This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2017.2781248, IEEE Transactions on Dependable and Secure Computing



# Bilateral Privacy-preserving Utility Maximization Protocol in Database-driven Cognitive Radio Networks

Zhikun Zhang, *Student member, IEEE,* Heng Zhang, *Member, IEEE,* Shibo He, *Member, IEEE,* and Peng Cheng, *Member, IEEE*

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

**Index Terms**—Location privacy, bilateral privacy preservation, cognitive radio networks.

## 1 Introduction

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

Cognitive radio networks have a wide spectrum of potential applications including smart grid networks, public safety networks, medical body area networks, etc [4]. Let's take medical body area networks (MBAN) as an example, MBAN is a promising way to allow body sensors to reliably and inexpensively collect the vital signs of patients and relay the monitoring information to clinicians for rapid diagnosing. Quality of service is a key requirement for MBAN, which requires clean and less crowded spectrum. However, the 2.4 GHz industrial, scientific and medical band is too crowded to support the life-critical medical applications. By using some PUs' vacant band on a *secondary basis*, i.e., acting as an SU, quality of service for MBAN can be better guaranteed [4]–[7].

- *Z. Zhang, S. He (Corresponding author) and P. Cheng are with State Key Laboratory of Industrial Control Technology, Zhejiang University, and Cyber Innovation Joint Research Center, Hangzhou, China. E-mail: zhangzhk@zju.edu.cn, s18he@zju.edu.cn, pcheng@iipc.zju.edu.cn*
- *H. Zhang is with Huaihai Institute of Technology, Lianyungang, China, is also with School of Computing, Engineering and Mathematics, Western Sydney University, Sydney, NSW, Australia E-mail: ezhangheng@gmail.com*

To enable dynamic channel access, SUs should be aware of which channels are locally available for reuse. There are mainly two ways for achieving this: 1) spectrum sensing and 2) database querying. Spectrum sensing method requires SUs to be equipped with specific sensors to detect the locally available channels [8]–[12]. Interference may occur when the sensors output false results, which may be caused by obstruction or channel fading. Database querying method requires SUs to provide their accurate locations to a centralized database [13]–[15]. In such a way, SUs can facilely figure out locally available channels and thus avoid interference by querying a database, which maintains an up-to-date spectrum availability repository.

Despite the huge advantage of database-driven cognitive radio networks, SUs' locations are exposed to enable efficient channel allocation, which may breach SUs' location privacy. For example, in the MBAN application, the location privacy of patients will inevitably be breached. Besides, the response from database contains information relevant to the distance between PUs and a queried SU, a malicious SU may infer PUs' locations through seemingly innocuous multiple database queries. The potential privacy breach risk of both PUs and SUs have been an obstacle to promote database-driven cognitive radio networks.

Previous studies mainly focus on unilateral location privacy preservation in database-driven cognitive radio networks, i.e., they assume that one party (PUs or SUs) is trustworthy and try to preserve the other's privacy [16], [17]. Furthermore, they fail to quantify the privacy preserving levels (PPLs) of PUs and SUs, making it difficult to analyze the tradeoff between both parties' PPLs and utilities. As aforementioned, both PUs' and SUs' location privacy could be potentially breached and thus should be preserved simultaneously. Simply applying previous mechanisms to

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2017.2781248, IEEE Transactions on Dependable and Secure Computing



preserve the privacy of PUs and SUs separately will suffer severe utility loss for both parties. As rational users, both parties intend to maximize their PPLs to efficiently thwart the attacker's threat. However, PPL and utility are always a paradox, in the sense that the increase of PPL will inevitably decrease SUs' available spectrum. Therefore, the bilateral location privacy issue should be jointly addressed, in which PUs and SUs can adjust their PPLs in order to maximize their utilities.

To address the above challenging issues, we first adopt the celebrated notion of differential privacy [18] to simultaneously preserve PUs' and SUs' privacy. Then, we design a quantitative privacy-preserving framework which is flexible for both PUs and SUs to adjust their PPLs. With this framework, we proceed to propose a novel privacy preserving Utility Maximization protocol (UMax) that allows both PUs and SUs to adjust their PPLs to achieve their maximum utilities. In UMax, PUs and SUs exchange information to decide their optimal PPLs. Firstly, SUs decide their optimal PPLs according to their utility function, which incorporate SUs' revenue and privacy lost. At the query epoch, SUs send their interested channels and expected transmit radius to database together with obfuscated locations generated based on their optimal PPLs. Secondly, based on SUs' expected information, the database decides PUs' optimal PPLs and SUs' available transmit power to maximize PUs' utilities.

The main contributions of this paper are summarized as follows:

1) To the best of our knowledge, this is the first work that simultaneously considers location privacy preservation for both PUs and SUs. Drawing on the concept of differential privacy, a quantitative framework is proposed to simultaneously preserve both PUs' and SUs' location privacy.
2) Based on the quantitative framework, we propose a novel database access protocol UMax, which allows both PUs and SUs to adjust their PPLs to maximize their utilities. We further prove the existence of optimal PPLs for both PUs and SUs.
3) We further generalize UMax protocol to the scenario where there are multiple PUs and multiple SUs with complex relative location combinations and allocation strategies.

The rest of this paper is organized as follows. Section 2 reviews the related work. Section 3 introduces the basic database access protocol and threat model. In Section 4, we propose novel location privacy-preserving mechanisms for both PUs and SUs. In Section 5, considering the single PU and single SU situation, we develop a new database access protocol that adjusts PU's and SU's PPL to improve their utility, respectively. Then we extend the proposed protocol to the multiple PUs multiple SUs situation in Section 6. Extensive simulations are performed in Section 7 to demonstrate the performance of the proposed protocol. Finally, Section 8 concludes this paper.

The notations that will be used in this paper are summarized in Table 1.

TABLE 1: Notations

| | |
|---|---|
| $r_{p,i}^0$ | $PU_i$'s protected contour radius |
| $r_{p,i}^\epsilon$ | Length added to $PU_i$'s protected contour radius |
| $L_{p,i}$ | $PU_i$'s PPL, i.e., $E(r_{p,i}^\epsilon)$ |
| $T_{p,i}$ | $PU_i$'s revenue |
| $C_{p,i}^{pri}$ | $PU_i$'s privacy cost |
| $loc_j$ | $SU_j$'s accurate location |
| $loc_j'$ | $SU_j$'s randomized location |
| $r_{s,j}^0$ | $SU_j$'s required transmit radius |
| $R_j$ | $SU_j$'s maximum transmit radius |
| $P_j$ | $SU_j$'s maximum transmit power |
| $r_{s,j}^\epsilon$ | $SU_j$'s privacy-preserving circle radius |
| $L_{s,j}$ | $SU_j$'s PPL, i.e., $r_{s,j}^\epsilon$ |
| $T_{s,j}$ | $SU_j$'s revenue |
| $C_{s,j}^{pri}$ | $SU_i$'s privacy cost |
| $C_{s,j}^{buy}$ | $SU_i$'s cost to buy spectrum |

## 2 Related Work

Most previous studies on cognitive radio focus on the performance improvements of spectrum sensing [19]–[22] or security issues [23], [24], whereas privacy issues are not well been studied, especially in the area of database driven cognitive radio. Although there are little works concern about privacy preservation in cognitive radio, plenty of privacy enhancing techniques are studied in other applications, which provide us useful reference on the design of privacy preserving technique for cognitive radio networks. We can classify the state-of-the-art privacy enhancing techniques into three categories: anonymization technique, cryptographic technique and differential privacy.

K-anonymity is the most widely used anonymization technique. One approach to achieve $k$-anonymity is to use *dummy locations* [25]. This technique properly selects $k-1$ dummy points, and then performs $k$ queries to database together with the real location. Another efficient method is *cloaking* [26], [27], which creates a dummy region that involves $k$ different points sharing the same property, and then queries the database with the dummy region. $l$-diversity [28] and $t$-closeness [29] are two anonymization techniques proposed to address the weaknesses of $k$-anonymity when homogeneity exists in the sensitive values in a group. However, the intrinsic drawback of $k$-anonymity is that a mechanism is difficult to be proved to satisfy this notion, since the attacker's auxiliary information may violate the guarantee of $k$-anonymity. In addition, $k$-anonymity based approaches are difficult to quantify the privacy preserving level.

