To appear in *IEEE DySPAN*, March 2017

# Location Privacy from Dummy Devices in Database-Coordinated Spectrum Sharing

Nirajan Rajkarnikar
Dept. of Engineering & Public Policy
Carnegie Mellon University *and*
Faculdade de Engenharia
Universidade do Porto
nrajkarn@alumni.cmu.edu

Jon M. Peha
Dept. of Engineering & Public Policy
Dept. Electrical & Computer Engineering
Carnegie Mellon University
Pittsburgh, USA
peha@cmu.edu

Ana Aguiar
Faculdade de Engenharia
Universidade do Porto
Porto, Portugal
anaa@fe.up.pt

***Abstract*— One way to make more spectrum available is through *white space* sharing, where secondary spectrum users are allowed to transmit from any location except inside *exclusion zones* (EZs) that are drawn around primary spectrum users (PUs). However, EZ boundaries reveal the locations of PUs, and for some devices, *location privacy* is extremely important. Location privacy can be improved by increasing the area blocked inside EZs, but this decreases *spectrum utilization efficiency*. This paper derives a Pareto optimal strategy that builds on two such approaches: generating dummy PUs and creating EZs around them, and making EZs larger than needed for interference protection alone. We find that in many circumstances, including cases where an attacker threatens a jamming attack, the optimal strategy is to maximize the number of dummy PUs while making EZs as small as possible. In the remaining circumstances, the optimal strategy is to generate no dummy EZs. We derive the Pareto optimal results achieved by using whichever of these strategies is best for given circumstances, and show that the results are far superior to those achieved with some previously proposed algorithms. Moreover, with our approach, even a small increase in the amount of area blocked from secondary use can greatly improve location privacy for PUs, although as more and more area is blocked, there are diminishing returns.**

***Keywords*— *spectrum sharing; location privacy; location confidentiality; dummy generation; obfuscation; spatial cloaking; database-driven cognitive radio network (CRN)***

## I. Introduction

Demand for spectrum is increasing rapidly [1]. Meeting this demand will increase public welfare and foster economic growth [2]. One way to make more spectrum available to meet this demand is through hierarchical sharing approaches such as primary-secondary schemes [3], [4] whereby lower-priority devices are only allowed to transmit if they do not cause harmful interference to protected devices. One way to do this is *white space* sharing, in which *Exclusion Zones* (EZs) are drawn around Primary Users of spectrum (PUs). All PUs have receivers that require protection from interference, and many have transmitters as well. Secondary Users (SUs) are transmitters that are allowed to transmit normally anywhere outside of EZs, and are not allowed to transmit inside EZs.[1] (An alternative is *gray space* sharing, where SUs adjust dynamically to PUs in some regions [5]–[8]). EZ information can be stored in a Geolocation Database (GDB), and SUs can determine whether they are allowed to transmit at a given location by querying that GDB. Spectrum regulators have already adopted this form of sharing in some bands, and it has been suggested that similar approaches be adopted more broadly [9]. For example, this form of spectrum sharing has been implemented in the TV band in a number of countries [10], [11], in the 3.5 GHz band in the US [12], and using the Licensed Shared Access (LSA) approach in Europe [13].

However, revealing information about EZs can threaten operational security (OPSEC) [14], [15]. An attacker can use the location and shape of EZs to undermine the PU's *location privacy*, i.e. to infer information about where PUs are located. Information about EZs can be obtained in a variety of ways, including making a series of queries to a GDB, intercepting the queries of other devices, or compromising a GDB directly [16], [17]. While PU location privacy is not a concern where PU operational characteristics are publicly known, as is the case for white space sharing in the TV band, location privacy can be extremely important in other cases. For example, the 3.5 GHz band in the U.S. and 2.3-2.4 GHz LSA band in Europe [18] contain military radars, satellite ground stations, air traffic control, and telemetry devices, for which location privacy can be important for national security [19], [20], [21]. Figuring out how to protect location privacy is critical for the implementation of spectrum sharing in these cases.

This paper will address this important problem by exploring solutions that allow efficient spectrum sharing while protecting PU location privacy. One goal of this research is to find strategies that maximize both spectrum utilization efficiency and location privacy to the extent possible, i.e. that achieve as much location privacy as possible for a given spectrum utilization efficiency and as much spectrum utilization

[1] Note that this is the definition of EZs used in this paper, but it is just one of three commonly used definitions [5].

Support for this research was provided by the Fundação para a Ciência e a Tecnologia (FCT, Portuguese Foundation for Science and Technology) through the Carnegie Mellon Portugal Program under Grant SFRH/BD/52159/2013.

efficiency as possible for a given location privacy. The other goal is to understand the inevitable tradeoff between spectrum utilization efficiency and location privacy, to help policymakers determine when the loss of one is worth the gain in the other. We use a combination of analysis and Monte Carlo simulation to achieve these research objectives.

This paper examines ways to protect location privacy even when attackers know the EZs by making the area covered by EZs larger than it needs to be for interference protection only. This can be done by (1) generating dummy PUs and blocking off EZs around them, (2) making EZs larger than the minimum needed for interference protection alone and offsetting them such that PU location within the EZ is unpredictable, or (3) some combination of the two.

The defender strategy affects both objectives: location privacy and spectrum utilization efficiency. Our location privacy metric *(P)* is the *number of real PUs that an attacker could harm* by an attack at the location that appears to the attacker to be most worth attacking. PUs are considered harmed if they are within the impact area of the attack location, as would be appropriate for a jamming attack or a kinetic attack. An attacker that knows more about the locations of PUs can pick a better attack location, thereby harming more PUs. Thus, a lower value of *P* implies better location privacy for the defender.

The other objective is maximizing spectrum utilization efficiency. SUs are allowed to transmit from any location outside the EZs. Thus, our spectrum utilization efficiency metric is the *fraction of area covered by EZs (B)*. If this metric is low, then spectrum utilization efficiency is high.

Section II presents some past related work. Section III presents the defender and attacker strategies. Section IV uses analysis to derive the Pareto optimal defender strategy and its effectiveness in the simplified case where EZs contain at most a single PU. In Section V, we drop this simplifying assumption, and use Monte Carlo simulation to determine the Pareto optimal strategy and its effectiveness. Section VI presents our conclusions and their policy implications.

## II. Related Work

Location privacy has been more widely studied in other contexts. One example is where applications on mobile devices share their location to obtain services, such as driving directions. Location obfuscation techniques in this context include submitting a region in which the device is located instead of the exact location [22], [23], or making additional service requests about locations far from where the device is actually located so that the service provider cannot tell which location is real [21], [24]–[27]. These two approaches have some similarities to making EZs larger than necessary and generating dummy PUs, respectively, in the context of white-space spectrum sharing. However, the issues are distinctly different, as use of incorrect or inaccurate location information does not make some regions unusable for location-based services the way it does with spectrum sharing.

Two approaches proposed to establish EZs that protect location privacy in shared spectrum are *k*-anonymity and *k*-clustering [16], [28], [29] which are based on the *k*-anonymity method devised for statistical databases [30]. In *k*-anonymity, EZs are formed such that their boundaries are the smallest circles that encompass *k* PUs each. In *k*-clustering, all PUs are grouped into the *k* smallest clusters and an EZ is formed around each cluster. We compare the effectiveness of these approaches to ours in Section V(d). A related approach is to extend *k*-anonymity to include *l*-diversity, i.e. at least *l* locations must be included when grouping PUs [28].

