Open access • Proceedings Article • DOI:10.1109/DYSPAN.2018.8610485

On the Privacy and Utility Tradeoff in Database-Assisted Dynamic Spectrum Access

Ahmed M. Salama, Ming Li, Loukas Lazos, Yong Xiao ...+1 more authors

Institutions: University of Arizona

Published on: 01 Oct 2018 - IEEE International Symposium on Dynamic Spectrum Access Networks

On the Privacy and Utility Tradeoff in Database-Assisted Dynamic Spectrum Access

Ahmed M. Salama[1], Ming Li[1], Loukas Lazos[1], Yong Xiao[1], Marwan Krunz[1,2]
[1] Dept. of ECE, The University of Arizona. [2] Dept. of EDE, University Technology Sydney.
E-mail{ahmedsalama,lim,llazos,yongxiao,krunz}@email.arizona.edu

***Abstract*—In dynamic spectrum access, commercially-operated database servers are often used to assist the opportunistic users (OUs) to query and access spectrum vacancies of incumbent users (IUs). The query and answer process in such DSA architectures introduce significant privacy concerns for potential leakage of the sensitive operational details of the IUs, especially their locations. Existing privacy-preserving mechanisms such as location cloaking or spatial obfuscation can be used to hide IUs' locations. They however cannot guarantee the interference from all surrounding access-allowed OUs staying under a given limit. In addition, the spectrum utilization (i.e., transmission opportunities) of OUs should also be considered in the design of mechanisms. The complex three-way tradeoff among privacy, interference and utility has not been systematically studied in the literature. In this paper, we first endeavor to tackle this challenge, by introducing a privacy zone within the exclusion zone. In the privacy zone the IU's location is indistinguishable, while the exclusion zone guarantees the interference limit within the privacy zone. Under two variants of the system model (either known OU locations or probabilistic locations with known density), we formulate and solve corresponding optimization problems to find the optimal tradeoff of one versus the other two objectives. Simulation results with real-world maps/parameters show that the IU's privacy increases with decreasing OUs' utility given a fixed allowable interference for the IUs.**

I. Introduction

Dynamic Spectrum Access (DSA) allows opportunistic users (OUs) to access the spectrum that is unoccupied or ineffectively used by the incumbent users (IUs) [1]. Database-driven DSA have been approved by FCC as one of the key architectures for increasing the spectrum utilization [2]. Major IT service providers offer free open-to-public spectrum database services, such as Google [3] TV white space database and Microsoft Spectrum Observatory [4]. In addition, FCC adopts the three-tier spectrum sharing framework to protect the IUs including authorized federal and satellite services currently operating in the the 3.5 GHz Citizens Broadband Radio Service (CBRS) band [5].

The spectrum databases collect and store detailed information about IUs' activity, such as the geo-location, frequency and time of transmitter/receivers which is very sensitive information. Therefore, much concern has been raised regarding the operational privacy of IUs [6]. For example, imagine a military base operating a passive radar in the 3.5 GHz band. If its location is recorded by a spectrum database, the location can be leaked when a database is compromised by hackers. Even if the database is well-protected, malicious OUs can issue multiple spectrum access queries to the server from different locations that ultimately allow them to pinpoint the location of the radar. Leakage of such sensitive information would put the safety of the personnel inside the military base and their equipment in danger. Therefore, protecting IU's operational details, most importantly its geo-location, is a critical need.

To protect an IU's location, a straw-man approach is to apply spatial cloaking techniques [7], [8]. The idea is depicted in Fig.1(a), where the IU first randomly perturb its real location x into a nearby x', and then the disk centered by x' (including x) is reported to the spectrum server, for which we call a privacy zone (PZ). In this way, x is indistinguishable (equally probable) with all other locations within the PZ, similar to the notion of k-anonymity [9]. However, this approach cannot guarantee OUs' interference to the IU is always under the allowable limit. If the spectrum access query result solely depends on whether OUs are inside the PZ or not (all the OUs outside this PZ are allowed to transmit), when IU's true location x is near the boundary of the PZ, the interference from nearby OUs right outside of the PZ can be high.

On the other hand, the traditional way of protecting the IU from OUs' interference is to designate an exclusion zone (EZ) surrounding the IU [10], [11], inside of which all the OUs must be silent. The size/radius of the EZ can be tuned according to the IU's allowable interference resulting in a tradeoff between the IU's interference protection and the OUs' transmission opportunity. This is illustrated in Fig. 1(b), where the red crosses denote the active OUs and the green squares inside of the EZ are the inactive OUs. However, such techniques were not designed with privacy as a criterion, since the IU is usually located at the center of the EZ uploaded to the database, which can be inferred by both the database and the OUs.

To resolve the above dilemma (reconcile both IU privacy requirement and interference constraints), we will need to introduce two zones (EZ and PZ) simultaneously, which is shown in Fig. 1(c). The IU's possible location is within the PZ, while no OU is allowed to transmit inside the EZ. Thus, the region between the PZ's and EZ's boundaries can be viewed as a "buffer zone" that prevents interference to IUs in the worst case. This new approach gives rise to an interesting three-way tradeoff among the IU's privacy, received interference, and OU's utility (transmission opportunity). Intuitively, if we fix the PZ and enlarge the EZ, the maximum interference received

This work was partly supported by NSF grants CNS-1731164, CNS-1619728, CNS-1564477, CNS-1563655, CNS-1409172 and IIP-1265960. Any opinions, findings, conclusions, or recommendations expressed in this paper are those of the author(s) and do not necessarily reflect the views of NSF.

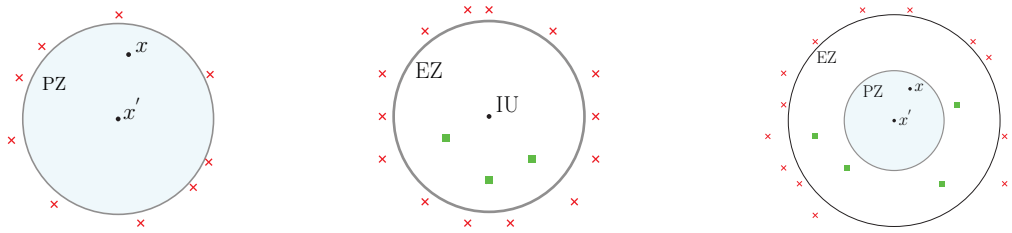


Figure 1: (a) Privacy Zone (PZ); (b) Traditional Exclusion Zone (EZ); (c) PZ is contained in the EZ.

by the IU will decrease but the area that can be allowed for OUs to access the spectrum will be less. If the IU cares about its privacy, it could make both PZ and EZ very large, but that would result in low spectrum utilization defeating the purpose of DSA. Also, the IU may have an incentive to allow more OUs to access its spectrum (e.g., it gains more revenue since it leases more spectrum to OUs). On the other hand, if the size of EZ is fixed and we enlarge the PZ, the IU's privacy will be higher but its interference in the worst case will increase as well. Consequently, an optimal balance should be made among IU's privacy, interference, and OUs' utility when designing the query and answer mechanism with spectrum databases.

