This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2019.2897099, IEEE Transactions on Mobile Computing

DPavatar: A Real-time Location Protection Framework for Incumbent Users in Cognitive Radio Networks

Jianqing Liu, Chi Zhang, Beatriz Lorenzo, and Yuguang Fang, *Fellow, IEEE*

Abstract—Dynamic spectrum sharing between licensed incumbent users (IUs) and unlicensed wireless industries has been well recognized as an efficient approach to solving spectrum scarcity as well as creating spectrum markets. Recently, both U.S. and European governments called a ruling on opening up spectrum that was initially licensed to sensitive military/federal systems. However, this introduces serious concerns on operational privacy (e.g., location, time and frequency of use) of IUs for national security concerns. Although several works have proposed obfuscation methods to address this problem, these techniques only rely on syntactic privacy models, lacking rigorous privacy guarantee. In this paper, we propose a comprehensive framework to provide real-time differential location privacy for sensitive IUs. We design a utility-optimal differentially private mechanism to reduce the loss in spectrum efficiency while protecting IUs from harmful interference. Furthermore, we strategically combine differential privacy with another privacy notion, *expected inference error*, to provide double shield protection for IU's location privacy. Extensive simulations are conducted to validate our design and demonstrate significant improvements in utility and location privacy compared with other existing mechanisms.

Index Terms—Differential privacy, location privacy, Bayesian inference attack, cognitive radio networks, optimization.

1 Introduction

Radio spectrum is a precious resource and a prerequisite for modern communication systems. However, current spectrum utilization efficiency is relatively low. For example, as of September 2012, National Telecommunications and Information Administration (NTIA) estimated that 43 percent of the spectrum between 225 MHz to 3,700 MHz (the spectrum most highly desired by the wireless community) is predominantly occupied by federal systems but is used inefficiently. Concurrently, there is an ever-increasing industrial demand for wireless spectrum. To mitigate the problem of unbalanced spectrum usage, dynamic spectrum access (DSA) technique has been well recognized as a promising solution. Federal Communications Commissions (FCC) in the U.S. recently issued a ruling that the 3,550-3,700 MHz band, which was initially licensed to DoD's military radar systems, will be opened to wireless industries for shared usage [1]. In Europe, a similar DSA framework named licensed shared access (LSA) is also being developed, and the 2.3-2.4 GHz band originally belonging to military aircraft services and police wireless systems is now open for wireless industries for shared access [2]. Among these rulings, a spectrum access system (SAS) database is recommended to be set up to manage the shared spectrum usage between licensed incumbent users (IUs) and unlicensed secondary users (SUs) [1]. Specifically, SUs send queries to the SAS database for the available spectrum and allowable transmit power. The SAS database responds according to IUs' operational information (e.g., location, frequency band, and time of operation) to ensure that no harmful interference is generated.

It is recognized that most IUs are not classified systems like fixed satellite radars whose operational information is public, but some are quite sensitive such as the Ground/Air Task Oriented Radar (GATOR) which is used to detect unmanned aerial systems, cruise missiles, rockets, mortars, etc [3]. In practice, the GATOR system operates in the lower adjacent 3.5 GHz band; has very low interference thresholds (e.g., -102 dBm for GATOR Block 3); and is frequently redeployed by a medium-tactical vehicle replacement (MTVR) to fulfill various homeland defense missions [4]. The SAS database, therefore, incorporates the protection for the GATOR system to avoid the high adjacent channel leakage from the 3.5 GHz band. Unfortunately, research studies have shown that the query-response process, which is initially intended to protect IUs from power interference, reveals unexpected useful information to adversaries who can compromise IUs' operational privacy [5], [6].

As we know, traditional cyber-attacks apply the in-field spectrum sensing technique to triangulate the radar system, whereas military systems normally react using the frequency hopping over a wide range of spectrum [7]. However, in the SAS database-based DSA system, adver-

J. Liu is with the Department of Electrical and Computer Engineering, University of Alabama in Huntsville, Huntsville, AL, 35899 USA e-mail: jianqing.liu@uah.edu
C. Zhang is with University of Science and Technology of China and Key Laboratory of Electromagnetic Space Information, Chinese Academy of Sciences, Hefei, 230027 P. R. China, e-mail: chizhang@ustc.edu.cn
B. Lorenzo is with the Atlantic Research Center for Information and Communication Technologies (AtlantTIC), University of Vigo, Vigo, 36310 Spain e-mail: blorenzo@gti.uvigo.es
Y. Fang is with the Department of Electrical and Computer Engineering, University of Florida, Gainesville, FL, 32611 USA e-mail: fang@ece.ufl.edu
The work of J.Liu and Y.Fang was supported by the US National Science Foundation under grant CNS-1343356 and IIS-1722791. The work of C.Zhang was supported by the National Key Research and Development Program of China under Grant 2017YFB0802202 and by the Natural Science Foundation of China (NSFC) under Grant 61201240. The work of B. Lorenzo was supported by MINECO, Spain, under Grant EUIN2017-88225.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2019.2897099, IEEE Transactions on Mobile Computing

saries gain extra or asymmetric advantages in this cyberspace battlefield, meaning that they can remotely initiate large number of innocuous database queries and infer the possible operational information of radar systems before deploying in-field sensing or jamming. This unfortunately benefits adversaries in terms of reducing their attacking cost and increasing the attacking accuracy. Therefore, to ensure successful military operations, it is critical to develop obfuscation techniques in the SAS database to complicate and confound adversaries in conducting cyber-attacks, which in turn avails IUs in this cyber battle.

Even though prior research work [5], [8]–[10] proposed several privacy-preserving mechanisms to protect IUs' operational privacy in terms of location, time and frequency of use, these approaches only focused on one time randomization or obfuscation. Besides, these approaches could fail for two reasons. First, in real-time series, independently applying these mechanisms for multiple times may help adversaries to remove the noise and compromise IUs' privacy. Second, the added noise could be filtered out by adversaries with certain prior knowledge that these works clearly ignore. Furthermore, these mechanisms typically add extra non-existing dummy records in spatial, temporal or spectral domain to preserve IUs' operational privacy, which yet sufficiently reduces spectrum efficiency.

In this paper, we consider a DSA system where users come or go in dynamic fashions, and we intend to protect the IU's location privacy in real-time series while minimizing the loss to SUs' spectrum efficiency. Specifically, we leverage user diversity to include SUs and IU in a location cloaking set such that every user therein is subject to obfuscation and could be released to represent the IU. Here, these SUs are coined as "avatars" and we propose a framework called **DPavatar** to achieve **D**ifferential location **P**rivacy for the IU by leveraging **avatar** SUs in real-time sequence. Our contributions are listed as follows.

- To the best of our knowledge, this is the first work to incorporate SUs to obfuscate IU's location. The benefit is to reduce the loss in spectrum efficiency by elevating any SU as the IU and protecting it from interference. However, natural concerns could rise up in the sense that these SUs could infer IU's location and the IU may suffer from harmful interference. We tackle the first concern by constructing the location cloaking set satisfying *reciprocity*, a property to preserve spatial K-anonymity so that the included SUs cannot distinguish which one is the real IU. For the second concern, we design a feedback control mechanism to suppress the power interference to the IU.
- The obfuscation is performed at certain time instants and we design an interference-utility-aware differentially private mechanism which is cast as a linear optimization problem. The optimal DP obfuscation distribution is obtained while the loss in spectrum efficiency is minimized.
- This is the first work so far to address IU's location privacy in the real-time setting. Specifically, we consider privacy loss due to continuous application of obfuscation mechanism and apply (ω, ε)-differential privacy mechanism to guarantee that the IU could retain ε-differential location privacy at any ω length of time window.
- We argue that differential privacy only confines adversary's information gain between prior and posterior knowledge but may not be sufficient for location protection if an adversary has certain prior knowledge that can uniquely identify the IU. We prove this claim both theoretically and numerically in this paper. To cope with this issue, we combine DP with another privacy notion named *expected inference error* [11] which takes adversary's specific prior knowledge into consideration. We claim that this strategic combination can double shield IU's location privacy by simultaneously limiting information leakage of the DP mechanism and ensuring the inference error to be constrained for inference attacks with prior information the adversary may have.

The reminder of this paper is organized as follows. Section II describes the related work. Section III introduces some background information and describes the adversary model. Essential preliminaries are followed at Section IV. Then our DPavatar scheme is discussed in details in Section V. Section VI gives the privacy analysis. The performance evaluations are presented in Section VI and finally, Section VII concludes the paper and outlines the future work.

2 Related Work

Spectrum sharing is an interactive process among different parties that could introduce security or privacy threats. One type of attacks such as Primary User Emulation Attack (PUEA) [12] and Spectrum Sensing Data Falsification (SSDF) attack [13] is about compromising the security of spectrum sharing, which is not necessarily based on SAS database system. Therefore, in this survey, we focus on works in protecting IU's operational privacy in database-driven DSA. Authors in [14], [15] consider the adversary model that the SAS database is semi-trusted. Cryptographic tools, namely CP-ABE in [14] and homomorphic Paillier cryptosystem [15], are used to protect IU's operational information such as IU's antenna height and gain, transmission power and interference threshold against the SAS database. Obfuscation strategies can also be applied to protect IU's operational information from being inferred. In [9], Robertson *et al.* insert to the SAS database dummy records of frequency bands that the IU operates on, so that adversaries cannot distinguish IU's exact operating spectrum. In [8], Bahrak *et al.* apply K-anonymity to preserve IU's location privacy and add false entries in time domain to prevent adversaries from learning IU's correct operational time. In [5], [10], authors add random noise to IU's operating information such as the radius of protected contour and interference threshold. As a result, the adversaries may not correctly infer IU's location.

Although these obfuscation strategies seem workable at first glance, they rely on syntactic privacy models without rigorous privacy guarantee. On the other hand, the differential privacy [16], initially applied in statistical databases, has been accepted as a standard for privacy protection. Recently, the notion of differential privacy has been extended to preserve location privacy [17]–[20]. In general, differentially

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2019.2897099, IEEE Transactions on Mobile Computing

private location obfuscation requires a location set containing the actual user's location and "neighbouring" locations, such that they have the similar probabilities (bounded by e^{ε}) to produce a pseudo-location. Andrés *et al.* [17] propose the notion geo-indistinguishability and a planar Laplace mechanism is developed to produce fake locations from a polar Laplacian distribution. Based on this work, Bordenabe *et al.* propose a utility-optimal obfuscation mechanism to achieve ε-geo-indistinguishability [18]. Chatzikokolakis *et al.* define privacy mass over an area and generalize the geo-indistinguishability by adaptively adjusting the privacy parameter. Xiao *et al.* in [19] consider temporal correlations of user's mobility pattern and obfuscate the location based on a planar isotropic mechanism.

