2015 IEEE 12th International Conference on Mobile Ad Hoc and Sensor Systems

Achieving Bilateral Utility Maximization and Location Privacy Preservation in Database-driven Cognitive Radio Networks

Zhikun Zhang, Heng Zhang, Shibo He, Peng Cheng
State Key Laboratory of Industrial Control Technology, Zhejiang University, China
{zhangzhk1993, ezhangheng}@gmail.com, {s18he, pcheng}@iipc.zju.edu.cn

***Abstract*—Database-driven cognitive radio has been well recognized as an efficient way to reduce interference between Primary Users (PUs) and Secondary Users (SUs). In database-driven cognitive radio, PUs and SUs must provide their locations to enable dynamic channel allocation, which raises location privacy breach concern. Previous studies only focus on unilateral privacy preservation, i.e., only PUs' or SUs' privacy is preserved. In this paper, we propose to protect bilateral location privacy of a PU and an SU. The main challenge lies in how to coordinate the PU and SU to maximize their utility provided that their location privacy is protected. We first introduce a quantitative method to calculate both PU's and SU's location privacy, and then design a novel privacy preserving Utility Maximization protocol (UMax). UMax allows for both PU and SU to adjust their privacy preserving levels and optimize transmit power iteratively to achieve the maximum utility. Through extensive evaluations, we demonstrate that our proposed mechanism can efficiently increase the utility of both PU and SU while preserving their location privacy.**

I. Introduction

Cognitive radio networks have been well recognized as an efficient way to increase the spectrum utilization and thus alleviate the spectrum scarcity issue [1][2][3]. In cognitive radio networks, there are two types of users: Primary Users (PUs) and Secondary Users (SUs). PUs have the priority to access the spectrum since they have registered a chunk of spectrum from the spectrum management entity such as FCC while SUs are allowed to access PUs' channels only when the interested channels are vacant.

To enable dynamic channel access, SUs should be aware of which channels are locally available for reuse. There are mainly two ways of achieving this: 1) spectrum sensing and 2) database querying. Spectrum sensing method requests SUs to be equipped with sensors to detect the locally available channels [4][5][6][7]. Interference may occur when detection sensors output false results, which may be caused by obstruction and channel fading. Database querying method requires SUs to provide their accurate locations to a centralized database [8][9][10]. In such a way, SUs can facilely figure out locally available channels and thus efficiently avoid interference by querying a database, which maintains an up-to-date spectrum availability repository.

Since SUs' locations are exposed to enable efficient channel allocation in database-driven cognitive radio networks, this raises location privacy breach risk of SUs. Furthermore, the response from database contains information relevant to the distance of PUs and a queried SU, a malicious SU may infer PUs' locations through seemingly innocuous multiple database queries. The potential privacy breach risk of both PU and SU has been an obstacle to promote database-driven cognitive radio networks.

The previous studies on the location privacy issue in database-driven cognitive radio networks concern only about unilateral privacy, i.e., they assume that one party (PUs or SUs) is trustworthy and try to preserve the other's privacy [11][12]. Further, they fail to quantify the Privacy Preserving Level (PPL) of PUs and SUs, making it difficult to analyze the tradeoff between PPL and spectrum utilization. As aforementioned, both PUs' and SUs' location privacy could be potentially breached and thus should be preserved simultaneously. Simply applying previous results to protect the privacy of PUs and SUs independently will suffer severe utility loss for both parties. As rational users, both parties intend to maximize their PPL to efficiently thwart the attacker's threat. However, PPL and utility are always a paradox, in the sense that unrestricted increase of PPL will result in no available spectrum for SUs to reuse. Therefore, the bilateral location privacy issue should be jointly addressed, in which PUs and SUs can adjust their PPL in order to maximize their utility. Clearly, the traditional two-step database access protocol, i.e. query and response, is impossible for PUs and SUs to adjust their PPL due to the lack of side information about the distance between PUs and the queried SUs.

To address such a challenging issue, we adopt the concept of differential privacy [13] to simultaneously preserve PUs' and SUs' privacy. We consider the case where one PU and one SU are involved. Then we design a quantitative privacy-preserving mechanism which is flexible for the PU and SU to adjust their PPL. With the mechanism framework, we proceed to propose a novel privacy preserving Utility Maximization protocol (UMax) that allows both PU and SU to adjust their PPL to achieve the maximum utility. In UMax, the PU and SU exchange information to decide their optimal PPL in an iterative way. Firstly, the SU chooses a relatively large expected PPL and sends it to database together with an obfuscated location, which is decided by PPL. Secondly, based on SU's expected information, the PU can decide its optimal PPL through solving an optimization problem as depicted in Section IV. Then the database calculates the SU's expected available transmitting radius and responds it to SU. Thirdly, SU adjusts its PPL to achieve a higher utility based on the

978-1-4673-9101-6/15 $31.00 © 2015 IEEE
DOI 10.1109/MASS.2015.93

PU's feedback, then resends it to the database. Finally, the PU decides the maximum transmit power that the SU can adopt to access the spectrum.

The main contributions of this paper are summarized as follows:

1) To the best of our knowledge, this is the first work that simultaneously considers the location privacy-preserving issue for both PU and SU.
2) We design a quantitative mechanism to preserve both PU's and SU's location privacy simultaneously, which is based on the concept of differential privacy.
3) Based on the mechanism framework, we further propose a novel database access protocol which allows PU and SU to adjust their privacy preserving levels. This new protocol consists of four steps, through which, the queried SU and PU can adjust their privacy preserving levels and optimize their transmit power iteratively to achieve the maximum utility.

The rest of this paper is organized as follows. Section VI reviews the related work. Section II introduces the basic database access protocol. In Section III, we propose a novel location privacy-preserving mechanism for PU and SU. In Section IV, we develop a new database access protocol to adjust the PU's and SU's privacy preserving level for improving their utility, respectively. Simulations are performed in Section V to demonstrate the performance of the proposed mechanism. Finally, Section VII concludes this paper.

