A Survey of System Architectures, Privacy Preservation, and Main Research Challenges on Location-Based Services

Mulugeta K. Tefera[1], Xiaolong Yang[2] and Qifu Tyler Sun*
[1,2,*]University of Science and Technology Beijing
Beijing, 100083-China
School of Computer and Communication Engineering
[e-mails: [1]mulugetaksw@gmail.com, [2]yangxl@ustb.edu.cn]
*Corresponding Author: Qifu Tyler Sun (e-mail: qfsun@ustb.edu.cn).

Received October 8, 2018; revised January 12, 2018; accepted February 20, 2019;
published June 30, 2019

Abstract

Location-based services (LBSs) have become popular in recent years due to the ever-increasing usage of smart mobile devices and mobile applications through networks. Although LBS application provides great benefits to mobile users, it also raises a sever privacy concern of users due to the untrusted service providers. In the lack of privacy enhancing mechanisms, most applications of the LBS may discourage the user's acceptance of location services in general, and endanger the user's privacy in particular. Therefore, it is a great interest to discuss on the recent privacy-preserving mechanisms in LBSs. Many existing location-privacy protection-mechanisms (LPPMs) make great efforts to increase the attacker's uncertainty on the user's actual whereabouts by generating a multiple of fake-locations together with user's actual positions. In this survey, we present a study and analysis of existing LPPMs and the state-of-art privacy measures in service quality aware LBS applications. We first study the general architecture of privacy qualification system for LBSs by surveying the existing framework and outlining its main feature components. We then give an overview of the basic privacy requirements to be considered in the design and evaluation of LPPMs. Furthermore, we discuss the classification and countermeasure solutions of existing LPPMs for mitigating the current LBS privacy protection challenges. These classifications include anonymization, obfuscation, and an encryption-based technique, as well as the combination of them is called a hybrid mechanism. Finally, we discuss several open issues and research challenges based on the latest progresses for on-going LBS and location privacy research.

Keywords: Location-based services, mobile user, privacy, location attacks, privacy protection mechanisms

http://doi.org/10.3837/tiis.2019.06.024 **ISSN : 1976-7277**

1. Introduction

Recent advances in mobile computing makes location based service (LBS) increasingly popular, which attract millions of individuals. LBS refers to a location information and convenient services provided to mobile users based on the geographic position and other information of users' mobile devices to obtain their real location data [1]-[2]. In this context, user oriented LBS applications are developed to obtain location related information relevant to their current position and surroundings. Common examples include direct location sharing with friends (e.g., uploading real-time location data and tagging services) and sharing with business sectors (e.g., search for near-by services, location check-in and search near-by friends), which help the user to share and determine their current position with friends in the communication networks [3]-[4]. Other typical examples of LBS applications include map applications (e.g., Google Maps), point of interest retrieval (e.g., Around-Me), coupons or discount offers (e.g., Group-on), GPS navigation (e.g., Tom-tom) and location-aware social networks (e.g., Face-book, Weibo, Foursquare, Wechat) [5]. A more large-scale LBS application could ask users around a region or even country to disclose their exact locations for security and safety purpose (e.g., in military, medical care, emergency relief, people's livelihood, etc [6].

However, while the convenient services provided by LBS brings great benefits to mobile users, their usage can also raise a serious privacy risks derived from the disclosure of user locations. The reason for this is that when users conveniently access various LBSs, they need to report their real-time location information and other related service attributes in the communication network. The context attached to this location information contains not only location privacy, but also other sensitive personal information that the user usually wants to protect them, such as health status, living habits, home address, and social relations [7]-[8]. Therefore, once the private information is leaked due to untrusted third parties (such as LBS providers), and then it would result in opening a door to abuse of personal data and posing a serious threats to all aspects of the user's privacy. For example, a malicious attacker or adversary using prior knowledge can re-identify personal home and work address from location traces (anonymous GPS data) [9]-[10], predict the user's past, present and future positions [11], and then infer the whereabouts of the individual from the frequency of their visits to a particular locations[12]-[13]. This problem has received significant attention from Smartphone users, LBS providers, research community, etc. Therefore, there is a growing interest in protecting the user's location privacy and private information from malicious attackers when using LBSs and media tag services.

A number of research works have focused on developing LPPMs that allow users to modify actual locations disclosed to the LBS provider using different types of protection strategies [14-16]. These protection mechanisms help to improve the adversary's ambiguity on the user's real positions by running a multiple of locations from where various consecutive queries have reported by mobile users. In the context of LBSs, various LPPMs, such as user anonymization (random permutation) [17], location obfuscation [18] and encryption-based mechanisms [19], are further proposed to allow users in LBSs. The most popular and widely used LPPM to protect user positions is obfuscation-based mechanism, which consists of reporting fake-locations or noisy version of their location information to the service provider. A different LPPM consists of hiding some regions of users' positions using mix zones) [20]-[21]. Using this mechanism, several users do not link with service provider by changing their pseudonym and prevent an adversary from attacking them. Another LPPM consists of adding location dummies to protect user's real location by reporting multiple false locations (dummies) to the LBSs provider together with the actual location [22]. The purpose of adding fake or dummy-locations is to increase the adversary's uncertainty on the users' real movements.

While these existing LPPMs are significant advantages, their implementation and evaluation methods also bring new problems and challenges. For example, generating high cost of dummy locations using resource constrained mobile devices over all LBS applications will be economically expensive in terms of resource consumption costs [23]. These are however likely to be an issue for self-interested LBS users in reality, since most applications are accessed from Smartphone devices and the users may not be sufficiently motivated to access them. Therefore, the presence of such malicious or selfish behaviors may have an adverse effect on privacy protection system. For these challenges, an effective protection design methods, such as adaptive and optimal clustering methods, are useful to account for resource limitations (e.g. reduce energy and bandwidth consumption) [24-26]. In addition, there are some LBS applications that require the mobile users to access them continuously (rather than sporadically), and on the other side, there are the majority of LBSs, such as various nearby points-of-interest search services where users reveal their location sporadically (rather than continuously). In this case, there are two successive accesses of a user to the LBS access pattern with non-negligible gaps in time. Therefore, an effective protection mechanism needs to secure in LBS applications when users to share their location continuously and sporadically over space and time [27]. Another important issue is that of the effectiveness of protecting the users' privacy and service quality requirements. For example, possible protection challenges include designing effective LPPMs together with the generic adversarial model and objectives, respecting and incorporating the user's service quality requirements and sensitivities. In particular, the assumption about designs of effective yet useful LPPMs tend to be incomplete, without adversarial knowledge and objective to track the users visiting particular locations [28]. Obviously, there is a mismatch between the designs of these LPPMs and the objective comparison results of them without considering a generic adversarial model. To be consistently model the goals and results of various LPPMs together with the adversary's objective and knowledge, new mechanisms to preserve the user's location privacy and service quality requirements are needed. In this respect, several authors have been recently presented toward formalizing the users' accesses to LBS and their desirable service quality and location privacy requirements, modeling various LPPM, and their suitable privacy metrics to evaluate the performance of the corresponding LPPMs [29-31]. These contributions support the foundation that establishes the relationships between different popular types of LBS privacy metrics. The quantification and protection models allow us to specify the existing evaluation methods for LPPM that explicitly accounts for a generic adversarial model for privacy metrics. This is a key issue in LBS and media-tagged service systems and therefore, it is a considerable attention of this survey paper.

In this paper, we survey the state-of-the-art research efforts for LPPMs applied in LBS applications. After a general description of privacy quantification framework and its main components, we analyses the potential privacy risks associated with LBSs, the architecture, and evaluation of LPPMs and then address some countermeasure solutions. For this purpose, we adopt the popular LPPMs, such as user anonymization, location obfuscation, encryption-based methods, and the combined system (hybrid mechanism) to address the current LBS privacy protection challenges. Finally, we highlight the most important issues to be considered in the design and evaluation of LPPMs, and then discuss several open research challenges based on the latest progresses in the topic of location privacy and the research community.

We present the structure of our contributions as follows. Section 2 describes the general system architecture of privacy quantification framework. Section 3 introduces LBS privacy requirements and performance metrics. Section 4 presents the state-of-art privacy measures and comparison analysis. Section 5 provides several open research challenges. Finally, Section 6 concludes our discussion with summary.

