. Similarly to strong k-anonymity clustering, historical information of multiple users is divided into blocks, where each block contains positions of at least k users. While the approach of Mascetti et al. is designed to secure sequential queries *online* (i.e. on-the-fly), Abul et al. concentrate on securing a *complete* published user trajectory offline. To this end, they apply an enhancement of k-anonymity [36] for spatial-temporal cloaking called (k, δ)-anonymity. The idea is that before publishing, the trajectories of at least k users are co-located within a "space tunnel" of radius $\delta/2$ that defines an uncertainty level.

Usually, k-anonymity approaches require a TTP (a trusted LS) which is aware of all precise user positions and acts as anonymizer. Several approaches such as [37, 38] try to avoid a single trusted anonymizer by implementing a decentralized approach. For instance, Chow et al. [38] use peer-to-peer (P2P) communication to find a spatial region which covers the needed number of k users of the cluster. After the required cluster is found, a randomly selected cluster member sends the intended query to the client to hide the identity of the query issuer. Another P2P approach called *MobiHide* is presented by Ghinita et al. [37] using Hilbert space-filling curves to hide the query initiator among a group of k users.

Hu and Xu [39] presented another decentralized approach providing user anonymity, where users measure the distance between their current position and the positions of the other peers, for example, based on the measurable WiFi signal strength. After calculating the k-cluster by this information, they use secure multi-party computation principles to calculate the obfuscation area within the cluster without revealing precise user information to other peers.

4.4 Obfuscation and Coordinate Transformation

Spatial obfuscation approaches try to preserve privacy by deliberately reducing the precision of position information sent from the user to the LS and in turn to the client. A classic spatial obfuscation approach is the one presented by Ardagna et al. [8], where a user sends a circular area instead of the precise user position to the LS.

The advantage of spatial obfuscation approaches is that they provide location privacy without a TTP, since the user himself can define the obfuscation area. However, this advantage comes at the price that clients are not provided with a precise user position. This trade-off between privacy and precision was studied by Cheng et al. [40]. They introduced a model for probabilistic range queries depending on the overlapping size of the query area and the obfuscation shapes.

Instead of using geometric obfuscation shapes like circles, Duckham and Kulik use *obfuscation graphs* to apply the concept of position obfuscation to road networks [41].

Gutscher et al. propose an approach based on **coordinate transformation** [42]. The mobile users perform some simple geometric operations (shifting, rotating) over their positions before sending them to the LS. In order to recover the original position, the transformation function needs to be distributed among clients. Otherwise, it is impossible to compare positions of different users obfuscated with different transformations, for instance, to perform range queries.

In [43], Yiu et al. present their framework called *SpaceTwist* to answer k-nearest-neighbor-queries while protecting user location privacy. Instead of sending precise user positions to the LS, users send a so called “anchor” representing a fake location to the LS. The anchor is then used to iteratively request data points based on various distances to the anchor. The user then calculates the query results based on his precise position and the received data points. Thus, precise k-nearest-neighbor-query results are provided to the user, while location privacy is achieved through higher query and communication costs.

In [44], Hashem et al. present a group-based approach, where a group of users, for example, wants to determine the next restaurant that minimizes the total travel distance for all users of the group. This approach protects the location privacy of the users by providing regions instead of precise positions within the group nearest neighbor query to the LS.

Beyond the obfuscation of spatial information, Gruteser et al. consider **spatio-temporal obfuscation** to protect movement trajectories of users [25]. Besides decreasing the precision of positions, they also decrease the precision of the temporal information associated with positions until a specified k-anonymity criterion is achieved. A similar idea was presented by Ghinita et al. for their *spatio-temporal cloaking* approach [45]. To improve the provided privacy of spatial cloaking, the authors consider background map knowledge represented by a set of privacy-sensitive features. Moreover, this approach resists advanced attacks based on the known maximum speed of objects (cf. maximum movement boundary attack introduced in the next section).

Besides these approaches, a number of similar approaches for protecting spatio-temporal location privacy were developed, including *trajectory clustering* [46], *trajectory transformation* [47], *uncertainty-aware path cloaking* [48], *virtual trip lines* [49], etc.

One problem with many spatial obfuscation techniques is that the effective size of the intended obfuscation area can be reduced if an adversary applies background knowledge, in particular, map knowledge. In order to resist such map matching attacks, Ardagna et al. proposed a *landscape-aware* obfuscation approach [50]. This approach is based on a probability distribution function defining the probability that a user is located in certain areas of a map. The obfuscation area is selected considering the probability of the user to be located in areas of the obfuscation shape.

Another advanced obfuscation approach [51] presented by Damiani et al. applies a similar principle to protect semantic locations such that a user position cannot be mapped with a high probability to certain critical locations such as a hospital. Their map-aware obfuscation approach expands the obfuscation area adaptively in a way that the probability of the user for being in a certain semantic location is below a given threshold.