II. Problem Formulation

A. Basic Database Access Protocol

A typical database-driven cognitive radio network comprises three main components: PUs, SUs and spectrum management database. Database maintains PUs' locations and spectrum utilization information, which consists of PUs' occupied channels and the corresponding protected contour. The protected contour of one channel is an area, where no SUs can transmit when the channel is occupied by PUs. However, if one SU is beyond PUs' protected contour, it is allowed to transmit with a certain power. The farther this SU is located from PUs, the larger power it can transmit. Whenever PUs change their spectrum utilization information, they will notify database to update the repository.

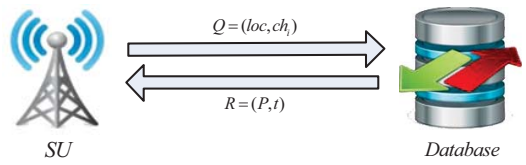


Fig. 1: Basic database access protocol.

We now show a basic database access protocol without considering the privacy breach issue as shown in Fig 1. Firstly, an SU sends a query $Q = (loc, ch_i)$ to database, where $loc = (x, y)$ is the accurate location of the SU and ch_i is the channel which the SU is interested in. Then, after receiving the SU's query, the database responds $R = (P, t)$ to the SU, where P is the Maximum Transmission Power (MTP) of the interested channel, t is the time duration in which the SU can utilize the channel, e.g., if the interested channel is locally unavailable, then the response is $R = (0, 0)$. The MTP can be calculated based on the following function

$$P = \begin{cases} 0, & d \le r_p^0, \\ h(d - r_p^0), & d > r_p^0, \end{cases} \quad (1)$$

where r_p^0 is the protected contour radius of the interested channel, d is the distance between the queried SU and the PU which is closest to the SU, and $h(\cdot)$ is a continuous monotone increasing function.

B. Threat Model and Assumptions

The basic database access protocol is based on the assumption that PUs and SUs trust each other. However, both PUs and SUs may suffer from potential privacy breach threat. This is because, to achieve the locally available channels, SUs should report their locations to database. As service provider, database manager may collect SUs' location information to make market decision or sales strategy, which violates SU's privacy.

In this paper, we assume that the database is an affiliated entity of PUs, e.g. China Mobile may maintain a spectrum management database if it decides to share the registered spectrum with SUs. Thus, we further assume that PUs and database trust each other, and database will not breach PUs' operational information. We also assume that PUs' location privacy threat is only incurred by malicious SUs, e.g., a malicious SU may infer PUs' locations through seemingly innocuous queries as depicted in Section III. Furthermore, we assume that a sophisticated malicious SU can obtain the MTP function which the database adopts [12].

C. Problem of Interest

Considering the potential privacy threat, both PUs and SUs need to adopt an appropriate mechanism to preserve their location privacy. Intuitively, regardless of their utility, PUs and SUs may choose a relatively high PPL. However, unrestricted increase PPL may seriously decrease both PUs' and SUs' utility. Thus we need to deal with the following two problems in our paper:

1) How to devise a quantitative mechanism to preserve the location privacy for both PUs and SUs?
2) How to design an efficient database access protocol which allows for both PUs and SUs to adjust their PPL to achieve the maximum utility?

III. Quantitative Privacy-preserving Mechanism

In this section, we introduce a bilateral privacy-preserving framework which allows for PUs and SUs to preserve their privacy simultaneously.

A. Location Privacy Preservation for PU

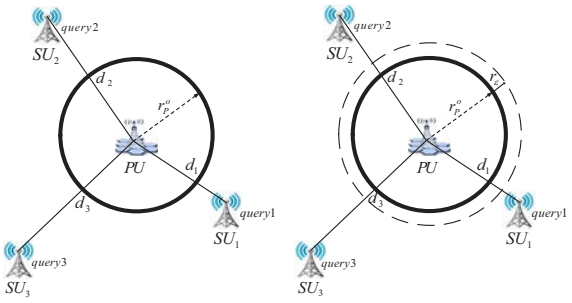
Before introducing the privacy-preserving mechanism for PUs, we illustrate how its location privacy may breach. Suppose PUs do not adopt any privacy-preserving mechanism. A malicious SU can infer PU's location through multiple

queries as shown in Fig. 2(a). Every time when it queries the database, one sophisticated malicious SU, which obtained the MTP function of database [12], can compute the distance between PU and itself. After multiple times of queries from different locations, the malicious SU can choose three query results that contain available transmit power to locate PU. The query results that do not allow SU to transmit is useless to conduct the inference attack.

We propose an obfuscation based mechanism as shown in Fig. 2(b) to thwart SU's inference attack. Every time when an SU queries the database, database will add a random length to PUs' real protected contour radius before computing the maximum transmit power. The malicious SU cannot calculate the accurate distance between PU and SU since the distance is randomized, which increases the difficulty to localize PU accurately. We adopt exponential distribution to generate the required random distance r_ϵ. The corresponding probability density function is

$$g(r_\epsilon) = \begin{cases} \frac{1}{b} e^{-\frac{r_\epsilon}{b}}, & r_\epsilon > 0, \\ 0, & r_\epsilon \leq 0, \end{cases}$$

where b is the rate parameter. Essentially, adding exponential noise is a special case of Laplacian mechanism. Notice that if r_ϵ is negative, the obfuscated protected contour will be less than the required one which may cause interference. Thus we should adopt the positive part of Laplacian distribution rather than the standard one, i.e. exponential distribution.



(a) Inference attack to PU (b) Privacy-preserving mechanism

Fig. 2: PU's location privacy threat and countermeasure

Intuitively, if the added noise is larger, the privacy-preserving level will be higher. So we adopt the expectation of r_ϵ to denote the privacy-preserving level of PU. It is well known that the expectation of r_ϵ is b. Thus, we can utilize the rate parameter b to quantify PU's privacy-preserving level.

B. Location Privacy Preservation for SU

As described in the basic database access protocol, SU should report its accurate location to achieve the locally available channels, in which situation SU is confronted with privacy breach risk. In this subsection, we propose a random mechanism, which permits SU to preserve its location privacy while achieving a given utility simultaneously, based on ϵ-geo-indistinguishability [14] mechanism.