2. Overview of Privacy Quantification Framework

In order to understand the LPPM and attack strategies deployed in a various LBS, we first need to know the structure of the general framework for privacy quantification and its main components that affect the location privacy of mobile users. Therefore, in this section we first present the general framework for the user's mobility and their access patterns to LBSs, and then describe its main components, as shown in **Fig. 1**. As shown in the figure, the framework consists of the following three main components [27], [30]. (i) A mobile users, a user's mobile devices are equipped with an integrated position sensor that uses a variety of positioning technology to access the LBS at different instant of times. (ii) The trusted system (LPPMs), which provide location privacy guarantees for mobile users before sending the user's real location trace to the LBS. What is the user's actual location when accessing LBS? The LPPM wants to protect the actual location(s) by producing appropriate pseudo-location(s).

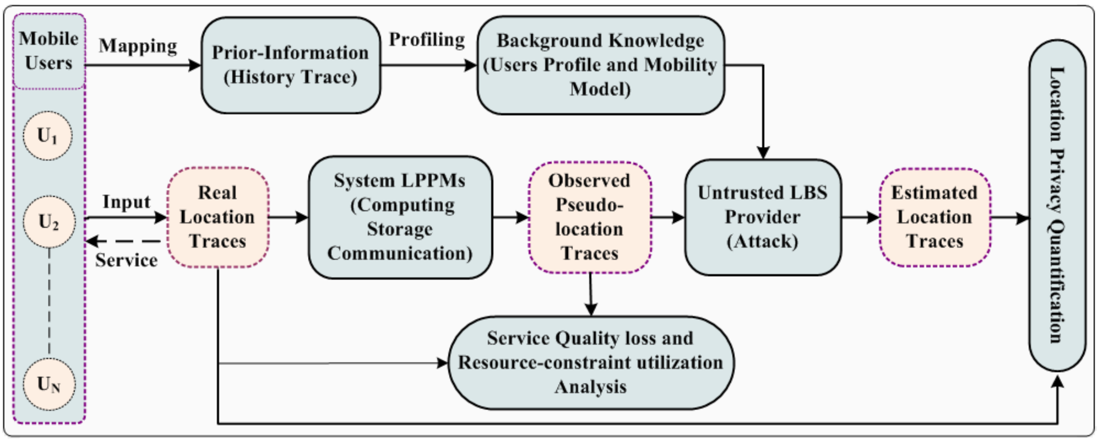
Mobile Users
U1
U2
UN
Mapping
Prior-Information (History Trace)
Profiling
Background Knowledge (Users Profile and Mobility Model)
Input
Service
Real Location Traces
System LPPMs (Computing Storage Communication)
Observed Pseudo-location Traces
Untrusted LBS Provider (Attack)
Estimated Location Traces
Service Quality loss and Resource-constraint utilization Analysis
Location Privacy Quantification

Fig. 1. General block diagram for user-specific privacy and quality-loss quantification model

Hence, when accessing the LBS, users only expose the output of LPPM, instead of sharing their actual locations and the adversary can infer it by the observed location traces. The existing LPPMs mainly include pseudonyms (removing the user's identity and using a temporary-identity), randomization (adding dummy locations), and obfuscation mechanisms (spreading or perturbing spatiotemporal information in queries). (iii) untrusted LBS providers (i.e., an adversary, who strives to observe the private information of mobile users exposed to the LBS). When a user uses various LBS applications, the service provider collects the user's information or service attributes attached to the location-related information.

The location-privacy of mobile users and the success rate of the adversary in his location tracking attacks on the impact of users' queries are two sides of one coin, which are highly interconnected together using LBS evaluation metrics. Given the users' observed location traces and a certain constraints of users' mobility profiles, the adversary tries to speculate and then infer the user's real location traces [11]. Hence, the users' obtained service quality and location privacy degree that they experience is evaluated given the users' real location traces, the result attack and output of LPPMs. Therefore, we describe two main evaluation metrics to evaluate the utility loss caused by the distortion of the original query and the cost of privacy decision made by the adversary. These evaluation metrics are the service-quality loss and energy cost metrics that incurred by using different types of LPPMs and location privacy of users (equivalently estimation error for adversary) under some location inference tracking-attacks. For the rest of this paper, we discuss the location privacy issues and potential threat model associated with LBSs, the existing LPPMs and their performance evaluation metrics for quantifying the privacy gain and use's obtained service quality.

3. Privacy Requirements and Threats in LBSs

Although LBS applications undeniably provide novel capabilities in terms of localization service through mobile and GPS (Global Positioning System), they can put the privacy of the mobile users at LBS provider. Obviously, the collected location information embedded in LBSs should have localization error and therefore used to extract (infer) sensitive private information about user's service request and responses. For example, we have mentioned earlier that most applications of LBS collect the location information attached in the LBS queries. The adversary can track the history of the user from the anonymous GPS data, and then infer the user's personal home address, work unit and social relations, etc. [9-11].

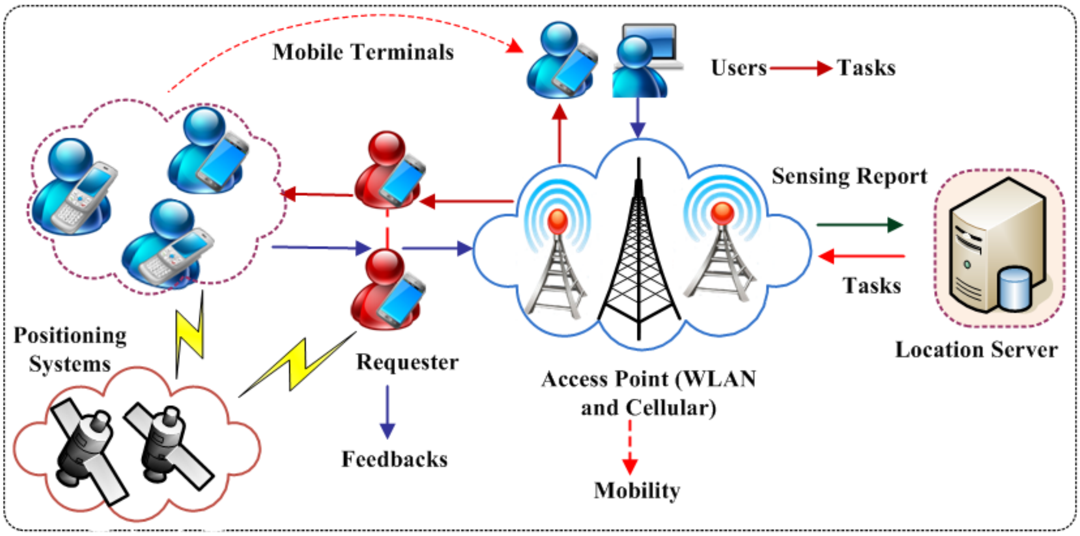

Fig. 2. A common client server system architecture

In location-aware smart mobile devices, it has become inevitable to protect the privacy assets of users from malicious attackers or untrusted-service providers for the maturation of a healthy LBS ecosystem. Therefore, the user's location information requires certain privacy measures to guarantee the obtained service quality and resource utilization constraints at all the times. The respect of the privacy of the mobile users primarily depends on the trusted LBS server who has direct access to the collected location information and ensures their response to end users.

The major location privacy requirements to ensure the safety of a LBS system and its extensive acceptance by its users are evaluated as follows: The first requirement is formalizing the desirable location privacy strategies that LPPMs should consider the user's service quality, location privacy and resource utilization costs that satisfy each user's requirements. LBS privacy protection strategy needs to protect the privacy of user's location while taking into account the quality of service and resource optimization cost (e.g., battery and bandwidth consumptions). The second requirement is based on incorporating the user's data model from anonymous and/or perturbed-locations. Otherwise, the adversary depends on users' prior knowledge and infers their activity traces when they visit a certain locations. The third and the most essential requirements are finding the right evaluation metrics to determine the degree of privacy in which the LPPMs' requirements are satisfied. In **Fig. 2**, we identify typical client-server system architecture common to the existing LBS architecture, where location information moves in the communication network and available with location server. We next define the architectural components conducted against the system depicted in **Fig. 2** and determine the possible location privacy attacks in the general system model.

