A Game-Theoretic Approach to Achieving Bilateral Privacy-Utility Tradeoff in Spectrum Sharing

Mengmeng Liu, Xiangwei Zhou, and Mingxuan Sun
School of Electrical Engineering and Computer Science, Louisiana State University, Baton Rouge, LA 70803
Email: {lmengm1, xwzhou}@lsu.edu, msun@csc.lsu.edu

***Abstract*—In this paper, the problem of privacy-utility tradeoff in a database-driven spectrum sharing system is considered, where both primary users (PUs) and secondary users (SUs) may suffer from location privacy leakage. To protect the location information of both parties, a bilateral privacy preservation mechanism is introduced, in which the privacy-preserving levels are quantified. To tackle the dilemma that a higher privacy level leads to less available spectrum to share and thus reduces the profits of both parties, a game-theoretic approach based on the Stackelberg model is proposed to achieve the tradeoff between the privacy-preserving level and user utility. With the proposed approach, both PUs and SUs can maximize their utilities by adjusting their location privacy to desired levels. Simulation results demonstrate that the proposed approach can effectively increase the utilities for both PUs and SUs in comparison with the privacy preservation mechanism with a fixed privacy level.**

I. Introduction

Spectrum sharing has shown to be an effective and promising technique for flexible and efficient utilization of the scarce spectrum resource. To enable dynamic channel access in database-driven systems, primary users (PUs) and secondary users (SUs) are required to provide their location information, which poses critical location privacy issues for these users. Many location privacy preservation mechanisms (LPPMs) have been proposed to raise user privacy level against location attack [1]. However, the location privacy-preserving level (PPL) and user utility are always a paradox, since a higher PPL will render less available spectrum to share and thus reduce the profits of both parties. Therefore, a challenging issue is how to coordinate the PUs and SUs to maximize their utilities while providing privacy preservation guarantee.

Most of the existing LPPMs for spectrum sharing focus on unilateral users' location information protection. In [2], PUs' locations are obfuscated by enlarging the exclusion zones (EZs) and injecting false positives into the responses to SUs' queries; however, the privacy level of the obfuscation mechanism is not quantified. In [3], a PU's location is protected by generating dummy PUs along with the corresponding EZs, and the privacy level is measured by the number of real PUs that an attacker can harm with one attack. Although the unavoidable tradeoff between the available spectrum for sharing and PUs' privacy levels is discussed, the solution to the dilemma is not given. In [4], k-anonymity and k-clustering methods are adopted to resist location privacy threats to PUs, where the metrics for privacy and spectrum utilization efficiency (SUE) are provided. However, the relation between the privacy metric and SUE metric is not formulated, which makes it difficult to quantify the influence of privacy levels on the SUE. In [5] and [6], the SU's location privacy issue is studied, where cryptographic approaches are proposed to protect users' locations. Although these methods can provide strict privacy guarantee, they either are computational expensive or require extra architectural entity. Furthermore, all the above work focuses on preserving the location for one party. Recent studies in [7] have shown that simply applying these LPPMs to protecting the privacy of PUs and SUs separately can result in severe utility loss for both parties. In [8], location privacy preservation for both PUs and SUs is considered, and the k-anonymity method is exploited. The privacy preservation mechanism maximizes users' privacy levels at the cost of sacrificing their utilities. In practice, however, a user's utility is an important concern. In addition, k-anonymity has been disregarded as a reasonable privacy preservation method in [9]. A utility maximization protocol is proposed in [10] to maximize PUs' and SUs' utilities while maintaining privacy guarantee. The expectation of a random length added to protect a PU's location is adopted as the privacy level. However, this measure is not sufficient. Since the random length is drawn from an exponential distribution, the expectation yields the scale parameter of the density, which can reveal the shape of the distribution but not the magnitude of the random length. As a result, the influences of different privacy levels on users' overall utilities cannot be explicitly shown.

In this paper, we introduce a privacy preservation mechanism based on the geo-indistinguishability notion [11] to protect the location information of both PUs and SUs. Both parties' PPLs are quantified in the mechanism. Based on the privacy preservation mechanism, the utility models of PUs and SUs are constructed, in which the privacy cost of each party is considered as a part of their utility model. The influence of different privacy levels on the overall utility are formulated. To achieve the tradeoff between user utility and privacy preservation, a Stackelberg model-based game theoretic approach is applied, which allows users to adjust their PPLs to optimal or expected values and therefore to maximize their utilities.