In this work, we endeavor to quantify the above three-way tradeoff, under two different scenarios. First, we consider the case when the OUs' locations are known to a spectrum access server (SAS) allowing us to obtain a concrete estimation of the interference received by the IU. For this case, we formulate an optimization problem to maximize the OUs' transmission opportunity under a given interference constraint and privacy level. We prove that the problem is convex and can be solved by selectively shutting down some OUs outside the PZ according to the IU's interference constraint. Then, we studied a more general case where the SAS cannot know the specific location of each OU but only know the OUs' distribution density and the maximum transmission power. We focus on the scenario that OUs are distributed randomly according to Poisson point process [12] over an area that can be regarded as infinite. For privacy protection, we choose a perturbed location in the center of a PZ that contains the IU; to guarantee the worst case expected interference, we surround the PZ with a circular EZ where no OU can transmit. We formulate a non-linear optimization problem [13] and derive the optimal radii of the EZ and PZ using the iterative optimality condition decomposition [14] algorithm. In both cases, our solutions preserve IU's location privacy since they ensure all the possible locations of OUs inside the PZ, including IU's true location, satisfy the same interference constraint, and the IU uniformly positioned at random inside the PZ.

Our main contributions are summarized as follows:

(1) To the best of our knowledge, this paper is the first to define and quantify the three-way tradeoff between IU's privacy, interference and OU's utility for database-assisted DSA. We introduce the novel concept of placing a PZ inside of a EZ to protect the IU's privacy and limit OUs' interference.

(2) For deterministic OU location case (DOL), we formulate an optimization problem that maximizes the OU's utility under a given interference constraint. We show that the problem is convex and present a simple algorithm to achieve the optimal transmission opportunity for OUs.

(3) For the case when OUs' density is known, called the Probabilistic OU location case (POL) case, we formulate a non-linear optimization problem that optimizes either EZ's or PZ's radius under a non-linear interference constraint.

(4) Simulation results based on real data of a military base and commercial cellular base station locations have been presented. Our result show that for the same EZ size, decreasing the allowable interference would shrink the size of PZ, and the ratio of PZ radius over EZ's increases almost linearly with higher interference.

The rest of the paper is organized as follows: In Section II, we give a brief literature review. In Section III, we describe the system model. The problem formulation and solution are depicted in Section IV. Section V presents the simulation results. Section VI concludes the paper.

II. Related Work

On of the early focuses of DSA was cooperative spectrum sensing paradigms, and their privacy concern is mainly on protecting OUs' locations rather than the IUs' [15]. Recently, Database-assisted spectrum access [16] has been introduced to overcome the cooperative spectrum sensing shortcomings such as its technical implementation difficulty, high deployment cost, and its tendency to be overly conservative by preventing the utilization of vacant channels as reported by FCC [17]. Spectrum databases monitor spectrum availability by a combination of information including IU activity prediction, IU *push* updates, and channel propagation modeling, thus IU's operational privacy becomes more important. While many privacy preserving techniques have been proposed in other settings such as location-based services (LBS), they are either not directly applicable to DSA or only partially address the challenges in DSA as OUs' interference is not considered.

Early techniques focused on location obfuscation or spatial cloaking [18], where a user's location is made indistinguishable among other $K-1$ users, which satisfies the notion of K-anonymity [19]. This can be applied to DSA; for example, Zhang *et al.* [20] proposes to ensure OUs' K-anonymity by making the SU query K locations surrounding its actual location, while the IU's K-anonymity is met by grouping K IUs together as one virtual IU to enlarge their protection region. Li *et al.* [21] apply k-anonymity to protect OUs' location privacy by making an OU submit queries for k channels, instead of one, to confuse the attackers and prevent them from using the spectrum utilization to localize an OU.

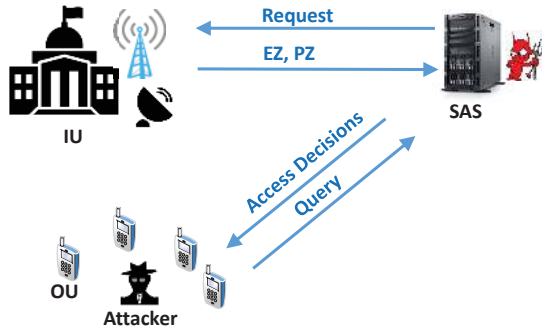


Figure 2: System architecture and query process.

Although these schemes achieve location privacy, they don't take into account the OUs' interference to the IU and require existence of $K-1$ other users or waste spectrum resources.

To enhance the utility while satisfying formal privacy definitions, Andres *et al*. [22] proposed geo-indistinguishability, which is a variant of differential privacy [23]. Their mechanism adds two dimensional Laplacian distribution noise to user's real location before uploading to an untrusted server. Various metrics, such as information-theoretic and estimation error, were proposed to quantify and optimize location privacy [24]. However, they all focused on the setting, in which the utility is defined as the location error, quite different from the interference and spectrum utilization in the DSA setting. In [6], Bahrak *et al*. used additive noise perturbation and privacy zone shape transfiguration to protect the IU against the location inference attacks performed by the OUs. This work first define an EZ for each IU that protect it from interference and then a number of K IUs are grouped together inside a larger EZ, which becomes also a PZ in the mean time, to achieve k-anonymity. However, this method degrades OU's transmission opportunity as grouping excludes large areas containing OUs. Also, the interference is not explicitly calculated or optimized.

Finally, cryptographic techniques [15] protects IU and/or OU locations by encrypting them. In [25], Troja *et al*. adopted private information retrieval for protecting OUs' query location privacy while taking into account OU's mobility. Dou *et al*. [26] presented a privacy-preserving SAS design that protects IU's privacy through secure computation on the ciphertext domain based on homomorphic encryption, so that the IU's EZ information is hidden from the SAS. Chen *et al*. [27] designed a secure protocol for database-driven spectrum sharing by combining secure computations and message authentication codes to enable verification. However, in all the crypto-based schemes, the exact query results must be revealed to the SAS and OUs, which still suffer from IU location inference attacks. The high computation/communication overhead introduced by encryption and decryption is also a concern. While we aim at preventing IU location inference, our schemes can be integrated with secure computation techniques to protect both IU's and OU's location privacy.

III. System Model

In this section, we provide an overview to the system architecture, assumptions, and threat model.

A. Spectrum Sharing Architecture and Query Process

We consider three types of entities: Incumbent Users (IUs), Opportunistic Users (OUs), and the spectrum access server (SAS) (shown in Fig. 2). IUs can be a government/military/commercial user which cares about its operational privacy. For simplicity, we consider a single IU for now; we will discuss how to extend our results into multi-IU cases later in the paper. The SAS collects and stores spectrum vacancy/activity information of the IU and answers access queries from OUs. Typically, an IU uploads its exclusion zone (EZ), channel access activity and access time period to the SAS (can either be push or pull-based updates). The OUs access the spectrum opportunistically by querying SAS. The query includes an OU's location y_i and the channel/time period it wishes to access, its intended transmission power, SAS checks the database and returns a binary answer – '1' if $y_i \notin EZ$ and the requested channel/time is available (granted access), and '0' otherwise (denied access).

The above architecture and query process follows the existing database-assisted spectrum sharing models, such as the FCC approved three-tier model [5] and the TV white spaces [2]. In this paper, for privacy protection, we assume that the IU computes its EZ and in addition to PZ, based on certain information of the OUs. We consider two different scenarios: (1) We assume that all the potential OUs' locations are known in advance to the SAS who forwards them to the IU in a request. This can be obtained when the OUs register themselves to participate in the system (to get initial authorization). Alternatively, the SAS can wait until all the OUs submit their queries and then forward their locations in the request. This model is mainly suitable for static OUs. (2) The OUs' locations cannot be known in advance and we follow a commonly adopted assumption and assume they follow a Poisson point process [12]. The density λ can be obtained from general location statistics data such as a heat-map, or prior query histories, which is also accessible by the IU. This could be achieved in reality as large companies like Microsoft and Google already have a spectrum access databases which the SAS uses. Hence the IU know the number of spectrum access requests from a specific area and use it to estimate λ. This model is applicable to mobile OUs as well since the exact location of OUs are not needed ahead of time. We believe that our modifications are compatible with existing models. In this work, privacy protection of the IU's active channel or time are not considered, which will be extended in our future work.

