Privacy Preservation in Location Based Services

Sahana Shivaprasad, Huian Li, Xukai Zou*
Department of Computer and Information Science Purdue University Indianapolis, Indiana 46202, USA.

* Corresponding author. Email: xzou@cs.iupui.edu
Manuscript submitted March 18, 2015; accepted June 23, 2015.
doi: 10.17706/jcp.11.5.411-422

Abstract: Location based service (LBS) is one of the most popular mobile services today, which offers wide range of services that are based on information about the physical location of a user or device. Typical LBS includes real-time turn-by-turn directions, points of interest (POI), and social network services such as Facebook, Foursquare, Loopt, and Qype. However, user location privacy is a major concern in today's mobile applications and there has been significant research dedicated to address this issue. Various location privacy preserving mechanisms (LPPM) have been used to preserve privacy of the location information of mobile users. This survey aims to present privacy preserving mechanisms employed in the location based services. Moreover, the LPPMs are classified into cryptographic and non-cryptographic mechanisms, and a taxonomy of mechanisms is also discussed. Multiple defense mechanism attributes/goals for the protection of location privacy have been described in the literature. Furthermore, classification and comparison of different mechanisms and location privacy attacks are presented based on their protection attributes and adversarial goals. Strengths and weaknesses of different mechanisms are also highlighted.

Keywords: Location based service, location privacy attack, privacy preservation.

1. Introduction

The location based services (LBS) refer to a wide range of services that are based on information about the physical location of a user or device. Typical LBS includes social networking services such as Facebook [1] or Foursquare [2], where the user shares his/her current location to friends by checking-in to places such as restaurants, cinemas, etc. Other examples of friend finding services are Loopt [3] which finds all the friends within the users region, and Qype [4] which helps the user to find her points of interest (POI) and enhances given information by providing features like coupons or special offers. Many users share their position/location movement trajectory information to service providers in real-time to estimate real-time traffic data from the accumulated positions.

Although LBS has the benefit of providing location specific information to a user, it comes at the cost of privacy. As the user accesses the LBS applications, she will reveal location details and sensitive personal information such as where she lives, her lifestyle (for example, visiting a hospital, restaurant, or cinema), etc. When the user position is revealed, there is possibility that the user's location may get attacked or could be misused for mugging or stalking by allowing an adversary to infer delicate information of user movements. The usage of these services may raise severe location privacy concerns as discussed in [5], [6]. Privacy issues in mobile networks have been well studied in the literature [7], [8]. There are a number of surveys that talk about the state of the art techniques [9], [10].

Since location privacy is a major concern in today's mobile applications, there has been significant

research dedicated to address this issue. Various location privacy preserving mechanisms (LPPM) have been used to preserve privacy of the location information of mobile users. These mechanisms provide location privacy through removing user's identity or reporting fake locations. However, the identity traces can be de-anonymized and the obfuscation mechanism can be inverted, given an adversary with some background knowledge on the user. Also obfuscation degrades the service quality in favor of maximizing location privacy. Furthermore, many of these mechanisms: 1) ignore adversary's knowledge about user's access pattern and algorithm implemented by the location privacy preserving mechanisms, and 2) disregard optimal attack. For instance, for a given protection mechanism, an adversary can design an optimal attack to minimize his estimation error in the inference attack [11]. Therefore, there is need for mechanisms that respect user's required service quality, user-based protection, and real-time protection to prevent the adversary's optimal attack.

In this paper, we present a taxonomy of mechanisms that have been used to preserve user location privacy in location based services (LBS). Besides the discussion on the privacy preserving mechanisms, this survey also highlights the strength and the weakness of the presented mechanisms. Furthermore, classification and comparison of different mechanisms are presented based on various attacks.

The rest of the paper is organized as follows. The defense mechanism attributes/goals are formally defined and explained in Section 2. Section 3 discusses privacy preserving mechanisms used in LBS and highlights the strengths and weaknesses of mechanisms. Location privacy attack models are presented in Section 4. A classification of the privacy preserving mechanisms is provided in Section 5. Section 6 concludes the paper.

2. Defense Mechanism Attributes/Goals

Before introducing various location privacy preserving mechanisms, this section formally defines multiple defense mechanism attributes such as user identity, spatial information, and temporal information that should be protected by these mechanisms. Each attribute controls the amount of shared information and thus directly affects user location privacy. These attributes can also be considered as a priori knowledge of an adversary to minimize user privacy and are discussed in the location privacy attack models section. Location privacy can be achieved by fulfilling some or all of the entities given below.