Definition 1: A random mechanism satisfies l-geo-indistinguishability if and only if for a reported location x, we have

$$\frac{P(x|x_0)}{P(x|x_0')} \leq e^l, \forall r_0 > 0, d(x_0, x_0') \leq r_0,$$
$$l = \epsilon r_0,$$

where r_0 is radius of the largest margin where the SU may locate through the random mechanism, x_0, x_0' are two accurate locations that may report x randomly.

Whether SU's accurate location is x_0 or x_0', the reported location can be x with certain probability, and their probability difference is upper bounded by e^l if the distance between x_0 and x_0' is less than r_0. The above definition guarantees that even a malicious database manager gets a reported location x from SU, he cannot infer SU's accurate location, i.e., whether SU is in x_0 or x_0'.

Notice that when the difference between $P(x|x_0)$ and $P(x|x_0')$ decreases, it is more difficult for malicious database manager to infer SU's accurate location, i.e. the privacy preserving level is higher. In [14], the authors consider that for a given radius r_0, smaller ϵ achieves higher privacy preserving level, i.e. ϵ-geo-indistinguishability mechanim.

From our perspective, given a certain l, we can adjust ϵ to achieve a larger r_0, every expected r_0 corresponds to an ϵ. Thus we can leverage r_0 to denote SU's privacy-preserving level, a larger r_0 means that SU can obfuscate its location in a larger scale with l-geo-indistinguishability. By this notion, SU can choose its protected scale flexibly, rather than adjust its privacy level in a fixed scale as ϵ-geo-indistinguishability mechanism shows.

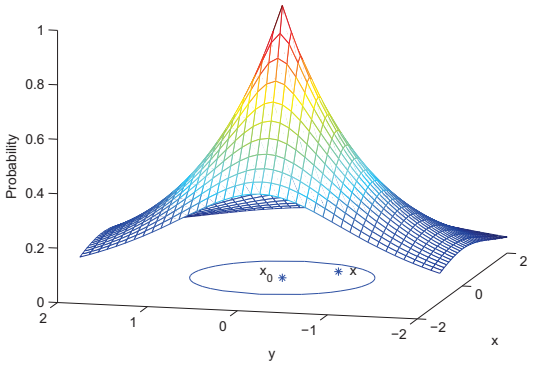


Fig. 3: The SU originally in x_0 randomly generates its obfuscated location with probability as shown in 'Probability' axis.

Miguel Andres et al. [14] proved that two dimensional Laplacian noise satisfies ϵ-geo-indistinguishability, and thus satisfies l-geo-indistinguishability. The probability density function of two dimensional Laplacian distribution is

$$f(x|x_0) = \frac{\epsilon^2}{2\pi} e^{-\epsilon d(x_0, x)}, \quad (2)$$

where $x_0 \in \mathbb{R}^2$ is the accurate location of SU and $x \in \mathbb{R}^2$ is the obfuscated location of SU through the random mechanism.

Fig. 3 shows how this mechanism works. When SU's accurate location is x_0, it may report x to the database with the

probability given by two dimensional Laplacian distribution. Since the two dimensional Laplacian distribution may generate a random location to infinite place which is meaningless to SU, thus we remap the location outside the required radius r_0 to the margin of it.

C. Bilateral Privacy Preservation Framework

In this paper, we consider a simple situation where there are only one PU and one SU in the system. The bilateral privacy preservation framework is shown in Fig. 4. The big solid circle is the real protected contour of PU, the dashed circle is the randomly generated protected contour based on the mechanism in the aforementioned subsection, and the small solid circle is the radius of area where l-geo-indistinguishability mechanism can generate a random location of SU. SU_1' and SU_2' are two randomly generated locations when the accurate location is SU.

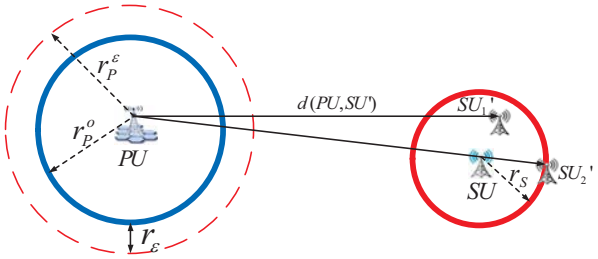


Fig. 4: Bilateral privacy preservation framework.

As presented in the aforementioned subsection, we adopt r_ϵ's expectation $E(r_\epsilon)$ to quantify PU's PPL and r_s to quantify SU's PPL. Intuitively, increasing PU's or SU's PPL can both decrease SU's maximum transmit power, which may degrade both PU's and SU's utility. To simplify, we leverage the available transmit radius to analyze the maximum transmit power, since the maximum transmit power is a continuous monotonically increasing function of the available transmit radius.

In a query process, when SU's expected PPL is r_s, and the database generates a random distance r_ϵ to obfuscate PU's real protected contour, the database can calculate SU's available transmit radius as follows

$$R_0 = d(PU, SU') - r_p^0 - r_\epsilon,$$

where $d(PU, SU')$ is the distance between PU and SU's randomly generated location, r_p^0 is the real protected contour of PU.

Notice that in the worst case, the randomly generated location may be in SU_2' as shown in Fig. 4. However, SU's real transmit location is SU. To avoid interference with PU, the previously calculated available transmit radius should substract SU's expected contour r_s as

$$R_0 = d(PU, SU') - r_p^0 - r_\epsilon - r_s. \tag{3}$$

In our proposed framework, PU and SU can flexibly choose their PPL $E(r_\epsilon)$ and r_s, respectively. Different from traditional database access protocol, that is impossible for PU and SU to choose the optimal PPL to maximize their utility, we propose a novel database access protocol in the next section.

IV. Privacy-preserving Database Access Protocol

In this section, we propose a new database access protocol called privacy preserving Utility Maximization protocol (UMax). This protocol allows for PU and SU to adjust their privacy preserving level to achieve the maximum utility.

A. Database Access Protocol Overview

Intuitively, if the distance between PU and SU is short, a smaller PPL may achieve higher utility; if the distance is long, a larger PPL may need to achieve higher utility. However, in our system, PU and SU do not have any side information about the distance of each other, the traditional two-step database access protocol, i.e., query and response, is impossible to enable both sides to decide the optimal PPL. In this situation, the most effective strategy is to choose a fixed PPL which is not always the optimal one.