3.1 LBS Privacy Threats

The system architecture shown in **Fig. 2** consists of four major components: the mobile terminal users, positioning systems, wireless communication networks, and location service provider. As shown in the figure, the system architecture empower LBS users through a range of mobile terminals (e.g. Smartphone and tablets) transmits location query to the service provider. Each user has GPS enabled smart mobile devices mounted with them, which will play part of location-enabled and media-tagged services. The mobile user uses a variety of positioning system (such as, localization through GPS) to request a service attributes in his nearest service of interest (e.g., hospitals) through communication networks (e.g., cellular network or WLAN). The location server (also known as LBS provider) responds to the user's query and then returns the customized result. For each request of service attributes, the server will return a small number of points of interest that match the user-specified service attributes. While a user conveniently accesses the various LBS applications, their location privacy may leak in the following three major parts (points), i.e., user's mobile devices, communication networks and location server by itself. However, the user's location-aware mobile device may also be identified (hijacked) based on the collected location information attached in the LBS queries [7]-[8]. Therefore, how to prevent the secuirity of users' mobile device from tracking them is also a vital importance to the well-being of LBS application [28], [29]. Secondly, the user's LBS query and customized results may be eavesdropped or subjected to man-in-the-middle attacks when transmitted over the wireless network. Apart from the user's mobile device and query results, the LBS server by itself can also be endangered. Assuming that a malicious or selfish attacker may be the LBS server itself and collects the user's location information or service attributes contained in the service query. By doing so, the LBS provider transmits location data through the wireless network and may provide knowledge to the malicious attackers (third-party adversarial entities) about themselves. With this knowledge, the malicious attacker or the owner of LBS could speculate, and then infer the user's sensitive data [8]. To simplify privacy protection issues, a generic privacy attack model assumes that the untrusted LBS provider is malicious or untrustworthy and system LPPM is secure and trustworthy. However, the LPPM's implementation often based on the attacker's prior knowledge about user's overall location traces. When the attacker (untrusted service-provider) understands the user's choice of LPPMs, it will use the prior knowledge to update his attacking strategy and effectiveness. The existing LPPMs such as trusted third party anonymizers (e.g., a trusted cellular service provider) and obfuscation mechanisms are also not matured to provide users' location privacy guaranteeing during services [32]-[33]. We next discuss the existing LPPMs for LBSs that takes a generic threat model in account. We also analyze how the adversary technically observes the users' location traces during designing and evaluation of various LPPMs.

3.2 LPPM Strategy and Functionality

After introducing the privacy issue and possible threats to privacy in the previous section, we now give an overview of existing LPPM's functionality to achieve the desirable location privacy of users. There are a large number of research works focuses on developing the state-of-the-art LPPMs to protect the user's location privacy [34-37]. These protection mechanisms are based on sending (reporting) a fake-locations and adding dummy-locations to the LBS [38] or hiding the real posisions of users by using mix-zones [39]-[40], anonymization and obfuscation mechanisms, in order to increase the adversary's uncertainty on the user's real positions. The first two protection mechanisms (i.e. hiding user's location, and reporting a fake-location) generates multiple set of user's positions together with real locations. The later two protection mechanisims are obfuscation mechanism used to modify a space-or time-obfuscated and location-stamps [18], [20]-[21], and location-anonymization (removing the user's real-identity) and replace by *k*-user location identity.

The earliest and most popularized mechanism to preserving data anonymization is location k-anonymity, which was first provided by [18] to determine the degree of user's privacy in anonymous networks. Location k-anonymity is an extensive-general privacy concept, and many works regarding location privacy-protection stemmed from the k-anonymity model. Using this mechanisms, the users' real-location R, is generated (modified) to separet the relation between adaptive adversary and LBS user, as illustrated in **Fig. 1**. To perform this end, the transformation function generates the real location R to other observed location and replaced by one of his valid pseudo-location R'. For instance, the spatio-temporal cloaking are the traditional mechanisms to protect location-privacy [18], [20], [39]. However, even though the spatial-cloaking mechanism gives a very good solution for privacy protection, it ignores the part of data integrity. To overcome the problem, several authors have been made a significant effort [39]-[40] to balance between location-privacy and service utility (data-integrity). Besides location *k*-anonymity, several other mechanisms have been applied using mix-zones to hide the actual-location of users. A mix-zone is an area of regions used to break the linkage between user and service-provider by changing their pseudonym [34], [41]. Therefore, when several users enter a mix-zone at the same time, this LPPM can effectively prevent an adversary from tracing them. Another popular mechanism to protect the privacy of users' location is based on adding dummy events [42]-[43], so that the real-locations are indistinguishable from the fake-locations, which have been generated to the syetem's service-provider. The purpose of this mechanism is to update the adversary's uncertainty by sending a multiple false-locations to the LBS observer together with user's true-location.

However, the evaluation of the existing LPPM's design strategy mostly ignores the reality that the adversary might have some previous experience and prior-knowledge about users' LBS access patterns and about the logic of internal-algorithm provided by the given LPPM. In order to capture the effectiveness of LPPMs, we abstract away the models for representing users' mobility and LPPM as as a single unit that separates the user's actual location traces and the adversary. **Fig. 3** shows the potential elements associated with LPPMs work through three main architectures [27]. These are centralized (server-side), distributed (user-side), and hybrid system architectures**.**

(i) Centralized (server-side) architecture; in this architecture, the user uses location-aware mobile devices to send the LBS query to the service provider and then obtained the final query result. The trusted anonymous server acts as an internal-anonymizer (privacy proxy server) that generates users' location information before sending to the service anonymizer. Advantages of this structure include that it is simple to design, the communication overhead between the mobile terminal and the anonymous server is small. However, the disadvantages include that: (a) anonymous third-party system-server may become the performance bottleneck and the only attack point of the system; (b) anonymous server has complete knowledge of location information or service attributes of all users. Once an anonymous provider is compromised, a singular point of failures may cause a serious privacy threat that all users can be compromised; (c) in reality, it is difficult to design and implement a trusted anonymous server with a broade-range of applications.

(ii) Distributed (user-side) architecture**;** in this architecture instead of letting each users report their position directly to the LBS server, users are organized in a separate peer-to-peer network, which provides all users' positions in a group, and forwards the group to service provider. At the same time, the service provider can give the correct result. The LPPMs are performed by candidate sets of users through cooperation by each user. Advantages of this architecture include: (a) eliminating the performance blockage of the system; (b) having the user's global information, so privacy protection effect is good. The disadvantage of this architecture includes (a) the mobile terminal communications and computing overhead increase compared with central architecture. This indicates that the distributed architecture is harder to design, and difficult to perform in real applications, because it cannot effectively ensure that other users involved in privacy protection are trusted; (b) when a user requesting a service does not have enough peers in the vicinity, the anonymous process is difficult to complete.

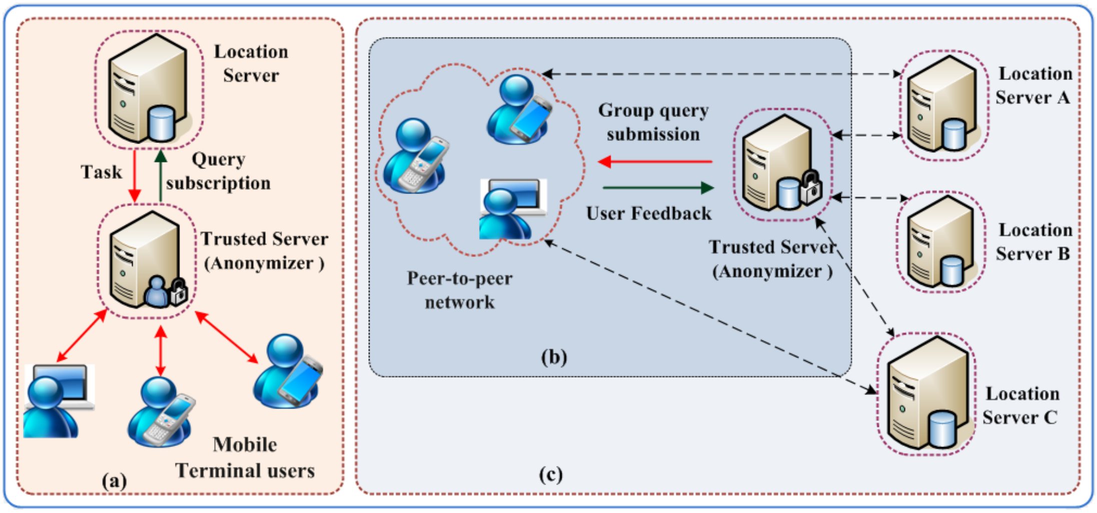

Fig. 3. A common LBS system architecture (a) Centralized (server-side) (b) Distributed (user-side) (c) hybrid architecture

(iii) hybrid architecture: the third type of protection architecture can be a hybrid of both server-centric (centralized) and distributed (user-centric) architectures. In this architecture, a mobile terminal user requests the service through a trusted anonymous server, which has complete knowledge of the user's identity, service request and real location, etc. The candidate sets use a peer-to-peer network to complete privacy protection based on personalized privacy, response time, and service quality requirements. The hybrid system architecture unifies the advantages of a centralized and a distributed architecture that can well balance the load between the client (user) and the anonymous server [44]. Its shortcoming is that there are a various system parameters, and the setting and adjustment are very complicated, so that its practicability has been seriously affected.