2.1. Spatial Information Privacy

Spatial information privacy is the ability to prevent unauthorized entities to access the spatial location information of a user. By choosing the granularity of spatial information, the level of privacy can be varied according to a user's requirement. For example, the user might be willing to provide coarse location information such as name of the city to a service provider but, might want to share more specific location such as latitude and longitude values with her friends. Another important goal of spatial information privacy is to hide the identity of the user's location. For instance, knowing that a user entered a hospital would reveal the user's private information about her health status.

2.2. Temporal Information Privacy

Temporal information is related to the point in time when spatial information becomes available. One of privacy preserving methods would be to delay a user's spatial information so that the time and location of the user cannot be related. The level of privacy can be managed by controlling the temporal resolution of the user's location. For example, if a user wants to share the location that she has visited but does not reveal that she is not present at her home, the user's location update can be delayed by a certain amount of time per her requirement. Hence by delaying the user's location update by "x" amount of time instead of providing real-time update, the user's private information can be protected. However, recent work [12] has found out that even sporadic location information under the pseudonym protection are exposed to location privacy threats.

2.3. User Identity Privacy

Another important goal of privacy protection is to hide user identity. A user's identity can be her name, social security number, address, or any such unique information. However, an attacker can still identify a user by correlating the user's location information and the type of location.

3. Privacy Preserving Mechanisms

In this section, we present an overview of existing location privacy preserving mechanisms (LPPMs).

Numerous mechanisms have been proposed to preserve privacy of the user information in LBS. Although the mechanisms such as anonymization [13] and spatial obfuscation [14] provide location privacy through hiding identity or reporting fake locations, they ignore adversary's knowledge about user's access pattern and LPPM algorithm, and disregard the optimal attack where an attacker may design in an inference attack to reduce his calculation error. Hence Shokri *et al*. [11] propose an optimization framework to determine the most optimal LPPM against the most effective/optimal inference attack.

Based on defense mechanism goals/attributes and attacker's knowledge, the privacy preserving mechanisms used in LBS can be classified into: (a) cryptographic and (b) non-cryptographic mechanisms at the top level. The cryptographic mechanisms utilize certain encryption methods to protect user location. Conversely, non-cryptographic mechanisms mainly use a trusted location server using an anonymizer or without any trusted location server. In this section, several technical mechanisms for protecting location privacy will be discussed.

3.1. Protecting Location Privacy: Optimal Strategy against Localization Attacks

Table 1. Summary of LPPMs

LPPMs	Cryptographic	Strength	Weakness
Spatial obfuscation [14]	No	• High server efficiency • Location privacy without a trusted • location server	• No identity privacy • Unlink ability • Superiority of information about an individual position is degraded in order to protect that mobile user's position
mix zone [15]	No	• Location and sampling accuracy	• Operation lack in multiple responders
k-anonymity [13]	No	• Location privacy • Reduce re-identification and location tracking risk	• No identity privacy • Unlink ability • Due to inherent delay, this mechanism may not be suitable for services that need quick response • Involve users to specify different ks at different times and requires a large value of K to be successful • Low quality of service (QoS) in LBS applications
Personalized *k*-anonymity [16]	No	• Provide location privacy • Control the trade off between accuracy and privacy protection for LBS user	• This mechanism relies on trusted third party • Location privacy is inversely proportional
PIR [17]	Yes	• Perfect privacy guarantee against the optimal and context- linking/observation attacks • Supports spatial queries	• Computation and communication overhead • Low LBS server efficiency • Hard to implement on a handheld/portable
dummies [18]	No	• Easy to integrate with existing mobile network • User can send multiple dummy events without any need for other trusted third party components	• Operation lack in multiple responders

The optimization framework in [11] determines the most optimal LPPM to increase a user's location privacy against the most optimal attack and also respect the user's service quality constraint. In this

framework, a user's access profile may be known to an adversary. The user finds an obfuscation function such that, it increases location privacy and respects a maximum tolerable service quality loss. An adversary observes the pseudo-location output from previous steps and finds an optimal attack function to decrease the user's location privacy. This problem is formulated as Zero-sum Bayesian Stackelberg game where there are two opponents: a leader (user) and a follower (adversary). Here the user decides on her strategy knowing that an adversary is observing her action.

The performance of both non-optimal LPPMs and inference attacks against the optimal strategies is evaluated through real location traces. The authors observe that the obfuscation LPPM concentrates around the true location of a user, whereas the optimal LPPM extends the pseudo-locations in the most possible regions. They conclude that the optimal mechanism against the optimal attack creates a stable equilibrium (for both user and adversary) when compared with the non-optimal ones.