To enable both sides to choose the optimal PPL, we propose a new database access protocol, that comprises four steps. The new protocol allows for PU and SU to exchange information to decide the optimal PPL. Firstly, SU generates a random location based on a relatively large expected PPL, then sends it to the database together with the expected PPL. Secondly, based on SU's expected information, PU can decide its optimal PPL through solving an optimization problem as depicted in the following subsection, and then responds SU with the expected available transmit radius. Thirdly, SU adjusts its PPL to achieve a higher utility based on PU's feedback, and resends it to database. Finally, PU calculates SU's maximum transmit power and reports it.

B. UMax Protocol

In this subsection, we elabrate our proposed database access protocol UMax, which is shown by a flow chart in Fig. 5, and is explained in the following.

Step 1: SU sends its interested channel and the expected privacy preserving level to database: An SU with accurate location (x, y) sends a query $Q = (ch_i, loc', r_s, r_0)$ to the database, where ch_i is SU's interested channel, $loc' = (\tilde{x}, \tilde{y})$ is the randomly generated location of SU based on l-geo-indistinguishability mechanism, and r_s denotes SU's expected PPL. In the real scenario, SU will not always expect to transmit with the maximum available transmit radius when the radius is long enough. It may request an expected transmit radius r_0 based on its service requirement.

Step 2: PU decides the optimal privacy preserving level to maximize its expected utility: Based on SU's requirement, i.e., interested channel, expected PPL and required transmission radius, database can decide how SU can access the interested channel. When SU's interested channel is vacant, database replies SU that it can access the channel with its requirement without optimization. However, if the interested channel is occupied by PU at the query time, database should first decide an optimal PPL for PU based on the following optimization problem:

Problem 4.1:

$$\max \ E[U_p],$$
$$s.t. \ E(r_\epsilon) \geq \underline{E(r_\epsilon)},$$

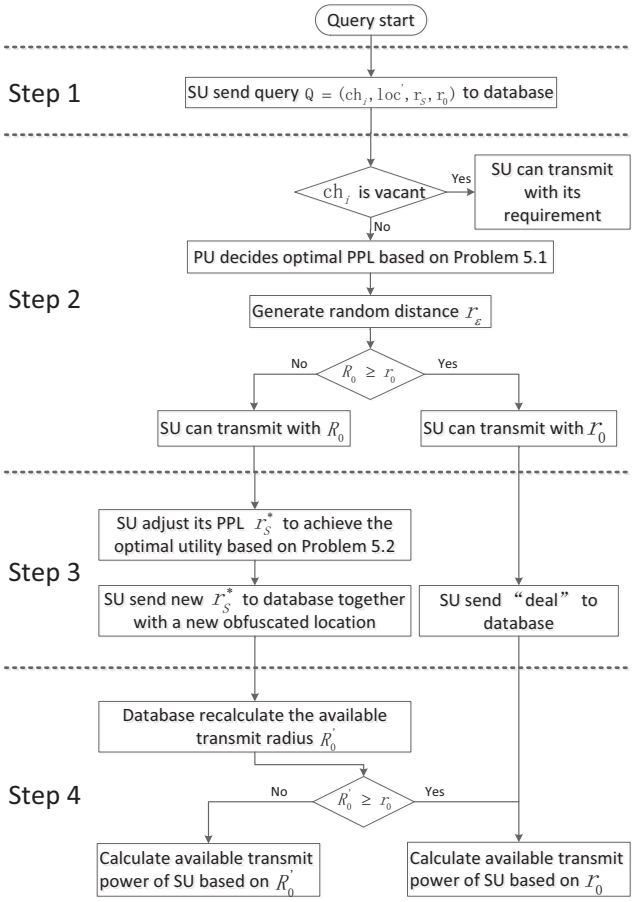


Fig. 5: Database access protocol flow chart.

where $E[U_p] = P_{sell} - C_{pri}$ is the expected utility of PU. P_{sell} is the revenue of PU by selling spectrum to SU, and C_{pri} is PU's privacy cost [15] which is inversely proportional to its PPL. $\underline{E(r_\epsilon)}$ is the lower bound of PPL that PU can tolerate. The details about the optimization problem will be introduced in the following subsection.

Solving problem 4.1 can achieve the optimal PPL of maximizing PU's utility. With the optimal PPL, the database can generate a random distance r_ϵ, and calculate SU's available transmit radius R_0 based on (3).

Finally, database makes the following decision: if $R_0 \geq r_0$, database responds SU that it can transmit with its required radius r_0. However, if $R_0 < r_0$, database responds SU that it can only transmit within the available radius R_0.

Step 3: SU adjusts its privacy preserving level to achieve higher utility based on PU's response: Based on database's feedback, SU adjusts its requirement accordingly. If it received r_0, SU's requirement is satisfied, then SU resends to database with "deal" which means that the transaction is done. However, if receiving the available radius R_0, SU adjusts its PPL parameter r_s to achieve higher utility based on the following optimization problem:

Problem 4.2:

$$\max \ E[U_s],$$
$$s.t. \ r_s \geq \underline{r_s},$$

where $E[U_s] = P_0 - C_{uns} - C_{buy} - C_{pri}$ is SU's expected utility. P_0 is SU's reward when its requirement is fully satisfied. C_{uns} is the cost of the unsatisfied part of the required transmit radius. Obviously, when the difference between R_0 and r_0 increases, C_{uns} becomes bigger. C_{buy} is SU's payment of utilizing the spectrum which is equal to P_{sell} of PU. C_{pri} is SU's privacy cost, and $\underline{r_s}$ is the lower bound on PPL which SU can tolerate.

Solving problem 4.2 can achieve the optimal PPL of SU, i.e., $r_s^\star$, to maximize SU's utility. Then SU resends to database with its optimal PPL $r_s^\star$.

Step 4: PU allocates the available channel to SU and calculates the corresponding transmit power: Based on SU's response, the database calculates SU's transmit power based on (1) accordingly. If SU's response is "deal", the database calculates SU's transmit power based on r_0. However, if SU's response is $r_s^\star$, the database first recalculates the available transmit radius $R_0' = d(PU, SU'') - r_p^0 - r_\epsilon - r_s^\star$. If $R_0' \geq r_0$, the database calculates SU's transmit power based on r_0, otherwise, the database calculates SU's transmit power based on R_0'. Finally, the database informs SU the calculated transmit power.