This work was supported in part by the National Science Foundation under Grant No. 1560437, 1927513, 1943486, and the Louisiana Board of Regents under Grant No. LEQSF (2017-20)-RD-A-29.

The main contributions of our work are summarized as follows:

1) To the best of the authors' knowledge, this is the first work that uses game-theoretic approach to handle the tradeoff between the privacy level and utilities of both PUs and SUs in spectrum sharing systems.

2) A novel additive noise perturbation method is proposed based on Gamma distribution to protect PUs' location information. The method contains minimum prior information of the distribution and thereby is more consistent with the privacy-preserving purpose.

3) Utility models for PUs and SUs are constructed. The privacy costs are built as part of the utility models. The revenues and costs caused by shared spectrum are modeled as a function of transmit radius, which is directly related to the privacy level. The role played by the privacy level in the overall utility is quantified and clearly revealed in the utility model.

II. Problem Formulation

A. Dynamic Channel Access

A dynamic channel access process can be described as follows: an SU requests a channel assignment from the system by sending a query to the database, which includes its location information loc_j and channel of interest ch_i. The database responds to the query with the availability information of the requested channel, including the maximum transmit power (MTP) P, which can be modeled as a monotonically increasing function of the maximum transmit radius (MTR), and the time duration t in which the SU is allowed to use the channel. If the SU is not allowed to transmit, the responded MTP and time duration are zeros.

B. Adversary Models and Location Privacy Threats

In the above process, both PUs and SUs may suffer from location information leakage caused by malicious attackers. Suppose that a sophisticated malicious SU can obtain the MTP calculation function adopted by the database. Then based on the MTP function, the SU can compute its MTR R_j in each query. Assume that the PU's location coordinate is (x_P, y_P) and the malicious SU receives three query responses at three different locations (x_i, y_i), $i = 1, 2, 3$. Then the SU will be able to accurately locate the PU and infer the corresponding EZ by solving

$$\begin{cases} (x_P - x_1)^2 + (y_P - y_1)^2 = \left(r_P^0 + R_1\right)^2, \\ (x_P - x_2)^2 + (y_P - y_2)^2 = \left(r_P^0 + R_2\right)^2, \\ (x_P - x_3)^2 + (y_P - y_3)^2 = \left(r_P^0 + R_3\right)^2. \end{cases} \tag{1}$$

On the other hand, a malicious PU can take advantage of being a service provider and collect SUs' location information to manipulate marketing and sales strategies. Combined with auxiliary information obtained from public data sets, the attacker could easily infer the preference and other characteristic information of the SUs, and sell this information to profitable enterprises such as advertising companies [1].

C. Problem of Interest

To protect PUs' and SUs' location information from malicious attacks, The LPPM must be applied. At the same time, however, unrestrictedly raising the PPL will significantly reduce the available transmission radius (ATR) and lead to a serious utility loss for both PUs and SUs. To find a solution to the dilemma, the following questions must be answered:

1) How to design a privacy preservation mechanism in which the PPL can be quantified and the influence of PPL on user utility can be revealed?
2) How to achieve the tradeoff between PPL and user utility such that both PUs and SUs can maximize their rewards while maintaining their privacy preservation to desired levels?

III. Bilateral Privacy Preservation Mechanism

A. Geo-indistinguishability

Geo-indistinguishability [11] is a privacy notion that allows users to protect their exact locations while releasing approximate information to get desired services in a location-based system. It is a generalization of the differential privacy [12]. In this paper, a modified version of geo-indistinguishability, named γ-geo-indistinguishability (γ-GI) is introduced to protect users' location information in a spectrum sharing scenario. The formal definition of γ-GI is presented as follows.

γ-Geo-indistinguishability: A randomized privacy preservation mechanism satisfies γ-GI if and only if for a reported location z:

$$\frac{P\left(z \mid z_0\right)}{P\left(z \mid z_0^*\right)} \leqslant e^{\gamma}, d\left(z_0, z_0^*\right) \leqslant l, \forall l > 0, \tag{2}$$

where z_0 and z_0^* are the exact locations of two users that may report their sanitized locations as z, $d\left(z_0, z_0^*\right)$ is the distance between z_0 and z_0^*, $\gamma = \epsilon l, \forall l > 0$ specifies the difference of the probabilities that two users report the same sanitized location, and ϵ determines the privacy preservation at unit distance.

