Preserving Incumbent User's Location Privacy Against Environmental Sensing Capability

Yousi Lin
Virginia Tech
Blacksburg, United States
yousil94@vt.edu

Yuxian Ye
Virginia Tech
Blacksburg, United States
herexian@vt.edu

Yaling Yang
Virginia Tech
Blacksburg, United States
yyang8@vt.edu

***Abstract*—In dynamic spectrum access (DSA), Environmental Sensing Capability (ESC) systems are implemented to detect the incumbent users' (IU) activities for protecting them from secondary users' (SU) interference as well as maximizing secondary spectrum usage. However, IU location information is often highly sensitive and hence it is preferable to hide its true location under the detection of ESCs. In this paper, we design novel schemes to preserve both static and moving IU's location information by adjusting IU's radiation pattern and transmit power. We first formulate IU privacy protection problem for static IU. Due to the intractable nature of this problem, we propose a heuristic approach based on sampling. We also formulate the privacy protection problem for moving IUs, in which two cases are analyzed: (1) protect IU's moving traces; (2) protect its real-time current location information. Our analysis provides insightful advice for IU to preserve its location privacy against ESCs. Simulation results show that our approach provides great protection for IU's location privacy.**

***Index Terms*—DSA, ESC, IU location privacy**

I. Introduction

The new Citizens Broadband Radio Service (CBRS) is promulgated by the Federal Communications Commission (FCC) for dynamic spectrum sharing between government and commercial users in the 3500-3700 MHz (referred to as 3.5 GHz band) [1], [2]. This new sharing paradigm allows CBRS devices (CBSD), which are also called secondary users (SUs), to opportunistically use the 3.5GHz band in locations and times where federal incumbent users (IUs) are not using this band. A spectrum access coordination system, called SAS, is used to grant spectrum access permissions to SUs based on the location and communication activities of IUs.

However, the prosperity of such a federal-commercial spectrum sharing system is contingent on how privacy issues of federal IUs are handled. On one hand, for the SAS system to accurately grant SUs spectrum access permissions, it must leverage the presence information of IUs. On the other hand, IUs in the 3.5 GHz band are mostly military systems, like U.S. naval radars. Locations of these IUs are highly sensitive. Directly revealing IU location information to the SAS system will compromise incumbents operation security (OPSEC). These conflicting requirements create a significant challenge for designing CBRS in 3.5GHz.

This work was funded by the National Science Foundation under Grant No 1824494 and 1547366.

From 2015, the Wireless Innovation Forum (WINNF) has been developing requirements to preserve OPSEC as required by FCC for operation in 3.5GHz band [3]. The current proposal from FCC uses Environmental Sensing Capability (ESC) system to mitigate this OPSEC challenge. ESC is a distributed network of sensing devices used for the protection of incumbent users (IUs) from CBSDs' transmissions [4]–[6]. ESC systems measure the received signal strength (RSS) of IU signal and provide such information to SAS. Deriving the IU presence information from the RSS information, SAS then allocates the unused frequency bands to CBSDs so that it can guarantee that CBSDs do not have mutual interference with IUs [7]. Since the location and activity information of IUs are not directly revealed to SAS, such an ESC-based system can provide some simple and basic OPSEC protection.

However, we argue that for highly sensitive IU operation data, the OPSEC protection in ESC-based system is not enough. This is because ESC-based system still sends IU sensing results (i.e. RSS measurements) to SAS. Such sensing results can be used to derived IU locations through RSS-based radio localization. This can create potential OPSEC violation if either SAS or ESCs are compromised by adversaries.

In this paper, we address the above OPSEC problem in 3.5GHz ESC-based DSA system through the use of smart antenna on the IU side. Our design uses the fact that the location and configuration of each ESC sensor are registered at FCC, which then are posted publicly. Leveraging these public information, our scheme tunes the antenna gains of an IU transmitter dynamically, such that it creates uncertainty in an IU's location even when an adversary obtains the ESC sensing results and uses RSS-based localization scheme to derive the IU's location. We provide a thorough theoretical analysis on how IU can maximize its location uncertainty, assuming that an adversary has full access to all ESCs sensing results. Our scheme ensure that even when both SAS and ESCs are compromised, the location privacy of IUs are still protected. Our scheme can be used to protect location privacy of both mobile and static IUs.

The remainder of the paper is organized as follows. Related work is given in Section II. Section III introduces the general system models for static IU and moving IU. Section IV provides the formulation and our approach for static IU location privacy preserving problem. Formulation and approaches for

moving IU's location privacy preservation is described in Section V. Experimental results are reported in Section VI. Finally, Section VII concludes the paper.

II. Related Work

Most of the existing works that focus on IU location privacy protection either add noise or distortion on IU location data or encrypt the location data using homomorphic cryptosystem before these data are sent to the SAS system [8]–[11]. However, these works are not applicable in 3.5GHz DSA system because IU location data is not sent to SAS in 3.5GHz. Instead, SAS obtains received signal strength indication (RSSI) measurements of IU signals from the ESC.

In an RSS-based localization system, there are multiple signal receivers placed at specific locations which measure the RSS of wireless nodes and report the measurements to the system [12]. These signal receivers are referred as "anchors". Localization algorithms are then used to compute location estimates based on anchor measurements. In DSA scenario, ESCs are the anchors measuring the RSS of incumbent transmitters and may potentially use this information to localize the transmitter. As previously discussed, IU location privacy is often highly sensitive, and thus the question becomes: is it possible for an IU to make its location or moving trajectory undetected even under ESCs' localization measurement?

Fortunately, most of the robust RSS based localization schemes all have limited effectiveness no matter what statistical methods they use [13]. In addition, [14] has shown that it is possible to spoof the location of a radio transmitter through tuning its antenna patterns. However, [14] assumes that the radio localization system believes the targeted transmitter is using omni-directional antenna and the localization system is unaware that the transmitter can tune its antenna pattern. In addition, [14] does not provide any strategy in terms of how a radio transmitter can best hide its location. Our scheme, on the other hand, does not rely on the assumption that the adversary is oblivious to the IU's capability of radiation pattern tuning. Our scheme also provides best privacy-protection strategy for both static and mobile IUs.

III. General System Model

A. Attack Model

The general attack model for IU privacy in 3.5GHz is illustrated in Figure 1. A moving IU transmitter and multiple ESCs are distributed in a certain area. ESCs measure the RSS of IU transmission. IU can control its radiation pattern so that it can tune its antenna gains at different directions subject to the constrain of its antenna capability. The adversary has full access to all ESC sensing results and knows the IU's full capability in tuning radiation pattern. The goal of the adversary is to localize and track the IU.

B. Location hiding using radiation pattern tuning

The design of our privacy-protection scheme is based on the following observation. If the RSS readings at ESCs for an IU at location A are the same as the RSS readings for the IU at location B, there is no way for an adversary to differentiate these two locations no matter how he analyzes the data. Since both A and B can be the IU's possible locations, this lowers the chance of finding this IU's location by half. Thus, by creating a large amount of possible locations that satisfy the above condition, an IU can greatly increase its location uncertainty and hence avoid being localized by the adversary.

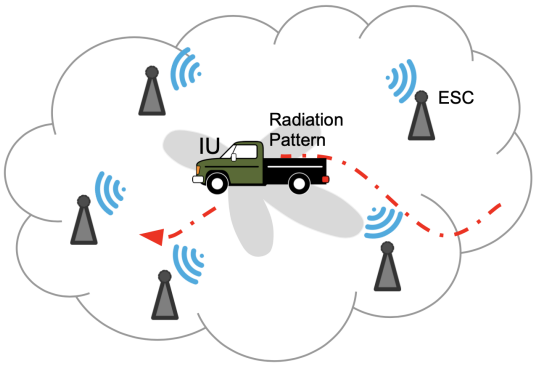

Figure 1. General system model.

To create such a large number of possible locations, an IU cannot use conventional omni-directional antennas with fixed transmit power. This is because the path loss from IU location to all ESCs will be different from the path loss from any other locations as long as the distance between them are different. Uniform transmit power to all directions cannot mask such location-dependent uniqueness from ESC sensing results.

Thus, in our scheme, we propose that a privacy-sensitive IU uses more advanced antenna designs, such as smart antenna that can electronically tune its radiation pattern or mechanical rotating directional antenna that can adjust its transmit power towards different directions. These advanced antenna designs are commonly found in IUs in 3.5GHz, which are often military radar systems. They can vary their transmit power to different directions, subject to hardware restrictions on their functionality, to mask the unique path loss characteristics of its location, and hence create ambiguity in ESC sensing results. Essentially, through tuning of antenna gains to different direction, an IU in location x with radiation pattern A can create the same ESC sensing results as an IU in a large set of other possible locations with various radiation patterns. Our IU privacy preservation scheme seeks to find the optimal antenna tuning strategies that maximize the set of possible locations.