However, most of them only consider obfuscation in a static scenario without considering privacy loss due to continuously applying differentially private obfuscation. Therefore, we resort to the ω-event ε-differential privacy proposed in [21], [22] to protect IU's location privacy on-the-fly in a dynamic spectrum sharing environment. Besides, it is well-known that the location obfuscation affects utility (or quality) of services. Here, by releasing pseudo-location in spectrum sharing scenario could incur harmful power interference to the IU, which is much more severe than just degrading utilities. Therefore, we propose an interference-aware differentially private mechanism in this paper to remedy this problem.

On the other hand, it has been recently recognized that the differential privacy may not be effective in location protection for Bayesian adversaries with sufficient prior knowledge [20], [23], [24]. Shokri *et al.* in [24] is the first to combine differential privacy with adversary's expected inference error using a linear programming framework to demonstrate the potential for privacy protection improvements. Yu *et al.* [23] based on this work propose a user defined personalized error bound in the differential privacy framework to limit Bayesian adversaries' inference accuracy. In this paper, we intend to bound the Bayesian adversary's inference error in our differential privacy framework to provide double-shield protection for IU's location privacy.

3 Background and Adversary Model

3.1 Overview of Spectrum Access Systems

An SAS generally consists of IUs, SUs and a centralized database system that coordinates the spectrum sharing between IUs and SUs. For instance, the 3.5 GHz SAS operates via a three-tier spectrum access approach, wherein IUs operate at the first tier with the highest priority, while SUs operate either at the second tier with licensed priority access (the small-cell services), or at the third tier with general authorized access. Fig.1 shows a typical spectrum access process and it is explained in details as follows. Firstly, IUs send the SAS database their operational data such as location x_{u^*}, occupied channels f_{u^*} and interference threshold $\Lambda_{u^*}^{th}$ for interference protection. Moreover, in our design, IUs can send a personalized error bound φ to the SAS database, specifying the required protection level against Bayesian adversaries. After receiving queries from SUs for available channels at specific locations x_u, SAS database responds with a list of available channels $\vec{f}$ along with the allowable transmit power $\vec{P_f}$. The power is calculated based on the accurate radio propagation model and IUs' operational data [1] such that the accumulated interference from all operating SUs is below IUs' interference threshold. Finally, upon receiving responses from the SAS database, the SU claims a channel and registers its usage at the SAS database.

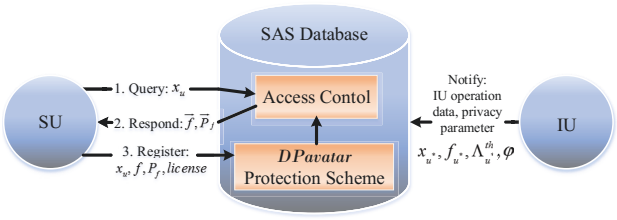


Figure 1: The system model of SAS database

3.2 Adversary Model

We assume Bayesian adversaries whose goal is to geo-locate the sensitive IU (e.g., the GATOR) through innocuous queries to the SAS database. We assume adversaries have sufficient computational resources in the sense that (1) they can generate a large number of fake locations to query the SAS database simultaneously; (2) and they can perform real-time analysis of database responses to triangulate the sensitive IU. Moreover, adversaries may possess a variety of prior knowledge, which is obtained from other public databases. For instance, the NTIA in [3] lists 30 coarse-grained installation locations of the GATOR system across the United States. In particular, we can assume the adversary has a prior (probability) distribution π of the IU over the set of possible locations Ψ (e.g., one of those 30 installation cities).

We consider the adversary as an informed one in the sense that it knows the location obfuscation mechanism, i.e., how it works and the exact obfuscation technique $\mathcal{A}$ (i.e., its probability distribution). Under this assumption, by geo-locating every released (real and dummy) IU using algorithms available in [5], [6], Bayesian adversaries aim to filter the dummy IUs and infer the real one. Particularly, Bayesian adversaries will firstly compute the following posterior probability distribution:

$$\Pr(x|x_{\widehat{u}}) = \frac{\pi(x)\Pr\left(\mathcal{A}(x_{\widehat{u}}|x)\right)}{\sum_{x\in\Psi}\pi(x)\Pr\left(\mathcal{A}(x_{\widehat{u}}|x)\right)} \tag{1}$$

Based on the posterior distribution, the adversary could infer IU's location through *Bayesian Inference Attack*, represented by

$$\widetilde{x_{u^*}} = \arg\max_{x\in\Psi} \Pr(x|x_{\widehat{u}}) \tag{2}$$

We further quantify IU's location privacy as the Bayesian adversary's error in her inference attack. We see for a given released dummy IU $\widehat{u}$, IU's conditional location privacy (i.e.,

1. Since SAS database knows users' exact locations, radio specs (e.g., antenna height/gain, terrain data, weather, etc) and transmit power, it can adopt the channel model (e.g., Longley-Rice) for interference calculation.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2019.2897099, IEEE Transactions on Mobile Computing

the conditional expected inference error) can be computed as follows:

$$Err = \sum_{x \in \Psi} \Pr(x|x_{\widehat{u}}) \cdot d_h(\widetilde{x_{u^*}}, x) \tag{3}$$

where $d_h(\cdot,\cdot)$ is the Hamming distance between two points and it equals to 1 if $\widetilde{x_{u^*}} \neq x$ and 0 otherwise. Note that this is an absolute measure of adversary's capability to geo-locate the IU given a specific prior knowledge π.

In the end, we claim that the SAS database is trusted since it is authorized and censused by FCC and NTIA to manage the DSA system, whereas the semi-trusted database model has been addressed elsewhere in Liu *et. al* [14]. Besides, the operating SUs that have obtained spectrum access opportunities are assumed curious about IU's location but they do not actively collude with each other or outside attackers.

4 Preliminaries

4.1 Differential Privacy

Differential privacy has become a *de facto* standard privacy model, which was originally introduced in statistical databases, requiring that a randomized mechanism should produce similar results when a query is applied to *neighbouring* databases. Formally, the notion of ϵ-differential privacy is formulated as follows [25].

Definition 4.1 (Differential Privacy). A privacy mechanism $\mathcal{A}$ gives ϵ-differential privacy where $\epsilon > 0$ if for any neighbouring databases D and $D^{'}$ differing on at most one record, and for all sets $S \subseteq Range(\mathcal{A})$, the following holds

$$e^{-\varepsilon} \leq \frac{\Pr(\mathcal{A}(D) \in S)}{\Pr(\mathcal{A}(D^{'}) \in S)} \leq e^{\varepsilon} \tag{4}$$

The commonly used technique to achieve ϵ-differential privacy is the Laplace mechanism [25], whose main idea is to add random noise drawn from a Laplace distribution into the statistics to be published. One of the most important properties of DP mechanisms is the *composition theorem*, meaning any DP mechanism is bound to cause privacy loss when used repeatedly [21].

Theorem 4.1 (Sequential Composition). Let $\mathcal{A}_1, \mathcal{A}_2, ..., \mathcal{A}_r$ be a set of mechanisms and each $\mathcal{A}_i$ provides ϵ_i-differential privacy. Let $\mathcal{A}$ be another mechanism that executes $\mathcal{A}_1(D), \mathcal{A}_2(D), ..., \mathcal{A}_r(D)$ using independent randomness for each $\mathcal{A}_i$. Then $\mathcal{A}$ satisfies $(\sum_{i=1}^{r} \varepsilon_i)$-differential privacy.

4.2 Differentially Private Location Obfuscation

The ϵ-differential privacy concept in statistical data release context can be naturally extended to the setting of location privacy preservation. Here, we define the ϵ-differential privacy on a discretized location set containing the IU, with the intuition that the released location z will not help an adversary to differentiate any instance inside this location set.

Definition 4.2 (Differential Location Privacy). A randomized mechanism $\mathcal{A}$ satisfies ϵ-differential privacy on location set $\mathcal{X}$ if for any released location $z \in \mathcal{X}$ and any two locations x and $x^{'} \in \mathcal{X}$, the following holds:

$$e^{-\varepsilon} \leq \frac{\Pr(\mathcal{A}(x) = z)}{\Pr(\mathcal{A}(x') = z)} \leq e^{\varepsilon} \tag{5}$$

The location set could be created in various ways according to different problem settings [17]–[19], [23]. Given the location set, noise could be generated to satisfy differential privacy following approaches such as 2-dimensional Laplace distribution [17], utility-optimal mechanism [18], [26], planar isotropic mechanism [19] and exponential mechanism [23].

4.3 (ω, ε)-Privacy

ω-event ϵ-differential privacy [21], [27], (ω, ε)-privacy used for short when there is no confusion, is proposed as an extension of differential privacy to address release of infinite streams. The model emphasizes the guarantee of user level ϵ-differential privacy in any ω contiguous time intervals in a sliding window.

Definition 4.3 ((ω, ε)-privacy). The randomized mechanism $\mathcal{A}$ gives (ω, ε)-privacy if for any two ω-neighbouring series of input databases $\mathbf{D}_\omega$ and $\mathbf{D}^{'}_\omega$, and for all sets $S \subseteq Range(\mathcal{A})$, the following holds

$$e^{-\varepsilon} \leq \frac{\Pr(\mathcal{A}(\mathbf{D}_\omega) \in S)}{\Pr(\mathcal{A}(\mathbf{D}^{'}_\omega) \in S)} \leq e^{\varepsilon} \tag{6}$$

Theorem 4.2. [21] Let $\mathcal{A}$ be a randomized mechanism that takes as input stream $\mathbf{D_t}$, where $\mathbf{D_t}[i] = D_i \in \mathcal{D}$, and outputs $\mathbf{s_t} = (s_1, ..., s_t) \in S$. Suppose $\mathcal{A}$ can be decomposed into t randomized mechanisms $\mathcal{A}_1, \mathcal{A}_2, ..., \mathcal{A}_t$ such that $\mathcal{A}_i(D_i) = s_i$, each $\mathcal{A}_i$ generates independent randomness and satisfies ϵ_i-differential privacy. Then , $\mathcal{A}$ achieves (ω, ε)-privacy iff

$$\forall i \in [t], \sum_{k=i-\omega+1}^{i} \varepsilon_k = \varepsilon$$

This theorem views ϵ as the privacy budget for every subsequence of length ω anywhere (i.e., in any sliding window of ω) in the original series of input databases. This is the fundamental theorem, based on which we design a novel real-time (ω, ε)-privacy mechanism by properly allocating portions of ϵ across multiple time instants.