Based on the γ-GI mechanism, two users within distance l will report their locations as z with similar probabilities, and the ratio of the probabilities is upper bounded by e^{γ}. As a result, an attacker that receives the user's reported location z will not be able to determine whether the user is located at z_0 or z_0^*, and thereby the user's location privacy will not be breached.

In a spectrum sharing system, the MTP and users' utilities are directly influenced by the radius l of the protected range, which makes it straightforward to focus on the adjustment of the radius scale. Therefore, the γ-GI can be interpreted as follows: provided the probability difference level γ, adjusting ϵ results in the protection of user location in a different scale l; a larger l indicates that the user can protect its location information in a larger range, and thus achieve stronger privacy. As a result, users can flexibly choose their desired privacy-preserving scale, and the radius l is denoted as the PPL accordingly.

B. Bilateral Privacy Preservation

Based on the γ-GI notion, a bilateral LPPM that simultaneously protects PUs' and SUs' location information is presented in the following, with the graphical interpretation given in Figure 1.

To thwart the location inference attack to SUs, in a query process the SU will report a randomized location generated based on the γ-GI notion, (x', y') or (x'', y'') in Figure 1, instead of the exact location (x, y). l_S in the figure is the radius of protected range in the γ-GI notion, and is adopted as the PPL for SUs.

To generate the random location, a proper distribution should be selected. It is proven in [11] that two-dimensional Laplacian noise can achieve geo-indistinguishability, and thus satisfies γ-GI.

Since the PDF of the planar Laplacian depends only on the distance between the exact location z_0 and the produced location z, it is more convenient to convert the Cartesian coordinates to the polar coordinates. The Laplacian PDF in polar coordinates is

$$f\left(r, \theta; \epsilon\right) = \frac{\epsilon^2}{2\pi} r e^{-\epsilon r}, \tag{3}$$

where r is the radial distance corresponding to the distance between z_0 and z in Cartesian coordinates, θ is the angle formed between the straight line connecting z and z_0 and the x axis of the Cartesian system.

Note that r and θ are independent of each other, and thereby the marginal densities of the two random variables $f\left(r; \epsilon\right)$ and $f\left(\theta; \epsilon\right)$ can be obtained respectively. As a result, r and θ can be generated independently. After the point (r, θ) is converted to the Cartesian system, a random location for the SU can be obtained.

To thwart the location inference attack to PUs, an obfuscation-based mechanism using the Gamma distribution is proposed. As shown in Figure 1, the database adds a randomized length, with maximum value l_ϵ, to the radius of the PU's actual EZ after receiving a query. Then the MTP is calculated based on the newly generated EZ, with radius $r_P^0 + r_\epsilon$ $(0 < r_\epsilon \leqslant l_\epsilon)$. As a result, a malicious SU cannot obtain the exact distance between the PU and itself based on the MTP. Moreover, r_P^0 in (1) is different every time since the maximum length l_ϵ is updated in each query-response round, which makes it more difficult to precisely locate the PU.

To generate the random length r_ϵ, the Gamma distribution is adopted. The Gamma distribution is the maximum entropy distribution and thus is least informative and minimizes the prior information included in the distribution. Moreover, physical systems are inclined to act towards maximum entropy configuration [13]. Therefore, it is suitable and effective to adopt Gamma density to generate random lengths for obfuscating PUs' EZs in practice. To determine the shape parameter and scale parameter, let r in (3) to be r_ϵ, and the integral over θ yields

$$f_R(r_\epsilon; \epsilon) = \int_0^{2\pi} \frac{\epsilon^2}{2\pi} r_\epsilon e^{-\epsilon r_\epsilon} \mathrm{d}\theta = \epsilon^2 r_\epsilon e^{-\epsilon r_\epsilon}, \tag{4}$$

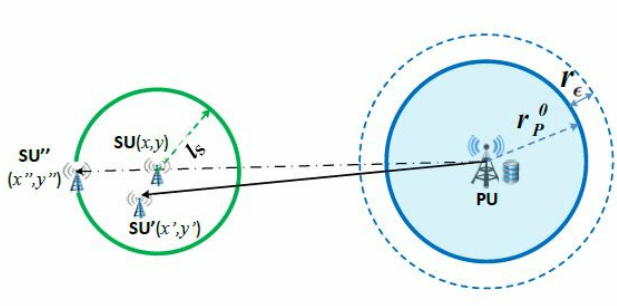

Fig. 1: Bilateral privacy preservation mechanism.

which is the Gamma distribution with scale $\frac{1}{\epsilon}$ and shape 2. Note that for PUs' privacy preservation, only random radius is needed. The larger the maximum obfuscation length l_ϵ is allowed, the stronger privacy preservation the PU will enjoy. Therefore, l_ϵ is used to quantify the PU's PPL.

