Distributed and Secure Power Control for Secondary Users in Dynamic Spectrum Access

Yousi Lin[1], Peiwen Qiu[1], Yaling Yang[1], Xiaojiang (James) Du[2], and Jie Wu[2]

[1]Virginia Tech

[2]Temple University

Email: [1]{yousil94,peiwenq,yyang8}@vt.edu, [2]{dux,jiewu}@temple.edu

Abstract

In dynamic spectrum access (DSA), secondary transmitters (SU-TX) should only be allowed to transmit on a licensed channel belonging to incumbent users (IU) when the signal-to-interference-noise-ratio (SINR) requirements of both IUs and SUs can be satisfied at the same time. However, in many DSA systems, the location and interference level of an IU are often considered sensitive data that should not be revealed, making it very challenging to ensure the QoS of both the IU and SUs while protecting IU operation security. In this paper, we propose a novel distributed SU transmit power control algorithm to solve this challenge. Our scheme can enable SINR-guaranteed coexistence between SUs and IUs and protect IUs from harmful interference, while requiring no information directly from IUs. Environmental sensing capability (ESC)'s local measurements of IU signals also undergo a security masking process to ensure IU location cannot be derived from its outputs, providing strong privacy protection for IUs. Our scheme's convergence and stability properties, as well as its privacy-protection strength, are both theoretically analyzed and experimentally demonstrated through simulations.

Index Terms

dynamic spectrum access, secondary user, power control.

I. Introduction

Due to the rapid growth in wireless communication demands, the frequency spectrum is becoming increasingly crowded. Dynamic spectrum access (DSA) is then proposed to enable the spectrum sharing between incumbent users (IUs) and secondary users (SUs) in underutilized spectrum to mitigate the spectrum scarcity problem. This paper focuses on the DSA architecture used in the 3.5 GHz band since it is one of the most prominent DSA system architectures. Besides IUs and SUs, this target architecture also includes a spectrum access coordination system (SAS) and an Environmental Sensing Capability (ESC) system [1]. ESC is a distributed network of sensing devices that monitor IU signal's received signal strength (RSS) and then provides such sensing information to SAS. Based on ESC inputs, SAS then grants spectrum access permissions to SUs accordingly. IUs in 3.5GHz are often military radars and satellite services, whose operation data is classified and demands strong privacy protection from the SAS-based DSA system.

In such a SAS-based DSA system, SUs can only be permitted to access the licensed bands when these SUs do not cause any harmful interference to the IUs based on ESC's IU sensing results and SUs' transmission parameters (e.g. SUs' transmission power and locations). Adaptive SU power control based on ESC's IU sensing results, hence, can be a viable way to ensure an SU can obtain such transmission permission to coexist with IUs. Multiple such SU power control schemes have been proposed recently. Unfortunately, none of these existing schemes can properly solve the SU power control problem in DSA. These existing SU power control algorithms can be classified into two categories: centralized and distributed power control [2]. Centralized power control algorithms, such as those proposed in [3], [4], lack scalability when the number of SUs in the system is large because the central controller has to coordinate all SUs and becomes the bottleneck. In addition, the central controller needs to know sensitive IU operation data, violating IU's privacy-protection demand. Distributed power control strategies, such as [5], [6], [2], solves the scalability issues, but is even worse in IU privacy protection since they have to distribute sensitive IU location and interference level information to all SUs.

Due to the limitations of existing schemes, in this paper, we propose a novel distributed and secure SU power control algorithm for SAS-based DSA systems. We theoretically prove the algorithm's convergence and also show that the maximum interference limit at IU and the minimum SINR requirement of SUs are both satisfied at the stable point. In addition, in our scheme, each SU self-adjusts its transmit power based on locally observable measurements and a few broadcasted global parameters from SAS. Hence, the system has excellent scalability since the central SAS does not need to perform per-SU computation. Furthermore, our proposed algorithm ensure that sensitive operation information of IU cannot be derived from the information exchanged in this system. The algorithm does not even require sharing of the raw IU signal strength sensed by ESC. Instead, ESC only gives SAS some masked values indirectly related to IU signal strength. Since only the masked values are shared among participating entities in our power control algorithm, even if the information is leaked, an adversary will not be able to infer sensitive information of the IU.

In the rest of the paper, we will discuss our algorithm design using the following organization. Section II discusses the related works on constrained SU power control and IU location protection. Section III introduces the system model and the QoS requirements for SU and IU. Section IV describes our power control algorithm for SUs to distributively adjust their transmit power. In Section V, we demonstrate the convergence and stability properties of our algorithm under different conditions. Section VI further shows how IU's interference requirement is statistically guaranteed. Section VII analyzes that even when the ESC-supplied information is leaked, it is still difficult for adversaries to infer the true IU location. In Section VIII, we present the evaluation of the proposed algorithm using simulations. Finally, Section IX concludes the paper.

II. Related Work

In recent years, plenty of research has been done on SU power control. Most of existing works can be classified into two categories: centralized and distributed power control [2]. In centralized power control strategies, there should be a central controller that manages the transmit power of all SUs within its coverage [7], [8]. Commonly, the basic idea adopted in centralized power control is that an SU is only allowed to transmit if it is authorized by the central controller. One obvious drawback of this type of strategy is the heavy communication cost since the central controller needs to know all the SU and IU information for decision making. Also, SU and IU privacy is a concern in centralized power control since the central controller will know sensitive location and operation state of IUs.

In distributed power control strategies, SUs adjust their transmit power based on locally observable measurements and received information. Some of these strategies, such as those in [9], [10],[2],[5], iteratively adapte SU transmit power based on some optimal formulation with target objective functions and constraints. The others, such as [11], use learning algorithm for SU power adaptation. Unfortunately, none of these distributed algorithms considers IU operation privacy protection. Many of them assumed that IUs' locations are known to all SUs and hence each SU can locally measure the channel gain between an IU and itself. Some even need to put a genie near an IU to obtain the interference level at the IU's location. Thus, these algorithms will not be compatible with the strict IU operation privacy protection requirement in 3.5GHz DSA systems.

In terms of privacy protection in DSA, there is a wealth of literature done to protect IU's location privacy. Works in [12], [13], [14], [15], [16], [17] assume that IUs participate in the spectrum allocation process, by adding noise or distortion on their location data or encrypting the data using homomorphic cryptosystems. Such a design is impractical in many DSA systems since it demands modification of IU designs. The work in [18] does not assume IUs' participation in spectrum allocation and leverages a proxy re-encryption scheme to encrypt the ESC's input to SAS. But this scheme requires a central trusted Key Issuer to distribute keys to SUs and ESCs. It is not clear how an IU can trust such a Key Issuer. In addition, the heavy encryption schemes used in [18] lead to high computation and communication overhead, where communication overhead and handling time per SU operation permission are in the magnitude of hundreds of MB and thousands of seconds, respectively. Such high overhead makes the scheme not scalable.

Different from these existing IU privacy protection schemes, our work does not demand IUs to participate in information exchange. Also, in our design, ESC does not provide any information directly related to an IU's location to SAS, so that no high-overhead encryption is needed to ensure IU privacy in the SU power allocation process. In Section VII, we formally demonstrate that under our design, it is difficult for an adversary (e.g., malicious SAS or SUs) to accurately infer the IU's location using ESC-provided information.

III. Problem Formulation

The system model in our algorithm is illustrated in Figure 1. Specifically, we assume that an IU, a SAS server, m ESC sensors, and n pairs of SU transmitters (SU-TX) and receivers (SU-RX) are distributed in an area. Both the IU and SU TXs/RXs can be mobile. All SU-TXs transmit on the same frequency band. We assume a SU-TX i ($i \in [1, n]$) only transmits towards a SU-RX i. If some transmitter transmits to multiple receivers, the transmitter can be modeled as multiple co-located SU-TXs, each transmitting to one receiver. Similarly, a receiver that receive messages from multiple transmitters can be simply modeled as multiple co-located SU-RXs, each receiving from one transmitter.

To formulate the power control problem, denote the transmit power of SU-TX i as P_i. The path attenuation from SU-TX i to SU-RX j is denoted by g_{ij}. φ denotes noise level at each SU-RX, including both the additive receiver noise and other environmental noise. The SINR at

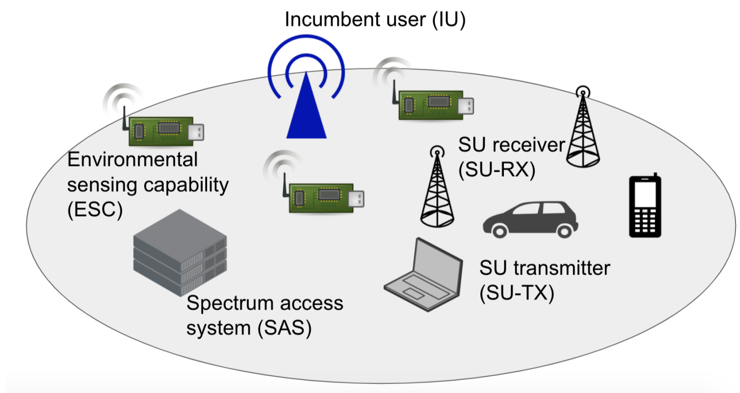

Fig. 1. System model.