5 DPavatar: Real-time Differential Location Privacy for the IU

5.1 Overview

Fig.2 illustrates the basic idea of how our proposed *DPavatar* protection scheme works. For the presentation clarity, we first give an overview of each function block in Fig.2 and then outline some assumptions that are essential in our design.

Firstly, we consider a time-slotted system where the SAS database only registers one user per time instant for the spectrum access. This is because the mutual authentication is executed in the registration phase and limiting the number of registered users per time instant can thwart the denial-of-service (DoS) attack. Besides, the time interval can be dynamically adjusted based on the number of users

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2019.2897099, IEEE Transactions on Mobile Computing

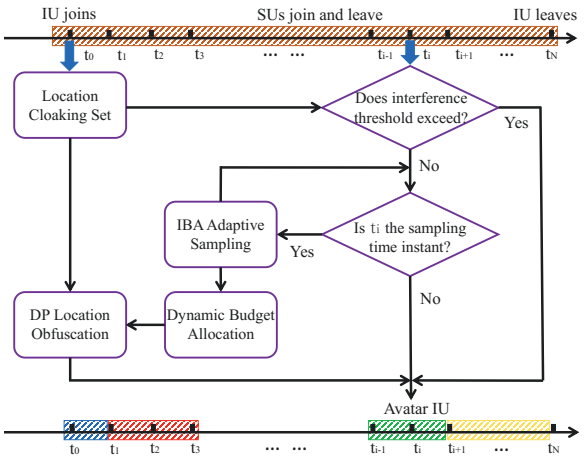


Figure 2: The overview of DPavatar protection scheme.

participating in the DSA system. Next, suppose when the IU registers in the SAS database at t_0, several operating SUs (i.e., avatars), including the IU, are selected to form a location cloaking set. We assume these avatar SUs are provided with incentives (e.g., power interference protection) to obfuscate the IU's location from t_0 to t_N, but they might be curious about IU's location. After t_0, the following procedures are carried out at each time instant t_i ($t_0 < t_i \leq t_N$):

- When a SU joins the DSA system at t_i, the SAS database checks whether the accumulated power interference to any user in the location cloaking set exceeds the threshold or not;
- If yes, the incoming SU is rejected and the interfered avatar IU is released at t_i for public queries; otherwise, the scheme continues to verify if t_i is the sampling time instant to perform the differentially private (DP) location obfuscation;
- If not, the SAS database utilizes the last released avatar IU for public queries; otherwise, the **I**nterference and **B**udget **A**ware (IBA) adaptive sampling function module calculates the next sampling time instant and meanwhile informs the dynamic budget allocation block to determine certain privacy budgets (i.e., ε) for the location obfuscation;
- The DP location obfuscation function block then takes ε and the location cloaking set as input and produces the avatar IU at t_i.

Note that if there are not many SUs participating in the DSA system, our scheme is naturally equivalent to the conventional approaches [5], [8] in the sense that dummy records (e.g., false locations, noisy interference threshold, etc.) are injected to create the location cloaking region, which is even similar to the Exclusion Zone (EZ) proposed by NTIA [28]. However, this work intends to examine how the design (i.e., privacy, spectrum efficiency, and power interference) would be different when the DSA system includes a large number of SUs. In other words, we aim to investigate how the user diversity can be fully leveraged to better protect IU's location privacy. Next, we will elaborate each function block in more details.

5.2 Location Cloaking Set

The application of standard differential privacy in statistical database is intended to "hide" a true database in its "neighbouring databases" which are obtained by adding or removing one record (or one user). However, location protection for a user only involves a single record, which is his own location. Hence, differential privacy in this context requires the definition of "neighbouring" location points to the targeted user's location. One intuitive method is to include a set of "neighbouring" locations and the user's actual location in a *location set*. In this case, differentially private mechanism can be applied to it such that a perturbed location is released but the real location cannot be differentiated among other instances in this set.

Instead of using a fake location, we argue that releasing the location of an operating SU to represent the location of IU is more beneficial. The reasons are two-fold. First, if the adversary with certain prior information knows that no radio devices are transmitting at the released fake location, it can confidently exclude it from the locations where the IU could possibly operate, thus reducing the size of the anonymity set. Second, releasing "IU's" location, regardless of the real or fake one, inevitably restricts SUs' spectrum access and reduces the spectrum efficiency. However, reporting the location of a SU (e.g., a pair of transceivers or a WiFi access point along with its served users) could reduce the overall spectrum efficiency loss because the SAS database protects it from power interference in the same way as how the IU is protected.

With this in mind, we intend to construct a location cloaking set containing the real IU and its "neighbouring" SUs. However, selecting the location cloaking set is by no means a trivial task especially when it comes to protect IU's location against operating SUs. In particular, at t_0 when the IU comes, some SUs might be cleared due to their interference to the IU, which unfortunately could help these SUs geo-locate the IU given this "firsthand experience". Moreover, after a long time observation from t_0 to t_N, all instances (i.e., locations) in the location cloaking set are likely released. Without proper design, the IU's location could be the "outlier" among others which is easily discerned. For instance, in [8], Bahrak *et al.* create a K-anonymity cloaking set by including $K-1$ nearest users around the targeted IU. However, we argue that using nearest neighbouring users may compromise IU's location in a scenario as shown in Fig.3. Since the adversary knows all locations in the cloaking set after continuous observations, the adversary could confidently decide u^* is IU's real location as the cloaking sets would have been different if u_1, u_2 or u_3 were the real IU.

The above observation motivates us to design a location cloaking set satisfying the following two properties: (1) any user/location in the location cloaking set excludes its interfered SUs; (2) the location cloaking set should preserve *reciprocity* whose definition can be found in [29].

To give a general picture, Alg.1 outlines the procedures in creating the location cloaking set. Firstly, based on the accurate channel fading model (e.g., Longley-Rice (L-R) model [30]) available at the SAS database and the operating parameters of all users, the SAS database is aware of

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2019.2897099, IEEE Transactions on Mobile Computing

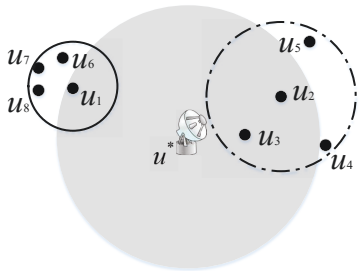
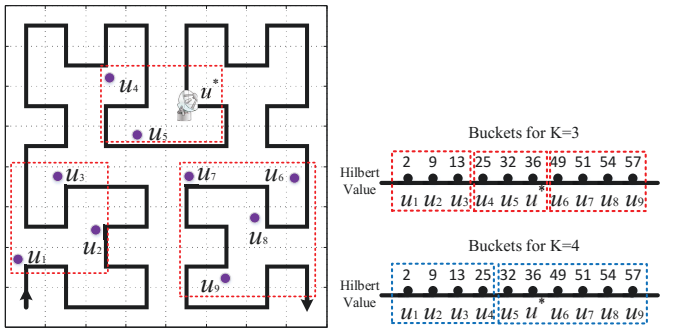


Figure 3: An example of forming the location cloaking set using nearest neighbouring users. Suppose the size of location cloaking set is 4 and $\{u^*, u_1, u_2, u_3\}$ is the cloaking set via nearest neighbouring algorithm. However, if u_1 were the IU, its cloaking set would have been $\{u_1, u_6, u_7, u_8\}$. Similarly, if u_2 were the IU, its cloaking set would have been $\{u_2, u_3, u_4, u_5\}$.



(a) 8×8 Hilbert Curve (b) User's sorted Hilbert values

Figure 4: Forming location cloaking sets of different sizes based on 8×8 Hilbert Curve.

Algorithm 1 Creating the Location Cloaking Set

Input: channel fading model; operating frequency, location, transmit power of all users; system parameters: ε_{th}, $\Lambda_{u^*}^{th}$, φ, x_{u^*}.

Output: location cloaking set $\mathcal{X}$.

1: Construct a conflict graph $G(V, E)$;
2: Find the maximum independent set $\mathcal{I}_{u^*}$;
3: Calculate the size of location cloaking set from (10);
4: Create the location cloaking set $\mathcal{X}$ of size K from $\mathcal{I}_{u^*}$.

the interference relationship between any two users and can construct a conflict graph $G(V, E)$. Specifically, each vertex v ($v \in V$) represents each user while an edge (u, v) ($(u, v) \in E$) between two vertices u and v indicates these two users interfere with each other (or conflict). Secondly, using $G(V, E)$, the SAS database then determines the maximum independent set (MIS) [31] $\mathcal{I}_{u^*}$ which includes the real IU u^*. The algorithm in [31] can be utilized as an efficient approach to constructing the MIS that includes the real IU.

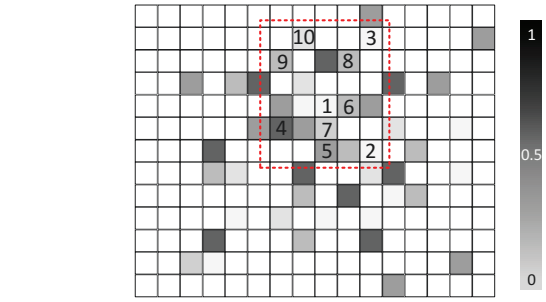
Next, we determine the size of the location cloaking set to guarantee a certain level of inference errors for Bayesian adversaries, and then we can create the location cloaking set of size K from $\mathcal{I}_{u^*}$. From our prior discussion, in Step 4 of Alg.1, the location cloaking set should be constructed to preserve *reciprocity*, which naturally leads us to an approach using the Hilbert space-filling curve [32]. The Hilbert curve maps the 2-D Cartesian coordinate of each user into a 1-D value, and provides that if two points are in close proximity in 2-D space, with high probability they will also be close after 1-D transformation. Fig.4, for instance, illustrates the location of 10 users and the Hilbert curve for a 8×8 space partitioning. It also shows users' sorted Hilbert values and how to construct cloaking sets of different sizes. In particular, users are split into K-buckets, each of which contains exactly K users except the last one which may contain at most 2·K-1 users. The cloaking set generated in this respect satisfies *reciprocity* because all users in the same bucket will generate the same cloaking set. Enlightened by the algorithm in [33], the cloaking set can be generated by the following procedures. Firstly, the SAS database obtains IU's Hilbert value $H(u^*)$ and gets its position R_{u^*} in the sorted sequence of all instances in $\mathcal{I}_{u^*}$. Given K, the SAS database then calculates the start and end positions defining the K-bucket that includes $H(u^*)$, as follows:

$$start = R_{u^*} - (R_{u^*} \bmod K)$$
$$end = start + K - 1$$

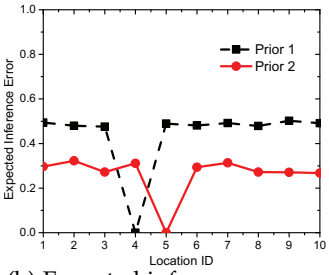
After the location cloaking set of K users are formed, the SAS database will exclude all other users that interfere with any of these K users. We will show later in Section 6 that the proposed Alg.1 can prevent adversaries from discerning the real IU from these $K - 1$ avatar SUs. Next, the natural question arises that how the size of K should be chosen. As it is shown in Fig.2, DP obfuscation mechanism is applied to this location cloaking set to provide geo-indistinguishability for these K users. However, studies [23] have shown that the notion of differential privacy does not protect against Bayesian inference attacks using prior information; whereas the other privacy notion, namely, the *expected inference error*, promotes resilience to Bayesian inference attacks but lacks differential privacy guarantee in terms of geo-indistinguishability. Therefore, we intend to combine these complementary privacy notions to provide double shield protection for the IU's location privacy. Specifically, we base the selection of K on the *expected inference error*, which can be thought of the first phase; then the DP obfuscation mechanism is applied to this location cloaking set in the later phase.

