Bilateral Privacy-Utility Tradeoff in Spectrum Sharing Systems: A Game-Theoretic Approach

Mengmeng Liu, Xiangwei Zhou, and Mingxuan Sun

***Abstract*—In spectrum sharing systems based on spectrum trading, user locations are vital for the efficiency of dynamic channel reuse. However, both primary users (PUs) and secondary users (SUs) undertake the risk of location information leakage: a malicious PU may illegally collect SUs' location information to manipulate market decisions; a malicious SU would threat a PU's operational privacy by inferring the PU's location through seemingly inoffensive queries. To protect both PUs' and SUs' location information in spectrum trading, a bilateral privacy preservation framework is introduced in this paper. 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 while maintaining their location privacy to desired levels. Simulation results demonstrate that the proposed approach can effectively enhance user utility gain and strengthen user privacy guarantee by flexibly adjusting their privacy levels in practice.**

***Index Terms*—Location privacy, spectrum trading, Stackelberg game, utility maximization.**

I. Introduction

The proliferation of bandwidth-hungry applications has contributed to an explosive increase in the demand for the radio spectrum. Spectrum sharing has shown to be an effective and promising technique for flexible and efficient utilization of the scarce spectrum resources. In typical spectrum sharing systems [2]–[4], a network of geolocation databases (GDBs) is utilized to monitor the spectrum occupation and perform real-time interference management [5]. To enable dynamic channel access, each secondary user (SU) is required to report its geo-location and device parameters to the GDB. The GDB then combines the SUs' information with the operational information acquired from the primary user (PU), such as its location, spectrum occupation, and susceptibility to interference, to assign available spectrum resources to the SUs.

Although spectrum sharing through GDBs brings many pragmatic advantages, it also raises potential security and privacy issues for both PUs and SUs. On the one hand, a malicious SU may be able to infer critical operational attributes of the incumbent system through legitimately collecting query responses from GDBs. Since many incumbent systems of the 3.5GHz band in the U.S. and of the 2.3-2.4 GHz band in Europe are military systems [6], tactical systems, telemetry devices, and satellite earth stations [5], operational information breach may lead to serious consequences, such as threats to national security. This issue of information leakage is termed as the operational security (OPSEC) problem and has become a major concern in realizing shared spectrum usage in these bands [7]. On the other hand, an untrusted commercial incumbent system may take advantage of being a service provider to illegally collect SUs' characteristic parameters and infer users' private information, such as user beliefs, preferences, and shopping patterns [8], to manipulate sale strategies and market decisions, and therefore make profits that cannot be achieved through fair competition.

One of the key aspects of users' information security is the location privacy, which has recently aroused extensive attention [9]–[13]. However, these existing studies are mainly devoted to preserving location information for unilateral users while assuming the other side is trustworthy. As aforementioned, both PUs and SUs may suffer from location privacy breach during spectrum sharing, and thus preserving their location information simultaneously is more pragmatic. Recent work in [14] has shown that simply applying schemes designed for unilateral users to protect the privacy of PUs and SUs separately can result in severe utility loss for both parties. Moreover, most studies neglect the affected user utilities due to the added privacy preservation to location information. However, the privacy-preserving level (PPL) and utility are always a paradox: a higher PPL will lead to less available spectrum to share and thus decrease both parties' payoffs.

Motivated by the above challenging practical issues, a privacy preservation mechanism is introduced in this paper, adopting the celebrated differential privacy notion to protect both PUs' and SUs' location information. Both PUs' and SUs' PPLs are quantified in the proposed mechanism. Based on the privacy preservation mechanism, the utility models of PUs and SUs are constructed. The privacy cost of each party is considered as a part of its utility model. Therefore, the influence of different PPLs on the overall utility can be clearly revealed. 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 thereby maximize their utilities.

The main contributions of our work are summarized as follows:

Manuscript received June 6, 2019; revised December 15, 2019, May 31, 2020, and December 1, 2020; accepted March 2, 2021. 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. This paper was presented in part at the IEEE Global Communications Conference, 2020 [1]. *(Corresponding author: Xiangwei Zhou.)*

M. Liu and X. Zhou are with the Division of Electrical and Computer Engineering, Louisiana State University, Baton Rouge, LA 70803. Email: {lmengm1, xwzhou}@lsu.edu.

M. Sun is with Division of Computer Science and Engineering, Louisiana State University, Baton Rouge, LA 70803. Email: msun@csc.lsu.edu.

1) To the best of our knowledge, this is the first work using the game-theoretic approach to handle the tradeoff between the PPLs and utilities of both PUs and SUs in spectrum sharing.

2) A novel additive noise perturbation method is proposed based on the 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 in as part of the utility models. The revenues and costs caused by spectrum trading are modeled as functions of transmit radius, directly related to the PPL. The role played by the privacy level in the overall utility is quantified and clearly revealed in the utility models.

4) The proposed approach is generalized to multi-PU multi-SU scenarios, where users' possible relative location combinations and the corresponding spectrum allocation strategies are studied.

II. Related Work

Three major approaches have been adopted in the existing work of location privacy preservation: k-anonymity, differential privacy, and transformation-based approaches [15].

The k-anonymity in user location protection aims to ensure that among a set of k points, each point is indistinguishable. One method to realize this goal is to generate dummy locations [16], [17]. First $k-1$ false locations (dummies) are created; then along with the real location, k queries are performed to the database. Another method to achieve k-anonymity is through cloaking [18]–[20]. In this method, a cloaking area that consists of k points is created; the query sent to the service provider is based on the cloaking area instead of an individual user. The major drawback of the k-anonymity based mechanisms is that unless necessary assumptions about the adversaries' auxiliary information are made, a system cannot be proved to satisfy the k-anonymity condition. If any auxiliary information can help rule out a point that is with low probability to be a real location, the k-anonymity condition would be violated immediately.

Another widely used approach for location privacy preservation is differential privacy [21] from the statistical database field. The goal of differential privacy is to preserve an individual's information while releasing synthesis information of the entire database. This approach ensures that changing an individual user's information would not have a notable effect on the query outcome. Mathematically, it can be interpreted as follows: a query applying to two adjacent databases where only one point differs should return a same response with certain probabilities, and the probability ratio should be upper bounded. A widely adopted technique to achieve differential privacy is adding controlled random noise drawn from Laplacian distribution to the query output. The major advantage of differential privacy is that the privacy guarantee is independent of attackers' auxiliary information. Two representative studies of applying differential privacy to location information protection are [22] and [23]. In [22], it is shown that by using an aggregate data generation mechanism, the statistical information for commuting pattern can be released while being maintained differentially private. In [23], the quadtree spatial decomposition method is adopted to achieve differential privacy in location pattern mining.

In transformation-based mechanisms, the user location is made completely invisible to the service provider. To achieve this goal, all the data in a query process are transformed to a different space, usually with cryptographic technique, and the data can be mapped back to spatial information only by users [24], [25]. The data saved in the database as well as the location information sent by the user are encrypted. By employing private information retrieval techniques, service provider can return information concerning the encrypted location without divulging which exact location it is related to. The transformation-based approach, however, is computationally demanding and requires data in service provider side to be encrypted, which makes this technique hard to be employed by service providers that need to access the real data.

Meanwhile, the majority of the existing work dealing with location privacy issues in spectrum sharing focuses on unilateral privacy preservation. For example, the issue of protecting PUs' location information is studied in [6], [26]–[28], and the problem of SUs' location information leakage is discussed in [29]–[33]. Few studies, however, address the bilateral location privacy protection for both parties.

Recently, the issue of balancing the user utility and privacy cost draws great attention in the privacy-preserving study. In [34], the privacy-utility tradeoff in terms of design options for the Spectrum Access System and privacy strategies of the PUs is studied. The problem is formulated as environmental sensing capability estimation and solved with machine learning methods. In [35], the tradeoff between energy cost and privacy protection strength is considered, and the balance is achieved by the design of adjustable system coefficients. However, the costs introduced by different PPLs are not quantified, and thus the analysis of privacy impacts can be difficult.

In [14] and [36], a utility maximization protocol, UMax, is proposed to maximize PUs' and SUs' utilities while maintaining privacy guarantee. Our work is different from [14] and [36] in three aspects. First, in [14] and [36], the expectation of a random length added to protect the PU's location is used as the PPL, but 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 changing PPLs on users' overall utilities cannot be explicitly shown. In our work, we use the upper bound of the distance to sanitize the location as the PPL. In this way, the privacy strength can be clearly revealed through its upper bound, and the influence of privacy preservation on the overall utility can be easily controlled by adjusting the upper bound, i.e., the PPL. Second, in [14] and [36], the privacy cost is modeled as a reciprocal function of the PPL, which is against the intuition and their statement that a higher PPL leads to a lower privacy cost. In our work, we model the privacy cost as a quadratic function of the PPL. Therefore, the privacy cost increases as the PPL raises. Moreover, the quadratic form makes the

construction of each term consistent in our model. Third, in [14] and [36], the utility maximization problems for PUs and SUs are modeled as separate optimization problems, and no inner connection is built between the problems. However, in a spectrum sharing system, the PUs and SUs are closely related, and the decision made by one party, such as the used PPL, should have influence on the system as a whole. In our work, we model the utility maximization problem as a Stackelberg game, where PUs and SUs make decisions interactively. As a result, the optimal solution obtained in our work is the Nash equilibrium, where both parties reach the best states, while the solution obtained in [14] and [36] is not. The game-theoretic approach has shown to be a powerful and efficient tool in modeling and solving dilemmas, while no existing work introduces this method to the privacy-utility tradeoff problem in spectrum sharing.

III. Problem Formulation

In this section, the spectrum sharing process without the privacy leakage risk involved is first described. Then the user location privacy threats are presented with the adversary models, based on which the problem to be addressed in the paper is formulated.

A. Dynamic Channel Access

A typical spectrum sharing system based on spectrum trading consists of three major components: PUs, SUs, and the database. Consider N PUs and M SUs in the system. Each PU is authorized to operate in a distinct channel and thus no interference exists between the PUs. As a result, they can be decoupled and separately considered. To avoid interference caused by the SUs, an exclusive zone exists for each PU, within which no SU is allowed to transmit over the same channel. Outside the exclusive zone, the SUs are allowed to transmit with power limits.