SU-RX i, thus, can be expressed by $SINR_i = \frac{P_i g_{ii}}{\sum_{j \neq i} P_j g_{ji} + \varphi}$. The QoS requirements of IU and SUs that our power adaption algorithm needs to satisfy, thus, can be formulated as:

$$\begin{cases} \frac{g_{ii} P_i}{\sum_{j \neq i} g_{ji} P_j + \varphi} - \tau_i = 0, i \in [1, n] & (a) \\ Prob(\sum_i g_{iI} P_i \leq T) \geq \chi & (b) \\ 0 \leq P_i \leq P_{max}, i \in [1, n] & (c), \end{cases} \tag{1}$$

where τ_i denotes the desired SINR level at SU-RX i, which is needed to maintain effective communications as shown by constraint (a). g_{iI} represents the signal attenuation from SU-TX i to the IU. T is the IU's interference tolerance threshold. Constraint (b) essentially states that the probability that the aggregated SU interference on the IU is no larger than T must be no smaller than a threshold χ. P_i is upper bounded by P_{max}, the maximum SU-TXs' transmit power, as shown by constraint (c).

While the constraints in (1) are straightforward, they are hard to guarantee directly. Due to privacy protection of IU's location information, g_{iI} in (1) should not be revealed to any SU/SAS/ESC. Thus, direct estimate of interference suffered by IU is not feasible. In addition, in 3.5GHz band, an IU usually does not have realtime communications with any SU/ESC/SAS. Thus, it is also impossible for IU to inform SU/SAS about its local interference level.

To solve this problem, we translate the constraints on IU interference level to the constraints on ESC's interference level, which can be either directly measured by ESC or theoretically estimated since ESC's locations are public information according to FCC regulation in 3.5GHz[19]. Specifically, we propose that when an ESC e has sensed the existence of an IU, it uses its sensing data to derive its requirement on local maximum SU interference level, denoted as T_e.

T_e is computed in a way such that if the aggregated SU-TXs signals on each ESC does not exceed T_e, the interference received at the IU is likely constrained to be below T(See Section VI for details). Hence, the constraint formulation in (1) is converted into:

$$\begin{cases} \frac{g_{ii}P_i}{\sum_{j\neq i} g_{ji}P_j+\varphi} - \tau_i = 0, i \in [1,n] \quad (a) \\ \sum_i g_{ie}P_i \leq T_e, e \in [i,m] \quad (b) \\ 0 \leq P_i \leq P_{max}, i \in [1,n] \quad (c), \end{cases} \tag{2}$$

where g_{ie} is the signal attenuation from SU-TX i to ESC e.

Denote the set of SU power settings that satisfy (2) as the solution set $R := \{\mathbf{P}|\mathbf{P}$ satisfies (2)$\}$, where $\mathbf{P}$ is a column vector and $\mathbf{P} = \{P_i, i \in [1,n]\}$. In the following sections, we will prove that when the solution set R is not empty, our algorithm successfully stabilizes at a unique equilibrium point in R. When a solution to (2) does not exist (a.k.a. $R = \emptyset$), meaning that a power setting that satisfies all three constraints in (2) does not exist, our power control algorithm will converge to a stable point that guarantees IU's QoS requirement (2b), while the constraint (2a) may be violated. We believe this is a desirable feature of our algorithm because, in an DSA system, the guarantee of IU's QoS is generally a strict requirement, while degrading SU communication quality is often acceptable when the system becomes too crowded with SUs.

IV. Our Distributed Power Control Algorithm

In this section, we present our distributed dynamic power control algorithm. The algorithm includes three parts: the ESC update algorithm, the SAS update algorithm, and the SU-TX update algorithm.

<u>ESC update algorithm:</u> Each ESC e measures its local aggregated SU interference, denoted as C_e, and computes and periodically updates SAS with

$$\omega_e = \frac{\xi_1(C_e - \xi_2 T_e)}{C_e}, \tag{3}$$

Here, ξ_1 and ξ_2 are two random numbers in the range of $(0,1]$. ξ_1 and ξ_2 take different values for each ω_e computation to increase the randomness in ω_e and to ensure privacy-protection on IU, and the detailed analysis can be found in Section VII. T_e is the maximum allowable interference at ESC e. ESC e generates T_e based on its local RSS of IU and the IU's maximum acceptable interference level T posted by the IU. In Section VI, we will discuss the details of T_e generation.

The above ESC update algorithm assumes that ESC can differentiate IU signals from SU signals based on the differences in their signal characteristics (e.g. modulation schemes). There are many existing approaches for realizing such signal classification [20], [21], [22]. Most existing ESC design proposals already have this capability.

SAS update algorithm: SAS periodically broadcasts global parameters $\Omega_e, e \in [1, m]$ and Γ_{min} to all SU-TXs, which are computed based on ESC-supplied ω_e as follows:

$$\Omega_e = f'(\omega_e) \cdot \lambda_e^2, \tag{4}$$

$$\Gamma_{min} = \min(-\omega_e), \tag{5}$$

$$\text{where } f(z) := \max(0, z). \tag{6}$$

Each λ_e for $e \in [1, m]$ is a non-zero positive time dependent variable that is updated by the following differential equation:

$$\dot{\lambda}_e = \frac{d\lambda_e}{dt} = -\beta_e f(\omega_e) \cdot 2\lambda_e. \tag{7}$$

where β_e is a positive number. β_e is designed to always guarantee $\lambda_e > 0$ when it is updated by ensuring:

$$\lambda_e + \dot{\lambda}_e = \lambda_e - \beta_e f(\omega_e) \cdot 2\lambda_e > 0 \Rightarrow 0 < \beta_e < \frac{1}{2f(\omega_e)} \tag{8}$$

Note that the initial $\lambda_e(0)$ must be positive, and it is easy to achieve because $\lambda_e(0)$ can be determined by SAS itself.

SU-TX update algorithm: SU-TX i adapts its transmit power by:

$$\dot{P}_i = \frac{dP_i}{dt} = \tilde{\dot{P}}_i + \sum_e g_{ie}\Omega_e \tilde{\dot{P}}_i, \tag{9}$$

$$\text{where } \tilde{\dot{P}}_i = \alpha_i \cdot \left(\frac{\tau_i}{SINR_i} - 1\right) P_i, \tag{10}$$

$$\alpha_i = \alpha_i(\Gamma_{min}, g_{ie}, \Omega_e, SINR_i) \tag{11}$$

In the above adaption algorithm, SU-TX i can obtain $SINR_i$ from its receiver SU-RX i's feedback. SU-TX can compute g_{ie} for each ESC sensor e using radio propagation model based on the sensor's location, which is public information. α_i is a locally computed step size based on a step size control function described in Section V-B2. α_i depends on both locally observable g_{ie} and $SINR_i$, and global scalar parameters Ω_e and Γ_{min} from SAS broadcasts.

Our algorithm is very simple to implement. Only locally observable information and some insensitive aggregated information broadcasted by SAS are required for each SU-TX to update its transmit power distributively. The broadcasted information from SAS reveals no IU location or IU interference levels. The information transmitted from ESC to SAS also cannot be used to derive IU location or interference level. The computation in SAS side is not difficult and require no privacy sensitive IU information. Since our algorithm does not require one-to-one information exchange between SU-TXs and SAS, it is highly scalable. In the next section, we prove that our system will asymptotically converge into a unique equilibrium point in R whenever R is nonempty. Then, we demonstrate how the system stabilizes when R is empty.

V. Convergence and Stability

To prove our algorithm's convergence, first note that theoretically, the aggregated SU interference at ESC e can be expressed as $C_e = \sum_i P_i g_{ie}$. In addition, according to (3) and (6), because C_e and ξ_1 are positive, we can see that the value of $f'(\omega_e)$ is identical to $f'(\omega_e C_e/\xi_1)$. Thus $f'(\sum_i P_i g_{ie} - \xi_2 T_e) = f'(\omega_e)$. Combining this with (3) (4) (7) (9) (10), the transmit power update algorithm at SU-TX i can be expressed as:

$$\dot{P}_i = \frac{dP_i}{dt} = \widetilde{\dot{P}}_i + \left[\sum_e f'(\sum_i P_i g_{ie} - \xi_2 T_e) g_{ie} \lambda_e^2\right] \widetilde{\dot{P}}_i, \tag{12}$$

$$\text{where } \widetilde{\dot{P}}_i = \alpha_i \left(\frac{\tau_i}{\frac{P_i g_{ii}}{\sum_{j \neq i} P_j g_{ji} + \varphi}} - 1 \right) P_i, \tag{13}$$

$$\dot{\lambda}_e = \frac{d\lambda_e}{dt} = -\beta_e f(\xi_1 \frac{\sum_i P_i g_{ie} - \xi_2 T_e}{\sum_i P_i g_{ie}}) \cdot 2\lambda_e. \tag{14}$$

Essentially, in this section, we will examine the system's convergence to a SU transmit power allocation set $\widetilde{R}$ that is defined as $\widetilde{R} := \{\mathbf{P} | \mathbf{P}$ satisfies all the constraints in (15)$\}$:

$$\begin{cases} \frac{g_{ii} P_i}{\sum_{j \neq i} g_{ji} P_j + \varphi} - \tau_i = 0, i \in [1, n] \ (a) \\ \sum_i g_{ie} P_i \leq \xi_2 T_e, e \in [i, m] \ (b) \\ 0 \leq P_i \leq P_{max}, i \in [1, n] \ (c) \end{cases} \tag{15}$$

Since $\widetilde{R} \subset R$, once the system converges into $\widetilde{R}$, it converges into R. We will prove that whenever there exists an nonempty power allocation solution set $\widetilde{R}$, our algorithm will stabilize at a unique solution inside $\widetilde{R}$ and hence is guaranteed to meet both IU and SUs' requirements. Even when an solution does not exist (i.e. $\widetilde{R} = \emptyset$), the system asymptotically converges to a unique stable point which always satisfies the ESC's interference constraint (15b).