First of all, let us examine the relationship between these two privacy notions. For demonstrative purposes, we give an example to evaluate IU's location privacy by applying differential privacy against Bayesian inference attack. As shown in Fig.5(a), the adversary may have a prior knowledge (denote as *prior 1*) of IU's appearance at a specific location at a given area of its interest. On the other hand, the adversary could obtain some side information that eliminates *loc.#4* as the possible IU's locations (denote as *prior 2*). We apply the exponential mechanism [23] to achieve differential privacy on the location cloaking set of 10 possible locations. The adversary's expected inference errors for IU's appearance at any of these locations are evaluated based on (2) and (3). As shown in Fig.5(b), the adversary could identify IU at *loc.#4* or *loc.#5* when adversary has *prior 1* or *2*, respectively. This figure also shows that by eliminating *loc.#4* as the possible locations from the cloaking set, the adversary could increase its inference success

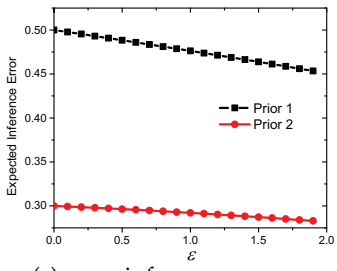
This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2019.2897099, IEEE Transactions on Mobile Computing



(a) The adversary's prior information on IU's location at a 16×13 region.



(b) Expected inference error



(c) ε v.s. inference error

Figure 5: Demonstrative example of how differential privacy can protect IU's absolute location privacy when adversary has different prior knowledge.

probability at every other possible location. In particular, considering the adversary with *prior 1* and the IU operating at *loc.#6*, Fig.5(c) plots how differential privacy could help protect IU's location privacy. We can see that the adversary's expected inference error decreases as the parameter ε increases. However, with the improved prior information, the adversary's inference error can be reduced despite the protection of differential privacy. Clearly, we can conclude that the adversary with different prior knowledge has different capability to compromise IU's absolute location privacy in terms of the inference error. The extreme case would be that the adversary having certain prior information could uniquely geo-locate IU while differential privacy clearly has no control over it.

From the above numerical analysis, we conclude that differential privacy is not robust to ensure absolute location privacy guarantee against Bayesian adversaries with certain prior knowledge. Furthermore, we also observe that when differential private mechanism is applied in the location cloaking set, it allows the adversary to narrow its guesses in a smaller area. Therefore, we propose a dynamic selection of the size of cloaking set K by taking the adversary's prior knowledge π and IU's privacy requirement φ into consideration. Next, we will theoretically explore how to decide K in accordance to π and φ. First, let us assume $\widetilde{x_{u^*}} = \arg\max_{x \in \Psi} \Pr(x|x_{\widehat{u}})$ to be the Bayesian adversary's estimated location. Based on (3), the conditional expected inference error can be calculated as:

$$\begin{aligned} Err &= \sum\nolimits_{x \in \mathcal{X}} \frac{\Pr(x|x_{\widehat{u}})}{\sum_{y \in \mathcal{X}} \Pr(y|x_{\widehat{u}})} \cdot d_h(\widetilde{x_{u^*}}, x) \\ &= \sum\nolimits_{x \in \mathcal{X}} \frac{\pi(x) \Pr\left(\mathcal{A}(x_{\widehat{u}}|x)\right)}{\sum_{y \in \mathcal{X}} \pi(y) \Pr\left(\mathcal{A}(x_{\widehat{u}}|y)\right)} \cdot d_h(\widetilde{x_{u^*}}, x) \\ &\geq e^{-\varepsilon} \sum\nolimits_{x \in \mathcal{X}} \frac{\pi(x)}{\sum_{y \in \mathcal{X}} \pi(y)} \cdot d_h(\widetilde{x_{u^*}}, x) \\ &\geq e^{-\varepsilon} \sum\nolimits_{x \in \mathcal{X}} \frac{\pi(x)}{\sum_{y \in \mathcal{X}} \pi(y)} \cdot d_h(\widetilde{x_{u^*}}', x) \\ &= e^{-\varepsilon} \sum_{x \in \mathcal{X} \setminus \{x = \widetilde{x_{u^*}}'\}} \frac{\pi(x)}{\sum_{y \in \mathcal{X}} \pi(y)} \end{aligned} \tag{7}$$

where the first inequality is due to (5) and the second inequality is due to $\widetilde{x_{u^*}}' = \arg\max_{x \in \mathcal{X}} \Pr(x|x_{\widehat{u}})$, which means the guessed location is now within the cloaking set. Above equation validates our numerical analysis in the previous discussion, where the adversary's inference error or IU's absolute location privacy is dependent on adversary's prior knowledge $\frac{\pi(x)}{\sum_{y \in \mathcal{X}} \pi(y)}$ whereas given an ε, differential privacy only guarantees a lower bound of it. Due to the fact that the SAS database may not know the adversary's prior information, we consider a simple scenario that all locations in $\mathcal{X}$ have equal prior probability and $\frac{\pi(x)}{\sum_{y \in \mathcal{X}} \pi(y)}$ would be $\frac{1}{K}$. As a result, (7) becomes

$$Err \geq e^{-\varepsilon}(1 - \frac{1}{K}) \tag{8}$$

Here, ε is chosen as the privacy budget for DP obfuscation and we shall see in Section 5.5 that any allocated privacy budget ε should be no greater than ε_{th}. Thus, the inequality (8) can be further written as follows:

$$Err \geq e^{-\varepsilon}(1 - \frac{1}{K}) \geq e^{-\varepsilon_{th}}(1 - \frac{1}{K}) \tag{9}$$

To guarantee the protection for IU's location privacy satisfies its specified requirement φ in any DP obfuscation case, we have to let $Err \geq \varphi$. To ensure that, it is sufficient to satisfy that $e^{-\varepsilon_{th}}(1 - \frac{1}{K}) \geq \varphi$. According to (9), we can see that the size of location cloaking set can be determined as follows:

$$K \geq \frac{1}{1 - e^{\varepsilon_{th}} \varphi} \tag{10}$$

Intuitively, the size of cloaking set should be set as large as possible. However, we shall see later that the larger of the cloaking set size, the higher the computational complexity in the obfuscation phase. Besides, when the cloaking set is large enough, the obfuscated locations may be distant from the IU's location which as a result will cause high obfuscation error in terms of power interference to the IU. Therefore, we can select K as the lower bound value in (10).

5.3 Interference Check

After the IU joins the system and the location cloaking set being constructed at t_0, new SUs could join the system at any time instant from t_0 to t_N. To avoid harmful interference to the IU while guaranteeing the IU is not inferred from the deterministic feature about releasing the IU as soon as the interference threshold exceeds, we propose that any avatar SU or the real IU will be released if the incoming SUs' transmissions interfere with it. In so doing, the adversary is expected to be incapable of discerning the IU from other avatar SUs from this function block.

To be specific, the aggregated power interference to any user in the location cloaking set is described as follows:

$$P_{\text{int},u} = \sum_{u' \in \mathcal{I}_u} P_{u'} \cdot h_{u',u} \tag{11}$$

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2019.2897099, IEEE Transactions on Mobile Computing

where $\mathcal{I}_u$ is the set of SUs that interfere with the user u in the location cloaking set; $P_{u'}$ is the transmit power of the SU u'; and $h_{u',u}$ represents the wireless channel gain between u and u'. Since the SAS database adopts accurate radio propagation model or deploys in-field sensors for interference management, the element of $\mathcal{I}_u$ can be easily obtained. Thus, the aggregated power interference $P_{\text{int},u}$ can be calculated in a timely manner.

Whenever the power interference exceeds the threshold, the interfered avatar SUs or the real IU will be released as the "avatar" IU and the respective interfering SUs will be excluded.

5.4 IBA Adaptive Sampling

If the interference threshold for all users in the location cloaking set is not violated at t_i, the DPavatar scheme then verifies whether to perform DP obfuscation or not. The reason is that each obfuscation comes at the cost of privacy budget (ϵ) while the total budget is constant. We are thus motivated to apply a sampling mechanism to select certain time instants for the DP obfuscation while reusing the previously released avatar IU between two consecutive obfuscation time instants, as shown in Fig.2. Although in this way the budget can be saved for future usage, using one avatar IU for a long time may cause power interference to other avatars or even the real IU. Based on this observation, we need to design an adaptive sampling mechanism by jointly considering the incurred power interference and the remaining privacy budget.

The previous work [34] in the context of numerical data (or histograms) publications adopt PID control [35] to adjust the sampling rate according to historical data dynamics. However, the framework therein uses a fixed rate sampling scheme and allocates equivalent budget to each predefined sampling time instant, which is not desirable in our setting to keep tracking of aggregated power interference (i.e., feedback error) as well as the remaining privacy budget and to adjust the sampling rate on-the-fly. In this paper, we propose a novel **I**nterference and **B**udget **A**ware adaptive sampling mechanism based on feedback error to cast a balance on power interference and remaining privacy budget. In particular, we use the PID control to characterize the effect of power interference on sampling intervals, and then determine the next sampling time instant by jointly considering the remaining privacy budget.

In our framework, the feedback error measure is defined as the proportion of the power interference increase between two sampling time instants to the remaining interference tolerance budget, as shown below:

$$E_{t_n} = \left(P_{\text{int}}^{t_n} - P_{\text{int}}^{t_{n-1}}\right) \Big/ \max\{\Lambda_{u^*}^{th} - P_{\text{int}}^{t_n}, 0\}, \tag{12}$$

where $P_{\text{int}}^{t_n} = \max\{P_{\text{int},u_1}^{t_n}, P_{\text{int},u_2}^{t_n}, ..., P_{\text{int},u_K}^{t_n}\}$ measures the largest power interference level of one particular user in the location cloaking set. We treat every user equally so that adversaries cannot deduce extra information from the variation of sampling time instants.