In the remainder of this paper, without loss of generality, we assume that the IU is equipped with a circular phased array antenna. The phased array antenna consists of N_{ant} isotropic elements placed over a circle with radius R and the i_{th} antenna element is located with the phase angle ϕ_i. The radiation pattern of this circular phased array antenna is expressed as [15]:

$$g(\theta, \boldsymbol{\omega}) = \sum_{i=1}^{N_{ant}} \omega_i \exp[j\frac{2\pi}{\lambda} R\cos(\theta - \phi_i)] \qquad (1)$$

where θ represents the direction, λ is the signal wavelength and

$\boldsymbol{\omega} = [\omega_1, \omega_2, ..., \omega_{N_{ant}}]^H$ is the complex weight vector which can be tuned to change the radiation pattern, and generally these weight vectors have limited range due to hardware and functionality restrictions hence $\omega_{min} \leq \boldsymbol{\omega} \leq \omega_{max}$.

For simplicity, let:

$$\boldsymbol{h_k} = \begin{bmatrix} exp[j\frac{2\pi}{\lambda}Rcos(\theta_k - \phi_1)] \\ exp[j\frac{2\pi}{\lambda}Rcos(\theta_k - \phi_2)] \\ \vdots \\ exp[j\frac{2\pi}{\lambda}Rcos(\theta_k - \phi_{N_{ant}})] \end{bmatrix} \tag{2}$$

Circular antenna array is used in this paper as an example for problem illustration because it can produce flexible asymmetric radiation patterns and easily deflect a beam through 2π [14]. However, our analysis is not restricted to any specific antenna model. We can plug different antenna models into the analysis by replacing Equation (1) with their corresponding radiation functions. For example, Dolph-Tschebyscheff array antenna can use radiation pattern function:

$$\begin{cases} g(\theta, \boldsymbol{\omega}) = \sum_{i=1}^{N_{ant}/2} \omega_i cos[(2n-1)u], \\ \quad when\ N_{ant}\ is\ even \\ g(\theta, \boldsymbol{\omega}) = \sum_{i=0}^{(N_{ant}-1)/2} \omega_i cos[2nu], \\ \quad when\ N_{ant}\ is\ odd \\ \quad u = \frac{\pi}{\lambda} d\cos(\theta/2) \end{cases} \tag{3}$$

to replace Equation (1).

For mechanically rotating directional antenna, we can use radiation pattern:

$$g(\theta, \boldsymbol{\omega}_\theta) = \sum_{i=1}^{N_{ant}} \omega_{\theta,i} \cdot I(\theta) \tag{4}$$

to replace Equation (1). Here, θ denotes the antenna's rotating angle, $\boldsymbol{\omega}_\theta$ is the antenna weights under θ, and $I(\theta)$ is an indicator function expressed by:

$$I(\theta) = \begin{cases} 1, if\ \phi_j \leq \theta \leq \phi_{j+1}, \exists j \in [1, \cdots, M-1] \\ 0, otherwise \end{cases} \tag{5}$$

The antenna's rotating angle is divided into M parts, each of which is denoted by (ϕ_j, ϕ_{j+1}), $j \in [1, M-1]$. To control its directional antenna gain and hence change the RSS readings at ESCs, IU tunes the antenna weights when it rotates to the direction of each ESC between corresponding (ϕ_j, ϕ_{j+1}).

C. Radiation pattern tuning under radar's performance requirements

The performance requirements for IU radars vary a great deal based on their specific services, such as range or angle determination and target tracking. Without loss of generality, this paper focuses on tracking radar as an example to show that the proposed radiation pattern tuning strategy will not affect incumbent radar's performance.

Two required factors in tracking radar systems are probability of detection P_D and probability of false alarm P_{fa} under a specific range. Given the required P_D and P_{fa}, the acceptable signal-to-noise ratio (SNR) for radar receiver can be generated using many approximations. One very accurate model proposed in [16] is:

$$P_D \approx 0.5 \times erfc(\sqrt{-lnP_{fa}} - \sqrt{SNR + 0.5}) \tag{6}$$

Considering both noise and interference, the radar's signal-to-interference-noise ratio SINR can be computed as [17]:

$$SINR = \frac{P_S}{(1 + 10^{\frac{INR}{10}}) \times P_N} \tag{7}$$

where P_S is the received signal power; P_N is the noise power; and INR is the interference-to-noise ratio at the radar receiver, which is specified to be at most $-6dB$ by regulatory authorities [18].

Apparently, changing the radar's transmit power and antenna radiation pattern will affect its SINR and will possibly degrade the radar's performance. To avoid this situation, in this paper, we ensure that all the tuning strategies will not break the P_D, P_{fa} and SINR requirements by adding a constraint on the required minimum SINR in our problem formulation.

IV. Location Privacy Protection for Static IU

A simple model for preserving static IU's location privacy is presented in Figure 2, where the circles denotes ESC sensors, the triangle is an IU at its true location and the square represents a possible IU location where the IU can create the same ESC sensing result as at the true IU location. The shaded area is the union of all possible IU locations given the ESC sensing result. PL_k denotes the path loss between an IU's true location and the k_{th} ESC, and $\widehat{PL}_k$ denotes the path loss between the possible IU location and the k_{th} ESC. Pt represents the IU's transmit power at its true location. $\widehat{Pt}$ is the transmit power that the IU should use at the possible location. Gt_k and $\widehat{Gt}_k$ are the antenna gain of the IU at true location and the possible location in the direction of k_{th} ESC, respectively.

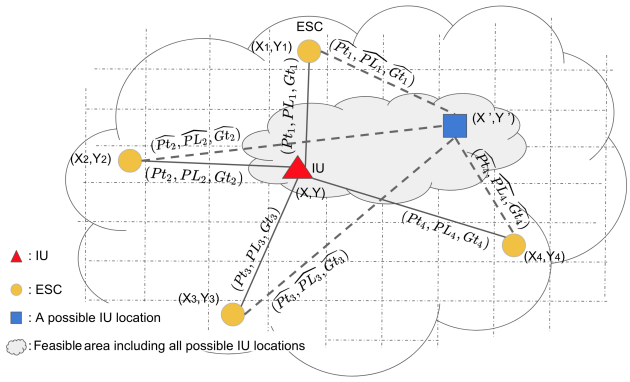

Figure 2. Model for static IU.

A. Problem Formulation

To understand how the IU can tune its transmitter to force the adversary to generate the largest possible IU area given ESCs' sensing outputs, we divide the analysis into two parts.

First part is from the adversary's perspective to compute the area of possible IU locations; second part is for IU to control the size of this area by tuning the transmit power and radiation pattern or rotating directional antenna gain. As in Figure 2, the space is segmented into grids to simplify the procedure of contouring the possible location area. Each grid is represented by its center position.

*1) **From adversary's perspective**:* Suppose the space is uniformly divided into N grids. There are K ESCs and their locations are denoted by (x_k, y_k), $k = 1, 2, ..., K$. The true location of the IU is (x, y). Each ESC will have a RSS reading received from the IU. The received power at the k_{th} ESC from the IU at true location (x, y) is Pr_k, and the received power at the k_{th} ESC if the IU is at the i_{th} grid l_i is denoted by $\widehat{Pr}_{i,k}$. The $< \widehat{\boldsymbol{\omega}}, \widehat{Pt} >$ tuple represents a feasible combination of antenna weight vector and transmit power that generates a $\widehat{Pr}_{i,k}$ approximately the same as Pr_k if IU locates at grid l_i.

After obtaining Pr_k from ESCs, adversaries will determine how many grids are possible IU locations. To do this, an adversary traverses every grid l_i to check whether, if the IU is at l_i, there exists a $< \widehat{\boldsymbol{\omega}}, \widehat{Pt} >$ tuple that makes every $\widehat{Pr}_{i,k}$ approximate to the corresponding Pr_k within a small noise threshold δ. If the solution exists, this grid l_i will be determined as a possible IU location and the number of possible locations $N_{possibleLoc}$ will be increased. This procedure is illustrated in Table I, where Z is the set of of the possible locations of the IU.