Figure 1 illustrates the overall bilateral privacy preservation framework. The green solid circle indicates the SU's preserved area with privacy level l_S, within which a malicious PU cannot determine the SU's actual location. The blue solid circle represents the PU's exact EZ, while the dashed circle represents the obfuscation area of the EZ with privacy level l_ϵ, which is constructed by adding a random obfuscation length r_ϵ with maximum value l_ϵ to the actual radius r_P^0 of the EZ.

Intuitively, adjusting the PU's or SU's privacy level will change the SU's MTP, and thus affect both parties' payoffs. Since MTP is a monotonic increasing function of the ATR, the ATR is adopted for simplicity to effectively analyze the influence of privacy preservation on PUs' and SUs' utilities. According to Figure 1, the MTR for the SU with location privacy preservation is

$$R_M = d(PU, SU') - r_P^0 - l_\epsilon - l_S, \tag{5}$$

where $d(PU, SU')$ is the distance between the PU and the SU's sanitized location. To guarantee no interference to the PU, the SU's ATR R_A should be upper bounded by R_M, i.e., $0 \leqslant R_A \leqslant R_M$.

IV. Tradeoff between Utility and Privacy Level

The major concern in the bilateral privacy preservation mechanism is how to determine the maximum obfuscation length l_ϵ for the PU and the protected range radius l_S for the SU. As aforementioned, a high PPL is desired to effectively protect user location information from leakage. However, increasing the PPL will reduce the ATR according to (5) and result in a considerable decline in user utilities. To tackle this dilemma, the Stackelberg game is used to achieve the tradeoff between the privacy level and user utilities. Here the single-PU-single-SU situation is considered.

A. Modeling Spectrum Sharing as Stackelberg Game

Spectrum sharing can be modeled as a Stackelberg game, in which the PU acts as the leader and the SU acts as the follower. The Stackelberg model can be used to find the

subgame perfect Nash equilibrium (SPNE), that is, the strategy that best serves each player given the strategies of the other players, i.e., each player plays in a Nash equilibrium in every subgame [14].

Let $\boldsymbol{S_P}$ denote the PU's strategy set and $\boldsymbol{S_S}$ denote the SU's strategy set. For a predicted strategy $s_S^0 \in \boldsymbol{S_S}$ chosen by the SU, the PU will select a response strategy $s_P^* \in \boldsymbol{S_P}$ that maximizes its own payoff U_P:

$$s_P^* = \text{argmax}_{s_P \in \boldsymbol{S_P}} U_P\{(s_P; s_S)|s_S = s_S^0\}. \quad (6)$$

After observing the PU's strategy s_P^*, the SU picks the expected strategy $s_S^* \in \boldsymbol{S_S}$, with which the SU achieves its maximum payoff:

$$s_S^* = \text{argmax}_{s_S \in \boldsymbol{S_S}} U_S\{(s_S; s_P)|s_P = s_P^*\}. \quad (7)$$

In this paper, the PU's strategy set is defined as

$$\boldsymbol{S_P} = \{l_\epsilon |\, l_\epsilon \geqslant r_\epsilon > 0,\, r_\epsilon \sim \Gamma(2, \epsilon)\}. \quad (8)$$

The SU's strategy set is defined as

$$\boldsymbol{S_S} = \{l_S \,|\, \frac{P(z|z_0)}{P(z|z_0^*)} \leqslant e^\gamma,\, d(z_0, z_0^*) \leqslant l_S,\, \gamma = \epsilon l_S\}. \quad (9)$$

Since the Stackelberg game is solved via backward induction [15], the most probable response of the SU should be calculated first given any strategy of the PU to compute the SPNE. With the predicted best response of the SU, the PU chooses l_ϵ^* that maximizes its utility. After knowing the PU's strategy, the SU selects the anticipated strategy l_S^* accordingly. Therefore, the equilibrium of the Stackelberg game can be obtained as (l_ϵ^*, l_S^*) such that

$$\begin{cases} U_P(l_\epsilon^*, l_S^*) \geqslant U_P(l_\epsilon, l_S), \\ U_S(l_\epsilon^*, l_S^*) \geqslant U_S(l_\epsilon, l_S), \end{cases} \quad \forall l_\epsilon \in \boldsymbol{S_P},\ \forall l_S \in \boldsymbol{S_S}. \quad (10)$$

B. Utility Functions

The PU's utility is composed of four parts: revenues from its own data transmission, P_R^P; payoffs from selling spectrum to the SU, P_{sell}; performance loss due to the shared spectrum with the SU, P_{lost}; the cost for privacy preservation, C_{prv}^P.