4.5 Cryptography-based Approaches

Cryptographic location privacy approaches use encryption to protect user positions. Mascetti et al. propose an approach to notify users when friends (also called buddies) are within their proximity without revealing the current user position to the LS [52]. To this end, the authors assume that each user shares a secret with each of his buddies and use **symmetric encryption** techniques. Approaches such as [53] proposed by Ghinita et al. make use of the *private information retrieval* (PIR) technique to provide location privacy. By using PIR, an LS can answer queries without learning or revealing any information of the query. The used PIR technique relies on the quadratic residuosity assumption, which states that it is computationally hard to find the quadratic residues in modulo arithmetic of a large composite number for the product of two large primes [53].

In order to deal with the problem of non-trusted LS infrastructures, Marias et al. [54] proposed an approach for the distributed management of position information based on the concept of secret sharing. The basic idea of this approach is to divide position information into shares, which are then distributed among a set of (non-trusted) LSs. In order to recover positions, the client needs the shares from multiple servers. The advantage of this approach is that a compromised LS cannot reveal any position information since it does not have all the necessary shares. The disadvantage of this approach is that LSs cannot perform any computations on the shares, for instance, to perform range queries.

In general, cryptographic approaches raise the question whether location-based queries such as nearest-neighbor-queries or range-queries can be performed efficiently over the encrypted data.

4.6 Position Sharing

To perform location-based queries such as nearest-neighbor or range queries while protecting user location privacy, Dürr et al. [55] proposed the concept of **position sharing** for the secure management of private position information in non-trusted systems. Position sharing splits up obfuscated position information into so called position shares, where a share defines a position of strictly limited precision. These shares are distributed among a set of non-trusted LSs such that each LS only has a position of limited precision, which can also be used to perform calculations on these shares. Through share combination algorithms, multiple shares can be fused into positions of higher precision such that clients can be provided with position information of different precision levels depending on the number of accessible shares. Since an LS only has information of limited precision, the approach has a graceful degradation property, where the precision of position revealed by an attacker gradually increases with the number of compromised LSs. In [56], the authors extended their work by taking map knowledge into account to prevent attackers from increasing the precision of positions. Another position sharing approach was proposed by Wernke et al. [57]. Unlike the position sharing approach of [55] which generates shares based on geometric transformations, they utilize the concept of *multi-secret sharing* [58] for share generation. Besides geometric information, this approach also supports symbolic location information.

5 Classification of Location Privacy Attacks

In this section, we first present a classification of attackers according to their knowledge which they exploit to derive private information. Then, we classify different attacks on location privacy.

5.1 Attacker Knowledge

We classify attacker knowledge according to two dimensions, namely *temporal information* and *context information* (cf. Figure 2). In the *temporal dimension*, we consider whether an attacker has only access to a single user position or whether the attacker can access historic information. In the first case, the attacker knows only a single snapshot of a user position. This is a common assumption for many privacy approaches. In the second case, the attacker knows a set of multiple position updates collected over time or even a whole movement trajectory. Such information could be revealed, for instance, by a compromised LS or a compromised client. In particular, if an LS got compromised, the attacker might also get historic position information of several users.

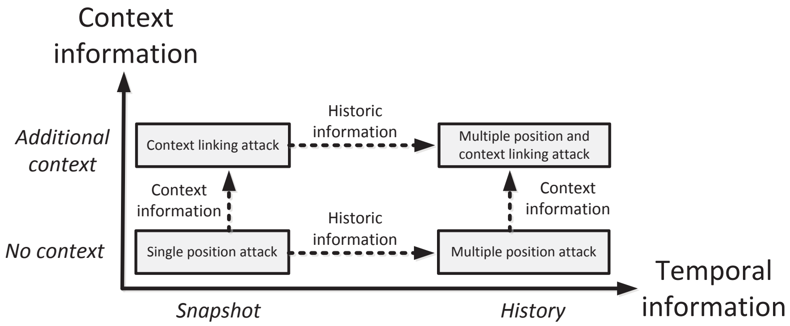

Fig. 2 Classification of attacker knowledge

In the *context dimension* we distinguish whether or not the attacker has additional context knowledge beyond spatio-temporal information. For instance, an advanced attacker might have additional context information provided by a phone book, statistical data, a map, etc. The attacker can use this information in addition to the known user positions. For instance, an attacker could decrease the size of the obfuscation area of a user by using map knowledge to determine where users can move, or use a phone book to determine the home address of a user.