C. PU's optimal decision

We define PU's revenue function as follows

$$P_{sell} = k_1 \bar{S},$$
$$\bar{S} = \begin{cases} \pi r_0^2, & R_\epsilon \geq r_0, \\ \pi R_\epsilon^2, & R_\epsilon < r_0, \end{cases} \tag{4}$$

where $\bar{S}$ is the expected area where SU can transmit, (PU can charge from SU according to the size of $\bar{S}$), and k_1 is the unit price of spectrum. R_ϵ is SU's expected available transmit radius which can be calculated as

$$R_\epsilon = d(PU, SU') - r_p^0 - r_s - E(r_\epsilon).$$

The decrease of PU's PPL may increase its revenue, but suffer from larger privacy breach risk which should be considered into PU's utility, i.e. privacy cost. Privacy cost can be defined in the following

$$C_{pri} = \frac{k_p}{E(r_\epsilon)}, \tag{5}$$

where k_p is the privacy cost coefficient.

Combining (4) and (5), we rewrite PU's expected utility as

$$E[U_p] = k_1 \bar{S} - \frac{k_p}{E(r_\epsilon)}. \tag{6}$$

Define $M_1 = d(PU, SU') - r_p^0 - r_s$, we can rewrite PU's expected utility function to the following form

$$E[U_p] = \begin{cases} k_1 \pi r_0^2 - \frac{k_p}{E(r_\epsilon)}, & E[r_\epsilon] \leq M_1 - r_0, \\ k_1 \pi (M_1 - E[r_\epsilon])^2 - \frac{k_p}{E(r_\epsilon)}, & E[r_\epsilon] > M_1 - r_0. \end{cases}$$

Theorem 4.1: The optimal privacy preserving level that solves *Problem 4.1* is given by

(1) When $\sqrt{\frac{k_p}{k_1\pi}} < M_1 - r_0$, we discuss the impact of the magnitude of $M_1 - r_0$ on the solution,

If $\underline{E(r_\epsilon)} < M_1 - r_0$,

$$E^\star(r_\epsilon) = M_1 - r_0,$$

else

$$E^\star(r_\epsilon) = \underline{E(r_\epsilon)}.$$

(2) When $\sqrt{\frac{k_p}{k_1\pi}} \geq M_1 - r_0$, similarly, we have,

If $\underline{E(r_\epsilon)} < \sqrt{\frac{k_p}{k_1\pi}}$,

$$E^\star(r_\epsilon) = \sqrt{\frac{k_p}{k_1\pi}},$$

else

$$E^\star(r_\epsilon) = \underline{E(r_\epsilon)}.$$

Proof: We can find the optimal solution of each part of the piecewise function, and then compare them to decide the optimal solution.

(1) When $E(r_\epsilon) \leq M_1 - r_0$,

$$\frac{dE(U_p)}{dE(r_\epsilon)} = \frac{k_p}{E^2(r_\epsilon)} > 0. \tag{7}$$

Formula (7) shows that the utility function is monotonically increasing in the interval $(0, M_1 - r_0]$. Thus, it can be seen that

$$E^\star(r_\epsilon) = M_1 - r_0,$$

(2) When $E(r_\epsilon) > M_1 - r_0$,

$$\frac{dE(U_p)}{dE(r_\epsilon)} = -k_1\pi + \frac{k_p}{E^2(r_\epsilon)}. \tag{8}$$

Let $\frac{dE(U_p)}{dE(r_\epsilon)} = 0$. We have

$$E(r_\epsilon) = \sqrt{\frac{k_p}{k_1\pi}}.$$

If $\sqrt{\frac{k_p}{k_1\pi}} < M_1 - r_0$,

$$E^\star(r_\epsilon) = M_1 - r_0,$$

else

$$E^\star(r_\epsilon) = \sqrt{\frac{k_p}{k_1\pi}}.$$

Comparing with the first case, we can achieve *Theorem 4.1*. ■

D. SU's optimal decision

The same to the analysis of PU, we can define C_{uns}, C_{buy} and C_{pri} as follows

$$C_{uns} = k_2\Delta S, \tag{9}$$
$$C_{buy} = k_1(S_0\Delta S), \tag{10}$$
$$C_{pri} = \frac{k_s}{r_s}, \tag{11}$$

where k_2 is the coefficient of unsatisfied cost, $\Delta S = \pi(r_0 - R_0)^2$ is the unsatisfied part compared to SU's requirement.

Combining (9), (10) and (11), SU's expected utility can be rewritten as

$$\begin{aligned} E[U_s] &= P_0 - k_2\Delta S - k_1(S_0 - \Delta S) - \frac{k_s}{r'_s} \\ &= P_0 - k_1S_0 - [(k_2 - k_1)\Delta S + \frac{k_s}{r'_s}]. \end{aligned}$$

Since $P_0 - k_1S_0$ is fixed, the original optimization problem is equivalent to the following problem

Problem 4.3:

$$\begin{aligned} &\min\ (k_2 - k_1)\Delta S + \frac{k_s}{r'_s}, \\ &s.t.\ r'_s \geq \underline{r'_s}, \end{aligned}$$

where

$$\begin{aligned} \Delta S &= \pi(r_0 - R'_0)^2 \\ &= \pi[r_0 - (d(PU, SU') - r_p^0 - r_\epsilon - r'_s)]^2 \\ &= \pi[r_0 - R_0 - r_s + r'_s]^2. \end{aligned}$$

Define $A = k_2 - k_1$ and $B = r_0 - R_0 - r_s$. The optimization problem becomes

Problem 4.4:

$$\begin{aligned} &\min\ \pi A(B + r'_s)^2 + \frac{k_s}{r'_s}, \\ &s.t.\ r_s \geq \underline{r_s}. \end{aligned}$$

Solving the above optimization problem can achieve the following theorem.