3.2. Mix Zone

Another mechanism to protect users privacy is mix zone [19]. The main idea of the mix zone mechanism is to define mix zone areas, and user positions are concealed such that their positions are unknown within these mix zone areas. This mechanism uses a trusted location server. A user identity is assorted with many others within the zone by changing pseudonyms whenever the user enters a mix zone. Thus, it protects the user's identity even when an adversary tries to trace the ingress and egress points of a mix zone and the adversary cannot link these various pseudonyms of the users.

This mechanism of preventing attackers from tracking long-term user movements can be better explained through an example discussed in [15]. Consider a scenario of the mix-zone where three users moving through a simple mix zone. The attacker can record the crossing points of the users between the zones and then makes use of the past information from close-by zones to model an attack based on users' movement, hence providing an attacker a chance in matching entering and exiting users with high reliability. These ingress/egress points and the times of user movement generate a movement matrix.

Observing these ingress and egress movements, an attacker can reconstruct correct mapping between all these events (mapping between new and old pseudonyms). This mapping could be related to a bipartite graph that represents possible mapping of ingress and egress pseudonyms. The attacker cannot model an attack with this little knowledge though. He needs to measure the probabilities of these mappings and then finds a perfect match.

The individual user anonymity can be explained by considering a scenario of two users $u1$ and $u2$, entering a mix zone at same time t as discussed in [15]. User $u1$ enters from north and $u2$ from east. Then the u1 exits from south at time $t+1$ and $u2$ stays in the mix zone. Now the attacker's measure of certainty depends on the user $u2$ exit with time $t+2$. If $u2$ exits from west, then the possible mapping will be (north to south, east to west) and (east to south, north to west). This user movement matrix makes the attacker more certain and can be easily cracked. Hence the identity matching can attack many pseudonyms of a user. The adversary can be certain and easily link all pseudonyms by connecting/correlating attributes to the same user identity. But if the user $u2$ had taken exit from south as the user $u1$, then the probabilities will look similar, that is (north to south, east to south) and (east to south, north to south). This movement matrix makes the attacker less certain.

MobiMix [20] is a mix zone mechanism that can be used for road networks. This mechanism considers the different context sensitive information that an adversary may use to obtain complete geometrical trajectory and temporal constraints.

The analysis in [21] identifies that the real-life deployment of communication patterns and mobility has been missed in existing identifier-change mechanisms. They demonstrate the effectiveness of standard mix zone based privacy protection mechanisms in a real-life setting.

3.3. *k*-Anonymity

Anonymity is defined in [22] as "the state of being not identifiable within a set of subjects, the anonymity set". A user is considered as k-anonymous, if and only if the location information reported is inseparable from the location information of at least $k-1$ other users. The idea of their framework is that a user reports to a client a cloaked region containing her position and the positions of $k-1$ other users instead of her exact position [13]. Due to inherent delay, this approach may not be suitable for services that need quick response. However, re-identification and location tracking risk can be reduced in this mechanism. Particularly, Bettini e*t al*. [23] propose a mechanism to provide *k*-anonymity guarantees for moving objects.

The basic concept of *k*-anonymity has been used by various approaches to increase the efficiency of *k*-anonymity, for example, clique cloak approach [24], personalized *k*-anonymity [16], [25], historical *k*-anonymity [23], and l- diversity [26], [27].

Personalized k-anonymity model [16] discusses about users having different privacy preferences based on different context and levels of privacy. It presents a few drawbacks in the existing anonymization mechanism [13] such as the mechanism involving users to specify different *ks* at different times and requiring a large value of *k* to be successful and also leads to bad quality of service (QoS) in LBS applications.

In the *l*-diversity mechanism [26] and [27], a user's location is unidentifiable from a collection of l different locations such as hospitals, restaurants, cinemas, pubs, etc. The *l*-diversity mechanism promises that the *l*-users positions are not only different but also they are located far enough from each other. If they do not differentiate this way, an adversary might know the specific victim user location with low imprecision because all the user positions might belong to the same semantic position.

A perturbation method is proposed in [28] to achieve geo-indistinguishability by adding random noise to the location of a user. Recently, the differential privacy mechanism [28] has become popular when compared to k- anonymity based mechanisms. Differential privacy is a notion of privacy that is in the area of statistical databases. It aims to protect single user information when publishing aggregate data.

Recent works in [29] and [30] have adopted entropy-based metrics to measurement the uncertainty of location privacy of a user. Basic and enhanced dummy location selection algorithms (DLS) [31] also utilize entropy metric to achieve k-anonymity. To ensure that the selected dummy locations spread out as far as possible, the dummy locations are chosen based on entropy metric. It has been shown through evaluation results that the enhanced DLS algorithm provides similar privacy levels as the basic DLS algorithm while enlarging the cloaking region.