Cryptography is another location privacy-preserving technique, which has been widely used [30]–[32]. This technique transforms all the data in a query process to a different space. The query result can be mapped back to spatial information only by the user. However, the computational overhead of cryptography based technique is too high.

The notion of differential privacy [18] comes from the area of statistical database. Its goal is to preserve individual's privacy while achieving good statistical accuracy. Recently, Andres et. al. [33] proposed the $\epsilon$-geo-indistinguishability mechanism, which generalized the notion of differential privacy to location based service. The main advantage of differential privacy is that the privacy

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2017.2781248, IEEE Transactions on Dependable and Secure Computing



guarantee is independent of attacker's auxiliary information, i.e., the mechanism has no need to update when new types of attack emerges. More importantly, differential privacy provides a solid mathematical definition which is convenient to quantify the privacy preserving level [34], [35]. Due to the advantage of differential privacy, we adopt the notion of differential privacy to preserve the location privacy for both PUs and SUs.

The existing works on the location privacy in database-driven cognitive radio concern only about unilateral privacy preservation. In [16], Gao et al. proposed a cryptography based location privacy-preserving protocol called PSAIR for SUs. PSAIR allows for SUs to access the locally available channels and preserve location privacy simultaneously. Bahrak et al. [17] pointed out that a malicious SU can infer PU's location through seemingly innocuous database queries. Then they proposed a $k$-anonymity based mechanism to preserve PU's privacy. To the best of our knowledge, there is no existing work that addresses the bilateral privacy preservation for PUs and SUs simultaneously.

## 3 Background and Threat Model

In this section, we first introduce the basic database access protocol that do not consider the privacy issues. Then, we present the threat model for the basic database access protocol as well as the problems to be addressed in this paper.

### 3.1 Basic Database Access Protocol

A typical database-driven cognitive radio network comprises three main components: PUs, SUs and spectrum management database. The database maintains PUs' locations and spectrum utilization informations. Whenever PUs change their spectrum utilization informations, they will notify database to update the repository.

We assume there are $M$ PUs and $N$ SUs in the network, which are denoted by $PU_i$ and $SU_j$, respectively. Each $PU_i$ owns a specific channel $ch_i$[1], which has two states, i.e., occupied or vacant. When $ch_i$ is occupied, $PU_i$ will delimit a protected contour where no SUs can transmit, and if an SU is beyond $PU_i$'s protected contour, it is allowed to transmit with a certain power. Intuitively, the farther an SU is located from $PU_i$, the larger power it can transmit. When $ch_i$ is vacant, it can be accessed by SUs freely.

A basic database access protocol without considering the privacy issues is shown in Fig. 1. The database query process is conducted in the beginning of each time slot, within which the channel access state do not change. At the beginning of each time slot, SUs send their queries $Q = (loc_j, ch_i)$ to the database, where $loc_j = (x_j, y_j)$ is the accurate location of $SU_j$, and $ch_i$ is the channel with the best quality for $SU_j$. Then, the database returns $R = P_j$ to $SU_j$, where $P_j$ is the maximum transmission power (MTP) for $SU_j$ when it access $ch_i$. The MTP can be calculated by the following function [17]:

$$P_j = \begin{cases} 0, & d_{ij} \le r^0_{p,i}, \\ h(d_{ij} - r^0_{p,i}), & d_{ij} > r^0_{p,i}, \end{cases} \quad (1)$$

1. We will use $PU_i$ and $ch_i$ interchangeably in the following part.

where $r^0_{p,i}$ is the protected contour radius of $ch_i$, $d_{ij}$ is the distance between $SU_j$ and $PU_i$, and $h(\cdot)$ is a continuous monotone increasing function.

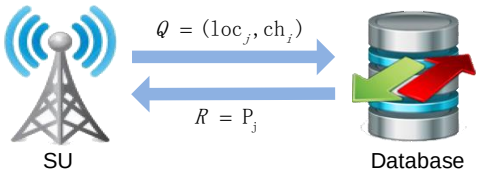



Fig. 1: Basic database access protocol.

### 3.2 Threat Model and Assumptions

In the basic database access protocol, both database and SUs are assumed to be trustworthy. However, this assumption may not always guaranteed in reality. The reason is that a curious database manager may collect SUs' location information, which should be reported to the database to achieve the locally available channels, to make market decision or sales strategy. In another hand, a malicious SU may infer PUs' locations through multiple seemingly innocuous queries as depicted in Section 4.

We assume that the database is an affiliated entity of PUs, e.g., China Mobile would maintain a spectrum management database if it decides to share the registered spectrum with SUs. Thus, we further assume that PUs and database trust each other, and database will not breach PUs' operational information. Besides, we assume that a sophisticated malicious SU can obtain the MTP function which the database adopts [17].

### 3.3 Problem of Interest

To defend the potential privacy threat, both PUs and SUs need to adopt an quantitative mechanism to preserve their location privacy. However, unrestricted increase PPL may seriously decrease both PUs' and SUs' utility. Thus, we need to deal with the following two problems in our paper:

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

## 4 Quantitative Privacy-preserving Mechanism

In this section, we first introduce the quantitative privacy-preserving mechanisms for both PUs and SUs. Then, an interference free framework is proposed to facilitate the analysis of the bilateral privacy-preserving protocol.

### 4.1 Quantitative Privacy-preserving Mechanism for PUs

Firstly, we present the location privacy threat for PUs when they do not adopt any privacy-preserving mechanisms. In brief, a malicious SU can infer PU's location through multiple seemingly innocuous queries as Fig. 2(a) shows.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2017.2781248, IEEE Transactions on Dependable and Secure Computing



Specifically, one sophisticated malicious SU, which obtained the MTP function of database, can compute its maximum transmit radius, i.e., $d_1$, $d_2$, $d_3$ and $d_4$, in each query location. Thus, after multiple queries in different locations, the malicious SU can choose at least four query results, that contain available transmit power, to locate PU by solving the following equations set:

$$\begin{aligned}(x_1-x_p)^2+(y_1-y_p)^2&=(d_1+r_p^0)^2\\(x_2-x_p)^2+(y_2-y_p)^2&=(d_2+r_p^0)^2\\(x_3-x_p)^2+(y_3-y_p)^2&=(d_3+r_p^0)^2\\(x_4-x_p)^2+(y_4-y_p)^2&=(d_4+r_p^0)^2\end{aligned} \tag{2}$$

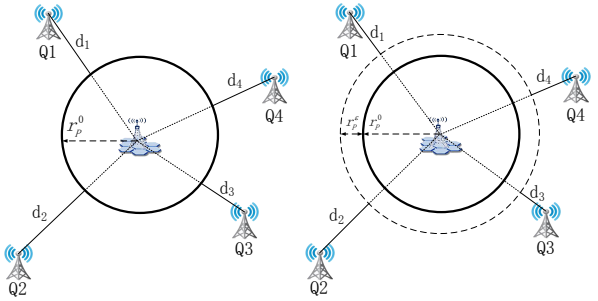
where $(x_i, y_i)$ is the location of $Q_i$, $(x_p, y_p)$ is the location of the PU to be inferred, $r_p^0$ is the protected contour radius of the PU. With the above equations set, the malicious SU can uniquely determine PU's accurate location $(x_p, y_p)$ and the corresponding protected contour radius $r_p^0$.

To thwart malicious SU's inference attack, we propose an obfuscation based mechanism as Fig. 2(b) shows. Before computing SUs' MTP, the database will add a random length to PUs' real protected contour radius, i.e., $r_p = r_p^0 + r_p^\epsilon$. With the randomized MTP, the $r_p^0$ term in equations set 2 is different, making the calculation of PU's accurate location $(x_p, y_p)$ difficult. In this paper, we adopt exponential distribution to generate the required random distance $r_p^\epsilon$. The corresponding probability density function is given by

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

where $b$ is the rate parameter. Notice that $r_p^\epsilon$ is always positive, since otherwise the obfuscated protected contour will be less than the required one which may cause interference.