Our proof includes two parts. In part 1, we prove the system's convergence under the case where $\widetilde{R}$ is nonempty. In Part 2, the case where $\widetilde{R}$ is empty is considered. In this case, SUs'

SINR requirements, SU's upper transmit power limit and IU's interference requirement cannot be satisfied simultaneously. The system in (12) - (14) will never converge to a point that satisfies all the constraints in Equation (2) since equilibrium points do not exist. Therefore, we propose a supplementary approach for this case which treats IU's interference constraint with higher priority than SU's SINR requirement. We prove the supplementary approach's convergence.

A. Part 1: Solution set $\widetilde{R}$ to (15) exists

In this subsection, we prove that whenever $\widetilde{R} \neq \emptyset$, meaning that there exists some feasible setting of SU-TX transmit power that satisfies (15), our algorithm stabilizes at a unique point inside $\widetilde{R}$. The proof is divided into two phases.

1) Phase 1: We relax the maximum power constraint in (15) to get a new relaxed solution set $\widetilde{Z}$, such that all $\mathbf{P} \in \widetilde{Z}$ satisfies:

$$\begin{cases} \frac{g_{ii}P_i}{\sum_{j\neq i} g_{ji}P_j+\varphi} - \tau_i = 0, i \in [1,n] \ (a) \\ \sum_i g_{ie}P_i \leq \xi_2 T_e, e \in [i,m] \ (b) \\ P_i \geq 0, i \in [1,n]. \ (c) \end{cases} \tag{16}$$

   Then, we analyze the algorithm's convergence and stability properties whenever $\widetilde{Z}$ exists.

2) Phase 2: We demonstrate that our algorithm will iteratively converge to $\widetilde{R}$ if $\widetilde{R}$ is a nonempty set.

1) Phase 1: convergence to a relaxed solution set $\widetilde{Z}$: In this phase, we analyze the algorithm's convergence to a unique equilibrium in $\widetilde{Z}$ under the condition that $\widetilde{Z}$ is nonempty. The analysis is summarized in two theorems. Theorem V.1 demonstrates that our algorithm asymptotically converges to an invariant set $\widetilde{Z}$. Theorem V.4 states that our algorithm will stabilize at a unique equilibrium point in $\widetilde{Z}$.

Theorem V.1. *Starting from any initial state $P_i(0) > 0$, the system described in (12) to (14) asymptotically converges to an invariant set $\widetilde{Z}$.*

Proof. The proof includes two steps. At Step 1, we prove that every point in $\widetilde{Z}$ is a saddle point. At step 2, by constructing a Lyapunov function, we prove that the system is asymptotically stable inside $\widetilde{Z}$ if it is an nonempty set.

Step 1: Denote $\boldsymbol{P}^* = \{P_i^*, i \in [1,n]\}$ as a saddle point of the system. Setting $\dot{\widetilde{P}}_i = 0$ and $\dot{\lambda}_e = 0, e \in [i,m]$, $\boldsymbol{P}^*$ is defined by:

$$\begin{cases} \dot{\widetilde{P}}_i = \alpha_i \left(\dfrac{\tau_i}{\frac{P_i^* g_{ii}}{\sum_{j\neq i} P_j^* g_{ji} + \varphi}} - 1 \right) P_i^* = 0 & \text{(17a)} \\ \dot{\lambda}_e = -\beta_e f(\xi_1 \dfrac{\sum_i P_i^* g_{ie} - \xi_2 T_e}{\sum_i P_i^* g_{ie}}) \cdot 2\lambda_e = 0 & \text{(17b)} \end{cases}$$

Since $\lambda_e > 0$, from (17b), it is clear that $f(\sum_i P_i^* g_{ie} - \xi_2 T_e) = 0$, which, based on $f(\cdot)$ definition in (6), means $\sum_i P_i^* g_{ie} - \xi_2 T_e \leq 0$. Based on (13), the solution set for $\dot{\widetilde{P}}_i = 0$ is $S = \{S_i := P_i^* - \frac{\tau_i}{g_{ii}}(\sum_{j\neq i} g_{ji} P_j^* + \varphi) = 0, i \in [1,n]\}$. Thus, (17a) and (17b) can be converted to:

$$\begin{cases} \frac{\tau_i}{\frac{g_{ii} P_i^*}{\sum_{j\neq i} g_{ji} P_j^* + \varphi}} = 1, \forall i \in [1,n] \\ \sum_i P_i^* g_{ie} \leq \xi_2 T_e, \forall e \in [1,m] \end{cases} \tag{18}$$

Clearly, (18) is equivalent to the definition of $\widetilde{Z}$. Hence, $\widetilde{Z}$ is the saddle points $\boldsymbol{P}^*$ for the system.

Step 2: In this step, we prove that $\boldsymbol{P}^* \in \widetilde{Z}$ is an equilibrium point of the system. We first show the convergence property of $\dot{\widetilde{P}}_i$ alone. From (13), $\dot{\widetilde{P}}_i$ can be rewritten as:

$$\dot{\widetilde{P}}_i = \alpha \left(\frac{\tau_i}{g_{ii}} \sum_{j\neq i} g_{ji} P_j - P_i \right) + \alpha \frac{\tau_i}{g_{ii}} \varphi = \boldsymbol{A}\boldsymbol{P} + \boldsymbol{b}, \tag{19}$$

where $\boldsymbol{A} = \{a_{ij}\}_{n\times n}$ is a $n \times n$ matrix with strictly negative entries along the diagonal and only positive entries off the diagonal. $a_{ii} = -\alpha$, and $a_{ij} = \alpha \frac{\tau_i}{g_{ii}} g_{ji}$ for $i \neq j$. $\boldsymbol{b} = \{b_i\}_n$ is a vector of n entries, and $b_i = \alpha \frac{\tau_i}{g_{ii}} \varphi$.

To further our proof of $\dot{\widetilde{P}}_i$'s convergence, we introduce Lemma V.2 and V.3 from existing literature [9], [23], [24].

Lemma V.2. *: If an $n \times n$ matrix has non-negative entries off the diagonal, and if it maps an $n \times 1$ vector, all of whose entries are positive, into an $n \times 1$ vector, all of whose entries are negative, each of the n eigenvalues of the matrix has negative real parts [23].*

Lemma V.3. *Given the dynamic system $\dot{\boldsymbol{x}} = \boldsymbol{A}\boldsymbol{x}$, for any $\boldsymbol{Q} = \boldsymbol{Q}^\top > 0$, there exists a positive definite solution $\boldsymbol{M}$ of the Lyapunov $\boldsymbol{A}^\top \boldsymbol{M} + \boldsymbol{M}\boldsymbol{A} = -\boldsymbol{Q}$. The solution $\boldsymbol{M}$ is unique if and only if every eigenvalues of $\boldsymbol{A}$ has negative real parts [24].*

Note that in phase 1 we assume $\widetilde{Z}$ is not empty. There exists $\boldsymbol{P}^* \in \widetilde{Z}$ that makes $\dot{\widetilde{P}}_i = 0$. Thus, according to (19), $\boldsymbol{A}\boldsymbol{P}^* = -\boldsymbol{b}$. According to Lemma V.2, all the eigenvalues of $\boldsymbol{A}$ have negative real parts. Thus, we can apply Lemma V.3 and find a positive definite matrix $\boldsymbol{M}$ that solves $\boldsymbol{A}^\top \boldsymbol{M} + \boldsymbol{M}\boldsymbol{A} = -\boldsymbol{Q}$ given any $\boldsymbol{Q} = \boldsymbol{Q}^\top > 0$. Hence, we can construct a Lyapunov function $V(\boldsymbol{P})$ for $\dot{\widetilde{P}}_i$ as

$$V(\boldsymbol{P}) := (\boldsymbol{P} - \boldsymbol{P}^*)^\top \boldsymbol{M}(\boldsymbol{P} - \boldsymbol{P}^*) \geq 0 \tag{20}$$

The time derivative of $V(\boldsymbol{P})$ is calculated by

$$\dot{V}(\boldsymbol{P}) = \sum_i \frac{\partial V(\boldsymbol{P})}{\partial P_i} \dot{\widetilde{P}}_i = -(\boldsymbol{P} - \boldsymbol{P}^*)^\top \boldsymbol{Q}(\boldsymbol{P} - \boldsymbol{P}^*) \leq 0 \tag{21}$$