Using a game theoretic approach [32], Liu *et al.* study the behaviors of self-interested users in a LBS system. The distributed dummy user generation is modeled as Bayesian games. A strategy selection algorithm is proposed to help users attain optimized payoffs.

3.4. Spatial Obfuscation

A popular spatial obfuscation mechanism [14] preserves location privacy by reducing the position information precision by sending a circular region to the location server when the user accesses LBS.

The advantage of spatial obfuscation approaches is that it provides location privacy without a fully trusted location server (LS). In addition, the user defines only an obfuscation area according to her preference. However, this advantage comes at the cost that the location service providers are not provided with a precise user location. Hence it decreases the quality of service. Also this mechanism does not provide user identity privacy, and superiority of information about an individual position is degraded in order to protect that mobile user's position.

3.5. Dummies

Another mechanism achieving location privacy is to mislead an adversary by sending multiple dummy

events (false positions) through an event injection method. Mechanisms in [18] and [33] mainly use this method. Generating a trace of events that seems to be a normal user's trajectory is one of the main challenges in these papers. An adversary can have some background knowledge of a user's sensitive context information such as a map and an address book, and can track the user for longer time to minimize user privacy.

3.6. Private Information Retrieval (PIR)

Cryptographic location privacy mechanisms in [17] utilize private information retrieval (PIR) to add and enhance location privacy. In a PIR approach, without disclosing/learning any query data, the location server answers a user's queries when she accesses LBS. The advantage of the PIR mechanism is that a compromised location server cannot disclose any user location information. The disadvantage of the PIR mechanism however is that the location server cannot execute computation on the shares, particularly range queries.

A drawback of PIR mechanism is the computation and communication overhead, making it hard to implement on handheld/portable devices. Also it is very difficult to service providers such as Google maps, as this will have more real time data.

3.7. Position Sharing

A framework in [34] executes location based queries like range queries while protecting location privacy of a user. The position sharing location privacy mechanism divides the obfuscated location information into position shares, such that each position share is restricted to strict precision. The work in [35] and [36] extends the framework to prevent an adversary from increasing the precision of locations by considering map knowledge.

4. Location Privacy Attacks

Before discussing the different types of attack, a structure of the attack model based on two factors, attacker knowledge and attack goals, will be presented. Each of these factors are explained in detail in the following sub-sections. The various attacks and their classification are then discussed. These location privacy attacks are classified based on background knowledge and position at the top level.

Location privacy attack in [37] describes that an attacker may utilize information about the distance between public knowledge on the average population density and information of users to find out a rough estimation of the user positions on the map. He may try to identify the positions of a moving object based on limited information on distance and on prior background knowledge of population density distribution. This attack is implemented in [37] to discover that an attacker can breach user's location privacy.

4.1. Attacker Knowledge

Attacker knowledge can be defined as, an adversary having prior knowledge of the system along with having access to the technologies that enables him to capture the events. The attacker may also have appropriate access credentials to the system which can enable him to alter the algorithm implemented by location privacy mechanisms. Having this knowledge, the adversary can learn location access profile of a user, where the access profile provides the probability of the user being at a particular location when accessing LBS.

A common approach to maximize location privacy is to replace the true locations with pseudo-locations. An adversary having prior knowledge of the user's access pattern can invert this protection mechanism and identify the user's actual location by correlating his observation of actual events with pseudo-locations.

4.2. Attacker Goals

A user's access to LBS database can be misused by an attacker by observing the user's movements and identifying if the user is present at a specific location or not. There are mainly three types of information that an attacker will target. These can be identified as user's identity information, spatial information, and temporal information that have been discussed in Section 2 as defense mechanism goals.

4.2.1. Identity

An adversary's goal is to obtain the identity information of a user to attack her private information. For instance, if the attacker has knowledge of the user's identity through his observation, he might devise an attack to access this user's bank account. This knowledge can evolve over time and the attacker can also correlate the relation between users, for example, a social network graph.

4.2.2. Space

Another important goal of an adversary is to obtain a user's spatial information. A user's access to LBS database can be misused by an attacker to observe the user's movements and to identify if the user is present at a specific location or not. An adversary might also estimate user's actual locations through his observation in his optimal attack.

4.2.3. Events

An attacker might have access to some actual events that are conducted before the observed time. Also an attacker might have some statistics/prior knowledge about typical users' behavior. For instance, he might know the probability of one particular event that can be executed by a user. An attacker could be aware of a user's mobility profile. For example, he might estimate the user's probability of moving from one location to another location in a particular time period.

