Spectrum Management Issues in Centralized and Distributed Dynamic Spectrum Access

Yousi Lin

Dissertation submitted to the Faculty of the
Virginia Polytechnic Institute and State University
in partial fulfillment of the requirements for the degree of

Doctor of Philosophy
in
Computer Engineering

Yaling Yang, Chair
Y. Thomas Hou
Jung-Min (Jerry) Park
Lingjia Liu
Wenjing Lou
A. Lynn Abbott

June 24, 2021
Blacksburg, Virginia

Keywords: dynamic spectrum access, spectrum monitoring, location privacy protection, transmit power control

Spectrum Management Issues in Centralized and Distributed Dynamic Spectrum Access

Yousi Lin

ABSTRACT

Dynamic spectrum access (DSA) is a powerful approach to mitigate the spectrum scarcity problem caused by rapid increase in wireless communication demands. Based on architecture design, DSA systems can be categorized as centralized and distributed. To successfully enable DSA, both centralized and distributed systems have to deal with spectrum management issues including spectrum sensing, spectrum decision, spectrum sharing and spectrum mobility. Our work starts by investigating the challenges of efficient spectrum monitoring in centralized spectrum sensing. Since central controllers usually require the presence information of incumbent users/primary users (IUs) for decision making, which is obtained during spectrum sensing, privacy issues of IUs become big concerns in some DSA systems where IUs have strong operation security needs. To aid in this, we design novel location privacy protection schemes for IUs. Considering the general drawbacks of centralized systems including high computational overhead for central controllers, single point failure and IU privacy issues, in many scenarios, a distributed DSA system is required. In this dissertation, we also cope with the spectrum sharing issues in distributed spectrum management, specifically the secondary user (SU) power control problem, by developing distributed and secure transmit power control algorithms for SUs.

In centralized spectrum management, the common approach for spectrum monitoring is to build infrastructures (e.g. spectrum observatories), which cost much money and manpower yet have relatively low coverage. To aid in this, we propose a crowdsourcing based spectrum monitoring system to capture the accurate spectrum utilization at a large geographical area, which leverages the power of masses of portable mobile devices. The central controller can accurately predict future spectrum utilization and intelligently schedule the spectrum monitoring tasks among mobile SUs accordingly, so that the energy of mobile devices can be saved and more spectrum activities can be monitored. We also demonstrate our system's ability to capture not only the existing spectrum access patterns but also the unknown patterns where no historical spectrum information exists. The experiment shows that our spectrum monitoring system can obtain a high spectrum monitoring coverage with low energy consumption.

Environmental Sensing Capability (ESC) systems are utilized in DSA in 3.5 GHz to sense the IU activities for protecting them from SUs' interference. However, IU location information is often highly sensitive in this band and hence it is preferable to hide its true location under the detection of ESCs. As a remedy, 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 problems 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.

Centralized DSA spectrum management systems has to bear several fundamental issues, such as the heavy computational overhead for central controllers, single point failure and privacy concerns of IU caused by large amounts of information exchange between users and controllers and often untrusted operators of the central controllers. In this dissertation, we propose an alternative distributed and privacy-preserving spectrum sharing design for DSA, which relies on distributed SU power control and security mechanisms to overcome the limitations of centralized DSA spectrum management.

Spectrum Management Issues in Centralized and Distributed Dynamic Spectrum Access

Yousi Lin

GENERAL AUDIENCE ABSTRACT

Due to the rapid growth in wireless communication demands, the frequency spectrum is becoming increasingly crowded. Traditional spectrum allocation policy gives the unshared access of fixed bands to the licensed users, and there is little unlicensed spectrum left now to allocate to newly emerged communication demands. However, studies on spectrum occupancy show that many licensed users who own the license of certain bands are only active for a small percentage of time, which results in plenty of underutilized spectrum. Hence, a new spectrum sharing paradigm, called dynamic spectrum access (DSA), is proposed to mitigate this problem. DSA enables the spectrum sharing between different classes of users, generally, the unlicensed users in the DSA system can access the licensed spectrum opportunistically without interfering with the licensed users. Based on architecture design, DSA systems can be categorized as centralized and distributed. In centralized systems, a central controller will make decisions on spectrum usage for all unlicensed users. Whereas in distributed systems, unlicensed users can make decisions for themselves independently. To successfully enable DSA, both centralized and distributed DSA systems need to deal with spectrum management issues, such as resource allocation problems and user privacy issues, etc. The resource allocation problems include, for example, the problems to discover and allocate idle bands and the problems to control users' transmit power for successful coexistence. Privacy issues may also arise during the spectrum management process since certain information exchange is inevitable for global decision making. However, due to the Federal Communications Commission's (FCC) regulation, licensed users' privacy such as their location information must be protected in any case. As a result, dynamic and efficient spectrum management techniques are necessary for DSA users.

In this dissertation, we investigate the above-mentioned spectrum management issues in both types of DSA systems, specifically, the spectrum sensing challenges with licensed user location privacy issues in centralized DSA, and the spectrum sharing problems in distributed DSA systems. In doing so, we propose novel schemes for solving each related spectrum management problem and demonstrate their efficacy through the results from extensive evaluations and simulations. We believe that this dissertation provides insightful advice for DSA users to solve different spectrum management issues for enabling DSA implementation, and hence helps in a wider adoption of dynamic spectrum sharing.

Dedication

This dissertation is dedicated to my mother, Guiming Wang, my father, Zhenen Lin, and my grandmother, Meichai Li, for their endless love, support and encouragement.

Acknowledgments

I would like to thank my supervisor, Dr. Yaling Yang, for her invaluable advice, continuous support, and patience during my PhD study. Her extensive knowledge and plentiful experience have encouraged me throughout my academic life and daily life. I would also like to thank Dr. Y. Thomas Hou, Dr. Jung-Min Park, Dr. Lingjia Liu, Dr. A. Lynn Abbott and Dr. Wenjing Lou for agreeing to serve on my committee and providing me inspiring and helpful suggestions. Finally, I would like to express my gratitude to my family and my friends. Without their tremendous understanding and encouragement in the past few years, it would be impossible for me to complete my study.

Contents

List of Figures

List of Tables

Part I

Introduction & Background

Chapter 1

Introduction

In this chapter, we first introduce a high level overview about DSA. Then we introduce the spectrum management for DSA systems, including the issues in both centralized and distributed spectrum management mechanisms. Next, we present the scope of our work and address our ideas on solving the above-mentioned issues. Finally, the research outline and work-flow are presented.

1.1 Dynamic Spectrum Access

Radio frequency spectrum is an important and limited resource for wireless communication. Due to the rapid growth in wireless communication demands, the spectrum is becoming increasingly crowded. Figure 1.1 strongly reveals this situation.

In traditional spectrum allocation policy, unshared access of fixed bands are given to licensed users [3]. However, this old allocation policy causes spectrum scarcity problem, where there is little spectrum left now to allocate to newly emerged communication demands. Moreover, studies on spectrum occupancy show that many licensed users who own the license of certain bands are only active for a small percentage of time, which results in plenty of underutilized spectrum.

Despite of the limited opportunities, actions have been taken towards exploring new unencumbered frequency bands for the use of wireless activities. Meanwhile, the idea of spectrum sharing has started to attract a great deal of interest from both academia and industry. Hence, DSA is then proposed to enable the spectrum sharing between IUs/PUs and SUs to mitigate the above mentioned spectrum scarcity problem.

There are five spectrum initiatives in the U.S. for enabling DSA [4]: (1) TV bands: Low power unlicensed users are permitted by FCC to access the unused channels in the TV broadcast bands (TVWS). A database-driven approach is mandated by FCC in this bands. To obtain

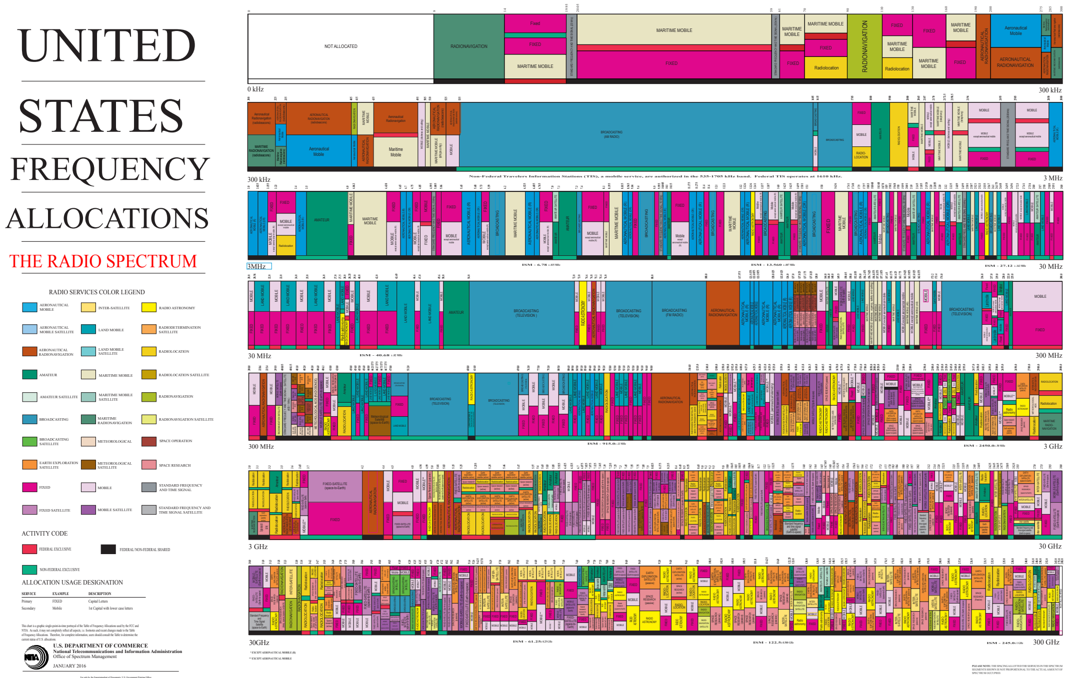

Figure 1.1: US frequency Allocation Chart [1]

the spectrum access permission, the unlicensed devices must register with a database that informs the spectrum availability. (2) AWS-3 Band: The auction of AWS-3 licenses in the 1695 - 1710 MHz, 1755 - 1780 MHz, and 2155 - 2180 MHz bands are completed by FCC in 2015. The IUs in this band are federal systems, including the federal meteorological-satellite (MetSat) systems. To protect the incumbents, the unlicensed users, e.g., the cellular service providers, operate on this band based on the manual coordination of protection zones. (3) 3.5 GHz Band: The new Citizens Broadband Radio Service (CBRS) is promulgated by the FCC for dynamic spectrum sharing between government and commercial users in the 3500-3700 MHz (referred to as 3.5 GHz band) [4, 5]. This new sharing paradigm allows CBRS devices (CBSD), which are also called SUs, to opportunistically use the 3.5GHz band in locations and times where federal IUs are not using this band. (4) 5 GHz Band: FCC intends to increase the utility of 5 GHz band by modifying the rules of the operation of Unlicensed National Information Infrastructure (U-NII) to ensure that U-NII devices do not trigger harmful interference to the IUs of these bands. (5) Millimeter Wave Bands: Non-federal use of Millimeter Wave Bands, which is commonly known as the 60 GHz band, are promoted by FCC to improve the use of unlicensed spectrum.

DSA systems deployed in 3.5 GHz band is one of the eminent DSA architectures. This architecture is composed of a SAS server and an ESC system [6], as shown in Figure 1.2. ESC system is a distributed network of sensors built to detect the IU's presence in 3.5 GHz band and inform SAS with its received signal strength (RSS) of IU signals. SAS is responsible for granting and coordinating SUs' access to the spectrum based on the reported activities of both IUs and SUs. Specifically, SAS cannot allow any SU access the licensed channel unless it can be concluded from ESC-provided IU sensing results that no harmful interference to the IUs will be triggered by the SUs' transmission. In this way, DSA can utilize the considerable amount of underutilized spectrum [7].

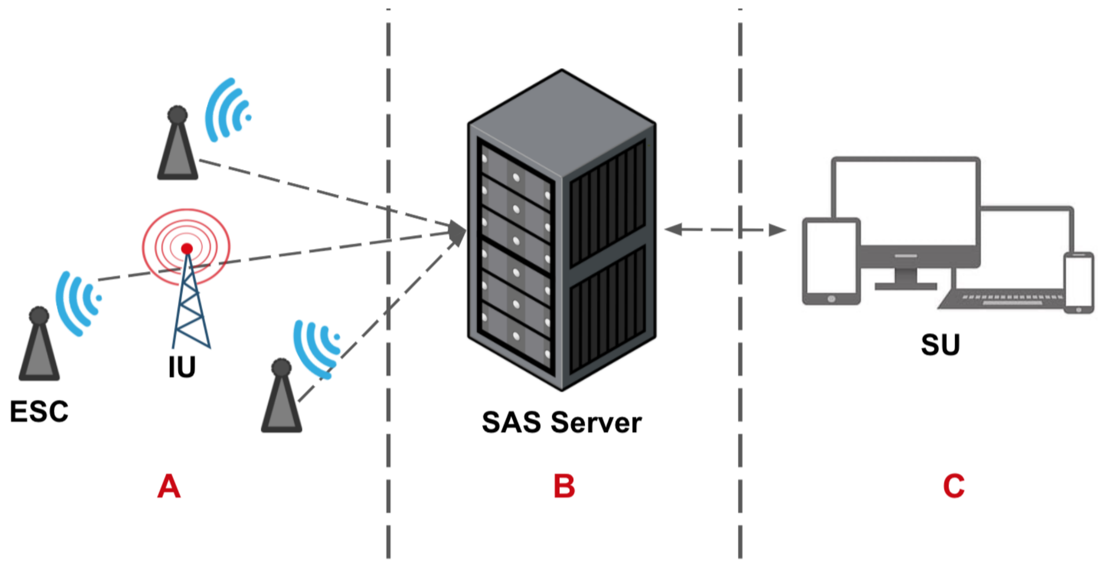

Figure 1.2: DSA system model in 3.5 GHz.