Other proposed approaches are closer to those considered in this paper. Some have considered adding random noise to the minimum distance required between a PU and a SU, thereby randomly increasing EZ radius when boundaries are circles [16], [31], or transforming EZ boundaries to polygons [16]. We similarly increase EZ radius to add protection, although deterministically rather than stochastically. If radius is random, then attackers are free to choose between attacking large and small EZs in a way that undermines location privacy. For example, if an attacker is more likely to harm a PU when attacking a smaller EZ, then what matters is the size of the smallest EZ, so variation benefits the attacker. [17] considered using dummy PUs as well as parameter randomization. They estimate how long it would take before an attacker can drive location privacy down to a given level by querying a database, and how adding dummy PUs can improve this metric. These results are instructive. However, none of this previous work compares the approaches quantitatively, or determines what combination of dummy PUs and larger EZ size is optimal for given circumstances, as this paper does.

In those cases where an attacker obtains information about EZs by querying a database, another way to protect location privacy is by limiting queries. For example, the database may not respond to a query from a SU that is not at its stated location [32], or when the database believes that the SU has accumulated too much knowledge [33], [34]. Another proposed approach [31] is to introduce a random element. For example, requests for spectrum might be denied randomly, either irrespective of location, or only if the query is close to an EZ. Approaches like these may improve location privacy in some scenarios, but they do not help when EZs are known to the attacker, which is the case considered in this paper. Even when EZs are determined through queries, limiting queries is of limited help when PU locations change very slowly relative to query rate. Attackers can also learn about EZs in other ways, such as compromising the database, or observing queries from other devices.

## III. Attacker & Defender Strategies

Attackers and defenders are engaged in a zero-sum game; attackers try to maximize location privacy metric *P* and defenders try to minimize it, while allowing as much spectrum as possible to be shared. To defend against an intelligent attack, the defender must assume that the attacker knows the defense algorithm, but not the input parameters. It is also assumed that the attacker knows EZ boundaries. The attacker may know EZ boundaries because they are in a public database, or by making a large number of queries to a database that is not public, or by cooperating with a database operator who is complicit with the attacker, or by compromising the database. Therefore, this model can be applicable even when the GDB acts as an "oracle" that responds to queries with only select necessary information. We also assume that the attacker has no source of information about PU locations other than EZ boundaries. Finally, we assume the attacker knows the interference that a protected PU can tolerate, and the path loss model used by the defender, so the attacker can infer from EZ boundaries which point(s) within the EZ that the defender protected from interference.

The attacker uses its knowledge of defender strategy and the EZ boundaries to determine the point at which the expected number of PUs harmed is highest. Similarly, the defender considers the locations of PUs, and chooses EZ boundaries to minimize the attacker's estimate of expected number of PUs at the point where it is greatest. The following subsections present the defender strategy and the attacker strategy.

### A. *Basic Defender Strategy*

The defender must set EZ boundaries such that every PU is within an EZ and is protected from SU interference. As described in Section I, to protect location privacy, the defender can include more area than is necessary in the EZs by (i) making EZs larger than they need to be and offsetting the EZ such that PU location within the EZ is unpredictable, (ii) creating more EZs than needed, or (iii) some combination of the two.

In cases where the defender generates more EZs than PUs, the first step is to create dummy PUs. Dummy PUs must be indistinguishable from real PUs to an attacker [27]. Thus, the locations of dummy PUs are generated randomly based on a probability distribution that is representative of the possible locations of real PUs. In the next step, EZs are defined around all PUs, both dummy and real, in the same manner. Thus, the size and shape of an EZ tells the attacker nothing about whether that EZ contains a real PU or a dummy PU.

We first consider generating EZs in the case where PUs are sufficiently far apart that no EZ contains more than one. When creating an EZ, the defender first selects an "inner region", which we define as the region that will be protected from SU interference. The defender makes the size and shape of that inner region the same for all EZs. The EZ then consists of all points where an SU transmitter would cause interference above threshold in the inner region. For this section on basic defender strategy, we assume that the defender has already determined the size and shape of this inner region and the number of EZs. Sections IV and V will investigate how a defender should make these choices to best achieve the defender's objectives.

For PUs that are close together, EZs are generated independently around each PU as described above and allowed to overlap. In some cases, the shape of the EZ might reveal to an attacker that there are multiple PUs inside, because the inner region does not have the correct shape for a single PU. In this way, this algorithm is not quite optimal; a defender may wish to make minor adjustments in these cases so that the attacker cannot tell that there are multiple PUs. However, this is close enough to optimal for our purposes.

### B. *Attacker Strategy / Threat Model*

We consider attacks which harm PUs within a certain impact area around the point of attack, such as jamming attacks and kinetic attacks. As described in Section I, our location privacy metric $P$ is the expected number of PUs harmed at the point where this number is greatest. To find this value, the attacker first calculates this expected number at every point, given the EZ boundaries observed and knowledge of path loss, which depends on terrain. The expected number of PUs is 0 outside EZs, and at points close to the EZ boundary where PUs certainly do not exist. For the remaining points, the expected number of PUs per area can be calculated from the area of the inner region. The attacker finds the expected number of PUs near any given location by adding up the expected value of all points within attack's impact area for that location. The attacker then determines the location where this value is highest, which is the best attack location, and this reveals the value of the privacy metric.

## IV. Analytical Determination Of Defender Strategy

The previous section described the basic defender strategy when given the number of dummy PUs and the area of each inner region. In this section, we determine analytically the Pareto optimal values for these parameters. We also explore the tradeoff between location privacy and spectrum utilization efficiency if this Pareto optimal strategy is adopted.

To make the analysis tractable, it is assumed in this section that there is a negligible probability that any two PUs are close enough together to be harmed by a single attack. This assumption is reasonable when the fraction of area within EZs is small. We relax this assumption in Section V. It is also assumed that path loss is isotropic, i.e. depends only on distance. Thus, a PU is protected if it is at least a protection distance $r_0$ away from any SU. Moreover, the danger from an attack depends only on the distance from that attack, so that a PU is harmed from an attack if and only if its distance to the attack location is less than attack radius $r_a$. Finally, we assume that PU locations are uniformly distributed and independent.

With isotropic path loss, for a given EZ area, the shape that maximizes the size of the inner region where a PU might be is a circle. We define $r_{\mathrm{EZ}}$ to be the EZ radius. To create a circular EZ such that a PU could be anywhere except within one protection distance $r_0$ of the edge, the defender randomly chooses a point within $(r_{EZ} - r_0)$ of the actual PU location using a uniform distribution, and makes that the center of an EZ with radius $r_{EZ}$. This algorithm is not quite optimal, in that a defender may wish to make the probability of placing a PU within an attack radius of the boundary slightly greater, but this algorithm is close enough to optimal for our purposes.

From the attacker's perspective, if the inner region of an EZ has a circular boundary, which the attacker can easily determine using its knowledge of EZ boundaries and path loss, then there is only one (real or dummy) PU inside, and its location has a uniform distribution among the points inside the EZ that are not within $r_0$ of the boundary. Thus, the expected number of PUs per area throughout this region is $\frac{1}{\pi\ (\mathrm{r_{EZ}} - \mathrm{r_0})^2}$. If the inner region does not have a circular boundary, then the inner region is the union of overlapping disks, each of which includes one (real or dummy) PU. For each point in such an EZ, the attacker determines how many overlapping disks could conceivably include that point, and multiplies the above estimate of expected PUs per area by that number.

### *A. Finding the Optimal Number of Dummy PUs (f)*

In this section, we determine the defender strategy that optimizes location privacy metric *P* for a given spectrum utilization efficiency. More specifically, we determine the fraction *f* of dummy PUs out of total PUs that minimizes *P* for a given fraction of area blocked by EZs *B*. Results depend on the density of real PUs, i.e. average number of real PUs per area, which we define to be *d*. At a constant *B* and *d*, increasing *f* would increase the number of EZs but decrease the radius $r_{EZ}$ of each EZ, so increasing *f* could either increase or decrease location privacy *P*. We first derive *P* as a function of *f*, *B*, *d*, minimum protection distance $r_0$, and attack radius $r_a$. For a given *B*, the $r_{EZ}$ is largest when $f = 0$, i.e. when there are no dummy PUs and all blockable area is used to enlarge EZs around real PUs. We call this $r_{EZ}$ value $r_{max}$. These variable definitions are summarized in Table I.