4.3. Background Knowledge Based Attacks

In background knowledge based attacks [26], an adversary could have prior knowledge to exploit sensitive context information of a user. The adversary could also have external background knowledge of a user such as a map to minimize users location privacy. Background knowledge based attacks can further be classified into four different kinds of attacks: probability distribution attack, observation attack, identity matching attack, and map matching attack.

4.3.1. Probability distribution attack

In a probability distribution attack, an adversary can derive a probability distribution function of a user's actual location over the obfuscated area. If the probability is uniformly distributed, the adversary may make estimation error in identifying the user's true location. If the probability distribution is more concentrated around the user actual location (not uniformly distributed), an adversary can easily find out the true location of user with high probability [38].

4.3.2. Observation attack

An observation attack [26] is based on observation knowledge that evolves over time. This can be related to back- ground knowledge as the adversary gathers information through his observation. For example, consider an adversary knows that a user visits a restaurant regularly at a specific point of time and assume that the user is using a simple obfuscation mechanism to protect her location privacy. The adversary can maximize his known precision of an acquired obfuscation position by minimizing the obfuscation area to locations of restaurants within the obfuscated area. Another instance, assuming that a user is using pseudonyms and the adversary can view the observed user, then just by a single correlation, the adversary can trace back all the user's previous locations for the same pseudonym.

4.3.3. Identity matching attack

In an identity matching attack [15], the adversary can attack different pseudonyms of a user and based on corresponding attributes the adversary links these pseudonyms to the same identity such that the given

privacy for the changed pseudonym is nullified. Although a user makes use of some LPPMs, the adversary can utilize his background knowledge and correlate all the related pseudonyms by linking the user's spatial and temporal information.

4.3.4. Map matching attack

In a map matching attack [39], an attacker refines a user position in the obfuscation area by eliminating all the irrelevant areas in a certain location. For example, if the user position is on a bridge, the adversary can reduce the obfuscation area size around the user position by removing area like lakes. The adversary could make use of semantic data which is provided by a map to further hinder the effective obfuscated area, for example, user's points of interest (POI) or particular type of building such as restaurants, clinics, and pubs.

Table 2. Comparison of LPPMs, with "../" Denoting that the Corresponding Attribute Is Protected, and "x" Otherwise

Defense Mechanism Goals			LPPMs
spatial info.	temporal info.	user identity	
✓	✓	✓	mix zone [4]
✓	✓	x	spatial and temporal cloaking [15]
✓	x	x	spatial obfuscation [2]
✓	✓	✓	historical *k*-anonymity [6]
✓	✓	✓	PIR [14]
✓	✓	✓	*k*-anonymity (privacy-aware LBS) [28]
✓	x	x	dummies [16]
✓	x	✓	*l*-diversity: *k*-anonymity [24]
✓	x	x	position sharing [9]

Table 3. Comparison of LPPMs with Respect to Location Privacy Attacks

LPPMs	Resist prob. distribution attack	Resist observation attack	Resist map matching attack	Resist location tracking attack	Resist ho-mogeneity attack
mix zone [19]	Yes	Not known	Yes	Yes	Yes
spatial and temporal cloaking [13]	No	No	No	No	Yes
spatial obfuscation [14]	No	No	No	No	Yes
historical k-anonymity [23]	Yes	Not known	Yes	Yes	Yes
PIR [17]	Yes	Yes	Yes	Yes	Yes
k-anonymity (privacy-awareLBS) [31]	Yes	Not known	Yes	Yes	Yes
Dummies [18]	No	Not known	Yes	No	Yes
l-diversity: *k*-anonymity [26]	Yes	No	Yes	Not known	Yes
position sharing [34]	No	Not known	No	Yes	Yes

4.4. Position Based Attacks

In position based attacks, an adversary analyzes user updates on a mobile network to obtain more specific information about the user position or user identity that is intended to be hidden by using some LPPMs. An adversary can also track multiple position updates of a user and correlate them to minimize the user location privacy.

4.4.1. Identification attack

In this attack, an attacker finds the actual identity of his target victim. The attacker is mainly interested in de-anonymizing a particular observed event on a small scale or the attacker might be interested in observing and discovering the user identity of some anonymous track of events on a large scale. The identification attack is achieved through some inference attacks that are based on attacker's background knowledge on the

correlation of users to delicate area such user's office or home address.