Theorem 4.2: Denote

$$H = \sqrt[n]{-\frac{q}{2} + \sqrt{(\frac{q}{2})^2 + (\frac{p}{3})^3}} + \sqrt[n]{-\frac{q}{2} - \sqrt{(\frac{q}{2})^2 + (\frac{p}{3})^3}},$$

where

$$\begin{aligned} p &= -12\pi^2A^2B, \\ q &= 16\pi^3A^3B^3 - 108\pi^2A^2k_s. \end{aligned}$$

The optimal PPL that solves *Problem 4.4* can be expressed as follows

(1) When $\underline{r_s} \leq H$,

$$r_s^\star = H,$$

(2) When $\underline{r_s} > H$,

$$r^{\star}_{S0} = \underline{r_s}.$$

Proof: We denote

$$F = \pi A(B + r'_s)^2 + \frac{k_s}{r'_s}.$$

The derivative of F can be calculated as

$$\frac{dF}{dr'_s} = 2\pi A(B + r'_s) - \frac{k_s}{r'_s}.$$

Let $\frac{dF}{dr'_s} = 0$. We have

$$2\pi ABr'^2_s + 2\pi Ar'^3_s - k_s = 0. \tag{12}$$

Equation (12) is a cubic equation. By the formula of root [16], we can obtain the result. ■

V. Simulation

In this section, we present extensive evaluations to demonstrate the performance of our proposed mechanism.

A. Simulation Setup

Given on SU's accurate location $x_0 \in \mathbb{R}^2$, it is difficult to generate the random location $x \in \mathbb{R}^2$ directly through the definition of Laplacian distribution as (2). Thus, in this subsection, we present an algorithm to generate a random location which follows two dimensional Laplacian distribution through uniform distribution.

Notice that the probability density function of two dimensional Laplacian distribution depends only on the distance between the accurate location x_0 and random location x. Thus, it will be more convenient to transform the Cartesian coordinate system to polar coordinate system. The probability density function of two dimensional Laplacian distribution under polar coordinates is then given by

$$f(r, \theta) = \frac{\epsilon^2}{2\pi} r e^{-\epsilon r}, \tag{13}$$

where r is the distance between x_0 and x. From (13) we know that r and θ are independent from each other. The joint probability density of r and θ is equal to the product of their marginal probability, which can be calculated as follows

$$f(r) = \int_0^{2\pi} f(r, \theta)\, d\theta = \epsilon^2 r e^{-\epsilon r}, \tag{14}$$

$$f(\theta) = \int_0^{\infty} f(r, \theta)\, dr = \frac{1}{2\pi}. \tag{15}$$

Since r and θ are independent of each other, we can generate r and θ separately. From (15). Thus, we know that the marginal probability of θ is a constant number, thus we can generate θ as a random number in the interval $[0, 2\pi]$ with uniform distribution.

As for r, we can first calculate its cumulative density function as follows

$$C(r) = \int_0^r \epsilon^2 \rho e^{-\epsilon\rho}\, d\rho = 1 - (1 + \epsilon r)e^{-\epsilon r}.$$

Then we generate a random number a in the interval $[0, 1]$ with uniform distribution. Finally, we generate r as

$$r = C^{-1}(a).$$

Given an accurate location $x_0 = (s, t)$, a random location that obey Laplacian distribution can be generated as

$$x = (s + r\cos\theta, t + r\sin\theta).$$

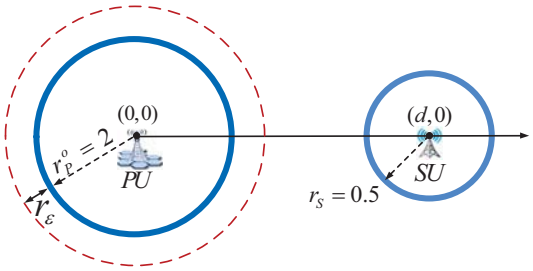


Fig. 6: Simulation setting.

B. Performance Comparison

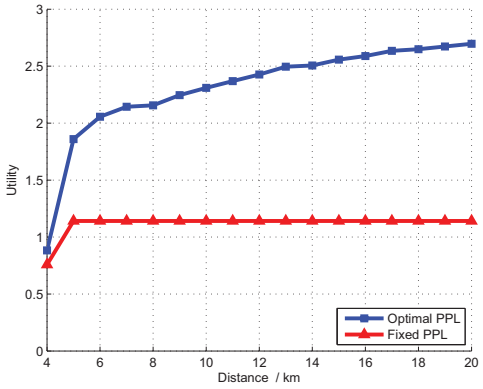
To corroborate the effectiveness of our mechanism, we perform simulations which is sketched in Fig. 6. Since the utility is only relevant to the distance between PU and SU, for simplicity, we set the coordinate of PU and SU to be $(0, 0)$ and $(d, 0)$ respectively, where d is the distance between PU and SU. It is easy to see that any instance of the real distance between PU and SU can be transformed to the above situation through coordinate transformation. The unit of distance is set to be *kilometer*.

In our simulation, we consider a simple scenario of one channel, one PU and one SU in our system. We set PU's real protected contour r_p^0 to be 2 and SU's expected PPL r_s to be 0.5 in the first query stage. The unit price parameter k_1 and k_2 are set to be 1 and 2, respectively, and the privacy cost parameters k_p and k_s are both set to be 1. To evaluate the average utility, we conduct 10000 queries for each distance between PU and SU.

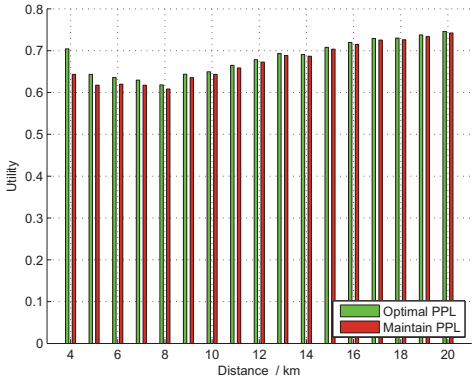
To illustrate the advantage of our proposed mechanism, we consider the following baseline: PU and SU choose a fixed PPL in every query process to preserve their location privacy, and the fixed PPL of PU and SU are both set to be 0.5.