Intuitively, larger noise means higher PPL, so that we can adopt the expectation of $r_p^\epsilon$, i.e., $E[r_p^\epsilon]$, to denote PU's PPL $L_p$[2].




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

Fig. 2: PU's location privacy threat and countermeasure. $Q_1$, $Q_2$ and $Q_3$ stand for three different query locations, $d_1$, $d_2$, $d_3$ and $d_4$ stand for their corresponding maximum transmit radius.

### 4.2 Quantitative Privacy-preserving Mechanism for SUs

Recall that SUs should report their accurate locations to achieve the locally available channels, leading to serious privacy breach threat. Therefore, drawing on the privacy-preserving mechanism in [33], we propose $l$-geo-indistinguishability ($l$-geoin) mechanism to preserve SUs' location privacy.

Informally, $l$-geoin allows for SUs to report randomized locations generated by certain distribution to the database. $l$-geoin guarantees that after receiving SUs' randomized locations, a curious database manager cannot figure out SUs' accurate locations with high confidence. The formal definition of $l$-geoin is given as follows:

**Definition 1.** *A privacy-preserving random mechanism satisfies $l$-geoin if and only if for a reported location $x$, we have*

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

where $r_s^\epsilon$ is the radius of the largest area where SU's privacy-preserving location may lie through the random mechanism, $x_0$ and $x_0'$ are two accurate locations of SU that may report $x$, $d(x_0, x_0')$ is the distance between $x_0$ and $x_0'$.

Definition 1 shows that whether SU's accurate location is $x_0$ or $x_0'$, the reported location can be $x$ with certain probability, and their probability difference is upper bounded by $e^l$ if the distance between $x_0$ and $x_0'$ is less than $r_s^\epsilon$. Notice that a larger $l$ means more difficult to infer SU's accurate location, leading to higher PPL.

In [33], the authors consider that for a given radius $r_s^\epsilon$, a smaller $\epsilon$ means higher PPL, they name it $\epsilon$-geo-indistinguishability ($\epsilon$-geoin) mechanism. From our perspective, given a certain $l$, we can adjust $\epsilon$ to achieve a larger $r_s^\epsilon$, every expected $r_s^\epsilon$ corresponds to an $\epsilon$. Thus, we can use $r_s^\epsilon$ to denote SU's PPL $L_s$[3], where a larger $r_s^\epsilon$ means that SU can obfuscate its location in a larger scale with $l$-geoin mechanism. By this notion, SU can choose its protected scale flexibly, rather than adjust its PPL in a fixed scale as $\epsilon$-geoin mechanism.

Andres et al. [33] proved that the two dimensional Laplacian distribution satisfies $\epsilon$-geoin, and thus satisfies $l$-geoin. The probability density function of two dimensional Laplacian distribution is given by

$$f(x|x_0)=\frac{\epsilon^2}{2\pi}e^{-\epsilon d(x_0,x)}, \tag{3}$$

where $x_0 \in \mathbb{R}^2$ is the accurate location of SU and $x \in \mathbb{R}^2$ is the corresponding randomized location, $d(x_0, x)$ is the distance between $x_0$ and $x$. Fig. 3 shows how this mechanism works. An SU located at $x_0$ can generate a randomized location $x$ within a circle with $r_s^\epsilon$ radius, i.e., the required PPL, from two dimensional Laplacian distribution.

### 4.3 Interference Free Framework

In this subsection, we propose an interference free framework to facilitate the decision procedure of database, as Fig. 4 shows.

2. We will use $E[r_p^\epsilon]$ and $L_p$ interchangably to denote PU's PPL.

3. We will use $r_s^\epsilon$ and $L_s$ interchangably to denote SU's PPL.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2017.2781248, IEEE Transactions on Dependable and Secure Computing



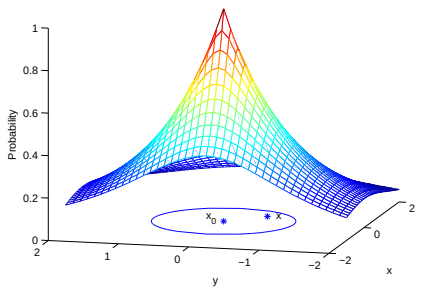



Fig. 3: SU located in $x_0$ generate randomized location $x$ with probability as shown in "Probability" axis.

We assume each SU has a required transmission radius $r_s^0$ based on its service requirement, and the database decide each SU's MTP based on its reported location and required transmit radius. In each query process, each SU would report a randomized location $x$ to the database to preserve its location privacy, such that a curious database manager cannot distinguish the SU's accurate location within a circle of radius $r_s^\epsilon$, as the inner solid circle shows in Fig. 4. From database's perspective, when allocating spectrum to SUs, all SUs' outer circles should not intersect with each other to avoid interference. The reason is that the furthest distance SU may transmit is the boundary of the outer solid circle, since the accurate location of SU maybe in the boundary of the inner solid circle, as $x_0^1$ and $x_0^2$ shows.

For brevity, we use **privacy preserving circle** and **interference free circle** to describe SUs' requirement in the following part, where privacy preserving circle and interference free circle correspond to the inner solid circle and outer solid circle in Fig. 4, respectively. Notice that, when any two SUs' privacy preserving circles intersect with each other, the possible location between the two SUs can be arbitrary close from database' perspective. Namely, no matter how much transmit radius we allocate to the two SUs, they may interfere with each other. Thus, only one SU is allowed to transmit.

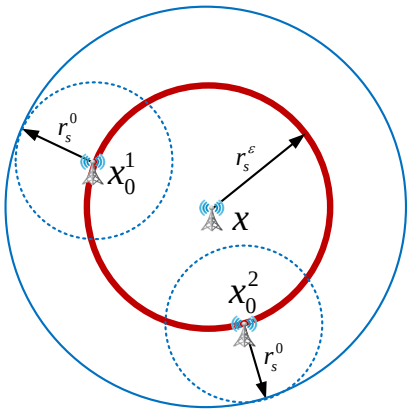



Fig. 4: Interference free framework. $x$ is SU's reported randomized location, $x_0^1$ and $x_0^2$ are two possible accurate location of the SU.

## 5 Privacy-preserving Database Access Protocol

In this section, we propose a new database access protocol UMax to allow for PUs and SUs to choose the optimal PPLs to achieve their maximum utilities. The single PU single SU situation is considered in this section, and we will generalize the proposed protocol to multiple PUs multiple SUs situation in Section 6.

We first provide an overview to the proposed UMax protocol in Section 5.1, then deeply study the optimal decision of SU and PU in Section 5.2 and Section 5.3.

### 5.1 Overview to UMax Protocol

In this subsection, we provide an overview to the proposed database access protocol UMax.

**Step 1: SU query the database with its optimal PPL:** SU with accurate location $(x, y)$ query the database with $Q = (ch_i, r_s^0, loc', r_s^\epsilon)$, where $ch_i$ is SU's interested channel, and $r_s^0$ is SU's expected transmit radius based on its service requirement. $loc' = (x', y')$ is a randomized location generated with the optimal PPL $r_s^\epsilon$, which can be calculated by solving the following optimization problem:

**Problem 5.1.**

$$\underset{L_s}{\text{argmax}}\ U_s(L_s) = T_s - C_s^{buy} - C_s^{pri},$$
$$s.t.\ L_s > 0.$$

In Problem 5.1, $U_s(L_s)$ is SU's utility function which consists of three parts: $T_s$ is SU's revenue by utilizing the spectrum, $C_s^{buy}$ is SU's payment to PU for utilizing the spectrum, and $C_s^{pri}$ is SU's privacy cost. Details of SU's optimal decision will be presented in Section 5.2.