Table I

From an adversary's perspective:
given $Pr_k, \forall k = 1, 2, \cdots, K$
for each l_i, $\forall i = 1, 2, \cdots N$
find $< \widehat{\boldsymbol{\omega}}, \widehat{Pt} >$:
$\widehat{\boldsymbol{\omega}} \in [\boldsymbol{\omega}_{min}, \boldsymbol{\omega}_{max}]$, $\widehat{Pt} \in [Pt_{min}, Pt_{max}]$
that satisfy: $\left\| Pr_k - \widehat{Pr}_{i,k}(\widehat{\boldsymbol{\omega}}, \widehat{Pt}) \right\| \leq \delta$,
$\forall k = 1, 2, \cdots, K; i = 1, 2, \cdots N$
if solution exists
$N_{possibleLoc} = N_{possibleLoc} + 1$
$Z = Z \cup l_i$

$\widehat{Pr}_{i,k}(\widehat{\boldsymbol{\omega}}, \widehat{Pt})$ in the formulation is computed by:

$$\widehat{Pr}_{i,k}(\widehat{\boldsymbol{\omega}}, \widehat{Pt}) = \widehat{Pt}_i + \widehat{Gt}_{i,k}(\widehat{\boldsymbol{\omega}}) - PL_{i,k} + Gr - Lr \quad (8)$$

where $\widehat{Pt}_i$ is what the transmit power of the IU should be if it is located at l_i and $\widehat{Pt}_i \in [Pt_{min}, Pt_{max}]$. Here, Pt_{min} and Pt_{max} respectively denote the minimum and maximum IU transmit power. Gr and Lr are the gain and loss at the receiver side. $\widehat{Gt}_{i,k}(\widehat{\boldsymbol{\omega}})$ denotes the feasible antenna gain of the IU at l_i towards the direction of k_{th} ESC, which is calculated by:

$$\widehat{Gt}_{i,k}(\widehat{\boldsymbol{\omega}}) = 10log_{10} \left| g(\theta_{i,k}, \widehat{\boldsymbol{\omega}}) \right|^2 \quad (9)$$

where $g(\theta, \boldsymbol{\omega})$ is the function of the antenna's radiation pattern.

In Equation (8), the expected path loss $PL_{i,k}$ from the center of l_i to the k_{th} ESC is expressed as:

$$PL_{i,k} = 20log_{10}(\frac{4\pi}{\lambda}) + 10nlog_{10}(d_{i,k}) \quad (10)$$

where n is the path loss exponent, which is set to $n = 2$ in this paper. $d_{i,k}$ denotes the distance between l_i and the k_{th} ESC, and λ denotes the transmitted wave length. However, our analysis is not constrained to this model. We can plug path loss models with other geometric forms into the analysis by replacing Equation (10) with their corresponding functions.

After traversing all the grids through the procedure discussed above, the adversary is able to depict an area of possible locations for the targeted IU.

*2) **From IU's perspective**:* Besides preserving its location privacy, an IU first needs to complete its tasks (e.g. object-tracking in this paper), hence any change it makes on transmit power or antenna gain must ensure that SINR at radar receiver should be no smaller the required minimum SNR (SNR_{min}). To protect its location privacy, the IU tunes its transmit power Pt and antenna weight vectors $\boldsymbol{\omega}$ to control the RSS readings at ESCs, and attempts to find a group of readings that ensures the adversary to compute the largest area of IU's possible locations. Here, we assume that the IU knows the locations of all surrounding ESC sensors, which are published by FCC according to 3.5GHz regulation.

The above problem from IU's perspective is formulated in Table II. In Table II, for each l_i, if there exist two groups of IU parameters, $< \boldsymbol{\omega}, Pt >$ for IU at true location and $< \widehat{\boldsymbol{\omega}}, \widehat{Pt} >$ for IU at l_i, that make the corresponding $Pr_k(\boldsymbol{\omega}, Pt)$ and $\widehat{Pr}_{i,k}(\widehat{\boldsymbol{\omega}}, \widehat{Pt})$ at ESCs approximately the same, and also satisfy the SNR requirement in which SNR_{min} is the minimum SINR for radar operation, the IU confirms this l_i to be a possible IU location and increases the count of possible locations $N(\boldsymbol{\omega}, Pt)_{possibleLoc}$. Finally, the IU can obtain a set of $< \boldsymbol{\omega}, Pt >$ that maximize the $N(\boldsymbol{\omega}, Pt)_{possibleLoc}$, and these $< \boldsymbol{\omega}, Pt >$s are the optimal choices for IU's transmit power and antenna weight vector.

Table II

From IU's perspective:
for each l_i, $\forall i = 1, 2, \cdots N$
find $\boldsymbol{\omega}$, Pt, $\widehat{\boldsymbol{\omega}}$, $\widehat{Pt}$:
$\boldsymbol{\omega}, \widehat{\boldsymbol{\omega}} \in [\boldsymbol{\omega}_{min}, \boldsymbol{\omega}_{max}]$, $Pt, \widehat{Pt} \in [Pt_{min}, Pt_{max}]$
that satisfy: constraint 1: $SINR(\boldsymbol{\omega}, Pt) \geq SNR_{min}$
constraint 2: $\left\| Pr_k(\boldsymbol{\omega}, Pt) - \widehat{Pr}_{i,k}(\widehat{\boldsymbol{\omega}}, \widehat{Pt}) \right\| \leq \delta$,
$\forall k = 1, 2, \cdots, K; i = 1, 2, \cdots N$
if solution exists
$N(\boldsymbol{\omega}, Pt)_{possibleLoc} = N(\boldsymbol{\omega}, Pt)_{possibleLoc} + 1$
$Z(\boldsymbol{\omega}, Pt) = Z(\boldsymbol{\omega}, Pt) \cup l_i$
$\boldsymbol{\omega}_{opt}, Pt_{opt} = \underset{\boldsymbol{\omega}, Pt}{\operatorname{argmax}} N(\boldsymbol{\omega}, Pt)_{possibleLoc}$

Claim 1: The problem in Table II is NP-hard in general.
Proof: See Appendix A.

B. Solving The Problem

1) Approximation Algorithm: Since the problem of preserving static IU's location privacy formulated in Table II is generally NP-hard, we cannot obtain the optimal solution by directly solving it. Therefore, in this subsection, we introduce a heuristic algorithm whose results approximate the optimal solutions. In the next subsection, we will explain the worst

case where our heuristic algorithm is deviated from the optimal solution. We will also provide an analysis on how to determine whether the worst case will happen at given circumstances.

To find the optimal $< \boldsymbol{\omega}, Pt > s$ that maximize the number of possible locations, instead of searching over continuous variable spaces as in Table VIII, we uniformly sample each variable into discrete points such that $\boldsymbol{\omega} \in [\boldsymbol{\omega}_1, \boldsymbol{\omega}_2, \cdots, \boldsymbol{\omega}_{N_1}]$ and $Pt \in [Pt_1, Pt_2, \cdots, Pt_{N_2}]$. We define a tuple $U_i =< \boldsymbol{\omega}_{n_1}, Pt_{n_2} > (\forall n_1 \in [1, N_1],\ n_2 \in [1, N_2],\ i \in [1, N_1 N_2])$ as a sampled IU transmit parameter setting. In this way, the problem formulated in Table II is approximately converted to the problem of finding the optimal U_i among all the sampled discrete parameter settings. Next, we describe how to find this optimal U_i that maximize the number of possible IU locations.

As in Table II, if a grid l_i is a possible IU location, there must exist a real IU parameter $U_i =< \boldsymbol{\omega}_{n_1}, Pt_{n_2} >$ at the IU's true location and at least another IU parameter set $\widehat{U_i} =< \widehat{\boldsymbol{\omega}}, \widehat{Pt} >$ for an IU located at l_i, such that both constraint 1 and 2 are satisfied in Table II.

To find the condition where such a U_i and $\widehat{U_i}$ pair exists, let us first exam constraint 1. Note that U_i at the IU's true location must satisfy constraint 1 (the radar's SNR requirement). In addition, according to Equation (7), $SINR \propto P_S$, $P_S \propto P_t + G_{target}(\boldsymbol{\omega}) + A$, where A denotes all the other constant parameters. Based on Equation (1), (3) and (4), we can further see that for many commonly used antennas, $G_{target}(\boldsymbol{\omega}) \propto \boldsymbol{\omega}$ where $G_{target}(\boldsymbol{\omega})$ denotes the antenna gain of IU towards the direction of the target. Thus, $SINR$ is monotonically increasing with respect to P_t and $\boldsymbol{\omega}$. This means that constraint 1 directly restricts the feasible domain of $U_i =< \boldsymbol{\omega}_{n_1}, Pt_{n_2} >$. Essentially, for l_i to be a possible IU location, in constraint 1's feasible domain of U_i, a pair of U_i and $\widehat{U_i}$ that satisfies constraint 2 must exist.