Fig. 7(a) shows that after deciding the optimal PPL, PU can increase its utility efficiently for every distance between PU and SU. When the distance is short, the available transmit radius for SU will be small. Thus, both mechanisms only achieve a low utility. With the distance increasing, the proposed mechanism adjusts its PPL to achieve the optimal utility, which leads to the increase of PU's utility. However, when the distance is long enough, SU's requirement can always be satisfied, and the revenue will not increase much. On the other hand, the effect of privacy cost drops sharply according to the cost function $C_{pri} = \frac{k_p}{E(r_\epsilon)}$. Therefor the utility of PU do not increase much when the distance keeps increasing after a certain point.

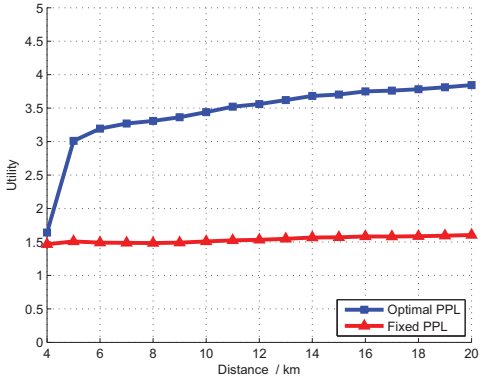
Fig. 7(b) shows that if PU makes the optimal decision, SU that follows to make optimal decision can achieve higher



(a) PU's utility of optimal PPL versus fixed PPL.



(b) SU's utility obtained in the case where SU follows to choose the optimal PPL versus the case where SU maintains the original PPL, after PU made the optimal decision.



(c) System utility of optimal PPL versus fixed PPL.

Fig. 7: An illustration of the efficiency of the proposed database access protocol.

utility, compared with the situation where SU maintains its PPL. Because when the distance is short, SU's requirement can not be always satisfied, therefore if SU adjusts its PPL may effectively achieve higher utility. However, as the distance expand, SU's requirement can always be satisfied. Thus it is unnecessary for SU to adjust its PPL. In such case, the advantage of optimal decision is not prominent.

We adopt the summation of PU's and SU's utility in one query process to denote the system utility. The system utility is not the simple summation of the result in Fig. 7(a) and 7(b). Essentially, this simulation is the system utility comparison between our proposed four-step mechanism and the traditional two-step mechanism. The simulation result shows that PU and SU making optimal decision simultaneously can increase the system utility compared to the fixed PPL mechanism.

VI. Related Work

Location privacy preservation is a hot research topic and attracts a lot of attention. There are a large amount of existing works on the location privacy-preserving techniques. Among them, k-anonymity [17] and cryptography [18] are two most widely adopted notions.

The notion of k-anonymity is the most well-known privacy-preserving technique [19]. One approach to achieve k-anonymity is to use *dummy locations* [20]. This technique properly selects $k-1$ dummy points, and then performs k queries to database together with the real location. Another efficient method is *cloaking* [21][22], which creates a dummy region that involves k different points sharing the same property, and then queries the database with the dummy region.

l-diversity [23] and t-closeness [23] techniques are proposed to address the weaknesses of k-anonymity when homogeneity exists in the sensitive values in a group. However, the intrinsic drawback of k-anonymity is that a mechanism is difficult to be proved to satisfy this notion, since the attacker's auxiliary information may violate the guarantee of k-anonymity. In addition, k-anonymity based approaches are difficult to quantify the privacy preserving level.

Cryptography is another location privacy-preserving technique, which has been widely used [24][25]. This technique transforms all the data in a query process to a different space. The query result can be mapped back to spatial information only by the user. However, the computational overhead of cryptography based technique is too high.

The existing works on the location privacy in database-driven cognitive radio are mainly based on the aforementioned techniques, which are either difficult to quantify the PPL or computational demanding. In [11], Gao et al. proposed a cryptography based location privacy-preserving protocol called PSAIR for SUs. PSAIR allows for SUs to access the locally available channels and preserve location privacy simultaneously. Bahrak et al. [12] pointed out that a malicious SU can infer PU's location through seemingly innocuous database queries. Then they proposed a k-anonymity based mechanism to preserve PU's privacy.

The notion of differential privacy [13] comes from the area of statistical database. Its goal is to preserve individual's privacy while achieving good statistical accuracy. The main advantage of differential privacy is that the privacy guarantee is independent of attacker's auxiliary information, i.e., the mechanism has no need to update when new types of attack emerges. More importantly, differential privacy provides a solid mathematical definition which is convenient to quantify the privacy preserving level [26][27].

Differential privacy is recently applied to preserve location privacy. Ho et.al. [28] leveraged a quadtree spatial decomposition technique to achieve differential privacy in a location database. In [14], the authors proposed ϵ-geo-indistinguishability mechanism, which is based on the notion of differential privacy, to preserve a single user's location privacy. Due to the advantage of differential privacy, we adopt the notion of differential privacy to preserve the location privacy of both PUs and SUs. Essentially, the notion of differential privacy provides guarantee to the privacy preserving level of a class of random mechanism. Gaussian mechanism and Laplacian mechanism [29] are the most widely adopted mechanisms to achieve differential privacy.

VII. Conclusion

In this paper, we proposed a novel location privacy preservation scheme, while achieving bilateral utilization maximization of both PU and SU. First, a quantitative mechanism was proposed to preserve the location privacy of both PU and SU simultaneously based on the concept of differential privacy. Based on the quantitative mechanism framework, we further proposed a novel privacy preserving Utility Maximization protocol (UMax). UMax allows for both PU and SU to adjust their privacy preserving levels to achieve the optimal utility in an iterative way. Extensive simulations demonstrated that our proposed mechanism can efficiently increase both PU's and SU's utility while preserving their location privacy. Our future work will focus on extending the result of UMax to the scenario with multiple PUs and SUs.

VIII. Acknowledgement

Research was supported in part by NSFC under grant 61402405, by the Fundamental Research Funds for the Central Universities under grant 2015FZA5011, by University Science Research General Project of Jiangsu Province 15KJB510002.

References

[1] Y.-C. Liang, K.-C. Chen, G. Y. Li, and P. Mahonen, "Cognitive radio networking and communications: An overview," *IEEE Transactions on Vehicular Technology*, vol. 60, no. 7, pp. 3386–3407, 2011.