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 loc_j and channel of interest ch_i. The database responds to the query with the availability of the requested channel, including the maximum transmit power (MTP) P and the duration t in which the SU is allowed to use the channel. The MTP can be calculated as follows:

$$P = \begin{cases} f\left(d - r_P^0\right), & if\ d > r_P^0, \\ 0, & if\ d \le r_P^0, \end{cases} \tag{1}$$

where d is the distance between the SU and PU, r_P^0 is the radius of the PU's exclusive zone, and $f(\cdot)$ is a monotonically increasing MTP calculation function. If the SU is not allowed to transmit, the responded MTP and 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. Firstly, a malicious SU can use a series of query responses to infer a PU's location with certain accuracy. Suppose that a sophisticated malicious SU can obtain the MTP calculation function adopted by the database. Then based on the MTP calculation function, the SU can compute its maximum transmission radius (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), $i = 1, 2, 3$, as shown in Figure 1. Then the SU will be able to accurately locate the PU and infer the corresponding exclusive zone by solving

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

Secondly, a curious database manager may pose serious location privacy threats to SUs. In the spectrum sharing system discussed above, an SU reports its precise location to the database to get spectrum availability information. As a result, a malicious PU can take advantage of this and collect the SUs' location information. Combined with auxiliary information obtained from public data sets, the preference and other characteristic information of the SUs could be easily inferred and sold to profitable enterprises. [29].

C. Problem of Interest

To protect PUs' and SUs' location information from malicious attacks, a privacy preservation mechanism needs to be adopted. At the same time, however, unrestrictedly raising the PPL will significantly reduce the available transmission radius (ATR), defined as the allowable transmission distance for SUs without causing interference to PUs, and therefore lead to serious utility losses for 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 expected levels?

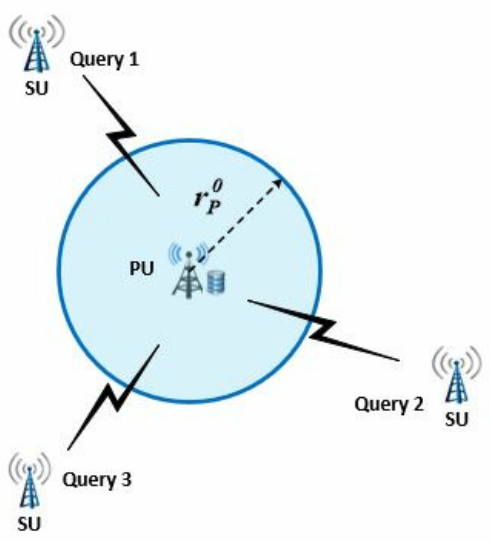
IV. Bilateral Privacy Preservation Mechanism

In this section, a bilateral privacy preservation framework is introduced based on the notion of geo-indistinguishability to protect the location privacy for both PUs and SUs.

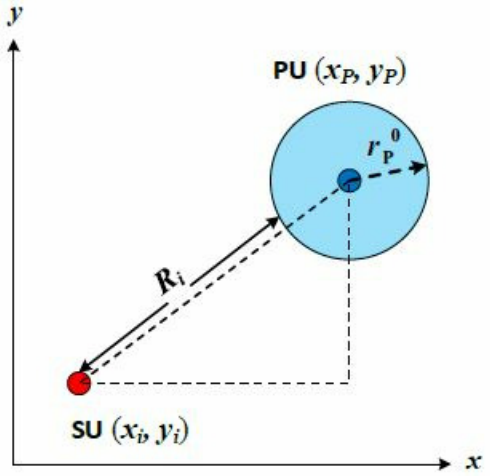
A. Geo-indistinguishability

Geo-indistinguishability 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 [15]. In this paper, a modified version of geo-indistinguishability, named γ-geo-indistinguishability (γ-GI), is adopted 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:



(a) Queries to locate PU



(b) Geometric description

Fig. 1: PU location inference.

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

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^*, $\gamma = \delta l$ specifies the difference level of the probabilities that two users report a same sanitized location, and δ determines the privacy preservation at unit distance.

The above definition shows that 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}. Therefore, an attacker will not be able to determine whether the user is located at z_0 or z_0^* when it obtains the user's location z, and thereby the user's location privacy will not be breached.

In [15], geo-indistinguishability is interpreted in the following way: given a fixed range of radius l centered at the user's exact location, reducing the parameter δ narrows down the difference between $P\left(z \mid z_0\right)$ and $P\left(z \mid z_0^*\right)$, and therefore the user enjoys a stronger privacy. 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 adjusting the radius. Therefore, we can interpret the γ-GI as follows: given the probability difference level γ, adjusting δ results in the protection of user location in a different scale l; a larger l indicates that the user can obfuscate its location information in a larger range and thus achieve stronger privacy. As a result, users can flexibly choose their desired privacy-preserving scale, i.e., the radius l, denoted as the PPL.

B. Bilateral Privacy Preservation

Based on the γ-GI notion, a bilateral privacy preservation mechanism that simultaneously protects both PUs' and SUs' location information is presented in the following, with the graphical interpretation given in Figure 2.

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, such as (x', y') or (x'', y'') in Figure 2, instead of the exact location (x, y), along with the bound l_S of the randomized radius. Here l_S is the radius of the protected range in the γ-GI notion and adopted as the PPL for SUs.

To generate the random location, a proper distribution should be selected. It is proven in [15] that the two-dimensional Laplacian noise can achieve geo-indistinguishability, and thus satisfies γ-GI. The probability density function (PDF) of a two-dimensional Laplacian distribution is

$$f\left(z \mid z_0\right) = \frac{\delta^2}{2\pi} e^{-\delta d(z_0, z)}, \tag{3}$$

where $z_0 \in \mathbb{R}^2$ is the real location of the SU and $z \in \mathbb{R}^2$ is the produced location using the privacy preservation mechanism.

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

$$f\left(r, \theta; \delta\right) = \frac{\delta^2}{2\pi} r e^{-\delta r}, \tag{4}$$

where r is the radial distance corresponding to the distance between z_0 and z in Cartesian coordinates, and 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 can be obtained as

$$f\left(r; \delta\right) = \int_0^{2\pi} f\left(r, \theta; \delta\right) \mathrm{d}\theta = \delta^2 r e^{-\delta r} \tag{5}$$

and

$$f\left(\theta; \delta\right) = \int_0^{\infty} f\left(r, \theta; \delta\right) \mathrm{d}r = \frac{1}{2\pi}, \tag{6}$$

respectively. By utilizing the densities described in (5) and (6), 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.

It is shown in [7] that differential privacy cannot be applied to the PU's location preservation. Different from the protocol that the SU reports its randomized location based on the γ-GI notion, the PU responds with the MTP, which is translated to a non-negative length rather than a location. Therefore, the geo-indistinguishability notion as a variation of the differential privacy cannot be used to protect the PU's location privacy. To thwart the location inference attack to PUs, an obfuscation-based mechanism using the Gamma distribution is proposed. As shown in Figure 2, the database adds a randomized length r_ϵ, with maximum value l_ϵ, to the radius of the PU's actual exclusive zone after receiving a query. Then the MTP is calculated based on the newly generated exclusive zone, with radius $r_P^0 + r_\epsilon$ $(0 < r_\epsilon \leqslant l_\epsilon)$. The PU responds to the SU with this sanitized exclusive zone radius R_j'. In this case, (2) becomes

$$\begin{cases} (x_P - x_1)^2 + (y_P - y_1)^2 = \left(r_P^0 + r_\epsilon^{(1)} + R_1'\right)^2, \\ (x_P - x_2)^2 + (y_P - y_2)^2 = \left(r_P^0 + r_\epsilon^{(2)} + R_2'\right)^2, \\ (x_P - x_3)^2 + (y_P - y_3)^2 = \left(r_P^0 + r_\epsilon^{(3)} + R_3'\right)^2, \end{cases} \tag{7}$$

which is extremely difficult to solve with a random $r_\epsilon^{(j)}$ in the jth query. Specifically, each query-response round would add an equation but also introduce one more unknown $r_\epsilon^{(j)}$. As a result, more queries/equations would not help solve (7). Therefore, a malicious SU cannot obtain the exact distance between the PU and itself based on the MTP. Moreover, r_ϵ is truncated by l_ϵ, where the maximum length l_ϵ is updated in each query-response round, making it more difficult to precisely locate the PU.

To generate the random length r_ϵ, the Gamma distribution is adopted:

$$f\left(r_\epsilon; \alpha, \beta\right) = \frac{\beta^\alpha r_\epsilon^{\alpha-1} e^{-\beta r_\epsilon}}{\Gamma(\alpha)} \text{ for } r_\epsilon > 0 \text{ and } \alpha > 0, \beta > 0, \tag{8}$$

where α is the shape parameter, β is the scale parameter, and $\Gamma(\alpha)$ is the gamma function. 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 [37]. Therefore, it is suitable and effective to adopt Gamma density to generate random lengths for obfuscating PUs' exclusive zones in practice. To determine the shape parameter and scale parameter, we let r in (4) to be r_ϵ. The integral over θ yields

$$f_R(r_\epsilon; \delta) = \int_0^{2\pi} \frac{\delta^2}{2\pi} r_\epsilon e^{-\delta r_\epsilon} \mathrm{d}\theta = \delta^2 r_\epsilon e^{-\delta r_\epsilon}, \tag{9}$$

which is the Gamma distribution with scale $\frac{1}{\delta}$ and shape 2. Note that to make it even more difficult to precisely locate the PU, r_ϵ is truncated by l_ϵ, which may no longer be of the maximum entropy distribution. However, the above analysis shows that the SU will be unable to effectively locate the PU and infer the corresponding exclusive zone, i.e., the PU can achieve privacy in practice.

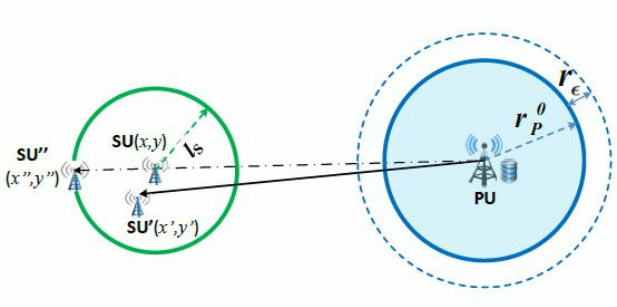


Fig. 2: Bilateral privacy preservation mechanism.

For PUs' privacy preservation, only random radius rather than obfuscated user location 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 and the generated random r_ϵ satisfying $r_\epsilon < l_\epsilon$ is selected.

Figure 2 illustrates the overall bilateral privacy preservation framework. The left solid circle indicates the SU's preserved area with PPL l_S, within which a malicious PU cannot determine the SU's actual location. The right solid circle represents the PU's exclusive zone, while the dashed circle represents the obfuscation area of the exclusive zone with PPL 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 exclusive zone.