Clearly, $\dot{\widetilde{P}}_i$ asymptotically converges to $\boldsymbol{P}_i^*$ whenever $S = \{S_i := P_i - \frac{\tau_i}{g_{ii}}(\sum_{j\neq i} g_{ji}P_j + \varphi) = 0, i \in [1,n]\}$ exists. Based on eigenvalue decomposition theorem, let us pick $\boldsymbol{Q} = \boldsymbol{H}^\top \boldsymbol{D}\boldsymbol{H}$, where $\boldsymbol{D}$ is an $n \times n$ eigenvalue matrix and each of its eigenvalue i is denoted by $\delta_i, i \in [1,n]$. Define $\boldsymbol{y} := \{y_1, y_2, ...y_n\} = \boldsymbol{H}(\boldsymbol{P} - \boldsymbol{P}^*)$. Hence, $\dot{V}(\boldsymbol{P})$ can be re-expressed as:

$$\dot{V}(\boldsymbol{P}) = \sum_i \frac{\partial V(\boldsymbol{P})}{\partial P_i} \dot{\widetilde{P}}_i = \sum_i \delta_i {y_i}^2 \tag{22}$$

Given the convergence properties of $\dot{\widetilde{P}}_i$, now we will prove the convergence and stability of the system with both $\dot{P}_i, \forall i \in [1,n]$ and $\dot{\lambda}_e, \forall e \in [1,m]$ by constructing a Lyapunov function $K(\boldsymbol{\lambda}, \boldsymbol{P})$ for the system as

$$K(\boldsymbol{\lambda}, \boldsymbol{P}) := F(\boldsymbol{\lambda}, \boldsymbol{P}) - F(\boldsymbol{\lambda}^*, \boldsymbol{P}^*), \tag{23}$$

$$\text{where } F(\boldsymbol{\lambda}, \boldsymbol{P}) := \sum_e f\Big(W(\boldsymbol{P}) \sum_i g_{ie} - \xi_2 T_e\Big){\lambda_e}^2, \tag{24}$$

$$W(\boldsymbol{P}) := V(\boldsymbol{P}) + \epsilon. \tag{25}$$

In the construction, $\boldsymbol{\lambda}^*, \boldsymbol{P}^*$ are the equilibrium points of the system. ϵ is a sufficiently large positive number such that $\epsilon > \frac{T_e}{\sum_i g_{ie}}$ and ϵ makes the following inequality always true:

$$W(\boldsymbol{P}) \sum_i g_{ie} - \xi_2 T_e = (V(\boldsymbol{P}) + \epsilon) \sum_i g_{ie} - \xi_2 T_e > 0. \tag{26}$$

Note this is possible because $V(\boldsymbol{P})$ is a definite positive function. Theorem A.1 in the Appendix shows that $K(\boldsymbol{\lambda}, \boldsymbol{P})$ is the Lyapunov function for the system and $\dot{K} = 0$ if and only if

$$\begin{cases} P_i = P_i^* = \frac{\tau_i}{g_{ii}} \left(\sum_{j\neq i} g_{ji}{P_j}^* + \varphi\right), \forall i \in [1,n] \\ \sum_i P_i g_{ie} - \xi_2 T_e \leq 0, \forall e \in [i,m]. \end{cases} \tag{27}$$

The above equation is equivalent to the definition of $\widetilde{Z}$. Hence, we prove that the system asymptotically converges into $\widetilde{Z}$. □

Theorem V.4. *$\widetilde{Z}$ only contains one equilibrium.*

Proof. Considering a large number of SUs moving inside a large geographical area, the $n \times n$ matrix $\boldsymbol{A}$ and $n \times 1$ matrix $\boldsymbol{b}$ defined in (19) can be assumed to be sufficiently random according to [9]. Hence matrix $\boldsymbol{A}$ and $\boldsymbol{b}$ can be assumed to have n distinct eigenvalues with probability one. Therefore, when $\widetilde{Z}$ is nonempty, there is only one unique point in $\widetilde{Z}$, which the system converges to. □

With Theorem V.1 and Theorem V.4, we now can conclude that the system asymptotically converges to a unique equilibrium in $\widetilde{Z}$ when $\widetilde{Z} \neq \emptyset$.

2) Phase 2: convergence to solution set $\widetilde{R}$: Since $\widetilde{Z}$ is the solution set for relaxing the SU-TX transmit power upper limit and $\widetilde{R}$ is the solution set where $P_i \leq P_{max}$ is enforced, we have $\widetilde{R} \subseteq \widetilde{Z}$. Since a non-empty $\widetilde{Z}$ only contains a single unique equilibrium point $\boldsymbol{P}^*$, if $\widetilde{R}$ is also not empty, we must have $\boldsymbol{P}^* \in \widetilde{R} = \widetilde{Z}$ and $P_i^* \leq P_{max}, i \in [1, n]$. Since we have proved that the system converges to the unique equilibrium $\boldsymbol{P}^* \in \widetilde{Z}$, we can state that as long as $\widetilde{R} \neq \emptyset$, starting from any initial state $\boldsymbol{P}(\boldsymbol{0}) > 0$, our algorithm iteratively converges to $\boldsymbol{P}^* \in \widetilde{R}$.

B. Part 2: Solution set $\widetilde{R}$ to (15) is empty

So far we have proved that, whenever $\widetilde{R}$ is nonempty, our algorithm asymptotically converges to a unique stable point $\boldsymbol{P}^* \in \widetilde{R}$. However, solution set $\widetilde{R}$ may not exist for some SUs and IU distribution. This may happen in two cases:

1) Case 1: This is the case where $\boldsymbol{P}^* \in \widetilde{Z}$ exists but $P_i^* > P_{max}$ for some i. In such a case, $\widetilde{R}$ is an empty set due to constraint on SU maximum transmit power. We show a stopping criterion of the algorithm in (12) - (14) to handle this case.
2) Case 2: This is the case $\widetilde{Z} = \emptyset$. This means SUs' SINR requirement and IU's interference requirement cannot be guaranteed at the same time. To handle this situation, a step size control method is proposed to always guarantee IU's interference requirement while sacrificing the SINR of SUs. Essentially, the algorithm treats IU's interference constraint with a higher priority than SU SINR.

Next, we introduce the details of our solution for these two cases.

1) Case 1: Stopping Criterion: In this case, even when the transmit power P_i of SU-TX i already reaches P_{max}, a solution still cannot be reached. In other words, the solution $\boldsymbol{P}^* \in \widetilde{Z}$ exists in the range $P_i > P_{max}$. In this case, SU-TX i will simply stop increasing its P_i and keep $P_i = P_{max}$ unless the algorithm guides it to decrease the transmit power, while other SU-TXs keep on updating their transmit power until the convergence of the system. By this procedure, the system can stabilize at a sub-optimal point where $\sum_{i\in[1,n]} P_i^* g_{ie} < T_e, e \in [1, m]$ and $0 \leq P_i^* \leq P_{max}, i \in [1, n]$ hold. However, this sub-optimal solution may fail to meet the SINR requirement.

2) Case 2: Step Size Control: When $\widetilde{Z} = \emptyset$, meaning that it is impossible to guarantee SUs' SINR requirement and IU's interference requirement at the same time, we choose to ensure IU' interference requirement first and sacrifice the SINR of SUs. This is because in DSA, FCC regulation demands that IU's performance has to be guaranteed. We realize this preferential treatment on IU by requiring our algorithm to stabilize at a point $\boldsymbol{P}^*$ meeting $\sum_i P_i^* g_{ie} < T_e, e \in [1, m]$.

This can be achieved by a step size control procedure that computes the feasible step size α_i in (9). The procedure need to ensure that the ESC's interference at any iteration to be smaller than its threshold T_e by enforcing :

$$\sum_{i\in[1,n]} (P_i + \dot{P}_i) g_{ie} < T_e, e \in [1, m] \tag{28}$$

In this way the requirement $\sum_i P_i^* g_{ie} < T_e$ can be guaranteed. Since C_e denotes the received interference at ESC e from all SU-TXs, given (3) - (9), (28) can be rewritten as:

$$C_e + \sum_i \alpha_i (\frac{\tau_i}{SINR_i} - 1)(1 + \sum_e \Omega_e g_{ie}) P_i g_{ie} < T_e \tag{29}$$

To guarantee (29), we set α_i to make the following inequality hold $\forall i \in [1, n]$:

$$\alpha_i (\frac{\tau_i}{SINR_i} - 1)(1 + \sum_e \Omega_e g_{ie}) < \Gamma_{min}, \tag{30}$$

which essentially means that SU-TX picks the stepsize α_i following:

1) If $\frac{\tau_i}{SINR_i} - 1 > 0$, $\alpha_i < \Gamma_{min} \frac{1}{(\frac{\tau_i}{SINR_i} - 1)(1 + \sum_e \Omega_e g_{ie})}$.
2) If $\frac{\tau_i}{SINR_i} - 1 < 0$, $\alpha_i > \Gamma_{min} \frac{1}{(\frac{\tau_i}{SINR_i} - 1)(1 + \sum_e \Omega_e g_{ie})}$.

By choosing α_i following the above rules, starting from any initial point $\boldsymbol{P}(0)$, the requirement $\sum_i P_i g_{ie} < T_e, e \in [1, m]$ is always guaranteed even when $\widetilde{Z} = \emptyset$.

Based on the discussion above, we have proved that the system will converge to a stable point which always meets ESC interference requirements, if the step size α_i for SU-TX i is tuned in each iteration by the proposed step size control method.