Next, we find the condition that such a $\widehat{U_i}$ exist for a given U_i in the feasible domain of constraint 1. Let us look at the relation between $\widehat{Pr}$ and $\widehat{U_i} =< \widehat{\boldsymbol{\omega}}, \widehat{Pt} >$ first. According to Equation (8), $\widehat{Pr}$ is monotonically increasing at $\widehat{P}_t$ and $\widehat{\boldsymbol{\omega}}$. Hence, no matter which l_i is considered, the minimum received power at k_{th} ESC from l_i is found at minimum $\widehat{P}_t$ and minimum $\widehat{\boldsymbol{\omega}}$, that is, $min\_\widehat{Pr}_{i,k} = \widehat{Pr}_{i,k}(\boldsymbol{\omega}_{min}, Pt_{min})$; and the maximum received power at each ESC is found at maximum $\widehat{P}_t$ and maximum $\widehat{\boldsymbol{\omega}}$, that is, $max\_\widehat{Pr}_{i,k} = \widehat{Pr}_{i,k}(\boldsymbol{\omega}_{max}, Pt_{max})$.

Due to the monotonicity of $\widehat{Pr}$ at $\widehat{\boldsymbol{\omega}}$ and $\widehat{Pt}$, for a grid l_i, the condition for $\widehat{U_i}$ to exist can be expressed as:

$$min\_\widehat{Pr}_{i,k} - \delta \leq Pr_k(\boldsymbol{\omega}_{n_1}, Pt_{n_2}) \leq max\_\widehat{Pr}_{i,k} + \delta \quad (11)$$

$\forall k = 1, 2, \cdots, K$. When this condition is satisfied, there must exist at least one $\widehat{U_i} =< \widehat{\boldsymbol{\omega}}, \widehat{Pt} >$ for IU at l_i that satisfies constraint 2, i.e.: $\forall k = 1, 2, \cdots, K$

$$\widehat{Pr}_{i,k}(\widehat{\boldsymbol{\omega}}, \widehat{Pt}) - \delta \leq Pr_k(\boldsymbol{\omega}_{n_1}, Pt_{n_2}) \leq \widehat{Pr}_{i,k}(\widehat{\boldsymbol{\omega}}, \widehat{Pt}) + \delta \quad (12)$$

Based on the discussion above, we design a brute-force algorithm in Table III that searches for the optimal tuple U_i as follows. The algorithm iterates through all possible U_i samples. For each U_i that is in constraint 1's feasible domain, the algorithm then iterates through all possible l_i locations. For each l_i location, if $\widehat{U_i}$ that satisfies Equation (11) can be found, l_i is a possible IU location and the algorithm increases the count of possible IU location for U_i. Eventually, the U_i of the maximum possible location count is identified.

Table III

Heuristic Algorithm:

suppose IU is at location (x, y)
for each l_i, $\forall i = 1, 2, \cdots N$
  compute the possible minimum received power $min\_\widehat{Pr}_{i,k}$ and maximum received power $max\_\widehat{Pr}_{i,k}$ at k_{th} ESC by:
  $min\_\widehat{Pr}_{i,k} = \widehat{Pr}_{i,k}(\boldsymbol{\omega}_{min}, Pt_{min})$
  $max\_\widehat{Pr}_{i,k} = \widehat{Pr}_{i,k}(\boldsymbol{\omega}_{max}, Pt_{max})$
  $\forall k = 1, 2, \cdots, K$
  for each tuple U_i = [$\boldsymbol{\omega}_{n_1}$, Pt_{n_2}]
  $\forall n_1 \in [1, 2, \cdots, N_1]$, $n_2 \in [1, 2, \cdots, N_2]$
    compute $SINR(U_i)$
    if $SINR(U_i) \geq SNR_{min}$
      compute $Pr_k(\boldsymbol{\omega}_{n_1}, Pt_{n_2})$
      if $min\_\widehat{Pr}_{i,k} - \delta \leq Pr_k(\boldsymbol{\omega}_{n_1}, Pt_{n_2}) \leq max\_\widehat{Pr}_{i,k} + \delta$, $\forall k = 1, 2, \cdots, K$
      /* count the number of possible locations corresponding to each IU configuration */
      $N(\boldsymbol{\omega}_{n_1}, Pt_{n_2})_{possibleLoc} = N(\boldsymbol{\omega}_{n_1}, Pt_{n_2})_{possibleLoc} + 1$
      /* record the area of possible locations corresponding to each IU configuration */
      $Z(\boldsymbol{\omega}_{n_1}, Pt_{n_2}) = Z(\boldsymbol{\omega}_{n_1}, Pt_{n_2}) \cup l_i$
    ($Z(\boldsymbol{\omega}_n, Pt_n)$: possible IU area given $\boldsymbol{\omega}_n, Pt_n$)

$\boldsymbol{\omega}_{opt}, Pt_{opt} = \underset{\boldsymbol{\omega}, Pt}{\operatorname{argmax}} N(\boldsymbol{\omega}, Pt)_{possibleLoc}$

2) Worst case: Table III's algorithm first samples the variable spaces and then traverses all the tuples of sampled variables for each l_i and each ESC to determine whether it is a possible location for IU. If the variable space is sampled finely enough, we can approach the optimal solution boundlessly. Apparently, the accuracy of the heuristic algorithm is closely related to the sampling interval. In this section, we define the worst case for the algorithm and provide the relation between the error and sampling interval.

The worst case occurs when the algorithm in Table III deviates the furthest in its computation results from the algorithm in Table II. This happens when all discrete samples of U_i in Table III cannot satisfy the constraints, while feasible setting of parameters do exist between sample intervals for algorithm in Table II. In the following, we analyze the mathematical conditions when the worst case happens.

Let us look at a simple scenario for the worst case. In the worst case, for a sampled position l_i, we cannot find any sampled parameter set $U_i =< \boldsymbol{\omega}_{n_1}, Pt_{n_2} >$ that makes l_i a possible IU location in Table III. But, there exists at least a $U_i =< \boldsymbol{\omega}_{n_1} + \Delta\boldsymbol{\omega},\ Pt_{n_2} + \Delta p >$, that satisfies the conditions for l_i to be IU's possible location in Table II, where $\Delta\boldsymbol{\omega}, \Delta p$ are small portions of the corresponding sample intervals. The lengths of complete sample intervals are denoted as Δp_{max} and $\Delta\omega_{max}$ respectively. Note that when $\Delta\boldsymbol{\omega}, \Delta p$ equal to 0 or a complete sample interval, the point at $< \boldsymbol{\omega}_{n_1} + \Delta\boldsymbol{\omega}, Pt_{n_2} + \Delta p >$ then becomes a sample U_i in Table III. For

example, $U_i =< \boldsymbol{\omega}_{n_1} + \Delta\boldsymbol{\omega}_{max}, Pt_{n_2} + \Delta p_{max} >$ equals to tuple $U_{i+1} =< \boldsymbol{\omega}_{n_1+1}, Pt_{n_2+1} >$.

Given above assumptions, we have the following group of inequalities for the worst case:

$$\begin{cases} Pr_k(\boldsymbol{\omega}_{n_1}, Pt_{n_2}) < \widehat{min\_Pr}_{i,k} - \delta \\ or \\ Pr_k(\boldsymbol{\omega}_{n_1}, Pt_{n_2}) > \widehat{max\_Pr}_{i,k} + \delta \\ \forall n_1, m_1 \in [1, N_1],\ \forall n_2, m_2 \in [1, M_1] \\ \widehat{min\_Pr}_{i,k} - \delta \le Pr_k(\boldsymbol{\omega}_{n_1} + \Delta\boldsymbol{\omega}, Pt_{n_2} + \Delta p) \le \\ \widehat{max\_Pr}_{i,k} + \delta, \exists n_1 \in [1, N_1],\ n_2, \in [1, N_2] \\ 0 \le \Delta p \le \Delta p_{max}; 0 \le \Delta\boldsymbol{\omega} \le \Delta\omega_{max} \end{cases} \tag{13}$$

Note that the above inequality does not include formulas that are derived from constraint 1. This is because, due to the monotonically increasing nature of P_S in respect to U_i, if two neighboring sample U_i and U_{i+1} all fail constraint 1 in Table III, then there does not exist any other U_j in their sample interval that can satisfy constraint 1 in Table II.

To find the $\Delta\boldsymbol{\omega}, \Delta p$ that can solve inequalities (13), we define a function f_{U_i} for a sample U_i as $f_{U_i}(\Delta\boldsymbol{\omega}, \Delta p) := Pr_k(\boldsymbol{\omega}_{n_1} + \Delta\boldsymbol{\omega}, Pt_{n_2} + \Delta p)$.