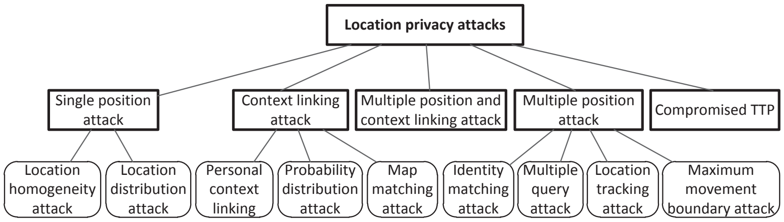

Fig. 3 Classification of location privacy attacks

5.2 Location Privacy Attacks

Our classification of attacks is shown in Figure 3. We distinguish between *single position attacks*, *context linking attacks*, *multiple position attacks*, attacks combining *context linking* and *multiple position attacks*, and attacks based on *compromising a TTP* component. Next, we are going to discuss these different attacks in detail.

5.2.1 Single Position Attack

The general idea of the single position attack is that the attacker analyzes a single query or an update from the user to infer more information about the position or the identity that the user intended to hide.

A **location homogeneity attack** [59] can be used against simple k-anonymity approaches. The attacker analyzes the positions of all k-cluster members. If their positions are almost identical (cf. Figure 4a), the position information of each member is revealed. If the cluster members are distributed over a larger area, the position information is protected (cf. Figure 4b). An advanced location homogeneity attack can utilize map knowledge to reduce the effective area size where users can be located. For instance, the area can be restricted to a single building (cf. Figure 4c). Here, the attacker analyzes the semantic location information of the cluster members and determines the diversity of the position information. Only diverse position information provides location privacy while homogeneous position information does not.

A **location distribution attack** [5] is based on the observation that users are often not distributed homogeneously in space. This can be utilized to attack some k-anonymity approaches. Consider a k-cluster whose members cover a densely and sparsely populated area as depicted in Figure 5. Here, the dark red area defines the calculated area of the k-cluster. In such a cluster the protected user is most likely the single user A located in the sparsely populated area far away from the other users, since in that case the obfuscation area has to be extended into the dense area to cover the requested number of k users. If B were the protected user, a completely different cluster would be the result (cf. the yellow area in Figure 5).

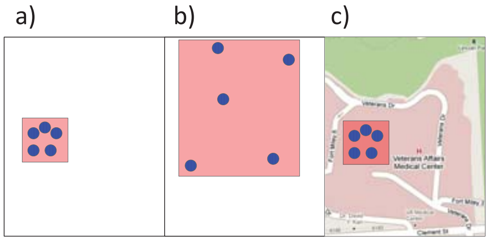

Fig. 4 Location homogeneity attack

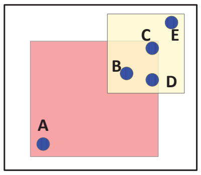

Fig. 5 Location distribution attack

5.2.2 Context Linking Attack

A context linking attack [59] exploits context information additionally to spatio-temporal information. An attacker can use personal context knowledge about a user as well as external background knowledge such as an office plan, an address book, a map, etc. to decrease user privacy. For the context linking attack, we distinguish between three different kinds of attacks: The *personal context linking attack*, the *probability distribution attack*, and *map matching*:

A **personal context linking attack** [25] is based on personal context knowledge about individual users such as user preferences or interests. For instance, assume it is known that a user visits a pub on a regular basis at a certain point in time and that he uses simple obfuscation mechanism to protect his location privacy. Then, an attacker can increase his known precision of an obtained obfuscated position by decreasing the obfuscation area to locations of pubs within the obfuscation area.

A special kind of the personal context linking attack is the **observation attack** [25], where the attacker has user knowledge gathered through observation. For instance, if a user is using pseudonyms and the attacker can see the observed user, then the attacker can retrace all prior locations of the user for the same pseudonym by a single correlation.

The **probability distribution attack** [60] is based on gathered traffic statistics and environmental context information. Here, the attacker tries to derive a probability distribution function of the user position over the obfuscation area. If the probability is not uniformly distributed, an attacker can identify areas where the user is located with high probability.

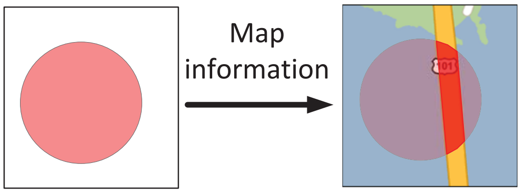

Fig. 6 Map matching attack refining a position to a road bridge

Map matching [61] can be used to restrict the obfuscation area to certain locations where users can be located by removing all the irrelevant areas. For instance, a map could be used to remove areas like lakes from the obfuscation area, which effectively shrinks the obfuscation area size below the intended size (cf. Figure 6). The attacker can also use semantic information provided by the map such as points of interest or type of buildings (bars, hospitals, residential building, etc.) to further restrict the effective obfuscation area size.

5.2.3 Multiple Position Attack

The general idea of a multiple position attack is that an attacker tracks and correlates several position updates or queries of a user to decrease user privacy.