In terms of architecture design, DSA systems can be categorized as centralized coordinated and distributed coordinated. In centralized coordinated system, a central controller is responsible for resource allocation to intended users; while distributed systems allow each SU to independently collect, exchange, and process the wireless information to utilize the spectrum resources [8].

1.2 Spectrum Management for Dynamic Spectrum Access

DSA is envisioned to provide mobile users the capability to share the radio frequency with licensed PUs or IUs in an opportunistic manner. Each user in DSA has to face many challenges [9]: 1. Determine the white space of spectrum; 2. Choose the best available channel; 3. Coordination among mobile users; 4. Interference protections to IUs. As a result, dynamic and efficient spectrum management techniques are necessary for DSA users.

Spectrum management is very challenging for enabling DSA which includes four main functions [9]:

1. Spectrum sensing: Before access to any frequency band, SU must detect if there are primary signals to avoid interference with PU. This goal can be realized through a powerful sensing mechanism of SU.

2. Spectrum decision: SU chooses an available channel to use after it obtains the sensing information of the presence of PUs. Meanwhile, this allocation decision not only depends on spectrum availability. There are other factors such as the quality of the wireless channels and PU-SU coexistence schemes that may also impact the SU's decision.

3. Spectrum sharing: As multiple SUs want to share the wireless channel simultaneously, a coordination of SU transmissions such as a media access control protocol must be utilized to avoid collisions.

4. Spectrum mobility: Once the SU transmissions on a specific channel are paused due to the presence of IU, the SUs should be able to switch between the available bands to continue their communication.

Based on different architecture designs for DSA systems, spectrum management can also be deployed in centralized or distributed manner. There are different challenges for spectrum management in centralized and distributed DSA systems, as covered in the next subsections.

1.2.1 Issues in Centralized Spectrum Management

In centralized spectrum management, a central controller will make the decision for SU resource allocation based on the collected spectrum usage information of IUs as well as the channel state information of SUs.

The first issue in a centralized spectrum management system is spectrum monitoring. A centralized system demands accurate and comprehensive monitoring of the constantly and rapidly changing spectrum usage information in its service area. Building such a powerful spectrum monitoring infrastructure in DSA systems [10] is difficult. Hence, researchers have proposed many crowdsourcing techniques for centralized spectrum management. Crowdsourcing takes advantage of sensors embedded in mobile smart devices of individuals to perform complex sensing tasks, such that the burden on spectrum monitoring is spread to each SU and hence the need of an dedicated monitoring infrastructure is removed. Such system requires highly efficient data collection and processing algorithm because the computational resource of each SU is very limited, and the SU's daily operation should not be influenced at any time.

The second issue is scalability. The heavy computational overheads and communication overheads over the central controller make the system hard to scale.

Finally, the privacy of IUs is also a concern for many DSA systems where operation security of IUs are critical demands. This is because the spectrum sensing results may reveal the location and operation status of IUs. While encryption is a common solution to prevent an adversary eavesdropping on sensing results that are transmitted to the central controller, the additional encryption operations further increase the computational overheads. Furthermore, the central controller is not necessarily operated by a trusted party. Hence the possibility of its being compromised by an adversary means that an adversary may still gain access to the sensing results despite encryption on the communication channel and threaten the privacy of IUs. The current proposal in 3.5GHZ from FCC uses ESC system to mitigate this OPSEC challenge. Because 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 the OPSEC protection in ESC-based system is not enough for highly sensitive IU operation data. ESC-based system will still send IU sensing results (i.e. RSS measurements) to SAS, which can then 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.

1.2.2 Issues in Distributed Spectrum Management

In distributed systems, SU can make a decision on spectrum access independently and autonomously [8]. Since each SU has to collect information about the ambient radio environment and make its decision locally, SUs will consume more computational resources than that are consumed by SUs in centralized system [8]. Also, it is difficult for SUs to make an optimal decision independently only based on its local information. Moreover, the amount of signaling overhead may get prohibitive as network dimension increases. Furthermore, considering the IU privacy issues, there should not be any IU sensitive information that are transmitted to potentially untrusted components even though frequent control message and information exchanges often exist in distributed systems. Therefore, how to design a system which can achieve the global optimal of its own objective as well as can satisfy each user's QoS requirement and IU privacy demands becomes a major difficulty.

1.3 Scope of the Work

In this work, for centralized DSA systems, we provides solutions for two issues: sensing and IU privacy protection. For sensing, we focus on crowdsourcing based spectrum monitoring to search for the idle bands for SU access. In our algorithm, the mobile SUs act as both users of available spectrum and moving spectrum monitoring devices to achieve efficient and low-cost spectrum monitoring at a large geographical scale. For IU privacy protection, we address the IU OPSEC problem through the use of smart antenna on the IU side. Our scheme ensures that even when either SAS or ESCs are compromised, the location privacy of both static and mobile IUs are still protected.

For distributed DSA systems, we mainly focus on the distributed SU power control within the spectrum sharing problem. Two primary challenges for power control in DSA scenarios are: (1) to guarantee IU's received interference below some tolerable limit during the simultaneous transmission of IUs and SU transmitters; (2) to protect IU's operation privacy. In this dissertation, we propose two power control schemes to overcome these challenges, which aim at minimizing system's power consumption and maximizing sum of SU rates in uplink, respectively. Both schemes satisfy the IU's interference requirement and the SUs' QoS requirements (e.g., the SUs' minimum SINR requirements and transmit power constraints), while do not reveal any sensitive IU information.

1.4 Research Outline

In this section, we outline the research topics discussed in this dissertation.

1. Part I (Background & Introduction):
   - Introduction
     - In this chapter, we first provide a high level overview about DSA. Then we introduce the issues in both centralized and distributed spectrum management mechanisms for DSA systems. Next, we show the related topics of our work and address our ideas on solving the above-mentioned issues. Finally, research outline and work-flow are presented.
   - Background
     - This chapter describes the technical background about spectrum monitoring, IU location privacy protection and power control algorithms, as well as a literature review related to each topic.
2. Part II (Spectrum Sensing Issues in Centralized Dynamic Spectrum Access):
   - Crowdsourcing Spectrum Monitoring at A Large Geographical Scale
     - Spectrum monitoring is one major approach to search for the idle bands for SU access. In this chapter, we propose a crowdsourcing based spectrum monitoring scheme to share the central controller's computational overhead during spectrum monitoring. In our algorithm, mobile SUs act both as users of available spectrum white space and moving spectrum monitoring devices. With a central controller coordinating a large amount of commodity secondary mobile devices through our proposed algorithm, our algorithm can achieve low-cost spectrum monitoring at a large geographical scale. Our algorithm is simulated based on real world spectrum occupancy data.

- Preserving Incumbent User's Location Privacy Against Environmental Sensing Capability
  - In this chapter, both static and moving IU's location privacy problems are formulated and are solved through the use of smart antenna on the IU side. The proposed scheme adjusts IU's radiation pattern and transmit power to tune the antenna gains of an IU transmitter dynamically, such that it creates uncertainty in an IU's location. We give a thorough availability analysis which provides insightful advice for IU to preserve its location privacy against ESCs. Our scheme ensures that even when either SAS or ESCs are compromised, the location privacy of both static and mobile IUs are still protected.

3. Part III (Power Control Strategies in Distributed Dynamic Spectrum Access):

   - Distributed and Secure Power Control for Secondary Users in Dynamic Spectrum Access
     - In this chapter, we formulate the problem of SU transmit power control in distributed DSA system and propose a distributed SU power control algorithm. Our scheme achieves the energy consumption minimization. It can enable SINR-guaranteed coexistence between SUs and IUs and protect IUs from harmful interference, while requiring no information directly from IUs. 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.
   - Distributed and Secure Uplink Power Control in Dynamic Spectrum Access
     - In this chapter, we develop secure and distributed transmit power control algorithm to achieve the optimal uplink utility in DSA networks. Our algorithm enables optimal SU power allocation to maximize the sum of SU rates. The desired SINR of SUs are guaranteed to maintain effective communication, while no security sensitive information is required to avoid harmful interference at IUs. Convergence and stability properties of the algorithm are analyzed and demonstrated. Our scheme only requires locally observable measurements and processed insensitive information provided by BSs. Finally, simulation results are presented to validate the effectiveness of our proposed algorithms.

4. Part IV (Future Work and Conclusions):

   - Future work is discussed in this chapter.
   - This chapter gives a conclusion of this work.

Figure 1.3 shows the relations between different chapters in this dissertation.

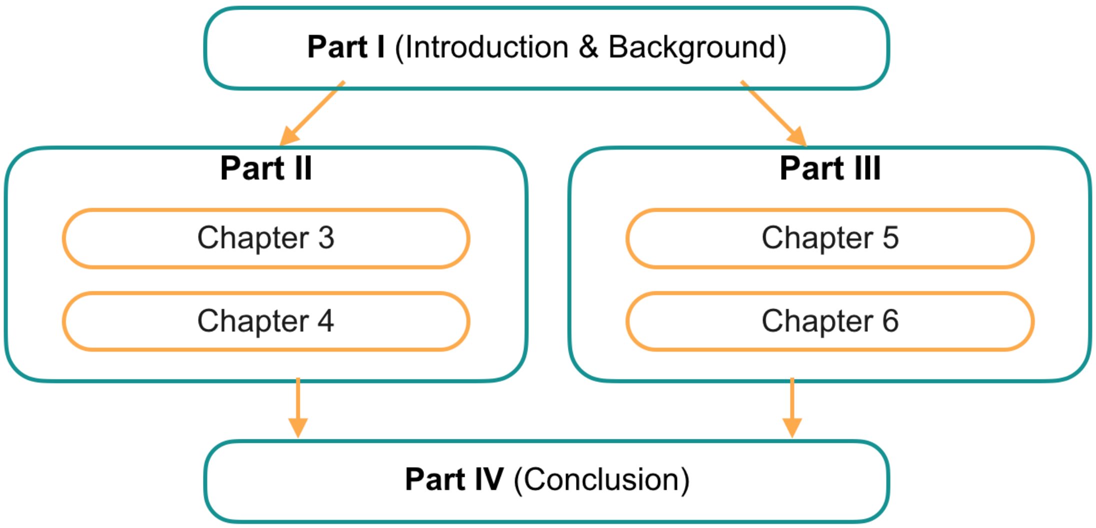

Figure 1.3: The dissertation organization.

1.5 Main Contributions

This dissertation presents novel solutions to the spectrum management issue in both centralized and distributed DSA systems.

First, we present a novel crowdsourcing based spectrum monitoring algorithm for a large geographical area that leverages the power of masses of commodity mobile devices [11]. The system accurately predicts future spectrum utilization depending on the past spectrum occupancy patterns, and intelligently schedules the spectrum monitoring tasks among mobile secondary users accordingly, so that the energy of mobile devices can be saved and more spectrum activities can be monitored. Besides the existing spectrum access patterns, our algorithm can also capture the unknown patterns where no historical spectrum information exists. Compared with existing works related to spectrum monitoring, our algorithm reduces the cost for spectrum monitoring and improves the efficiency. Our work is the first that leverages the idea of crowdsoucing in a spectrum monitoring system with intelligent task scheduling algorithms to coordinate among mass mobile devices.

Second, because the central controller usually requires IU presence information obtained during spectrum sensing to accurately allocate the spectrum resources, IU privacy protection becomes a primary concern in spectrum management. We argue that the protection provided by current ESC-based systems is not enough for highly sensitive IU operation data, since ESC may also be compromised. Specifically, IU location information is often highly sensitive and hence it is preferable to hide its true location under the detection of ESCs.

In this chapter, we design novel schemes to preserve both static and moving IU's location information by adjusting IU's radiation pattern and transmit power. With our schemes, large biases are introduced to IU location estimation results generated by the adversary. Our problem formulation and analysis provide insightful advice for IU to preserve its location privacy against ESCs. Moreover, our scheme doesn't require IU participation or a third party. It needs little computational overhead and is also simple for implementation. Simulation results show that our algorithm enhances IU location privacy protection even in the worst case where ESC are all compromised.

Third, as centralized systems must face several fundamental issues, in many scenarios, distributed systems are required. Hence, we also investigate the spectrum sharing issues in distributed DSA, specifically the power control problem. We propose two novel distributed SU transmit power control algorithms with different objectives, one of which aims at minimizing the system energy consumption and another achieves the optimal uplink network utility. Our schemes can enable SINR-guaranteed coexistence between SUs and IUs and protect IUs from harmful interference, while requiring no information directly from IUs. 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. To the best of our knowledge, our algorithms are the first two power control algorithms that meet the CBRS operational security requirements for 3.5 GHz DSA.

1.6 Chapter Summary

In this chapter, we provide an overview and background of the spectrum management for DSA systems. We discuss the spectrum monitoring issues and the IU location privacy issues on centralized spectrum management, and then introduce our ideas on solving SU power control problems in distributed spectrum management. Finally, the organization and outline of the dissertation are listed.

Chapter 2

Background

This chapter presents the technical background and literature review related to the dissertation topics.