Intuitively, adjusting the PU's or SU's PPL will change the SU's MTP, and thus affect both parties' utilities. 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 2, the MTR for the SU with location privacy preservation is

$$R_M = d(PU, SU') - r_P^0 - l_\epsilon - l_S, \tag{10}$$

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., $R_A \leqslant R_M$.

V. 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 (10) and result in decreased user utilities. To tackle this dilemma, the Stackelberg game is used to achieve the tradeoff between the PPLs and user utilities. The single-PU-single-SU case is studied in this section, and the generalization to the multi-PU-multi-SU case will be given in Section VI.

A. Modeling Spectrum Sharing as Stackelberg Game

Spectrum sharing can be modeled as a Stackelberg game, in which PUs act as the leader and SUs act 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 [38].

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:

$$s_P^* = \text{argmax}_{s_P \in \boldsymbol{S_P}} U_P\{(s_P; s_S)|s_S = s_S^0\}. \quad (11)$$

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:

$$s_S^* = \text{argmax}_{s_S \in \boldsymbol{S_S}} U_S\{(s_S; s_P)|s_P = s_P^*\}. \quad (12)$$

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

$$\boldsymbol{S_P} = \{l_\epsilon |\, l_\epsilon \geqslant r_\epsilon > 0,\, r_\epsilon \sim \Gamma(2, \frac{1}{\delta})\}. \quad (13)$$

The SU's strategy set is defined as

$$\boldsymbol{S_S} = \{l_S \mid \frac{P(z|z_0)}{P(z|z_0^*)} \leqslant e^\gamma,\, d(z_0, z_0^*) \leqslant l_S,\, \gamma = \delta l_S\}. \quad (14)$$

Since the Stackelberg game is solved via backward induction [39], 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

$$\begin{cases} U_P(l_\epsilon^*, l_S^*) \geqslant U_P(l_\epsilon, l_S), \\ U_S(l_\epsilon^*, l_S^*) \geqslant U_S(l_\epsilon, l_S), \end{cases} \quad \forall l_\epsilon \in \boldsymbol{S_P},\ \forall l_S \in \boldsymbol{S_S}. \quad (15)$$

B. Utility Functions

To construct a meaningful utility function with respect to the privacy level, the following conditions must be satisfied: first, the obtained privacy level based on the utility function must be non-negative; second, the obtained privacy level should be proportional to the distance between the PU and SU, and the available transmit radius for the SU; third, the obtained privacy level must be within a certain range, not too small or too large, to make the results meaningful in practice. A quadratic form is used in modeling user utility in spectrum sharing, which makes the construction of each term consistent in our model.

Consider the example as shown in Figure 1. Each user in the figure can be a base station or access point of a cellular system, serving end users around it. The PU is the license holder of the spectrum so it can utilize the spectrum to serve its end users and share with the SU via spectrum trading. Therefore, the PU's utility is composed of four parts that are relevant to the privacy level: revenues from its own data transmission to serve its end users, payoffs from selling spectrum to the SU, performance loss due to the shared spectrum with the SU, and the cost for privacy preservation. As a result, the PU's utility function is defined as

$$U_P = P_R^P + P_{sell} - P_{lost} - C_{prv}^P. \quad (16)$$

The construction of each term in (16) is based on the quadratic form stated above and the observations from the example: the PU's data transmission revenue P_R^P is modeled as a function of its exclusive zone, that is, $P_R^P = k_R^P \pi (r_P^0)^2$, where k_R^P is the unit revenue of data transmission, within which the PU can transmit signals and therefore gain payoffs by providing services; P_{sell} and P_{lost}, denoting the PU's revenue and cost due to spectrum trading, respectively, are modeled as functions of the ATR, i.e., $P_{sell} = k_T \pi (d_{PS} - r_P^0 - l_\epsilon - 2l_S)^2$, $P_{lost} = k_{lost} \pi (d_{PS} - r_P^0 - 2l_\epsilon - 2l_S)^2$, where k_T is the unit spectrum trading price, d_{PS} is the distance between the PU and SU, and k_{lost} is the coefficient of the PU's performance loss; C_{prv}^P, defined as the PU's privacy cost, is modeled as a function of its PPL l_ϵ, i.e., $C_{prv}^P = k_{prv}^P l_\epsilon^2$, where k_{prv}^P is the PU's privacy preservation coefficient. Note that the minimum distance between the preserved area of the SU and the obfuscation area of the exclusive zone of the PU is $d_{PS} - r_P^0 - l_e - l_S$. As the SU only reports its sanitized location along with the bound l_S of the randomized radius, $d_{PS} - r_P^0 - l_e - 2l_S$ is the minimum radius of the traded spectrum area perceived by the PU, within which the SU can always transmit and provide services. Similarly, $d_{PS} - r_P^0 - 2l_e - 2l_S$ is the minimum radius of the traded spectrum area $(d_{PS} - r_P^0 - l_\epsilon - 2l_S)$ reduced by l_ϵ, where the PU can no longer use for its own transmission due to spectrum trading. Therefore, the utility function of the PU becomes

$$\begin{aligned} U_P &= k_R^P \pi (r_P^0)^2 + k_T \pi (d_{PS} - r_P^0 - l_\epsilon - 2l_S)^2 \\ &- k_{lost} \pi (d_{PS} - r_P^0 - 2l_\epsilon - 2l_S)^2 - k_{prv}^P l_\epsilon^2. \end{aligned} \quad (17)$$

The coefficient of P_{sell}, i.e., k_T, should be larger than the coefficient of P_{lost}, i.e., k_{lost}, such that PUs are willing to share their spectrum with SUs. However, k_T should not be much larger than k_{lost}; otherwise PUs will prefer selling spectrum rather than providing services themselves, which may cause service disruption. The distance d_PS does not have to be the exact distance between the PU and SU, which can be an approximated value calculated and also reported by the PU.

Similarly, the SU's utility function consists of three parts relevant to the privacy level: rewards gained through its data transmission to serve end users, payment for accessing the spectrum, and cost for location privacy preservation. The SU's utility function is defined as

$$U_S = P_R^S - P_{buy} - C_{prv}^S, \quad (18)$$

where P_R^S denotes the SU's rewards obtained by providing services with the acquired spectrum, modeled as a function of the transmit radius accessible to the SU, i.e., $P_R^S = k_R^S \pi (d_{PS} - r_P^0 - l_\epsilon - l_S)^2$, where k_R^S is the SU's unit reward; P_{buy} is the SU's payment for utilizing the channel, which is equal to P_{sell} in the single-PU-single-SU scenario; C_{prv}^S is the SU's privacy-preserving cost, modeled as a quadratic function of the SU's PPL l_S, i.e., $C_{prv}^S = k_{prv}^S l_S^2$, where k_{prv}^S is the SU's privacy preservation coefficient. Therefore, the utility function of the SU becomes

$$\begin{aligned} U_S &= k_R^S \pi (d_{PS} - r_P^0 - l_\epsilon - l_S)^2 \\ &- k_T \pi (d_{PS} - r_P^0 - l_\epsilon - 2l_S)^2 - k_{prv}^S l_S^2. \end{aligned} \quad (19)$$

(17) and (19) show that by altering users' PPLs l_ϵ and l_S, user utilities U_P and U_S will change accordingly. The influence of the PPL on a user's utility can thus be revealed and quantified. To capture the value that a PU or SU holds for achieving more privacy, the coefficient of the last term in the utility function of (17) or (19) can be generally adjusted. In the case that a user favors more towards privacy, the coefficient k^P_{prv} or k^S_{prv} can be set to a negative value.

C. Stackelberg Equilibrium

Since users' utilities are affected by the PPLs that they choose, it is desired to find out the optimal PPLs that maximize both parties' profits. The solution is proposed based on the Stackelberg game. Note that the number of parameters in the above utility models is minimized in the sense that only the parameters that determine the unit price and the unit performance loss are kept and no extra parameter is used. These coefficients also introduce flexibility to the model. In practice, the designer can freely determine the coefficients of each term in the utility models, as long as the coefficients satisfy the constraints given in the following theorems, to make the user utility models suitable for a specific scenario.

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 PPL is first determined according to Theorem 1.

Theorem 1. *When $0 < k_T < k^S_R < 2k_T$, there exists an optimal solution $\overline{l^*_S}$ to the following problem*

$$\text{argmax}_{l_S \in \boldsymbol{S_S}} U_S$$

subject to $l_S > 0$, where $U_S = k^S_R\pi(d_{PS} - r^0_P - l_\epsilon - l_S)^2 - k_T\pi(d_{PS} - r^0_P - l_\epsilon - 2l_S)^2 - k^S_{prv}l^2_S$, $\forall l_\epsilon > 0$. The optimal solution is

$$\overline{l^*_S} = \frac{(2k_T\pi - k^S_R\pi)(d_{PS} - r^0_P - l_\epsilon)}{4k_T\pi + k^S_{prv} - k^S_R\pi}.$$

The proof of Theorem 1 is given in Appendix A. The condition $0 < k_T < k^S_R < 2k_T$ in Theorem 1 indicates that the SU's unit reward is chosen larger than the spectrum unit price but no more than twice of the spectrum unit price. Theorem 1 shows that given any PPL l_ϵ picked by the PU, the SU's best strategy is to set its PPL l_S as $\overline{l^*_S}$ presented in the theorem.

Note that the SU's optimal PPL $\overline{l^*_S}$ obtained in this step is expressed as a function of the PU's PPL l_ϵ. With the information of the SU's predicted PPL, the best response function of the PU can be found. The optimal PPL l^*_ϵ for the PU can be determined according to Theorem 2.

Theorem 2. *When $0 < k_{lost} < k_T < 2k_{lost}$, there exists an optimal PPL l^*_ϵ to the following problem*

$$\text{argmax}_{l_\epsilon \in \boldsymbol{S_P}} U_P$$

subject to $l_\epsilon > 0$, where $U_P = k^P_R\pi(r^0_P)^2 + k_T\pi(d_{PS} - r^0_P - l_\epsilon - 2\overline{l^*_S})^2 - k_{lost}\pi(d_{PS} - r^0_P - 2l_\epsilon - 2\overline{l^*_S})^2 - k^P_{prv}l^2_\epsilon$ and $\overline{l^*_S} = f(l_\epsilon)$. The optimal solution is

$$l^*_\epsilon = \frac{[k_{lost}\pi(2-2\xi)(1-2\xi) - k_T\pi(1-2\xi)^2](d_{PS} - r^0_P)}{k_{lost}\pi(2-2\xi)^2 + k^P_{prv} - k_T\pi(1-2\xi)^2},$$

where $\xi = \frac{2k_T\pi - k^S_R\pi}{4k_T\pi + k^S_{prv} - k^S_R\pi}$.