Identity matching [23] can be used to attack several pseudonyms of a user. The attacker links several pseudonyms based on equal or correlating attributes to the same identity such that the provided privacy of the changed pseudonyms is broken.

For a **multiple-query attack** [31], the attacker analyses several queries or updates. The attacker can perform the attack as *shrink region attack* or as *region intersection attack*:

A **shrink region attack** [31] can reveal the identity and the position of a user. To this end, the attacker monitors consecutive updates or queries and the corresponding members of the k-anonymity set. If the members of the set change, an attacker can infer which user sent the initial update or query. As an example consider three users A, B, and C located at different positions. User A issues two different queries to the same client. The simple k-anonymity approach used by A once generates the k-anonymity set (A, B) for the first query and the anonymity set (A, C) for the second query. If the client can now correlate both queries, the client can infer that A originally issued the query.

The **region intersection attack** [31] can be used against location obfuscation approaches to increase the precision of obfuscated positions. To this end, the attacker uses several imprecise position updates or queries from a user to calculate their intersection. From the intersections, the attacker can infer where privacy sensitive regions of the user are, or where the user is located. As example for this attack, consider a random obfuscation mechanism generating different obfuscation areas whenever the user reaches his home. Then, the intersection of different obfuscation areas can be used to decrease user privacy.

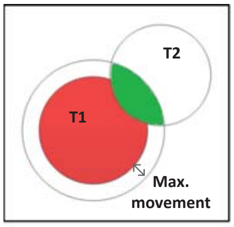

Fig. 7 Maximum movement boundary attack

A **location tracking attack** [25] makes use of several position updates known to the attacker. For example, this attack can be used against randomly changing pseudonyms without using mix zones. Here, the attacker can correlate succeeding pseudonyms by linking spatial and temporal information of succeeding position updates or queries, even if an obfuscation mechanism is used. For instance, the attacker can try to reconstruct the movement of a user based on the provided positions of several pseudonyms.

In a **maximum movement boundary attack** [45] the attacker calculates the maximum movement boundary area, where the user could have moved between two succeeding position updates or queries. As shown in Figure 7, the position of the first update performed at time T1 helps the attacker to increase the precision of the update sent at T2. In this example, only a small part of the area of T2 is reachable within the maximum movement boundary. Therefore, the remaining area of the position update can be excluded by the attacker.

5.2.4 Combination of Multiple Position and Context Linking Attack

Instead of using only one single attack presented so far, an attacker can also combine several of the proposed attacks or use them in sequence to undermine the user's location privacy. For instance, an attacker could combine the knowledge of map restrictions gathered by the map matching attack and the restrictions of the maximum movement boundary attack to determine where the user is moving.

5.2.5 Compromised TTP

The attack of compromising a trusted third party (TTP) describes the fact that an attacker could get access to the data stored on a TTP. For instance, an attacker could compromise a trusted LS and get access to the stored user data. This attack is not considered in approaches that rely on a TTP, as it would undermine every approach using a TTP. However, as it is shown in [6], the attack on a TTP is realistic and not negligible. Therefore, it is at least questionable to assume the trustworthiness of a TTP.

6 Classification of Location Privacy Approaches

In this section, we present our classification of selected location privacy approaches based on the analysis which protection goals they fulfill for different attacks (cf. Table 2).

As we have shown in Section 3, we distinguish between different protection goals of a mobile user, defined by the attributes *identity*, *position*, and *time*. These protection goals are represented in Table 2 on the vertical axis. For each protection goal, we depicted the basic approaches presented in Section 4 providing the corresponding protection goal. For each approach, we marked whether it needs a trusted third party (TTP) or not. We arranged the different approaches based on their primary protection goal. Approaches marked by "*" provide the protection goal as a sub-goal in addition to their primary protection goal.

The horizontal axis of Table 2 represents possible location privacy attacks as presented in Section 5. For a clearer presentation, we omitted the location distribution attack and the identity matching attack, which are only applicable to a small set of approaches in the area of *k*-anonymity and changing pseudonyms. In the main part of Table 2, we use a "✓" to show for each combination of a location privacy approach and a location privacy attack that the corresponding protection goal can be provided. An empty cell shows that the attack can successfully undermine the privacy approach such that the protection goal cannot be achieved. Next, we will summarize the key findings that can be derived from Table 2.

Most approaches protecting the user's identity against different attacks are based on *k*-anonymity. However, with the exception of few approaches ([53, 22, 62]), all of these approaches require a TTP (an anonymizer).

If the user wants to preserve location privacy without protecting his identity, the most popular technique to apply is spatial obfuscation. Its major drawback is that clients can only retrieve an obfuscation area instead of a precise user position. To overcome this problem, the method of position sharing [55, 57, 56] has been proposed, where the user can flexibly manage the precision provided to each client.