2.1 Spectrum Monitoring in Dynamic Spectrum Access

As mentioned above, SU must detect the presence of IU before accessing the idle bands. One major way to search for the idle bands for SU access is spectrum monitoring. Spectrum monitoring is a powerful tool that help users effectively manage the frequencies to avoid improper usage and determine the sources of interference.

In centralized DSA, there are some dedicated spectrum monitoring observatories and stations providing detailed spectrum occupancy information. These systems keep scanning the spectrum, and extract useful information, which will be finally stored in various spectrum databases. Spectrum occupancy pattern is a common type of the extracted information. Each pattern represents the spectrum utilization block in both time and frequency domain. It is a time-frequency representation of corresponding PU's behavior.

Nevertheless, there are two crucial disadvantages of the old systems and monitoring approaches. Firstly, today's spectrum observatories are not widely deployed and are mostly installed by government or well-capitalized enterprises due to the expensive and cumbersome hardware that is difficult to manipulate. Secondly, most of these systems merely scan the spectrum sequentially which is naive and inefficient.

To address the current limitations, we propose to leverage the power of mass on the concept of crowdsourcing [12]. Specifically, we let the mobile SUs to act both as users of available spectrum white space and moving spectrum monitoring devices. With a central controller coordinating a large amount of commodity secondary mobile devices, we can achieve low-cost spectrum monitoring at a large geographical scale.

Crowdsourcing based spectrum monitoring face two non-trivial problems: limited energy and dynamics in crowd distribution. Mobile users have their own daily usage routines. Spectrum monitoring functions should not interfere with the normal operation of other applications. Therefore, the energy of the mobile devices that can be spared on spectrum monitoring is limited. Also, one important characteristic of mobile users is mobility. The number of devices within an area that can be used to monitor the spectrum varies at different times and may lead to temporary insufficiency in local device number. Hence, the difficulty lies in how to achieve the highest spectrum monitoring coverage with the limited energy and changing number of mobile users.

We solve these challenges by leveraging the PU occupancy pattern. As defined in [13], PU pattern is essentially a consecutive time sequence of this PU's signals which represents how this PU acts in both time and frequency domain. In our study we will use the same definition of spectrum pattern used in [13].

2.2 Location Privacy Issues of Incumbents in Dynamic Spectrum Access

Another issue that must be addressed by DSA users is the operation privacy protection for IUs/PUs. The prosperity of DSA system is contingent on how privacy issues of federal PUs 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.

From 2015, the Wireless Innovation Forum (WINNF) has been developing requirements to preserve OPSEC as required by FCC for operation in 3.5GHz band [14]. 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 IUs from CBSDs' transmissions [15–17]. 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 [18]. 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.

2.3 Power Control in Dynamic Spectrum Access

In a SAS-based DSA system, SAS cannot allow any SU access the licensed channel unless it can be concluded from ESC-provided IU sensing results that no harmful interference to the IUs will be triggered by the SUs' transmission. Power control for secondary networks, thus, can be a viable way to ensure an SU can obtain such transmission permission to coexist with IUs. One crucial challenge of designing power control schemes for the DSA system is that some IU information (e.g. IU location information) required in making an optimal power allocation is sensitive and cannot be revealed to any other user. Therefore, efficient power control strategies which have been proposed for improving the user performance in mobile networks cannot be directly applied to DSA networks, because they do not take IU privacy into consideration. SU power control in DSA networks should protect both the transmission and privacy of IUs with the highest priority to avoid any deterioration in IU's performance or any invasion of IU's operation privacy.

Fortunately, SU transmit power control aiming at different goals, such as efficient channel reuse and network utility optimization, is also studied in literature. Several existing works attempt to partially address the SU power control problem, and they can be classified into three categories: centralized optimization algorithms, distributed power control algorithms for SUs only and distributed power control algorithms for all tiers of users. Centralized optimization algorithms, such as those proposed in [19, 20], 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 SU power control strategies, such as [21–23], 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. Distributed power control algorithms for all tiers of users, such as [24, 25], do not share the IU's information with SUs, but they assume that all users (including both SUs and IUs) will participate in the power adaptation procedure simultaneously. Such assumption is also not feasible in 3.5 GHz DSA since IU operations in this band, which are satellite and radar, are independent to SU operations and classified. Thus, none of these existing schemes can properly handle the SU power control problem in DSA.

2.4 Literature Review

In this section, we review the existing works related to our scope of work including dynamic spectrum access and cognitive radio, crowdsourcing spectrum monitoring, incumbent user's location privacy protection, and power control theory in cognitive radio networks.

2.4.1 Dynamic Spectrum Access

Research on DSA has grown explosively in recent years due to the increasing demand of spectrum for all kinds of users and services. DSA implementations has attracted much interest from regulatory agencies (e.g., NTIA, FCC, OFCOM) to various of industrial or educational standardization forums such as IEEE and ACM [26]. There are plenty of DSA techniques spanning different areas such as spectrum sensing and sharing from physical layer to network layer. A survey on DSA can be found in [27].

Research in physical layer includes the topics like spectrum sensing, adjacent channel interference control and physical layer security challenges and so forth [28–30]. Specifically, high sampling rate, high speed signal processors and high resolution analog to digital converters (ADCs) with large dynamic range are necessary hardware requirements of spectrum sensing for DSA implementations [31].

In MAC layer, there exist many studies focusing on designing MAC protocols to facilitate DSA. Typical MAC protocol for DSA systems can be categorized into collaborative and collaborative MAC protocols [32]. In non-collaborative MAC protocols [33], each SU independently makes probabilistic decisions by monitoring the channels and predicting other SUs' behaviors via the proposed reasoning process. Based on different types of negotiation among SUs that are used to allocate spectrum, collaborative MAC protocols are classified into sender–receiver negotiation or group negotiation [32]. The core idea behind the sender–receiver negotiation based MAC protocols is that the sender first sends a request packet including the available channel list through the common control channel to the receivers, then the receiver replies with a selected channel based on some proposed decision making policy. In group negotiation based MAC protocols, the channel information obtained by each group member will be sent over a common control channel.

Many routing protocols are designed for DSA schemes in network layer. Most of existing routing protocols for DSA networks are traditional multi-channel routing protocols with spectrum-awareness adding into path selection, and joint routing protocols are utilized for spectrum assignment to select a path for upper layer protocol [34].

Cross layer design is also an emerging topic in DSA. For example, [35] and [36] present a physical-network cross-layer resource allocation design for overlay DSA, [37] provides a physical-network cross-layer scheme based on DQN for an ad-hoc secondary network working with underlay DSA.

2.4.2 Crowdsourcing Spectrum Monitoring

Mobile crowdsensing (MCS) is increasingly growing in popularity due to the extensive use of sensor-equipped mobile devices, and has been adopted in a diverse of sensing applications ranging from environment monitoring to human activities detection [38]. This paper mainly focuses on MCS works related to the real world spectrum monitoring. These works can be categorized into two aspects: (1) *Hardware implementation* [39, 40]: These existing works have built the hardware prototypes for distributed spectrum monitoring systems using commodity mobile devices. However, these papers do not address how to manage their systems for optimal monitoring performance. (2) *Spectrum monitoring based on fixed sensors* [2, 41]: These works assume spectrum sensors are dedicated and fixed devices. Their sensor coordination schemes are also simply letting each sensor to sequentially scanning the spectrum. An exception to this is a smart scheduling algorithm proposed in [13]. But this work is only designed for a single fixed sensor. Our work is the first that designs a crowdsoucing based spectrum monitoring system with intelligent task scheduling algorithms to coordinate among mass mobile devices (e.g. smartphones with spectrum monitoring capability).

To participate in crowdsourcing spectrum monitoring, mobile users would naturally expect certain payoff for the consumed time and energy. This situation requires effective incentive mechanisms. It is divided by [42] into the following categories: (1) Incentive schemes designed for collecting certain number of data samples through adjusting the reward [43, 44]. (2) Incentive schemes based on quality [45,46]: in this kind of schemes, not only the quantity and cost of collected data but also the quality are taken into consideration. (3) Incentive schemes considering the QoI and credibility of the collected data [47, 48]. These existing incentive schemes for attracting users to participate in crowdsourcing tasks are complementary to our spectrum usage monitoring system. We can adopt any one of them in our system.

Other related existing works focus on how to classify PU patterns [49,50] and how to predict future spectrum utilization [49,51]. PU pattern classification and prediction are also required in our system, but they are not the emphasis of this work. We apply a classic pattern classification method for PU pattern classification [52] and adopt an approach from [13] for future pattern prediction.

2.4.3 Incumbent User Location Privacy Protection

In terms of privacy protection in DSA, there is a wealth of literature done to protect IU's location privacy. Works in [6, 53–57] 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 [58] 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 [58] 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. Moreover, in an ESC-based DSA system, IU location data will not be sent to SAS. 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 [59]. 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 [60]. In addition, [61] has shown that it is possible to spoof the location of a radio transmitter through tuning its antenna patterns. However, [61] 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, [61] 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.

2.4.4 Secondary User Transmit Power Control

Several existing works can partially address the optimal SU power control problem in DSA, and I will discuss them in three categories: centralized optimization algorithms, distributed power control algorithms for SUs only and distributed power control algorithms for all tiers of users.

In the first category [62–65], several centralized algorithms are proposed to achieve the optimal power allocation. These algorithms either offer some theoretical and mathematical solutions such as convex relaxation and branch-and-bound methods to the target optimization problem, or provide some centralized strategies with a central controller to manage the transmit power of all SUs within its coverage. The theoretical solutions provide no indication on the implementation, and centralized algorithms 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. Also, SU and IU privacy is a concern in centralized power control because the central controller needs to know the location information and operation states of SUs and IUs. For example, to handle the constraint on IU's received interference, the theoretical methods or central controller in a centralized method need to measure the channel gain between SU and IU, and this is impractical in 3.5 GHz DSA because it leads to the failure of CBRS operational security (OPSEC) as described in [66]: "It is required, for OPSEC purposes, that ESCs and SASs not reveal any information pertaining to the movement or position of any federal system. Thus, ESC operators and SAS Administrators interfacing with one or more ESCs must ensure at all points in their design that the location of incumbent activity cannot be accurately estimated or tracked."

Second group of approaches [67–72] focus on distributed SU power control strategies, where SUs distributively adapt their transmit power based on some optimal formulation with target objective functions and constraints. Only locally observable measurements and received information are used for SU power adaptation. This type of algorithm 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. Many of them assumed that IU's location is known to all SUs and hence each SU can locally measure the channel gain between 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 the 3.5GHz DSA system.

Algorithms in the third category [24,25] distributively adjust the transmit power of different tiers of users (including SUs and IUs) simultaneously to achieve maximum network utility. They developed the cognitive radio network duality which decouples the transmit power, SINR assignment and the interference threshold allocation. IU's location information is assumed unknown to SU in their algorithms. However, the assumption that IUs will coordinate with SUs to simultaneously adapt their transmit powers is also not feasible in 3.5 GHz DSA since IU operations in this band, which are satellite and radar, are independent to SU operations and classified.

All of the above schemes require IUs to either reveal their private information or actively join the power adaptation in secondary networks to ensure their received interference will not exceed an allowable threshold, which violates the CBRS OPSEC requirements in 3.5 GHz DSA. Our algorithm successfully avoids the above problem. It does not require IU to participate in either information exchange or power adaptation process. In our designs, ESC does not provide any information directly related to an IU's location to SAS, it only gives SAS some masked values indirectly related to IU signal strength.

2.4.5 Practical assumptions for power control in 3.5 GHz DSA and the corresponding FCC regulations

As discussed, the assumptions of the existing power control algorithms on IU, SU, ESC and SAS operations are not applicable in 3.5 GHz DSA. Thus, we list the practical assumptions that are used in our algorithms and the corresponding regulations.

1. SU transmit power adaptation must not cause any harmful interference to IUs.
   Regulations:

   (a) 47 CFR §§ 2.106, 97.303(d), (f): "Non-federal amateur services operating in the 3.3-3.5 GHz portion of the band must not cause harmful interference to operations such as radio astronomy stations and stations authorized by other nations for radiolocation service." [73]

   (b) 3.5 GHz R&O and FNRPM, 30 FCC Rcd at 3962, para. 4: "Incumbent users receive interference protection from Citizens Broadband Radio Service users." [73]

2. IUs' location information in the 3.5 GHz DSA system is highly sensitive and hence should not be derived from any messages transmitted at any point of our power control system.
   Regulations:

   (a) CBRS Operational Security: "It is required, for OPSEC purposes, that ESCs and SASs not reveal any information pertaining to the movement or position of any federal system. Thus, ESC operators and SAS Administrators interfacing with one or more ESCs must ensure at all points in their design that the location of incumbent activity cannot be accurately estimated or tracked." [66]

3. SAS cannot store or transmit any sensitive information on IU's location (e.g. channel gain between SU and IU).
   Regulations:

   (a) The FCC Part 96 rules: "96.55 – Information Gathering and Retention – (c) The SAS shall only retain records of information or instructions received regarding federal Incumbent User transmissions from the ESC in accordance with information retention policies established as part of the ESC approval process." [74]

   (b) The FCC Part 96 rules: "96.63 – Spectrum Access System Administrators – (n)(2) Ensure that the SAS does not store, retain, transmit, or disclose operational information on the movement or position of any federal system or any information that reveals other operational information of any federal system that is not required by this part to effectively operate the SAS." [74]

4. ESC cannot store or transmit any sensitive information on IU's location.
   Regulations:

(a) The FCC Part 96 rules: "96.67 - Environmental Sensing Capability – (c)(7) Ensure that the ESC ... does not store, retain, transmit, or disclose operational information on the movement or position of any federal system or any information that reveals other operational information of any federal system that is not required by this part to effectively operate the ESC." [74]

(b) R2-ESC-[SENSOR CONSTRAINTS]: "The ESC shall meet the following requirements:

- Sensors shall not store or transmit any time-series data for detecte incumbent signals.
- Sensors shall not store or transmit any incumbent radar signal characteristics other than the minimum required for incumbent radar activity determination.
- Sensors shall not convey timing information whose accuracy and precision is sufficient to enable geolocation techniques.
- Sensors shall only report quantized received signal strength indication (RSSI) measurements.
- Sensors shall not employ highly directional antennas for purposes of precision angle of arrival (AoA) estimation.