VI. ESC INTERFERENCE REQUIREMENTS

As discussed in Section III, due to the sensitivity in IU's location privacy, the interference from SU-TXs to an IU cannot be directly measured and thus the problem formulation in (1) cannot be solved directly. Therefore, we estimate the interference from SU-TX to ESC instead and create problem formulation (2). In Section V, we have proved that our algorithm asymptotically stabilize at an equilibrium that solves the problem in (2). In this section, we describes how our algorithm computes ESC's interference constraint T_e and verify that using this T_e computation, the solution to the problem in (2) is approximately also a solution to the problem in (1).

On a high level, denoting $\mathbf{T_E}$ as the set of all T_e, $\mathbf{T_E}$ is computed by solving the following formula:

$$U(\mathbf{T_E}) := Pr(I \leq T | C_e \leq T_e, \text{for all } e \in [1, m]) \geq \Psi \tag{31}$$

where the constant threshold $\Psi \in [0, 1]$ and $\Psi \approx 1$. The left side of (31), denoted as $U(\mathbf{T_E})$, represents the conditional probability that the IU's received SU interference I does not exceed its requirement T given that the SU interference level at each ESC e is bounded by $\mathbf{T_E}$. The formula essentially means that $\mathbf{T_E}$ should be set at a right value so that the probability on the left side will be close to 1.

Next, we explicitly derive the expression of $U(\mathbf{T_E})$. To achieve this, we first derive the statistical distribution of C_e in Section VI-A. In Section VI-B, we model the conditional statistical distribution of I, given ESC's local RSS of IU. Next, Section VI-C solves (31) as a cumulative density function of a conditional normal distribution, and use this function to identify T_E that guarantees $U(\mathbf{T_E}) \geq \Psi$.

A. Distribution of C_e

To derive the statistical distribution of $C_e = \sum_{i \in [1,n]} P_i g_{ie}$ for ESC sensor e, the path loss g_{ie} between SU-TX i and ESC e needs to be estimated. Since an SU-TX's location is usually not known to an ESC due to SU location privacy protection, we can not measure or compute g_{ie} directly. Thus, we establish a statistical model of g_{ie} between SU-TX and ESC.

Without loss of generality, we assume that each ESC is in charge of detecting the IU's presence in a large circular area centered at itself with a radius l, and SUs are uniformly distributed inside this area. Based on the simplified propagation model, $g_{ie} = \eta {d_{ie}}^{-\upsilon}$, where d_{ie} is the distance between ith SU-TX and eth ESC, υ is the path loss exponent and η is a small constant coefficient. Note that the probability density function (PDF) of d_{ie}, denoted as $\rho_{D_e}(d_{ie})$, can be expressed as $\rho_{D_e}(d_{ie}) = \frac{2d_{ie}}{l^2}$. Using $\rho_{D_e}(d_{ie})$, the distribution of channel gain g_{ie} is derived by:

$$Prob(g_{ie} \leq g) = 1 - Pr(d_{ie} \leq (\frac{g}{\eta})^{-\frac{1}{\upsilon}}) \tag{32}$$

$$\rho_{G_e}(g) = \frac{\partial Prob(g_{ie} \leq g)}{\partial g} = \frac{\eta^{\frac{1}{\upsilon}}}{\upsilon} g^{-\frac{1+\upsilon}{\upsilon}} \rho_{D_e}((\frac{g}{\eta})^{-\frac{1}{\upsilon}}) \tag{33}$$

The expectation and variance of g_{ie}, denoted as μ_e and σ_e^2 respectively, can be calculated based on:

$$\mu_e = \int_{\eta l^{-\upsilon}}^{\eta \epsilon_1^{-\upsilon}} \frac{2\eta^{\frac{2}{\upsilon}} g^{-\frac{2}{\upsilon}}}{\upsilon l^2} \mathrm{d}g, \quad \sigma_e^2 = \int_{\eta l^{-\upsilon}}^{\eta \epsilon_1^{-\upsilon}} (g - \mu_e)^2 \frac{2\eta^{\frac{2}{\upsilon}} g^{-\frac{2+\upsilon}{\upsilon}}}{\upsilon l^2} \mathrm{d}g \tag{34}$$

where ϵ_1 is the minimum distance between an SU and ESC.

Since all SU-TXs are independent, $g_{ie}, \forall i \in [1, n]$ is i.i.d. Using the Central Limit Theorem and the Law of Large Numbers, when n increases, $C_e = \sum_{i=1}^{n} P_i g_{ie}$ can be approximated by a normal distribution, $C_e \sim N(\hat{\mu}_e, \hat{\sigma}_e^2)$, where

$$\hat{\mu}_e = \sum_{i=1}^{n} P_i \mu_e, \quad \hat{\sigma}_e^2 = \sum_{i=1}^{n} (P_i)^2 \sigma_e^2. \tag{35}$$

B. Distribution of I

In this section, we model the statistical distribution of an IU's received SU interference I. Denoting g_{iI} as the path loss from the ith SU to the IU, we have $I = \sum_{i \in [1,n]} P_i g_{iI}$. Same as how we compute C_e's distribution by modeling g_{ie} in the previous section, to model I, we again need to derive g_{iI}'s statistical distribution. Since the IU's location is not explicitly known due to IU location privacy protection, g_{iI} has to be estimated using ESC's local measurement of IU signals. Note that due to FCC's security regulation, ESCs must not share any IU's location-related information. Thus, each ESC must independently calculate g_{iI}. No exchange of these IU-related information with other ESC is allowed.

The first step is to roughly estimate the IU's location distribution using ESC's local measurement. Note that the distance between an ESC and the IU, denoted as d_0, is given by $d_0 = (\frac{g_0}{\eta})^{-\frac{1}{\upsilon}}$, where g_0 denotes the channel gain from the ESC to the IU. In addition, we have $g_0 = P_r/P_t$, where P_t is the IU's transmit power and P_r is the ESC's received IU signal strength. Since it is easy to find the common transmit power of radar systems, which are the main types of IUs in the 3.5GHz band, we assume P_t is known. Assuming IU's signal is transmitted through a Rayleigh fading channel, the cumulative distribution function (CDF) of P_r, thus, can also be modeled as $\Xi_{PR}(P_r) = 1 - \exp(-\frac{P_r}{r_e})$, where r_e is the expectation of P_r, which can be measured by ESC sensor e. Therefore, the CDF of g_0 can be derived by:

$$\Xi_{G_0}(g_0) = 1 - \exp(-\frac{g_0 P_t}{r_e}). \tag{36}$$

The CDF of d_0 is then computed by:

$$\Xi_{D_0}(d_0) = \exp(-\frac{\eta d_0^{-\upsilon} P_t}{r_e}), \tag{37}$$

and the probability distribution function (PDF) of d_0 is:

$$\rho_{D_0}(d_0) = \exp(-\frac{P_t \eta d_0^{-\upsilon}}{r_e})\frac{\upsilon P_t \eta}{r_e} d_0^{-\upsilon-1}. \tag{38}$$

The above CDF and PDF of d_0 are essentially a location distribution of the IU expressed in the form of a uniform distribution over a circle of a radius d_0 and a center at an ESC. Using this IU location distribution, we can derive the distance between ith SU and the IU, denote as d_{iI}, as follows. Note that the PDF of d_{iI} conditioned on d_0, denoted as $\rho_{D_I|D_0}(d_{iI}|d_0)$, is:

$$\rho_{D_I|D_0}(d_{iI}|d_0) = \begin{cases} \frac{2d_{iI}}{l^2}, & 0 \le d_{iI} \le l - d_0 \\ \frac{2d_{iI}}{\pi l^2} \arccos(\frac{d_0^2 + d_{iI}^2 - l^2}{2d_0 d_{iI}}), & l - d_0 < d_{iI} \le l + d_0. \end{cases} \tag{39}$$

Thus, combining (39) with (38), $\rho_{D_I}(d_{iI})$ can be computed by:

$$\rho_{D_I}(d_{iI}) = \begin{cases} \int_0^{l-d_{iI}} \frac{2d_{iI}}{l^2} \exp(-\frac{P_t \eta d_0^{-\upsilon}}{r_e}) \cdot \quad \frac{\upsilon P_t \eta}{r_e} d_0^{-\upsilon-1} \mathrm{d}d_0, \\ \qquad\qquad\qquad\qquad\qquad\qquad 0 \le d_{iI} \le l \\ \int_{d_{iI}-l}^{l} \frac{2d_{iI}}{\pi l^2} \arccos(\frac{d_0^2 + d_{iI}^2 - l^2}{2d_0 d_{iI}}) \cdot \quad \exp(-\frac{P_t \eta d_0^{-\upsilon}}{r_e}) \\ \frac{\upsilon P_t \eta}{r_e} d_0^{-\upsilon-1} \mathrm{d}d_0, \qquad\qquad l < d_{iI} \le 2l \end{cases} \tag{40}$$