**Step 2: Database decides SU's MTP based on the channel state:** When SU's interested channel is vacant, database calculates SU's MTP based on $r_s^0$. When the channel is occupied, database should first decide PU's optimal PPL then calculate SU's MTP. PU's optimal PPL can be calculated by solving the following optimization problem:

**Problem 5.2.**

$$\underset{L_p}{\text{argmax}}\ E[U_p(L_p)] = T_p - C_p^{pri},$$
$$s.t.\ L_p > 0.$$

In Problem 5.2, $E[U_p(L_p)]$ is PU's utility function in the expectation sense which consists of two parts: $T_p$ is PU's revenue by selling spectrum to SU which is equal to $C_s^{buy}$, and $C_p^{pri}$ is PU's privacy cost. Details of PU's optimal decision will be presented in Section 5.3.

Then, the database can generate a random distance $r_p^\epsilon$ based on the optimal PPL, i.e., $E[r_p^\epsilon]$. SU's maximum transmission radius (MTR)[4] is given by $R = d_{sp} - r_p^0 - r_p^\epsilon - r_s^\epsilon$ as Fig. 5 shows, where $d_sp$ is the distance between PU and SU.

4. Notice that SU's MTP is decided by its maximum transmission radius (MTR) so that we would use MTP and MTR interchangeably in the following part.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2017.2781248, IEEE Transactions on Dependable and Secure Computing



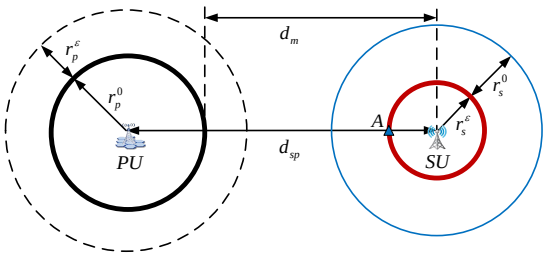



Fig. 5: Relative location between PU and SU.

### 5.2 SU's optimal decision

In this subsection, we elaborate the optimal decision of SU.

We define SU's revenue as

$$T_s = k_2\pi(r_s^0)^2, \tag{4}$$

where $k_2$ is SU's revenue of using unit area spectrum, and $r_s^0$ is SU's expected transmit radius.

As Fig. 4 shows, SU's expected transmit radius is $r_s^0$. It seems that PU should charge SU based on $r_s^0$. However, to satisfy SU's privacy-preserving requirement, PU need to allocate an area of radius $r_s^0 + r_s^\epsilon$ to avoid interference. To incentivize PU to share its spectrum, SU need to pay for the extra spectrum incurred by its privacy preserving requirement. Thus, we can define SU's payment as

$$C_s^{buy} = k_1\pi(r_s^\epsilon + r_s^0)^2,$$

where $k_1$ is the payment for using *unit area* spectrum. $\pi(r_s^\epsilon + r_s^0)^2$ is the area that PU allocate to SU for accessing a given spectrum. Since SU's PPL $L_s$ is equal to $r_s^\epsilon$, we can transform the above formula into the following form

$$C_s^{buy} = k_1\pi(L_s + r_s^0)^2. \tag{5}$$

The decrease of SU's PPL may increase its revenue with larger privacy breach risk. This kind of privacy breach risk is the cost which should be included into PU's utility function. Privacy cost can be defined as follows [36]

$$C_s^{pri} = \frac{k_s}{L_s}, \tag{6}$$

where $k_s$ is the privacy cost coefficient.

Combining (4), (5) and (6), we can rewrite Problem 5.1 as

**Problem 5.3.**

$$\begin{aligned}&\underset{L_s}{\text{argmax}}\ E[U_s] = k_2\pi(r_s^0)^2 - k_1\pi(L_s + r_s^0)^2 - \frac{k_s}{L_s},\\ &s.t.\ L_s > 0.\end{aligned}$$

Then, we show that Problem 5.3 has optimal solution and provide efficient method to achieve it.

**Theorem 5.1.** *There exists an optimal PPL for SU, i.e., $L_s^*$, to solve Problem 5.3.*

*Proof.* The second order derivative of $E[U_s]$ is given by

$$\frac{d^2E[U_s]}{dL_s^2} = -2k_1\pi - 2\frac{k_s}{L_s^3},$$

Notice that $\frac{d^2E[U_s]}{dL_s^2}$ is always less than zero, which means $E[U_s]$ is a concave function. In addition, the constraint of Problem 5.3 is convex. Thus, Problem 5.3 is a convex optimization problem, which have an optimal solution. □

Since Problem 5.3 is a convex optimization problem, we can solve it by existing convex solver such as gradient decent method [37].

### 5.3 PU's optimal decision

In this subsection, we elaborate the optimal decision of PU.

To avoid interference, SU's expected transmit radius $r_s^0$ may not be fully satisfied. To incentivize SU to reuse the vacant spectrum continuously, PU can reduce the unit price of spectrum to compensate expenses of SU. Thus, PU's revenue can be defined as

$$\begin{aligned}T_p &= \frac{R}{r_s^0}k_1\pi(r_s^\epsilon + R)^2\\ &= \frac{k_1\pi}{r_s^0}(d_m - L_p - r_s^\epsilon)(d_m - L_p)^2,\end{aligned} \tag{7}$$

where $R$ is SU's MTR, and $\frac{R}{r_s^0}$ stands for SU's satisfaction ratio.

Similar to the analysis of SU, we can define PU's privacy cost as follows

$$C_p^{pri} = \frac{k_p}{L_p} \tag{8}$$

Combining (7) and (8), we can rewrite PU's expected utility as

$$E[U_p] = \frac{k_1\pi}{r_s^0}(d_m - L_p - r_s^\epsilon)(d_m - L_p)^2 - \frac{k_p}{L_p}$$

The optimal value of $L_p$ lies in $[d_m - r_s^\epsilon - r_s^0, d_m - r_s^\epsilon]$ as Fig. 5 shows. The reason is that if $L_p \le d_m - r_s^\epsilon - r_s^0$, SU's expected transmit radius can always be satisfied. In this case, the revenue $T_p = k_1\pi(r_s^\epsilon + r_s^0)^2$ is a constant, we can always achieve better utility by extending $L_p$. In addition, if $L_p \ge d_m - r_s^\epsilon$, the database can not decide SU's MTR. Since arbitrary transmit radius may cause interference with PU when SU is located in point $A$ as Fig. 5 shows. Thus, Problem 5.2 becomes

**Problem 5.4.**

$$\begin{aligned}&\underset{L_p}{\text{argmax}}\ E[U_p] = \frac{k_1\pi}{r_s^0}(d_m - L_p - r_s^\epsilon)(d_m - L_p)^2 - \frac{k_p}{L_p},\\ &s.t.\ L_p > 0,\\ &\quad d_m - r_s^\epsilon - r_s^0 \le L_p \le d_m - r_s^\epsilon.\end{aligned}$$

Then, we show that Problem 5.4 has optimal solution and provide efficient method to achieve it.

**Theorem 5.2.** *There exists an optimal PPL for PU, i.e., $L_p^*$, to solve Problem 5.4.*

*Proof.* The first order derivative of $E[U_p]$ is given by

$$\begin{aligned}\frac{dE[U_p]}{dL_p} =& \frac{k_1\pi}{r_s^0}\Big[-3L_p^2 + (6d_m - 2r_s^\epsilon)L_p\\ &- 3d_m^2 + 2r_s^\epsilon d_m\Big] + \frac{k_p}{L_p^2}.\end{aligned}$$

Recall that the roots of equation $\frac{dE[U_p]}{dL_p} = 0$ is the stationary points of the objective function $E[U_p]$. Notice that $\frac{dE[U_p]}{dL_p} = 0$ is a *quartic equation* and have at most 4 real roots, such that $E[U_p]$ have at most 4 stationary points. Further, we observe that $E[U_p]$ is a continuous function, and the feasible region of Problem 5.4 lies in a closed interval

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2017.2781248, IEEE Transactions on Dependable and Secure Computing



$L_p \in [d_m - r_s^\epsilon - r_s^0, d_m - r_s^\epsilon]$. Thus, Problem 5.4 has an optimal solution in the interval $[d_m - r_s^\epsilon - r_s^0, d_m - r_s^\epsilon]$. □

To calculate the optimal PPL, we first calculate the real roots for equation $\frac{dE[U_p]}{dL_p} = 0$ with existing quartic equation solver [38], and calculate the value of $E[U_p]$ using the real roots and the boundary value, i.e., $d_m - r_s^\epsilon - r_s^0$ and $d_m - r_s^\epsilon$. Then, we compare all the calculated value of $E[U_p]$ to choose the optimal PPL. If there exist two $L_p$ at which $E[U_p]$ achieves the optimal value, we will choose the larger $L_p$ as the optimal PPL.