3.3 The Performance Metrics for LPPMs

In this section, we present intuitive privacy evaluation metrics in order to qualitatively evaluate and then compare the effectiveness of the corresponding protection mechanisms. The existing evaluation methods for LPPM targets mostly on sporadic-location and correlated settings at the time of LBS query issuing, and infrequently consider a trajectory-aware mechanism from where a number of queries are issued [6]. The major privacy quantification challenges to evaluate the performance of LPPMs are finding the right privacy metrics and incorporating user's mobility model to which the desirable location privacy requirements are satisfied. In the topic of LBS and media-tag services, numerous privacy measurement methods have been presented to evaluate the privacy degree of users [27], [45-47]. Examples of these privacy metrics are uncertainty-based (location-entropy), k-anonymity, location ℓ-diversity, expected error-based estimator, ε-differential privacy, etc. For example, the authors of [47] propose a distortion-based privacy metrics to evaluate the various LPPMs and classify them in three categories: location-k-anonymity, location-entropy (uncertainty-based), and expected distance error (error-based). However, most of these privacy metrics are more specific to certain applications and concrete attack objectives, and therefore it is difficult to conclude for other frame of references [31]. The studies have shown that these privacy metrics are inappropriate for evaluating user's location privacy, even for a particular case, various LBS privacy metrics can be exist. Because, once the location tracking attack model changes, the LBS privacy metric is not sufficient for evaluating the impact of query behavior on corresponding LPPMs performance. Therefore, it is still not clear which privacy metric is most suitable for a given privacy protection scenario [6]. Recently, a comprehensive comparison of existing privacy quantification methods has been proposed in prior research to address these problems. For instance, a similar but more commonly used expected error-based framework was further proposed in [27], [37] and [48]-[49] to formalize the impact of location accuracy associated with attacker reasoning attacks. This method can be applied to any attack model that correctly defines the distance between the actual-location of users and attacker's estimated value. However, this method also considers the quality of service and user attributes. This framework allows an adversary to understand the user's location access patterns and logic of LPPM strategy, and then to capture user's identity. Different research works also have adopted this analytical framework as an evaluation method and further applied to quantify location privacy, taking in to account the attack model, privacy threats, LPPMs' evaluation methods, privacy metrics and other factors affecting user's privacy. For example, the authors of [48] proposed a unified privacy quantification model, which can comprehensively compare the effectiveness of various LPPMs and evaluation metrics in different attack models.

In later work, without considering any possible background knowledge possessed by the adversary, differential privacy [50] has become popular for quantifying location privacy. However, the authors justified their invent work by extending the notation of differential privacy to the optimal sporadic-location privacy, and then defined the formal notation of geo-indistinguishability to quantify the observed information lekeage incured by LPPMs.

4. The State-of-the-art Countermeasures

In the LBS privacy protection community, protecting the user's privacy is a basic requirement for the successful deployment of LBS and media-tagged service applications. Currently, a number of privacy protection mechanisms have been proposed to enhance user privacy, but no single strategy can provide a complete solution. We herein present the current state-of-the-art privacy measures that address the major privacy threats highlighted in Section 3.1. For this purpose, we build upon a user-specific protection model common to the existing privacy quantification model, which represents the information sharing between an adversary and the user [30], as shwon in the **Fig. 4** below. For each studied countermeasure solutions, **Table 1** summarizes the classification, architecture, privacy threats, and service quality loss/resource overhead of the different LPPMs. Note that, we consider that the defense (relative to the attack) takes into consideration the attack (relative to the defense), which is imposed by the adversary. In addition, the solution also consider that the adversary observes the user's profile *ψ(r)* and output of LPPM, as well as the resource constraints in terms of quality-loss Q_{loss}^{max}, bandwidth $B_{\cos t}^{max}$ and energy cost $E_{\cos t}^{max}$ requirements. For this context, according to the work in [30], the system model allows us to specify the current state-of-the-art privacy measures with respect to different attacks. This is because most of the existing proposals mostly focus on preserving users' LBS privacy at the instant time of query issuing, and few are done on the trajectory privacy of users raising a several-number of successive locations. Our privacy measure uses this analytical model as an evaluation method to quantify the different levels of user's privacy requirements, measuring the privacy protection effect and service availability.

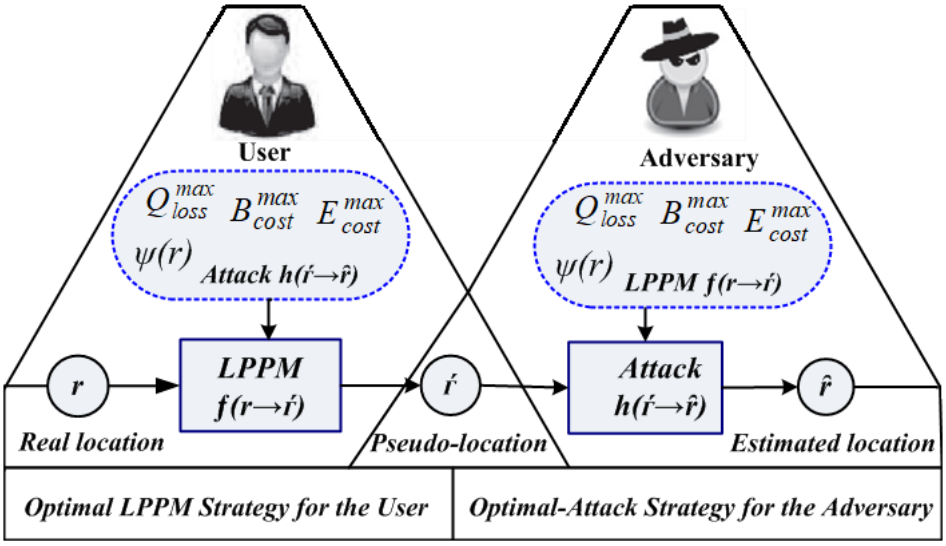
User
Q_{loss}^{max} B_{cost}^{max} E_{cost}^{max}
$\psi(r)$
Attack $h(\acute{r}\to\hat{r})$
Adversary
Q_{loss}^{max} B_{cost}^{max} E_{cost}^{max}
$\psi(r)$
LPPM $f(r\to\acute{r})$
r
LPPM $f(r\to\acute{r})$
ŕ
Attack $h(\acute{r}\to\hat{r})$
r̂
Real location
Pseudo-location
Estimated location
Optimal LPPM Strategy for the User
Optimal-Attack Strategy for the Adversary

Fig. 4. Information sharing between user and adversary in user-specific protection model

We assume that the mobile users want to preserve their location information and corresponding LBS access traces from malicious attacker (an untrusted observers) that can observes the location exposed to the LBS. Specifically for protecting location privacy, several LPPMs and evaluation methods have been proposed in order to address the current LBS privacy protection challenges. These popular approaches can be categorized as anonymization (removing the user's actual location), obfuscation (reporting a fake or noisy version of their location) and encryption-based techniques (using cryptographic tools) [51], which are outlined as follows.

4.1 Anonymization-based Mechanisms

These mechanisms aim to protect the privacy threats associated with LBSs transforming the user's real location information in to a generalized service query that represents a group of users, e.g., location anonymization methods for snapshot queries [37], trajectory anonymization methods for continuous queries [52]-[53], etc. We consider as an example that, Alice uses a smartphone and request queries to a LBS provider for the nearest hospital and then the LBS server calculates the set of users and service request area based on its known user's locations. Due to untrusted LBS server, Alice's sensitive information may be compromised or misused. Without using anonymization mechanism, this access service could disclose to the adversary that Alice has health condition problems. Therefore, it is required that all calculated anonymization set of users sent to the LBS server to share the same service request area such that the LBS server cannot directly interact with the issued position to the original location of Alice. The basic concept of anonymization mechanism has been extended by various important mechanisms to increase privacy protection. The following are the most prominent extensions in this category, not to be discussed in depth here, and interested readers can refer to the literatures. These are k-anonymity [54], Tessellation [55], l-diversity [56], micro-aggregation [57], data aggregation [58], t-closeness [59], and historical k-anonymity [60].