The relation between d_{iI} and g_{iI} is the same as the relation between d_{ie} and g_{ie} in (33), the expectation μ_I and variance σ_I^2 of g_{iI} can be computed by:

$$\mu_I = \int_g \int_{d_0} \frac{\eta^{\frac{1}{\upsilon}}}{\upsilon} g^{-\frac{1}{\upsilon}} \rho_{D_I}((\frac{g}{\eta})^{-\frac{1}{\upsilon}}) \mathrm{d}d_0 \mathrm{d}g \tag{41}$$

$$\sigma_I^2 = \int_g \int_{d_0} \frac{(g - \mu_I)^2 \eta^{\frac{1}{\upsilon}}}{\upsilon} g^{-\frac{1+\upsilon}{\upsilon}} \rho_{D_I}((\frac{g}{\eta})^{-\frac{1}{\upsilon}}) \mathrm{d}d_0 \mathrm{d}g, \tag{42}$$

Because all SU-TXs are independent, the distribution for g_{iI} is also i.i.d $\forall i \in [1,n]$. Using the Central Limit Theorem and Law of Large Numbers, as n increases, $I = \sum_{i=1}^{n} P_i g_{iI}$ can be approximated by a normal distribution, $I \sim N(\hat{\mu}_I, \hat{\sigma}_I^2)$, where

$$\hat{\mu}_I = \sum_{i=1}^{n} P_i \mu_I, \quad \hat{\sigma}_I^2 = \sum_{i=1}^{n} (P_i)^2 \sigma_I^2. \tag{43}$$

C. Determine ESCs' interference constraints

As discussed in Section VI-A and VI-B,C_e and I are both approximated by normal distributions. The remaining problem is how each ESC e computes a proper value of T_e to satisfy $U(\mathbf{T_E}) \geq \Psi$ in (31), which can be rewritten to:

$$U(\mathbf{T_E}) = Pr\Big(\sum_{i\in[1,n]} P_i g_{iI} \leq T\Big| \sum_{i\in[1,n]} P_i g_{ie} \leq T_e, \text{for all } e \in [1,m]\Big) \geq \Psi. \tag{44}$$

Note that since g_{iI} and g_{ie} are all positive, we have:

$$\begin{aligned} &Pr\left(\sum_{i\in[1,n]} P_i g_{iI} \leq T \,\middle|\, \sum_{i\in[1,n]} P_i g_{ie} \leq T_e, \text{for all } e\right) \\ \geq\ &Pr\left(\sum_{i\in[1,n]} P_i g_{iI} \leq T \,\middle|\, \sum_{i\in[1,n]} P_i g_{ie} \leq T_e, \text{for some } e\right) \\ \geq\ &Pr\left(\sum_{i\in[1,n]} P_i g_{iI} \leq T \,\middle|\, \sum_{i\in[1,n]} P_i g_{ie} = T_e, \text{for some } e\right) \end{aligned}$$

Thus, as long as each ESC sensor e locally chooses a T_e that guarantees the following inequality:

$$Pr\left(I \leq T \,|C_e = T_e\right) \geq \Psi, \tag{45}$$

we know (44) must hold, which means IU's interference requirement is statistically satisfied.

According to the theory of conditional normal distribution[25], the conditional random variable $I|C_e = T_e$ is normally distributed, whose $\hat{\mu}_{Ie}$ and variance $\hat{\sigma}_{Ie}$ are:

$$\hat{\mu}_{Ie} = \hat{\mu}_I + \frac{\Sigma_{12}}{\Sigma_{22}}(T_e - \hat{\mu}_e), \tag{46}$$

$$\hat{\sigma}_{Ie} = \Sigma_{11} - \frac{\Sigma_{12}^2}{\Sigma_{22}}, \tag{47}$$

$$\text{where } \Sigma_{11} = cov(I, I), \Sigma_{12} = cov(I, C_e), \tag{48}$$

$$\Sigma_{22} = cov(C_e, C_e), \tag{49}$$

Here, function $cov(\cdot)$ is the covariance of the two input distributions. With the distribution of $I|C_e = T_e$ known, given a Ψ, the $\hat{\mu}_{Ie}$ value that makes $Pr\left(I \leq T \,|C_e = T_e,\right) \geq \Psi$, denoted as μ_0, can be computed as

$$\mu_0 = T - \hat{\sigma}_{Ie}\Phi^{-1}(\Psi), \tag{50}$$

where $\Phi^{-1}(\cdot)$ is the quantile function of standard normal distribution. Then, based on (46), T_e can be computed by

$$T_e = (\mu_0 - \hat{\mu}_I)\frac{\Sigma_{22}}{\Sigma_{12}} + \hat{\mu}_e. \tag{51}$$

(51) is the formula that each ESC e uses to generate T_e independently as its interference requirement. Bring this T_e into (3), the IU's interference requirement is statistically guaranteed.

VII. Analysis on IU location protection

In this section, we demonstrate how the IU's location privacy is protected in our algorithm. As seen from our algorithm, since ESC is responsible for detecting an IU's existence in the spectrum and measuring the average received IU signal strength, ESC is the only entity that obtains information directly related to the IU's location. In our attack model, we assume ESCs are trustworthy so an adversary cannot know its raw measurement of IU RSS. But the adversary may see all the information exchanged in the DSA system by compromising SAS, SUs or the communication channel. The attacker will attempt to derive sensitive IU location data from information that they observed.

According to (3) - (11) and Section VI, each ESC e uses the average detected IU signal strength r_e to generate its interference requirement T_e, and computes ω_e which is then sent to SAS and SUs. From the adversary's perspective, since ω_e's computation is based on T_e, which is again related to the distance between IU and ESC e, ω_e may carry some IU location information and can be used to infer the changes in IU's true location. To ensure that IU-ESC distance changes cannot be discovered in a sequence of ω_e, our method increases the randomness in the value of ω_e by using random numbers ξ_1 and ξ_2 in the generation of ω_e as shown in Equation (3). To analyze if the variations in ω_e are related with the changes in IU's location, one can calculate the correlation and p-value between the sequence of ω_es and the IU-ESC distances [26]. A lower p-value can be interpreted as a stronger correlation between two sets of data, and a p-value higher than 0.05 means that the correlation is not statistically significant [26]. If the sequences of ω_es and IU-ESC distances have a low correlation coefficient with a large p-value, we can say that the correlation between ω_es and IU-ESC distances is not statistically significant, and the attacker can hardly use ω_es to infer the IU's true location. Using this method, in evaluation section VIII-C, we compute the correlation coefficient and p-value using simulation. The results show that the correlation is not statistically significant. Thus, it is difficult for an attacker to infer IU's true location changes.

VIII. Evaluation

In this section, we evaluate the proposed transmit power control algorithm by simulations. To create a realistic distributions of SU nodes in our simulation, we assume the SU communication system follow a infrastructure-based architecture that is similar to WiFi, where multiple SU user-end devices (UE) communicate with SU base stations (BS). Specifically, the simulation area is set to a $6km \times 6km$ square coastal area. We randomly distribute multiple SU BS inside the area. Around each BS, 10 UE associated with the BS are normally distributed with a scattering standard deviation of 40m. Both the BS and its pairing UE can be regarded as SU-TX or SU-RX. We consider two scenarios in the simulation. In Scenario 1, the BS serves as the receiver and its UEs are transmitters. The BS can be modeled as 10 co-located SU-RXs each receiving from one associated UE (i.e. a SU-TX). In Scenario 2, the BS acts as the transmitter and transmit to its UEs. The BS is then modeled as 10 co-located SU-TXs, each transmitting to one associated UE (i.e. SU-RX). We assume that all SU-TXs/RXs are located inland and the IU is in the sea. Five ESCs are randomly situated near the coast line for detecting the IU's activity. Both IU and SUs are mobile in the simulation. The speed of each SU-TX is set to $1m/s$ and the speed of IU is $10m/s$. Figure 2 shows an example of our simulation topology setting.

For every millisecond, each ESC senses the interference from both SUs and IU, and SAS broadcasts the global parameters. Each SU-TX reads its location information at a rate of 10Hz from a GPS sensor. A standard path loss model is applied for each SU-TX. The path loss exponent is set to 4. The environment interference φ is set to -80dbm. The system is assumed to be stable when the fluctuations in every SU transmit power are smaller than $0.0001W$.

A. Stability analysis

The evaluation first examines the stability of our algorithm under different cases discussed in Section V. We denote the case where solution set $\widetilde{R}$ to (15) exists as Case 1, the case where $\widetilde{R}$ is empty but solution set $\widetilde{Z}$ exists as Case 2, and the case where $\widetilde{Z}$ is empty as Case 3. The different parameter settings for Case 1, 2 and 3 are given in Table I. For each simulation setting, we run the simulation 100 times. Each simulation simulates 10 minutes operation time of the DSA network (600000 iterations). Simulation results for the three cases in both Scenario 1 and 2 are shown in Table II and III. In Table II, it can be observed that, on average, an SU-TX only spends less than 3% of its total operation time in the convergence process in all cases, even though mobility of IUs and SUs are constantly changing the system states.

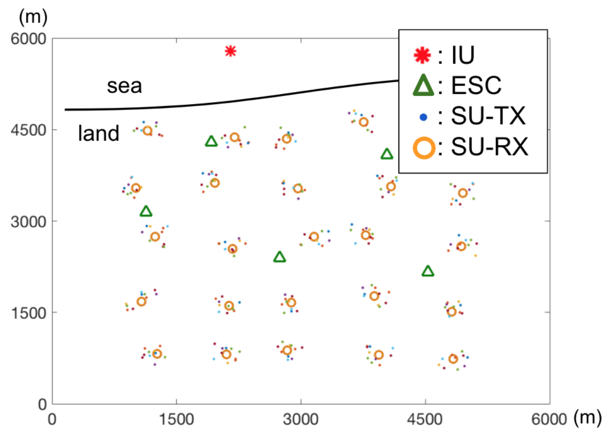

Fig. 2. Example of our simulation settings.