The construction of each term is based on the following rules: P_R^P is modeled as a function of its EZ; P_{sell} and P_{lost} are formulated as functions of the ATR; C_{prv}^P is modeled as a function of its privacy level l_ϵ. Therefore,

$$\begin{aligned} U_P = {} & k_R^P \pi (r_P^0)^2 + k_T \pi (d_{PS} - r_P^0 - l_\epsilon - 2l_S)^2 \\ & - k_{lost} \pi (d_{PS} - r_P^0 - 2l_\epsilon - 2l_S)^2 - k_{prv}^P l_\epsilon^2, \end{aligned} \quad (11)$$

where k_R^P is the unit revenue of data transmission, d_{PS} is the distance between the PU and SU, k_T is the spectrum unit trading price, k_{lost} is the coefficient of the PU's performance loss, and k_{prv} is the PU's privacy preservation coefficient.

The SU's utility function consists of three parts: the rewards gained through its data transmission, P_R^S; the payment for accessing the spectrum, P_{buy}; the cost for location privacy preservation, C_{prv}^S.

Each term is constructed as follows: P_R^S is modeled as a function of the transmit radius accessible to the SU; P_{buy} is equal to P_{sell} in the single-PU-single-SU situation; C_{prv}^S is modeled as a quadratic function of the SU's privacy level l_S. Therefore,

$$\begin{aligned} U_S = {} & k_R^S \pi (d_{PS} - r_P^0 - l_\epsilon - l_S)^2 \\ & - k_T \pi (d_{PS} - r_P^0 - l_\epsilon - 2l_S)^2 - k_{prv}^S l_S^2, \end{aligned} \quad (12)$$

where k_R^S is the SU's unit reward and k_{prv}^S is the SU's privacy preservation coefficient.

(11) and (12) show that by altering users' privacy levels l_ϵ and l_S, user utilities U_P and U_S will change accordingly. The influence of privacy level on user utility thus can be revealed and quantified.

C. Stackelberg Equilibrium

Sine user utilities are affected by the privacy levels that they choose, it is desired to find out the optimal privacy levels that maximize both parties' profits. The solution is proposed based on the Stackelberg game.

In a Stackelberg model, the follower's probable strategy is first computed to achieve the SPNE. Given the spectrum sharing scenario, the SU's anticipated privacy level is first determined.

Theorem 1: Provided $0 < k_T < k_R^S < 2k_T$, there exists an optimal PPL $\overline{l_S^*}$ for the SU, which is given as

$$\overline{l_S^*} = \frac{(2k_T\pi - k_R^S\pi)(d_{PS} - r_P^0 - l_\epsilon)}{4k_T\pi + k_{prv}^S - k_R^S\pi}. \quad (13)$$

The proof of Theorem 1 is given in Appendix A. The condition indicates that the SU's unit reward is larger than the spectrum unit price but no more than twice of the spectrum unit price. Theorem 1 states that given any privacy level l_ϵ picked by the PU, the SU's best strategy is to set its privacy level l_S as $\overline{l_S^*}$ presented in (13).

Note that the SU's optimal privacy level $\overline{l_S^*}$ obtained in this step is expressed as a function of the PU's privacy level l_ϵ. With the information of the SU's predicted PPL, the best response function of the PU can be found.

Theorem 2: Provided $0 < k_{lost} < k_T < 2k_{lost}$, there exists an optimal PPL l_ϵ^* for the PU, which is given as

$$l_\epsilon^* = \frac{[k_{lost}\pi(2-2\xi)(1-2\xi) - k_T\pi(1-2\xi)^2](d_{PS} - r_P^0)}{k_{lost}\pi(2-2\xi)^2 + k_{prv}^P - k_T\pi(1-2\xi)^2}, \quad (14)$$

where $\xi = \frac{2k_T\pi - k_R^S\pi}{4k_T\pi + k_{prv}^S - k_R^S\pi}$.