Assumptions made for analytical simplicity in this section are:

- No two EZs *i* and *j* are close enough that a PU in EZ *i* and a PU in EZ *j* are within an attack radius of a single point.
- PUs are uniformly distributed across an infinite plane, so edge effects can be ignored.

PUs need to be inside EZs and at least a minimum protection distance $r_0$ away from the EZ boundaries, so a PU can only exist within the inner circle at the center of the EZ with the radius of $(r_{EZ} - r_0)$. If $(r_{EZ} - r_0)$ is less than the attack radius $r_a$, then the attacker always hits the PU if it attacks the center of that EZ, and by assumption for this section, an attacker can never attack two EZs at once. Thus, the expected number of PUs hit is the probability that an EZ has a PU, which is $(1-f)$. On the other hand, if $(r_{EZ} - r_0) > r_a$, then an attack may not hit the PU. The defender algorithm makes it equally likely that the PU is at any point within this inner circle of radius $(r_{EZ} - r_0)$. Therefore, the best achievable expected number of PUs hit is *the probability that an EZ has a PU* times *the area within an attack radius* divided by *the area where a PU in that EZ could be*, which is $(1-f) \times \frac{\pi\, r_a^2}{\pi\,(r_{EZ}-r_0)^2}$

TABLE I. SYSTEM VARIABLES AND THEIR DESCRIPTIONS

| **Variable** | **Description/Definition** |
|---|---|
| $B$ | fraction of area blocked by EZs |
| $f$ | fraction of dummy PUs out of total PUs |
| $D$ | Avg. density of real PUs, i.e. avg. number of real PUs per area |
| $r_a$ | radius within which the attack can harm a PU |
| $r_0$ | Minimum protection distance of the PUs |
| $r_{EZ}$ | radius of EZ |
| $r_{max}$ | radius of EZ at *f* = *0*. This is the largest EZ radius for a given *B* value and given *d*. |
| $P$ | Location Privacy Metric i.e. no. of PUs hit by an attack of radius $r_a$ |

$$\therefore \mathit{Expected\ number\ of\ real\ PUs\ hit}, P =$$

$$\begin{cases} (1-f) \times \frac{r_a^2}{(r_{EZ}-r_0)^2}, \ if\ r_a \le (r_{EZ} - r_0) \\ \\ (1-f), \ if\ r_a \ge (r_{EZ} - r_0) \end{cases} \tag{1}$$

where radius of each EZ ($r_{EZ}$) can be calculated as:

$$r_{EZ}(B,f,d) = \sqrt{\frac{B}{\frac{d}{1-f} \times \pi}} \tag{2}$$

From the equations above, we prove the following theorems:

1) Location privacy metric *P* increases with *f* when EZ radius $r_{EZ}$ > attack radius $r_a$ + minimum protection distance $r_0$

2) Location privacy metric *P* decreases with *f* when EZ radius $r_{EZ}$ < attack radius $r_a$ + minimum protection distance $r_0$

3) Corollary 1: if there is a value of *f* at which exclusion zone radius $r_{EZ}$ = attack radius $r_a$ + minimum protection distance $r_0$, then *P* is greatest at this value of *f*

4) Corollary 2: Location privacy metric *P* is smallest either when *f=0* or when *f* is at maximum feasible value $f_{max}$

*Proof for Theorem 1*: When $r_{EZ} \ge (r_a + r_0)$ or equivalently, $r_a \le (r_{EZ} - r_0)$, taking a partial derivative of *P* yields:

$$\frac{\partial P}{\partial f} = \frac{r_a^2 r_0}{\left(\sqrt{\frac{B(1-f)}{d\pi}} - r_0\right)^3} = \frac{r_a^2 r_0}{(r_{EZ} - r_0)^3}$$

Since radii are positive and $r_{EZ} \ge r_0$, the partial derivative $\frac{\partial P}{\partial f}$ above is always positive. Therefore, location privacy degrades, i.e. *P* increases, with increasing *f* in this scenario.

*Proof for Theorem 2:* When $r_{EZ} \le (r_a + r_0)$ or equivalently, $r_a \ge (r_{EZ} - r_0)$, $P$ is $(1-f)$. The expression $(1-f)$ decreases linearly with increasing *f*.

Therefore, theorems (1) and (2) collectively show that at a given *B* value, the best value of location privacy for the defender (i.e. lowest *P*) is obtained at either *f = 0* (i.e. lowest value of *f* ) or *f* = $f_{max}$ (i.e. highest value of *f*). For a given *B* value, to determine whether *f = 0* or $f_{max}$ provides the best location privacy, we compute and compare *P* at these *f* values.

From (1), at *f = 0*,

$$P = \begin{cases} \frac{r_a^2}{(r_{max}-r_0)^2}, \ if\ r_a \le (r_{max} - r_0) \\ \\ 1, \ if\ r_a \ge (r_{max} - r_0) \end{cases} \tag{3}$$

where $r_{max}$ is defined as the value of $r_{EZ}$ when $f = 0$. From (2), $r_{max} = \sqrt{\frac{B}{\pi d}}$

When *f* is at its maximum $f_{max}$, the number of dummy PUs is maximized, which means the EZ radius is set to its minimum feasible value, i.e. $r_{EZ} = r_0$. By (1), if $(r_{EZ} - r_0) = 0$ then $P = (1 - f_{max})$. From (2), $f_{max} = \left(1 - \frac{d\pi r_0^2}{B}\right)$.

$$\therefore At\ f = f_{max},\ P = \frac{d\pi r_0^2}{B} \tag{4}$$

The next step is to determine when $f = f_{max}$ yields better $P$ than $f = 0$. First, $f = 0$ is never better when $f = 0$ yields $P = 1$, i.e. when $r_a \geq (r_{max} - r_0)$. This is apparent from (4), which shows that when $f = f_{max}$, $P$ is the minimum area that can be blocked divided by the area that is actually blocked, and this ratio can never exceed 1.

Thus, $f = 0$ is better if and only if $\mathrm{r_a} < (\mathrm{r_{max}} - \mathrm{r_0})$ and $\frac{r_a^2}{(r_{max} - r_0)^2} < \frac{d\pi r_0^2}{B}$. The latter simplifies to $r_a < r_0 - r_0^2\sqrt{\frac{d\pi}{B}} = \frac{r_0}{r_{max}}(r_{max} - r_0)$, with (2). Since $r_0$ cannot exceed $r_{max}$, we know $r_0 - r_0^2\sqrt{\frac{d\pi}{B}} < (\mathrm{r_{max}} - \mathrm{r_0})$ so $r_a < r_0 - r_0^2\sqrt{\frac{d\pi}{B}}$ is the sufficient condition. Therefore, in all cases where $r_a > r_0 - r_0^2\sqrt{\frac{d\pi}{B}}$, introducing as many dummy PUs as possible (i.e. $f = f_{max}$ ) provides the best location privacy. When $r_a < r_0 - r_0^2\sqrt{\frac{d\pi}{B}}$, enlarging EZs as much as possible around real PUs (i.e. $f = 0$) provides the best location privacy.

TABLE II. SUMMARY OF OPTIMAL STRATEGIES

| Scenario | Optimal Strategy |
|---|---|
| $r_a \leq r_0 - r_0^2\sqrt{\frac{d\pi}{B}}$ | enlarging EZs as much as possible around real PUs (i.e. $f = 0$)<br>$P = \frac{\mathrm{r_a^2}}{\left(\sqrt{\frac{B}{\pi d}} - \mathrm{r_0}\right)^2}$ |
| $r_a \geq r_0 - r_0^2\sqrt{\frac{d\pi}{B}}$ | introducing as many dummy PUs as possible (i.e. $f = f_{max}$ )<br>$\mathrm{P} = \frac{\mathrm{d\pi r_0^2}}{\mathrm{B}}$ |

In practice, we expect that $r_a > r_0$ in many cases, especially for jamming attacks, as it is likely that a jammer can cause harmful interference at a much larger distance than a typical SU. Because *d, B, and* $r_0$ are all positive quantities, $r_0 - r_0^2\sqrt{\frac{d\pi}{B}}$ is always less than $r_0$, which means that the strategy of maximizing the number of dummy PUs is always optimal when $r_a > r_0$.