B. Threat Model

We assume that some of the OUs are curious about IU's operational details, who will perform inference attacks to estimate the IU's location x. They could be commercial competitors, enemies, or blackmailers. To carry out the inference, one OU can launch multiple spectrum queries using different locations (could be faked), or multiple OUs can collude with each other to submit queries if a rate limiting/location verification mechanism is deployed by the SAS. If a traditional EZ is adopted (IU is located at the center of EZ), with an enough number of queries, the OUs will be able to accurately

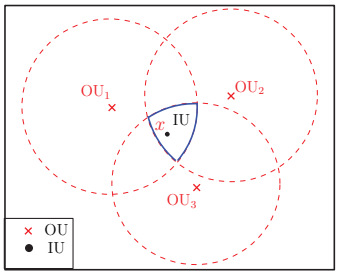


Figure 3: Intersection attack.

estimate the location of IU through an "intersection attack". That is, for each query that returns '0', it means that the IU is located within a circle with radius equal to the transmission range of the IU (up to an error margin), centered at the OU's query location. This scenario is shown in Fig.3.

In addition, the SAS can also be untrusted. We assume it is honest-but-curious (i.e., it will honestly execute the protocol but is interested in the operational details of the IUs too). This is due to either possibilities of a data breach or compromise of the SAS by external hackers, or insiders within the SAS's organization who may peek into the stored sensitive IU profiles and reveal/sell them to third-parties. This is especially relevant considering that nowadays most spectrum databases are hosted by cloud/Internet service providers.

That said, we assume that the adversary cannot physically measure the IU's location (e.g., via deploying multiple sensors nearby the IU and use tri-lateration techniques). It would be quite costly, since in the real-world, the sensitive regions are typically physically protected. However, the adversary knows the algorithm used by the IUs to generate their EZ/PZ, and the inputs (OU locations or density, except the IU's location and internal random coin flipping) and outputs (EZ/PZ, and query results) can be eavesdropped by the attacker. Note that all the communication links can be encrypted and the eavesdropping happens at the SAS/OUs. We don't assume adversary possess precise background knowledge about IU's locations, other than the default uniform prior distributions over a certain region (e.g., knowing that a radar is inside a military base).

IV. The Three-way tradeoff between Privacy, Interference, and Utility

In this section, we define the design objectives and formulate the three-way tradeoff between the IU's privacy, interference, and the OUs' spectrum utilization. We formulate relevant optimization problems for the DOL and POL scenarios and characterize the tradeoffs by deriving optimal solutions.

A. Definitions

1) Privacy Metric: Since the IU's goal is to prevent the adversary (SAS and OUs) from inferring its true location x, we can use conditional entropy ($H(X|EZ, PZ)$) to quantify the remaining uncertainty given the information available to the adversary, that is, the EZ and PZ uploaded by the IU. Note that, the EZ does not provide any additional information about x, since by design, we know that the IU cannot reside in the region between the PZ and EZ. Thus, it is safe to say that $H(X|EZ, PZ) = H(X|PZ)$:

Definition 1 (Privacy ($\mathcal{P}$))**.** *Let random variable X represent the IU's location. The privacy $\mathcal{P}$ of the IU is defined as the conditional entropy $H(X|PZ)$, i.e, the uncertainty about X given the knowledge of PZ.*

When X has a uniform prior distribution, $H(X|PZ)$ is maximized when the posterior probability is uniform:

$$P(X = x|PZ) = \frac{1}{|PZ|}, \forall x \in PZ, \tag{1}$$

where $|PZ|$ is the size of the PZ. In other words, by publishing the PZ, the IU's location is indistinguishable among all the locations in the PZ. Note that, $P(X = x|PZ)$ is inversely proportional to the PZ size. In addition, $H(X|PZ)$ increases with the PZ size. Thus, in the rest of the paper, we focus on the PZ size as the privacy objective. In the DOL case, the PZ consists of K discrete location cells. In the POL case, the PZ is a disk of continuous points, so the area is πr^2 and the probability density function should be used instead.

Note that, for non-uniform prior knowledge, the optimal PZ generation mechanism that maximizes the conditional entropy depends on that prior knowledge, and does not have a simple analytic form. We leave the treatment of this non-uniform case as future work. Note also that, although differential privacy (DP) [22] protects against adversaries with arbitrary prior knowledge, it only provides indistinguishability guarantees between two locations, but doesn't offer a concrete guarantee in terms of posterior probability of location inference. Also, DP mechanisms such as geo-indistinguishability incur non-uniform posterior (i.e., higher inference probability for points near x, under the same PZ size).

2) Interference: The normal operation of IU requires that the total interference from active OUs is under a certain threshold. Thus, we define interference as follows:

Definition 2 (Interference ($\mathcal{I}$))**.** *The aggregated interference experienced at location j from the set of active OUs $\mathcal{S}_A$ is defined as $I_j = \sum_{i \in \mathcal{S}_A} I_{ij}$, where I_{ij} is the interference caused by the ith OU at location j, and $\mathcal{I}$ is the maximum aggregated interference experienced by any location in PZ: $\mathcal{I} = max_{j \in PZ} I_j$.*

The calculation of I_{ij} for all pairs of OU i and $j \in$ PZ can be achieved by channel modeling. In the DOL case, the exact interference can be computed since we know the OUs' locations in advance. For the POL case, we can only calculate an expected interference based on the distribution of OUs. $\mathcal{I}$ represents the worst-case aggregated interference the IU receives from all the active OUs (as the IU could be located anywhere in the PZ).

3) Utility Definition: To guarantee interference constraints we need to selectively deny spectrum access to a subset of OUs. However, this will impact the spectrum utilization. Our goal is to preserve the transmission opportunity of the OUs. To quantify this, we could try to use a concrete metric such as throughput, or quality of service, which are however very difficult to derive without knowing specific scheduling

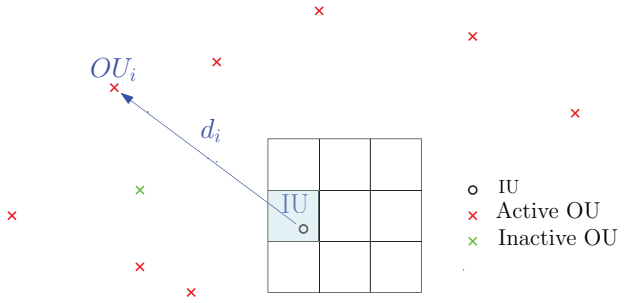


Figure 4: The Deterministic OU location (DOL) model.

schemes, channel conditions and interference among the OUs, and the channel access protocols, etc. Also, computing such metrics only adds complexity without adding more insight for the tradeoff. Thus, we use the number of OUs that are granted access to represent OUs' transmission opportunity:

Definition 3 (Utility ($\mathcal{U}$))**.** *We define the OUs' utility $\mathcal{U}$ as the number of OUs that are granted access (allowed to transmit). In the case of DOL, this number is exact. In the case of POL, this is an expected number of OUs.*