As discussed before, received power Pr_k at k_{th} ESC is monotonically increasing at Pt and $\boldsymbol{\omega}$. Hence, $f_{U_i}(\Delta\boldsymbol{\omega}, \Delta p)$ is monotonically increasing at $\Delta\boldsymbol{\omega}$ and Δp. The maximum of $f_{U_i}(\Delta\boldsymbol{\omega}, \Delta p)$ is determined as

$$f_{max} = f_{U_i}(\Delta\boldsymbol{\omega}_{max}, \Delta p_{max}) = f_{U_{j1}}(0, 0),$$

where the tuple $U_{j1} =< \boldsymbol{\omega}_{n_1} + \Delta\boldsymbol{\omega}_{max}, Pt_{n_2} + \Delta p_{max} >=< \boldsymbol{\omega}_{n_1+1}, Pt_{n_2+1} >$, and the minimum can be found at

$$f_{min} = f_{U_i}(\Delta\boldsymbol{\omega}_{min}, \Delta p_{min} = f_{U_{j2}}(0, 0).$$

where $U_{j2} =< \boldsymbol{\omega}_{n_1} + \Delta\boldsymbol{\omega}_{min}, Pt_{n_2} + \Delta p_{min} >=< \boldsymbol{\omega}_{n_1}, Pt_{n_2} >$. Hence f_{max} is obtained at U_{j1}, $f_{max} = Pr_k(\boldsymbol{\omega}_{n_1+1}, Pt_{n_2+1})$ and f_{min} is obtained at U_{j2}, $f_{min} = Pr_k(\boldsymbol{\omega}_{n_1}, Pt_{n_2})$. According to the assumptions, there are three cases for f_{max} and f_{min}:

1) $f_{min} \le f_{max} < \widehat{min\_Pr}_{i,k} - \delta$: since we cannot find any $f_{U_i}(\Delta\boldsymbol{\omega}, \Delta p)$ between f_{max} and f_{min} that satisfies $\widehat{min\_Pr}_{i,k} - \delta \le f_0 \le \widehat{max\_Pr}_{i,k} + \delta$, the inequalities are infeasible.
2) $f_{max} \ge f_{min} > \widehat{max\_Pr}_{i,k} + \delta$: same as above.
3) $f_{max} > \widehat{max\_Pr}_{i,k} + \delta$ and $f_{min} < \widehat{min\_Pr}_{i,k} - \delta$: since $f_{U_i}(\Delta\boldsymbol{\omega}, \Delta p)$ is continuous within $[f_{min}, f_{max}]$, there must be a set of solutions that satisfy $\widehat{min\_Pr}_{i,k} - \delta \le f_{U_i}(\Delta\boldsymbol{\omega}, \Delta p) \le \widehat{max\_Pr}_{i,k} + \delta$. Only in this case the inequalities are feasible such that the worst case happens.

Hence, for k_{th} ESC, if all sample of IU parameter settings cannot make l_i a possible IU location, whether a worst case exists between tuple $U_i =< \boldsymbol{\omega}_{n_1}, Pt_{n_2} >$ and its adjacent tuple $U_{i+1} =< \boldsymbol{\omega}_{n_1+1}, Pt_{n_2+1} >$ can be examined directly using the values of $Pr_k(\boldsymbol{\omega}_{n_1}, Pt_{n_2})$ and $Pr_k(\boldsymbol{\omega}_{n_1+1}, Pt_{n_2+1})$. If the values satisfy the condition in the third case, we can say that the worst case exists between $\boldsymbol{\omega_{n_1}}$,$Pt_{n_2}$ and $\widehat{\omega}_{m_1}, \widehat{Pt}_{m_2}$. Otherwise, it does not.

V. Location Privacy Protection For Moving IU

So far, we discussed how to preserve IU location privacy for a static IU. However, IUs like shipborne radars are often mobile. It is also critical to protect their location privacy even when they are moving. We consider two location privacy cases for mobile IUs. The first case is to hide an IU's real-time current location and the second case is to hide an IU's entire moving trajectory. Hiding real-time current location prevents the IU from being located at the current moment, while hiding moving trajectory attempts to keep additional information confidential, such as the IU's past route and moving direction. Same as in the static IU model, adversaries have the capability to calculate the area where IU may appear at each moment using both current and historical RSS readings at ESCs. Meanwhile, they can also estimate the IU's possible moving ranges based on the feasible range of IU speed.

In this section, we present our algorithm that tunes an IU's transmit power and radiation pattern during movement to optimally preserve its privacy. We assume that the IU knows its future moving route, which is reasonable since a mobile IU usually knows where it is going and hence can plan its route beforehand. The design of our algorithm is based on the relation between IU's tunable parameters and the adversary's estimation of the possible moving traces of IU. We assume the IU can adjust its transmit power and radiation pattern at any moment subject to hardware restrictions on its functionality.

A. Location Privacy Model for Moving IUs

Model for moving IU is the same as in Figure 2 except that the IU is mobile in this case. Consider a discrete time range $T = [t_1, ..., t_n]$, where each time slot t_i is of the same size. During time T, IU is moving along a planned route and ESCs detect the IU's signal and record the RSS readings at each time slot. From these RSS readings, the possible IU area at a time slot $t_i \in T$ can be computed and is denoted as Z_i.

It is important to note that computing Z_t is different from Section IV's computation of the area of static IU possible locations. This is because the adversary has access to historical RSS data and there is realistic upper limit on IU moving speed. From the adversary's point of view, the past possible location area Z_{i-1} constrains the possible locations of IU at current time t_i because the distances between possible locations cannot be larger than an IU's maximum moving speed times a time slot. For example, the shape of Z_1 will restrict the area of Z_2, and the shrunken Z_2 will further impact Z_3. Conversely, feasible area of possible IU locations at current time t_i (i.e. Z_i) will also cause shrinking of the possible IU area estimation for previous time slots. This essentially means that the current Z_i will also reduce Z_{i-1} and all the way to Z_1, essentially restricting the size of the past moving trajectory. The algorithm in Table IV shows how the adversary can narrow down the possible location traces of moving IUs through such correlation between historical location estimation and current location estimation. In this algorithm, the adversary assumes the maximum speed of IU is Δ per time interval.

An example in Figure 3 shows how adversaries generate possible area for a moving IU using the algorithm in Table IV. The procedure can be divided into three steps: (1) Step 1: Based on Table I, an adversary uses the RSS readings obtained from ESCs' sensing results to compute the initial estimations of Z_1 and Z_2 on IU's possible area at time t_1 and t_2. (2) Step 2: Since the past possible location area Z_{i-1} constrains the possible locations of IU at current time t_i, the adversary update current estimation Z_2 at t_2 based on the past estimation Z_1 at t_1. The blue area refers to the updated possible IU area at time t_2 and the gray area refers to the pruned old possible IU area at time t_2. It is no longer considered as possible area, because the locations inside the gray area cannot be reached by any locations in initial Z_1 within a time slot due to the IU speed limit. (3) Step 3: The gray area is removed from possible IU area Z_1 since the feasible IU area at current time t_2 will also impose an effect on feasible IU area of previous Z_1. Based on the 3 steps above, given a current time t_n, the adversary can obtain all the final possible IU area Z_j, $j \in [1, n]$.

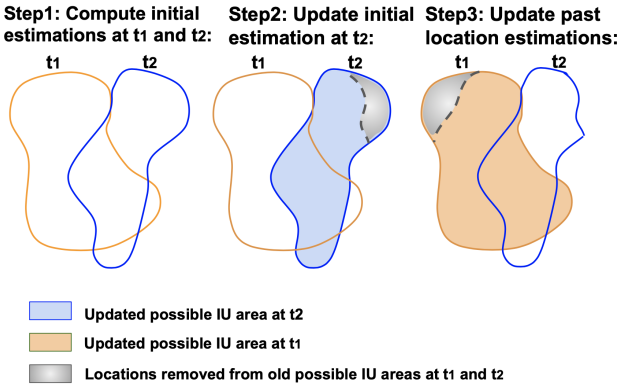

Figure 3. An example showing how adversary generates possible areas for moving IU.