Most approaches protecting the attributes *position* and *time* focus on single position updates and queries of a user. Only few approaches ([45, 57]) consider multiple position updates and queries. Thus, only these approaches can resist a multiple query attack or a maximum movement boundary attack.

Map matching as used against spatial obfuscation approaches has received great attention in research. Being a relative novel research question, the corresponding approaches can still be improved to deal with map-related knowledge provided by modern map services. These services can provide, for instance, frequently visited points of interests and opening hours from shops. An attacker could use this information to perform more advanced probability distribution attacks. Furthermore, semantic location information should be considered by new approaches as this information is also available to an attacker by modern map services.

Regarding the protection of spatio-temporal information, many approaches tend to limit the considered problem by taking into account only maximum movement boundary attacks or an already published complete trajectory. However, a challenging problem here remains to have a privacy mechanism protecting continuous user position updates in real-time as used for online tracking.

Finally, we use the information of Table 2 to determine relevant combinations of protection goals and attacks that are not considered by any existing approach and define interesting future research areas. We marked the corresponding cells in Table 2 in gray and discuss them now in more detail.

Currently, only few approaches ([34, 53]) can resist a personal context linking attack. Most approaches cannot protect any combination of the attributes *identity*, *position*, and *time* against such an attack. Therefore, future research needs to consider user habits, regular user behavior, user interests, etc.

Moreover, the combination of the map matching and the maximum movement boundary attack is most beneficial against approaches trying to protect the attribute *position* as well as the attributes *position* and *time*. Thus, approaches providing the corresponding protection goal considering this combination of attacks are required. In general, combinations of attacks are rarely considered. Therefore, approaches considering advanced attackers using different types of attacks should be investigated in future research.

Goals			Approaches							
ID	Pos.	Time								
✓	✓	✓	[13]^{TTP} Hist. k-anon.	✓	✓	▨	✓	✓	✓	✓
			[24]^{TTP} Mix zones	✓	✓	▨	✓	✓	✓	✓
			[32]^{TTP} Dynam. cloaking	✓	✓	▨	✓			
			[22] SybilQuery	✓	✓	▨	✓	✓	✓	✓
		✗	[26]^{TTP} k-anon. + A_{min}	✓			✓	✓		
			[59]^{TTP} l-diverse k-anon.	✓	✓		✓		✓	✓
			[34]^{TTP} p-sensitive k-an.		✓	✓	✓		✓	✓
			[29]^{TTP} Strong k-an.	✓	✓		✓	✓	✓	✓
	✗	✓	[24]^{TTP} Mix zones *	✓	✓	▨	✓	✓	✓	✓
		✗	[62] Pseudonyms		✓			✓	✓	✓
			[53] PIR based approach	✓	✓	✓	✓	✓	✓	✓
✗	✓	✓	[25] Spat.-temp. cloak.	✓		▨				▨
			[48] Path cloaking	✓	✓	▨	✓			▨
			[46] Trajectory clustering	✓		▨			✓	▨
			[45] Max. velocity protect.	✓		▨		✓	✓	▨
		✗	[8] Spatial obfuscation	✓		▨				▨
			[57] Position sharing	✓		▨		✓	✓	▨
			[56] Map-aw. pos. sharing	✓	✓	▨				▨
			[18]^{TTP} Map-aware obf.	✓	✓	▨	✓			▨
			[21] Dummies approach	✓	✓	▨				▨
	✗	✓	[25]*, [32]^{TTP}*, [13]^{TTP}*	✓	✓	▨	✓	✓	✓	✓
		✗	(No approach required)							
			General techniques (no attack)	Location homogeneity attack	Map matching	Personal context linking	Probability dist. attack	Multiple query attack	Maximum movement boundary	Map matching & max. movement boundary
				Attacker knowledge						

Table 2 Classification of location privacy approaches. Each protection goal is defined by whether the attribute identity, position, and time should be protected (✓) or not (✗). The stated techniques provide the corresponding protection goal assuming a certain attacker knowledge. If the technique can resist an attacker with a certain attack, this is denoted by a ✓ in the main part of the table, whereas an empty cell denotes that the attack can be successful against the stated technique. The gray cells indicate possible future research directions not covered by the stated techniques.

7 Summary

Driven by the availability of modern mobile devices with integrated position sensors, location-based services have become very popular recently. Since these services access private position information, location privacy concepts are mandatory to ensure the user acceptance of such services. The literature describes many different concepts and approaches to protect location privacy, which differ in terms of the protected information and their effectiveness for different attacks.

In order to assess the applicability and effectiveness of location privacy approaches systematically, we first stated different protection goals in this paper. In detail, we distinguished between the protection of personal information (user identity), spatial information (user position), and temporal information (identity/position + time). In a second step, we gave an overview of existing fundamental concepts and approaches to protect location privacy, before we introduced a classification of possible attacks that try to reveal the protected information. Finally, we analyzed existing approaches with respect to their protection goals and their ability to resists the introduced attacks.