B. Problem Formulations

The three-way tradeoff between $\mathcal{P}$, $\mathcal{U}$, and $\mathcal{I}$ can be represented by the following general formulations:

$$F_1 \quad : \quad \{\max \mathcal{P} \mid \mathcal{I} \leq I_{TH},\ \mathcal{U} \geq U_{TH}\}, \tag{2}$$

$$F_2 \quad : \quad \{\min I_{TH} \mid \mathcal{P} \geq P_{th},\ \mathcal{I} \leq I_{TH}, \mathcal{U} \geq U_{TH}\}, \tag{3}$$

$$F_3 \quad : \quad \{\max \mathcal{U} \mid \mathcal{P} \geq P_{th},\ \mathcal{I} \leq I_{TH}\}, \tag{4}$$

where P_{th}, I_{TH}. U_{TH} represent privacy, interference and utility thresholds, respectively. For the IU, we would like to guarantee that its worst case interference caused by the permitted spectrum access of all OUs is below a threshold, denoted as I_{TH}. To maintain IU's privacy, this constraint must hold for every point inside the PZ. For the DOL case, the solution of $\mathcal{I}$ is deterministic since the exact OU locations are known. Given this knowledge, it's sufficient to shut down some SUs to form an EZ that satisfies I_{TH}. For the POL case, the expected interference is calculated as we only have density λ. The EZ in this case is a disk-shaped area around the IU.

The use of a specific formulation depends on the importance of a given objective function to be optimized. For example, for F_1, maximizing $\mathcal{P}$ subject to interference and utility constraints means that F_1 is prioritized $\mathcal{P}$ over $\mathcal{I}$ and $\mathcal{U}$. We will observe, in the subsequent sections, that some formulations are equivalent, i.e., they give the same solutions under similar conditions. Also, we will see a formulation could be easier in terms of finding a solution than the others which makes it favorable. Furthermore, some formulations could be integrated together to jointly optimize two metrics, privacy and interference for example, which we will see later in the results section.

C. The Deterministic OU Location (DOL) Case

In the DOL setting, we assume that the set $\mathcal{Y} = \{y_i\}_{i=1}^{N}$ of the OUs' locations are known in advance to the SAS. The IU utilizes both its own location x and the known OUs locations to generate the PZ. To ensure countability when calculating interference, we divide the PZ into a finite number K of discretized grid cells. The IU is located in one of these cells, which are contiguous to minimize the utility loss for the OUs. To satisfy our privacy definition, the IU should generate the PZ by choosing a contiguous set consisting of K grid cells uniformly at random, from all possible such sets that contain the IU's location inside. This can be achieved in practice by first generating one fixed-shape area as a mask, and then randomly select one of the cells and fix it to be the IU's location x, thus fixing the PZ. The basic idea is depicted in Fig.4. We choose the square shape to represent the PZ cells for two reasons: a) the square shape is one of the shapes that leaves no spacing when aggregated which makes the PZ cells contiguous b) makes it easy to force the same interference threshold I_{TH} over all the cells. However, for the overall shape of the PZ, any geometric shape, would be technically equivalent as the PZ is adjusted randomly around the IU irrespective of the shape, which delivers the same privacy level even if the overall PZ is not square.

The EZ is implicitly formed when the IU selects, by optimization, a subset of surrounding OUs to deny their spectrum access, which will guarantee I_{TH} to be met for all the cells inside PZ. To compute the interference from the i-th OU to the j-th cell in the PZ, we can use any existing signal propagation model, however, we use a path-loss model to represent the interference which has two merits. First, it simplifies the calculations. Second, it gives the upper bound on the experienced interference [28]. Hence, the interference caused by the ith OU at the center of ith PZ cell is given by

$$I_{ij} = \frac{P_i}{d_{ij}^{\eta}}, \tag{5}$$

where d_{ij} is the distance between the ith OU's location y_i and the center of the j-th cell in the PZ, and $\eta \geq 2$ is the path-loss exponent. When $\eta = 2$ the worse case is achieved. Let a binary variable v_i denote whether the i-th OU is granted access to access the spectrum. And as said before, the total interference experienced at cell j from the set of active OUs $\mathcal{S}_A$ is $\mathcal{I} = \sum_{i \in \mathcal{S}_A} I_{ij}$.

To guarantee the privacy of the IU, we enforce that the $\mathcal{I} \leq I_{TH}$, *for every cell inside the PZ* (not only the IU's cell). Otherwise, if some cell in the PZ does not meet the interference constraint, the adversary can easily deduce that the IU is not located in that cell. Thus, in the IU's optimization formulation, this interference constraint must be the same for every cell in the PZ to prevent OUs from inferring of the IU's true location. Recall that the utility of OUs corresponds to number of active OUs. Alternatively, this can also be represented as the aggregated communication capacity of all the active OUs (neglecting the scheduling and interference among them). The capacity C_i of the i-th OU is $B \log_2(1+\frac{P_i}{N_o})$, where P_i is the ith OU's maximum power which is assumed to be a constant P_o, and N_o is the noise power and B is the bandwidth. Note that OUs' utility is important for the spectrum access system as well, as OUs pay it for spectrum access.

Summarizing, to maximize OUs' utility and limit the interference to the IU while maintaining achieving privacy, we

formulate the DOL problem according to choose F_3. We choose for F_3 because it is hard for the IU to put a U_{TH} that satisfy all the OUS as follows:

$$DOLP: \quad \max_{\mathbf{v}} \quad \sum_{i=1}^{N} \frac{B}{N} \log_2(1 + \frac{P_i v_i}{N_o}), \tag{6}$$

$$\text{s.t.} \quad 0 \leq v_i \leq 1; \quad \forall i = 1...N \tag{7}$$

$$\sum_{i=1}^{N} I_{ij} v_i \leq I_{TH}; \quad \forall j \in \text{PZ}, \tag{8}$$

where v_i is the decision variable. Note that, to avoid an integer program, we use a continuous decision variable v_i to denote the percentage of maximum power P_o that the i-th OU can transmit at. When $v_i = 0$, OU is denied access completely by the SAS. If $v_i = 1$ the OU can transmits with full power. If $0 \leq v_i \leq 1$, the OU transmits with $P_i v_i$ can also be viewed as the probability of shutting down the ith SU. The interference constraints are presented in (7). This problem is a convex optimization problem with linear constraints. Thus, this problem can be solved in polynomial time. We use set $\mathcal{S}_D$ to denote those OUs denied access. The procedure of DOL is described in **Algorithm** 1.

Algorithm 1: DOL procedure.

Input: I_{TH}, $\mathcal{Y}$, N, P_o and x.
Step 1: Given the desired level of privacy, K is chosen, and given K, the PZ's overall shape is formed such that the cells are contiguous.
Step 2: The IU selects uniformly at random PZ from the group of all sets with size K that contain x.
Step 3: The IU solves the $DOLP$.
Output: $\mathcal{S}_{\mathcal{D}}$, $\mathcal{S}_{\mathcal{A}}$ and $\{v_i, \forall i \in \mathcal{S}_A\}$ is sent to SAS

Let's reason about why privacy is achieved in this case. First, all the PZ cells experience interference no more than I_{TH} as a result of the interference constraint. Secondly, since the IU's location is randomly fitted to one of the PZ cells, and the optimization solution is deterministic given the PZ, no matter what is the pattern of the actual interference experienced by all the points in PZ, it is uncorrelated with the IU's true location. In other words, the posterior probability $P(X = x|PZ)$ will be uniform over all the PZ cells such that

$$P(X = x|PZ) = \frac{1}{K}. \tag{9}$$

D. The Probabilistic OU Location (POL) Case

In reality, knowing the OUs locations may not be practical. Also, the optimal solution of the DOLP changes as the OUs move. In this section, we analyze the case where the OU spatial distribution is statistically known. To make the tradeoff analysis tractable, we assume that the OUs are distributed over an infinite area around the IU with density λ users per unit area according to a Poisson point process [29], which is equivalent to the uniform distribution in the a 2D space. Although the OU locations may follow a different spatial distribution, a Poisson process allows us to analytically quantify the privacy, interference, utility tradeoff. The results qualitatively extend to other spatial distributions. Another advantage of the probabilistic location model is that, the detailed location information of each OU is not disclosed to the IU or SAS, which protects the OUs' location privacy. The query procedure can be protected using privacy-preserving computation schemes.