The proof of Theorem 2 is given in Appendix B. The condition indicates that the unit spectrum trading payoff is higher than the unit performance loss, but no more than twice of the unit performance loss.

The privacy level l_ϵ^* obtained in Theorem 2 is the PU's best response to the reaction of the SU in the equilibrium. After observing the PU's strategy l_ϵ^*, the SU's actual privacy level can be found by substituting l_ϵ^* into its reaction function obtained in Theorem 1, which yields

$$l_S^* = \frac{\xi[k_{lost}\pi(2-2\xi) + k_{prv}^P](d_{PS} - r_P^0)}{k_{lost}\pi(2-2\xi)^2 + k_{prv}^P - k_T\pi(1-2\xi)^2}. \quad (15)$$

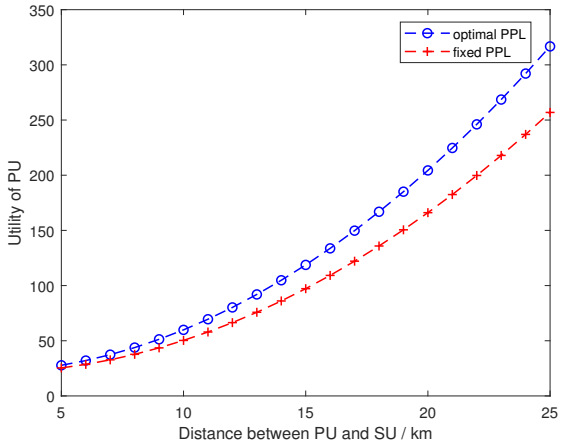

Fig. 2: PU utility comparison.

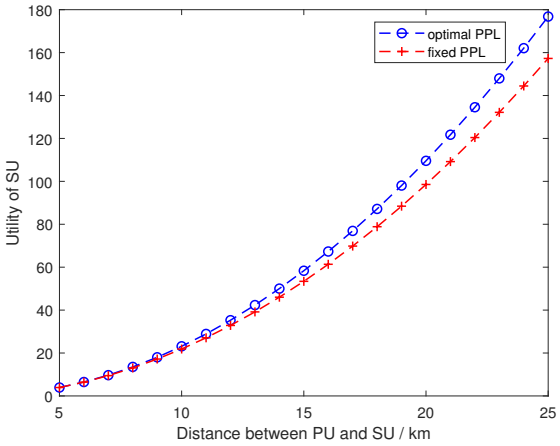

Fig. 3: SU utility comparison.

Therefore, the Stackelberg model based LPPM for spectrum sharing operates as follows: after receiving the SU's query, the PU responds to the SU with its expected privacy level l_ϵ^*; after observing the PU's strategy, the SU sets its privacy level to be l_S^*. At this point, both parties achieve the equilibrium (l_ϵ^*, l_S^*) of the Stackelberg game, where both the PU's and SU's utilities are maximized while their location privacy is preserved to a satisfactory level.

V. Simulation Results

In this section, numerical results are presented to demonstrate the performance enhancement of the proposed approach.

In the simulation, the PU's actual EZ radius r_P^0 is 1.5 km. The PU's unit revenue is $k_R^P = 3$, unit spectrum trading price is $k_T = 1$, unit performance loss is $k_{lost} = 0.8$, and privacy cost coefficient is $k_{prv}^S = 1$. The SU's unit reward k_R^S is set to be 1.5, and privacy cost coefficient k_{prv}^S is set to be 1.

To illustrate the superiority of the proposed approach, we compare our approach with the approach in which the PUs and SUs choose predefined fixed privacy levels to preserve their location information. The performance of the proposed approach is evaluated from two aspects: 1) the utilities of the PUs in different location settings where the relative distances between the PUs and SUs vary; 2) the utilities of the SUs in different location settings.

In Figures 2 and 3, the user utilities with the optimal PPL and fixed PPL are shown. Figure 2 gives the PU's utility comparison and demonstrates that the PU with the optimal PPL can achieve significantly higher utility than the PU using a fixed privacy level, with about 23% increase in the utility achievement. As the distance between the PU and SU becomes larger, the PU with the optimal PPL has a much higher utility gain. This is because in our proposed approach, the PU can adjust its PPL to a desired level based on the distance to the SU and maximize its utility. When the distance between the PU and SU becomes small, the utility difference reduces. This is because when the SU is close to the PU, the ATR for the SU is limited. As a result, the PU with either adjustable PPL or fixed PPL can only achieve a low utility.