The proof of Theorem 2 is given in Appendix B. The condition $0 < k_{lost} < k_T < 2k_{lost}$ indicates that the unit spectrum trading payoff is chosen higher than the unit performance loss but no more than twice of the unit performance loss. The PPL l^*_ϵ presented 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 PPL can be found by substituting l^*_ϵ into the response function in Theorem 1, which yields

$$l^*_S = \frac{\xi[k_{lost}\pi(2-2\xi) + k^P_{prv}](d_{PS} - r^0_P)}{k_{lost}\pi(2-2\xi)^2 + k^P_{prv} - k_T\pi(1-2\xi)^2}.$$

According to the above analysis, the Stackelberg game for spectrum sharing can be summarized as follows: after receiving the SU's query, the PU responds to the SU with its expected PPL l^*_ϵ; after observing the PU's strategy, the SU sets its PPL 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.

VI. Utility and Privacy Level Tradeoff for Multi-PU-multi-SU Case

In this section, the Stackelberg model for utility-privacy tradeoff is generalized to the case of multiple PUs and multiple SUs. The multi-user case is more complicated, where the combinations of multiple locations among PUs and SUs are possible. As the relative locations of PUs and SUs vary, the influence of possible interference and transmission limitation on the privacy levels and user utilities will be discussed.

Since different PUs occupy different channels and allocate their spectrum separately, the multi-PU-multi-SU problem can be reduced to the single-PU-multi-SU problem. To start with, the single-PU-two-SU case is considered. There are two possible cases for spectrum sharing between one PU and two SUs: 1) after spectrum allocation, the SUs' allowable transmission ranges do not overlap; 2) the SUs' transmission ranges overlap with high possibility. Note that when there are multiple SUs requesting the same channel, the PU can estimate its distances to the SUs after receiving SUs' transmitted query messages, through which the PU can tell whether the SUs will interfere with the PU and other SUs or not.

In Case 1, the SUs will not interfere with each other when they both access the channel with full ATR, as shown in Figure 3.

In this case, the PU's utility can be defined as

$$U_P = P^P_R + P^{SU1}_{sell} + P^{SU2}_{sell} - P^{SU1}_{lost} - P^{SU2}_{lost} - C^P_{prv}, \quad (20)$$

where P^{SU1}_{sell} and P^{SU2}_{sell} are the PU's payoffs by trading its spectrum to SU_1 and SU_2, respectively, and P^{SU1}_{lost} and P^{SU2}_{lost} are the PU's performance losses due to the shared spectrum with SU_1 and SU_2, respectively. Accordingly, the PU's utility can be expressed as

$$\begin{aligned} U_P &= k^P_R\pi(r^0_P)^2 + k_T\pi(d_{PS1} - r^0_P - l_\epsilon - 2l_{S1})^2 \\ &+ k_T\pi(d_{PS2} - r^0_P - l_\epsilon - 2l_{S2})^2 \\ &- k_{lost}\pi(d_{PS1} - r^0_P - 2l_\epsilon - 2l_{S1})^2 \\ &- k_{lost}\pi(d_{PS2} - r^0_P - 2l_\epsilon - 2l_{S2})^2 - k^P_{prv}l^2_\epsilon, \quad (21) \end{aligned}$$

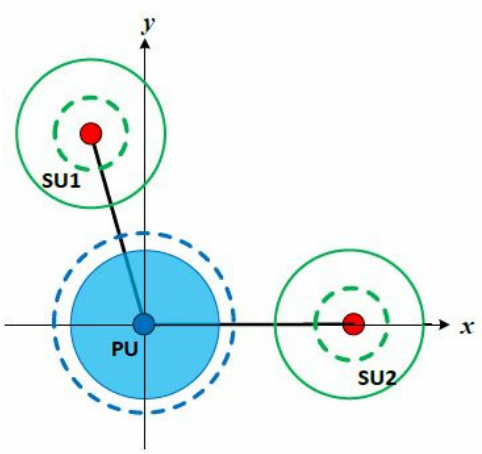


Fig. 3: SUs do not interfere with each other.

where d_{PS1} is the distance between the PU and SU_1, l_{S1} is SU_1's PPL, d_{PS2} is the distance between the PU and SU_2, and l_{S2} is SU_2's PPL.

Since both SUs can access the spectrum with full ATR, the utility model of each SU is defined in the same way as (18). Each SU's utility can be expressed as

$$\begin{aligned} U_{Si} &= k_R^{Si}\pi(d_{PSi} - r_P^0 - l_\epsilon - l_{Si})^2 \\ &- k_T\pi(d_{PSi} - r_P^0 - l_\epsilon - 2l_{Si})^2 - k_{prv}^{Si} l_{Si}^2, \quad (22) \end{aligned}$$

where U_{Si} represents the utility of SU_i, $(i = 1, 2)$, k_R^{Si} is the unit reward, and k_{prv}^{Si} is the privacy preservation coefficient.

Based on the user utility functions above, the multi-player Stackelberg game [40] is used to achieve the SPNE. Similar to the two-player Stackelberg model, the best responses of the SUs are first determined in Theorem 3 via backward induction.

Theorem 3. *When $0 < k_T < k_R^{S1} < 2k_T$ and $0 < k_T < k_R^{S2} < 2k_T$, there exists an optimal solution $(\overline{l_{S1}^*}, \overline{l_{S2}^*})$ to the following problem*

$$\text{argmax}_{l_{S1} \in \boldsymbol{S_{S1}}} U_{S1}$$

and

$$\text{argmax}_{l_{S2} \in \boldsymbol{S_{S2}}} U_{S2}$$

subject to $l_{S1} > 0$ and $l_{S2} > 0$, where $U_{S1} = k_R^{S1}\pi(d_{PS1} - r_P^0 - l_\epsilon - l_{S1})^2 - k_T\pi(d_{PS1} - r_P^0 - l_\epsilon - 2l_{S1})^2 - k_{prv}^{S1} l_{S1}^2$ and $U_{S2} = k_R^{S2}\pi(d_{PS2} - r_P^0 - l_\epsilon - l_{S2})^2 - k_T\pi(d_{PS2} - r_P^0 - l_\epsilon - 2l_{S2})^2 - k_{prv}^{S2} l_{S2}^2, \forall l_\epsilon > 0$. The optimal solution is

$$\overline{l_{S1}^*} = \frac{(2k_T\pi - k_R^{S1}\pi)(d_{PS1} - r_P^0 - l_\epsilon)}{4k_T\pi + k_{prv}^{S1} - k_R^{S1}\pi}$$

and

$$\overline{l_{S2}^*} = \frac{(2k_T\pi - k_R^{S2}\pi)(d_{PS2} - r_P^0 - l_\epsilon)}{4k_T\pi + k_{prv}^{S2} - k_R^{S2}\pi}.$$

The proof of Theorem 3 is similar to that of Theorem 1. Since both SUs can fully access the spectrum as much as the ATR, their best PPLs can be calculated independently. By replacing d_{PS}, k_R^S, and k_{prv}^S with d_{PSi}, k_R^{Si}, and k_{prv}^{Si}, $i = 1, 2$, we can easily obtain the above results.

With the knowledge of the two SUs' predicted best PPLs $(\overline{l_{S1}^*}, \overline{l_{S2}^*})$, the PU's optimal PPL can be found according to Theorem 4.

Theorem 4. *When $0 < k_{lost} < k_T < 2k_{lost}$, there exists an optimal PPL l_ϵ^* to the following problem*

$$\text{argmax}_{l_\epsilon \in \boldsymbol{S_P}} U_P$$

subject to $l_\epsilon > 0$, where $U_P = k_R^P\pi(r_P^0)^2 + k_T\pi(d_{PS1} - r_P^0 - l_\epsilon - 2\overline{l_{S1}^*})^2 + k_T\pi(d_{PS2} - r_P^0 - l_\epsilon - 2\overline{l_{S2}^*})^2 - k_{lost}\pi(d_{PS1} - r_P^0 - 2l_\epsilon - 2\overline{l_{S1}^*})^2 - k_{lost}\pi(d_{PS2} - r_P^0 - 2l_\epsilon - 2\overline{l_{S2}^*})^2 - k_{prv}^P l_\epsilon^2$, $\overline{l_{S1}^*} = f_1(l_\epsilon)$, and $\overline{l_{S2}^*} = f_2(l_\epsilon)$. The optimal solution is

$$l_\epsilon^* = \frac{U_1}{k_{lost}\pi(\Omega_1 + \Omega_2) + k_{prv}^P - k_T\pi(\Gamma_1 + \Gamma_2)},$$

where $U_1 = k_{lost}\pi[\sqrt{\Gamma_1\Omega_1}(d_{PS1} - r_P^0) + \sqrt{\Gamma_2\Omega_2}(d_{PS2} - r_P^0)] - k_T\pi[\Gamma_1(d_{PS1} - r_P^0) + \Gamma_2(d_{PS2} - r_P^0)]$, $\Gamma_1 = (1 - 2\phi_1)^2$, $\Omega_1 = (2 - 2\phi_1)^2$, $\Gamma_2 = (1 - 2\phi_2)^2$, and $\Omega_2 = (2 - 2\phi_2)^2$, with $\phi_1 = \frac{2k_T\pi - k_R^{S1}\pi}{4k_T\pi + k_{prv}^{S1} - k_R^{S1}\pi}$ and $\phi_2 = \frac{2k_T\pi - k_R^{S2}\pi}{4k_T\pi + k_{prv}^{S2} - k_R^{S2}\pi}$.