Table IV

Adversary generates possible areas for moving IU:
At the current time t_n:
Given the RSS readings at t_n
Step 1: Compute initial estimation of Z_n using RSS readings according to Table I in Section IV.
Step 2: /* update current Z_n by Z_{n-1} */
$Z_n = \{l_i \| l_i \in Z_n$ and $\exists l_j \in Z_{n-1}$ such that $\| l_i - l_j \| \leq \Delta\}$
Step 3: /* Update past location trajectory based on Z_n*/
From $t_j = t_{n-1}$ to $t_j = t_1$:
$Z_j = \{l_k \| l_k \in Z_j$ and $\exists l_u \in Z_{j+1}$ such that $\| l_k - l_u \| \leq \Delta\}$

With the above assumption on how an adversary leverages historical ESC readings, the problem of maximizing the privacy protection for moving IUs must consider the correlation between past moving trajectory and current location estimation. Hence, selecting the optimal IU transmit parameters at each time slot is not equivalent to finding one single global optimal parameters for the entire time period. Instead, an IU must dynamically tune its antenna patterns and transmit power at each slot to defend its moving trajectory and current location. Next, we will present our analysis about (1) how an IU can hide its true moving trajectory; (2) how an IU can hide its real-time current location.

B. Conceal IU's Moving Trajectories

We know that an IU can change the RSS readings at ESC side by adjusting its transmit power and radiation pattern, so that it can control an adversary's estimation on the area of possible IU locations. Thus, assuming the IU knows its future route, it can make a plan of how to adjust these tunable parameters along its way to reduce the adversary's probability on finding out the IU's true trace. We define this probability as a summation of the reciprocal of the size of possible IU area Z_j ($\forall\, j \in [1, n]$) for every time slot t_j in T. The problem of concealing IU trajectory, thus, can be formulated as:

$$opt\boldsymbol{\omega}_j, optPt_{j,j\in[1,n]} = \underset{\boldsymbol{\omega}_j, Pt_j, j\in[1,n]}{\arg\min} \sum_{j=1}^{n} \frac{1}{size(Z_j(\boldsymbol{\omega}_j, Pt_j))} \tag{14}$$

The algorithm in Table V compute the above Equation (14). Here, we assume the adversary will use the algorithm in Table IV to compute Z_j and the IU can estimate the RSS readings at ESCs for each of its future location based on the published ESC locations and some radio propagation model.

Table V

IU maximize the number of possible traces:
Step 1: Discretizes the IU's future route plan into a series of points, where a point L_i corresponds to the planed IU position at time t_i.
Step 2: For each location point L_i, run algorithm in Table III to compute the set of $Z_i(\boldsymbol{\omega}_{n_1}, Pt_{n_2})$, which is the collection of possible location areas for each possible IU configuration at time t_i. Denote the set as $\widetilde{Z_i} = \{Z_i(\boldsymbol{\omega}_{n_1}, Pt_{n_2}) \|$ for all $(\boldsymbol{\omega}_{n_1}, Pt_{n_2})\}$
Step 3: For every possible sequence of IU parameter tuning, which is denoted as $s = \{(\omega_{n_1}, Pt_{n_2})_i \| i = 1...n\}$, retrieve the corresponding sequence of Z_i and narrow down these Z_i based on Step 2 and 3 in Table IV.
Step 4: Pick the best sequence S_{opt} that satisfies Equation (14) among all sequences.

C. Conceal IU's Real-time Location

Consider that an adversary is using the algorithm in Table IV to obtain the feasible area of possible IU locations at any moment given the IU parameters. If the IU wants to best conceal its location at a current time t_n, it needs to find a certain group of IU parameters that minimize the probability on finding out its true location at t_n, which can be formulated as minimizing the reciprocal of Z_n as follows:

$$opt\boldsymbol{\omega}_n, optPt_n = \underset{\boldsymbol{\omega}_n, Pt_n}{\arg\min} \frac{1}{size(Z_n(\boldsymbol{\omega}_n, Pt_n))} \tag{15}$$

An algorithm similar to the one in Section V-B can be used to find the solution for this goal. The only change is in Step

4, where the metric of selecting the optimal tuning sequence should be Equation (15) instead of Equation (14).

VI. Simulation Results

In this section, we simulate the static IU and the moving IU location privacy protection problem described in Section IV and V to analyze the feasibility of our privacy-protection scheme under different circumstances. We assume the IUs are equipped with tracking radars. Our simulation confirms that by adjusting its transmit power and antenna's radiation pattern, probability of the IU's location being detected by adversaries using ESCs' sensing outputs can be reduced to a very low level. We also analyze how different numbers of antenna elements, noise thresholds, and ESC number will affect the simulation results for preserving an IU's location privacy.

Simulation results for static IUs using circular phased array antenna are shown in Figure 4. The parameters used in this simulation are $N_{ant} = 2$ or 5, $\delta = 2dB$, $K = 4$, the grid length is set to $100m$. The target of IU's tracking radar is located in grid $(4, 104)$, which is approximately $10km$ away from the IU. P_D and P_{fa} are set to 0.96 and 10^{-6} at a range of $60km$. In Figure 4, the circle represents a true IU location, the plus signs represent ESCs' locations and the asterisks represent possible IU locations computed by adversaries. We can see that the true IU location is successfully hidden inside the computed possible locations. It is not surprising that the areas close around true location will have high probabilities to be a possible IU location, and the simulation results proved this speculation. However, there are many points very far away from the true location that still end up as possible IU locations, which shows the strong feasibility for preserving IU's static location privacy.

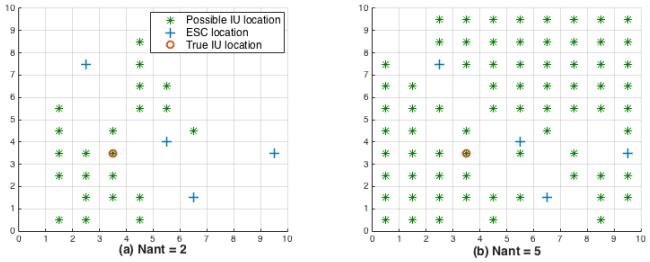

Figure 4. Examples showing maximized possible location area for static IU when $N_{ant} = 2$ and $N_{ant} = 5$.

In our simulation of mobile IUs, we set the speed of IU as between 0 to 2 (grid per time interval). Figure 5 shows an example of possible IU locations at 6 consecutive points of time while an IU is moving, where N_{ant} is set to 2 and K equals 4. As in each sub-figure, the IU is successfully hidden within a bunch of possible IU locations, which is a positive factor for protecting the IU's location information. Though the possible locations tend to appear around the true IU location, many of them also exist in distant grids, which is another positive factor to preserve moving IU's location privacy.

Figure 6 (a) shows 10 randomly picked possible traces for one IU's real route (There are many more that we cannot show for figure clarity reason). We can see that merely using 2 antenna elements, an IU can still befog ESCs with many fake traces.

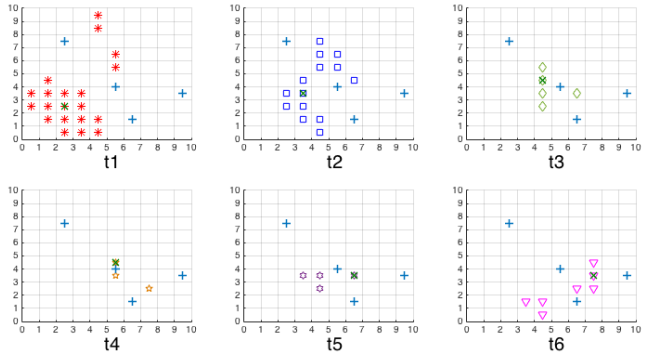

Figure 5. Maximal areas of possible IU locations at each point of time. The crosses in all sub-figures denote the true IU locations, the plus signs denote the ESC locations, and the other markers are computed possible IU locations.

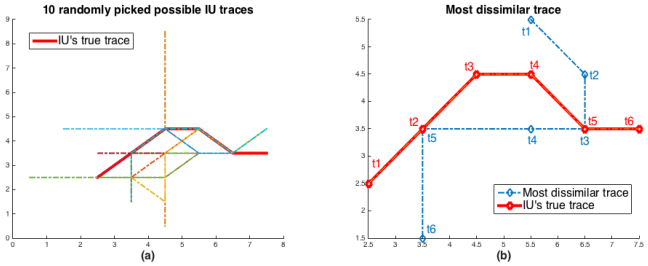

Figure 6. Sub-figure (a) shows 10 randomly picked possible IU traces in dash-dot lines and the IU's real route in a sold red line. Sub-figure (b) shows an example of the most dissimilar trace, $t_i, i \in [1, 6]$ denotes each time step.

The most dissimilar trace to the true IU route is presented in Figure 6 (b). Similarity between two traces is measured by:

$$dist = \sum_{t=t_1}^{t_n} \sqrt{(L1_t - L2_t)^2} \tag{16}$$

where n is the number of time points of these two traces, and $L1_t$ is the location of trace 1 at time t ($t \in [t_1, t_n]$), $L2_t$ is the location of trace 2 at time t. As in Figure 6, the existence of the possible traces that are far away from the true trace make preservation of moving IU's location privacy feasible.