### *B. Diminishing Returns in Location Privacy*

As there is a tradeoff, increasing the fraction of area covered by EZs ($B$) improves location privacy when the best defender strategy is used. This section explores whether there are diminishing returns, i.e. whether incremental gains in location privacy decrease as $B$ increases.

From Section IV(a), location privacy *P* when using the best defender strategy is as follows. This equation shows the Pareto optimal relationship between *P* and *B*.

$$P = \begin{cases} \frac{r_a^2}{(r_{max} - r_0)^2}\ i.e.\ at\ f = 0, & if\ r_a \leq r_0 - r_0^2\sqrt{\frac{d\pi}{B}} \\ \frac{d\pi r_0^2}{B}\ \ i.e.\ at\ f = f_{max}, & iif\ r_a \geq r_0 - r_0^2\sqrt{\frac{d\pi}{B}} \end{cases}$$

There are diminishing returns at a given value of $B$ if the second derivative of the Pareto optimal curve of achievable $P$ vs. $B$ is positive. As shown in Section IV(a), if $r_a \geq r_0$, then $f = f_{max}$ is always optimal. For values of $B$ where $f = f_{max}$ is optimal, the first- and second-order partial derivatives with respect to $B$ (i.e. *P*' and *P*" ) are as follows. Thus, while increasing blocked area $B$ does improve privacy, there are indeed diminishing returns if $r_a \geq r_0$.

$$\frac{\partial P}{\partial B} = \frac{\partial}{\partial B}\left(\frac{d\pi r_0^2}{B}\right) = -\left(\frac{d\pi r_0^2}{B^2}\right) < 0$$

$$\frac{\partial^2 P}{\partial B^2} = \frac{\partial^2}{\partial B^2}\left(\frac{d\pi r_0^2}{B}\right) = \frac{2d\pi r_0^2}{B^3} > 0$$

If $r_a < r_0$, then $f = 0$ is optimal for values of $B$ below a critical point which we call $B_c$. This is determined by $r_a = r_0 - r_0^2\sqrt{\frac{d\pi}{B_c}}$, which simplifies to $B_c = \frac{d\,\pi\, r_0^4}{(r_0 - r_a)^2}$. For values of $B$ below $B_c$, the first- and second-order partial derivatives are as follows:

$$\frac{\partial P}{\partial B} = \frac{\partial}{\partial B}\left(\frac{r_a^2}{(r_{max} - r_0)^2}\right) = -\left(\frac{r_a^2\sqrt{\frac{B}{d\pi}}}{B\left(\sqrt{\frac{B}{d\pi}} - r_0\right)^3}\right) < 0$$

$$\frac{\partial^2 P}{\partial B^2} = \frac{0.5\, r_a^2}{d\pi B\sqrt{\frac{B}{d\pi}}\left(\sqrt{\frac{B}{d\pi}} - r_0\right)^3} + \frac{1.5\, r_a^2}{d\pi B\left(\sqrt{\frac{B}{d\pi}} - r_0\right)^4} > 0$$

Because second-order derivatives are positive, there are diminishing returns for values of $B$ less than $B_c$ and greater than $B_c$. To determine whether this is the case when $B = B_c$, we calculate the ratio of $B'$ just below $B_c$ to $B'$ just above $B_c$.

$$\frac{P'\ just\ below\ B_c}{P'\ just\ above\ B_c} = \frac{P'\ at\ B_c\ when\ f = fmax\ is\ optimal}{P'\ at\ B_c\ when\ f = 0\ is\ optimal} = \frac{-\left(\frac{(r_0 - r_a)^4}{d\pi r_0^6}\right)}{-\left(\frac{(r_0 - r_a)^4}{d\pi\ \ a r_0^5}\right)} = \frac{r_a}{r_0} \tag{5}$$

Since the critical point only exists when $r_a < r_0$, the above ratio is less than 1. Because *P*' is negative both below and above $B_c$, we can conclude that the slope decreases at the critical point $B_c$. Therefore, there are diminishing returns everywhere on the Pareto optimal curve.

## V. SIMULATIONS

In Section IV, we derived the number of dummy PUs that optimize location privacy *P* for any given *B* and produced the resulting Pareto optimal curve under the assumption that PUs are far enough apart that an attack could at most only hit one PU at a time. In this section, we relax that assumption. Because this makes analysis intractable, we use a stochastic Monte Carlo simulation to show that the same general conclusions hold even when EZs can overlap. As in Section IV, we assume isotropic path loss and uniformly distributed PU locations.

In Section IV, we found that the best defender strategy depends on whether $r_a > r_0 - r_0^2\sqrt{\frac{d\pi}{B}}$, which is the case for all $B$ if and only if $r_a \geq r_0$. We must therefore compare analysis and simulation results when attack radius $r_a$ is both greater than and less than minimum protection distance $r_0$. In Section V(a), we provide detailed simulation results for a scenario where $r_a = 2\,r_0$, and in Section V(b) we provide similar results for a scenario where $r_a = .6\,r_0$. We consider a broader range of input variables in Section V(c), and show how they affect the Pareto optimal curves. Section V(d) shows how the Pareto optimal results obtained with our approach compare with a previously proposed approach [16].

### A. *When Attack Radius $r_a$ > Min. Protection Distance $r_0$*

As in Section IV(a), we determine the fraction of dummy PUs $f$ and the EZ radius $r_{EZ}$ that yield the best location privacy $P$ for a given fraction of area covered by EZs $B$. A stochastic Monte Carlo simulation is performed over an area of 1000 x 1000 units. 10 real PUs are stochastically generated for each run with uniform probability over all locations. The minimum protection distance ($r_0$) is 5 units, and the attack radius ($r_a$) is 10 units, resulting in a $r_a/r_0$ ratio of 2. Analytical results showed that when this ratio exceeds 1, adding the maximum number of dummies (i.e. $f = f_{max}$) is the best strategy.

Figure 1 shows the location privacy $P$ achieved by both simulation and analysis when varying $f$. Different curves are shown for different values of $B^*$, which is the area of a disk surrounding a PU multiplied by number of PUs. If all EZs are circular because none are formed by overlapping disks, as was assumed in our analytic results, then $B^* = B$. If some EZs are non-circular, as can occasionally happen in simulation, then $B^*$ is slightly larger than $B$. Each curve spans from $f = 0$, where there are no dummy PUs, to $f = f_{max}$, where the number of dummy PUs is as great as possible for the given value of $B^*$. The error bars represent 95% confidence intervals. In the analytical results in Figure 1b, the curves for $B^* = 0.001$ and $B^* = 0.005$ overlap completely because for that portion of the graph $r_a \geq (r_{EZ} - r_0)$ and, $P = (1 - f)$, from (1). Therefore, location privacy is a function of $f$ only. For the same reason, on this graph, curves for $B^* = 0.01$ and $B^* = 0.05$ partially overlap with curves for $B^* = 0.001$ and $B^* = 0.005$ at higher values of $f$.