In summary, considering the variety of possible attacks, the protection of location privacy remains a big challenge. A user always has to trade off the benefits gained from services based on private information and the possibility that his private information might be revealed at least partially. As a conclusion, we can state that in particular the combination of different attacks still poses a problem to existing approaches. Also many approaches only consider limited attacker models, which becomes a problem for advanced attackers applying, for instance, background knowledge like map information or other context information to reveal private information.

References

1. Qype. www.qype.com (February 2012)
2. Loopt. www.loopt.com (February 2012)
3. Facebook: Places. www.facebook.com/places (February 2012)
4. Foursquare. www.foursquare.com (February 2012)
5. Mokbel, M.F.: Privacy in location-based services: State-of-the-art and research directions. In: IEEE International Conference on Mobile Data Management (MDM 2007). (2007) 228
6. Privacy Rights Clearinghouse: Privacy rights clearinghouse. http://www.privacyrights.org/data-breach (February 2012)
7. Pedreschi, D., Bonchi, F., Turini, F., Verykios, V.S., Atzori, M., Malin, B., Moelans, B., Saygin, Y.: Privacy protection: Regulations and technologies, opportunities and threats. In: Mobility, Data Mining and Privacy. Springer (2008) 101–119
8. Ardagna, C., Cremonini, M., Damiani, E., De Capitani di Vimercati, S., Samarati, P.: Location privacy protection through obfuscation-based techniques. In: Proc. of the 21st Annual IFIP WG 11.3 Working Conference on Data and Applications Security, Redondo Beach, CA, USA (July 2007)
9. Kalnis, P., Ghinita, G., Mouratidis, K., Papadias, D.: Preventing location-based identity inference in anonymous spatial queries. IEEE Transactions on Knowledge and Data Engineering **19**(12) (December 2007) 1719–1733

10. Solanas, A., Domingo-Ferrer, J., Martínez-Ballesté, A.: Location privacy in location-based services: Beyond ttp-based schemes. In: International Workshop on Privacy in Location-Based Applications (PiLBA 2008). (2008)
11. Barker, K., Askari, M., Banerjee, M., Ghazinour, K., Mackas, B., Majedi, M., Pun, S., Williams, A.: A data privacy taxonomy. In: BNCOD. (2009) 42–54
12. Khoshgozaran, A., Shahabi, C.: A taxonomy of approaches to preserve location privacy in location-based services. Int. J. Comput. Sci. Eng. **5** (November 2010) 86–96
13. Bettini, C., Mascetti, S., Wang, X.S., Freni, D., Jajodia, S.: Anonymity and historical-anonymity in location-based services. In: International Workshop on Privacy in Location-Based Applications (PiLBA 2009). (2009) 1–30
14. Krumm, J.: A survey of computational location privacy. Personal and Ubiquitous Computing **13**(6) (August 2009) 391–399
15. Gilbert, P., Cox, L.P., Jung, J., Wetherall, D.: Toward trustworthy mobile sensing. In: Proc. of the 11th Workshop on Mobile Computing Systems & Applications (HotMobile 2010). (February 2010)
16. Golle, P., Partridge, K.: On the anonymity of home/work location pairs. In: Proceedings of the 7th International Conference on Pervasive Computing. Pervasive '09, Berlin, Heidelberg, Springer-Verlag (2009) 390–397
17. Bettini, C., Wang, X., Jajodia, S.: Protecting privacy against location-based personal identification. In Jonker, W., Petkovic, M., eds.: Secure Data Management. Volume 3674 of Lecture Notes in Computer Science. Springer Berlin / Heidelberg (2005) 185–199
18. Damiani, M.L., Bertino, E., Silvestri, C.: Protecting location privacy against spatial inferences: the probe approach. In: Proceedings of the 2nd SIGSPATIAL ACM GIS 2009 International Workshop on Security and Privacy in GIS and LBS. SPRINGL '09, New York, NY, USA, ACM (2009) 32–41
19. Wang, T., Liu, L.: From data privacy to location privacy. In Tsai, J.J.P., Yu, P.S., eds.: Machine Learning in Cyber Trust: Security, Privacy, and Reliability. Springer US (April 2009) 217–247
20. Chow, C.Y., Mokbel, M.F.: Trajectory privacy in location-based services and data publication. SIGKDD Explorations **13**(1) (2011) 19–29
21. Kido, H., Yanagisawa, Y., Satoh, T.: An anonymous communication technique using dummies for location-based services. In: Proceedings of the International Conference on Pervasive Services (ICPS '05). (July 11–14, 2005) 88–97
22. Shankar, P., Ganapathy, V., Iftode, L.: Privately querying location-based services with sybilquery. In: International Conference on Ubiquitous Computing (UbiComp 2009). (2009) 31–40
23. Beresford, A.R., Stajano, F.: Mix zones: User privacy in location-aware services. In: PerCom Workshops. (2004) 127–131
24. Palanisamy, B., Liu, L.: Mobimix: Protecting location privacy with mix-zones over road networks. In: Proceedings of the 2011 IEEE 27th International Conference on Data Engineering. ICDE '11, Washington, DC, USA, IEEE Computer Society (2011) 494–505
25. Gruteser, M., Grunwald, D.: Anonymous usage of location-based services through spatial and temporal cloaking. In: Proceedings of the 1st international conference on Mobile systems, applications and services (MobiSys '03), New York, NY, USA, ACM (2003) 31–42
26. Mokbel, M.F., Chow, C.Y., Aref, W.G.: The new casper: query processing for location services without compromising privacy. In: Proceedings of the 32nd international conference on Very large data bases (VLDB '06), VLDB Endowment (2006) 763–774
27. Gedik, B., Liu, L.: Location privacy in mobile systems: A personalized anonymization model. In: International Conference on Distributed Computing Systems (ICDCS 2005). (2005) 620–629
28. Gedik, B., Liu, L.: Protecting location privacy with personalized k-anonymity: Architecture and algorithms. IEEE Transactions on Mobile Computing **7**(1) (January 2008) 1–18
29. Zhang, C., Huang, Y.: Cloaking locations for anonymous location based services: a hybrid approach. Geoinformatica **13**(2) (June 2009) 159–182