The intent of these requirements is to prevent the ESC from performing any form of precision geolocation." [66]

2.5 Chapter Summary

This chapter discussed the technical background of the research topics studied in this dissertation, including spectrum monitoring issues and IU's location privacy problem in centralized DSA and SU transmit power control strategies in distributed DSA. A literature review of the topics is also provided.

Part II

Spectrum Sensing Issues in Centralized Dynamic Spectrum Access

Chapter 3

Crowdsourcing Spectrum Monitoring at A Large Geographical Scale

This chapter studies the topic on crowdsourcing based spectrum monitoring. Spectrum monitoring is an important way to search for the idle bands for SU access. A crowdsourcing based spectrum monitoring system for a large geographical area is proposed that leverages the power of masses of portable mobile devices. The system can accurately predict future spectrum utilization and intelligently schedule the spectrum monitoring tasks among mobile SUs accordingly, so that the energy of mobile devices can be saved and more spectrum activities can be monitored. We also demonstrate our system's ability to capture not only the existing spectrum access patterns but also the unknown patterns where no historical spectrum information exists. The experiment shows that our spectrum monitoring system can obtain a high spectrum monitoring coverage and low energy consumption.

3.1 Introduction

This section presents an introduction of the crowdsourcing based spectrum monitoring and the challenges that must be faced.

Spectrum monitoring is a powerful tool in DSA to help SUs access the unused spectrum white space. The common approach for spectrum monitoring is to build infrastructures (e.g. spectrum observatories), which cost much money and manpower but have relatively low coverage. Crowdsourcing based spectrum monitoring face two non-trivial problems: limited energy and dynamics in crowd distribution. Mobile users have their own daily usage routines. Spectrum monitoring functions should not interfere with the normal operation of other applications. Therefore, the energy of the mobile devices that can be spared on spectrum monitoring is limited. Also, one important characteristic of mobile users is mobility. The number of devices within an area that can be used to monitor the spectrum varies at

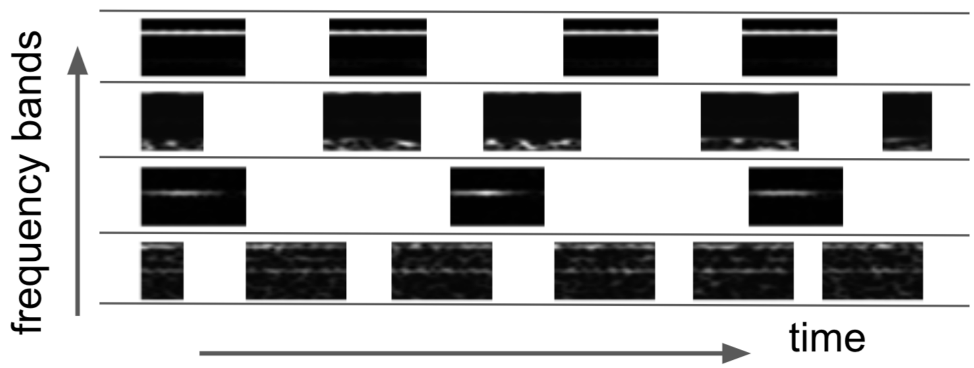

Figure 3.1: From top to bottom, 4 examples of PU patterns from Cityscape Spectrum Observatory [2] used in our experiment.

different times and may lead to temporary insufficiency in local device number. Hence, the difficulty lies in how to achieve the highest spectrum monitoring coverage with the limited energy and changing number of mobile users.

We solve these challenges by leveraging the PU occupancy pattern. As shown in Figure 3.1, real spectrum access behaviors exhibit clear patterns. In this figure, a white block denotes a period of channel idle time, and the dark parts with some bright texture denote the behavior of active spectrum users. Thus, recorded past spectrum dataset not only can be used to extract past spectrum access patterns, but also can implicate the future dynamics in spectrum access. Thus, our spectrum monitoring system uses a smart scheduling algorithm that discovers the dynamic patterns of past spectrum activities to improve monitoring efficiency and reduce energy consumption within this system. Besides existing patterns, our system also includes an algorithm to intelligently watch for and learn new patterns that have not been found in past history.

The rest of this chapter is arranged as follows. Section 3.2 explains our system model. Section 3.3 and 3.4 describes how we use pattern information to intelligently assign monitoring tasks among SUs and how we discover new patterns. Section 3.5 evaluate our schemes.

3.2 System Model

As in Figure 3.2, our system is built upon a model where there are multiple PUs and a large group of SUs scattered inside a large geographical region. The SUs are controlled by the central controller. The design of our model is based on two fundamental observations [13]: (1) PU signal has semi-regular pattern. The spectrum usage pattern represents how PU acts in both time and frequency domain. Because a PU's activities will not be completely random, we are able to find a certain distribution for the corresponding spectrum usage patterns. We refer a burst of a PU's transmission as one PU occurrence and the PU's pattern is essentially a sequence of its signal occurrences. In general, the intervals between consecutive occurrences of a PU have an uneven distribution. (2) PU's occurrence can be learned from history. The probability of a PU occurrence appearing within a certain time period can be calculated using the PU pattern's probability density function (PDF). Figure 3.3 shows the distributions of the occurrence intervals of 4 different PUs from real spectrum monitoring trace [2], which shows distributions similar to Gaussian distributions.

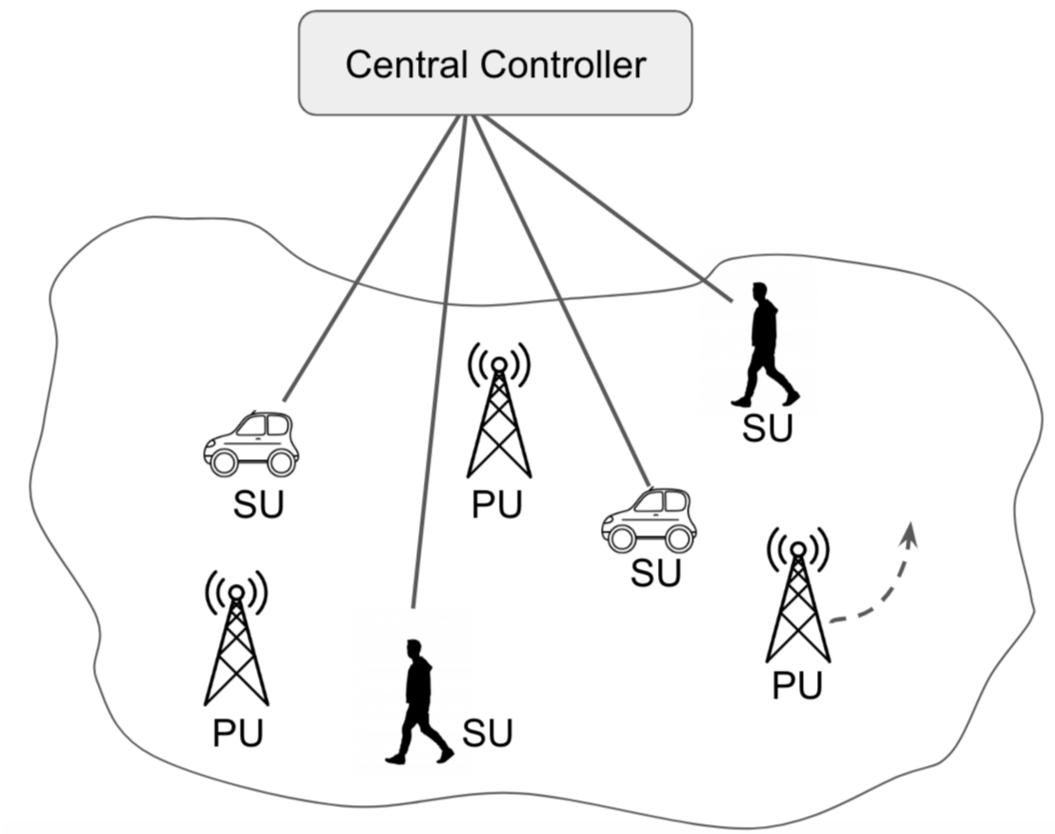

Figure 3.2: Our system model.

We assume some PUs are static and some PU can be mobile. All SUs are assumed to be mobile. According to [40], there already exist several distributed spectrum monitoring prototypes built on smartphones. Hence, we can also assume all SUs have spectrum monitoring capabilities.

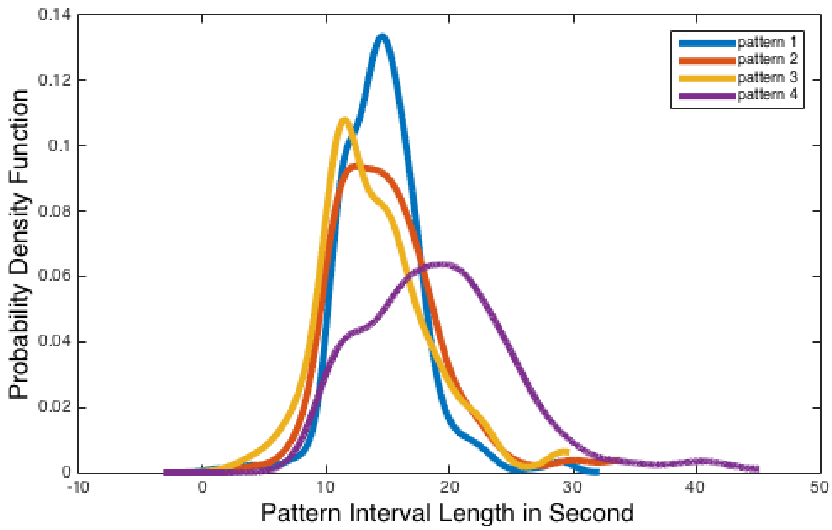

Figure 3.3: PDFs of 4 kinds of pattern interval τ.

3.3 Existing PU Pattern Monitoring

In this chapter, we deal with two types of PU activity patterns. The first type is called *existing PU pattern*, which refers to on-going PU transmission activities that also appeared in the past and hence were recorded. The second type is called *unknown PU pattern*, which refers to PU transmission activities that are not included in existing recorded dataset. In this section, we discuss our existing PU pattern monitoring scheme. In section 3.4, we will outline unknown pattern monitoring.

Existing PU pattern monitoring leverages PU activity history in the spectrum databases for future spectrum monitoring. However, the PU activity information in these databases are all raw data. Therefore, a PU pattern classification procedure is required to identify existing PU patterns and compute the statistical distribution of occurrences in each pattern.

We extract PU patterns from existing PU activity datasets by the following two steps. First, we obtain the raw in-phase and quadrature (I/Q) information from the datasets and generate time-frequency occurrences. Second, we group PU occurrences into pattern groups based on similarity of the occurrences in frequency and time domain. The similarity is characterized by a 2D cross-correlation function [75] as:

$$P_1 \circ P_2(x, y) = \sum_{i=0}^{X} \sum_{j=0}^{Y} P_1(i, j) P_2(x + i, y + j), \tag{3.1}$$

where P_1, P_2 denote two occurrences, (X, Y) represent the discretized size of each occurrence at time and frequency domain, and the x, y denote the shifts of P_2 in time and frequency respectively. If two occurrences have a high cross-correlation, they are very similar in both time and frequency domain, thus they can be considered as in the same pattern.

For each existing pattern identified in the above process, we derive the statistical distribution of intervals between neighboring occurrences. Based on these distributions, a smart scheduling algorithm then assigns targeted monitoring tasks of existing PU patterns among SUs, so that we can reduce the energy consumption of PU monitoring. Essentially, our existing PU pattern monitoring algorithm leverages the fact that efficient monitoring of known patterns does not need to monitor every frequency band all the time. It can perform targeted monitoring only on time and spectrum range where the patterns have a chance to occur.

Three approaches for existing PU pattern monitoring are proposed as follows: The method named ideal optimal assignments is explained in Section 3.3.1. This method generates the optimal monitoring assignments under ideal and unrealistic assumptions. Its performance is treated as the upper bound for other approaches. A heuristic algorithm is presented in Section 3.3.2. It can be regarded as a substitute to ideal optimal assignments with realistic assumptions

3.3.1 Ideal Optimal Assignments

The core of existing PU pattern monitoring is essentially the problem of coordinating SUs to achieve the optimal monitoring assignments based on PU occurrence time.

Consider a case where K PUs are scattered on a certain area, and N SUs are moving inside the area. K PUs generate a total number of M PU occurrences within a certain long period of time T (e.g. a day). The appearance time of the kth occurrence is denoted as T^k_{appear} and assume the indexes of the occurrences are sorted in ascending order of their occurrence time (i.e. $j < k \to T^j_{appear} < T^k_{appear}$). The energy budget in any SU i at time t for monitoring jobs is the energy left by all the other applications and is denoted as $E_i(t)$. For SU i ($i \in [1, N]$) and occurrence j ($j \in [1, M]$), define $A^j_i = 1(0)$ as (not) assigning SU i to detect occurrence j. L^j_i denotes the relation of SU i and occurrence j such that $L^j_i = 1(0)$ represents that SU i is (not) close enough to detect occurrence j. When monitoring the spectrum, SU devices require a short period of lead time to switch to a targeted frequency band, which is called a switching delay sd. Sensing duration dt is the time that an SU needs in sensing an occurrence of PU transmission. Monitoring power p_i is the power used when SU is active on spectrum monitoring.