Figure 1 shows that analysis and simulation do not yield identical results, meaning that non-circular EZs have some impact, but the basic conclusions from the analysis of Section IV are also true for the simulation results. In both cases, the location privacy metric P increases with $f$ when EZ radius exceeds something close to attack radius + minimum protection distance, and decreases with $f$ when this is not the case. As long as this is the case, best strategy for the defender is always

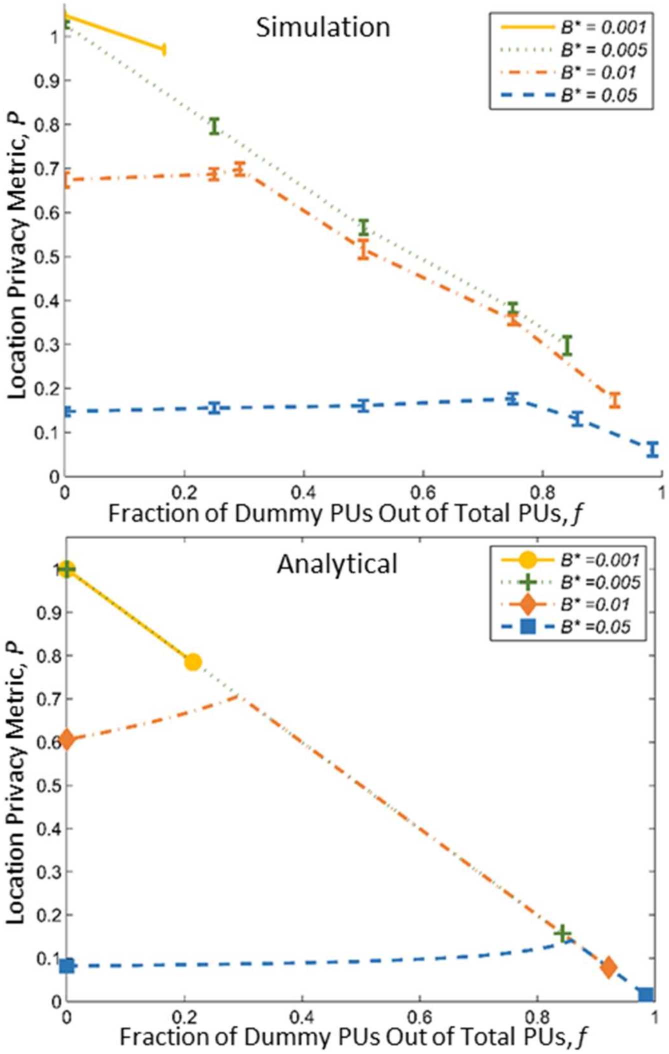

Figure 1: Privacy $P$ as a function of fraction $f$ of dummy PUs for different values of B*. Min protection distance $r_0$ = 5. Attack radius $r_a$ = 10. Figure 1a shows results of simulation. Figure 1b shows results of analysis.

either f=0 or $f = f_{max}$. For these values of attack radius and minimum protection distance, $f = f_{max}$ is always best. P achieved is similar for both graphs, but P is slightly higher in simulation, especially for large values of $B^*$. This is because in the simulation an attacker can sometimes attack multiple PUs at once, whereas the assumptions make this impossible in the analysis.

Obviously, the more area one blocks, the more privacy can be achieved. Figure 2 shows the relationship between $B$ and location privacy $P$ for both of the approaches that have the potential to be optimal: $f = 0$ and $f = f_{max}$. As expected for cases where $r_a > r_0$, the defender should always choose $f = f_{max}$ because $P$ is greater for all values of $B$. Thus, the $f = f_{max}$ curve is the Pareto optimal result. The shape of the Pareto optimal curve has a steep slope at low values of $B$ and flatter slope at higher values of $B$. In other words, there are diminishing returns with increasing $B$. Numerical results are quite similar for both analysis and simulation, although $P$ is slightly higher with simulation.

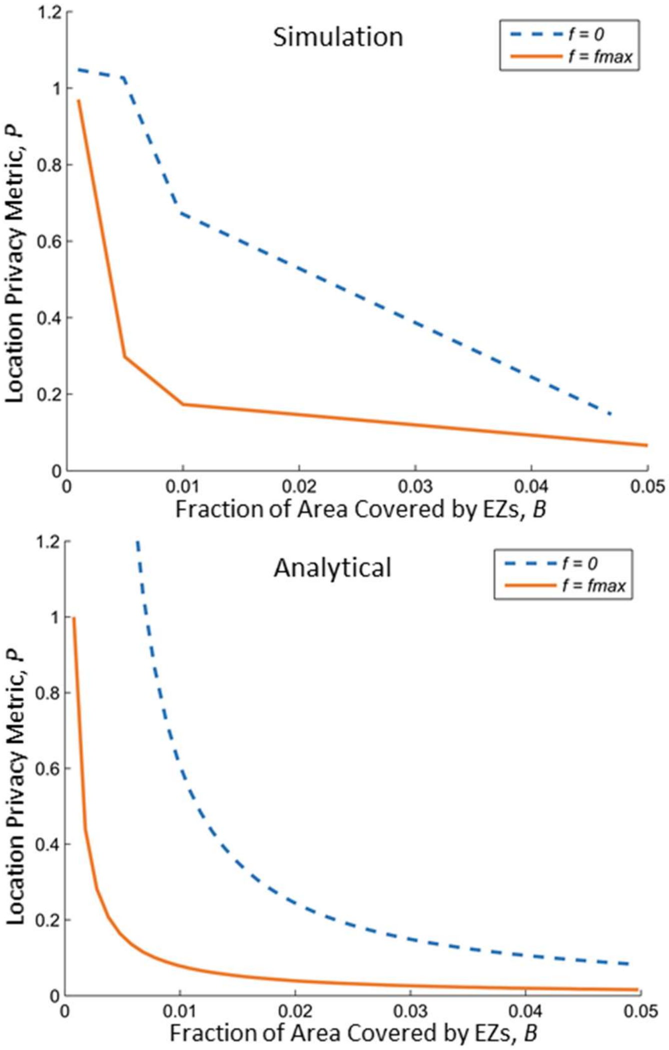

Figure 2: Privacy $P$ as a function of B comparing $f$=0 and $= f_{max}$ . Min. protection distance $r_0 \ = \ 5$. Attack radius $r_a \ = \ 10$. Figure 2a shows results of simulation. Figure 2b shows results of analysis.

### B. When Attack Radius $r_a <$ Min. Protection Distance $r_0$

In this section, we address the same issues as in Section V(a) under the same assumptions, except with an attack radius $r_a$ of 3 units, which is smaller than the minimum protection distance $r_0$ of 5 units. Again, our conclusions from simulation results mirror those from analytical results, so relaxing the assumption that PUs are not too close together has little effect.

Much like Figure 1, Figure 3 shows how location privacy $P$ varies with the fraction $f$ of dummy PUs for different values of $B^*$. Again, we see that numerical results are similar for analysis and simulation. Again, we see that in both graphs $P$ increases with $f$ when EZ radius exceeds something close to attack radius + minimum protection distance, and decreases with $f$ when this is not the case, so $f = 0$ or $f = f_{max}$ has to be best for the defender strategy. This time, as expected based on the results of Section IV for the smaller attack radius, $f = f_{max}$ is not always best. This is clearer with Figure 4, which like Figure 2, shows how location privacy $P$ varies with $B$ when $f = 0$ and $f = f_{max}$. In both simulation and analysis, the $f = 0$ and $f = f_{max}$ curves cross when B is close to the critical value, so $f = 0$ is best for the defender when $B$ is above the critical value, and $f = f_{max}$ is best otherwise.

### C. Effect Of Varying Parameters

Decisions regarding how much spectrum to sacrifice in order to improve location privacy, i.e. about the appropriate value of $B$, would depend in large part on the Pareto optimal curve that shows the tradeoff between $B$ and location privacy $P$. In this section, we show how that curve depends on important factors. More specifically, Figure 5 shows the Pareto optimal curves at different PU densities, and Figure 6 shows the Pareto optimal curves at different attack radii. In both figures, all input parameters are the same as in Section V(a) except the variables which are explicitly varied in the figure shown, i.e. PU density or attack radius.