The IU does not know the active number of OUs nor their exact locations. In POL, the PZ is a circular area with a perturbed location x' as its center and radius r_1, where x' is drawn randomly and uniformly from a another circular with radius r_u. This step is necessary to make sure that the x' doesn't have any relation with x other than they are included in the same circle. Also, we use the uniform distribution to choose x', will decrease the privacy. For example, suppose we have the Laplacian distribution for choosing x'. In this case, the OU will implicitly know that choice of x' will always be concentrated around x', a property of Laplacian distribution [30], which will decrease the efficiency of the PZ. In order to maximize the IU's security, the PZ needs to be carefully designed. Also, in order to limit the interference at the IU, we surround the IU with another protective circular region called the EZ with radius r_2 as shown in Fig. 5. Inside the EZ, the OUs are shut down by a request made by the IU to the SAS. Therefore, the IU can control the interference it experiences by shrinking and expanding the EZ ,i.e, decreasing or increasing r_2. However, to achieve location indistinguishability, the interference experienced by all the PZ points must be below the same threshold I_{TH}.

Since the SAS cannot know the detailed location of each OU, it cannot calculate the corresponding interference generated by each individual OU to the IU. Instead, the interference now on a certain point y on the PZ is sum off the interferences caused by all the OUs, outside EZ, that surrounding y. However, we only know the λ on a circular area A with a variable radius r which ranges from $r_2 - r_1$, because there is no OUs inside the EZ, to ∞. For every value of r, a circle has an average number of OUs = $2\pi r\lambda$ and each OU on this circle $B(y, r)$ produces interference $P_o r^{-\eta}$. Therefore, to calculate the aggregated interference I_A of A on y, we must integrate over all the values of r:

$$I_A = \int_A P_o r^{-\eta} \lambda (2\pi r)\, dr. \tag{10}$$

We have the following remarks about (10). First, as depicted in Fig.5, we only calculate the interference at boundary point on the PZ because that all the boundary points are equivalent due to symmetry and because any point on the boundary receives more interference than the interior point. In other words, the interference decreases as we go inside the PZ, hence all PZ points experience interference less than I_{TH} if the interference calculated at y is less than I_{TH} (see Appendix C). Second, As the EZ and PZ are concentric, (10) cannot be applied over all the values of r because between $r_2 - r_1 \leq r \leq r_2 + r_1$ (Case1) not all the circumference of the circle $B(y, r)$ causes interference as a part of it hides inside the EZ. However, when $r_2 + r_1 \leq \infty$ (Case2), all of $B(y, r)$ cause interference at y as seen in Fig.5 and Fig.6. For each

case of r, we calculate the two interference values I_1 and I_2. We present the detailed derivations in Appendices A and B.

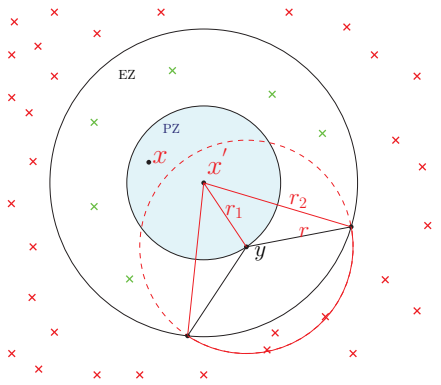


Figure 5: Case 1: $r_2 - r_1 \leq r \leq r_2 + r_1$.

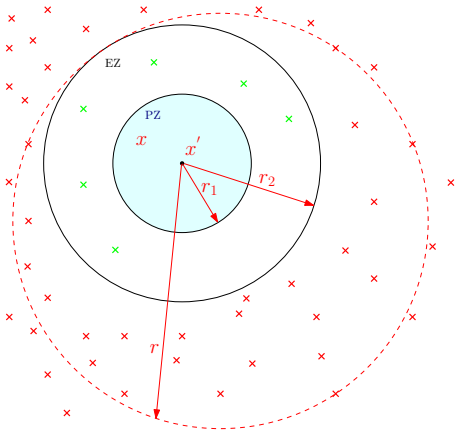


Figure 6: Case 2: $r_2 + r_1 \leq \infty$.

As mentioned earlier, the privacy increases when $P(X = x|x^{'})$ becomes uniform or in other words, when $P(X = x|x^{'}) = 1/\pi r_1^2$. Now, to maximize the privacy and limit the interference, we use F_1 to formulate the three-way tradeoff which is equivalent to F_2, i.e., they give the same solution under the same conditions. The formulation is given by:

$$POLP: \max_{r_1} \quad \pi r_1^2, \tag{13}$$

$$\text{s.t.} \qquad 0 \leq r_1 \leq r_2 \tag{14}$$

$$(I_1 + I_2) \leq I_{TH}; \quad \forall y \in PZ, \tag{15}$$

where (14) makes sure that the PZ inside the EZ. Also, note that by fixing r_2, we solve for a certain OU utility as the EZ represents the area that contains the OUs which will be shutdown. (15) makes sure that the interference is below I_{TH}.

$POLP$ is a non-linear optimization problem because of constraint (15). We propose the optimality condition decomposition (OCD)-based method to solve $POLP$. Given that the problem has a convex/concave objective function, OCD is an iterative method that is proved to converge to the optimal solution in a cubic time by trying to approach satisfying a non-linear constraint, such as 15, by small steps represented by iterative updates. The updating continuous until the update

Algorithm 2: OCD Algorithm

- Formulate the Lagrangian function $\mathcal{L}(r_1, \mu) = \pi r_1^2 + \mu(I_1 + I_2)$, where μ is a Lagrange multiplier.

for $t = 1, \cdots, T$ **do**

- Calculate the gradients $\nabla_{r_1}\mathcal{L}(r_1, \mu)$ and $\nabla^2_{r_1}\mathcal{L}(r_1, \mu)$. Then, solve the following equation for the updates $\triangle r_1$ and $\triangle\mu$ of r_1 and μ respectively

$$\nabla^2\mathcal{L}(r_1, \mu) = -[\triangle r_1, \triangle\mu]^\top \nabla\mathcal{L}(r_1, \mu). \tag{11}$$