## 6 Multiple PUs Multiple SUs Situation

In this section, we generalize UMax to multiple PUs multiple SUs situation. Recall that different PUs occupy different channels so that PUs can allocate their spectrum separately. Thus, we can reduce the multiple PUs multiple SUs problem to the single PU multiple SUs problem. In addition, when the number of SUs that apply for the same channel are arbitrary, the relative location combinations and allocation strategies is infinite, which makes it difficult to analyze the general case. To start, we consider the situation where there are at most two SUs applying for the same channel.

In practice, we extend UMax as follows:

**Step 1:** SUs decides their optimal PPLs based on Problem 5.3, and query the database with $Q = (ch_i, loc'_j, r^0_{s,j}, r^\epsilon_{s,j})$, where $ch_i$ is $SU_j$'s interested channel, $loc'_j$ is the randomized location based on optimal PPL $r^\epsilon_{s,j}$, and $r^0_{s,j}$ is $SU_j$'s expected transmit radius.

**Step 2:** Database decide $PU_i$'s allocation strategy based on $ch_i$'s channel state. When $ch_i$ is vacant, database decide each SU's optimal transmit radius directly on the condition that SUs do not interfere with each other. And when $ch_i$ is occupied, database should first decide $PU_i$'s optimal PPL, and decide SU's optimal transmit radius on the condition that $PU_i$ do not interfere with all SUs.

In the following subsection, we will discuss PU's allocation strategy in different channel states.

### 6.1 The channel is vacant

We define $PU_i$'s revenue as $T_{p,i} = T^1_{p,i} + T^2_{p,i}$, and

$$T^1_{p,i} = \frac{R_1}{r^0_{s,1}} k_1 \pi (r^\epsilon_{s,1} + R_1)^2,$$
$$T^2_{p,i} = \frac{R_2}{r^0_{s,2}} k_1 \pi (r^\epsilon_{s,2} + R_2)^2,$$

where $T^1_{p,i}$ and $T^2_{p,i}$ are revenues from $SU_1$ and $SU_2$, respectively, $R_j (j = 1, 2)$ is $SU_j$'s MTR, $r^\epsilon_{s,j}$ is $SU_j$'s optimal PPL, and $r^0_{s,j}$ is $SU_j$'s expected transmit radius.

When there are two SUs applying for $ch_i$, we can decide SUs' MTR in the following three cases.

**Case 1: Interference free circles** do not intersect with each other, as Fig. 6 shows. In this case, both $SU_1$ and $SU_2$ can access the channel with its expected transmit radius.

**Case 2: Interference free circles** intersect with each other, as Fig. 7 shows. In this case, our goal is to maximize $PU_i$'s revenue

$$T_{p,i} = \frac{R_1}{r^0_{s,1}} k_1 \pi (r^\epsilon_{s,1} + R_1)^2 + \frac{R_2}{r^0_{s,2}} k_1 \pi (r^\epsilon_{s,2} + R_2)^2. \quad (9)$$

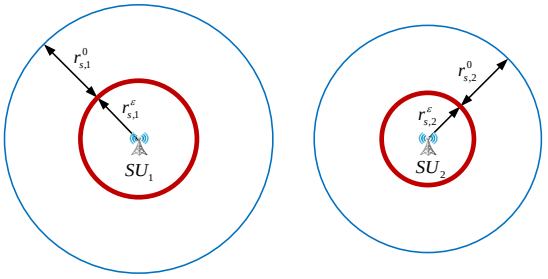



Fig. 6: Interference free circles do not intersect with each other.

Intuitively, we observe that $PU_i$ can achieve the maximum utility if and only if the interference free circles of both $SU_1$ and $SU_2$ are tangent with each other. The reason is that if there is an allocation strategy which the interference free circles are not tangent with each other, we can always find a better allocation strategy by expanding an arbitrary SU's interference free circle to achieve better utility. Thus, we have

$$R_2 = d_{12} - r^\epsilon_{s,1} - r^\epsilon_{s,2} - R_1,$$

Define $M = d_{12} - r^\epsilon_{s,1} - r^\epsilon_{s,2}$, $M$ is a constant. Thus, the best allocation strategy can be achieved by solving the following optimization problem:

**Problem 6.1.**

$$\begin{aligned} \underset{R_1}{\text{argmax}} \ T_{p,i} = & \frac{R_1}{r^0_{s,1}} k_1 \pi (r^\epsilon_{s,1} + R_1)^2 + \\ & \frac{M - R_1}{r^0_{s,2}} k_1 \pi (r^\epsilon_{s,2} + M - R_1)^2, \\ s.t. \quad & 0 \le R_1 \le r^0_{s,1}, \\ & M - r^0_{s,2} \le R_1 \le M, \end{aligned}$$

Then, we show that Problem 6.1 has optimal solution and provide efficient method to achieve it.

**Theorem 6.1.** *There exists an optimal PPL for SU $L^*_s$ to solve Problem 6.1.*

*Proof.* The second order derivative of $R_p$ is

$$\frac{d^2 T_{p,i}}{dT^2_{p,i}} = \frac{4 k_1 \pi}{r^0_{s,1}} (r^\epsilon_{s,1} + R_1) + \frac{2 k_1 \pi}{r^0_{s,2}} (M - R_1).$$

Since $\frac{d^2 T_{p,i}}{dT^2_{p,i}}$ is always larger than zero, so that $T_{p,i}$ is a convex function. In addition, the constraint of Problem 6.1 is convex. Therefore, Problem 6.1 is a convex optimization problem, which have an optimal solution. □

Since Problem 6.1 is a convex optimization problem, we can solve it by existing convex solver such as gradient decent method [37].

**Case 3: Privacy preserving circles** intersect with each other, as Fig. 8 shows. In this case, only one SU is allowed to access $ch_i$ as the analysis in Section 4.3. The best allocation strategy is to choose the SU which brings more revenue to PU. After excluding one SU, the remaining one can transmit with its expected transmit radius. And $PU_i$'s maximum revenue is $T^*_{p,i} = max\{T^1_{p,i}, T^2_{p,2}\}$.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2017.2781248, IEEE Transactions on Dependable and Secure Computing



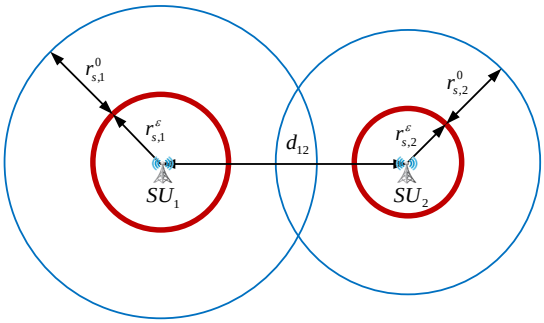



Fig. 7: Interference free circles intersect with each other.

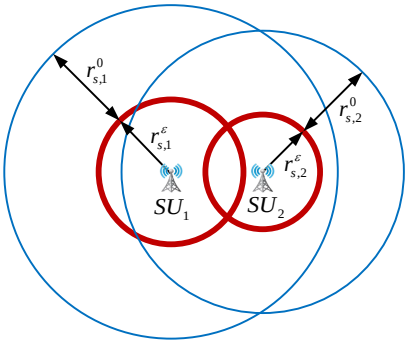



Fig. 8: Privacy preserving circles intersect with each other.

### 6.2 The channel is occupied

When the channel is occupied, database should decide $PU_i$'s optimal PPL and each SU's MTR. Similar to Section 6.1, we only consider the two SUs situation.