We observe that the shape of the Pareto optimal curve remains similar, regardless of PU density and attack radius. These results are the same with both analysis and simulation results. In all cases, location privacy improves rapidly if the

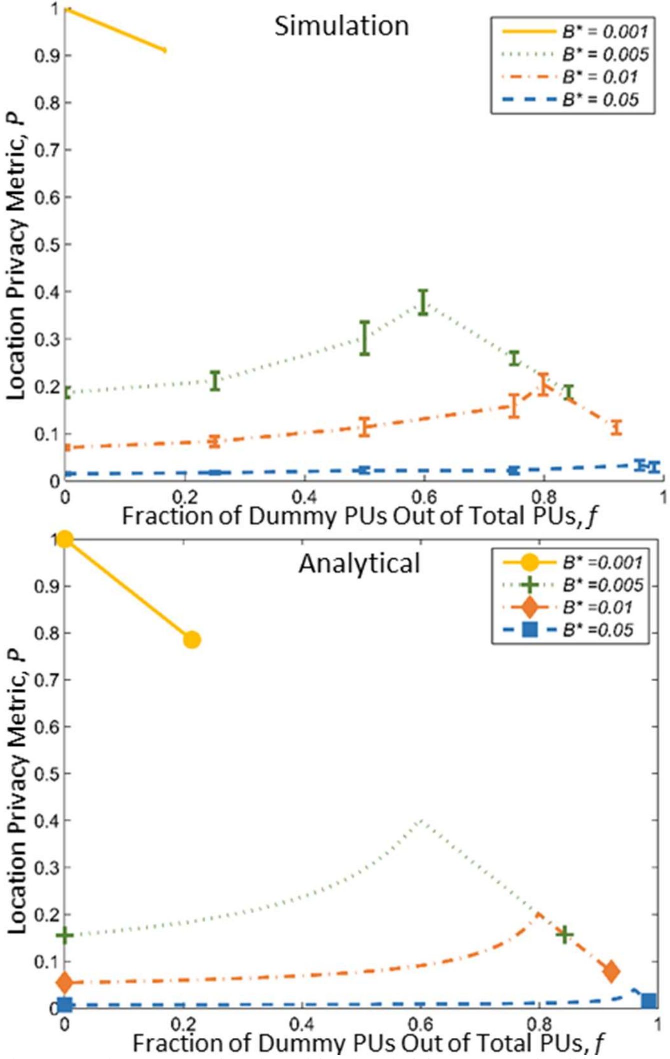

Figure 3: Privacy $P$ as a function of fraction $f$ of dummy PUs for different values of B*. Min protection distance $r_0 \ = \ 5$. Attack radius $r_a \ = \ 3$. Figure 3a shows results of simulation. Figure 3b shows results of analysis.

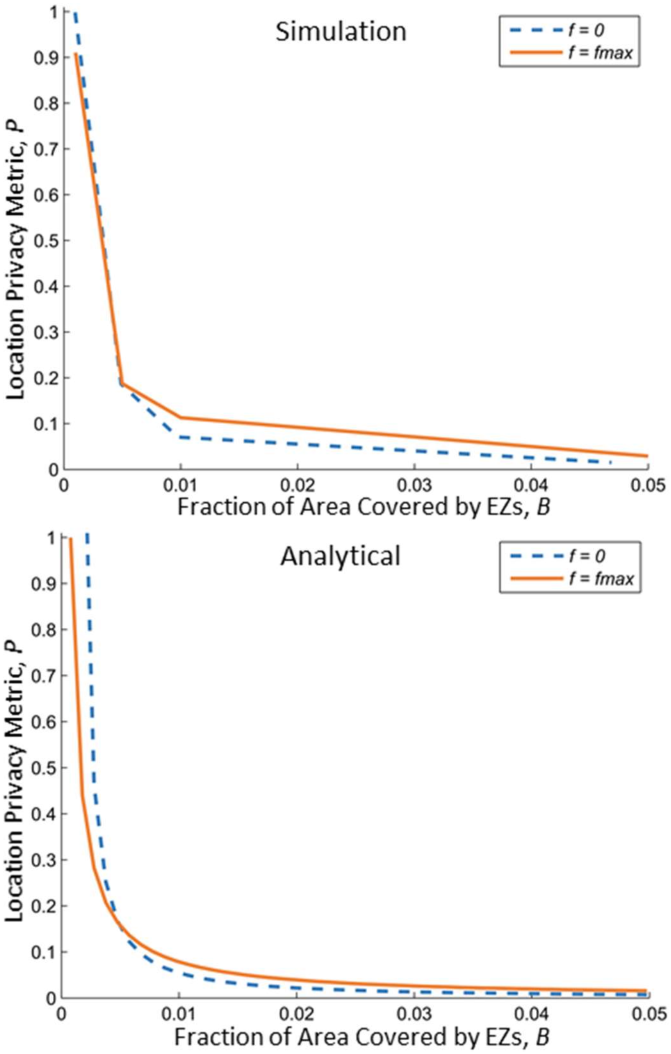

Figure 4: Privacy $P$ as a function of $B$ comparing $f = 0$ and $f = f_{max}$. Min protection distance $r_0 = 5$. Attack radius $r_a = 3$. Figure 4a shows results of simulation. Figure 4b shows results of analysis.

fraction of area covered by EZs $B$ is increased a small amount beyond the minimum necessary. However, there are diminishing returns after that. Thus, for example, a tremendous improvement in location privacy is possible by blocking 0.5% of the area, and relatively modest improvements are possible by increasing the area blocked from 0.5% to 5%.

### *D. Comparison With State-of-Art Methods*

This section compares the effectiveness of the defender strategy developed in this paper with two previously proposed approaches: $k$-anonymity and $k$-clustering [16]. Both approaches seek location privacy by including more PUs in an EZ while keeping EZs circular and as small as possible, rather than by expanding EZs or creating dummy PUs as in our approach. In $k$-anonymity, EZ boundaries are the smallest circles that contain $k$ PUs each. In $k$-clustering, $k$ EZs contain all PUs such that the total area of the $k$ EZs is as small as possible. See Section II for more on these algorithms.

As described in Section III(b), an attacker uses the EZ boundaries and its knowledge of defender strategy to determine the probability that a PU is at any given location. The attacker then determines the location where the expected number of PUs within one attack radius is maximized. The difference is in how the attacker determines those probabilities. If an EZ has a radius equal to the minimum protection radius, then there is one PU at the center of the EZ. Thus, the expected number of PUs is 1 at that point and 0 elsewhere. With $k$-anonymity and $k$-clustering, for EZs that have larger radii, the EZ must contain multiple PUs. Since these EZs are as small as possible, the ring of points exactly one minimum protection distance away from the EZ circular boundary contains two or more PUs. There may or may not be additional PUs inside the ring. Our heuristic attacker algorithm assumes that there are exactly two PUs on the ring, and that all points inside this ring in all EZs have a constant probability of containing a PU, no matter how large the EZ is. This constant probability is chosen so that expected PU density over the entire region will equal actual density $d$. In reality, the probability that a PU will be located at a point inside an EZ depends on the size of that EZ, so this attacker algorithm is suboptimal. Results for these defender algorithms would be