Table VI shows the number of possible IU trajectories computed under five different routes of the IU, and the amount of possible trajectories varies much on different IU routes. The maximal distance refers to the similarity between true IU route and possible traces. It is computed by Equation (16). The total distance between a true route and a possible trace within 6 points of time is as large as thousands. The average Euclidean distance (max dist./6 time points) between true IU trace and possible IU trace is usually larger than $200m$.

Next, we assume an IU moves within 6 time steps, and record the number of possible IU locations at last time step, which can be regarded as the possible current locations for the IU. We also record the number of possible IU traces along

Table VI
POSSIBLE IU TRACES COMPUTED UNDER 5 DIFFERENT IU ROUTES

IU routes number	1	2	3	4	5
Possible routes	1389	2567	2158	7169	4443
max dist. (×100m)	18.11	14.36	16.99	15.63	22.39

Table VII
NUMBER OF POSSIBLE IU TRACES AND CURRENT LOCATIONS

	δ	K	$N_{ant}=2$	$N_{ant}=5$
Possible IU traces	1 dB	4	40	6124905
		6	14	4924908
	2 dB	4	1389	10153583
		6	186	9037580
Possible IU locations	1 dB	4	4	74
		6	2	71
	2 dB	4	12	89
		6	8	86

the way. Three general trends in Table VII can be observed. First, both the number of possible current IU locations and the number of possible IU trajectories increases when the number of antenna elements N_{ant} increases. This is because a smart antenna array with more elements has more flexibility in adjusting the radiation pattern. Mathematically, more antenna elements leads to more tunable $\boldsymbol{\omega}$ and hence larger degree of freedom in the problems. Therefore, it is easier for an IU to create different RSS readings at ESCs. Second, the number of possible IU locations and trajectories also increases as the value of acceptable noise level increases. The reason is that larger noise level indicates looser bounds in determining a possible IU location. Third, both the numbers of possible IU locations at last time step and possible IU trajectories decrease when the number of ESCs (i.e. K) grows. Mathematically, adding ESCs means adding extra constraints to problem in Table II, and further reduce the l_i's probability of being regarded as a possible IU location.

VII. CONCLUSION

In this paper, we analyzed the feasibility of preserving both static and moving IU's location privacy by adjusting its radiation pattern and transmit power. We defined the way to preserve an IU's location privacy as to hide its true location inside all other possible IU locations estimated by adversaries using ESCs' RSS readings. We investigated how an IU's transmit power, radiation pattern and ESC deployment influence the IU's capability of hiding its location. We formulated the problem for a static IU to protect its location information, and show this feasibility problem is NP-hard in general. We then proposed a sampling method to solve this problem. Based on this, we then formulated the problem for moving IUs, in which two cases are analyzed: the first is to protect an IU's moving traces and the second is to protect its real-time location information. Our analysis provides insightful guidance for an IU to preserve its location information whether it is static or moving against the potential localization attack of ESCs. Simulation results also show that our approach provides great effectiveness for an IU's location privacy protection.

APPENDIX

A. Proof of Claim 1

To prove the feasibility of the problem in Table II, let us consider a sub-problem, which is to determine whether a single l_i is a possible IU location:

Table VIII

sub-problem:

find any $\boldsymbol{\omega}$, Pt, $\widehat{\boldsymbol{\omega}}$, $\widehat{Pt}$
that satisfy: $SINR \geq SNR_{min}$

$$\left| 10log_{10}\frac{\widehat{Pt}\left|\widehat{\boldsymbol{\omega}}^H\widehat{\boldsymbol{h}_k}\right|^2}{(\frac{4\pi}{\lambda}\widehat{d}_k)^2} - 10log_{10}\frac{Pt|\boldsymbol{\omega}^H\boldsymbol{h_k}|^2}{(\frac{4\pi}{\lambda}d_k)^2}\right| \leq \delta \quad \forall k=1,2,\cdot,K$$

$$\Leftrightarrow \frac{1}{\delta'} \leq \left| \frac{\widehat{Pt}\left|\widehat{\boldsymbol{\omega}}^H\widehat{\boldsymbol{h}_k}\right|^2}{(\frac{4\pi}{\lambda}\widehat{d}_k)^2} \Big/ \frac{Pt|\boldsymbol{\omega}^H\boldsymbol{h_k}|^2}{(\frac{4\pi}{\lambda}d_k)^2} \right| \leq \delta'$$

In Table VIII, SINR at a radar receiver is computed using Equation (7), SNR_{min} is calculated based on Equation (6) given the required minimum P_D and maximum P_{fa}.

Firstly, we relax the SINR constraint from the sub-problem by setting SNR_{min} to be infinitesimal. Then we have the relaxed version of sub-problem without the SINR constraint. The original sub-problem's feasible domain is a subset of the relaxed sub-problem's feasible domain. If we prove the relaxed sub-problem to be NP-hard, the original sub-problem should also be NP-hard.

To prove the feasibility of the relaxed sub-problem, let us consider its complementary problem (for simplicity, let $\widehat{\boldsymbol{f}_k} = \frac{\widehat{\boldsymbol{h}_k}}{\frac{4\pi}{\lambda}\widehat{d}_k}$ and $\boldsymbol{f_k} = \frac{\boldsymbol{h_k}}{\frac{4\pi}{\lambda}d_k}$) in Table IX.

Table IX

complementary problem:

$$\max_{\boldsymbol{\omega},Pt,\widehat{\boldsymbol{\omega}},\widehat{Pt}} \; t = \min_k \left\{ \frac{\widehat{Pt}\left|\widehat{\boldsymbol{\omega}}^H\widehat{\boldsymbol{f}_k}\right|^2}{Pt|\boldsymbol{\omega}^H\boldsymbol{f_k}|^2} \right\}_{k=1}^{K}$$

s.t. $\dfrac{\widehat{Pt}\left|\widehat{\boldsymbol{\omega}}^H\widehat{\boldsymbol{f}_k}\right|^2}{Pt|\boldsymbol{\omega}^H\boldsymbol{f_k}|^2} \leq \delta', \; k=1,2,\cdot,K.$

equivalent problem:

find any $\boldsymbol{\omega}$, Pt, $\widehat{\boldsymbol{\omega}}$, $\widehat{Pt}$
that satisfy: $\eta \leq \dfrac{\widehat{Pt}\left|\widehat{\boldsymbol{\omega}}^H\widehat{\boldsymbol{f}_k}\right|^2}{Pt|\boldsymbol{\omega}^H\boldsymbol{f_k}|^2} \leq \delta'$
$\forall k=1,2,\cdot,K$

The relaxed sub-problem is feasible if and only if the solution t^* to complementary problem in Table IX satisfies $t^* \geq \frac{1}{\delta'}$ and it is infeasible if and only if $t^* < \frac{1}{\delta'}$. Conversely, assume relaxed sub-problem can be solved in polynomial time, then for any given value of η that lies in $[0, \delta']$, we can also solve the following equivalent problem in Table IX in polynomial time.

Comparing two problems in Table IX, if we can find the maximum value of η which makes equivalent problem feasible, we can obtain the solution to the complementary problem. Since $\eta \in [0, \delta]$, suppose there exists a turning point η' such that when $\eta \leq \eta'$, equivalent problem in Table IX is feasible, while for $\eta > \eta'$, the equivalent problem is infeasible. Thus this turning point η' is exactly the maximum value of η

and is the solution to the complementary problem in Table IX. Bisection method can be used here to find this turning point η'. Because bisection method computes within polynomial time, the reduction from complementary problem in Table IX to problem in Table VIII is also polynomial. Hence, to prove that relaxed sub-problem is NP-hard, we can first show complementary problem in Table IX is NP-hard.

Now consider the case where the solution to complementary problem in Table IX is obtained when $t^* = \frac{\widehat{Pt}\left|\widehat{\boldsymbol{\omega}}^H \widehat{\boldsymbol{f_k^*}}\right|^2}{Pt\left|\boldsymbol{\omega}^H \boldsymbol{f_k^*}\right|^2}$, and then we have Table X.