4.2 Location Obfuscation-based Mechanisms

The most prominent mechanism to protecting location privacy is to send a location-stamp version of the users' real locations to the LBS provider. Examples of these protection mechanisms are position sharing [1], [61], random perturbation [62]-[63], point-of-interest [64]-[65], negative survey [19], [66]. In these mechanisms, the privacy protection is achieved by generating each user's real location r in to an observed pseudo-location (obfuscated location) $\acute{r}$ before reporting them to the LBS. This transformation is made according to a probability distribution $f(\acute{r} \backslash r)= Pr(\hat{r} \backslash \acute{r})$. Hence, the user exposes its pseudo-location r' to the LBS provider instead of its actual location r. The main idea of this mechanism is that a user reports an observed pseudo-locations $\acute{r}$ to a LBS provider or a LBS containing his location information instead of his actual location r i.e., protected by LPPM.

4.3 Encryption-based Mechanisms

In these mechanisms, privacy protection is achieved by using the cryptographic methods to make the user's LBS query invisible to the LBS server [67]-[68] (e.g., group signature [69], double encryption [70]). Encryption-based LPPM adopts a distributed architecture, which cannot reveal any user's location information while ensuring service availability, and achieves more stringent privacy protection, such as LBS privacy protection based on private information retrieval. However, although the recently proposed homomorphic encryptions [71] are available for LBS query results without decrypting user queries, one important problem is that these mechanisms do not consider privacy metrics and then the efficiency is still a big problem to provide full protection of location privacy. Therefore, there exists a tradeoff between privacy and the experienced quality of service for users.

4.4 A Hybrid Mechanism

Notice that, in general, using the three types of LPPMs have their own advantages and disadvantages. The mechanism based on policy law is simple to implement, and provide high quality of service for users, but the privacy protection effect is poor. The combination of the two LPPMs (obfuscation and anonymization) are highly efficient, and can achieve a good balance between service quality and location privacy, but the user's location information or service attributes have certain inaccuracies and are vulnerable to attacks with full background knowledge. On the other hand, cryptography-based mechanisms can fully guarantee data accuracy and security, and provide more stringent privacy protection, but require additional hardware support and complex algorithm, communication, and computation overhead. The conclusion from these protection mechanisms is that it is important to take into consideration the quality of service and resource consumption issues, such as bandwidth, battery and energy consumptions, in order to protect all the user's present, past, and future locations. A hybrid LPPM is designed to improve the user's obtained quality of information while guaranteeing a good level of privacy protection and minimum energy consumption [51] [72-74]. The design strategy of this mechanism takes the data verification process into account and then combines the advantages of the three popular LPPMs (such as, obfuscation, anonymization, and encryption) to increase the level of privacy and information quality without additional consumption of energy. Therefore, this hybrid mechanism dynamically changes the concepts of grid area of interest cell sizes in accordance with the variable being measured and selects the various protection mechanisms rely on the cell sizes. When the size of the cell increases, then the variable interest becomes low and therefore it is more important to protect the real location of users.

4.5 Privacy Protection Challenges and Comparison Analysis

During the normal operation of the LBS application, each user transmits the location information to the LBS provider. Some of the major limitations of these existing applications are no restrictions imposed about users' experience, concern, interest and trustworthiness. In addition, there is a lack of strong motivations to comply the location services' requirements. Therefore, these applications associate the location data (e.g. time and location of the user) are vulnerable to erroneous LBS contributions as well as to uncertain contributions from users' selfish behavior. The location of the user is available in spatial as well as temporal form. For instance, it is possible for an attacker to obtain the access of users' current location information and history traces, i.e. called as temporal access. In other scenarios, spatial access is considered critical if the user's position is located geographically. Hence, these spatial and temporal resolutions associate with the position and time of the user are important parameters for defining location privacy. As we have mentioned earlier that there are various mechanisms to protect the location privacy such as user anonymization (k-anonymity), location obfuscation, encryption-based techniques, etc. Through the evaluation of privacy protection mechanism, various kinds of privacy protection factors can be analyzed and determined. By hindering these factors, we have analyzed the various challenges of location privacy such as to protect users present and past locations, incorporating the user's data model from anonymous and/or perturbed-locations, and finding an appropriate evaluation metrics to quantify location privacy. Each individual mechanism has their own advantages and disadvantages by analyzing the key issues and architecture of LBS privacy protection, the strengths and weaknesses to measure the location privacy of users.

Table 1 on the following analyzes the various LPPMs presented in this earlier section along with their classification, architecture, privacy protection and service quality or resource overhead of the main LBS protection techniques. To indicate the degree of privacy protection system, we use the descriptions “high”, “medium” and “low”, and similarly, the services quality is described by “good”, “general” and “poor” respectively. According to [75], the quality of service becomes orthogonal to location privacy in the case of LBS applications. It can be seen from **Table 1** that each type of protection mechanism has different advantages and performances for different application requirements. The choice of specific protection mechanisms depends on the application scenario and user's actual privacy requirements. For instance, the LBS privacy protection mechanism in this scenario is mainly aims at users' personalized and different levels of privacy requirements, measuring the privacy protection effect and service availability.

Table 1. Summary of various LPPMs for the current privacy measures [75]

LPPM type & solutions	**Architecture**	**Threats from**	**Service quality- loss**	**Resource consumption**	**Computational complexity**
A. Anonymization-based Mechanisms					
1) Tessellation [55]	Centralized	External	High	Medium	Low
2) Micro aggregation [19]	Centralized/ Distributed	External	Medium	Medium	Low
3) l-diversity[56]	Centralized	External	Medium	Medium	Low/Medium
4) Data aggregation [58]	Distributed	Internal/ External	Low	High	High
B. Obfuscation-based Mechanisms					
1) Position sharing [1]	Distributed	External	Low	High	Medium
2) Point-of-Interest [30]	Centralized/ Distributed	Internal/ External	Medium	Low	Medium
3) Random-perturbation [63]	Centralized/ Distributed	External	Medium	Medium	Medium
4) Negative survey [19]	Centralized	External	Medium	Medium	Low
C. Encryption-based Mechanisms					
1) Group-Signature [69]	Distributed	External	Low	High	High
2) Double Encryption [70]	Distributed	External	Low	High	High
Hybrid mechanism [51]	Centralized /Distributed	Both Internal & External	Medium	Low/mediu/high, depending on encrypted records	High

According to [51], the quality of service is normally measured by the location information loss, the size of the invisible area, the Euclidean distance of the true and false position, and the user's query generation rate, etc. Hence, an evaluation metric meant to indicate how different the generated location data are from the real ones. The degree of privacy protection mainly depends on the number of anonymous centralized users or tracks, the amount of added noise, the distance between true and false positions, the similarity between the true and blurred positions, the level of cooperation of users and the performance of the encryption protocol etc. The LPPMs for LBS applications that require reporting real-time location data should be simple in terms of computational complexity, if not they will discharge the battery consumption issues of the mobile device very quickly. We observe that the principle behind some complex LPPMs can be implemented in a central architecture, usually called the central anonymity server or anonymizer. The protection mechanism can be performed by the users or on their mobile device at the expense of its resources, as the LPPM is designed in a distributed architecture with taking the resource constraints in mind [76]. Therefore, it is important to reduce the amount of resource overhead in order to minimize energy consumption in resource-constrained mobile devices. Finally, how to design an optimized LPPM that satisfies the service quality and resource overhead according to user privacy requirements and given attack model is significantly important research direction for location privacy [77].

5. Open Issues and Research Challenges

We have highlighted the progress of current privacy measures for LBS applications in Section 4. While working on this topic still attracts many novel countermeasure solutions, some LBS privacy challenges remain and needs further discussions. In this section, we present some of the major research challenges/ problems in LPPMs for LBSs.

1) In the Integration of the gap between design and evaluation of LPPMs

Majority of the existing LPPMs' design principle and evaluation methods merely consider a non-strategic adversary and relatively some LPPMs consider a strategic adversary to minimize the privacy risks. For example, the authors of [21], [37], [48] have considered that the concept of location privacy is incomplete without adversarial knowledge to track the users visiting particular locations. Obviously, there is an absence of strategic measurement mechanisms to specify the different LPPMs without considering adversarial knowledge in the evaluation. In other words, differential privacy is not sensitive to background knowledge and not even considered in the evaluation to quantify LBS privacy [50]. Therefore, there is still a problem to integrate the design and evaluation of different LPPMs and their comparative features. The primarly challenge therfore is how to design the best LPPMs with consideration of the adversarial background knowledge and reasoning ability, so as to reduce the user's privacy disclosure risk while providing a tolerable service quality-loss.