As users most likely try to visit some places like restaurant and fitness center regularly, the identification could leverage on users mobility pattern or access pattern. It can be achieved indirectly by de-anonymizing [40], [41] a social network (e.g., friend-finding services) that is correlated to the user's observed events over time. If the attacker finds out the true trajectory moments of the user, then the user identification can be easily identified. Particularly when an attacker has some access to the user's location information like office address or home that includes a lot of private information about the user identity, the attacker would not find it difficult to track particular user's true trajectory.

4.4.2. Location tracking attack

Location tracking attack uses adversary's prior knowledge of multiple position updates of a user. For example, when a user provides positions of multiple pseudonyms, the adversary can try to rebuild the user's actual movement trajectory that has been distorted by a LPPM and can also identify the positions that a user has visited.

With this knowledge, an adversary can also predict future positions/locations of a user. Here, the adversary might be interested in knowing the user's coordinates (i.e., latitude and longitude information) that have been visited at a specific time period (e.g., particular hospital). The location tracking attack can be used against arbitrarily changing pseudonyms that are not making use of the mix zone mechanism.

4.4.3. Homogeneity attack

In homogeneity attack [26], an adversary can analyze all the positions/locations of k-users to check if the user positions are identical. If all the k-users' positions are more concentrated around the user's true location, then each user's position information will be disclosed. But if the users positions are distributed uniformly over a big area, the users' true location information is protected. This attack can be used against the simple k-anonymity approaches. If the adversary has some map knowledge, he can minimize the effective area size to locate a user's actual location.

Certainly, the classification of all these attacks is not absolute. Some attacks may take advantage of the knowledge of both background and position. For example, the identification attack and the location tracking attack listed under position based attacks exploit background knowledge to further tune the target.

5. Classification and Comparison of Location Privacy Preserving Mechanisms

Tables 2 and 3 gives a classification and comparison of the different privacy preserving mechanisms used in LBS. Each mechanism is focused on protecting certain attributes such as user identity, spatial information and temporal information based on defense mechanism goals and adversary knowledge. And each mechanism resists particular location privacy attacks and has its limitations as discussed in earlier sections.

The PIR mechanism [17] resists probability distribution attack by protecting user identity, spatial information, and temporal information. In case of spatial obfuscation [14], the probability distribution attack will be successful as mechanism only protects user's spatial location information and doesn't protect user's temporal information. Some of the major disadvantages of spatial obfuscation mechanism are that the mechanism can be inverted by an adversary (given an adversary with some prior knowledge about the algorithm implemented by obfuscation mechanism and user access pattern). Also, instead of retrieving a precise user position, the clients can retrieve only the obfuscation region. Some enhanced techniques have been proposed by researchers to address this issue.

Mechanisms like spatial obfuscation [14], dummies [18], spatial and temporal cloaking [13] are not aimed at resisting probability distribution attack [38], but their mechanisms can indirectly prevent some types of attacks like homogeneity attack [26]. On the other hand, mechanisms like private information retrieval [17], l-diversity, and k- anonymity [26], are designed to resist certain attacks such as probability distribution attack

[38]. However, they have their own limitations. Many approaches cannot protect multiple attributes against an observation attack.

6. Conclusion and Future Directions

The privacy of location information in the mobile computing environment is a serious issue that requires special considerations. In this paper, we present a survey on the mechanisms and attacks that are currently being used to deal with this issue of privacy. The location privacy preserving mechanisms are classified into cryptographic and non-cryptographic approaches. Moreover, we give classification of these location privacy mechanisms. In addition, we provide detailed comparison of these mechanisms and attacks are presented from the perspective of the fulfillment of defense mechanism goals and adversarial goals. Despite all the efforts made to enhance location privacy of the user sensitive information, there are certain areas and issues still open and need more attention. Currently, only PIR [17] mechanism can resist observation attack. In Table 3, the cells that are marked as "Not known" are potential areas for future research.

A user has to trade off between preserving maximum location privacy and the quality of service. A user may prefer to protect only the spatial information, without concerning about temporal/identity information, then the best approach in this situation is spatial obfuscation mechanism. One problem with obfuscation mechanisms is that the effective size of the targeted obfuscation area can be minimized if an adversary applies some prior knowledge (map knowledge). The adversary can derive a probability distribution attack function of the user actual location over the obfuscation area. If the probability is not uniformly distributed (i.e., distribution being more concentrated around the user actual location), an adversary can easily find out the true location of user with high probability. Hence privacy is dependent on the adversary, and neglecting adversary's knowledge and capabilities limits the privacy protection. Some approaches cannot protect different combinations of the attributes such as identity, spatial information, and temporal information against attacks. Therefore, the future research needs to consider user based protection and real-time protection along with considering different user habits or interests or preferences. Also the combination of different attacks where an adversary can apply his background knowledge like map information or personal context information to disclose delicate private information should be investigated.