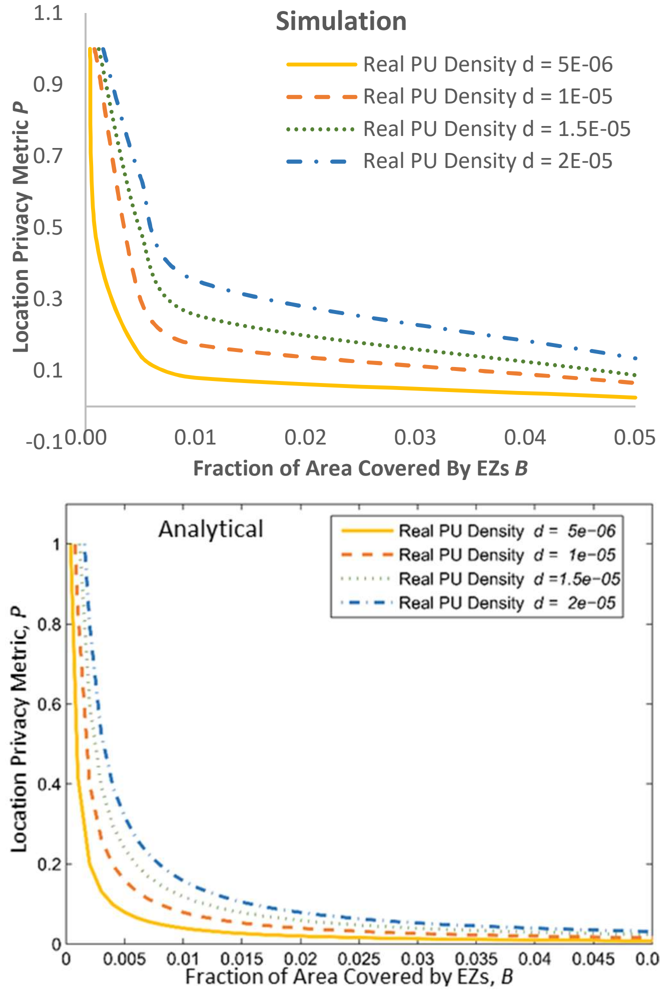

Figure 5: Privacy $P$ as a function of $B$ when using the optimal defender strategy. Min protection distance $\boldsymbol{r_0} = \mathbf{5}$. Attack radius $r_a = 10$. Figure 5a shows results of simulation. Figure 5b shows results of analysis.

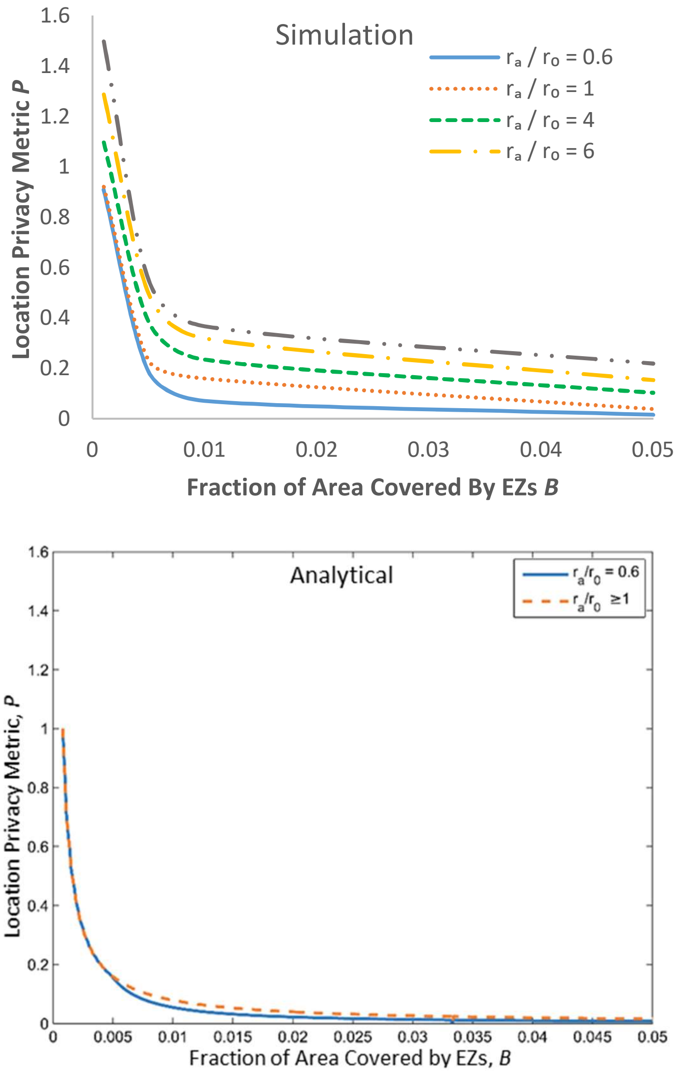

Figure 6: Privacy $P$ as a function of $B$ when using the optimal defender strategy. Min. protection distance $r_0 = 5$. Density of real PUs $d = 1E-5$. Figure 6a shows results of simulation. Figure 6b shows results of analysis.

worse with an optimal attacker algorithm.

Figure 7 shows $P$ vs. $B$ for the defender strategy derived in this paper, $k$-clustering and $k$-anonymity. For the latter two, the results are obtained by varying $k$ from 1 to 10. We use the same assumptions here as in Section V(a). For all $B$ values, our approach provides far more location privacy than $k$-anonymity or $k$-clustering, or equivalently, our approach provides the same location privacy while blocking far less area within EZs. This is because $k$-anonymity and $k$-clustering require more PUs per EZ, and this can produce EZs that cover a very large area. At the same time, trying to keep EZs small while including multiple PUs means PUs are more likely to be near the edge of an EZ, which is helpful to attackers. Thus, at least for this measure of location privacy, creating dummy PUs is a more effective strategy.

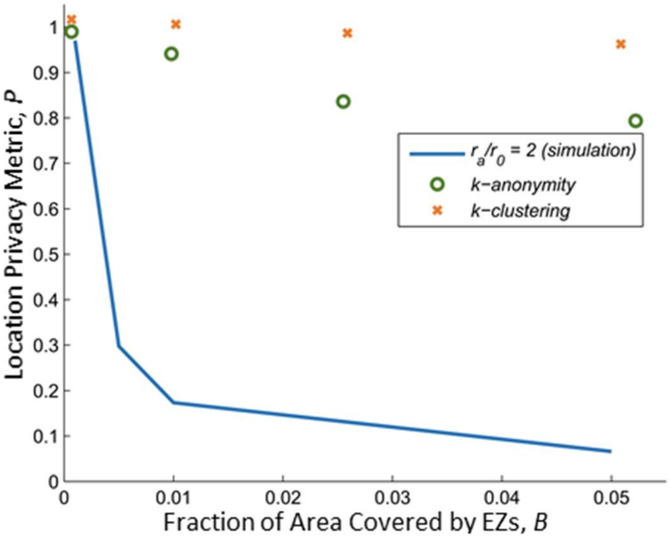

Figure 7. Privacy $P$ as a function of $B$ when using the optimal defender strategy compared with results of $k$-clustering and $k$-anonymity. Attack radius $r_a = 10$. Min. protection distance $r_0 = 5$. Density of real PUs $d = 1E-5$.

## VI. Conclusions And Policy Implications

There are societal costs and opportunity costs to blocking unused spectrum from use. However, for some devices, there is a strong need for location privacy and operational location privacy may be a matter of national security. Thus, without an effective way of protecting location privacy for those devices that need it, it may not be possible to free up some valuable spectrum.

We have explored a novel and effective approach for protecting location privacy by generating dummy primary users (PUs). For scenarios where attack radius $r_a$ is greater than minimum protection distance $r_0$, we find that for a given amount of area blocked for exclusion zones (EZs), the most effective defender strategy is to keep EZs as small as possible and generate as many dummy PUs as possible. Where attacks are done through jamming, we would expect $r_a > r_0$, as it is unreasonable to expect that a typical secondary user (SU) that is just under $r_0$ from a PU would cause harmful interference, but a jammer in this location would not. Even if $r_a < r_0$, as might occur if the attack is kinetic, then the best defender strategy is to generate as many dummy PUs as possible if the fraction of area to be blocked $B$ is below a critical threshold. For higher $B$, the better strategy for a defender is to generate no dummy PUs and to expand the size of EZs.

When our defender strategy is employed with optimal parameters, it greatly outperforms some previously proposed approaches [16] in the scenarios considered. More specifically, our approach can achieve a greater location privacy for a given fraction of blocked area, or equivalently, a smaller fraction of blocked area for a given location privacy.