30. Ghinita, G., Kalnis, P., Skiadopoulos, S.: Prive: anonymous location-based queries in distributed mobile systems. In: Proceedings of the 16th international conference on World Wide Web (WWW '07), New York, NY, USA, ACM (2007) 371–380
31. Talukder, N., Ahamed, S.I.: Preventing multi-query attack in location-based services. In: Proceedings of the third ACM conference on Wireless network security. WiSec '10, New York, NY, USA, ACM (2010) 25–36
32. Bamba, B., Liu, L., Pesti, P., Wang, T.: Supporting anonymous location queries in mobile environments with privacygrid. In: Proceeding of the 17th international conference on World Wide Web (WWW '08), New York, NY, USA, ACM (2008) 237–246
33. Li, N., Li, T., Venkatasubramanian, S.: t-closeness: Privacy beyond k-anonymity and l-diversity. In: Proceedings of the IEEE 23rd International Conference on Data Engineering (ICDE 2007). (April 15–20, 2007) 106–115
34. Solanas, A., Sebé, F., Domingo-Ferrer, J.: Micro-aggregation-based heuristics for p-sensitive k-anonymity: one step beyond. In: Proceedings of the 2008 international workshop on Privacy and anonymity in information society (PAIS '08), New York, NY, USA, ACM (2008) 61–69
35. Mascetti, S., Bettini, C., Wang, X.S., Freni, D., Jajodia, S.: Providenthider: An algorithm to preserve historical k-anonymity in lbs. In: IEEE International Conference on Mobile Data Management (MDM 2009). Volume 0., Los Alamitos, CA, USA, IEEE Computer Society (2009) 172–181
36. Abul, O., Bonchi, F., Nanni, M.: Never walk alone: Uncertainty for anonymity in moving objects databases. In: IEEE 24th International Conference on Data Engineering (ICDE 2008). (April 2008) 376–385
37. Ghinita, G., Kalnis, P., Skiadopoulos, S.: MOBIHIDE: a mobile peer-to-peer system for anonymous location-based queries. In: Proceedings of the 10th international conference on Advances in spatial and temporal databases SSTD'07, Springer-Verlag Berlin (July 2007) 221–238
38. Chow, C.Y., Mokbel, M.F., Liu, X.: Spatial cloaking for anonymous location-based services in mobile peer-to-peer environments. GeoInformatica **15**(2) (November 2011) 351–380
39. Hu, H., Xu, J.: Non-exposure location anonymity. In: IEEE 25th International Conference on Data Engineering (ICDE). (March 2009) 1120–1131
40. Cheng, R., Zhang, Y., Bertino, E., Prabhakar, S.: Preserving user location privacy in mobile data management infrastructures. In: 6th Workshop on Privacy Enhancing Technologies. Volume 4258/2006., Springer Berlin / Heidelberg (2006) 393–412
41. Duckham, M., Kulik, L.: A formal model of obfuscation and negotiation for location privacy. In: Proceedings of the International Conference on Pervasive Computing (Pervasive 2005). (2005) 152–170
42. Gutscher, A.: Coordinate transformation - a solution for the privacy problem of location based services? In: Proceedings of 20th International Parallel and Distributed Processing Symposium IPDPS 2006. (April 25–29, 2006) 7pp.
43. Yiu, M.L., Jensen, C.S., Mø ller, J., Lu, H.: Design and analysis of a ranking approach to private location-based services. ACM Transactions on Database Systems **36**(2) (May 2011) 1–42
44. Hashem, T., Kulik, L., Zhang, R.: Privacy preserving group nearest neighbor queries. In: Proceedings of the 13th International Conference on Extending Database Technology - EDBT '10, New York, New York, USA, ACM Press (March 2010) 489–500
45. Ghinita, G., Damiani, M.L., Silvestri, C., Bertino, E.: Preventing velocity-based linkage attacks in location-aware applications. In: Proc. of the 17th ACM SIGSPATIAL Int. Conf. on Advances in Geographic Information Systems. (2009)
46. Lee, J.G., Han, J., Whang, K.Y.: Trajectory clustering: a partition-and-group framework. In: SIGMOD Conference. (2007) 593–604
47. Terrovitis, M., Mamoulis, N.: Privacy preservation in the publication of trajectories. In: 9th International Conference on Mobile Data Management (MDM '08). (April 2008) 65–72
48. Hoh, B., Gruteser, M., Xiong, H., Alrabady, A.: Preserving privacy in gps traces via uncertainty-aware path cloaking. In: Proceedings of the 14th ACM conference on Computer and communications security (CCS '07), New York, ACM (2007) 161–171