2) Making privacy-preserving mechanisms measurable (specifically in the selection of the appropriate privacy metrics)

Most of the aforementioned evaluation methods for LPPM still focus on providing location privacy at each time-instant of issuing a service query, and infrequently consider for protecting trajectory privacy from where a number of consecutive queries are reported [30]. There are different intuitive privacy metrics and methods that can be used to evaluate the privacy protection performance of different LPMMs. Examples of these privacy metrics [47] includes location-k-anonymity and entropy (uncertainty-based), error-based estimator, ε-differential privacy, etc. How ever, most of them are specific to a particular systems and attack models and therefore these metrics are difficult to use in the universal context. The major challenge is then how to find the right (universal) privacy metric for evaluating the effectiveness of location privacy.

3) In Hybrid LPPMs to trade-offs between privacy, service quality, and resource consumption

Recently, due to an increasing number of LPPMs consider the potential tradeoffs between location privacy, quality of service and energy consumption for mobile users to make use of LBSs. For example, solutions have been provided in [51] that propose a hybrid LPPM in order to address the problem of balancing the privacy protection, quality of service and energy consumption based on the cells size. This double-encryption mechanism combines the strong protection effects of obfuscation, anonymization, and encryption techniques in the design consideration. Moreover, with the increase of mobile computing, the encryption and decryption performance of a static location data has been well resolved.

However, although all the running encryption and decryption algorithms are available in mobile devices, the performance of dynamic location data update is still big challenges, which are limited on mobile devices and then demand a high amount of energy consumption. This is because the type and quantity of location-aware equipments (e.g. automobiles, smart phones, etc.) faced by LBS applications are huge, and they will be moved frequently. As a result, they will generate massive and frequent updated location data, and these data may be missing and discontinuous. In order to ensure the user's acceptance of LBSs, balancing the joint-effect on privacy, service data quality and energy consumption is still an important open problem. Therefore, how to design a new optimal privacy protection method with fusion encryption technology to protect a dynamic location data during effective service leakage is also an open problem and research direction.

6. Conclusion

Today's LBS relies on user's mobile devices and integrate the results of location-related research with other new features to produce aggregated knowledge. In this setting, a serious privacy issue can discourage an extensive adoption of attractive features. To address this problem, a large number of research works has been done to preserve users' private information and to evaluate the user's obtained service quality. In this paper, we have discussed the current state-of-the-art LPPMs and analyzed their intuitive evaluation metrics within the architecture of user-specific protection model. For this purpose, a block diagram of privacy quantification and protection model is presented to quantify the location privacy and then to find effective LPPMs in the existing systems. In the next level, we have surveyed the main characteristic of privacy requirements and their associated threats to privacy used in service quality aware LBSs. We then summarized the existing LBS privacy metrics, and then presented privacy countermeasure solutions with a focus on location anonymization, obfuscation, encryption-based, and hybrid mechanisms. In the anonymization-based mechanism, the LPPMs generate the actual location information via anonymization in which the users' privet data are generalized to a set of different users. In the obfuscation mechanism, the users' location information is modified without considering the location data from other users. In the encryption-based technique, the user's privacy is preserved using using cryptographic techniques, in which the users selectively decide the time and place to report the location data to the LBS server. A hybrid mechanism combines the advantages of the above three LPPMs to achieve a good balance between location privacy and information quality without a high consumption of energy. In addition, this paper summarizes the architecture of different LPPMs and qualitative evaluations in terms of the privacy threat model, service quality loss, energy consumption, and computational complexity associated with each mechanism. Finally, we have presented and discussed several open issues and research challenges in the topic of location privacy.

References

[1] M. Wernke, P. Skvortsov, F. Dürr, and K. Rothermel, "A classification of location privacy attacks and approaches," *Personal and ubiquitous computing*, 18, no. 1, 163-175, 2014. Article (CrossRef Link).

[2] J.J.C. Ying, W.C. Lee, and V.S. Tseng, “Mining geographic-temporal-semantic patterns in trajectories for location prediction,” *ACM Transactions on Intelligent Systems and Technology (TIST)*, 5, no. 1, 2, 2013. Article (CrossRef Link).

[3] H. Li, H. Zhu, S. Du, X. Liang, and X. S. Shen, “Privacy leakage of location sharing in mobile social networks: Attacks and defense,” *IEEE Transactions on Dependable and Secure Computing*, 15, no. 4, 646-660, 2018 Article (CrossRef Link).

[4] I. Bilogrevic, K. Huguenin, S. Mihaila, R. Shokri,and J.P. Hubaux, “Predicting users' motivations behind location check-ins and utility implications of privacy protection mechanisms,” in *Proc. of 22nd Network and Distributed System Security Symposium (NDSS)*, 2015. Article (CrossRef Link).

[5] P. Skvortsov, B. Schembera, F. Dürr, and K. Rothermel, “Optimized Secure Position Sharing with Non-trusted Servers,” *arXiv preprint arXiv:1702.08377*, 2017. Article (CrossRef Link).

[6] K. G. Shin, X. Ju, Z. Chen, and X. Hu, “Privacy protection for users of location-based services,” *IEEE Wireless Communications*, 19, no. 1, 30-39, 2012. Article (CrossRef Link).

[7] P. Aditya, B. Bhattacharjee, P. Druschel, V. Erdélyi, and M. Lentz, “Brave new world: Privacy risks for mobile users,” *ACM SIGMOBILE Mobile Computing and Communications Review*, 18, no. 3, 49-54, 2015. Article (CrossRef Link).

[8] X. Yi, R. Paulet, E. Bertino, and V. Varadharajan, “Practical approximate k nearest neighbor queries with location and query privacy,” *IEEE Transactions on Knowledge and Data Engineering*, 28, no. 6, 1546-1559, 2016. Article (CrossRef Link).

[9] P. Golle,and K. Partridge, “On the anonymity of home/work location pairs,” in *Proc. of International Conference on Pervasive Computing, Springer, Berlin, Heidelberg*, pp. 390-397, 2009. Article (CrossRef Link).

[10] S. Gambs, M.O. Killijian, and M.N. del Prado Cortez, “Show me how you move and I will tell you who you are,” in *Proc. of the 3rd ACM SIGSPATIAL International Workshop on Security and Privacy in GIS and LBS*, pp. 34-41, 2010. Article (CrossRef Link).

[11] C. Song, Z. Qu, N. Blumm, and A.L. Barabási, “Limits of predictability in human mobility,” *Science*, 327, no. 5968, 1018-1021, 2010. Article (CrossRef Link).

[12] J. Freudiger, R. Shokri, and J.P. Hubaux, “Evaluating the Privacy Risk of Location-Based Services,” *Financial Cryptography and Data Security*, 31-46, 2012. Article (CrossRef Link).

[13] J. Krumm, “Inference Attacks on Location Tracks,” *nternational Conference on Pervasive Computing*, 127-143, 2007. Article (CrossRef Link).

[14] B. Niu, Q. Li, X. Zhu, G Cao, and H. Li, Qinghua Li, Xiaoyan Zhu, Guohong Cao, and Hui Li, “Enhancing privacy through caching in location-based services,” in *Proc. of Computer Communications (INFOCOM), 2015 IEEE Conference on*, pp. 1017-1025, 2015. Article (CrossRef Link).

[15] W. Li, B. Niu, H. Li, and F Li, “Privacy-preserving strategies in service quality aware location-based services,” in *Proc. of Communications (ICC), 2015 IEEE International Conference on*, pp. 7328-7334, 2015. Article (CrossRef Link).

[16] Y. Wang, Y. Xia, J. Hou, S. Gao, X. Nie, and Q. Wang, “A fast privacy-preserving framework for continuous location-based queries in road networks,” *Journal of Network and Computer Applications*, 53, 57-73, 2015. Article (CrossRef Link).

[17] C. Bettini, S. Mascetti, XS. Wang, D. Freni, and S. Jajodia, “Anonymity and historical-anonymity in location-based services,” *Privacy in location-based applications, Springer, Berlin, Heidelberg*, pp. 1-30, 2009.

[18] Gedik, Bugra, and L. Liu, “Location privacy in mobile systems: A personalized anonymization model,” in *Proc. of Distributed computing systems, 2005. ICDCS 2005. Proceedings. 25th IEEE international conference on*, pp. 620-629, 2005. Article (CrossRef Link).

[19] M.M. Groat, B. Edwards, J. Horey, W. He, and S. Forrest, “Enhancing privacy in participatory sensing applications with multidimensional data,” in *Proc. of Pervasive Computing and Communications (PerCom), 2012 IEEE International Conference on*, pp. 144-152, 2012. Article (CrossRef Link).

[20] A.R. Beresford, and F. Stajano, “Location privacy in pervasive computing,” *IEEE Pervasive computing*, 2, no. 1, 46-55, 2003. Article (CrossRef Link).