Our results show that this approach is highly effective at protecting location privacy, and may give both those who want to free spectrum and those who want better location privacy most of what they seek. Although there is an unavoidable tradeoff between maximizing amount of spectrum available for SUs and optimizing location privacy for PUs, even a very small increase in amount of area blocked from SUs can greatly improve location privacy for PUs, as long as best defender strategy is employed. However, as more and more area is blocked, there are diminishing returns, i.e. there is less improvement in location privacy for each square meter of area blocked.

## References

[1] Federal Communications Commission (FCC), “National Broadband Plan,” 2010.

[2] B. Obama, “Presidential Memorandum, Unleashing the Wireless Broadband Revolution,” 2010.

[3] J. M. Peha, “Approaches to spectrum sharing,” *Commun. Mag. IEEE*, vol. 43, no. 2, pp. 10–12, 2005. https://users.ece.cmu.edu/~peha/papers.html

[4] J. M. Peha, “Sharing spectrum through spectrum policy reform and cognitive radio,” *Proc. IEEE*, vol. 97, no. 4, pp. 708–719, 2009. https://users.ece.cmu.edu/~peha/papers.html

[5] J. M. Peha, “Spectrum sharing in the gray space,” *Telecomm. Policy*, vol. 37, no. 2, pp. 167–177, 2013. https://users.ece.cmu.edu/~peha/papers.html

[6] R. Saruthirathanaworakun, J. M. Peha, and L. M. Correia, “Gray-Space Spectrum Sharing between Multiple Rotating Radars and Cellular Network Hotspots,” in *2013 IEEE 77th Vehicular Technology Conference (VTC Spring)*, 2013, pp. 1–5. https://users.ece.cmu.edu/~peha/papers.html

[7] R. Saruthirathanaworakun and J. M. Peha, “Dynamic primary-secondary spectrum sharing with cellular systems,” in *2010 Proceedings of the Fifth International Conference on Cognitive Radio Oriented Wireless Networks and Communications*, 2010, pp. 1–6. https://users.ece.cmu.edu/~peha/papers.html

[8] J. M. Peha and S. Panichpapiboon, “Real-time secondary markets for spectrum,” *Telecomm. Policy*, vol. 28, no. 7, pp. 603–618, 2004. https://users.ece.cmu.edu/~peha/papers.html

[9] President’s Council of Advisors on Science and Technology (PCAST), “Realizing the full potential of government-held spectrum to spur economic growth,” 2012.

[10] Federal Communications Commission (FCC), “White Space.” [Online]. Available: https://www.fcc.gov/general/white-space. [Accessed: 08-Sep-2016].

[11] FCC, *Third Memorandum Opinion and Order, ET Docket No FCC 12-36A1*. 2012.

[12] FCC, *Enabling Innovative Small Cell Use In 3.5 GHZ Band NPRM & Order. GN Docket No. 12-354*. 2012.

[13] European Commission Digital Single Market, “Promoting the shared use of Europe’s radio spectrum,” 2016. [Online]. Available: https://ec.europa.eu/digital-single-market/node/315.

[14] F. Slimeni, B. Scheers, and Z. Chtourou, “Security threats in military cognitive radio networks,” in *2015 International Conference on Military Communications and Information Systems (ICMCIS)*, 2015, pp. 1–10.

[15] M. McHenry, “ISART 2011 Panel: Sharing Radar Bands with Commercial Systems,” 2011. [Online]. Available: http://www.its.bldrdoc.gov/media/31114/McHenryISART2011Panelv1.pdf.

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

[17] M. Clark and K. Psounis, “Can the Privacy of Primary Networks in Shared Spectrum be Protected?,” in *Proceedings of IEEE INFOCOM*, 2016.

[18] “Mobile broadband services in the 2300 MHz - 2400 MHz frequency band under Licensed Shared Access regime.” [Online]. Available: http://www.ict-crsi.eu/index.php/standardization-streams/licensed-shared-access.

[19] National Telecommunications and Information Administration (NTIA), “Assessment of the Near-Term Viability of Accommodating Wireless Broadband Systems in the 1675-1710 MHz, 1755-1780 MHz, 3500-3650 MHz, 4200-4220 MHz, and 4380-4400 MHz Bands (Fast Track Evaluation),” 2010. [Online]. Available: https://www.ntia.doc.gov/report/2010/assessment-near-term-viability-accommodating-wireless-broadband-systems-1675-1710-mhz-17.

[20] National Telecommunications and Information Administration (NTIA), “NTIA Technical Report TR-16-521 - Using On-Shore Detected Radar Signal Power for Interference Protection of Off Shore Radar Receivers,” 2016. [Online]. Available: http://www.its.bldrdoc.gov/publications/2828.aspx.

[21] National Telecommunications and Information Administration (NTIA), “Federal Government Spectrum Use Reports 225MHz – 5GHz.” [Online]. Available: https://www.ntia.doc.gov/page/federal-government-spectrum-use-reports-225mhz-5ghz. [Accessed: 15-Dec-2015].

[22] A. Khoshgozaran, C. Shahabi, and H. Shirani-Mehr, “Location privacy: Going beyond K-anonymity, cloaking and anonymizers,” *Knowl. Inf. Syst.*, vol. 26, no. 3, pp. 435–465, 2011.

[23] N. Xu, D. Zhu, H. Liu, J. He, X. Du, and T. Liu, “Combining Spatial Cloaking and Dummy Generation for Location Privacy Preserving,” in *Advanced Data Mining and Applications*, Springer, 2012, pp. 701–712.

[24] B. Niu, Z. Zhang, X. Li, and H. Li, “Privacy-area aware dummy generation algorithms for Location-Based Services,” in *2014 IEEE International Conference on Communications (ICC)*, 2014, pp. 957–962.

[25] P. Jagwani and R. Kumar, “Taxonomy of Dummy Generation Techniques for Preserving Location Privacy,” *Int. J. Comput. Sci. Netw.*, vol. 2, no. 6, pp. 174–178, 2013.

[26] S. Li, H. Zhu, Z. Gao, X. Guan, K. Xing, and X. Shen, “Location privacy preservation in collaborative spectrum sensing,” in *2012 Proceedings of IEEE INFOCOM*, 2012, pp. 729–737.

[27] F. Tang, J. Li, I. You, and M. Guo, “Long-term location privacy protection for location-based services in mobile cloud computing,” *Soft Comput.*, 2015.

[28] J. Park and J. H. Reed, “Ensuring Operational Privacy of Primary Users in Geolocation Database-Driven Spectrum Sharing,” 2013. [Online]. Available: https://www.ntia.doc.gov/files/ntia/publications/ssd-summary_report-tr1_1_link_5.pdf.

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

[30] L. Sweeney, “k-anonymity: A model for protecting privacy,” *Int. J. Uncertainty, Fuzziness Knowledge-Based Syst.*, vol. 10, no. 05, pp. 557–570, 2002.

[31] P. R. Vaka, S. Bhattarai, and J. Park, “Location privacy of non-stationary incumbent systems in spectrum sharing,” in *2016 IEEE Global Communications Conference (GLOBECOM), Washington, DC, USA*, 2016.

[32] Y. Li, L. Zhou, H. Zhu, and L. Sun, “Secure and Privacy-Preserving Location Proof in Database-Driven Cognitive Radio Networks,” in *Wireless Algorithms, Systems, and Applications*, Springer, 2015, pp. 345–355.

[33] B. Bahrak, “Ex Ante Approaches for Security , Privacy , and Enforcement in Spectrum Sharing,” PhD Thesis, Virginia Tech, 2013.

[34] B. Bahrak and J. Park, “Location Privacy of Primary Users in Geolocation Database-Driven Spectrum Sharing,” 2013. [Online]. Available: https://pdfs.semanticscholar.org/88b4/417516c7662693c84c0c72861373adeaeb0f.pdf.