Ideally, given all the parameters mentioned above, the problem is essentially to optimally assign the SUs to monitor all of the PU occurrences while minimizing the total energy consumed by monitoring assignments, which is formulated as the optimization Problem 1 in Table 3.1. Sometimes due to the lack of SU devices or available energy for monitoring, the optimal formulation in Problem 1 becomes infeasible. If this happens, the goal of optimal assignment changes into finding an SU monitoring schedule that maximizes the number of

Table 3.1: Ideal optimal assignments

Given:	L_i^j, E_i for $i \in [1, N]$, $j \in [1, M]$
	sd, T_{appear}, p_i, dt
Find:	A_i^j
Problem 1:	Minimize Energy Consumption
Minimize:	$\sum_{j=1}^{M} \sum_{i=1}^{N} A_i^j \times dt \times p_i$
Subject to:	(3.2), (3.3), (3.4), (3.5)
Problem 2:	Maximize Monitored Occurrences
Maximize:	$\sum_{j=1}^{M} \sum_{i=1}^{N} A_i^j$
Subject to:	(3.2), (3.3), (3.4), (3.6)

PU occurrences that are monitored. This can be formulated as the optimal Problem 2 in Table 3.1.

There are four constraints for optimal formulation in step 1. The first constraint specifies that each SU only has a limited monitoring range. During assignments, SU i cannot be assigned for occurrence j if occurrence j is out of SU i's geographical sensing range, which can be formulated as:

$$if\ L_i^j = 0, then\ A_i^j = 0,\ for\ i \in [1, N],\ j \in [1, M]. \tag{3.2}$$

The second constraint indicates that one SU can only be assigned at most one time to monitor one PU occurrence among the occurrences that appear within a period shorter than switching delay. This can be formulated as:

$$\begin{gathered} if\ j < k\ and\ T_{appear}^k - T_{appear}^j < sd + dt,\ then \\ \sum_{j_1=j}^{k} A_i^{j_1} \leq 1, for\ i \in [1, N],\ j,\ k \in [1, M] \end{gathered} \tag{3.3}$$

The third constraint needs to ensure that PU monitoring should not deplete energy for other SU normal activities. Thus, this constraint states that the algorithm can only use the leftover energy from other applications, as expressed as:

$$\begin{gathered} \sum_{j=1}^{j_1} A_i^j \times p_i \times dt \leq E_i(T_{appear}^{j_1} + dt), \\ for\ i \in [1, N],\ j_1 \in [1, M] \end{gathered} \tag{3.4}$$

The fourth constraint ensures that each PU occurrence should be detected by at least one

SU, as shown as:

$$\sum_{i=1}^{N} A_i^j \geq 1, \ for \ j \in [1, M] \tag{3.5}$$

When the formulation in Problem 1 is infeasible, we will execute the formulation in Problem 2. The constraints for Problem 2 are the same to Problem 1 except for constraint (3.5). Under Problem 2, the last constraint states that an SU should not be assigned to monitor the same PU occurrence twice. This can be formulated as:

$$\sum_{i=1}^{N} A_i^j \leq 1, \ for \ j \in [1, M] \tag{3.6}$$

3.3.2 Fast Heuristic Algorithm

Note that the optimal assignment problem 1 and problem 2 in the last subsection only provide an upper limit on the performance of SU assignment algorithm. This is because they demand that the appearing time of every future occurrence and the leftover energy at every SUs are precisely known, which is impractical. Thus, in this subsection, we propose a heuristic algorithm based on uncertain future as a practical solution for existing PU pattern monitoring. This heuristic strategy can handle the uncertainty in the time and frequency information of PU occurrences and energy budget. Note that when there is uncertainty in PU occurrences, an SU may need to monitor a frequency band for a much longer amount of time than the sensing duration dt while listening and waiting for the possible PU occurrence to appear. Thus, the essence of our heuristic approach is to heuristically allocate the energy-limited monitoring time so that we can maximize our statistical coverage of PU occurrences in a short period T_{step} from the current time. The heuristic computation is then repeated at the beginning of every T_{step} as time progresses. In the following, we describes the detail of this heuristic approach.

To maximize the monitoring tasks' statistical coverage of PU occurrences, the first step is to analyze the statistical distribution of PU occurrences. As in Figure 3.3, the occurrence time of each pattern will follow a certain distribution which can be learned from history. Probability that a PU occurrence appears within a certain time range can thus be computed based on the distribution. If we assign SU's limited monitoring time to span only those time ranges with high occurrence probability, we can maximize our coverage.

We define the time between two consecutive occurrences of a same pattern as the pattern interval τ. The statistical distribution of τ is computed based on this pattern's historical data. Its mean μ determines the mean occurrence interval, and standard deviation σ measures the variation of occurrences intervals in each pattern.

As in Figure 3.4, the distribution of τ can be used to generate a reliable future occurrence sequence in T_{step}. Assuming T_{last} is the last time where we observed a PU pattern's occurrence, distribution of the pattern's k_{th} future occurrence after T_{last} can be computed as the PDF function in Figure 3.5 with the mean shifted to $k\mu + T_{last}$. The cumulative density function (CDF) for each PU pattern is calculated based on PDF function. We then assign an SU monitoring time to maximize the probability of occurrence detection based on the CDFs.

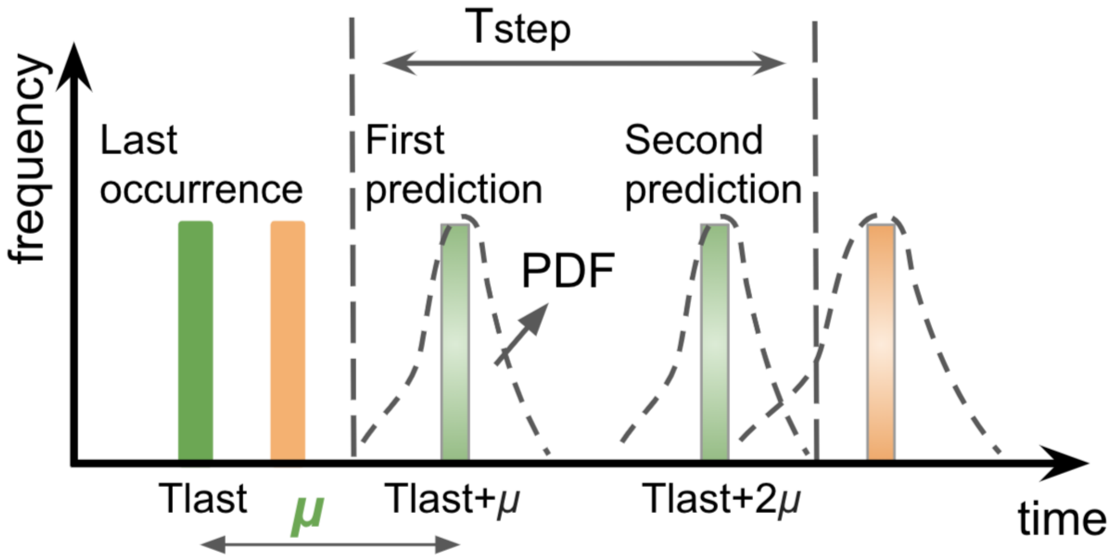

Figure 3.4: Future occurrences of the pattern after T_{last} can be computed as PDF function with its mean shifted to $k\mu + T_{last}$. Here, different color represents occurrences in different patterns.

Since the exact energy budget for monitoring (i.e. leftover energy of other applications) is also uncertain, a prediction of energy budget for spectrum monitoring in the current T_{step} is also needed to figure out the limit on monitoring time in each SU. In our heuristic optimization, the prediction is based on profiles of mobile device usage. Using the usage information, at the current time t, we can predict the time when the next charging event will happen, denoted as T_{charge} , and other applications' future energy consumption till the next charging event, denoted as $E_{app}(t)$. We can also obtain the current battery energy $E_{battery}(t)$. Hence, the energy budget for each SU per T_{step} can be estimated by

$$E_i(t) = \frac{E^i_{battery}(t) - E^i_{app}(t)}{total\ number\ of\ T_{step}s\ before\ T^i_{charge}}, \tag{3.7}$$

We further suppose that SUs report their locations at the beginning of each T_{step}, and they will stay adjacent to this location within T_{step}. Thus, the relation L_i^j between SU i and occurrence j can be computed using the location information.

Essentially, the heuristic algorithm is an iteration method to quickly generate the assignments with limited loss in coverage for this T_{step} time. The heuristic algorithm has two steps: step 1 is to identify segments as assignment units to simplify the PDF of each predicted occurrence; step 2 is the segment-based SU scheduling.

Step 1: In step 1, we first divide the PDF of a PU occurrence from the center into 7 *sensing segments*, and each segment has a length of a standard deviation σ of the PDF as shown in Figure 3.5. Assuming that PU occurrences follow a PDF similar to normal distribution, which has been validated in analysis of PU behaviors as shown in Figure 3.3, the probability that an occurrence appears outside of the 7σ range can be approximated as 0. Each segment is the smallest time unit considered in our scheduling algorithm. Given the energy that should be reserved for each SU at each T_{step}, the goal of our scheduling algorithm is to properly utilize the energy within each T_{step} to monitor as much segments as possible for all pattern occurrences in T_{step}. If each segment of every occurrence has an assigned SU to monitor the corresponding PU's activity, then all PU activities will almost surely be captured by our scheduling algorithm.

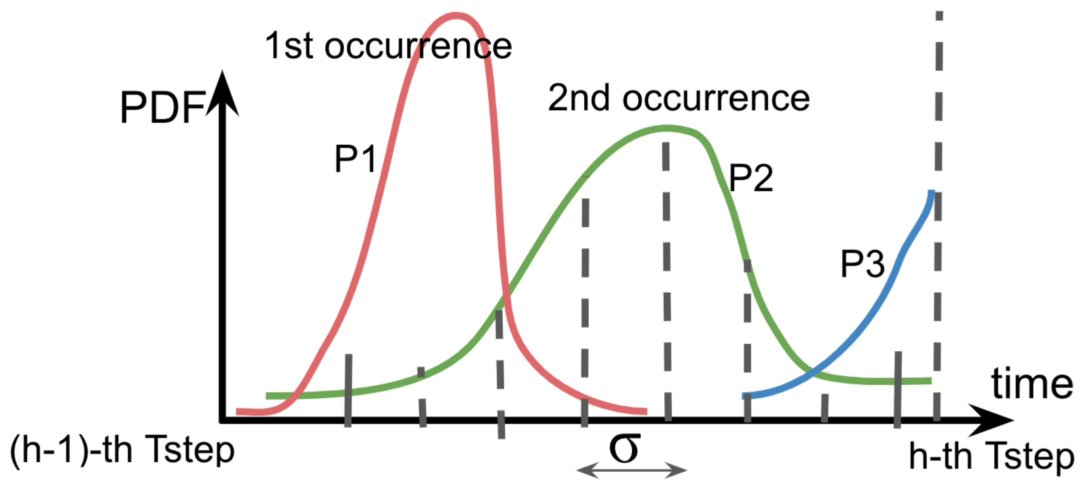

Figure 3.5: An example showing how we divide the PDF into 7 portions. The interval between 2 consecutive dash lines are a portion of σ.

Step 2: In step 2, we assign SU's monitoring jobs in unit of segment. There are *two scheduling cases* for each segment: (1) If there exists any SU that is capable of monitoring the PU for the entire sensing segment, the task of this segment will be allocated to a single SU. (2) For the segment with no feasible assignment, we will use best effort assignment strategy.

For both cases, we first compute the relation L_i^j at the beginning of T_{step}. Based on L_i^j, we can obtain a list of SUs which are close enough to detect a PU j's signal. For each segment of a PU occurrence, we further narrow down the SU list to only include those with sufficient energy and have no other on-going monitoring assignment to cover the entire segment. If the resulted list is not empty, we have case 1 and use a metric $reward_{i,j}^k$ for picking the best SU from the list to monitor the target segment. The higher the value of $reward^k_{i,j}$ is, the more preferable that SU i is for monitoring segment k of PU j's occurrence. When we cannot find any SU that has adequate energy or time to sense an entire segment, we have case 2 and will use best effort strategy. In this case, SU with the largest reward metric $reward^k_{i,j}$ will provide its best effort to cover as much of the segment as possible, and then leave the rest of the segment to the SU with the second largest reward and so forth, until the segment is entirely covered, or there is no assignable SU left. Essentially, the two cases described above ensures that we first try to assign a single SU to monitor an entire segment before we resort to the best effort assignment that assigns monitoring tasks with finer time span. This preference for larger time unit in assignment is because an SU needs to pay the cost of switching delay. Thus, assignment of an SU to monitor a too small time period is not efficient in terms of monitoring time management.