[21] J. Freudiger, M.H. Manshaei, J.P. Hubaux, and D. C. Parkes, “On non-cooperative location privacy: a game-theoretic analysis,” in *Proc. of the 16th ACM conference on Computer and communications security*, pp. 324-337, 2009. Article (CrossRef Link).

[22] X. Chen, A. Mizera, and J. Pang, “Activity tracking: A new attack on location privacy,” in *Proc. of Communications and Network Security (CNS), 2015 IEEE Conference on*, pp. 22-30, 2015. Article (CrossRef Link).

[23] H Jafari, M Nazari, S. Shamshirband, “Optimization of energy consumption in wireless sensor networks using density-based clustering algorithm,” *International Journal of Computers and Applications*, 1-10, 2018. Article (CrossRef Link).

[24] S. Shamshirband, and H. Soleimani, “LAAPS: an efficient file-based search in unstructured peer-to-peer networks using reinforcement algorithm,” *International Journal of Computers and Applications*, 1-8, 2018. Article (CrossRef Link).

[25] PGV Naranjo, Z Pooranian, S Shamshirband, J.H. Abawajy, and M. Conti, “Fog over virtualized IoT: New opportunity for context-aware networked applications and a Case Study,” *Applied Sciences*, 7, no. 12, 1325, 2017. Article (CrossRef Link).

[26] M. Shojafar, N. Cordeschi, JH. Abawajy, and E. Baccarelli, “Adaptive energy-efficient qos-aware scheduling algorithm for tcp/ip mobile cloud,” in *Proc. of Globecom Workshops (GC Wkshps), 2015 IEEE*, pp. 1-6, 2015. Article (CrossRef Link).

[27] R. Shokri, “Quantifying and protecting location privacy [Ph.D. Thesis],” *it-Information Technology*, 57, no. 4, 257-263, 2015. Article (CrossRef Link).

[28] R. Shokri, G. Theodorakopoulos, C. Troncoso, J.P. Hubaux, and J.Y. Le Boudec, “Protecting location privacy: optimal strategy against localization attacks,” in *Proc. of the 2012 ACM conference on Computer and communications security*, pp. 617-627, 2012. Article (CrossRef Link).

[29] R. Shokri, G. Theodorakopoulos, and C. Troncoso, “Privacy games along location traces: A game-theoretic framework for optimizing location privacy,” ACM Transactions on Privacy and Security (TOPS), 19, no. 4, 11, 2017. Article (CrossRef Link).

[30] H. Shen, G. Bai, M. Yang, and Z. Wang, “Protecting trajectory privacy: A user-centric analysis,” *Journal of Network and Computer Applications*, 82, 128-139, 2017. Article (CrossRef Link).

[31] X. Zhang, X. Gui, F. Tian, S. Yu, and J. An, “Privacy quantification model based on the Bayes conditional risk in Location-based services,” *Tsinghua Science and Technology*, 19, no. 5, 452-462, 2014. Article (CrossRef Link).

[32] V. Bindschaedler,and R. Shokri, “Synthesizing plausible privacy-preserving location traces,” in *Proc. of Security and Privacy (SP), 2016 IEEE Symposium on*, pp. 546-563, 2016. Article (CrossRef Link).

[33] W.X. Zhao, N. Zhou, W. Zhang, J.R. Wen, S. Wang, and E.Y. Chang, “A probabilistic lifestyle-based trajectory model for social strength inference from human trajectory data,” *ACM Transactions on Information Systems (TOIS)*, 35, no. 1, 8, 2016. Article (CrossRef Link).

[34] J. Freudiger, M. H. Manshaei, J.Y. Le Boudec, and J. P. Hubaux, “On the age of pseudonyms in mobile ad hoc networks,” in *Proc. of INFOCOM, 2010 Proceedings IEEE*, pp. 1-9, 2010. Article (CrossRef Link).

[35] Y. Pan, and J. Li Pan, “Cooperative pseudonym change scheme based on the number of neighbors in VANETs,” *Journal of Network and Computer Applications*, 36, no. 6, 1599-1609, 2013. Article (CrossRef Link).

[36] X. Liu, H. Zhao, M. Pan, H. Yue, X. Li, and Y. Fang, “Traffic-aware multiple mix zone placement for protecting location privacy,” in *Proc. of INFOCOM, 2012 Proceedings IEEE*, pp. 972-980, 2012. Article (CrossRef Link).

[37] R. Shokri, G. Theodorakopoulos, G. Danezis, J.P. Hubaux, and J.Y. Le Boudec, “Quantifying location privacy: the case of sporadic location exposure,” in *Proc. of International Symposium on Privacy Enhancing Technologies Symposium*, pp. 57-76, 2011. Article (CrossRef Link).

[38] J. Shi, R. Zhang, Y. Liu, and Y. Zhang, “Prisense: privacy-preserving data aggregation in people-centric urban sensing systems,” in *Proc. of INFOCOM, 2010 Proceedings IEEE*, pp. 1-9, 2010. Article (CrossRef Link).

[39] R. Shokri, J. Freudiger, and J. P. Hubaux, “A unified framework for location privacy,” *No. EPFL-REPORT-148708*, 2010. Article (CrossRef Link).

[40] D. Houshmand Mozafari, “Providing Location Privacy for the Users of Location-based Services,” 2012.

[41] Li, Qinghua, and Guohong Cao, “Efficient and privacy-preserving data aggregation in mobile sensing,” in *Proc. of Network Protocols (ICNP), 2012 20th IEEE International Conference on*, pp. 1-10, 2012. Article (CrossRef Link).

[42] R. Zhang, J. Shi, Y. Zhang, and C.Zhang, “Verifiable privacy-preserving aggregation in people-centric urban sensing systems,” *IEEE Journal on Selected Areas in Communications*, 31, no. 9, 268-278, 2013. Article (CrossRef Link).

[43] Z. Xu, H. Zhang, and X. Yu, “Multiple mix-zones deployment for continuous location privacy protection,” in *Proc. of Trustcom/BigDataSE/I SPA, 2016 IEEE*, pp. 760-766, 2016. Article (CrossRef Link).

[44] B. Niu, Q. Li, X. Zhu, G. Cao,and H. Li, “Achieving k-anonymity in privacy-aware location-based services,” in *Proc. of INFOCOM, 2014 Proceedings IEEE*, pp. 754-762, 2014. Article (CrossRef Link).

[45] B. Niu, Z. Zhang, X. Li, and H. Li, “Privacy-area aware dummy generation algorithms for location-based services,” in *Proc. of Communications (ICC), 2014 IEEE International Conference on*, pp. 957-962, 2014. Article (CrossRef Link).

[46] X. Liu, K. Liu, L. Guo, X. Li, and Y. Fang, “A game-theoretic approach for achieving k-anonymity in location based services,” in *Proc. of INFOCOM, 2013 Proceedings IEEE*, pp. 2985-2993, 2013. Article (CrossRef Link).

[47] R Shokri, J Freudiger, M Jadliwala, and J.P. Hubaux, “A distortion-based metric for location privacy,” in *Proc. of the 8th ACM workshop on Privacy in the electronic society*, pp. 21-30, 2009. Article (CrossRef Link).

[48] R. Shokri, G. Theodorakopoulos, J.Y. Le Boudec, and J.P. Hubaux, “Quantifying location privacy,” in *Proc. of Security and privacy (sp), 2011 ieee symposium on*, pp. 247-262, 2011. Article (CrossRef Link).

[49] R. Shokri, “Privacy games: Optimal user-centric data obfuscation,” *Proceedings on Privacy Enhancing Technologies*, 2015, no. 2, 299-315, 2015. Article (CrossRef Link).

[50] M.E. Andrés, N.E. Bordenabe, K. Chatzikokolakis, and C. Palamidessi, “Geo-indistinguishability: Differential privacy for location-based systems,” in *Proc. of the 2013 ACM SIGSAC conference on Computer & communications security*, pp. 901-914, 2013. Article (CrossRef Link).

[51] I.J. Vergara-Laurens, D. Mendez, L.G. Jaimes, and M. Labrador, “A-PIE: An algorithm for preserving privacy, quality of information, and energy consumption in Participatory Sensing Systems,” *Pervasive and Mobile Computing*, 32, 93-112, 2016. Article (CrossRef Link).

[52] T. Xu and Y. Cai, “Exploring historical location data for anonymity preservation in location-based services,” in *Proc. of INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*, pp. 547-555, 2008. Article (CrossRef Link).

[53] R.H. Hwang, Y.L. Hsueh, and H.W.Chung, “A novel time-obfuscated algorithm for trajectory privacy protection,” *IEEE Transactions on Services Computing*, 7, no. 2, 126-139, 2014. Article (CrossRef Link).