References

[1] Facebook. Retrieved April 2014, from http://www.facebook.com/places/

[2] Foursquare. Retrieved April 2014, from http://www.foursquare.com/

[3] Loopt. Retrieved April 2014, from http://www.loopt.com/

[4] Qype. Retrieved April 2014, from http://www.qype.com/

[5] Pedreschi, D., Bonchi, F., Turini, F., Verykios, V., Atzori, M., Malin, B., Moelans, B., & Saygin, Y. (2008). Privacy protection: Regulations and technologies, opportunities and threats. Mobility*, Data Mining and Privacy*, 101–119.

[6] Mokbel, M. F. (2007). Privacy in location-based services: State-of-the-art and research directions. *Proceedings of 2007 International Conference on Mobile Data Management* (pp. 228–228).

[7] Shin, K., Ju, X., Chen, Z., & Hu, X. (2012). Privacy protection for users of location-based services. *Wireless Communications, 19(1)*, 30–39.

[8] Li, Q., & Cao, G. (2013). Providing privacy-aware incentives for mobile sensing. *Proceedings of 2013 IEEE International Conference on Pervasive Computing and Communications* (pp. 76–84).

[9] Krumm, J. (2009). A survey of computational location privacy. *Personal and Ubiquitous Computing, 13(6)*, 91–399.

[10] Chow, C. Y., & Mokbel, M. F. (2011). Trajectory privacy in location-based services and data publication.

ACM SIGKDD Explorations Newsletter, 13(1), 19–29.

[11] Shokri, R., Theodorakopoulos, G., Troncoso, C., Hubaux, J. P., & Le Boudec, J. Y. (2012). Protecting location privacy: optimal strategy against localization attacks. *Proceedings of the 2012 ACM Conference on Computer and Communications Security* (pp. 617–627).

[12] Liu, X., Zhao, H., Pan, M., Yue, H., Li, X., & Fang, Y. (2012). Traffic-aware multiple mix zone placement for protecting location privacy. *Proceedings of IEEE INFOCOM* (pp. 972–980).

[13] Gruteser, M., & Grunwald, D. (2003). Anonymous usage of location-based services through spatial and temporal cloaking. *Proceedings of the 1st International Conference on Mobile Systems, Applications and Services* (pp. 31–42).

[14] Ardagna, C. A., Cremonini, M., Damiani, E., Di Vimercati, S. D. C., & Samarati, P. (2007). Location privacy protection through obfuscation-based techniques. *Data and Applications Security XXI* (pp. 47–60). Springer.

[15] Beresford, A. R., & Stajano, F. (2004) Mix zones: User privacy in location-aware services. *Proceedings of PerCom Workshops* (pp. 127–131).

[16] Gedik, B., & Liu, L. (2005). Location privacy in mobile systems: A personalized anonymization model. *Proceedings of 25th IEEE International Conference on Distributed Computing Systems* (pp. 620–629).

[17] Ghinita, G., Kalnis, P., Khoshgozaran, A., Shahabi, C., & Tan, K. L. (2008). Private queries in location based services: anonymizers are not necessary. *Proceedings of the 2008 ACM SIGMOD International Conference on Management of Data* (pp. 121–132).

[18] Kido, H., Yanagisawa, Y., & Satoh, T. (2005). An anonymous communication technique using dummies for location-based services. *Proceedings of International Conference on Pervasive Services* (pp. 88–97).

[19] Beresford, A. R., & Stajano, F. (2003). Location privacy in pervasive computing. *Pervasive Computing, IEEE, 2(1)*, 46–55.

[20] Palanisamy, B., & Liu, L. (2011). Mobimix: Protecting location privacy with mix-zones over road networks. *Proceedings of 2011 IEEE 27th International Conference on Data Engineering* (pp. 494–505).

[21] Bindschaedler, L., Jadliwala, M., Bilogrevic, I., Aad, I., Ginzboorg, P., Niemi, V., & Hubaux, J. P. (2012). Track me if you can: On the effectiveness of context-based identifier changes in deployed mobile networks. *Proceedings of the 19th Annual Network and Distributed System Security Symposium*.

[22] Pfitzmann, A., & Ko¨hntopp, M. (2001). Anonymity, unobservability, and pseudonymitya proposal for terminology. *Designing Privacy Enhancing Technologies*, 1–9.