For both cases, we use a metric $reward^k_{i,j}$ for picking the best SU from a list of SU candidates to be assigned to monitor the target segment. This $reward^k_{i,j}$ is designed to be a product of three factors as follows:

$$reward^k_{i,j} = W^k_{i,j} \times E_i \times value^j_i, \tag{3.8}$$

where $W^k_{i,j}$ denotes SU i's relative profit of sensing the segment k of PU j's occurrence comparing to the choices of monitoring the segments of other PUs' occurrences; $value^j_i$ denotes how valuable is SU i's potential monitoring service for occurrence j comparing to the other possible choices of SUs for this monitoring job. The calculation for energy budget E_i follows equation (3.7). $W^k_{i,j}$ is computed as below:

$$w^k_{i,j} = prob^k_j \times L^j_i;\ W^k_{i,j} = w^k_{i,j} - maxW^k_j if\ w^k_{i,j} > 0 \tag{3.9}$$

where $prob^k_j$ is the probability that an PU j's occurrence appears in segment k , $w^k_{i,j}$ denotes the absolute profit (i.e. chance of capturing an occurrence) if we assign SU i to monitor segment k of PU j, and $maxW^k_j$ is defined as the largest w value that can be obtained by SU i if SU i spends segment k's time to monitor other PUs occurrences instead of PU j's occurrence. Mathematically,

$$maxW^k_j = \max_{l \neq j,m} w^m_{i,l} L^l_i O^{k,m}_{j,l}, \forall i,j \text{ satisfying } L^j_i = 1, \tag{3.10}$$

where $O^{k,m}_{j,l} = 1$ if segment k of PU j's occurrence time overlaps with segment m of PU l's occurrence time and $O^{k,m}_{j,l} = 0$ for other cases. Essentially $maxW^k_j$ is a loss that should be taken into account for relative profit calculation because an SU cannot simultaneously monitor multiple PUs. If an SU is allocated to monitor a segment of one PU, it will lose the probability of capturing occurrences of other PUs.

The design of the $value^j_i$ is based on the following rationale. Assuming an SU i is able to hear more than one PUs' signal, the urgency of mandating SU i to monitor a particular PU

j's segment is related to the number of SUs within the area that can also sense PU j's signal. If many SUs can detect PU j's signal, then it is not a big issue to arrange SU i to sense other PUs' signal since it is easy to find alternative SUs for the monitoring task of PU j. Thus, the $value_i^j$ will be small in this case. Based on this reasoning, we define:

$$value_i^j = 1 - \frac{X_j}{\sum_{l \in S(i)} X_l} \tag{3.11}$$

where X_j denotes the number of SUs that can hear PU j's signal and $S(i)$ is defined as the set of PUs whose signal can be heard by SU i.

At the beginning of each T_{step}, we determine which case will be encountered and then perform the reward metrics computation. The procedure will be repeated for each T_{step}.

3.4 Unknown PU Pattern Monitoring

So far, we only mandated SUs to monitor the PU patterns occurred in the past. However, historical information will grow inaccurate as time goes by due to PUs' spectrum access behavior change and mobility, which will finally degrade the performance of our proposed system. To keep our system updated with PU dynamics, we also need to discover new PU patterns, which is defined as pattern exploration in [13].

Using **unknown pattern** to represent new PU patterns that are not included in our existing pattern dataset, our design aims to watch as many unknown patterns as possible while stably monitoring the occurrences of existing patterns.

3.4.1 Heuristic Algorithm based on SU Location

Suppose that after finishing existing pattern detection at the beginning of each T_{step}, some SUs may still have extra remaining energy and idle time to be utilized for detecting unknown PU occurrences. Optimal assignments for this scenario can be generated using the same optimization formulation as in Table 3.1 of Section 3.3.1, except that occurrence i in this formulation means unknown pattern occurrence i. Again, the optimal assignments strategy assumes an ideal situation where pattern occurrence sequence and the locations of all SUs and PUs are known beforehand.

Due to the optimal assignments' unrealistic assumptions, we propose another heuristic algorithm for unknown PU pattern monitoring. The core of this algorithm lies in: (1) Without any prior information on new PU patterns, SUs randomly scan the spectrum to capture new PU occurrences. (2) If any new occurrences are detected, the central controller will quickly model the distribution of intervals between new occurrences, so that future monitoring job assignments on new PU patterns can be more targeted and accurate.

The design of the heuristic algorithm has five parts: grouping SUs based on locations, deciding SUs' monitoring schedule, random monitoring, targeted monitoring, and updating patterns in existing pattern sets.

Group SUs based on locations

Intuitively, different SUs will have high correlation in sensing outputs if they are geographically close enough. We define the SUs whose sensing ranges have adequate overlap as one group, closeby SUs belonging to the same group are considered to monitor the same area. We treat the SUs in a group as an aggregate for monitoring jobs to reduce energy consumption of each SU.

There is a trade-off between energy consumption and sensing accuracy when choosing the overlap threshold. On one hand, smaller overlap threshold may result in a loss of sensing coverage since the algorithm may not detect new PU signals that only occurred in the non-overlapping area. On the other hand, the number of SUs in a group decreases as the threshold increases, which means an SU will need to spend more energy and time to handle this group's monitoring tasks. In this work, we set the overlap threshold to 80% of a device's sensing range. This value is adjustable based on the desired level of trade-off between energy consumption and sensing accuracy.

Decide SUs monitoring schedule

For each group, we need to decide the monitoring schedule of SUs inside it to maximize the aggregated monitoring time. There are two problems: How much usable time will this group have? How much time and energy each SU should contribute to this group? For each T_{step}, the assignable time of a group is determined by the idle time and energy of its SUs. Our goal is to assure as much usable time as possible for that group. Therefore, we set a metric $R_{user\_in\_group}$ as the criterion to allocate SUs' idle periods to the groups. A SU is more valuable to its group if it has larger $R_{user\_in\_group}$ compared to other SUs. This metric R is determined by the sensor priority Sp and energy budget E_i of SU i as:

$$R_{user\_in\_group} = Sp_i \times E_i \tag{3.12}$$

Sensor priority is a parameter characterizing the importance of an SU's monitoring service in a group, which is related to the number of SUs in that group. If a group contains many SUs, it is trivial not assigning a particular SU to sense an occurrence since it is easy to find alternative SUs for that monitoring job. The priority of SUs in a group is computed as the reciprocal of the group's SU number. If an SU is included in multiple groups, it will be treated as different devices as in computing the corresponding metrics. For example, if SU 1 is in both group A and B, suppose group A and B has 2 and 3 SUs respectively, the rewards of SU 1 in group A and B are calculated as $R_{1\_in\_A} = \frac{1}{2} \times E_1$ and $R_{1\_in\_B} = \frac{1}{3} \times E_1$.

In each step, all the values of $R_{user\_in\_group}$ are sorted in a descending order. Then, we allocate the idle time of each SU to its corresponding group following this list of $R_{user\_in\_group}$. Specifically, when taking an entry of $R_{i\_in\_A}$ in the list, we first check if T_{step} is totally covered in group A. If the answer is yes, we skip to check the next entry in the list. Otherwise, we allocate SU i's idle time for monitoring job in group A. The process continues until T_{step} is totally covered in every group or no usable time or energy of the SUs is left. Time segments of different SUs assigned to the same group should not be superposed as to reduce energy consumption.

Random monitoring

Note that there is no prior knowledge on where and when a new pattern will appear. Hence, we uniformly divide a groups' sensing time into multiple small pieces and randomly select a frequency band to sense during each time piece. If any unknown occurrences are found, we record the time and frequency of those occurrences, and the locations where the SUs stayed when detecting the new occurrences. We also cluster the occurrences into different patterns. This stage creates the unknown pattern dataset.

Targeted monitoring

After capturing some new PU occurrences, we can enter the targeted monitoring stage, where we compute the mean and deviation of each new pattern's intervals to model its statistic distribution.

When a new pattern just starts to occur, it is more likely that there is not enough occurrence observations to accurately characterize the new pattern's occurrence distribution. However, we can see from the observations in Figure 3.3 that the distributions of different pattern intervals are usually approximate Gaussian distributions. Therefore, when pattern samples are inadequate, we model the pattern intervals as Gaussian distributions using computed mean and deviation. If only two occurrences of a pattern are found, we use the interval between these two occurrences as the mean value, and choose the average deviation of all kinds of patterns within the dataset as the new pattern's predetermined deviation. If just one occurrence of a pattern is detected, we use both the average mean and deviation of all kinds of patterns as the preset values for modeling. The mean and deviation value will be updated after each T_{step}.

We will be able to leverage the rough pattern interval models to predict where and when other new occurrences of this PU pattern will appear in the next T_{step}. Heuristic algorithm in Section 3.3.2 is adopted here to generate a group's sensing scheduling, except that the "worker" in this section is changed from SUs to groups.

After group scheduling is finished, we again do the random monitoring by uniformly dividing each group's remaining sensing time and randomly choosing a frequency band to monitor, in order to explore more unknown PU patterns.

Update patterns in existing pattern sets

There are two updates in existing pattern sets at the end of each T_{step}: (1) we will add newly discovered patterns to the pattern sets, and update the mean and deviation value of each pattern interval distribution. We will check if the location where we discovered a PU pattern is moving. If it is, the location information will be updated. (2) we will remove PU patterns that have not occurred for a long time from the sets.

Unknown pattern monitoring algorithm ensures that our system can start to function even when no historical data is provided. It gradually creates the pattern set and improve its monitoring intelligence based on the past data. New pattern exploration is not isolated from our scheduling algorithm. The scheduling algorithm always uses up-to-date spectrum information obtained from both existing and unknown monitoring algorithms, thus is not wedded to a wrapped dataset.

3.4.2 Update Relations between PU and SU Locations

In all previous discussions of existing and unknown pattern monitoring, we assume that we know PU and SU locations so that we can determine if an SU can hear a PU's signal. An SU's location is easy to obtain from its location updates which are commonly performed by modern-day mobile devices. The location of PU, on the other hand, is not readily available . In this section, we will explain how we obtain and update the location information of PU.

During unknown PU pattern monitoring, the initial random assignment of monitoring jobs ensures that the occurrences of a new PU pattern will likely be detected by different SUs. These SUs are at different locations and the sensing results of these SUs can then be used to localize the PU through radio localization techniques such as trilateration and proximity [60].

When a new PU pattern becomes stably detected at predicted appearing times, it becomes an existing pattern.

At this stage, it is possible that only one SU is assigned by the existing PU pattern monitoring algorithm to monitor this pattern. Overtime, a mobile PU may drift away from its old location and the SU assigned by existing PU pattern monitoring algorithm using its old location may not hear the PU's signal anymore. If the unknown PU pattern monitoring algorithm in other SUs picked up the PU's signal before this happens, we know that this known PU has moved its location and can use radio localization techniques to recompute its new location. If the unknown PU pattern monitoring algorithm did not pick up the moving PU's signal before it went off the radar, this PU is considered disappeared. However, the PU is not lost permanently. It may soon get picked up by the unknown pattern detection algorithm at some SU as a new pattern and its new location will be identified again following the procedure of the previous paragraph.

3.5 Simulation Results

In this section, we evaluate the performance of our crowdsourcing based spectrum monitoring scheme using simulations that are based on real world data. We did two sets of simulations. The first set examines the case where all patterns are stable and there is no unknown pattern, and the second set evaluates the cases where there are many unknown patterns. In the first set of simulations, we evaluated the heuristic algorithm and use the ideal optimal assignments as the benchmark. In the second simulation set, we evaluated the performance of heuristic algorithm with the ideal optimal assignments as a higher bound and a naive random detection method as a lower bound.

In our simulation, 44 types of real PU patterns in TV frequency bands are extracted from data in Cityscape Observatory spectrum databases [2], where 34 of them are used as existing PU patterns that are present from the beginning of an simulation, and another 10 patterns start in the middle of the simulation to act as unknown PU patterns. We also artificially makes 3 of the existing PU patterns to be from mobile PUs since the mobility of PUs should also be under consideration. The mobility of the PU is reflected in the changes of signal strength in SU's sensing results. We have to add artificial mobility of PU into the spectrum monitoring results because such sensed signal strength changes were not observed in existing spectrum dataset. Hence, we manually add the traces to some PUs to simulate the case where a PU is also moving. Figure 3.1 shows 4 examples of the PU patterns.

We utilize 100 taxi trajectories from mobility traces dataset of taxi cabs in San Francisco [76] to represent SU mobility traces. Figure 3.6 shows a smaller scale illustration of our simulation setting with 60 taxi traces and 10 PU deployment.

To ensure our evaluation is based on realistic energy consumption on mobile devices, we utilized a Device Analyzer dataset from University of Cambridge [77] which contains: (1) times when a phone is turned on and off; (2) times at which the phone is charging; (3)the real time battery level and voltage, etc. Hence, we are able to compute from this dataset the real energy consumption of phone applications, which can be used for computing (3.7) in heuristic algorithm. For the energy consumption of spectrum sensing, according to [40], SU devices being active on sensing draws about 1.5W as the monitoring power and the sensing duration dt is set to be 5ms based on [13]. We also set the frequency switching delay sd in our simulation to 50ms based on the empirical measurement in [40].