**Case 1: Interference free circles** do not intersect with each other, as Fig. 9 shows.

To simplify the analysis, we consider a special situation where $PU_i$ and two SUs are on a straight line as shown in Fig. 9. The other relative locations between $PU_i$ and SUs can be transformed to the above situation, since $PU_i$'s decision is only relevant to the distance between $PU_i$ and the two SUs.

When $PU_i$'s interference free circle is tangent with $SU_j$'s

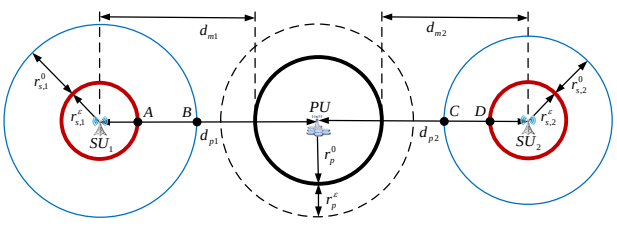



Fig. 9: Interference free circles do not intersect with each other.

interference free circle, we have

$$\begin{aligned} T^1_{p,i} &= \frac{R_1}{r^0_{s,1}} k_1\pi(r^\epsilon_{s,1}+R_1)^2 \\ &= \frac{k_1\pi}{r^0_{s,1}}(d_{m1}-r^\epsilon_{s,1}-L_p)(d_{m1}-L_p)^2, \\ T^2_{p,i} &= \frac{R_2}{r^0_{s,2}} k_1\pi(r^\epsilon_{s,2}+R_2)^2, \\ &= \frac{k_1\pi}{r^0_{s,2}}(d_{m2}-r^\epsilon_{s,2}-L_p)(d_{m2}-L_p)^2. \end{aligned}$$

In this case, $PU_i$'s utility function is piecewise, and is relevant to the relative locations of point $A$, $B$, $C$ and $D$. The reason is that when $L_p$ extends from 0, the interference free circle of $PU_i$ will intersect with the two SUs' circles in point $A$, $B$, $C$ and $D$ in different order. And for each order, $PU_i$'s utility function is different. We will discuss all the possible orders as follows:

(a) The order is $B \to C \to A \to D$.

$$E[U_p] = \begin{cases} T^1_{p,i} + k_1\pi(r^\epsilon_{s,2}+r^0_{s,2})^2 - \frac{k_p}{L_p} \\ \quad \text{if } d_{m1}-r^\epsilon_{s,1}-r^0_{s,1} \le L_p \le d_{m2}-r^\epsilon_{s,2}-r^0_{s,2} \\ T^1_{p,i} + T^2_{p,i} - \frac{k_p}{L_p} \\ \quad \text{if } d_{m2}-r^\epsilon_{s,2}-r^0_{s,2} < L_p \le d_{m1}-r^\epsilon_{s,1} \\ T^2_{p,i} - \frac{k_p}{L_p} \\ \quad \text{if } d_{m1}-r^\epsilon_{s,1} < L_p \le d_{m2}-r^\epsilon_{s,2} \end{cases}$$

(b) The order is $B \to C \to D \to A$.

$$E[U_p] = \begin{cases} T^1_{p,i} + k_1\pi(r^\epsilon_{s,2}+r^0_{s,2})^2 - \frac{k_p}{L_p} \\ \quad \text{if } d_{m1}-r^\epsilon_{s,1}-r^0_{s,1} \le L_p \le d_{m2}-r^\epsilon_{s,2}-r^0_{s,2} \\ T^1_{p,i} + T^2_{p,i} - \frac{k_p}{L_p} \\ \quad \text{if } d_{m2}-r^\epsilon_{s,2}-r^0_{s,2} < L_p \le d_{m2}-r^\epsilon_{s,2} \\ T^1_{p,i} - \frac{k_p}{L_p} \\ \quad \text{if } d_{m2}-r^\epsilon_{s,2} < L_p \le d_{m1}-r^\epsilon_{s,1} \end{cases}$$

(c) The order is $B \to A \to C \to D$.

$$E[U_p] = \begin{cases} T^1_{p,i} + k_1\pi(r^\epsilon_{s,2}+r^0_{s,2})^2 - \frac{k_p}{L_p} \\ \quad \text{if } d_{m1}-r^\epsilon_{s,1}-r^0_{s,1} \le L_p \le d_{m1}-r^\epsilon_{s,1} \\ k_1\pi(r^\epsilon_{s,2}+r^0_{s,2})^2 - \frac{k_p}{L_p} \\ \quad \text{if } d_{m1}-r^\epsilon_{s,1} < L_p \le d_{m2}-r^\epsilon_{s,2}-r^0_{s,2} \\ T^2_{p,i} - \frac{k_p}{L_p} \\ \quad \text{if } d_{m2}-r^\epsilon_{s,2}-r^0_{s,2} < L_p \le d_{m2}-r^\epsilon_{s,2} \end{cases}$$

Since other orders, i.e., $PU_i$'s interference free circle first intersect with $C$ rather than $B$, is symmetric with the above three orders, we will not list here.

Our goal is to decide the optimal $L^*_p$ to maximize $E[U_p]$. To solve this optimization problem, we can find the optimal point in each interval of the objective function, and choose the point which achieves the global optimum. We observe that the objective function is similar to Problem 5.4 in each interval. Thus, we can find the optimal point in each interval as the analysis in Problem 5.4.

**Case 2: Interference free circles** intersect with each other, as Fig. 10 shows.

In this case, we need to optimize $PU_i$'s PPL and SUs' MTR. At the same time, we need to guarantee that the interference free circles of both $PU_i$ and SUs do not intersect with each other. To optimize $PU_i$'s utility, there are two

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2017.2781248, IEEE Transactions on Dependable and Secure Computing



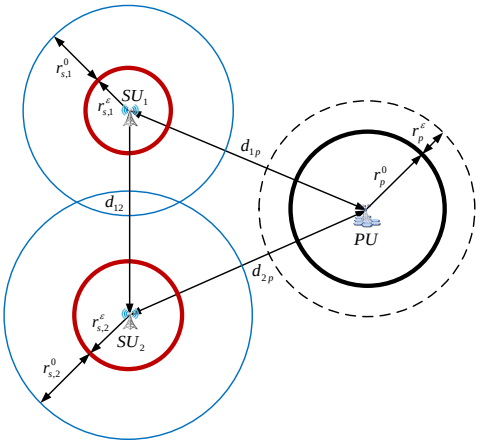



Fig. 10: Interference free circles intersect with each other.

situations: One is that only one SU is available, i.e., the other SU's MTR is 0. The other is that both two SUs are available.

When only one SU is available, we need to find $PU_i$'s optimal PPL in the situation where only $SU_1$ or $SU_2$ exist (similar to the analysis in Section 5), and we denote the optimal PPL as $L^{1*}_{p,1}$ and $L^{1*}_{p,2}$, respectively.