TABLE I

PARAMETER SETTINGS FOR CASE 1, 2 AND 3

Parameter	Case 1	2	3
number of SUs	90	160	250
SU SINR target τ	50	100	100
SU's maximum transmit power (W)	2	1	1
IU's allowable interference (W)	10^{-6}	10^{-6}	10^{-9}

1) Case 1: Solution set $\widetilde{R}$ to (15) *exists:* The first simulation examines our algorithm's performance when the optimal power settings in $\widetilde{R}$ exist to satisfy both the IU's interference requirement and the SU-TXs' SINR requirements within the SU-TXs' maximum power constraint. As shown in Table III, the fraction of time an SU's SINR does not satisfy its target τ is very small due to quick convergence of our algorithm and the algorithm's stable point's guarantee of SU's SINR under case 1. IU's interference requirement is satisfied 100% of time because our algorithm guarantees IU's interference constraint at any time.

2) Case 2: $\widetilde{R}$ is empty but solution set $\widetilde{Z}$ exists: The second simulation looks at those cases where not all SU-TXs can achieve the required SINR all the time because of the maximum transmit power limit on SU-TXs. To simulate this case, as shown in Table I, we increase the number of SU-RX to 16 and the target SINR of SU BSs to 100, and decrease an SU's maximum transmit power to $1W$. This will make it harder for all SU-TXs to satisfy their RXs' SINR requirements within the allowable range of transmit power. In this case, we expect some SU-RX

TABLE II

AVERAGE CONVERGENCE SPEED OF SU-TXS' TRANSMIT POWER IN CASE 1, 2 AND 3 OF SCENARIO 1 AND 2

Fraction of time used for convergence	Case 1	Case 2	Case 3
Scenario 1	0.0241	0.0245	0.0251
Scenario 2	0.0239	0.0241	0.0244

TABLE III

SIMULATION RESULTS FOR CASE 1, 2 AND 3 IN SCENARIO 1 AND 2

		Fraction of time transmit power $<$ the maximum	Fraction of time when SU's SINR $\geq \tau$	Fraction of time when SU interference to IU $\leq T$
Scenario 1	Case 1	1	0.9784	1
	Case 2	0.5260	0.5840	1
	Case 3	1	0.0422	1
Scenario 2	Case 1	1	0.9771	1
	Case 2	0.5423	0.6267	1
	Case 3	1	0.0531	1

will not get its SINR satisfied despite its SU-TX using maximum transmit power, while other SU-RXs can maintain their SINR. Table III's simulation results exactly match this expectation. In addition, Table III shows that our scheme still ensure the IU's interference level is below the threshold in this case.

3) Case 3: $\widetilde{Z}$ is empty: In the third simulation, as shown in Table I, we reduce the IU's interference requirement to an extremely low $10^{-9}W$, and further increase the number of SU BS to 25. As discussed in Section V-B2, such a setting makes it impossible to guarantee SU-RXs' SINR requirements due to the strict IU interference constraint. In this case, our algorithm should ensure IU's interference requirement first and sacrifice the SU's SINR. This expectation matches results in Table III. SU's SINR requirement is hardly satisfied in the simulation due to the extremely low IU interference requirement, while this extremely-low IU's interference requirement is still always satisfied.

In addition, as shown in Table II, only a tiny increase in the convergence time is observed as the total number of SUs increases from 90 to 250 among the three cases, which indicates good scalability of our algorithm.

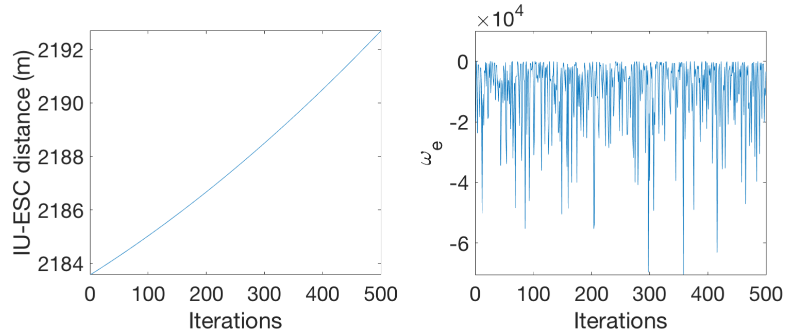

Fig. 3. Left figure shows 500 iterations of one sequence of IU-ESC distances and right figure shows the corresponding ω_e sequence.

B. Efficiency evaluation

We compare our algorithm with the existing IU protection schemes [27], [28] in terms of network capacity under the same IU interference protection level. A geographic exclusion zone (GEZ) scheme in [27] calculates the minimum radius of the primary exclusion zone based on the primary outage constraint, and [28] proposes a shapeless PU protection scheme called the discrete exclusion zone (DEZ), which is achieved by switching off the first $k-1$ nearest neighboring SUs surrounding the PU. With the number of SUs equal to 500, in order to ensure IU's interference requirement equal to $10^{-8}W$, the minimum radius of exclusion zone in GEZ is set to 3000 m and the number of SUs being switched off in DEZ is set to 150. The results show that under these settings, our scheme can improve the total SU capacity by 50% over GEZ and by 47% over DEZ.

C. Evaluation on IU location protection

In the evaluation, we randomly generate 500 settings of the locations of a moving IU, 3 ESCs and 250 static SUs. Each simulation with one setting lasts for 60000 iterations. Figure 3 zooms in for the 500 iterations of example sequences of IU-ESC distances and ω_es. The average correlation coefficient between the sequences of IU-ESC distances and ω_es is around 0.08 which can be considered negligible [29], and the p-value is around 0.28 which is larger than 0.05 [26]. Hence we can conclude that the correlation is not statistically significant. Such low correlation indicates that it is difficult for an attacker to infer IU's true location from ω_es.

D. Evaluation of communication overhead

We also compare the communication overhead of our algorithm with other privacy preservation schemes for DSA systems. Because in our algorithm the messages transmitted between entities only contain several 64-bit numbers, the average communication overhead per SU per convergence period is around 0.00112MB in our simulation. However, in the existing IU privacy protection schemes[16], [18], the communication overhead for each SU to obtain a temporary permission is in the magnitude of dozens or hundreds of MB. Our algorithm requires much lower communication overhead compared with these existing IU privacy-preserving works.

IX. Conclusion

In this paper, we proposed a distributed SU transmit power control algorithm aiming at effective channel reuse in DSA, subject to IU's interference requirement and SU-TXs' SINR requirements and upper power constraints. Due to security considerations, our algorithm does not depend on any sensitive information from IU. Each SU-TX only requires locally observable measurements and aggregated insensitive information provided by ESC to adjust its transmit power distributively. Through the analysis on the algorithm's convergence and stability properties, we demonstrate that our algorithm will converge to a unique stable point which always satisfies the IU's interference constraint. Whenever there exists a power setting meeting both IU and SUs' requirements, our algorithm will stabilize at that setting. Finally, the simulation results validate the effectiveness of the proposed algorithm.

Appendix

Theorem A.1. *$K(\boldsymbol{\lambda}, \boldsymbol{P})$ defined in* (23) *is a Lyapunov function for the system defined in* (12) - (14). *In addition, $\dot{K} = 0$ if and only if $\boldsymbol{P} = \boldsymbol{P}^*$ and $\sum_i P_i g_{ie} \leq \xi_2 T_e$.*

Proof: The partial derivative of $F(\boldsymbol{\lambda}, \boldsymbol{P})$ in (23) over P_i and λ_e are derived as:

$$\frac{\partial F}{\partial P_i} = \frac{\partial F}{\partial W} \cdot \frac{\partial W}{\partial P_i} = \frac{\partial F}{\partial W} \cdot \frac{\partial V}{\partial P_i} \tag{52}$$

$$\frac{\partial F}{\partial W} = \sum_e [f'(W \sum_i g_{ie} - \xi_2 T_e) {\lambda_e}^2 \sum_i g_{ie}] > 0 \tag{53}$$

$$\frac{\partial F}{\partial \lambda_e} = f(W \sum_i g_{ie} - \xi_2 T_e) \cdot 2\lambda_e > 0 \tag{54}$$

To prove K is a Lyapunov function of the system, we prove that (1) K is positive definite and (2) the time derivative of K satisfies $\dot{K} \leq 0$. $\dot{K} = 0$ if and only if $\boldsymbol{P} = \boldsymbol{P}^*$ and $\boldsymbol{P}^* \in \widetilde{Z}$.

Step (1): Clearly, when $\boldsymbol{P} = \boldsymbol{P}^*$ and $\boldsymbol{\lambda} = \boldsymbol{\lambda}^*$, $K(\boldsymbol{\lambda}, \boldsymbol{P}) = 0$. Then we need to prove that $K(\boldsymbol{\lambda}, \boldsymbol{P}) > 0$ for all values of $\boldsymbol{P} \neq \boldsymbol{P}^*$ or $\boldsymbol{\lambda} \neq \boldsymbol{\lambda}^*$. It is equivalent to prove that $F(\boldsymbol{\lambda}, \boldsymbol{P}) - F(\boldsymbol{\lambda}^*, \boldsymbol{P}^*) > 0$ when $\boldsymbol{P} \neq \boldsymbol{P}^*$ or $\boldsymbol{\lambda} \neq \boldsymbol{\lambda}^*$.