- Update r_1 and μ as follows:

$$r_1 = r_1 + \triangle x, \;\; \mu = \mu + \triangle\mu. \tag{12}$$

- Check convergence

if $[\triangle r_1, \triangle\mu] \leq [\epsilon_1, \epsilon_2]$ **then**

- **Stop**

else

- **Continue**

end if

end for

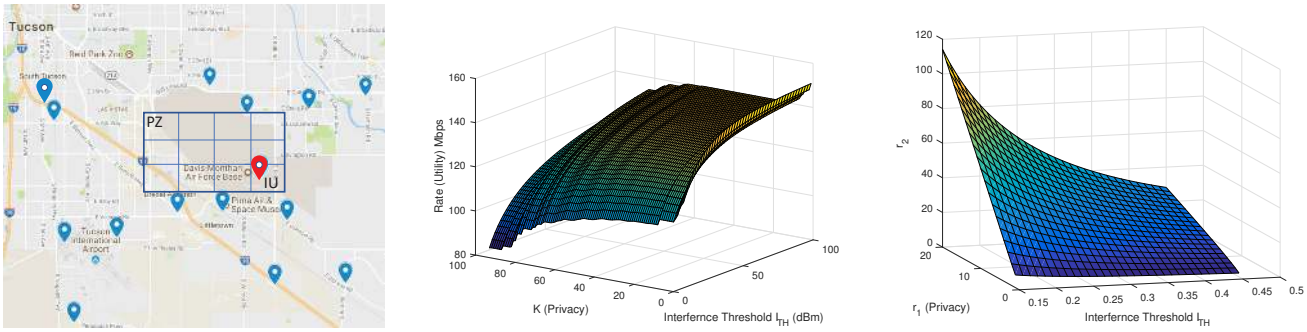
is zero, meaning that the constraint is met or until the update is less than a very small threshold. Due to the complexity of constraints, we present the detailed procedures of our proposed OCD method in Algorithm 2. The OCD algorithm is a modified version of the Lagrangian relaxation (LR) where we solve the Newton equation in (11) to get the updates instead of solving the dual Lagrangian problem as in (LR). The algorithm converges to zero within a very 12 iterations at most as seen in Fig. 11. The solution is considered to be optimal as the updates converges to zero which happens in our case. Another issue is how to choose the convergence constant ϵ. ϵ should be chosen proportionally to the values of r_1 and μ. For example $\epsilon_1 = 10^{-4}$ can be a good choice when $r_1 = 100$, but it will be not suitable when $r_1 = 10$ and the same thing applies for μ. Therefore, a safe choice is to select ϵ_1 to be very as small.

Algorithm 3: POL procedure

Input: x, I_{TH}, λ and r_2.
Step 1: The interference at the boundary of PZ is calculated as the sum of interference in two cases:
1) Case 1: $r_2 - r_1 \leq r \leq r_2 + r_1$.
2) Case 2: $r_2 + r_1 \leq r \leq \infty$.
Step 2: Solve POLP with inputs I_{TH}, λ and r_2, obtain r_1^*.
Step 3: The perturbed location $x^{'}$ is selected uniformly at random from $B(x, r_1^*)$, PZ is the disk $B(x', r_1^*)$.
Step 4: The EZ is centered at $x^{'}$ and has a radius of r_2.
Output: IU outputs EZ, PZ and sends them to SAS.

V. Evaluation

In this section, we evaluate the privacy, utility, interference tradeoff under the DOL and POL models.



(a) (b) (c)

Figure 7: (a) Topology of a real-world deployment, (b) DOL: the three-way tradeoff, (c) POL: the three-way tradeoff.

A. The Tradeoff under the DOL model

For the DOL model, we consider the real-world scenario depicted in Fig. 7(a). The IU is located inside a military base with the PZ being divided into $K = 12$ cells. However, in simulations, we range K from 1 to 100. For paper anonymity purposes we do not reveal the true dataset used. This will become available in the camera-ready version. The IU's original location x lies at the red pin. Thirteen base stations (blue pins) that belong to different mobile operators represent OUs whose locations are known. Google Maps was used to draw this figure. For a cell j inside the PZ, we measure the distances in kilometers and the interference and power in dBms. Using the interference value at each cell, the IU solves the DOLP in (6) and determines the set of OUs that are denied access so that the I_{TH} is satisfied, the privacy is implicitly achieved and the OUs' utility is maximized.

In Fig. 8, we show the total rate, derived by substituting the optimal solution of (6) in it's objective, as a function of I_{TH}. We observe that as I_{TH} increases, the rate increases until it saturates. In other words, the OUs can transmit at the same rate for a much tighter I_{TH}.

In Fig. 9, we show the rate as a function of P_o, when $I_{TH} = 100dBm$. We observe that increasing P_o has the same effect on the OU's rate, as increasing the I_{TH}.

In Fig. 10, we show the tradeoff between the OUs' utility, represented by rate, against the privacy level represented by the number of privacy cells in the PZ. As we increase the privacy, the average rate decreases due to the interference constraint which leads to more OUs being denied access. Fig. 7(b) shows the three-way tradeoff where we can see that increasing privacy cells from 0 to 15 while tightening I_{TH} only degrades the rate by a small amount.

B. The Tradeoff under the POL Model

Simulating POL goes as follows. If we have chosen to fix the EZ radius r_2, first, we initialize r_1, λ by zeros. Second, we calculate $\nabla_{r_1}\mathcal{L}(r_1, \mu)$ and $\nabla^2_{r_1}\mathcal{L}(r_1, \mu)$ and solve (11) which gives us the update values. Third, we update the current values of r_1, μ using $\triangle r_1$ and $\triangle\mu$ and check for convergence. Note that the distances in POL simulation are relative.

Fig. 11 shows the convergence of optimal r_1. Typically, we obtain the steady state value of r_1 after 10 to 15 iterations.

In Fig. 12, we plot the I_{TH} against the optimal r_1 for different r_2 values. We notice that as we allow more interference from the OUs, the PZ radius r_1 increase to approaches r_2. In other words, IU's privacy (PZ area) increases to defy the effect of increasing I_{TH}. Specifically, as a reaction for increasing I_{TH}, r_1 increases to decrease the chance that IU be on PZ's boundary has more interference. This case studies fixing a EZ and trying to obtain the best PZ for it. On the other hand, to have fixed PZ with controllable EZ, we can use F_3 to formulate POLP to calculate the optimal r_2, like Fig. 13. We can see that as the allowable interference I_{TH} increases the EZ shrinks as less OUs are required to shut down. Also, as P_o increases, the EZ expands to decrease the interference on the PZ.

In Fig. 14, we plot I_{TH} against the ratio r_1/r_2. We can see that as I_{TH} increases, the ratio approaches 1, which is the optimal condition we might have when the PZ and the EZ are exactly the same. However, because the chance of having a OUs close to the boundary of the PZ, and get close to IU, this ratio never reaches 1 as (11) doesn't have a solution.

In Fig. 15 and Fig. 16, we see the effect of increasing P_o on r_1 and increasing λ on r_2. We can deduce that increasing P_o makes the PZ shrinks so that the IU be as far as possible from the nearest interferer. However, increasing λ is equivalent to increase interference which is overcame by expanding r_2.

In Fig. 7(c), we plot OUs' lost transmission opportunity, represented by EZ radius r_2, against privacy, represented by PZ radius r_1 and interference. The area of EZ gives the relative amount of OUs that are shut down which is an appropriate complement measure of utility. In Fig. 7, we can see that the lost opportunity and privacy are proportional meaning that we can't increase a quantity without decreasing the other. For example, if we increase the utility, i.e., decreasing the EZ and increasing the interference on the PZ, the PZ shrinks in order to be as far as possible from the OUs and as a result the IU privacy is compromised with having a smaller PZ.