The proof of Theorem 4 is provided in Appendix C. The PPL l_ϵ^* obtained in Theorem 4 is the PU's best PPL to the reactions of the two SUs in equilibrium. After receiving the PU's PPL, the SUs' best responses can be decided by substituting l_ϵ^* into their response functions described in Theorem 3, which yields

$$l_{S1}^* = \frac{\phi_1 U_2}{k_{lost}\pi(\Omega_1 + \Omega_2) + k_{prv}^P - k_T\pi(\Gamma_1 + \Gamma_2)}$$

and

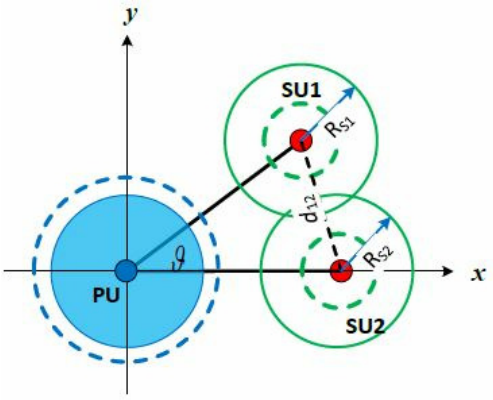
$$l_{S2}^* = \frac{\phi_2 U_3}{k_{lost}\pi(\Omega_1 + \Omega_2) + k_{prv}^P - k_T\pi(\Gamma_1 + \Gamma_2)},$$

where $U_2 = [k_{lost}\pi(\sqrt{\Omega_1} + \Omega_2) + k_{prv}^P - k_T\pi\Gamma_2](d_{PS1} - r_P^0) - (k_{lost}\pi\sqrt{\Gamma_2\Omega_2} - k_T\pi\Gamma_2)(d_{PS2} - r_P^0)$ and $U_3 = [k_{lost}\pi(\Omega_1 + \sqrt{\Omega_2}) + k_{prv}^P - k_T\pi\Gamma_1](d_{PS2} - r_P^0) - (k_{lost}\pi\sqrt{\Gamma_1\Omega_1} - k_T\pi\Gamma_1)(d_{PS1} - r_P^0)$.

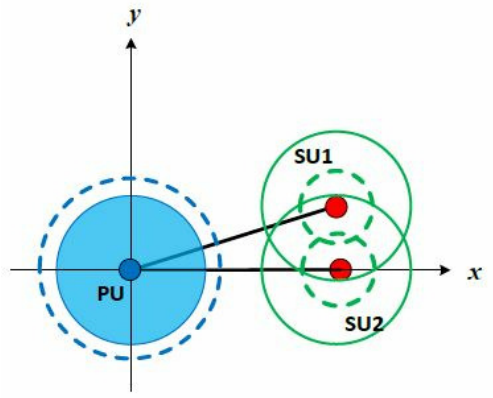
Therefore, in the single-PU-two-SU spectrum sharing case where both SUs can fully access the spectrum without interference to each other, the Stackelberg game can be described as follows: after receiving the SUs' queries, the PU responds to the two SUs with its desired PPL l_ϵ^*; after seeing the PU's response, the two SUs choose their PPLs to be l_{S1}^* and l_{S2}^*, respectively. At this point, the PU and SUs reach the equilibrium $(l_\epsilon^*, l_{S1}^*, l_{S2}^*)$ of the Stackelberg game, where all the users achieve the desired PPLs and their utilities are maximized.

In Case 2, the two SUs are located relatively close to each other. If they access the spectrum with the ATR determined in the above case, it is highly likely that the two SUs will interfere with each other. Two possible circumstances may occur in this case: 1) both SUs can still access the spectrum simultaneously, but their ATR needs to be reduced; 2) the two SUs are extremely close to each other, such that only one SU is allowed to transmit at one time. The graphical illustration is given in Figure 4.

For the first circumstance, the utility composition of the PU and SUs can be described as in (20) and (18). By modeling



(a) Both SUs can access the spectrum



(b) Only one SU is allowed to transmit

Fig. 4: Two SUs interfere each other with high possibility.

spectrum sharing as a Stackelberg game, the best PPLs of the SUs and PU can be determined by Theorems 5 and 6, respectively, using backward induction.

Theorem 5. *There exists an optimal solution* $(\overline{l_{S1}^*}, \overline{l_{S2}^*})$ *to the following problem*

$$\text{argmax}_{l_{S1}\in\boldsymbol{\mathcal{S}_{S1}}} U_{S1}$$

and

$$\text{argmax}_{l_{S2}\in\boldsymbol{\mathcal{S}_{S2}}} U_{S2}$$

subject to $l_{S1}>0$, $l_{S2}>0$, $0\leqslant R_{S1}<d_{PS1}-r_P^0-l_\epsilon-l_{S1}$, *and* $0\leqslant R_{S2}<d_{PS2}-r_P^0-l_\epsilon-l_{S2}$, *where* $U_{S1}=k_R^{S1}\pi R_{S1}^2-k_T\pi(R_{S1}-l_{S1})^2-k_{prv}^{S1}l_{S1}^2$ *and* $U_{S2}=k_R^{S2}\pi R_{S2}^2-k_T\pi(R_{S2}-l_{S2})^2-k_{prv}^{S2}l_{S2}^2, \forall l_\epsilon>0$. *The optimal solution is*

$$\overline{l_{S1}^*}=\frac{k_T\pi R_{S1}}{k_T\pi+k_{prv}^{S1}}$$

and

$$\overline{l_{S2}^*}=\frac{k_T\pi R_{S2}}{k_T\pi+k_{prv}^{S2}}.$$

The proof of Theorem 5 is presented in Appendix D. R_{S1} and R_{S2} are the actual transmit radii of SU_1 and SU_2, respectively. The two conditions on R_{S1} and R_{S2} indicate that when the two SUs may interfere with each other, they are not allowed to transmit with full ATR as in Case I. The actual transmit region must be reduced to avoid interference.

With the SUs' predicted PPLs $(\overline{l_{S1}^*}, \overline{l_{S2}^*})$, the PU's optimal PPL can be calculated.

Theorem 6. *There exists an optimal solution* $(l_\epsilon^*, R_{S1}^*, R_{S2}^*)$ *to the following problem*

$$\text{argmax}_{R_{S1},R_{S2},l_\epsilon\in\boldsymbol{\mathcal{S}_P}} U_P$$

subject to $R_{S1}+R_{S2}\leqslant d_{12}$, $R_{S1}+r_P^0+l_\epsilon<d_{PS1}$, *and* $R_{S2}+r_P^0+l_\epsilon<d_{PS2}$, *where* $U_P=k_R^P\pi(r_P^0)^2+k_T\pi(R_{S1}-\overline{l_{S1}^*})^2+k_T\pi(R_{S2}-\overline{l_{S2}^*})^2-k_{lost}\pi(R_{S1}-l_\epsilon-\overline{l_{S1}^*})^2-k_{lost}\pi(R_{S2}-l_\epsilon-\overline{l_{S2}^*})^2-k_{prv}^P l_\epsilon^2$, $l_\epsilon>0$.

The solution can be obtained by applying the gradient descent method [41]. Here d_{12} is the distance between the two SUs as shown in Figure 4a. It can be calculated based on the law of cosines: $d_{12}=\sqrt{d_{PS1}^2+d_{PS2}^2-2d_{PS1}d_{PS2}\cos\vartheta}$, where ϑ is the angle formed between the line PU-SU_1 and the line PU-SU_2.

After receiving the PU's response, the SUs' best PPL (l_{S1}^*, l_{S2}^*) can be obtained by substituting R_{S1}^* and R_{S2}^* into the results presented in Theorem 5. Therefore, both parties reach the equilibrium $(l_\epsilon^*, l_{S1}^*, l_{S2}^*)$ of the Stackelberg game.

If the two users are very close to each other and their privacy-preserving ranges overlap, as shown in Figure 4b, the PU will allow only one SU to access the spectrum based on which SU can bring the PU higher payoffs.

According to the Stackelberg model, the predicted PPLs of the SUs are first calculated separately. In this circumstance, the determination of the SUs' anticipated PPLs is the same as in Case 1 describe by Theorem 3. The best PPLs $\overline{l_{S1}^*}$ and $\overline{l_{S2}^*}$ thereby can be obtained using the results provided in the theorem. With the information of the predicted PPLs of the SUs, the PU decides its optimal PPL and which SU to trade the spectrum with according to Theorem 7.

Theorem 7. *When* $0<k_{lost}<k_T<2k_{lost}$, *there exists an optimal PPL* l_ϵ^* *to the following problem*

$$\text{argmax}_{l_{\epsilon i}\in\boldsymbol{\mathcal{S}_P}} U_{PSi}$$

subject to $l_{\epsilon i}>0$, *where* $U_{PSi}=k_R^P\pi(r_P^0)^2+k_T\pi(d_{PSi}-r_P^0-l_{\epsilon i}-2\overline{l_{Si}^*})^2-k_{lost}\pi(d_{PSi}-r_P^0-2l_{\epsilon i}-2\overline{l_{Si}^*})^2-k_{prv}^P l_{\epsilon i}^2$, $(i=1,2)$ *and* $\overline{l_{Si}^*}=f_i(l_{\epsilon i})$. *The optimal solution is*

$$l_\epsilon^*=\{l_{\epsilon i}^*|\max\{U_{PSi},\, i=1,2\}\},$$

where $l_{\epsilon i}^*=\frac{[k_{lost}\pi(2-2\xi_i)(1-2\xi_i)-k_T\pi(1-2\xi_i)^2](d_{PSi}-r_P^0)}{k_{lost}\pi(2-2\xi_i)^2+k_{prv}^P-k_T\pi(1-2\xi_i)^2}$ *with* $\xi_i=\frac{2k_T\pi-k_R^{Si}\pi}{4k_T\pi+k_{prv}^{Si}-k_R^{Si}\pi}$.

The proof of Theorem 7 is similar to that of Theorem 2. U_{PSi} and $l_{\epsilon i}$ are the PU's utility and PPL when it shares its spectrum with SU_i, $i=1,2$. After deciding which SU is selected to trade the spectrum with and the corresponding optimal PPL l_ϵ^*, the PU will notify the two users of the decision. The SU that is allowed to transmit then sets its best strategy as $l_{Si}^*=\frac{(2k_T\pi-k_R^{Si}\pi)(d_{PSi}-r_P^0-l_\epsilon^*)}{4k_T\pi+k_{prv}^{Si}-k_R^{Si}\pi}$, $i=1$ or 2. Now the PU and the selected SU reach the SPNE (l_ϵ^*, l_{Si}^*).

Note that although the multi-user case is generalized from the single-PU-single-SU case, the results obtained for the latter cannot be simply degenerated from the former. For example,

the utility models of the PU in these cases are quite different; therefore, the PU privacy level in the single-PU-single-SU case has to be recalculated rather than being directly degenerated from the results in the multi-user case.