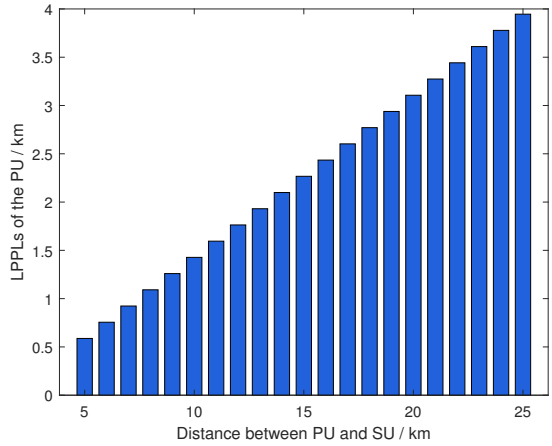

Fig. 4: PU's privacy level.

The SU's utility comparison is given in Figure 3. We can see that the SU following the PU's strategy achieves much higher utility than the SU maintaining its fixed privacy level after knowing the PU's strategy. The utility increase is more than 12%. As the distance between the PU and SU increases, the utility difference becomes more obvious. This is because the SU that adjusts its PPL based on the PU's strategy reaches the Nash equilibrium of the Stackelberg game, where the objective function, i.e., its utility, is maximized. When the distance between the PU and SU is small, the SU utility difference is not significant, which is similar to the PU's situation shown in Figure 2. Due to the small ATR for the SU, neither mechanism can achieve a very large utility.

The optimal location privacy-preserving levels (LPPLs) obtained based on our LPPMs for the PU and SU in different location settings are presented in Figures 4 and 5, respectively. It can be seen that as the distance between the PU and SU gets farther, the allowable maximum obfuscation lengths for both

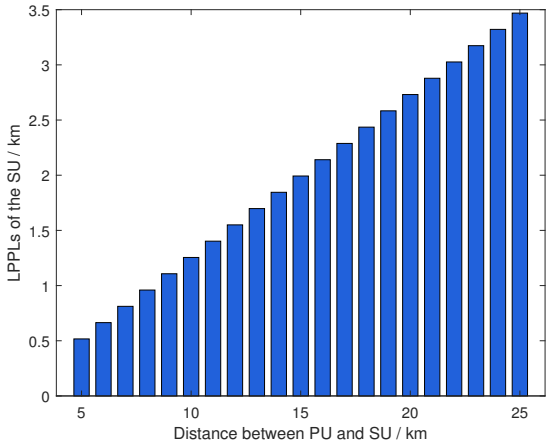

Fig. 5: SU's privacy level.

parties become larger, which means the users can protect their locations within a broader range. Combined with the results in Figures 2 and 3, this PPL increase will not cause utility decline, since the ATR also grows as the SU is more apart form the PU.

VI. Conclusions

In this paper, a novel bilateral LPPM for users participating in database-driven spectrum sharing systems is proposed. With this privacy preservation mechanism, PUs and SUs can flexibly adjust their PPLs such that their utilities are maximized and their location information is protected within desired ranges. Furthermore, the privacy costs of the users are built as part of their utility models in the proposed mechanism. In this way, the influence of privacy preservation on the overall utilities is quantified. Therefore, the decision maker can flexibly control the privacy cost and utility gain by adjusting the privacy level in practice. Simulation results indicate that the proposed privacy preservation mechanism can effectively enhance the utilities of both parties while providing satisfactory privacy guarantee. In the future work, the results will be extended to the scenario where multiple PUs and multiple SUs participate in spectrum sharing.

Appendix A
Proof of Theorem 1

Proof: Given $\forall l_\epsilon > 0$, taking the second-order derivative of U_S in (12) with respect to l_S yields

$$\frac{\partial^2 U_S}{\partial l_S^2} = -8k_T\pi - 2k_{prv}^S + 2k_R^S\pi.$$

It is obvious that $\frac{\partial^2 U_S}{\partial l_S^2}$ is negative on the interval $(0, \infty)$, i.e., U_S is strictly concave. Therefore, U_S has at most one global maximum and l_S that yields the global maximum is the optimal solution.