Table X

$$\begin{array}{l} \max\limits_{\boldsymbol{\omega}, Pt, \widehat{\boldsymbol{\omega}}, \widehat{Pt}} \dfrac{\widehat{Pt}\left|\widehat{\boldsymbol{\omega}}^H \widehat{\boldsymbol{f_k^*}}\right|^2}{Pt\left|\boldsymbol{\omega}^H \boldsymbol{f_k^*}\right|^2} \\ \text{s.t. } \dfrac{\widehat{Pt}\left|\widehat{\boldsymbol{\omega}}^H \widehat{\boldsymbol{f_k}}\right|^2}{Pt\left|\boldsymbol{\omega}^H \boldsymbol{f_k}\right|^2} \leq \delta' \\ \quad \dfrac{\widehat{Pt}\left|\widehat{\boldsymbol{\omega}}^H \widehat{\boldsymbol{f_k}}\right|^2}{Pt\left|\boldsymbol{\omega}^H \boldsymbol{f_k}\right|^2} \geq \dfrac{\widehat{Pt}\left|\widehat{\boldsymbol{\omega}}^H \widehat{\boldsymbol{f_k^*}}\right|^2}{Pt\left|\boldsymbol{\omega}^H \boldsymbol{f_k^*}\right|^2} \end{array}$$

To make the analysis simpler, we change the objective function in this formulation into logarithmic form. By moving $\frac{\widehat{Pt}\left|\widehat{\boldsymbol{\omega}}^H \widehat{\boldsymbol{f_k^*}}\right|^2}{Pt\left|\boldsymbol{\omega}^H \boldsymbol{f_k^*}\right|^2}$ to the other side of the inequality, the problem is finally reformulated as in Table XI.

Table XI

$$\begin{array}{l} \max\limits_{\boldsymbol{\omega}, Pt, \widehat{\boldsymbol{\omega}}, \widehat{Pt}} \; log\ \widehat{Pt} - log\ Pt + log\ \left|\widehat{\boldsymbol{\omega}}^H \widehat{\boldsymbol{f_k}}\right|^2 - log\ \left|\boldsymbol{\omega}^H \boldsymbol{f_k}\right|^2 \\ \text{s.t. } \dfrac{\widehat{Pt}\left|\widehat{\boldsymbol{\omega}}^H \widehat{\boldsymbol{f_k}}\right|^2}{Pt\left|\boldsymbol{\omega}^H \boldsymbol{f_k}\right|^2} \leq \delta' \\ \quad \dfrac{\widehat{Pt}\left|\widehat{\boldsymbol{\omega}}^H \widehat{\boldsymbol{f_k}}\right|^2}{Pt\left|\boldsymbol{\omega}^H \boldsymbol{f_k}\right|^2} - \dfrac{\widehat{Pt}\left|\widehat{\boldsymbol{\omega}}^H \widehat{\boldsymbol{f_k^*}}\right|^2}{Pt\left|\boldsymbol{\omega}^H \boldsymbol{f_k^*}\right|^2} \geq 0 \\ \Leftrightarrow \widehat{\boldsymbol{\omega}}^H \left(\frac{\widehat{Pt}}{Pt\left|\boldsymbol{\omega}^H \boldsymbol{f_k^*}\right|^2} \boldsymbol{f_k^*} \boldsymbol{f_k^{*H}} - \frac{\widehat{Pt}}{Pt\left|\boldsymbol{\omega}^H \boldsymbol{f_k}\right|^2} \boldsymbol{f_k} \boldsymbol{f_k^H} \right) \widehat{\boldsymbol{\omega}} \leq 0 \end{array}$$

This is a multivariate optimization problem. Commonly, to find absolute maximum and minimum values of such functions, we first try to determine all critical points of this function and evaluate it at these points. In our case, suppose we want to find the critical points over $\widehat{\boldsymbol{\omega}}$, we need to treat all the other variables as constants. Now the problem is reduced to a univariate problem. Hence, if we can show this reduced problem is NP-hard, we prove that problem in Table XI is NP-hard too.

As observed in Table XI, $\boldsymbol{f_k} \boldsymbol{f_k^H}$ now becomes a Hermitian positive semi-definite matrix and

$$\left(\frac{\widehat{Pt}}{Pt\left|\boldsymbol{\omega}^H \boldsymbol{f_k^*}\right|^2} \boldsymbol{f_k^*} \boldsymbol{f_k^{*H}} - \frac{\widehat{Pt}}{Pt\left|\boldsymbol{\omega}^H \boldsymbol{f_k}\right|^2} \boldsymbol{f_k} \boldsymbol{f_k^H} \right)$$

is an indefinite matrix. Thus, the reduced problem is a non-convex quadratically constrained quadratic programming (QCQP) problem, which is NP-hard in general [19]. Thus, complementary problem in Table IX is NP-hard in general and so is sub-problem in Table VIII. Since the sub-problem should be computed for each l_i in order to solve the problem in Table II, clearly problem in Table II is also NP-hard in general.

REFERENCES

[1] P. R. Vaka, S. Bhattarai, and J.-M. Park, "Location privacy of non-stationary incumbent systems in spectrum sharing," in *Global Communications Conference (GLOBECOM), 2016 IEEE*, pp. 1–6, IEEE, 2016.

[2] S. Bhattarai, J.-M. J. Park, B. Gao, K. Bian, and W. Lehr, "An overview of dynamic spectrum sharing: Ongoing initiatives, challenges, and a roadmap for future research," *IEEE Transactions on Cognitive Communications and Networking*, vol. 2, no. 2, pp. 110–128, 2016.

[3] Y. Dou, K. C. Zeng, H. Li, Y. Yang, B. Gao, C. Guan, K. Ren, and S. Li, "P 2-sas: preserving users' privacy in centralized dynamic spectrum access systems," in *Proceedings of the 17th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, pp. 321–330, ACM, 2016.

[4] S. Joshi, K. Manosha, M. Jokinen, T. Hänninen, P. Pirinen, H. Posti, and M. Latva-aho, "Esc sensor nodes placement and location from moving incumbent protection in cbrs," in *Proceedings of WInnComm 2016*, 2016.

[5] T. T. Nguyen, A. Sahoo, M. R. Souryal, and T. A. Hall, "3.5 ghz environmental sensing capability sensitivity requirements and deployment," in *Dynamic Spectrum Access Networks (DySPAN), 2017 IEEE International Symposium on*, pp. 1–10, IEEE, 2017.

[6] J. R. Agre and K. D. Gordon, "Summary of recent federal government activities to promote spectrum sharing," 2015.

[7] F. C. Commission *et al.*, "Wireless telecommunications bureau and office of engineering and technology establish procedure for registering environmental sensing capability sensors," *FCC Public Notice*, 2018.

[8] 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*, pp. 236–247, IEEE, 2014.

[9] 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*, pp. 7640–7645, IEEE, 2015.

[10] 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*, pp. 2486–2493, IEEE, 2017.

[11] H. Li, Y. Dou, C. Lu, D. Zabransky, Y. Yang, and J.-M. J. Park, "Preserving the incumbent users location privacy in the 3.5 ghz band," in *2018 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*, pp. 1–10, IEEE, 2018.

[12] H. Xiao, H. Zhang, Z. Wang, and T. A. Gulliver, "An rssi based dv-hop algorithm for wireless sensor networks," in *Communications, Computers and Signal Processing (PACRIM), 2017 IEEE Pacific Rim Conference on*, pp. 1–6, IEEE, 2017.

[13] J. Xiao, Z. Zhou, Y. Yi, and L. M. Ni, "A survey on wireless indoor localization from the device perspective," *ACM Computing Surveys (CSUR)*, vol. 49, no. 2, p. 25, 2016.

[14] T. Wang and Y. Yang, "Analysis on perfect location spoofing attacks using beamforming," in *INFOCOM, 2013 Proceedings IEEE*, pp. 2778–2786, IEEE, 2013.

[15] R. Vescovo, "Pattern synthesis with null constraints for circular arrays of equally spaced isotropic elements," *IEE Proceedings-Microwaves, Antennas and Propagation*, vol. 143, no. 2, pp. 103–106, 1996.

[16] D. O. North, "An analysis of the factors which determine signal/noise discrimination in pulsed-carrier systems," *Proceedings of the IEEE*, vol. 51, no. 7, pp. 1016–1027, 1963.

[17] N. N. Krishnan, R. Kumbhkar, N. B. Mandayam, I. Seskar, and S. Kompella, "Coexistence of radar and communication systems in cbrs bands through downlink power control," in *MILCOM 2017-2017 IEEE Military Communications Conference (MILCOM)*, pp. 713–718, IEEE, 2017.

[18] F. H. Sanders, R. L. Sole, B. L. Bedford, D. Franc, and T. Pawlowitz, "Effects of rf interference on radar receivers," *NTIA Report TR-06-444*, 2006.

[19] Z.-Q. Luo, W.-K. Ma, A. M.-C. So, Y. Ye, and S. Zhang, "Semidefinite relaxation of quadratic optimization problems," *IEEE Signal Processing Magazine*, vol. 27, no. 3, pp. 20–34, 2010.