49. Hoh, B., Gruteser, M., Herring, R., Ban, J., Work, D., Herrera, J.C., Bayen, A.M., Annavaram, M., Jacobson, Q.: Virtual trip lines for distributed privacy-preserving traffic monitoring. In: Proceeding of the 6th international conference on Mobile systems, applications, and services (MobiSys '08), New York, NY, USA, ACM (2008) 15–28
50. Ardagna, C.A., Cremonini, M., Gianini, G.: Landscape-aware location-privacy protection in location-based services. Journal of Systems Architecture - Embedded Systems Design **55** (April 2009) 243–254
51. Damiani, M.L., Bertino, E., Silvestri, C.: The PROBE Framework for the Personalized Cloaking of Private Locations. Transactions on Data Privacy **3**(2) (August 2010) 123–148
52. Mascetti, S., Freni, D., Bettini, C., Wang, X.S., Jajodia, S.: Privacy in geo-social networks: proximity notification with untrusted service providers and curious buddies. The VLDB Journal **20**(4) (December 2010) 541–566
53. Ghinita, G., Kalnis, P., Khoshgozaran, A., Shahabi, C., Tan, K.L.: Private queries in location based services: anonymizers are not necessary. In: Proceedings of the 2008 ACM SIGMOD international conference on Management of data (SIGMOD '08), New York, NY, USA, ACM (2008) 121–132
54. Marias, G., Delakouridis, C., Kazatzopoulos, L., Georgiadis, P.: Location privacy through secret sharing techniques. In: Proceedings of the 1st International IEEE WoWMoM Workshop on Trust, Security and Privacy for Ubiquitous Computing (WOWMOM '05), Washington, DC, USA, IEEE Computer Society (June 2005) 614–620
55. Dürr, F., Skvortsov, P., Rothermel, K.: Position sharing for location privacy in non-trusted systems. In: Proceedings of the 9th IEEE International Conference on Pervasive Computing and Communications (PerCom 2011), Seattle, USA (March 2011)
56. Skvortsov, P., Dürr, F., Rothermel, K.: Map-aware position sharing for location privacy in non-trusted systems. In: Proceedings of the 10th International Conference on Pervasive Computing (Pervasive 2012), Newcastle, UK (June 2012)
57. Wernke, M., Dürr, F., Rothermel, K.: PShare: position sharing for location privacy based on Multi-Secret sharing. In: Proceedings of the 10th IEEE International Conference on Pervasive Computing and Communications (PerCom 2012), Lugano, Switzerland (March 2012)
58. Chan, C.W., Chang, C.C.: A scheme for threshold multi-secret sharing. Applied Mathematics and Computation **166**(1) (2005) 1–14
59. Machanavajjhala, A., Kifer, D., Gehrke, J., Venkitasubramaniam, M.: L-diversity: Privacy beyond k-anonymity. ACM Transactions on Knowledge Discovery from Data **1**(1) (2007) 3
60. Shokri, R., Theodorakopoulos, G., Le Boudec, J., Hubaux, J.: Quantifying location privacy. In: IEEE Symposium on Security and Privacy (SP 2011). (may 2011) 247 –262
61. Krumm, J.: Inference attacks on location tracks. In LaMarca, A., Langheinrich, M., Truong, K., eds.: Pervasive Computing. Volume 4480 of Lecture Notes in Computer Science. Springer Berlin / Heidelberg (2007) 127–143
62. Beresford, A.R., Stajano, F.: Location privacy in pervasive computing. IEEE Pervasive Computing **2**(1) (January 2003) 46–55