[23] Bettini, C., Mascetti, S., Wang, X. S., Freni, D., & Jajodia, S. (2009). Anonymity and historical-anonymity in location-based services. *Privacy in Location-Based Applications*, 1–30.

[24] Pan, X., Xu, J., & Meng, X. (2012). Protecting location privacy against location-dependent attacks in mobile services. *IEEE Transactions on Knowledge and Data Engineering, 24(8),* 1506–1519.

[25] Gedik, B., & Liu, L. (2008). Protecting location privacy with personalized k-anonymity: Architecture and algorithms. *IEEE Transactions on Mobile Computing, 7(1),* 1–18.

[26] Machanavajjhala, A., Kifer, D., Gehrke, J., & Venkitasubramaniam, M. (2007). l-diversity: Privacy beyond k-anonymity. *ACM Transactions on Knowledge Discovery from Data, 1(1),* 3.

[27] Bamba, B., Liu L., Pesti, P., & Wang, T. (2008). Supporting anonymous location queries in mobile environments with privacygrid. *Proceedings of the 17th International Conference on World Wide Web* (pp. 237–246).

[28] Andres, M. E., Bordenabe, N., Chatzikokolakis, K., & Palamidessi, C. (2013). Geo-indistinguishability: Differential privacy for location-based systems. *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security* (pp. 901–914).

[29] Niu, B., Zhu, X., Chi, H., & Li, H. (2013). 3plus: Privacy-preserving pseudo-location updating system in

location-based services. *Proceedings of IEEE Wireless Communications and Networking Conference* (pp. 4564–4569).

[30] Zhu, X., Chi, H., Niu, B., Zhang, W., Li, Z., & Li, H. (2013). Mobicache: When k-anonymity meets cache. *Proceedings of IEEE GLOBECOM.*

[31] Niu, B., Li, Q., Zhu, X., Cao, G., & Li, H. (2014). Achieving k-anonymity in privacy-aware location-based services. *Proceedings of IEEE INFOCOM*.

[32] Liu, X., Liu, K., Guo, L., Li, X., & Fang, Y. (2013). A game-theoretic approach for achieving k-anonymity in location based services. *Proceedings of IEEE INFOCOM* (pp. 2985–2993).

[33] Krumm, J. (2009). Realistic driving trips for location privacy. *Pervasive Computing*, 25–41.

[34] Durr, F., Skvortsov, P., & Rothermel, K. (2011). Position sharing for location privacy in non-trusted systems. *Proceedings of 2011 IEEE International Conference on Pervasive Computing and Communications* (pp. 189–196).

[35] Skvortsov, P., Du¨ rr, F., & Rothermel, K. (2012). Map-aware position sharing for location privacy in non-trusted systems. *Pervasive Computing*, 388–405.

[36] Wernke, M., Durr, F., & Rothermel, K. (2012). Pshare: position sharing for location privacy based on multi-secret sharing. *Proceedings of 2012 IEEE International Conference on Pervasive Computing and Communications* (pp. 153–161).

[37] Mascetti, S., Bertolaja, L., & Bettini, C. (2012). Location privacy attacks based on distance and density information. *Proceedings of the 20th International Conference on Advances in Geographic Information Systems* (pp. 514–517).

[38] Shokri, R., Theodorakopoulos, G., Le Boudec, J. Y., & Hubaux, J. P. (2011). Quantifying location privacy. *Proceedings of 2011 IEEE Symposium on Security and Privacy* (pp. 247–262).

[39] Krumm, J. (2007). Inference attacks on location tracks. *Pervasive Computing*, 127–143.

[40] Narayanan, A., & Shmatikov, V. (2009). De-anonymizing social networks. *Proceedings of 30th IEEE Symposium on Security and Privacy* (pp. 173–187).

[41] Wondracek, G., Holz, T., Kirda, E., & Kruegel, C. (2010). A practical attack to de-anonymize social network users. *Proceedings of 2010 IEEE Symposium on Security and Privacy* (pp. 223–238).

Sahana Shivaprasad is a graduate student (MS) at the Department of Computer and Information Sciences at Indiana University-Purdue University Indianapolis. Her research interest is network security.

Huian Li is a graduate student (PhD candidate) at the Department of Computer and Information Sciences at Indiana University-Purdue University Indianapolis. His research interests include applied cryptography, network security, and scientific applications and performance tuning.

Xukai Zou is a faculty member with the Department of Computer Sciences at Indiana University-Purdue University Indianapolis (IUPUI). His current research focus is applied cryptography, network security, biometrics, authentication and electronic voting. His research has been supported by NSF, the Department of Veterans Affairs and Industry such as Cisco and Northrop Grumman.