From (8) and (14) we can see that $\dot{\lambda}_e \leq 0$ is always true. Thus, starting from any initial point λ_e, the equilibrium λ_e^* will always be no larger than the initial λ_e and will be the smallest value within the initial λ_e's feasible region. Also, it is already proved that $V(\boldsymbol{P})$ is a positive definite function based on the (20). Moreover, given (24) and (25), it is seen that $F(\boldsymbol{\lambda}, \boldsymbol{P})$ is increasing with respect to $\boldsymbol{\lambda}(\boldsymbol{\lambda} > 0)$ and $V(\boldsymbol{P})$. Now it can be proved that $F(\boldsymbol{\lambda}, \boldsymbol{P}) > F(\boldsymbol{\lambda}^*, \boldsymbol{P}^*)$ when $\boldsymbol{\lambda} \neq \boldsymbol{\lambda}^*$ or $\boldsymbol{P} \neq \boldsymbol{P}^*$. Therefore, K is a positive definite function.

Step (2): The time derivative of K is computed by

$$\dot{K} = \sum_i \frac{\partial K}{\partial P_i} \dot{P}_i + \sum_e \frac{\partial K}{\partial \lambda_e} \dot{\lambda}_e \tag{55}$$

We first calculate the value of $\sum_e \frac{\partial K}{\partial \lambda_e} \dot{\lambda}_e$ as following:

$$\sum_e \frac{\partial K}{\partial \lambda_e} \dot{\lambda}_e = \sum_e \frac{\partial F}{\partial \lambda_e} 2\lambda_e \beta_e \left(-f(\xi_1 \frac{\sum_i P_i g_{ie} - \xi_2 T_e}{\sum_i P_i g_{ie}}) \right) \leq 0, \tag{56}$$

and $\sum_e \frac{\partial K}{\partial \lambda_e} \dot{\lambda}_e = 0$ if and only if $\sum_i P_i g_{ie} \leq \xi_2 T_e$.

Next step is to compute $\sum_i \frac{\partial K}{\partial P_i} \dot{P}_i$. Given (21), (22), (52),

$$\begin{aligned} \sum_i \frac{\partial K}{\partial P_i} \dot{P}_i &= \sum_i \frac{\partial F}{\partial P_i} \left(\dot{\widetilde{P}}_i + \sum_e \Omega_e g_{ie} \dot{\widetilde{P}}_i \right) \\ &= \sum_i \frac{\partial F}{\partial W} \left(1 + \sum_e \Omega_e g_{ie} \right) \delta_i {y_i}^2 \leq 0 \end{aligned} \tag{57}$$

Hence, $\sum_i \frac{\partial K}{\partial P_i} \dot{P}_i = 0$ if and only if $y_i = 0$, that is $\boldsymbol{P} = \boldsymbol{P}^*$. K is proved to be a Lyapunov function of our system.

References

[1] Thao T Nguyen, Anirudha Sahoo, Michael R Souryal, and Timothy A Hall. 3.5 ghz environmental sensing capability sensitivity requirements and deployment. In *2017 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*, pages 1–10. IEEE, 2017.

[2] Sooyeol Im, Hyoungsuk Jeon, and Hyuckjae Lee. Autonomous distributed power control for cognitive radio networks. In *2008 IEEE 68th Vehicular Technology Conference*, pages 1–5. IEEE, 2008.

[3] Sudheer A Grandhi, Rajiv Vijayan, David J Goodman, and Jens Zander. Centralized power control in cellular radio systems. *IEEE Transactions on Vehicular Technology*, 42(4):466–468, 1993.

[4] Anestis Tsakmalis, Symeon Chatzinotas, and Björn Ottersten. Centralized power control in cognitive radio networks using modulation and coding classification feedback. *IEEE Transactions on Cognitive Communications and Networking*, 2(3):223–237, 2016.

[5] Yiping Xing and R Chandramoul. Qos constrained secondary spectrum sharing. In *First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005.*, pages 658–661. IEEE, 2005.

[6] Lijun Qian, Xiangfang Li, John Attia, and Zoran Gajic. Power control for cognitive radio ad hoc networks. In *2007 15th IEEE Workshop on Local & Metropolitan Area Networks*, pages 7–12. IEEE, 2007.

[7] Hong-Sam T Le and Qilian Liang. An efficient power control scheme for cognitive radios. In *2007 IEEE Wireless Communications and Networking Conference*, pages 2559–2563. IEEE, 2007.

[8] Wei Wang, Tao Peng, and Wenbo Wang. Optimal power control under interference temperature constraints in cognitive radio network. In *2007 IEEE Wireless Communications and Networking Conference*, pages 116–120. IEEE, 2007.

[9] Gerard J Foschini and Zoran Miljanic. A simple distributed autonomous power control algorithm and its convergence. *IEEE transactions on vehicular Technology*, 42(4):641–646, 1993.

[10] Sudheer A Grandhi, Jens Zander, and Roy Yates. Constrained power control. *Wireless Personal Communications*, 1(4):257–270, 1994.

[11] Xingjian Li, Jun Fang, Wen Cheng, Huiping Duan, Zhi Chen, and Hongbin Li. Intelligent power control for spectrum sharing in cognitive radios: A deep reinforcement learning approach. *IEEE access*, 6:25463–25473, 2018.

[12] Behnam Bahrak, Sudeep Bhattarai, Abid Ullah, Jung-Min Jerry Park, Jeffery Reed, and David Gurney. Protecting the primary users' operational privacy in spectrum sharing. In *2014 IEEE International Symposium on Dynamic Spectrum Access Networks (DYSPAN)*, pages 236–247. IEEE, 2014.

[13] Matthew Clark and Konstantinos Psounis. Can the privacy of primary networks in shared spectrum be protected? In *IEEE INFOCOM 2016-The 35th Annual IEEE International Conference on Computer Communications*, pages 1–9. IEEE, 2016.

[14] Sudeep Bhattarai, Pradeep Reddy Vaka, and Jung-Min Park. Thwarting location inference attacks in database-driven spectrum sharing. *IEEE Transactions on Cognitive Communications and Networking*, 4(2):314–327, 2017.

[15] Yanzhi Dou, He Li, Kexiong Curtis Zeng, Jinshan Liu, Yaling Yang, Bo Gao, and Kui Ren. Preserving incumbent users' privacy in exclusion-zone-based spectrum access systems. In *2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)*, pages 2486–2493. IEEE, 2017.

[16] Chaowen Guan, Aziz Mohaisen, Zhi Sun, Lu Su, Kui Ren, and Yaling Yang. When smart tv meets crn: Privacy-preserving fine-grained spectrum access. In *2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)*, pages 1105–1115. IEEE, 2017.

[17] Yousi Lin, Yuxian Ye, and Yaling Yang. Preserving incumbent user's location privacy against environmental sensing capability. In *2019 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*, pages 1–10. IEEE, 2019.

[18] He Li, Yanzhi Dou, Chang Lu, Doug Zabransky, Yaling Yang, and Jung-Min Jerry Park. Preserving the incumbent users' location privacy in the 3.5 ghz band. In *2018 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*, pages 1–10. IEEE, 2018.

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

[20] Octavia A Dobre, Ali Abdi, Yeheskel Bar-Ness, and Wei Su. Survey of automatic modulation classification techniques: classical approaches and new trends. *IET communications*, 1(2):137–156, 2007.

[21] Timothy J O'Shea, Johnathan Corgan, and T Charles Clancy. Convolutional radio modulation recognition networks. In *International conference on engineering applications of neural networks*, pages 213–226. Springer, 2016.

[22] Yi Shi, Kemal Davaslioglu, Yalin E Sagduyu, William C Headley, Michael Fowler, and Gilbert Green. Deep learning for rf signal classification in unknown and dynamic spectrum environments. In *2019 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*, pages 1–10. IEEE, 2019.

[23] Marvin Marcus and Henryk Minc. *A survey of matrix theory and matrix inequalities*, volume 14. Courier Corporation, 1992.

[24] Mohammed Dahleh, Munther A. Dahleh, and George Verghese. Lectures ondynamic systems and control. 2004.

[25] Jagdish K Patel and Campbell B Read. *Handbook of the normal distribution*, volume 150. CRC Press, 1996.

[26] HM James Hung, Robert T O'Neill, Peter Bauer, and Karl Kohne. The behavior of the p-value when the alternative hypothesis is true. *Biometrics*, pages 11–22, 1997.

[27] Utku Tefek and Teng Joon Lim. Interference management through exclusion zones in two-tier cognitive networks. *IEEE Transactions on Wireless communications*, 15(3):2292–2302, 2015.

[28] Chen Sun and Ruicheng Jiao. Discrete exclusion zone for dynamic spectrum access wireless networks. *IEEE Access*, 8:49551–49561, 2020.

[29] Dennis E Hinkle, William Wiersma, and Stephen G Jurs. *Applied statistics for the behavioral sciences*, volume 663. Houghton Mifflin College Division, 2003.