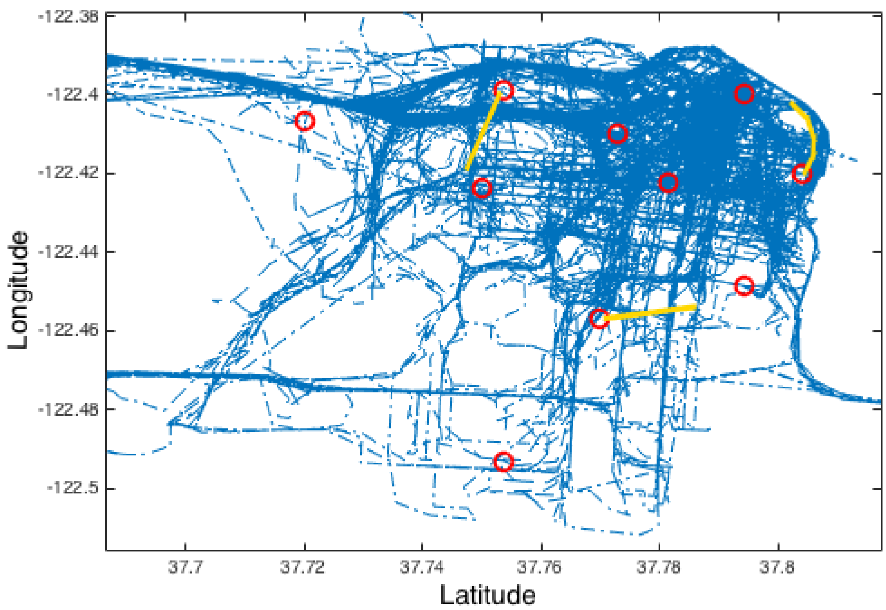

Figure 3.6: A trace-driven simulation. (dash-dot lines: taxi movement trajectories. circles: PUs.) We also add movements (yellow lines) to 3 PUs.

3.5.1 Existing PU Pattern Monitoring

In this experiment, we simulated a crowdsourcing spectrum monitoring scenario of 2 hour duration, in which 34 PUs transmitting known patterns are deployed among 10 to 100 SU traces. A T_{step} lasts for 5 seconds. At each T_{step}, SUs report their locations to the central controller.

First, we compare existing pattern coverage, defined as

$$EPcoverage = \frac{DetectedExistingPatternNumber}{TotalExistingPatternNumber}. \tag{3.13}$$

among optimal assignments and fast heuristic algorithm in Figure 3.7. In the experiment, the SU number is increased from 10 to 100 to see the changes in the coverage. For each parameter setting, we run 10 independent random simulations and show the average results in Figure 3.7. From the figure, it can be observed that the coverage is apparently increasing with the growth of SU numbers.

Figure 3.8 further shows the total energy consumption of our spectrum monitoring algorithm in the above experiment, which is the summation of energy consumption of spectrum monitoring from all the SUS.

We also plot an energy ratio (presented in dash-dot lines) to show how much energy spectrum

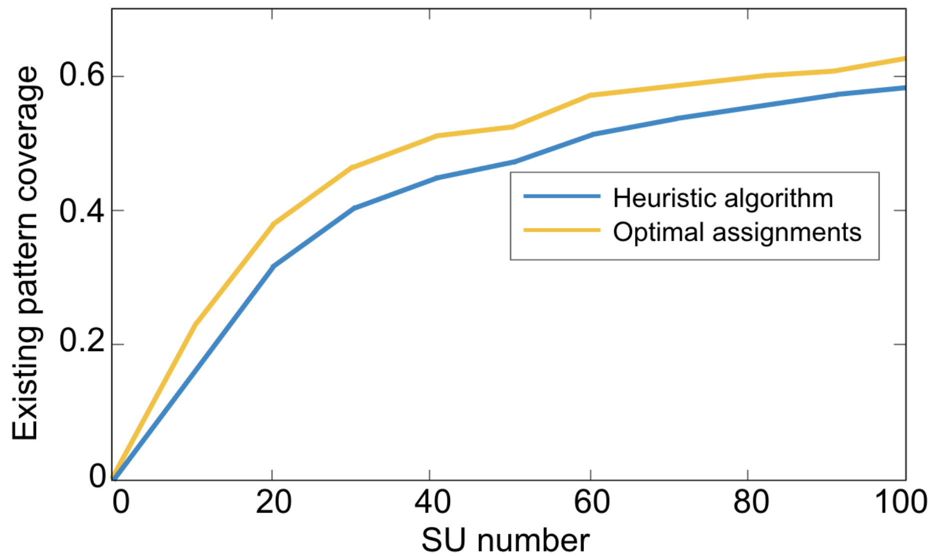

Figure 3.7: Existing pattern coverage comparison. (Yellow line: Optimal assignments. Blue line: Heuristic algorithm)

sensing really consumed against the total usable energy budget, which is defined as:

$$EnergyRatio = \frac{TotalUsedEnergyForSensing}{TotalUsableEnergyBudget} \tag{3.14}$$

From Figure 3.8, it can be seen that as the number of SUs increases, more total energy is used to get better coverage of PU signals, while the per SU's energy consumption actually decreases since more sensors are sharing the monitoring responsibility.

Figure 3.9 shows how the number of SUs available for spectrum monitoring jobs changes over time. An SU is available if it has extra energy to monitor spectrum in the next T_{step} time. We define the available SU ratio as:

$$AvailableSURatio = \frac{AvailableSUNumber}{TotalSUNumber}, \tag{3.15}$$

and record its changes in each T_{step}. As shown in Figure 3.9, the available SU ratio of heuristic algorithm fluctuates. This is due to the randomness in the energy budget, which is caused by the randomness in other applications' energy consumption. However, we do not observe drastic decrease in available SU numbers, because the energy budget used by spectrum monitoring at each T_{step} is portioned based on an SU's past energy profile.

3.5.2 Unknown PU Pattern Monitoring

In this set of simulation, we add an additional 10 unknown patterns besides the 34 existing patterns. The other settings of the simulation is the same. As a reference, we run a random

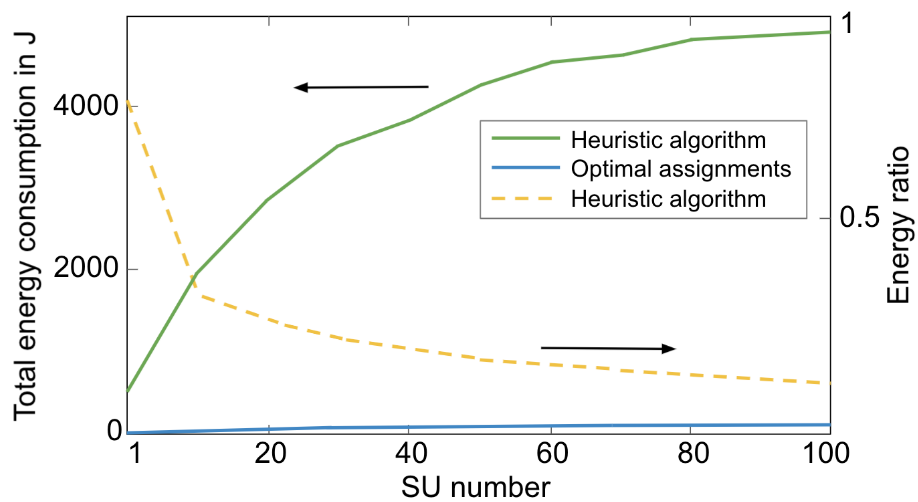

Figure 3.8: Energy consumption evaluation. Left side shows the total energy consumption in J. Optimal assignments and heuristic algorithm are presented using solid blue and green lines, respectively. Right side shows the energy ratio of heuristic algorithm, which is presented using orange dash-dot lines.

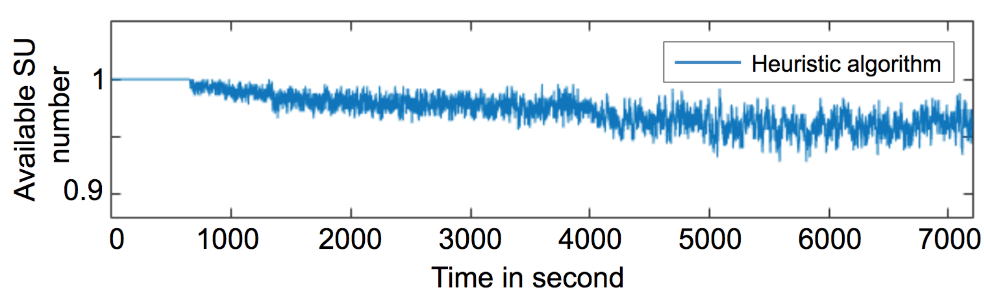

Figure 3.9: Changes of available SU number in heuristic algorithm across time.

detection algorithm, which divides available sensing time of each SU uniformly into small time chunks of 50 ms in length. Each time chunk is assigned to monitor a random frequency band and the algorithm is not able to learn from history.

First, we show an unknown PU pattern coverage comparison over optimal assignments, SU location based heuristic algorithm and the random detection method. The coverage represents the method's capability of capturing new patterns. This unknown pattern coverage is defined as:

$$UPcoverage = \frac{DetectedUnknownPatternNumber}{TotalUnknownPatternNumber} \tag{3.16}$$

As in Figure 3.10, the output of random detection method is barely 25% percent of the output of our heuristic algorithm. This is because our heuristic algorithm can learn from history to assign the limited SU monitoring time on the most likely frequency and time of PU occurrence. There is still a gap between our heuristic algorithm and the ideal optimal assignments since the optimal assignment unrealistically assumes known future, while the heuristic algorithm is designed with uncertain future.

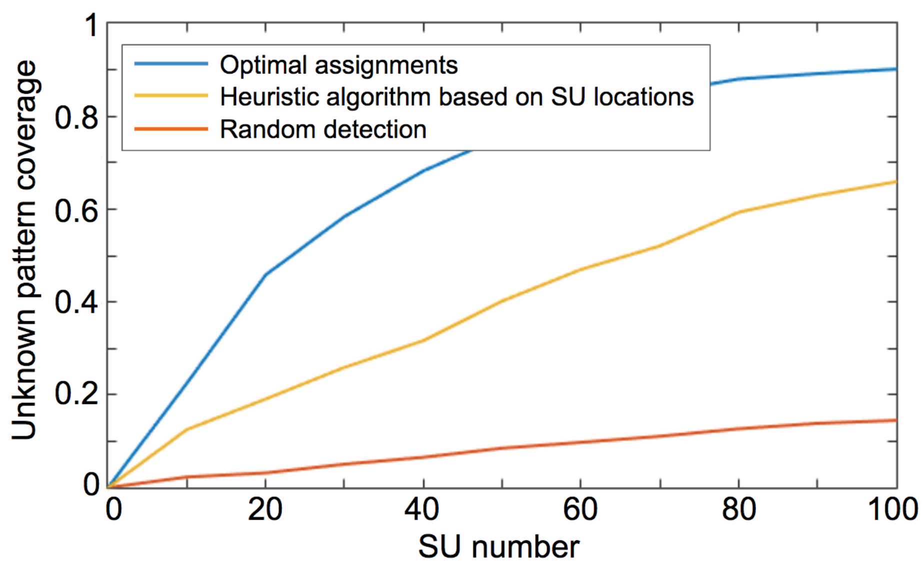

Figure 3.10: Unknown pattern coverage comparison. Blue line: Optimal assignments. Yellow line: Heuristic algorithm based on SU location. Red line: Random detection.

Since unknown PU pattern monitoring consumes energy, it may affect future energy budget for existing pattern monitoring. Thus, we compare existing pattern coverage of our heuristic algorithm with and without the unknown pattern monitoring part. Figure 3.11 shows the results. There is indeed a small coverage drop after adding unknown pattern monitoring. However, we believe that this small drop in existing pattern coverage is worthy to ensure our system can detect dynamic PU patterns as well as mobile PUs.

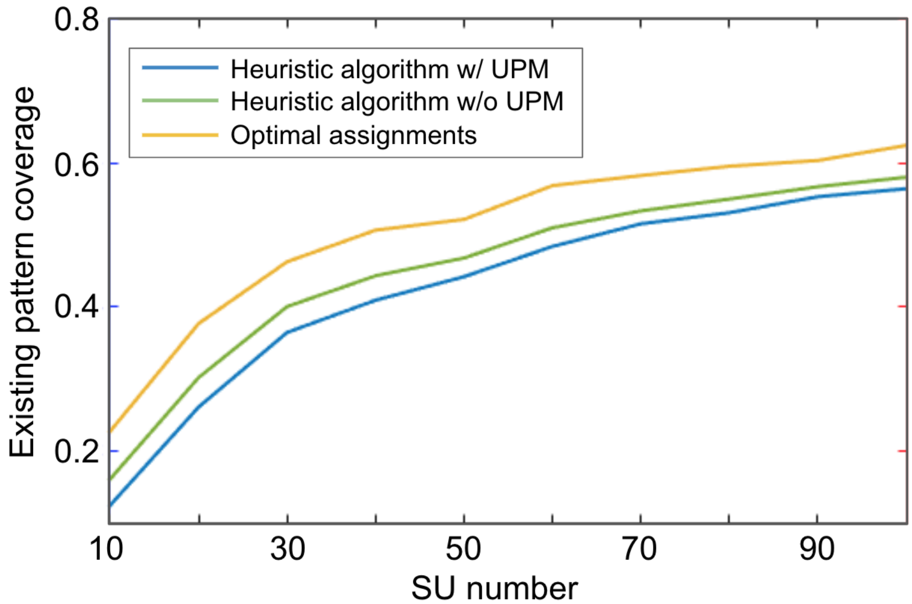

Figure 3.11: A comparison showing how the unknown pattern monitoring (UPM) affects existing PU pattern coverage.

3.6 Chapter Summary

Efficient and low-cost spectrum monitoring is one of the important methods to capture the spectrum utilization. To improve efficiency and reduce the computational overhead of the central controller, this chapter presents a novel crowdsourcing based spectrum monitoring system, which can intelligently schedule the monitoring tasks for masses of portable mobile devices, by leveraging the PU occupancy patterns. We propose novel scheduling algorithms based on practical spectrum usage data for existing pattern monitoring and unknown pattern monitoring. Simulation results show that our system achieves a high spectrum monitoring coverage. Our system is also capable of running efficiently even when no historical spectrum information is available.