When both two SUs are available, we need to solve the following optimization problem

**Problem 6.2.**

$$\begin{aligned}\underset{R_1,R_2,L_p}{\text{argmax}}\ E[U_p] =& k_1\pi[\frac{R_1}{r^0_{s,1}}(r^\epsilon_{s,1}+R_1)^2+\frac{R_2}{r^0_{s,2}}(r^\epsilon_{s,2}+R_2)^2]\\ &-\frac{k_p}{L_p}\\ s.t.\quad & R_1+r^\epsilon_{s,1}+r_p+L_p\le d_{1p}\\ & R_2+r^\epsilon_{s,2}+r_p+L_p\le d_{2p}\\ & R_1+r^\epsilon_{s,1}+R_2+r^\epsilon_{s,2}\le d_{12}\\ & 0\le R_1\le r^0_{s,1}\\ & 0\le R_2\le r^0_{s,2}\\ & L_p>0\end{aligned}$$

Since the objective function is nonconvex, we will adopt the gradient decent method [37] to find an approximate solution. After finding the optimal PPL $L^{2*}_p$, we can decide the global optimal PPL

$$L^*_p = max\{L^{1*}_{p,1}, L^{1*}_{p,2}, L^{2*}_p\}.$$

**Case 3: Privacy preserving circles** intersect with each other as Fig. 11 shows.

In this case, similar to the analysis in Case 3 of channel vacant situation, we only need to satisfy one SU's requirement and exclude the other one to avoid interference. To achieve the maximum utility, PU can exclude one SU and decide its optimal PPL separately, and then choose the SU which can achieve the maximum utility. If only one SU exist, we decide $PU_i$'s optimal PPL $L^*_{p,1}$ and $L^*_{p,2}$, respectively. And $PU_i$'s global optimal PPL is given by

$$L^*_p = max\{L^*_{p,1}, L^*_{p,2}\}.$$

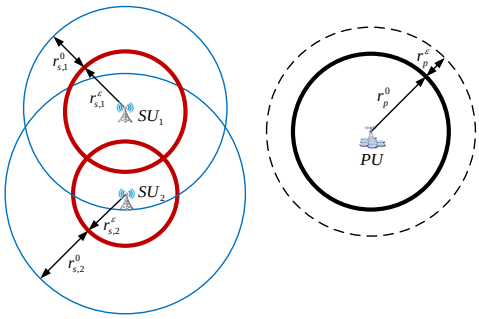



Fig. 11: Privacy preserving circles intersect with each other.

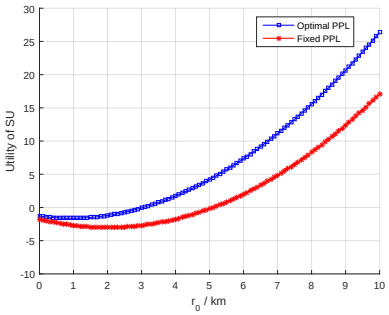



Fig. 12: Optimal PPL Vs. fixed PPL to SU's utility.

## 7 Simulation

In this section, we first introduce the simulation setup. Then, we illustrate the advantage of our proposed UMax protocol by comparing with the baseline protocol.

### 7.1 Simulation Setup

Firstly, we present the baseline protocol: different from the proposed UMax protocol where SUs and PUs decide their optimal PPLs before querying the database and deciding the allocation strategy, both PUs and SUs in the baseline protocol choose a predefined fixed PPLs.

For brevity, we set the unit of the distance in the simulation to *kilometer*, and only utilize the number to describe the distance in the following part. We set the fixed PPLs of SUs and PUs in the baseline protocol to be 2 and 1, respectively. The privacy cost coefficient $k_s$ and $k_p$ are set to be 1 and 2, $k_1$ and $k_2$ are set to be 0.1 and 0.2.

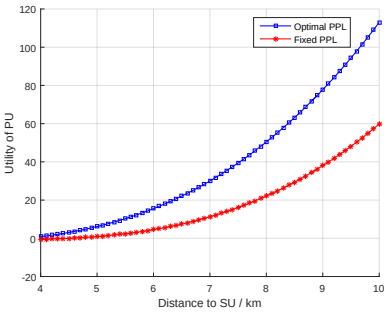
Then, we introduce the simulation settings: 1) We compare SUs' utilities when they choose different required transmit radius; 2) PUs' utilities are compared in different location settings, i.e., the relative distance between PUs and SUs are different. 3) We construct an $20 * 20$ area and randomly deploy 10 PUs and 20 SUs, we then compare the utilities of different PUs.

### 7.2 Performance Comparison

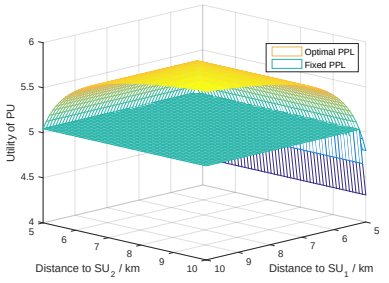
Fig. 12 compares the utilities of the proposed protocol with the baseline protocol for SUs. The simulation result shows that the proposed protocol can improve SUs' utility efficiently for different required transmit radius $r_0$. Notice that SU's utility is negative when $r_0$ is shorter than a threshold, e.g.,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2017.2781248, IEEE Transactions on Dependable and Secure Computing

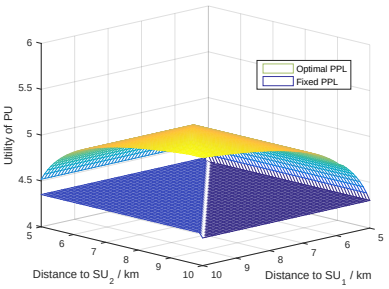





(a) Single PU single SU scenario.




(b) Single PU two SUs scenario where SUs do not intersect with each other.



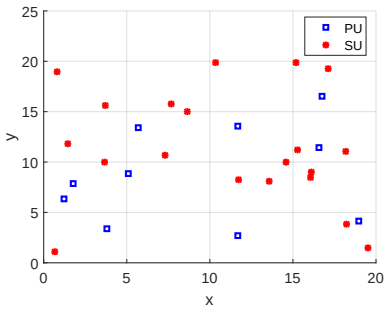

(c) Single PU two SUs scenario where SUs intersect with each other.

Fig. 13: Optimal PPL Vs. fixed PPL to PU's utility.

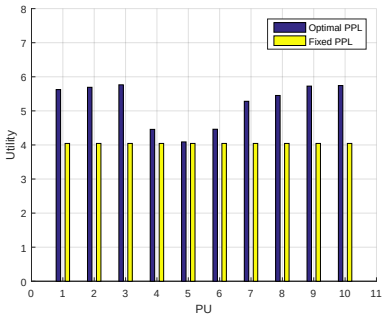
3 for optimal PPL and 5 for fixed PPL. The reason is that when $r_0$ is shorter than a threshold, SU's revenue $R_s$ is few which is obvious in Problem 5.3. In another hand, SUs' should choose a small PPL to guarantee their privacy. As a result, SU's payment $C_{buy}$ would be larger than its revenue $R_s$ which lead to a negative utility.

Fig. 13 compares the utilities of the proposed protocol with the baseline protocol for PUs in different location settings. The simulation is conducted in three different scenarios: (i) Single PU single SU scenario; (ii) Single PU two SUs scenario where SUs do not intersect with each other; (iii) Single PU two SUs scenario where SUs intersect with each other.

Fig. 13(a) shows that, in the single PU single SU scenario, PUs in the proposed protocol achieves higher utility compared with the baseline where PUs choose the fixed PPL. In another hand, PUs achieves higher utility when the distance between PU and SU increase. The reason is that, PUs would receive more revenue through selling spectrum to SUs when the distance increase. Fig. 13(b) and Fig. 13(c) illustrate the advantage of the proposed protocol where there are one




(a) Distribution map of PUs and SUs




(b) Utility of different PUs.

Fig. 14: PUs' utilities with random deployment.

PU and two SUs, where $x$ coordinate refers to the distance between PU and $SU_1$, and $y$ coordinate refers to the distance between PU and $SU_2$. Specifically, Fig. 13(b) shows the scenario where SUs do not intersect with each other, the theoretic analysis of which is given in Section 6.2 **Case 1**, and Fig. 13(c) shows the scenario where SUs intersect with each other, the theoretic analysis of which is given in Section 6.2 **Case 2**. Both 13(b) and 13(c) shows that PUs achieves higher utility compared with the baseline where PUs choose fixed PPLs.

Fig. 14 compares PUs' utilities of the proposed protocol with the baseline protocol when we randomly deploy some PUs and SUs in a given area. In Fig. 14(a), we randomly deploy 10 PUs and 20 SUs in an $20*20$ area. Fig. 14(b)compares the utilities of different PUs. The simulation result shows that the proposed protocol achieves higher utility compared with the baseline protocol for all PUs.

## 8 Conclusion

In this paper, we proposed a novel location privacy preservation scheme, while achieving bilateral utilization maximization of both PUs and SUs. First, a quantitative mechanism was proposed to preserve the location privacy of both PUs and SUs simultaneously based on the concept of differential privacy. Based on the quantitative mechanism framework, we further proposed a novel privacy preserving Utility Maximization protocol (UMax). UMax allows for both PUs and SUs to adjust their privacy preserving levels to achieve the optimal utility. Extensive simulations demonstrated that our proposed mechanism can efficiently increase both PUs' and SUs' utility while preserving their location privacy.