[54] S. Gao, J. Ma, W. Shi, G. Zhan, and C. Sun, “TrPF: A trajectory privacy-preserving framework for participatory sensing,” *IEEE Transactions on Information Forensics and Security*, 8, no. 6, 874-887, 2013. Article (CrossRef Link).

[55] C. Cornelius, A. Kapadia, D. Kotz, D. Peebles, M. Shin, and N. Triandopoulos, “Anonysense: privacy-aware people-centric sensing,” in *Proc. of the 6th international conference on Mobile systems, applications, and services*, pp. 211-224, 2008.

[56] A. Solanas, Ú. González-Nicolás, and A. Martínez-Ballesté, "Mixing genetic algorithms and V-MDAV to protect microdata," in *Proc. of Computational Intelligence for Privacy and Security, Springer, Berlin, Heidelberg*, pp. 115-133, 2012. Article (CrossRef Link).

[57] B. Zhou,and J**.** Pei, "The k-anonymity and l-diversity approaches for privacy preservation in social networks against neighborhood attacks," *Knowledge and Information Systems*, 28, no. 1, 47-77, 2011. Article (CrossRef Link).

[58] H. Jin, L. Su, H Xiao, and K. Nahrstedt, "Inception: Incentivizing privacy-preserving data aggregation for mobile crowd sensing systems," in *Proc. of the 17th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, pp. 341-350, 2016. Article (CrossRef Link).

[59] D.E. Cho, S. Kim, and S.Yeo, "Double privacy layer architecture for big data framework," *International Journal of Software Engineering and Its Applications*, 10, no. 2, 271-278, 2016. Article (CrossRef Link).

[60] B. Lee, J. Oh, H. Yu,and J. Kim , "Protecting location privacy using location semantics," in *Proc. of the 17th ACM SIGKDD international conference on Knowledge discovery and data mining*, pp. 1289-1297, 2011. Article (CrossRef Link).

[61] P. Wightman, W. Coronell, D. Jabba, M. Jimeno, and M. Labrador, "Evaluation of location obfuscation techniques for privacy in location based information systems," in *Proc. of Communications (LATINCOM), 2011 IEEE Latin-American Conference on*, pp. 1-6, 2011. Article (CrossRef Link).

[62] R.K. Ganti, N. Pham, YE. Tsai, and T.F. Abdelzaher, "PoolView: stream privacy for grassroots participatory sensing," in *Proc. of the 6th ACM conference on Embedded network sensor systems*, pp. 281-294, 2008. Article (CrossRef Link).

[63] D. Lian, X. Xie, VW.Zheng, NJ. Yuan, F. Zhang, and E. Chen, "CEPR: A collaborative exploration and periodically returning model for location prediction," *ACM Transactions on Intelligent Systems and Technology (TIST)*, 6, no. 1, 8, 2015. Article (CrossRef Link).

[64] I.J. Vergara-Laurens, and M.A. Labrador, "Preserving privacy while reducing power consumption and information loss in lbs and participatory sensing applications," In *GLOBECOM Workshops (GC Wkshps), 2011 IEEE*, pp. 1247-1252, 2011. Article (CrossRef Link).

[65] W.X. Zhao, N. Zhou, W. Zhang, J.R. Wen, S. Wang, and E.Y. Chang, "A probabilistic lifestyle-based trajectory model for social strength inference from human trajectory data," *ACM Transactions on Information Systems (TOIS)*, 35, no. 1, 8, 2016. Article (CrossRef Link).

[66] R. Shokri, G. Theodorakopoulos, P. Papadimitratos, E. Kazemi, and J. P. Hubaux, "Hiding in the mobile crowd: Location privacy through collaboration," *IEEE transactions on dependable and secure computing*, 11, no. 3, 266-279, 2014. Article (CrossRef Link).

[67] I.J. Vergara-Laurens, D. Mendez-Chaves, and M.A. Labrador, "On the interactions between privacy-preserving, incentive, and inference mechanisms in participatory sensing systems," in *Proc. of International Conference on Network and System Security*, pp. 614-620, 2013. Article (CrossRef Link).

[68] S. Hoteit, S. Secci, S. Sobolevsky, G.Pujolle, and C. Ratti, "Estimating real human trajectories through mobile phone data," in *Proc. of MDM 2013-14th IEEE International Conference on Mobile Data Management*, pp. 148-153, 2013. Article (CrossRef Link).

[69] M.C. Gonzalez, C.A. Hidalgo, and A.L. Barabasi, "Understanding individual human mobility patterns," *nature*, 453, no. 7196, 779-782, 2008. Article (CrossRef Link).

[70] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.L. Tan, "Private queries in location based services: anonymizers are not necessary," in *Proc. of the 2008 ACM SIGMOD international conference on Management of data*, pp. 121-132, 2008. Article (CrossRef Link).

[71] Z. Jing, M. Chen, and F. Hongbo, "WSN key management scheme based on fully bomomorphic encryption," in *Proc. of Control And Decision Conference (CCDC), 2017 29th Chinese*, pp. 7304-7309, 2017. Article (CrossRef Link).

[72] A.N. Khan, M.L.M. Kiah, M. Ali, SA Madani, and S. Shamshirband, "BSS: block-based sharing scheme for secure data storage services in mobile cloud environment," *The Journal of Supercomputing*, 70, no. 2, 946-976, 2014. Article (CrossRef Link).

[73] A.N. Khan, M.L.M. Kiah, M. Ali, and S. Shamshirband, “A cloud-manager-based re-encryption scheme for mobile users in cloud environment: a hybrid approach,” *Journal of Grid Computing*, 13, no. 4, 651-675, 2015. Article (CrossRef Link).

[74] M. Shojafar, N. Cordeschi, J.H. Abawajy, and E. Baccarelli, “Adaptive energy-efficient qos-aware scheduling algorithm for tcp/ip mobile cloud,” in *Proc. of Globecom Workshops (GC Wkshps), 2015 IEEE*, pp. 1-6, 2015. Article (CrossRef Link).

[75] I.J. Vergara-Laurens, L.G. Jaimes, and M. A. Labrador, “Privacy-preserving mechanisms for crowd sensing: Survey and research challenges,” *IEEE Internet of Things Journal*, 4, no. 4, 855-869, 2017. Article (CrossRef Link).

[76] M.R. Ra, B. Liu, T.F. La Porta, and R. Govindan, “Medusa: A programming framework for crowd-sensing applications,” in *Proc. of the 10th international conference on Mobile systems, applications, and services, ACM*, pp. 337-350, 2012. Article (CrossRef Link).

[77] S. Mishra, R. Sagban, A. Yakoob, and N.Gandhi, “Swarm intelligence in anomaly detection systems: an overview,” *International Journal of Computers and Applications*, 1-10, 2018. Article (CrossRef Link).

Mulugeta K.Tefera received a Bachelor degree in Electrical and Electronics Technology from Adama University, Adama-Ethiopia in 2008 and M.Eng degree in Signal and Information Processing Technology from Tianjin University of Technology and Education (TUTE), P.R. China in 2011. He is currently pursuing a Ph.D. degree in information and communication engineering with the School of Computer and Communication Engineering, University of Science and Technology Beijing (USTB), Beijing, China. His research interests include; Wireless Sensor Network, Mobile Crowd Sensing and Computing, and next-generation of Internet of Things (IOT).

Xiaolong Yang received the B.Eng., M.S., and Ph.D degrees in communication and information system from the University of Electronic Science and Technology of China (UESTC), Chengdu, China, in 1993, 1996, and 2004, respectively. He is currently a Professor with the School of Computer and Communication Engineering and the Institute of Advanced Networking Technologies and New Services (ANTS), University of Science and Technology Beijing, Beijing, China. His research focuses on optical switching and Internetworking, and next-generation Internet. He has fulfilled more than 40 research projects, including the National Natural Science Foundation of China, National Hi-Tech Research and Development Program (863 Program), and National Key Basic Research Program (973 Program). He has authored more than 120 papers in his research fields and hold 30 patents.

Qifu Tyler Sun received the B. Eng. (first class honors) and Ph.D. degrees from the Department of Information Engineering, The Chinese University of Hong Kong, Shatin, NT, Hong Kong, in 2005 and 2009, respectively. He has been a postdoctoral fellow at the Institute of Network Coding, the Chinese University of Hong Kong and a visiting research fellow at the University of New South Wales. He is currently an associate professor at the School of Computer and Communication Engineering, University of Science and Technology Beijing, China. He has been holding, as the principal investigator, three research grants of National Science Foundation of China.