Furthermore, the remaining interference tolerance budget defined in (12) captures that the feedback error is infinity if the interference power exceeds IU's threshold, whereas the feedback error is a proportional measure of the interference increase if not. Then, we can apply the PID control to evaluate the effect of feedback errors on the sampling rate. First of all, the PID error control law Δ is defined as follows:

$$\Delta = C_p E_{t_n} + C_i \frac{\sum_{j=n-T_i+1}^{n} E_{t_j}}{T_i} + C_d \frac{E_{t_n} - E_{t_{n-1}}}{t_n - t_{n-1}} \tag{13}$$

where the first term represents the *proportional* error with C_p being the proportional gain which amplifies the current error; the second term is the *integral* error standing for the accumulated error in the past T_i integral time window and C_i denotes the integral gain; the third term is the *derivative* error capturing the predicted errors to prevent large errors in the future with C_d being the derivative gain. In general, the control gains C_p, C_i and C_d denote the weights that account for the final calibrated PID error control and they satisfy the following constraints:

$$\begin{aligned} &C_p, C_i, C_d \geq 0 \\ &C_p + C_i + C_d = 1 \end{aligned} \tag{14}$$

From our prior discussion, we know the sampling rate should increase when the feedback error is high. In other words, avatar IUs should be frequently released to suppress the power interference due to the incoming SUs. With this in mind, the adjusted new sampling interval (the time between two sampling time instants) can be determined as:

$$I' = \max\{1, I + \theta(1 - e^{\Delta - \nu \cdot \lambda_r})\}, \tag{15}$$

where θ is the system parameter to adjust the sampling interval and ν is the scaling factor to unify the PID error control and the remaining budget λ_r which is $\frac{1}{\varepsilon_r}$. Here, we assume the smallest sampling interval is 1. The time unit could be in any degree of granularity such as seconds, minutes or hours depending on the time scale of SUs' joining rate. The reason of applying (15) to determine sample interval is as follows. It is intuitive that the sampling interval I is a decreasing function w.r.t. PID control error Δ and remaining privacy budget ε_r. In other words, obfuscation should be applied frequently when PID error is large (to avoid interference) or when there is enough privacy budget left (to select an avatar with high utility). That is to say ε_r (or λ_r) and Δ jointly affect whether the sampling interval should be reduced or increased. Thus, ν is introduced as a weighting factor to bias between λ_r and Δ for determining a new sample interval. Specifically, $e^{\Delta - \nu \cdot \lambda_r}$ is greater than 1 when $\Delta > \nu \cdot \lambda_r$ and the new sampling interval is reduced; and $e^{\Delta - \nu \cdot \lambda_r}$ is less than 1 when $\Delta < \nu \cdot \lambda_r$ and the new sampling interval is increased.

5.5 Dynamic Budget Allocation

Next, if t_i is the sampling time instant, it implies that the DP obfuscation should be performed over the location cloaking set. Thus, our next objective is to determine the amount of privacy budget to be allocated for the obfuscation.

In this section, we propose a dynamic budget allocation mechanism that adapts to the variation of sampling intervals and allocates privacy budget accordingly to guarantee (ω, ε)-privacy in the sense that the sum of budget usage within any sliding window of length ω is less than the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2019.2897099, IEEE Transactions on Mobile Computing

total budget ϵ. Recall that in the prior IBA adaptive sampling mechanism, the sampling interval decreases when the feedback error increases. In other words, we anticipate more sampling time instants within a time window of length ω, which as a result leads us to allocate smaller share of budget at each sampling time instant so that more available budget will be reserved for the successive ones. On the contrary, when the feedback error decreases, we have fewer sampling time instants within the ω time window and thus a large fraction of remaining budget can be allocated at the current sampling time instant to preserve utilities.

With this in mind, we need to first obtain the remaining budget in window $[n-\omega+1, n]$ as $\varepsilon_r = \varepsilon - \sum_{i=n-\omega+1}^{i=n-1} \varepsilon_i$. Next we need to determine the fraction of privacy budget to be allocated at the current sampling time instant. Based on our previous analysis, we realize the logarithmic function can perfectly capture the relationship between the sampling interval $I^{'}$ and the fraction f. Thus, we define the amount of the privacy budget allocated at the current sampling time instant as follows:

$$\varepsilon_n = \min\{\mu \ln(I^{'}+1) \cdot \varepsilon_r, \varepsilon_{th}\} \tag{16}$$

where μ is the normalizing factor to scale the fraction in $(0, 1)$ and we use $\ln(I^{'}+1)$ instead of $\ln I^{'}$ in order to avoid zero since $I^{'}$ could be 1. Besides, the reason we setup a minimum privacy budget is to prevent from leaving too few budget to the future.

5.6 Differentially Private Location Obfuscation

Given location cloaking set $\mathcal{X}$, our scheme achieves differential privacy (with privacy budget ε_n) on it to protect IU's location. We attempt to obtain an optimal obfuscation mechanism $\mathcal{A}(\cdot|\cdot)$ in such a way that the utility loss is minimized while the differential privacy guarantee and the interference protection are satisfied. In particular, the mechanism $\mathcal{A}(\cdot|\cdot)$ achieving differential privacy means that any two users in the location cloaking set have approximately the same probability (within a factor of e^{ε}) to generate the released avatar IU. The utility loss in our context is defined as the loss in spectrum efficiency.

In our proposed scheme, operating SUs instead of non-existing dummy users are selected to obfuscate the real IU's location. The benefit is that when an avatar SU is released as an IU, it is protected from harmful interference so its quality of service is guaranteed. Even though the avatar SU rejects its interfering SUs in the same way as the real IU, the overall spectrum efficiency loss is much less than that by relying on non-existing users. Specifically, the utility loss in spectrum efficiency (bits/s/Hz) by releasing avatar u as IU can be described as follows:

$$c(u) = \sum_{u^{'} \in I_u} \log_2(1 + \frac{P_{Rx}(u^{'})}{P_{\text{int},u^{'}} + N_0}) - \left[\log_2\left(1 + \frac{P_{Rx}(u)}{\min\{\Lambda_{u^*}^{th}, P_{\text{int},u}\} + N_0}\right) - \log_2(1 + \frac{P_{Rx}(u)}{P_{\text{int},u} + N_0})\right] \tag{17}$$

where $P_{Rx}(*)$ is the receiving power at a particular user and $P_{\text{int},*}$ is the aggregated interference power on that user which can be calculated in the same way as in (11). Note that the first term represents the loss of spectrum efficiency by expelling SUs while the latter two terms in square brackets indicate the spectrum efficiency gain due to elevating the avatar SU to become the IU. In particular, if the real IU is released, the utility loss in spectrum efficiency is calculated as follows:

$$c(u^*) = \sum_{u \in I_{u^*}} \log_2(1 + \frac{P_{Rx}(u)}{P_{\text{int},u} + N_0}) \tag{18}$$

With the utility function defined as above, we also assume a prior π over $\mathcal{X}$, representing the probability of the real IU being at any location at any given time. Therefore, given the allocated privacy budget ε_n at n^{th} sampling time instant, we can construct an optimal mechanism by solving a linear optimization problem, minimizing the expected utility loss while satisfying ε_n-differential privacy:

$$\begin{aligned}
\underset{\mathcal{A}}{\text{minimize}} \quad & \sum_{x_{u^*}, x_{\widehat{u}} \in \mathcal{X}} \pi(x_{u^*}) \Pr(\mathcal{A}(x_{\widehat{u}}|x_{u^*})) c(\widehat{u}) \\
\text{subject to} \quad & \Pr(\mathcal{A}(x_{\widehat{u}}|x_{u^*})) \le e^{\varepsilon_n} \Pr\left(\mathcal{A}(x_{\widehat{u}}|x^{'})\right) && x_{u^*}, x^{'}, x_{\widehat{u}} \in \mathcal{X} \\
& \sum_{x_{\widehat{u}} \in \mathcal{X}} \Pr(\mathcal{A}(x_{\widehat{u}}|x_{u^*})) = 1 && x_{u^*} \in \mathcal{X} \\
& 0 \le \Pr(\mathcal{A}(x_{\widehat{u}}|x_{u^*})) \le 1 && x_{u^*}, x_{\widehat{u}} \in \mathcal{X} \\
& \mathbb{E}(P_{\text{int},u^*}) \le \Lambda_{u^*}^{th} && x_{u^*} \in \mathcal{X}
\end{aligned} \tag{19}$$

In the above optimization problem, the first three constraints are set to guarantee differential privacy while the last constraint is to make sure the expected interference to the real IU by releasing $\widehat{u}$ does not exceed the threshold. More explicitly, the fourth constraint can be written as follows:

$$\sum_{x_{u^*} \in \mathcal{X}} \sum_{x_{\widehat{u}} \in \mathcal{X}} \pi(x_{u^*}) \Pr(\mathcal{A}(x_{\widehat{u}}|x_{u^*})) \sum_{u \in I_{u^*} \setminus I_{\widehat{u}}} P_u h_{u,u^*} \le \Lambda_{u^*}^{th}. \tag{20}$$

We also observe that there are $|\mathcal{X}|^2$ decision variables and up to $O(|\mathcal{X}|^3)$ constraints in (19). Based on our analysis at Section V.A, it is clear that with the increasing size of the location cloaking set, the IU's location privacy is better preserved but the computational complexity will increase dramatically. We will examine this tradeoff in the following evaluation section. As far, after the optimal obfuscation strategy $\mathcal{A}$ is obtained, the SAS database could follow this probabilistic distribution and release the avatar IU accordingly. To have a clearer picture of the working flow and interactions of the above-mentioned mechanics, Algorithm 2 sketches the outline of DPavatar protection scheme.

6 Privacy Analysis

We show in this section that the design blocks, namely the location cloaking set and the IBA adaptive sampling, leaks no extra information to adversaries facilitating their attacks to our scheme. Based on that, we prove the proposed DPavatar scheme achieves (ω, ε)-privacy over the IU's operating time. Before the analysis, we pose one fundamental assumption that adversaries cannot manipulate the SAS database by registering fake SUs at certain locations due to the authentication process.

Firstly, the location cloaking set is constructed to preserve *reciprocity* through searching for the MIS and then

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2019.2897099, IEEE Transactions on Mobile Computing

Algorithm 2 DPavatar Protection Scheme

Input: user join/leave dynamics; channel fading model; system parameters: ε, ω, θ, υ, ε_{th}, μ, C_p, C_i, C_d; IU's parameters: $\Lambda_{u^*}^{th}$, φ, x_{u^*}; the next sampling time instant ns, the time span N.