Taking the first-order derivative of U_S in (12) and setting $\frac{\partial U_S}{\partial l_S} = 0$, we can obtain $\overline{l_S^*}$. ■

Appendix B
Proof of Theorem 2

Proof: Substituting $\overline{l_S^*} = f(l_\epsilon)$ provided in Theorem 1 into the PU's utility function in (11) and taking the second derivative with respect to l_ϵ, we obtain

$$\frac{\partial^2 U_P}{\partial l_\epsilon^2} = -2k_{lost}\pi\left(\frac{4k_T\pi + 2k_{prv}^S}{4k_T\pi + k_{prv}^S - k_R^S\pi}\right)^2 - 2k_{prv}^P + 2k_T\pi\left(\frac{k_R^S\pi + k_{prv}^S}{4k_T\pi + k_{prv}^S - k_R^S\pi}\right)^2.$$

It can be easily shown that $\frac{\partial^2 U_P}{\partial l_\epsilon^2}$ is a constant and negative on the interval $(0, \infty)$. Thus U_P is a strictly concave downward function, and has one and only one global maximum. Thereby the value of l_ϵ achieving the maximum is the optimal privacy level for the PU. Taking the first derivative of U_P and setting $\frac{\partial U_P}{\partial l_\epsilon} = 0$, we can obtain l_ϵ^*. ■

References

[1] M. Grissa, B. Hamdaoui, and A. A. Yavuza, "Location privacy in cognitive radio networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 3, pp. 1726–1760, 3rd Quart. 2017.

[2] P. R. Vaka, S. Bhattarai, and J. Park, "Location privacy of non-stationary incumbent systems in spectrum sharing," in *Proc. IEEE Global Commun. Conf.*, Dec. 2016, pp. 1–6.

[3] N. Rajkarnikar, J. M. Peha, and A. Aguiar, "Location privacy from dummy devices in database-coordinated spectrum sharing," in *Proc. IEEE Int. Symp. Dyn. Spectr. Access Netw.*, Mar. 2017, pp. 1–10.

[4] B. Bahrak, S. Bhattarai, A. Ullah, J. J. Park, J. Reed, and D. Gurney, "Protecting the primary users' operational privacy in spectrum sharing," in *Proc. IEEE Int. Symp. Dyn. Spectr. Access Netw.*, Apr. 2014, pp. 236–247.

[5] M. Grissa, A. A. Yavuz, and B. Hamdaoui, "Preserving the location privacy of secondary users in cooperative spectrum sensing," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 2, pp. 418–431, Feb. 2017.

[6] ——, "Location privacy preservation in database-driven wireless cognitive networks through encrypted probabilistic data structures," *IEEE Trans. Cogn. Commun. Netw.*, vol. 3, no. 2, pp. 255–266, Jun. 2017.

[7] Z. Zhang, H. Zhang, S. He, and P. Cheng, "Bilateral privacy-preserving utility maximization protocol in database-driven cognitive radio networks," *IEEE Trans. Depend. Sec. Comput.*, vol. 17, no. 2, 2020.

[8] L. Zhang, C. Fang, Y. Li, H. Zhu, and M. Dong, "Optimal strategies for defending location inference attack in database-driven CRNs," in *Proc. IEEE Int. Conf. Commun.*, June 2015, pp. 7640–7645.

[9] R. Shokri, C. Troncoso, C. Diaz, J. Freudiger, and J.-P. Hubaux, "Unraveling an old cloak: k-anonymity for location privacy," in *Proc. 9th Annu. ACM Workshop Privacy Electron. Soc.*, 2010, pp. 115–118.

[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 *Proc. IEEE 12th Int. Conf. Mobile Ad Hoc Sensor Syst.*, Oct. 2015, pp. 181–189.

[11] M. E. Andrés, N. E. Bordenabe, K. Chatzikokolakis, and C. Palamidessi, "Geo-indistinguishability: Differential privacy for location-based systems," in *Proc. ACM SIGSAC Conf. Comput. Commun. Security*, 2013, pp. 901–914.

[12] C. Dwork, "Differential privacy: A survey of results," in *Proc. 5th Int. Conf. Theory and Applications of Models of Computation*, 2008, pp. 1–19.

[13] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. New York, NY: John Wiley & Sons, 1991.

[14] M. Simaan and J. B. Cruz, "On the Stackelberg strategy in nonzero-sum games," *J. Optimiz. Theory Appl.*, vol. 11, no. 5, pp. 533–555, 1973.

[15] ——, "Additional aspects of the Stackelberg strategy in nonzero-sum games," *J. Optimiz. Theory Appl.*, vol. 11, no. 6, pp. 613–626, 1973.