[2] R. Deng, J. Chen, X. Cao, Y. Zhang, S. Maharjan, and S. Gjessing, "Sensing-performance tradeoff in cognitive radio enabled smart grid," *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 302–310, 2013.

[3] J. Chen, Q. Yu, B. Chai, Y. Sun, Y. Fan, and X. Shen, "Dynamic channel assignment for wireless sensor networks: a regret matching based approach," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 1, pp. 95–106, 2015.

[4] A. S. Rawat, P. Anand, H. Chen, and P. K. Varshney, "Collaborative spectrum sensing in the presence of byzantine attacks in cognitive radio networks," *IEEE Transactions on Signal Processing*, vol. 59, no. 2, pp. 774–786, 2011.

[5] J. Chen, J. Li, S. He, T. He, Y. Gu, and Y. Sun, "On energy-efficient trap coverage in wireless sensor networks," *ACM Transactions on Sensor Networks (TOSN)*, vol. 10, no. 1, p. 2, 2013.

[6] J. Chen, J. Li, and T. H. Lai, "Energy-efficient intrusion detection with a barrier of probabilistic sensors: Global and local," *IEEE Transactions on Wireless Communications*, vol. 12, no. 9, pp. 4742–4755, 2013.

[7] ——, "Trapping mobile targets in wireless sensor networks: An energy-efficient perspective," *IEEE Transactions on Vehicular Technology*, vol. 62, no. 7, pp. 3287–3300, 2013.

[8] Y. Zhao, J. Gaeddert, K. K. Bae, and J. H. Reed, "Radio environment map enabled situation-aware cognitive radio learning algorithms," in *Proceedings of SDR Forum Technical Conference'06*, 2006.

[9] S. N. Khan, M. A. Kalil, and A. Mitschele-Thiel, "Distributed resource map: A database-driven network support architecture for cognitive radio ad hoc networks," in *Proceedings of ICUMT'12*, 2012, pp. 188–194.

[10] R. Murty, R. Chandra, T. Moscibroda, and P. Bahl, "Senseless: A database-driven white spaces network," *IEEE Transactions on Mobile Computing*, vol. 11, no. 2, pp. 189–203, 2012.

[11] Z. Gao, H. Zhu, Y. Liu, M. Li, and Z. Cao, "Location privacy in database-driven cognitive radio networks: Attacks and countermeasures," in *Proceedings of IEEE INFOCOM'13*, 2013, pp. 2751–2759.

[12] B. Bahrak, S. Bhattarai, A. Ullah, J.-M. J. Park, J. Reed, and D. Gurney, "Protecting the primary users' operational privacy in spectrum sharing," in *Proceedings of IEEE DYSPAN'14*, 2014, pp. 236–247.

[13] C. Dwork, "Differential privacy," in *Automata, Languages and Programming*. Springer, 2006, pp. 1–12.

[14] M. E. Andrés, N. E. Bordenabe, K. Chatzikokolakis, and C. Palamidessi, "Geo-indistinguishability: Differential privacy for location-based systems," in *Proceedings of ACM SIGSAC conference on Computer & communications security,13*, 2013, pp. 901–914.

[15] A. Ghosh and A. Roth, "Selling privacy at auction," *Games and Economic Behavior*, 2013.

[16] L. Guilbeau, "The history of the solution of the cubic equation," *Mathematics News Letter*, pp. 8–12, 1930.

[17] L. Sweeney, "k-anonymity: A model for protecting privacy," *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, vol. 10, no. 05, pp. 557–570, 2002.

[18] Y. Fan, Y. Jiang, H. Zhu, J. Chen, and X. Shen, "Network coding based privacy preservation against traffic analysis in multi-hop wireless networks," *IEEE Transactions on Wireless Communications*, vol. 10, no. 3, pp. 834–843, 2011.

[19] V. Cambazoglu, C. Rohner, and B. Victor, "The impact of trace and adversary models on location privacy provided by k-anonymity," in *Proceedings of the First Workshop on Measurement, Privacy, and Mobility'12*, 2012, p. 6.

[20] P. Shankar, V. Ganapathy, and L. Iftode, "Privately querying location-based services with sybilquery," in *Proceedings of the international conference on Ubiquitous computing'09*, 2009, pp. 31–40.

[21] R. Shokri, C. Troncoso, C. Diaz, J. Freudiger, and J.-P. Hubaux, "Unraveling an old cloak: k-anonymity for location privacy," in *Proceedings of annual ACM workshop on Privacy in the electronic society'10*, 2010, pp. 115–118.

[22] A. Khoshgozaran, C. Shahabi, and H. Shirani-Mehr, "Location privacy: going beyond k-anonymity, cloaking and anonymizers," *Knowledge and Information Systems*, vol. 26, no. 3, pp. 435–465, 2011.

[23] A. Machanavajjhala, D. Kifer, J. Gehrke, and M. Venkitasubramaniam, "l-diversity: Privacy beyond k-anonymity," *ACM Transactions on Knowledge Discovery from Data (TKDD)*, vol. 1, no. 1, p. 3, 2007.

[24] A. Khoshgozaran and C. Shahabi, "Blind evaluation of nearest neighbor queries using space transformation to preserve location privacy," in *Advances in Spatial and Temporal Databases*. Springer, 2007, pp. 239–257.

[25] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan, "Private queries in location based services: anonymizers are not necessary," in *Proceedings of the ACM SIGMOD international conference on Management of data'08*, 2008, pp. 121–132.

[26] C. Dwork and A. Roth, "The algorithmic foundations of differential privacy," *Theoretical Computer Science*, vol. 9, no. 3-4, pp. 211–407, 2013.

[27] H. Zhang, Y. Shu, P. Cheng, and J. Chen, "Privacy and performance trade-off in cyber-physical systems," *IEEE Networks*, to appear.

[28] S.-S. Ho and S. Ruan, "Differential privacy for location pattern mining," in *Proceedings of ACM SIGSPATIAL International Workshop on Security and Privacy in GIS and LBS'11*, 2011, pp. 17–24.

[29] J. Le Ny and G. J. Pappas, "Differentially private filtering," *IEEE Transactions on Automatic Control*, vol. 59, no. 2, pp. 341–354, 2014.