Output: $x_{\widehat{u}}$

construct the location cloaking set according to Alg.1;
$ns \leftarrow 1$; $I \leftarrow 1$
for n = 1:N **do**
  for i = 1:K **do**
    if $P_{\text{int},u_i}^n > \Lambda_{u^*}^{th}$ **then**
      release $x_{\widehat{u}}^{ns} \leftarrow x_{u_i}^n$;
      jump to Step 3;
    end if
  end for
  if n == ns **then**
    n is the sampling time instant;
    calculate P_{int}^n according to (11);
    calculate PID error Δ according to (13);
    update interval $I^{'}$ according to (15);
    $ns \leftarrow ns + I^{'}$; $I \leftarrow I^{'}$;
    compute remaining budget $\varepsilon_r = \varepsilon - \sum_{i=n-\omega+1}^{i=n-1} \varepsilon_i$;
    calculate budget allocation ε_n from (16);
    solve the optimization problem (19) and obtain $\mathcal{A}$;
    release $x_{\widehat{u}}^n$ according to $\mathcal{A}$;
  else
    n is not the sampling time instant; keep using $x_{\widehat{u}}^{ns}$;
  end if
end for

using Hilbert curve. Although the number of MISs in a graph is dependent on the number of vertices n and edges, normally for a random graph (without adversarial manipulations) like our scenario, the number of MISs containing the real IU is at least $n^{1-\tau}$ (τ is a small value) whereas the number of elements in any MIS is almost surely $2\,(1 + O\,(1))\log_2 n$ [36]. This indicates that the operating SUs and adversaries have extremely low probability to discern the IU from the MIS phase when the number of operating SUs are large. On the other hand, the sufficient number of elements in any MIS guarantees the Hilbert curve can be applied to construct the location cloaking set to preserve *reciprocity*.

Secondly, it seems that adversaries can learn from the change of sampling intervals to gain extra information about where the IU is. However, the IBA adaptive sampling block calculates the sampling interval based on the maximum power interference to all the users in the location cloaking set. By doing so, adversaries cannot deduce the specific user, to which the power interference causes to, actually results in the variation of the sampling interval.

Last but not least, we argue that the DPavatar scheme preserves (ω, ε)-privacy for the IU from t_0 to t_N. First of all, the DP obfuscation scheme is applied to the location cloaking set that has been proven to be private and it cannot be manipulated in any stage. Then, we see that the dynamic budget allocation guarantees that $\sum_{i=n-\omega+1}^{i=n-1} \varepsilon_r \leq \varepsilon$ for any slide window of size ω, and at any sampling time instant $\varepsilon_{th} \leq \varepsilon_n \leq \varepsilon$. Therefore, the DP obfuscation at any time instant is ε_n-differential privacy and consequently, the DPavatar scheme is (ω, ε)-privacy across t_0 to t_N.

7 Performance Evaluation

In this section, we conduct simulations to evaluate the performance of our DPavatar scheme, and compare it with other differentially private mechanisms on utility and privacy.

We focus on an 13×13 Km^2 geographical area, where the IU could possibly operate. At the initialization as shown in Fig.6, we randomly generate 50 users and scatter them into this area. We select randomly one and set it as the IU, for instance the solid dot in Fig.6, whose interference tolerance threshold is assumed as 0dBm and personalized privacy requirement is φ. For the channel model, we consider the large scale fading which is described as $P_{Rx} = \gamma d^{-\xi} P_{Tx}$ [37]. Here, we set the antenna gain γ=2.5, the transmitting power P_{Tx}=10W and the path loss factor ξ=4, while d is the Euclidean distance between transceiver pairs. We assume that two nodes interfere with each other when the interference power exceeds -40dBm and we can therefore build a bipartite interference graph for these users, as shown in Fig.6. Also considering the AWGN channel, we assume the noise power $N_0 = 10^{-9}$W. Since we consider the real-time scenario, we assume that the IU's operation duration is 30 minutes and the granularity of SUs' joining/leaving rate is in seconds. To be specific, we set each time interval to be 10 seconds, during which with probabilities α and β one SU joins and leaves the DSA system, respectively. Equivalently, we can claim that on average the SUs' net arrival rate is $\rho = 6\,(\alpha - \beta)$ users/minute. Note that here the departing SUs are those who finish their services but not the expelled SUs. On the other hand, incoming SUs are admitted according to SAS database access control and they are randomly placed in this area. In the simulation, we set $\{C_p, C_i, C_d\} = \{1, 0, 0\}$, θ=5, υ=0.1, ε_{th}=0.3, μ=0.1 while privacy budget ϵ and time window ω are evaluated to examine their impacts on the performance.

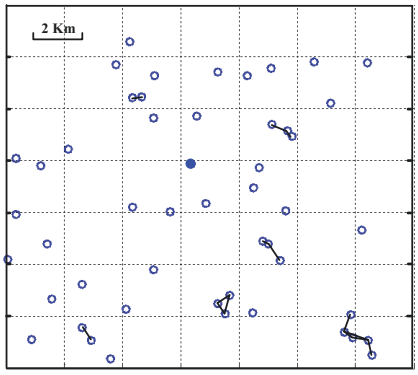
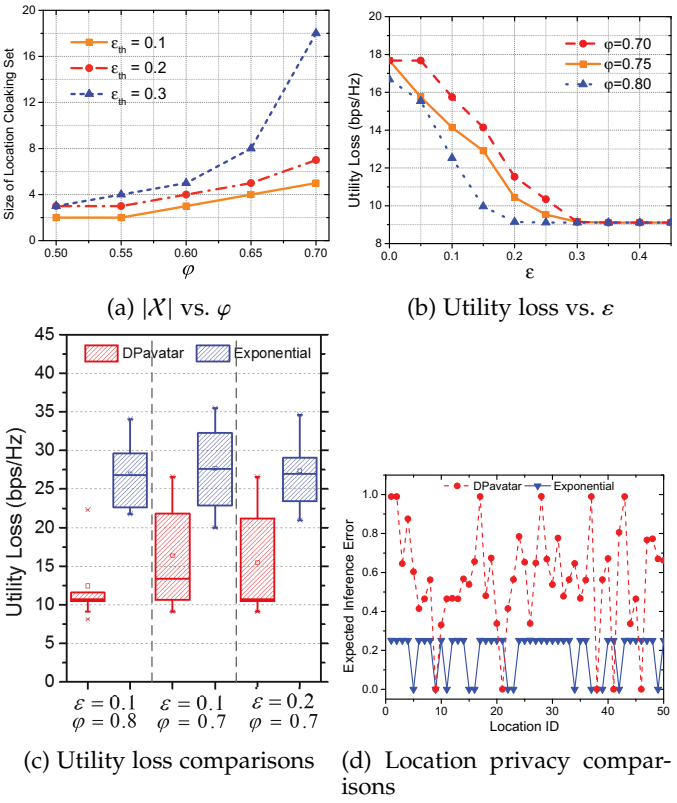


Figure 6: The initialization of simulations, where 50 users are distributed in an 13×13 Km^2 area and their bipartite interference relationship is also given.

The metrics we use in the evaluation are the following: the size of $\mathcal{X}$, the computational time in DP obfuscation, the utility loss concerning spectrum efficiency, the privacy in terms of the adversary's expected inference error, the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2019.2897099, IEEE Transactions on Mobile Computing



(a) $|\mathcal{X}|$ vs. φ (b) Utility loss vs. ε

(c) Utility loss comparisons (d) Location privacy comparisons

Figure 7: System performance at a given sampling time instant.

aggregated power interference to the IU. We examine how the designed variables impact the system performance with respect to these metrics.

7.1 Performance of the Obfuscation at a Sampling Time Instant

First, we focus on evaluating the performance at one specific sampling time instant when the obfuscation mechanism is performed. Simulations are conducted for the IU being at any of these 50 possible locations and we then take the average of 100 independent runs.

$|\mathcal{X}|$ vs. φ. To perform location obfuscation, the location cloaking set should be constructed by taking the adversary's prior knowledge into consideration. Fig.7a indicates the impact of privacy parameter φ and ε on the selection of the location cloaking set. For the same ε, with the increase of φ, the cloaking set size (technically, the lower bound) becomes larger because more SUs should be included for obfuscation to satisfy the IU's higher error (location privacy) demand. On the other hand, for the same φ, the cloaking set size increases when ε increases, which coincides with our theoretical analysis on (7).

Utility loss vs. ε. At the sampling time instant when the location obfuscation is performed according to the optimization problem (19), we can see that the lower the ε is, the tighter the differential privacy constraint (the 1st inequality in (19)) is, which results in more similar probabilistic distributions for every cloaking user. As a result, the released avatar may not be the one giving low utility loss. When ε increases, the utility loss decreases but barely changes when ε becomes large enough as shown in Fig.7b, which coincides with our intuition about differentially private mechanisms. On the other hand, given the same ε, the utility loss decreases when φ increases. The reason is that larger φ gives bigger cloaking set which includes more SUs, which takes advantages of user diversity and could possibly generate an avatar with low utility loss. However, we shall see later that the increase of cloaking set has negative impact on the power interference to the IU.

Utility loss comparison. We compare the utility loss in our scheme with the loss by applying exponential mechanism [23]. The results are shown in Fig.7c, from which we can see that our differentially private mechanism by solving an utility-based optimization problem outperforms the exponential mechanism at any value settings of privacy parameters. Besides, the trend of the utility loss regarding different values of privacy parameters coincides with the previous results.

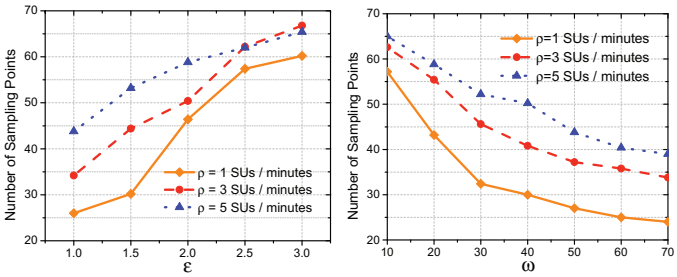
Location privacy comparison. Next, we show the comparison with respect to the location privacy provided by our scheme and the exponential mechanism. As shown in Fig.7d, our scheme at most locations provides higher expected inference error or location privacy than the exponential mechanism. It is interesting to note that the reason for the large variation of inference error in our scheme is that different locations creating the cloaking set have different utility loss values, which is taken into account in the obfuscation mechanism by solving the optimization (19).