VI. Conclusion

In this paper, we studied the three-way tradeoff among IU's location privacy, interference, and the OUs' utility. We introduce the novel concept of a privacy zone within an exclusion zone, to simultaneously achieve privacy and guarantee interference. Under two models with either known or

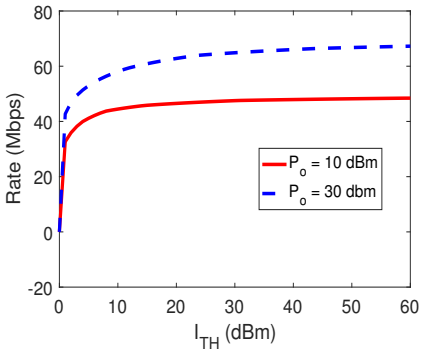


Figure 8: I_{TH} vs. Rate.

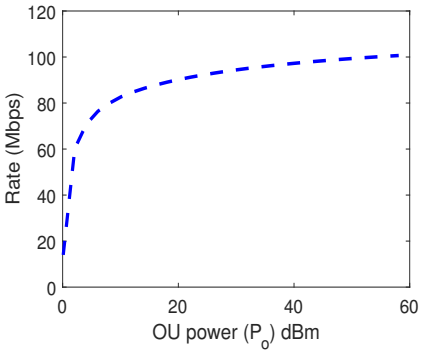


Figure 9: Power level vs. Rate.

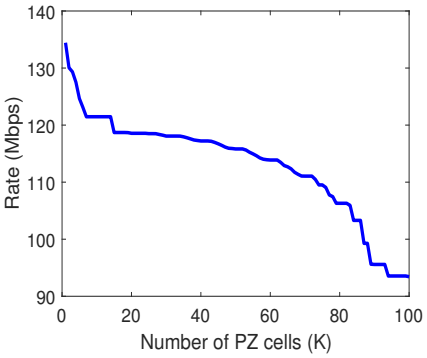


Figure 10: PZ cells vs Rate.

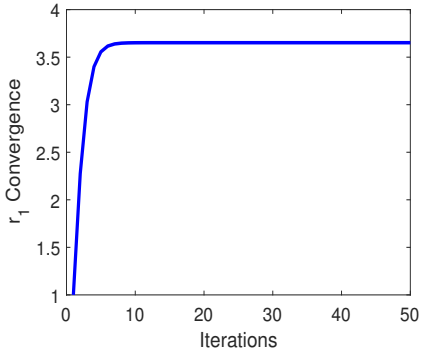


Figure 11: Iterations vs. r_1 Conv.

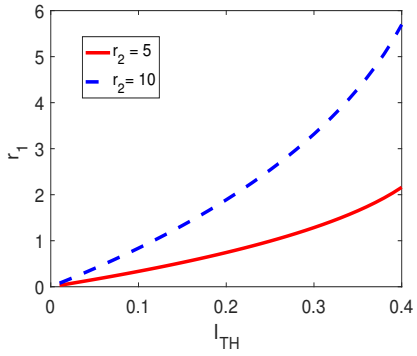


Figure 12: I_{TH} vs. r_1.

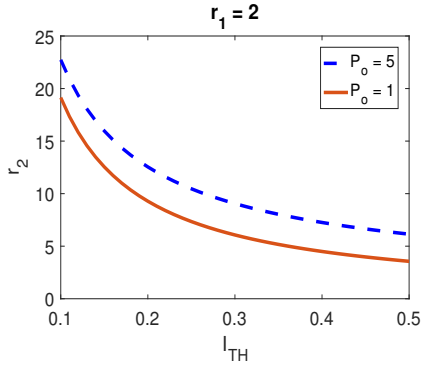


Figure 13: I_{TH} vs. r_2.

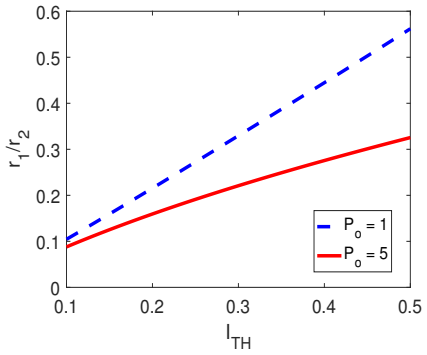


Figure 14: I_{TH} vs. r_1/r_2 ratio.

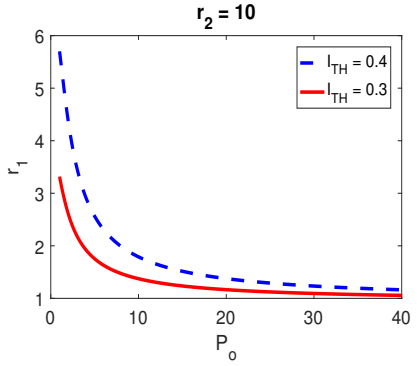


Figure 15: OU power (P_o) vs. r_1.

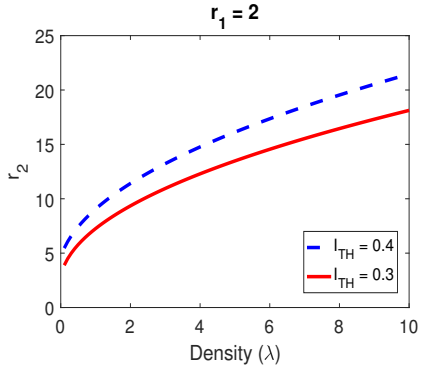


Figure 16: r_2 vs. λ.

probabilistic OU locations, we derive optimized solutions to minimize/maximize one of the objectives subject to two other objectives given. The simulation results show that the the IU's privacy increases with the allowable interference. Also, it shows that the OUs' utility decrease as the privacy increases. For future work, we will extend to mobile OU settings, and consider privacy protection of the frequency and time domains of IU's operations. In addition, we will study the three-way tradeoff from a game-theoretic perspective.

VII. APPENDIX

A. *Case 1:* $r_2 - r_1 \leq r \leq r_2 + r_1$

. We calculate the interference resulting from changing r between $[r_2 - r_1, r_2 + r_1]$ because before $r_2 - r_1$, the interference circle would be inside the EZ and after $r_2 + r_1$, the calculation differs. Fig.5 shows *case 1*. To calculate the interference on the boundary point y in *case 1* we reuse 10 as follows:

$$I_1 = \int_{r_2 - r_1}^{r_2 + r_1} P_o r^{-\alpha} \lambda A_{arc} dr, \tag{16}$$

where A_{arc} is the circumference of the arc that results from the intersection between the EZ and the interference circle (the intersection is the solid red arc) and I_1 is the interference in *case 1*. A_{arc} is given as follows:

$$A_{arc} = \frac{4\pi r \lambda}{360} cos^{-1} \frac{r_1^2 + r_2^2 - r^2}{2 r_1 r_2}. \tag{17}$$

The integration in (16) doesn't have a closed form solution, so we use the approximation used in [31] to have a closed form integral. The approximation is given as follows:

$$cos^{-1}(x) = \frac{\pi}{2}(1 - 2.55 \frac{x(1 - .61\sqrt{1 - x^2})}{1.55 + x^2}). \tag{18}$$

This approximation gives an error margin less than 0.5% as indicated in [31]. After substituting (18) in (17), setting $\alpha = 3$ [32], [33] and doing the integration, the result becomes:

$$I_1 = \frac{P_o \lambda \pi}{2} \frac{6222\pi r_1^3 - 200\left(31r_1^2 - 102r_2r_1 + 31r_2^2\right)\ln\left(\frac{r_2-r_1}{r_1+r_2}\right)}{6200\left(r_2r_1^3 + r_2^3r_1\right)}. \tag{19}$$

B. Case 2: $r_2 + r_1 \leq r \leq \infty$

. In *case 2*, we calculate the interference beyond the arc of *case 1*, i.e., the interference will be calculated for the OUs exist on the complete circle at the center y. Fig.6 shows *case 2*. The interference is calculated as follows:

$$I_2 = \int_{r_2+r_1}^{\infty} (P_o r^{-\alpha})(\lambda 2\pi r) dr = 2\pi P_o \lambda \frac{(r_2 + r_1)^{2-\alpha}}{\alpha - 2}. \tag{20}$$

C. The Interior has less interference

To prove that the boundary of PZ has more interference than its interior, we must prove that the $I_1 + I_2 \propto r_1$.