## ACKNOWLEDGMENTS

This work is partially supported by NSFC under Grant 61731004, by ZJU-SUTD joint project under Grant 188170-11102/012, by Nature Science Foundation of Jiangsu Province under Grant BK20171264.

## REFERENCES

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

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

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

[4] J. Wang, M. Ghosh, and K. Challapali, "Emerging cognitive radio applications: A survey," *IEEE Communications Magazine*, vol. 49, no. 3, 2011.

[5] M. Patel and J. Wang, "Applications, challenges, and prospective in emerging body area networking technologies," *IEEE Wireless communications*, vol. 17, no. 1, 2010.

[6] "Ex-parte comments of ge healthcare in docket 06-135," http://fjallfoss.fcc.gov/ecfs/document/view?id=6519820996/.

[7] X. Duan, C. Zhao, S. He, P. Cheng, and J. Zhang, "Distributed algorithms to compute walrasian equilibrium in mobile crowdsensing," *IEEE Transactions on Industrial Electronics*, vol. 64, no. 5, pp. 4048–4057, 2017.

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

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

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

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

[12] G. Yang, S. He, Z. Shi, and J. Chen, "Promoting cooperation by the social incentive mechanism in mobile crowdsensing," *IEEE Communications Magazine*, vol. 55, no. 3, pp. 86–92, 2017.

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

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

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

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

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

[18] C. Dwork, "Differential privacy," *Automata, languages and programming*, pp. 1–12, 2006.

[19] R. Chen, J.-M. Park, and K. Bian, "Robust distributed spectrum sensing in cognitive radio networks," in *Proceedings of IEEE INFOCOM'08*.

[20] A. W. Min, X. Zhang, and K. G. Shin, "Detection of small-scale primary users in cognitive radio networks," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 2, pp. 349–361, 2011.

[21] J. Chen, K. Hu, Q. Wang, Y. Sun, Z. Shi, and S. He, "Narrowband internet of things: Implementations and applications," *IEEE Internet of Things Journal*, vol. DOI: 10.1109/JIOT.2017.2764475, to appear.

[22] S. He, J. Chen, F. Jiang, D. K. Yau, G. Xing, and Y. Sun, "Energy provisioning in wireless rechargeable sensor networks," *IEEE Transactions on Mobile Computing*, vol. 12, no. 10, pp. 1931–1942, 2013.

[23] R. Chen, J.-M. Park, and J. H. Reed, "Defense against primary user emulation attacks in cognitive radio networks," *IEEE Journal on Selected Areas in Communications*, vol. 26, no. 1, pp. 25–37, 2008.

[24] A. W. Min, K. G. Shin, and X. Hu, "Secure cooperative sensing in ieee 802.22 wrans using shadow fading correlation," *IEEE Transactions on Mobile Computing*, vol. 10, no. 10, pp. 1434–1447, 2011.

[25] P. Shankar, V. Ganapathy, and L. Iftode, "Privately querying location-based services with sybilquery," in *Proceedings of ACM UbiComp'09*, pp. 31–40.

[26] R. Shokri, C. Troncoso, C. Diaz, J. Freudiger, and J.-P. Hubaux, "Unraveling an old cloak: k-anonymity for location privacy," in *Proceedings of ACM WPES'10*, 2010, pp. 115–118.

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

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

[29] N. Li, T. Li, and S. Venkatasubramanian, "t-closeness: Privacy beyond k-anonymity and l-diversity," in *Proceedings of IEEE ICDE'07*, 2007, pp. 106–115.

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

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

[32] D. He, N. Kumar, S. Zeadally, A. Vinel, and L. T. Yang, "Efficient and privacy-preserving data aggregation scheme for smart grid against internal adversaries," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2411–2419, 2017.

[33] M. E. Andrés, N. E. Bordenabe, K. Chatzikokolakis, and C. Palamidessi, "Geo-indistinguishability: Differential privacy for location-based systems," in *Proceedings of ACM CCS'13*, pp. 901–914.

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

[35] H. Zhang, Y. Shu, P. Cheng, and J. Chen, "Privacy and performance trade-off in cyber-physical systems," *IEEE Network*, vol. 30, no. 2, pp. 62–66, 2016.

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

[37] S. Boyd and L. Vandenberghe, *Convex optimization*. Cambridge University Press, 2004.

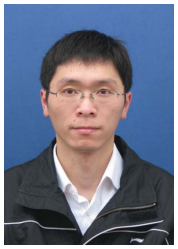
[38] R. Garver, "On the nature of the roots of a quartic equation," *Mathematics News Letter*, pp. 6–8, 1933.

**Zhikun Zhang** received the B.Eng. degree in automation in 2014 from Shandong University, Jinan, China. From Oct. 2017 to Oct. 2018, he is a visiting scholar with Purdue University, West Lafayette, IN, USA. He is currently working toward the Ph.D. degree in the Group of Networked Sensing and Control (IIPC-NeSC) in the State Key Laboratory of Industrial Control Technology, Zhejiang University. His research interests include location privacy, differential privacy and its applications in cognitive radio, crowdsensing system and machine learning.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TDSC.2017.2781248, IEEE Transactions on Dependable and Secure Computing



**Heng Zhang** received the Ph.D. degree in control science and engineering from Zhejiang University in 2015. He is currently an associate professor at the School of Science, Huaihai Institute of Technology, Lianyungang, Jiangsu, China. He is also a research fellow at Western Sydney University. His research interests include security and privacy in cyber-physical systems, control and optimization theory. He is an editor board member of several academic journals, including IET Wireless Sensor Systems, EURASIP Journal on Wireless Communications and Networking, KSII Transactions on Internet and Information Systems, etc. He also serves as a guest editor of Journal of The Franklin Institute, Peer-to-Peer Networking and Applications. He is also an active reviewer of IEEE TAC, IEEE TCNS, IEEE TIFS, and IEEE TWC, etc.



**Shibo He** (M'13) received the Ph.D. degree in control science and engineering from Zhejiang University, Hangzhou, China, in 2012. From Nov. 2010 to Nov. 2011, he was a visiting scholar with the University of Waterloo, Waterloo, ON, Canada. He was an Associate Research Scientist from March 2014 to May 2014, and a postdoctoral scholar from May 2012 to February 2014, with Arizona State University, Tempe, AZ, USA. He is currently a Professor at Zhejiang University. His research interests include wireless sensor networks, crowdsensing and big data analysis.

Dr. He serves on the editorial board of IEEE Transactions on Vehicular Technology, Springer Peer-to-Peer Networking and Application, KSII transactions Internet and Information Systems, and is a guest editor of Elsevier Computer Communications and Hindawi International Journal of Distributed Sensor Networks. He served as publicity chair for IEEE SECON 2016, Registration and Fiance chair for ACM MobiHoc 2015, TPC Co-chair for IEEE ScalCom 2014, TPC Vice Co-chair for ANT 2013-2014, Track Co-chair for the Pervasive Algorithms, Protocols, and Networks of EUSPN 2013, Web Co-Chair for IEEE MASS 2013, and Publicity Co-chair of IEEE WiSARN 2010. Dr. He is the recipient of IEEE Asia-Pacific outstanding researcher award, 2015.

**Peng Cheng** (M'10) received the B.E. degree in Automation, and the Ph.D. degree in Control Science and Engineering in 2004 and 2009 respectively, both from Zhejiang University, Hangzhou, P.R. China. Currently he is a Professor with the Department of Control Science and Engineering, Zhejiang University. He serves as Associate Editor for Wireless Networks, International Journal of Distributed Sensor Networks, and International Journal of Communication systems. He also served as publicity co-Chair for IEEE MASS 2013 and Local Arrangement Chair for ACM MobiHoc 2015. His research interests include networked sensing and control, cyber-physical systems, and robust control.