Computational Cost for Solving Problem (19)		
$\{\varepsilon_{th}, \varphi\}$	$\lvert\mathcal{X}\rvert$	Time(s)
$\{0.1, 0.7\}$	5	0.0156
$\{0.25, 0.7\}$	10	0.1092
$\{0.25, 0.725\}$	15	1.7316
$\{0.27, 0.725\}$	20	8.7985

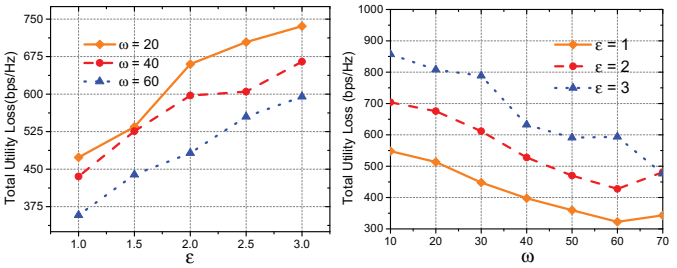
Table 1: Execution time of our obfuscation approach for different values of φ, ε_{th}.

Responsiveness: From previous analysis, we know that larger cloaking set increases adversaries' expected inference error. Here we examine the computational time for solving optimization (19) w.r.t. different sizes of cloaking set. Note that the delay of our framework mainly comes from constructing the location cloaking set, calculating privacy budget and solving optimization problem (19). On one hand, the cloaking set construction is a one-time computation at the system initialization which can be considered to have no impact on the responsiveness of our framework in later time. On the other hand, solving optimization problem (19) dominates the delay of our framework while the overhead for calculating privacy budget can be neglected. Thus, we only consider the responsiveness of our framework according to the delay incurred in solving (19). The measurements are based on a desktop of Intel i3 processor and 8GB memory while we use Simplex algorithm to solve problem (19). Table 1 shows that the execution time of our obfuscation approach increases for larger size of cloaking set. However, we anticipate that using spanning graph to approximate the Hamming distance of (19) as in [18] and higher computing capacity in real SAS database (e.g., enterprise-level computers) the responsiveness of our framework will be highly improved.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2019.2897099, IEEE Transactions on Mobile Computing

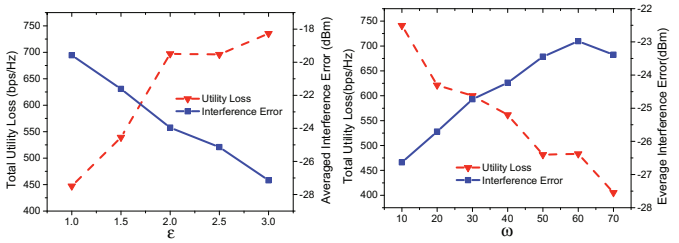


(a) Sampling Times vs. ε (b) Sampling Times vs. ω



(c) Total utility loss v.s. ε (d) Total utility loss vs. ω

Figure 8: Impact of design variables ε, ω on system performance.



(a) Utility vs. error w.r.t. ε (b) Utility vs. error w.r.t. ω

Figure 9: Utility/interference error tradeoff w.r.t. design variables.

7.2 Real-time Performance

Now, we examine the system performance in real-time with SUs joining in and departing from the targeted area. The number of time instants during IU's operation duration can be calculated as $N = 180$. Here, we fix the IU's personalized privacy requirement φ as 0.7.

Sampling Times vs. ε First, we set $\omega = 20$ and examine how the total privacy budget affects the number of sampling points. Here, the sampling point is the time instant when the obfuscation is about to execute. As shown in Fig.8a, the number of sampling points increases with the increase of ε since more privacy budget allows our scheme to squeeze in more sampling time instants in any ω sliding window and each of them could be allocated with a fair amount of ε. Besides, given ε, more incoming SUs cause higher power interference to users in the location cloaking set so the number of sampling time instants increases to suppress the interference.

Sampling Times vs. ω Here, we set privacy budget $\varepsilon = 2.0$ and vary the length of sliding window to see its impact on number of sampling points. As shown in Fig.8b, the number of sampling points reduces when ω increases. The reason is intuitive in the sense that with ε being fixed, the sampling rate is lower when the window size increases in order to save the privacy budget. On the other hand, the more incoming SUs also increases the number of sampling points for the same reason we described previously. It should be noted that the number of sampling time instants affects the computational complexity of the SAS database system since it needs to solve optimization problem (19).

Total utility loss vs. ε Besides the complexity cost we envision, we now show the total utility loss w.r.t. the design parameter ε and ω. First, by setting $\rho = 5$, we conduct simulations to examine the impact of ε on the total utility loss and the results are shown in Fig.8c. Clearly, higher privacy budget gives larger utility loss since our observation at Fig.8a indicates that more frequent obfuscation happens when the privacy budget becomes higher. As a result, the avatar is released more often to expel interfering SUs which brings down the total utility.

Total utility loss vs. ω The same effect can be observed for the design parameter ω as shown in Fig.8d. Larger sliding window size reduces the total utility loss because the obfuscation is not performed frequently enough and not many SUs are expelled.

From the previous analysis, it seems that ε and ω should be designed in such a way that the obfuscation times must be as few as possible to reduce the utility loss. However, we shall see that there is a tradeoff between the utility loss and the IU's interference error, which should be balanced by selecting appropriate ε and ω.

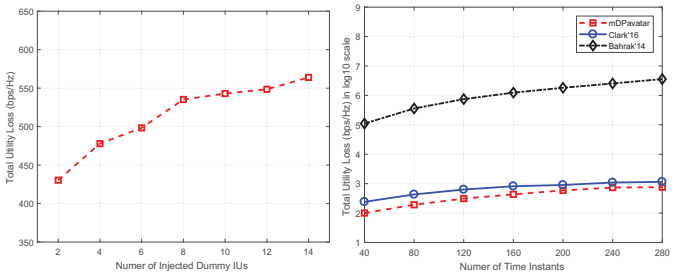
Utility loss vs. interference error w.r.t. ε**.** First, we examine the tradeoff between the total utility loss and the IU's interference error w.r.t. ε. Here, the interference error is averaged across the total time horizon (i.e., $N = 180$) and ω is set to 20. The result shown in Fig.9a indicates that higher privacy budget gives lower average interference error since more obfuscation are performed so that avatars are frequently released to suppress the power interference. On the other hand, an opposite phenomenon is observed for the utility loss curve, whose analysis was given previously. Therefore, there is a clear tradeoff between these two measuring quantities and ε should be chosen to cast a balance between them.

Utility loss vs. interference error w.r.t. ω**.** Similarly, when we conduct simulations on the tradeoff relationship w.r.t. ω, the result shown in Fig.9b implies the same observation. Actually, the design goal should be that ε and ω are chosen to cause as few obfuscation as possible while satisfying the IU's interference error below the threshold.

7.3 Performance Comparison with Other Schemes

To assess the performance of our scheme compared to other state-of-the-art ones, we refer to Clark *et al.* [5] and Bahrak *et al.* [8] as benchmark schemes. Both works focused on location preservation for static IUs under a strong adversary assumption that all SUs are malicious. Specifically, the former work applied power allocation randomization and false location injection interchangeably to maximize IU's privacy-preservation time (coined as *Clark'16*) whereas the latter one obfuscated IU's location in a larger area (coined as *Bahrak'14*). Since our work is based a weaker adversary assumption that operating SUs are not malicious, to make

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMC.2019.2897099, IEEE Transactions on Mobile Computing



(a) Utility loss vs. number of injected dummy IUs.

(b) Utility loss of different schemes.

Figure 10: Comparison with the state-of-the-art schemes.

a fair comparison, we adopt the same threat model as in [5], [8] so the IU has to inject dummy locations whose release still ensures differential-privacy guarantee (coined as *mDPavatar*). However, one can easily expect that the total spectrum-efficiency loss increases as the IU introduces more dummy locations to substitute the untrusted SUs. A simple numerical simulation for an anonymity set of $k = 15$ over $N = 200$ time instants is conducted as shown in Fig.10a.

Note that the simulation settings in *Clark'16*, *Bahrak'14* and our work are different, so we adopt them in our setting for fair comparison. Besides, we follow [5] and break the whole area into small grids, each of which only has one user. IU's privacy is then evaluated using Eq.(3) but the Euclidean distance measurement is applied to unify these three schemes. Moreover, we let these schemes run sufficient amount of time and the total utility loss is then calculated. With respect to a Bayesian adversary in both our work and [5], the IU's corresponding privacy level can be derived after sufficient runtime (or adversary's inference periods).

Since there is a clear tradeoff between privacy and utility, we only compare the utility of these schemes for the same privacy target. Here, we set the privacy level to be 4.3Km and then randomization parameters of these designs can be traced backward. Specifically, in our design, the budget of $\{\varepsilon_{th}, \varphi\} = \{0.25, 0.725\}$ gives an anonymity set of size 15, which satisfies the above privacy level. Similarly, *Clark'16* is estimated to apply a uniform distribution of mean 3.7dB to reduce SUs' power assignment profile for a setting of $P_{Tx} = 10W$ and a new IU's interference threshold -80dBm and this calculation is based on their proposed *single PU error (SPE)* adversarial estimation scheme. In addition, *Bahrak'14* is expected to generate a protected contour of $16.81 \times 16.81 Km^2$ to provide the same privacy level. Notice that a protected contour of such size covers the whole region of interest so *Bahrak'14* serves as the baseline case where the utility loss is the maximum.

Simulation results are shown in Fig.10b. It is clear that our scheme causes the least spectrum-efficiency loss over a long time period, but the performance gap between our scheme and *Clark'16* shrinks as the IU operates longer time. The reason is that when N is relatively small, our scheme selects an avatar with utility awareness as in (19) but *Clark'16* randomizes power allocation attempting to prolong the expected time of privacy preservation [5]. However, as N increases, the gain vanishes as our scheme releases avatars directly without solving (19) due to power interference from joined SUs. In other words, our scheme operates similar to *Clark'16* in the sense that dummy records (in mDPavatar) and obfuscated response (in *Clark'16*) are applied respectively.

8 Conclusion

In this paper, we proposed DPavatar, a real-time differential privacy framework to preserve IU's location privacy. This work novelly leveraged operating SUs as the obfuscated objects and included them in a location cloaking set, in which we developed an utility-optimal differentially private mechanism. We strategically combined differential privacy with the expected inference error in our design to improve IU's location privacy. Moreover, we adopted the (ω, ε)-privacy notion to ensure differential privacy guarantee for the IU in real time. Privacy analysis was given and evaluation results showed that DPavatar framework can achieve better utility and location privacy performance than existing solutions and other differentially private mechanisms.