VII. Simulation Results

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

A. Simulation Setup

To produce the sanitized location of the SU, (r, θ) is first generated based on the density functions in (5) and (6). Note that r and θ can be generated separately as they are independent. The marginal PDF of θ is a constant value $\frac{1}{2\pi}$, so θ can be produced from a uniform distribution on the interval $[0, 2\pi]$. To generate r, its cumulative density function (CDF) needs to be specified:

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

Accordingly, a random number b is first generated from a uniform distribution on the interval [0, 1]. Then r is produced as

$$r = C^{-1}(b)$$

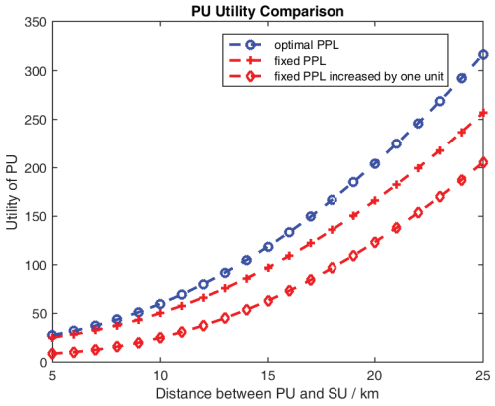
with the Lambert W function, i.e., the W_{-1} branch of the inverse of function $f(x) = xe^x$. Given an SU's accurate location $\boldsymbol{z} = (x, y)$, its sanitized location can be produced as $\boldsymbol{z'} = (x + r\cos\theta, y + r\sin\theta)$.

In the simulation, the distance unit is kilometer (km). The PU's actual exclusive zone 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 $k_{prv}^P = 1$. In the single-PU-single-SU case, 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. In the multi-PU-multi-SU case, all SUs' parameters are set to be the same as in the single-PU-single-SU case.

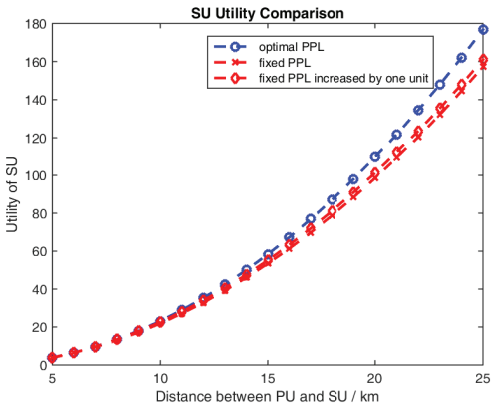
B. Performance Evaluation

To illustrate the superiority of the proposed approach, we compare our approach with the approach that the PUs and SUs choose predefined fixed PPLs to preserve their location information. The value of the fixed PPL is set as a fixed number that does not change as the distance between the PU and SU increases. Local search is used in the simulation to select fixed PPLs that result in better utilities to compare with the optimal PPL case. The performance of the proposed approach is evaluated from three aspects: 1) PUs' utility achievements are compared in different location settings where the relative distances between the PUs and SUs vary; 2) SUs' utility achievements are compared in different location settings; 3) with 15 PUs and 30 SUs randomly deployed in a certain region, the PUs' utility achievements with the optimal PPLs and predefined PPLs are compared.

In Figure 5, the user utilities with the optimal PPL and fixed PPLs in the single-PU-single-SU case are shown. Figure 5a gives the PU's utility comparison and demonstrates that



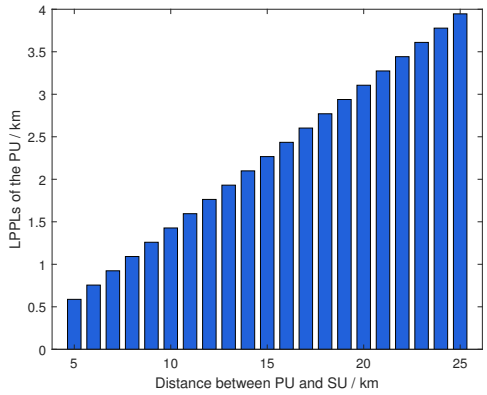
(a) PU utility comparison



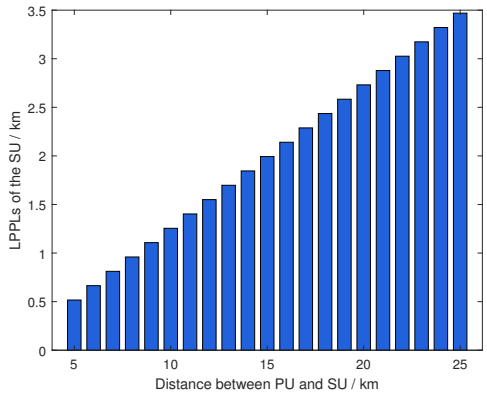
(b) SU utility comparison

Fig. 5: Performance comparison in the single-PU-single-SU case.

the PU with the optimal PPL can achieve significantly higher utility than the PU using a fixed PPL. And as the distance between the PU and SU becomes larger, the PU with the optimal PPL has a 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 between the PU with the optimal PPL and the PU using a fixed PPL is small. This is because when the SU is close to the PU, the ATR for the SU is small. As a result, the PU with either adjustable PPL or fixed PPL can only achieve a low utility. The utilities of the SU with different privacy preservation mechanisms are given in Figure 5b. As shown in the figure, the SU that follows the PU's strategy achieves much higher utility than the SU that maintains its fixed PPL after the PU decides its optimal strategy. 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, can be 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 5a. Due to the small ATR for the SU, neither mechanism can achieve a very

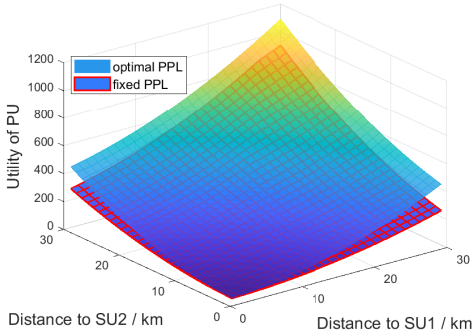


(a) PU's privacy level.

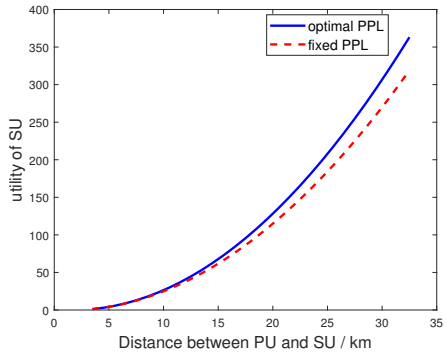


(b) SU's privacy level.

Fig. 6: Users' optimal privacy levels in the single-PU-single-SU case.



(a) PU utility comparison



(b) SU utility comparison

Fig. 7: Performance comparison in the single-PU-two-SU case when the two SUs do not interfere with each other.

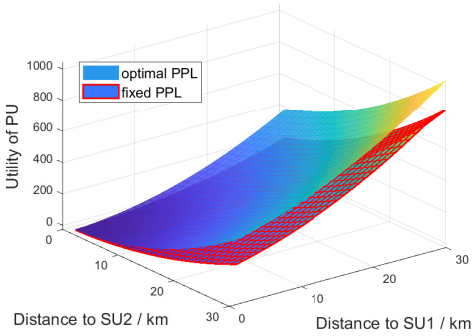
large utility. To show the influence of different fixed PPLs on user utilities, we also increase the fixed PPLs (baseline) by one unit for both the PU and SU. It can be seen that when the values of the fixed PPLs increase by one unit, the SU does not experience a significant change on the utility, while the utility of the PU adopting the fixed PPL declines significantly.

The optimal PPLs obtained for the PU and SU in different location settings are presented in Figure 6a and Figure 6b, respectively. It can be seen that the optional PPL is around 10% of the distance between the PU and SU, neither too small nor too large, satisfying the condition on the obtained privacy level discussed at the beginning of Section V-B. As the distance between the PU and SU becomes further, the allowable maximum obfuscation lengths for both parties become larger, which indicates that the users can protect their locations within a broader range. Combined with the results in Figure 5a and Figure 5b, this PPL increase will not cause utility decline, since the ATR also grows as the SU is further from the PU.

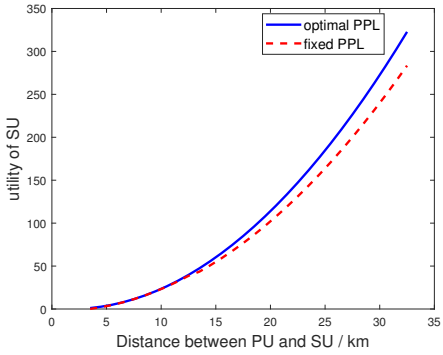
In Figure 7, the user utilities based on the proposed approach and the baseline are compared in the single-PU-two-SU case, where the SUs can transmit with full ATR and do not interfere with each other, corresponding to the theoretical analysis given by Case 1 in Section VI. Figure 7a displays the PU's utilities with the x-axis representing the distance between the PU and SU_1, and y-axis representing the distance between the PU and SU_2. It is obvious that the PU with the optimal PPL has significantly higher utilities over the PU with a fixed PPL. Figure 7b displays the SUs' utilities. In the single-PU-two-SU case where both SUs can access the spectrum, the SUs play equivalent roles, and the results are similar to those presented in Figure 5b. It can be seen that the SUs following the PU's strategy and choosing the optimal PPL achieve obviously higher utilities than the SUs using fixed PPLs. Note that the curves start from the distance of 3 km. This is because when the SUs are very close to the PU, they can be in the PU's exclusive zone and not allowed to transmit.

The utility comparison results when the SUs are relatively close to each other and cannot transit with full ATR are shown in Figure 8, corresponding to the theoretical analysis in the first circumstance of Case 2 in Section VI. The results indicate that the users, including both the PU and SUs, adopting the proposed privacy preservation mechanism can achieve higher utilities than the users using fixed PPLs. It should be noted that in this case, both the PU's and SUs' utilities are lower than those shown in Figure 7. This is because the SUs' actual ATR is reduced in this case to avoid possible interference with each other. As a result, the PU's trading payoffs and the SUs' service rewards decrease.

When the two SUs requesting for the same channel are too close to each other, only one SU is allowed to transmit and

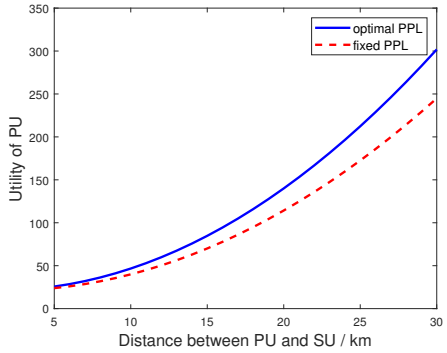


(a) PU utility comparison

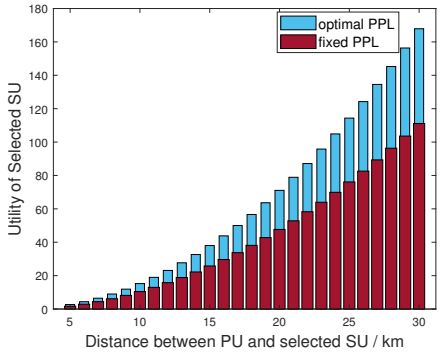


(b) SU utility comparison

Fig. 8: Performance comparison in the single-PU-two-SU case when both SUs transmit with ATR reduction.