Theorem VII.1. *The interference is increasing with r_1, in other words, $\nabla_{r_1}(I_1 + I_2) > 0$*

Proof. Using Leibniz rule we have:

$$\nabla_{r_1}(I_1 + I_2) = \frac{\pi - 1}{(r_1 + r_2)^2} + \int_{r_2-r_1}^{r_2+r_1} r^{1-\alpha} \frac{r_2^2 - r_1^2 - r^2}{2r_2r_1^2\sqrt{1 - \frac{(r_2^2+r_1^2-r^2)^2}{4r_1^2r_2^2}}}\, dr. \tag{21}$$

The integration $\mathcal{I}$ in (21) has no solution, so we take the upper-bound of its denominator $g(r_1)$ in order to have a lower-bound on $\mathcal{I}$ and hence, a lower bound on the gradient itself. The upper bound on $g(r_1)$ is obtained by getting the maximum value for r_1 and then substitute back in $g(r_1)$. The upper bound on $g(r_1)$ is $4r_2^3r^2r_2^2$ and After doing the integration $\mathcal{I}$ we have:

$$\mathcal{I} = \frac{r_1}{3r_2(r_2^2 - r_1^2)}. \tag{22}$$

Consequently we have:

$$\nabla_{r_1}(I_1 + I_2) \geq \frac{\pi - 1}{(r_1 + r_2)^2} + \frac{r_1}{3r_2(r_2^2 - r_1^2)} > 0. \quad \square \tag{23}$$

References

[1] I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, and S. Mohanty, "Next generation/dynamic spectrum access/cognitive radio wireless networks: a survey," *Computer Networks*, vol. 50, no. 13, pp. 2127–2159, 2006.

[2] F. C. Commission *et al.*, "White space database administration," 2016.

[3] Google, *Google Spectrum Data Base*, 2013. [Online]. Available: https://www.google.com/get/spectrumdatabase/

[4] Microsoft, *Microsoft White Spaces Database*, 2009. [Online]. Available: http://whitespaces.microsoftspectrum.com/

[5] F. C. Commission *et al.*, "Enabling innovative small cell use in 3.5 ghz band nprm & order," *FCC 12*, vol. 148, 2012.

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

[7] A. R. Beresford and F. Stajano, "Location privacy in pervasive computing," *IEEE Pervasive computing*, vol. 2, no. 1, pp. 46–55, 2003.

[8] M. Duckham and L. Kulik, "A formal model of obfuscation and negotiation for location privacy," in *International Conference on Pervasive Computing*. Springer, 2005, pp. 152–170.

[9] L. Sweeney, "Achieving k-anonymity privacy protection using generalization and suppression," *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, vol. 10, no. 05, pp. 571–588, 2002.

[10] A. Babaei, M. Haenggi, P. Agrawal, and B. Jabbari, "Interference statistics of a poisson field of interferers with random puncturing," in *MILITARY COMMUNICATIONS CONFERENCE, 2011-MILCOM 2011*. IEEE, 2011, pp. 384–388.

[11] R. W. Heath, M. Kountouris, and T. Bai, "Modeling heterogeneous network interference using poisson point processes," *IEEE Transactions on Signal Processing*, vol. 61, no. 16, pp. 4114–4126, 2013.

[12] R. E. Miles, "On the homogeneous planar poisson point process," *Mathematical Biosciences*, vol. 6, pp. 85–127, 1970.

[13] D. P. Bertsekas, *Nonlinear programming*. Athena scientific Belmont, 1999.

[14] A. J. Conejo, E. Castillo, R. Minguez, and R. Garcia-Bertrand, *Decomposition techniques in mathematical programming: engineering and science applications*. Springer Science & Business Media, 2006.

[15] M. Grissa, B. Hamdaoui, and A. A. Yavuza, "Location privacy in cognitive radio networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 3, pp. 1726–1760, 2017.

[16] 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.

[17] E. FCC, "Docket no. 08-260,"," *Second Report and Order and Memorandum Opinion and Order," Nov*, 2008.

[18] M. Gruteser and D. Grunwald, "Anonymous usage of location-based services through spatial and temporal cloaking," in *Proceedings of the 1st international conference on Mobile systems, applications and services*. ACM, 2003, pp. 31–42.

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

[20] L. Zhang, C. Fang, Y. Li, H. Zhu, and M. Dong, "Optimal strategies for defending location inference attack in database-driven crns," in *Communications (ICC), 2015 IEEE International Conference on*. IEEE, 2015, pp. 7640–7645.

[21] H. Li, Q. Pei, and W. Zhang, "Location privacy-preserving channel allocation scheme in cognitive radio networks," *International Journal of Distributed Sensor Networks*, vol. 12, no. 7, p. 3794582, 2016.

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

[23] C. Dwork, "Differential privacy," in *Encyclopedia of Cryptography and Security*. Springer, 2011, pp. 338–340.

[24] J. Krumm, "A survey of computational location privacy," *Personal and Ubiquitous Computing*, vol. 13, no. 6, pp. 391–399, 2009.

[25] E. Troja and S. Bakiras, "Efficient location privacy for moving clients in database-driven dynamic spectrum access," in *Computer Communication and Networks (ICCCN), 2015 24th International Conference on*. IEEE, 2015, pp. 1–8.

[26] Y. Dou, H. Li, K. C. Zeng, J. Liu, Y. Yang, B. Gao, and K. Ren, "Preserving incumbent users' privacy in exclusion-zone-based spectrum access systems," in *Distributed Computing Systems (ICDCS), 2017 IEEE 37th International Conference on*. IEEE, 2017, pp. 2486–2493.

[27] Z. Chen, L. Chen, and H. Zhong, "Towards secure and verifiable database-driven spectrum sharing," in *Dependable Systems and Networks (DSN), 2017 47th Annual IEEE/IFIP International Conference on*. IEEE, 2017, pp. 285–296.

[28] J. B. Andersen, T. S. Rappaport, and S. Yoshida, "Propagation measurements and models for wireless communications channels," *IEEE Communications Magazine*, vol. 33, no. 1, pp. 42–49, 1995.

[29] J. F. C. Kingman, *Poisson processes*. Wiley Online Library, 1993.

[30] R. S. Burington and D. C. May, "Handbook of probability and statistics with tables," 1970.

[31] E. Seevinck, "Simple, wide-range approximations to trigonometric and inverse trigonometric functions useful in real-time signal processing," in *IEE Proceedings G (Electronic Circuits and Systems)*, vol. 128, no. 1. IET, 1981, pp. 41–45.

[32] M. Haenggi, "On distances in uniformly random networks," *IEEE Transactions on Information Theory*, vol. 51, no. 10, pp. 3584–3586, 2005.

[33] D. Moltchanov, "Distance distributions in random networks," *Ad Hoc Networks*, vol. 10, no. 6, pp. 1146–1166, 2012.