References

[1] F. C. Commission, "Enabling innovative small cell use in 3.5 ghz band nprm & order," 2012. [Online]. Available: https://apps.fcc.gov/edocs_public/attachmatch/FCC-12-148A1_Rcd.pdf

[2] K. Kim, Y. Jin, D. Kum, S. Choi, M. Mueck, and V. Ivanov, "Etsi-standard reconfigurable mobile device for supporting the licensed shared access," *Mobile Information Systems*, 2016.

[3] U. A. F. E. Segundo, "Ground/air task oriented radar (g/ator)," 2015. [Online]. Available: http://www.dtic.mil/docs/citations/AD1019434

[4] U. M. Corps, "An/tps-80 ground/air task oriented radar (g/ator)," 2017, https://marinecorpsconceptsandprograms.com/programs/aviation/antps-80-groundair-task-oriented-radar-gator.

[5] M. Clark and K. Psounis, "Can the privacy of primary networks in shared spectrum be protected," in *International Conference on Computer Communications (INFOCOM)*. IEEE, 2016, pp. 1–9.

[6] P. R. Vaka, S. Bhattarai, and J.-M. Park, "Location privacy of non-stationary incumbent systems in spectrum sharing," in *Global Communications Conference (Globecom)*. IEEE, 2016, pp. 1–6.

[7] D. of Defense, "Electromagnetic spectrum strategy," 2013. [Online]. Available: http://archive.defense.gov/news/dodspectrumstrategy.pdf

[8] B. Bahrak, S. Bhattarai, A. Ullah, J.-M. Park, J. Reed, and D. Gurney, "Protecting the primary users' operational privacy in spectrum sharing," in *International Symposium on Dynamic Spectrum Access Networks (DySpan)*. IEEE, 2014, pp. 236–247.

[9] A. Robertson, J. Molnar, and J. Boksiner, "Spectrum database poisoning for operational security in policy-based spectrum operations," in *Military Communications Conference (Milcom)*. IEEE, 2013, pp. 382–387.

[10] Z. Zhang, H. Zhang, S. He, and P. Cheng, "Achieving bilateral utility maximization and location privacy preservation in database-driven cognitive radio networks," in *International Conference on Mobile Ad Hoc and Sensor Systems (Mass)*. IEEE, 2015, pp. 181–189.

[11] R. Shokri, G. Theodorakopoulos, C. Troncoso, J.-P. Hubaux, and J.-Y. Le Boudec, "Protecting location privacy: optimal strategy against localization attacks," in *Proceedings of the 2012 ACM conference on Computer and communications security*. ACM, 2012, pp. 617–627.

[12] C. Chen, H. Cheng, and Y.-D. Yao, "Cooperative spectrum sensing in cognitive radio networks in the presence of the primary user emulation attack," *IEEE Transactions on Wireless Communications*, vol. 10, no. 7, pp. 2135–2141, 2011.

[13] L. Zhang, G. Ding, Q. Wu, Y. Zou, Z. Han, and J. Wang, "Byzantine attack and defense in cognitive radio networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 3, pp. 1342–1363, 2015.

[14] J. Liu, C. Zhang, H. Ding, H. Yue, and Y. Fang, "Policy-based privacy-preserving scheme for primary users in database-driven cognitive radio networks," in *Global Communications Conference (Globecom)*. IEEE, 2016, pp. 1–6.

[15] Y. Dou, K. C. Zeng, H. Li, Y. Yang, B. Gao, C. Guan, K. Ren, and S. Li, "P^2-sas: preserving users' privacy in centralized dynamic spectrum access systems," in *Proceedings of the 17th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*. ACM, 2016, pp. 321–330.

[16] C. Dwork, "Differential privacy: A survey of results," in *International Conference on Theory and Applications of Models of Computation*. Springer, 2008, pp. 1–19.

[17] M. E. Andrés, N. E. Bordenabe, K. Chatzikokolakis, and C. Palamidessi, "Geo-indistinguishability: Differential privacy for location-based systems," in *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*. ACM, 2013, pp. 901–914.

[18] N. E. Bordenabe, K. Chatzikokolakis, and C. Palamidessi, "Optimal geo-indistinguishable mechanisms for location privacy," in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2014, pp. 251–262.

[19] Y. Xiao and L. Xiong, "Protecting locations with differential privacy under temporal correlations," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2015, pp. 1298–1309.

[20] K. Chatzikokolakis, C. Palamidessi, and M. Stronati, "Constructing elastic distinguishability metrics for location privacy," *Proceedings on Privacy Enhancing Technologies*, vol. 2015, no. 2, pp. 156–170, 2015.

[21] G. Kellaris, S. Papadopoulos, X. Xiao, and D. Papadias, "Differentially private event sequences over infinite streams," *Proceedings of the VLDB Endowment*, vol. 7, no. 12, pp. 1155–1166, 2014.

[22] Q. Wang, Y. Zhang, X. Lu, Z. Wang, Z. Qin, and K. Ren, "Rescuedp: Real-time spatio-temporal crowd-sourced data publishing with differential privacy," in *International Conference on Computer Communications (INFOCOM)*. IEEE, 2016, pp. 1–9.

[23] L. Yu, L. Liu, and C. Pu, "Dynamic differential location privacy with personalized error bounds," *Network and Distributed System Security Symposium (NDSS)*, 2017.

[24] R. Shokri, "Privacy games: Optimal user-centric data obfuscation," *Proceedings on Privacy Enhancing Technologies*, vol. 2015, no. 2, pp. 299–315, 2015.

[25] C. Dwork, F. McSherry, K. Nissim, and A. Smith, "Calibrating noise to sensitivity in private data analysis," in *Theory of Cryptography Conference*. Springer, 2006, pp. 265–284.

[26] J. Liu, C. Zhang, and Y. Fang, "Epic: A differential privacy framework to defend smart homes against internet traffic analysis," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 1206–1217, 2018.

[27] Q. Wang, Y. Zhang, X. Lu, Z. Wang, Z. Qin, and K. Ren, "Real-time and spatio-temporal crowd-sourced social network data publishing with differential privacy," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 4, pp. 591–606, 2018.

[28] NTIA, "3.5 ghz exclusion zone analyses and methodology," 2015. [Online]. Available: https://www.ntia.doc.gov/report/2015/35-ghz-exclusion-zone-analyses-and-methodology

[29] P. Kalnis, G. Ghinita, K. Mouratidis, and D. Papadias, "Preventing location-based identity inference in anonymous spatial queries," *IEEE Transactions on Knowledge and Data Engineering*, vol. 19, no. 12, pp. 1719–1733, 2007.

[30] U. FCC, "Longley-rice methodology for evaluating tv coverage and interference," *OET Bulletin*, vol. 69, 2004.

[31] J. M. Robson, "Algorithms for maximum independent sets," *Journal of Algorithms*, vol. 7, no. 3, pp. 425–440, 1986.

[32] J. K. Lawder and P. J. H. King, "Querying multi-dimensional data indexed using the hilbert space-filling curve," *ACM Sigmod Record*, vol. 30, no. 1, pp. 19–24, 2001.

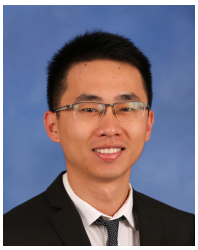
[33] G. Ghinita, P. Kalnis, and S. Skiadopoulos, "Prive: anonymous location-based queries in distributed mobile systems," in *Proceedings of the 16th international conference on World Wide Web*. ACM, 2007, pp. 371–380.

[34] L. Fan and L. Xiong, "An adaptive approach to real-time aggregate monitoring with differential privacy," *IEEE Transactions on Knowledge and Data Engineering*, vol. 26, no. 9, pp. 2094–2106, 2014.

[35] M. King, *Process Control: A Practical Approach*. John Wiley & Sons, 2016.

[36] U. Feige and E. Ofek, "Finding a maximum independent set in a sparse random graph," *Lecture notes in computer science*, vol. 3624, p. 282, 2005.

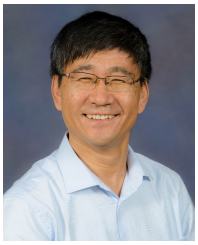
[37] J. Liu, H. Ding, Y. Cai, H. Yue, Y. Fang, and S. Chen, "An energy-efficient strategy for secondary users in cooperative cognitive radio networks for green communications," *IEEE Journal on Selected Areas in Communications*, vol. 34, no. 12, pp. 3195–3207, 2016.



Jianqing Liu (M'18) received the Ph.D. degree from University of Florida in 2018 and the B.Eng. degree from University of Electronic Science and Technology of China in 2013. He is currently an assistant professor in the Department of Electrical and Computer Engineering at University of Alabama in Huntsville. His research interest is to apply cryptography, differential privacy and convex optimization to design secure and efficient protocols for networked systems.

Chi Zhang received the B.E. and M.E. degrees in electrical and information engineering from the Huazhong University of Science and Technology, China, in 1999 and 2002, respectively, and the Ph.D. degree in electrical and computer engineering from the University of Florida in 2011. He joined the School of Information Science and Technology, University of Science and Technology of China, as an Associate Professor in 2011. His research interests include the areas of network protocol design and performance analysis and network security particularly for wireless networks and social networks. He received the 7th IEEE ComSoc Asia-Pacific Outstanding Young Researcher Award. He is a member of the IEEE.

Beatriz Lorenzo (S'08–M'12) received the M.Sc. degree in telecommunication engineering from the University of Vigo, Spain, in 2008, and the Ph.D. degree from the University of Oulu, Finland, in 2012. Since 2014, she has been a Senior Researcher with the Atlantic Research Center for Telecommunication Technologies, University of Vigo. Her research interests include wireless networks, network architectures and protocol design, mobile computing, optimization, and network economics. She received the Fulbright Visiting Scholar Fellowship, University of Florida, from 2016 to 2017.



Yuguang Fang (F'08) received the M.S. degree from Qufu Normal University, China, in 1987, the Ph.D. degree from Case Western Reserve University in 1994, and the Ph.D. degree from Boston University, in 1997. He joined the Department of Electrical and Computer Engineering, University of Florida, in 2000, where he has been a Full Professor since 2005. He held a University of Florida Research Foundation Professorship from 2006 to 2009, a Changjiang Scholar Chair Professorship with Xidian University, China, from 2008 to 2011, and also with Dalian Maritime University since 2015, and a Guest Chair Professorship with Tsinghua University, China, from 2009 to 2012. He is a fellow of the IEEE and AAAS. He was the Editor-in-Chief of the IEEE Transactions on Vehicular Technology from 2013 to 2017 and the IEEE Wireless Communications from 2009 to 2012.