(a) PU utility comparison



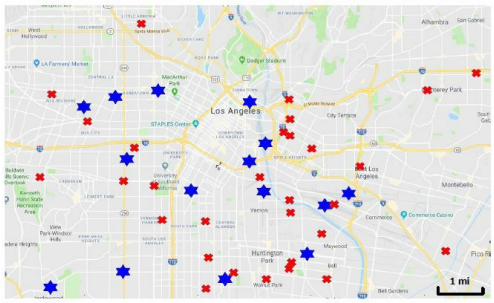
(b) SU utility comparison

Fig. 9: Performance comparison in the single-PU-two-SU case when only one SU is allowed to transmit.

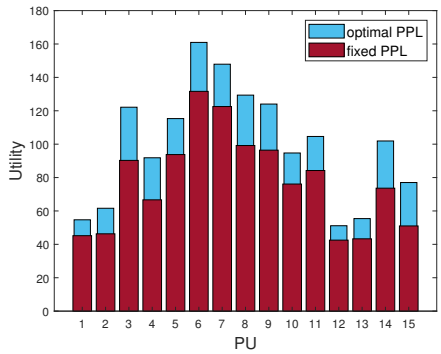
the utility comparison results in this case are shown in Figure 9, corresponding to the theoretical analysis in the second circumstance of Case 2 in Section VI. Figure 9a gives the PU's utility comparison. It can be seen that the PU using the proposed mechanism to adjust its PPL in the query process achieves a higher utility than the PU utilizing a fixed PPL. Figure 9b gives the bar plot of the utility of the selected SU, i.e., the SU permitted by the PU to access the desired channel. It is obvious that the SU adopting the proposed privacy preservation mechanism achieves a higher utility than the SU using a predefined PPL.

In Figure 10a, a more practical scenario is depicted, where 15 PUs and 30 SUs are randomly deployed in an area of Los Angeles, with the hexagrams representing the PUs and the crosses representing the SUs. Figure 10b gives each PU's utility in the proposed privacy preservation mechanism and the baseline. The comparison shows that the proposed mechanism results in a higher utility in comparison with the baseline for all the PUs.

A direct comparison with [14], [36] is difficult because (a) the system models and settings are different, (b) the privacy levels of the PUs and SUs are measured in different ways, and (c) some of the parameters used in the utility models of [14] and [36] are unavailable. However, we make a best-effort comparison of the user utility enhancement in percentage shown in Figure 11 between our work and [14], [36] where the PU's utility is based on Fig. 14b in [36] and the SU's

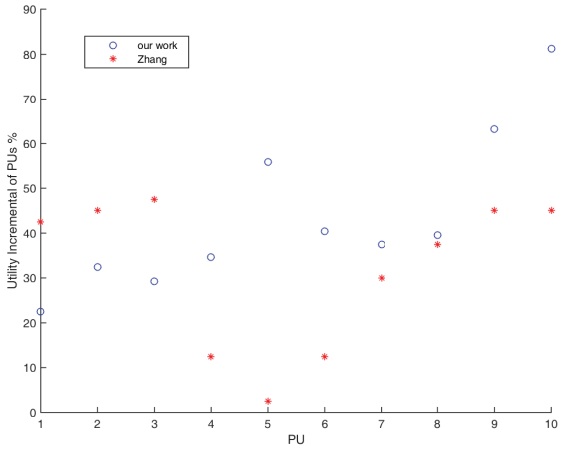


(a) Topology of a real-world scenario

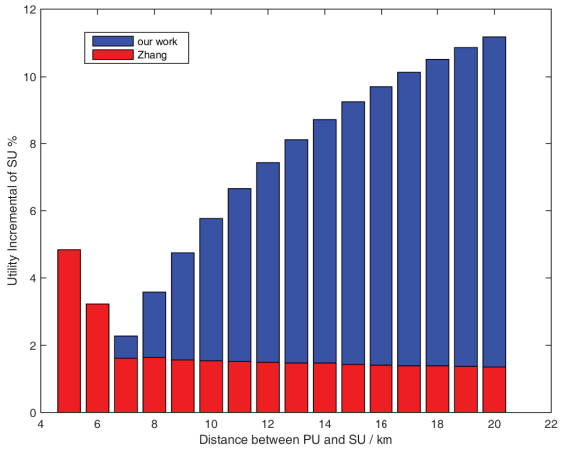


(b) Utility of each PU

Fig. 10: PU utility comparison with random deployment.



(a) PU utility enhancement comparison



(b) SU utility enhancement comparison

Fig. 11: User utility enhancement comparison.

utility is obtained in the case where SU follows to choose the optimal PPL. Figure 11a provides the utility enhancement comparison of 10 PUs in the multi-PU-multi-SU case. It can be seen that the majority of the PUs enjoy a higher utility enhancement with our method, and a PU even experiences an 85% increase in its utility. Figure 11b gives the utility enhancement comparison of the SU in the single-PU-single-SU case. It can be seen that when the distance between the PU and SU is short, below 6 km, the method in [14] and [36] helps the SU achieve more utility enhancement. However, when the distance between the PU and SU exceeds 6 km, the SU in our method achieves much better utility enhancement. Furthermore, as the distance increases, the utility enhancement achieved with our method grows significantly, while the utility enhancement suffers a slight decrease with the method in [14] and [36]. Therefore, both parties experience higher utility enhancements with our method.

VIII. Conclusions

In this paper, a novel bilateral location privacy preservation mechanism for users participating in spectrum sharing is proposed. With this privacy preservation mechanism, PUs and SUs can flexibly adjust their privacy preservation to optimal levels such that their utilities are maximized and their location information is protected within desired ranges. Furthermore, users' privacy costs are built in as part of their utility models in the proposed mechanism. In this way, the influence of privacy preservation to the overall utilities is quantified. As a result, the decision maker can effectively control the privacy cost by adjusting the PPL in practice. Simulation results demonstrate the effectiveness of the proposed approach.

Appendix A
Proof of Theorem 1

Proof: Given $\forall l_\epsilon > 0$, taking the second-order derivative of U_S in (19) 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 the l_S that yields the global maximum is the optimal solution.

Taking the first-order derivative of U_S in (19), we have

$$\begin{aligned}\frac{\partial U_S}{\partial l_S} &= \frac{\partial}{\partial l_S}\{k_R^S\pi(d_{PS} - r_P^0 - l_\epsilon - l_S)^2 \\ &- k_T\pi(d_{PS} - r_P^0 - l_\epsilon - 2l_S)^2 - k_{prv}^S l_S^2\} \\ &= -2k_R^S\pi(d_{PS} - r_P^0 - l_\epsilon - l_S) \\ &+ 4k_T\pi(d_{PS} - r_P^0 - l_\epsilon - 2l_S) - 2k_{prv}^S l_S.\end{aligned}$$

Let $\frac{\partial U_S}{\partial l_S} = 0$. $\overline{l_S^*}$ can be obtained. ■

Appendix B
Proof of Theorem 2

Proof: Given the SU's best reaction $\overline{l_S^*}$ expressed as a function of the PU's PPL l_ϵ in Theorem 1, the PU's utility function in (17) becomes

$$\begin{aligned}U_P &= k_R^P\pi(r_P^0)^2 + k_T\pi\left(d_{PS} - r_P^0 - l_\epsilon\right. \\ &- \left. 2\frac{(2k_T\pi - k_R^S\pi)(d_{PS} - r_P^0 - l_\epsilon)}{4k_T\pi + k_{prv}^S - k_R^S\pi}\right)^2 \\ &- k_{lost}\pi\left(d_{PS} - r_P^0 - 2l_\epsilon\right. \\ &- \left. 2\frac{(2k_T\pi - k_R^S\pi)(d_{PS} - r_P^0 - l_\epsilon)}{4k_T\pi + k_{prv}^S - k_R^S\pi}\right)^2 - k_{prv}^P l_\epsilon^2.\end{aligned}$$

Taking the second-order derivative with respect to l_ϵ yields

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

It can be easily shown that $\frac{\partial^2 U_P}{\partial l_\epsilon^2}$ is a constant and negative on the interval $(0, \infty)$. As a result, U_P is a strictly concave

downward function, and has one and only one global maximum. Therefore, the value of l_ϵ achieving the maximum is the optimal PPL for the PU.

Taking the first derivative of U_P, we have

$$\begin{aligned}\frac{\partial U_P}{\partial l_\epsilon} &= -2k_T\pi(1-2\xi)^2(d_{PS}-r_P^0)+2k_T\pi(1-2\xi)^2 l_\epsilon \\ &+ 2k_{lost}\pi(1-2\xi)(2-2\xi)(d_{PS}-r_P^0) \\ &- 2k_{lost}\pi(2-2\xi)^2 l_\epsilon - 2k_{prv}^P l_\epsilon.\end{aligned}$$

Let $\frac{\partial U_P}{\partial l_\epsilon}=0$. l_ϵ^* can be obtained. ∎

Appendix C
Proof of Theorem 4

Proof: Provided the SUs' predicted best responses $(\overline{l_{S1}^*}, \overline{l_{S2}^*})$ in Theorem 3, the PU's utility function becomes

$$\begin{aligned}U_P &= k_R^P\pi(r_P^0)^2+k_T\pi[d_{PS1}-r_P^0-l_\epsilon-2\phi_1(d_{PS1}-r_P^0-l_\epsilon)]^2 \\ &+ k_T\pi[d_{PS2}-r_P^0-l_\epsilon-2\phi_2(d_{PS2}-r_P^0-l_\epsilon)]^2 \\ &- k_{lost}\pi[d_{PS1}-r_P^0-2l_\epsilon-2\phi_1(d_{PS1}-r_P^0-l_\epsilon)]^2 \\ &- k_{lost}\pi[d_{PS2}-r_P^0-2l_\epsilon-2\phi_2(d_{PS2}-r_P^0-l_\epsilon)]^2-k_{prv}^P l_\epsilon^2.\end{aligned}$$

Taking the second derivative of U_P with respect to l_ϵ yields

$$\begin{aligned}\frac{\partial^2 U_P}{\partial l_\epsilon^2} &= -2k_{lost}\pi[(\frac{4k_T\pi+2k_{prv}^{S1}}{4k_T\pi+k_{prv}^{S1}-k_R^{S1}\pi})^2 \\ &+ (\frac{4k_T\pi+2k_{prv}^{S2}}{4k_T\pi+k_{prv}^{S2}-k_R^{S2}\pi})^2]-2k_{prv}^P \\ &+ 2k_T\pi[(\frac{k_R^{S1}\pi+k_{prv}^{S1}}{4k_T\pi+k_{prv}^{S1}-k_R^{S1}\pi})^2+(\frac{k_R^{S2}\pi+k_{prv}^{S2}}{4k_T\pi+k_{prv}^{S2}-k_R^{S2}\pi})^2].\end{aligned}$$

It can be shown that $\frac{\partial^2 U_P}{\partial l_\epsilon^2}$ is negative on the interval $(0,\infty)$. Therefore, U_P is strictly concave on $(0,\infty)$ with one and only one global maximum, and the value of l_ϵ that achieves the maximum is the optimal PPL for the PU. Taking the first derivative of U_P, we have

$$\begin{aligned}\frac{\partial U_P}{\partial l_\epsilon} &= -2k_T\pi\Gamma_1(d_{PS1}-r_P^0)-2k_T\pi\Gamma_2(d_{PS2}-r_P^0) \\ &+ 2k_T\pi\Gamma_1 l_\epsilon+2k_T\pi\Gamma_2 l_\epsilon+2k_{lost}\pi\sqrt{\Gamma_1\Omega_1}(d_{PS1}-r_P^0) \\ &+ 2k_{lost}\pi\sqrt{\Gamma_2\Omega_2}(d_{PS2}-r_P^0)-2k_{lost}\pi\Omega_1 l_\epsilon \\ &- 2k_{lost}\pi\Omega_2 l_\epsilon-2k_{prv}^P l_\epsilon.\end{aligned}$$

Let $\frac{\partial U_P}{\partial l_\epsilon}=0$. l_ϵ^* can be obtained. ∎

Appendix D
Proof of Theorem 5

Proof: Taking the second derivative of U_{Si} with respect to l_{Si} (i =1, 2), we have

$$\frac{\partial^2 U_{Si}}{\partial l_{Si}^2} = -2k_T\pi - 2k_{prv}^{Si}.$$

Since $\frac{\partial^2 U_{Si}}{\partial l_{Si}^2}$ is a constant that is negative on the interval $(0,\infty)$, U_{Si} is strictly concave with one and only one global maximum. The l_{Si} that yields the maximum is the optimal solution.

By taking the first derivative $\frac{\partial U_{Si}}{\partial l_{Si}}$ and setting it to zero, we can obtain the results. ∎

References

[1] M. Liu, X. Zhou, and M. Sun, "A game-theoretic approach to achieving bilateral privacy-utility tradeoff in spectrum sharing," in *Proc. IEEE Global Commun. Conf.*, Dec. 2020, pp. 1–6.

[2] FCC 15-47, "Report and order and second further notice of proposed rulemaking," Apr. 2015.

[3] FCC 16-55, "Order on reconsideration and second report and order," Apr. 2016.

[4] C. Blackman, S. Forge, and R. Horvitz, "Liberating Europe's radio spectrum through shared access," *Info*, vol. 15, no. 2, pp. 91–101, 2013.

[5] S. Bhattarai, P. R. Vaka, and J. Park, "Thwarting location inference attacks in database-driven spectrum sharing," *IEEE Trans. Cogn. Commun. Netw.*, vol. 4, no. 2, pp. 314–327, Jun. 2018.

[6] 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.

[7] M. A. Clark and K. Psounis, "Trading utility for privacy in shared spectrum access systems," *IEEE/ACM Trans. Netw.*, vol. 26, no. 1, pp. 259–273, Feb. 2018.

[8] S. B. Wicker, "The loss of location privacy in the cellular age," *Communications of the ACM*, vol. 55, no. 8, pp. 60–68, 2012.

[9] X. Gong, X. Chen, K. Xing, D. Shin, M. Zhang, and J. Zhang, "From social group utility maximization to personalized location privacy in mobile networks," *IEEE/ACM Trans. Netw.*, vol. 25, no. 3, pp. 1703–1716, Jun. 2017.

[10] S. Farhang, Y. Hayel, and Q. Zhu, "PHY-layer location privacy-preserving access point selection mechanism in next-generation wireless networks," in *Proc. IEEE Conf. Commun. Netw. Security*, Sep. 2015, pp. 263–271.

[11] M. Grissa, A. A. Yavuz, and B. Hamdaoui, "When the hammer meets the nail: Multi-server PIR for database-driven CRN with location privacy assurance," in *Proc. IEEE Conf. Commun. Netw. Security*, Oct. 2017, pp. 1–9.

[12] Y. Li, L. Zhou, H. Zhu, and L. Sun, "Privacy-preserving location proof for securing large-scale database-driven cognitive radio networks," *IEEE Internet Things J.*, vol. 3, no. 4, pp. 563–571, Aug. 2016.

[13] M. M. E. A. Mahmoud and X. Shen, "A cloud-based scheme for protecting source-location privacy against hotspot-locating attack in wireless sensor networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 10, pp. 1805–1818, Oct. 2012.

[14] 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.

[15] 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.

[16] H. Kido, Y. Yanagisawa, and T. Satoh, "Protection of location privacy using dummies for location-based services," in *Proc. 21st Int. Conf. Data Eng. Workshops*, Apr. 2005, pp. 1248–1248.

[17] P. Shankar, V. Ganapathy, and L. Iftode, "Privately querying location-based services with SybilQuery," in *Proc. 11th Int. Conf. Ubiquitous Comput.*, 2009, pp. 31–40.

[18] B. Bamba, L. Liu, P. Pesti, and T. Wang, "Supporting anonymous location queries in mobile environments with privacygrid," in *Proc. 17th Int. Conf World Wide Web*, Apr. 2008, pp. 237–246.

[19] M. Duckham and L. Kulik, "A formal model of obfuscation and negotiation for location privacy," in *Proc. 3rd Int. Conf. Pervasive Comput.*, 2005, pp. 152–170.

[20] M. Xue, P. Kalnis, and H. K. Pung, "Location diversity: Enhanced privacy protection in location based services," in *Proc. 4th Int. Symp. Location Context Awareness*, vol. 5561, 2009, pp. 70–87.

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

[22] A. Machanavajjhala, D. Kifer, J. Abowd, J. Gehrke, and L. Vilhuber, "Privacy: Theory meets practice on the map," in *Proc. 24th IEEE Int. Conf. Data Eng.*, Apr. 2008, pp. 277–286.

[23] S.-S. Ho and S. Ruan, "Differential privacy for location pattern mining," in *Proc. ACM SIGSPATIAL Int. Workshop Security Privacy GIS LBS*, 2011, pp. 17–24.

[24] A. Khoshgozaran and C. Shahabi, "Blind evaluation of nearest neighbor queries using space transformation to preserve location privacy," in *Proc. 10th Int. Conf. Advances Spatial Temporal Databases*, 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 *Proc. ACM SIGMOD Int. Conf Management of Data*, 2008, pp. 121–132.

[26] 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.

[27] 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.

[28] M. Clark and K. Psounis, "Can the privacy of primary networks in shared spectrum be protected?" in *Proc. IEEE INFOCOM*, Apr. 2016, pp. 1–9.

[29] 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.

[30] X. Jin and Y. Zhang, "Privacy-preserving crowdsourced spectrum sensing," *IEEE/ACM Trans. Netw.,*, vol. 26, no. 3, pp. 1236–1249, Jun. 2018.

[31] 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.

[32] ——, "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.

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

[34] M. Clark and K. Psounis, "Achievable privacy-performance tradeoffs for spectrum sharing with a sensing infrastructure," in *Proc. 14th Annu. Conf. Wireless On-Demand Netw. Syst. Services*, Feb. 2018, pp. 103–110.

[35] Y. Jian, S. Chen, Z. Zhang, and L. Zhang, "A novel scheme for protecting receiver's location privacy in wireless sensor networks," *IEEE Trans. Wireless Commun.*, vol. 7, no. 10, pp. 3769–3779, Oct. 2008.

[36] 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.

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

[38] 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.

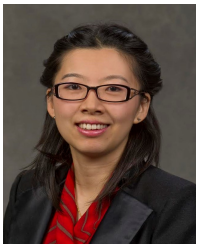
[39] ——, "Additional aspects of the Stackelberg strategy in nonzero-sum games," *J. Optimiz. Theory Appl.*, vol. 11, no. 6, pp. 613–626, 1973.

[40] T. Nakamura, "One-leader and multiple-follower Stackelberg games with private information," *Econ. Lett.*, vol. 127, pp. 27–30, 2015.

[41] S. Boyd and L. Vandenberghe, *Convex Optimization*.Cambridge, UK: Cambridge Univ. Press, 2004.

Mengmeng Liu received the B.Eng. degree and the Ph.D. degree from Harbin Engineering University, Harbin, China, in 2011 and 2017, respectively. She is now pursuing the Ph.D. degree in Electrical and Computer Engineering, Louisiana State University, Baton Rouge, LA, USA. Her research interests include statistical signal processing, statistical inference, and information fusion.

Xiangwei Zhou received the B.S. degree in communication engineering from Nanjing University of Science and Technology, Nanjing, China, the M.S. degree in information and communication engineering from Zhejiang University, Hangzhou, China, and the Ph.D. degree in electrical and computer engineering from Georgia Institute of Technology, Atlanta, GA, USA, in 2005, 2007, and 2011, respectively. He is an Associate Professor with the Division of Electrical and Computer Engineering, Louisiana State University, Baton Rouge, LA, USA. His research interests include wireless communications and statistical signal processing, with current emphasis on coexistence of wireless systems, Internet of Things, and machine learning for intelligent communications. He was the recipient of the Best Paper Award at the 2014 International Conference on Wireless Communications and Signal Processing and served as an Editor for the IEEE Transactions on Wireless Communications from 2013 to 2018.



Mingxuan Sun received the B.S. degree in computer science and engineering from Zhejiang University, Hangzhou, China in 2004, the M.S. degree in computer science from University of Kentucky, Lexington, KY, USA in 2006, and the Ph.D. degree in computer science from Georgia Institute of Technology, Atlanta, GA, USA in 2012. Since August 2015, she has been an Assistant Professor with the Division of Computer Science and Engineering, Louisiana State University, Baton Rouge, LA, USA. Prior to that, she was a Senior Scientist with Pandora Media, Inc., Oakland, CA, USA, from 2012 to 2015. Her research interests include machine learning, information retrieval, and data mining. She is also interested in machine learning and AI applications in social informatics, security, and wireless communications. She has published research papers in leading journals and conferences including PAMI, JMLR, NIPS, AAAI, AISTATS, KDD, ICDM, WWW, WSDM, etc.