Chapter 4

Preserving Incumbent User's Location Privacy Against Environmental Sensing Capability

Due to large amount of data exchange during the centralized sensing process, privacy issues of IUs become big concerns. According to CBRS OPSEC requirements, the protection provided by current ESC-based systems is not enough for highly sensitive IU operation data, since ESC may also be compromised. Specifically, IU location information is often highly sensitive and hence it is preferable to hide its true location under the detection of ESCs. In this chapter, we design novel schemes to preserve both static and moving IU's location information by adjusting IU's radiation pattern and transmit power. Firstly, IU privacy protection problem is formulated 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.

4.1 Introduction

In DSA, ESC systems are implemented to detect the IU activities for protecting them from 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 chapter, we address the IU location privacy 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 work is organized as follows. Section 4.2 introduces the general system models for static IU and moving IU. Section 4.3 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 4.4. Experimental results are reported in Section 4.5.

4.2 General System Model

4.2.1 Attack Model

The general attack model for IU privacy in 3.5GHz is illustrated in Figure 4.1. 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.

4.2.2 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.

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

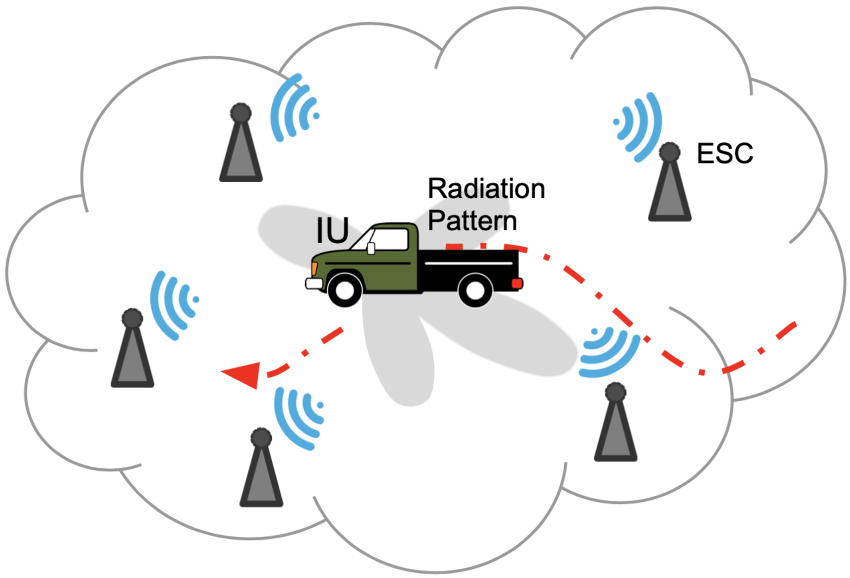

Figure 4.1: General system model.

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 chapter, 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 [78]:

$$g(\theta, \boldsymbol{\omega}) = \sum_{i=1}^{N_{ant}} \omega_i \exp[j\frac{2\pi}{\lambda} R \cos(\theta - \phi_i)] \tag{4.1}$$

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:

$$\boldsymbol{h_k} = \begin{bmatrix} exp[j\frac{2\pi}{\lambda}Rcos(\theta_k - \phi_1)] \\ exp[j\frac{2\pi}{\lambda}Rcos(\theta_k - \phi_2)] \\ \vdots \\ exp[j\frac{2\pi}{\lambda}Rcos(\theta_k - \phi_{N_{ant}})] \end{bmatrix} \tag{4.2}$$

Circular antenna array is used in this work as an example for problem illustration because it can produce flexible asymmetric radiation patterns and easily deflect a beam through 2π [61]. However, our analysis is not restricted to any specific antenna model. We can plug different antenna models into the analysis by replacing Equation (4.1) with their corresponding radiation functions. For example, Dolph-Tschebyscheff array antenna can use radiation pattern function:

$$\begin{cases} g(\theta, \boldsymbol{\omega}) = \sum_{i=1}^{N_{ant}/2} \omega_i cos[(2n-1)u], \\ \quad when\ N_{ant}\ is\ even \\ g(\theta, \boldsymbol{\omega}) = \sum_{i=0}^{(N_{ant}-1)/2} \omega_i cos[2nu], \\ \quad when\ N_{ant}\ is\ odd \\ \quad u = \frac{\pi}{\lambda} d \cos(\theta/2) \end{cases} \tag{4.3}$$

to replace Equation (4.1).

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

$$g(\theta, \boldsymbol{\omega_\theta}) = \sum_{i=1}^{N_{ant}} \omega_{\theta,i} \cdot I(\theta) \tag{4.4}$$

to replace Equation (4.1). 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:

$$I(\theta) = \begin{cases} 1, if\ \phi_j \leq \theta \leq \phi_{j+1}, \exists j \in [1, \cdots, M-1] \\ 0, otherwise \end{cases} \tag{4.5}$$

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}).

4.2.3 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 work 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 [79] is:

$$P_D \approx 0.5 \times erfc(\sqrt{-lnP_{fa}} - \sqrt{SNR + 0.5}) \tag{4.6}$$

Considering both noise and interference, the radar's signal-to-interference-noise ratio SINR can be computed as [80]:

$$SINR = \frac{P_S}{(1 + 10^{\frac{INR}{10}}) \times P_N} \tag{4.7}$$

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 [81].

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 chapter, 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.

4.3 Location privacy protection for Static IU

A simple model for preserving static IU's location privacy is presented in Figure 4.2, 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.

4.3.1 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.

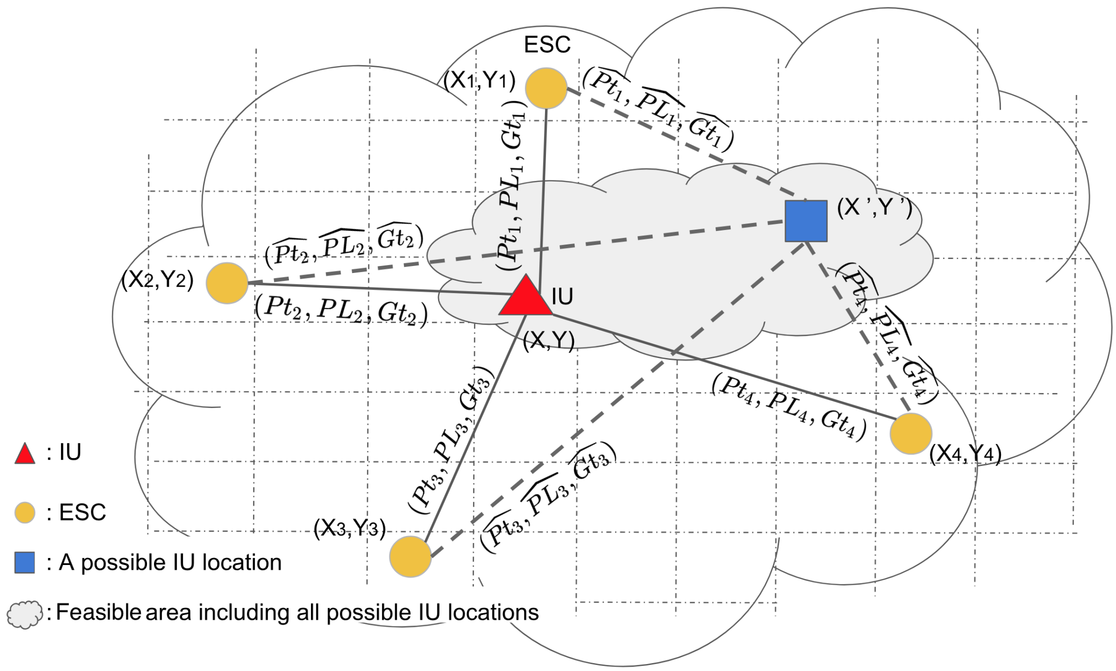

Figure 4.2: Model for static IU.

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 4.2, the space is segmented into grids to simplify the procedure of contouring the possible location area. Each grid is represented by its center position.

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 4.1, where Z is the set of of the possible locations of the IU.

Table 4.1: Procedure for adversary

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:

$$\widehat{Pr}_{i,k}(\widehat{\boldsymbol{\omega}}, \widehat{Pt}) = \widehat{Pt}_i + \widehat{Gt}_{i,k}(\widehat{\boldsymbol{\omega}}) - PL_{i,k} + Gr - Lr \tag{4.8}$$

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:

$$\widehat{Gt}_{i,k}(\widehat{\boldsymbol{\omega}}) = 10log_{10} \left| g(\theta_{i,k}, \widehat{\boldsymbol{\omega}}) \right|^2 \tag{4.9}$$

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

In Equation (4.8), the expected path loss $PL_{i,k}$ from the center of l_i to the k_{th} ESC is expressed as:

$$PL_{i,k} = 20log_{10}(\frac{4\pi}{\lambda}) + 10nlog_{10}(d_{i,k}) \tag{4.10}$$

where n is the path loss exponent, which is set to $n = 2$ in this work. $d_{i,k}$ 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 (4.10) 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.

From IU's perspective

Besides preserving its location privacy, an IU first needs to complete its tasks (e.g. object-tracking in this work), 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 4.2. In Table 4.2, 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 4.2: Procedure for IU

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 4.2 is NP-hard in general.

Proof: See Appendix A.1.

4.3.2 Approximation Algorithm and Worst Case

Approximation Algorithm

Since the problem of preserving static IU's location privacy formulated in Table 4.2 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 A.1, 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 4.2 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 4.2, 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 4.2.

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 (4.7), $SINR \propto P_S$, $P_S \propto P_t + G_{target}(\boldsymbol{\omega}) + A$, where A denotes all the other constant parameters. Based on Equation (4.1), (4.3) and (4.4), 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 (4.8), $\widehat{Pr}$ 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:

$$min\_\widehat{Pr}_{i,k} - \delta \leq Pr_k(\boldsymbol{\omega}_{n_1}, Pt_{n_2}) \leq max\_\widehat{Pr}_{i,k} + \delta \tag{4.11}$$

$\forall k = 1, 2, \cdots, K$. 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.: $\forall k = 1, 2, \cdots, K$

$$\widehat{Pr}_{i,k}(\widehat{\boldsymbol{\omega}}, \widehat{Pt}) - \delta \leq Pr_k(\boldsymbol{\omega}_{n_1}, Pt_{n_2}) \leq \widehat{Pr}_{i,k}(\widehat{\boldsymbol{\omega}}, \widehat{Pt}) + \delta \tag{4.12}$$

Based on the discussion above, we design a brute-force algorithm in Table 4.3 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 (4.11) 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 4.3: Heuristic algorithm

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

Worst case

Table 4.3'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 4.3 deviates the furthest in its computation results from the algorithm in Table 4.2. This happens when all discrete samples of U_i in Table 4.3 cannot satisfy the constraints, while feasible setting of parameters do exist between sample intervals for algorithm in Table 4.2. 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 4.3. 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 4.2, 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 4.3. 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:

$$\begin{cases} Pr_k(\boldsymbol{\omega}_{n_1}, Pt_{n_2}) < min\_\widehat{Pr}_{i,k} - \delta \\ or \\ Pr_k(\boldsymbol{\omega}_{n_1}, Pt_{n_2}) > max\_\widehat{Pr}_{i,k} + \delta \\ \forall n_1, m_1 \in [1, N_1],\ \forall n_2, m_2 \in [1, M_1] \\ min\_\widehat{Pr}_{i,k} - \delta \le Pr_k(\boldsymbol{\omega}_{n_1} + \Delta\boldsymbol{\omega}, Pt_{n_2} + \Delta p) \le \\ max\_\widehat{Pr}_{i,k} + \delta, \exists n_1 \in [1, N_1],\ n_2, \in [1, N_2] \\ 0 \le \Delta p \le \Delta p_{max}; 0 \le \Delta\boldsymbol{\omega} \le \Delta\omega_{max} \end{cases} \tag{4.13}$$

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 4.3, then there does not exist any other U_j in their sample interval that can satisfy constraint 1 in Table 4.2.

To find the $\Delta\boldsymbol{\omega}, \Delta p$ that can solve inequalities (4.13), 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. $f_{min} \leq f_{max} < min\_\widehat{Pr}_{i,k} - \delta$: since we cannot find any $f_{U_i}(\Delta\boldsymbol{\omega}, \Delta p)$ between f_{max} and f_{min} that satisfies $min\_\widehat{Pr}_{i,k} - \delta \leq f_0 \leq max\_\widehat{Pr}_{i,k} + \delta$, the inequalities are infeasible.

2. $f_{max} \geq f_{min} > max\_\widehat{Pr}_{i,k} + \delta$: same as above.

3. $f_{max} > max\_\widehat{Pr}_{i,k} + \delta$ and $f_{min} < min\_\widehat{Pr}_{i,k} - \delta$: 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 $min\_\widehat{Pr}_{i,k} - \delta \leq f_{U_i}(\Delta\boldsymbol{\omega}, \Delta p) \leq max\_\widehat{Pr}_{i,k} + \delta$. 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 $\boldsymbol{\omega}_{\boldsymbol{n_1}}$,$Pt_{n_2}$ and $\widehat{\boldsymbol{\omega}}_{m_1}, \widehat{Pt}_{m_2}$. Otherwise, it does not.

4.4 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.

4.4.1 Location Privacy Model for Moving IUs

Model for moving IU is the same as in Figure 4.2 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 4.3'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 4.4 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 4.3 shows how adversaries generate possible area for a moving IU using the algorithm in Table 4.4. The procedure can be divided into three steps: (1) Step 1: Based on Table 4.1, 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, $j \in [1, n]$.

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

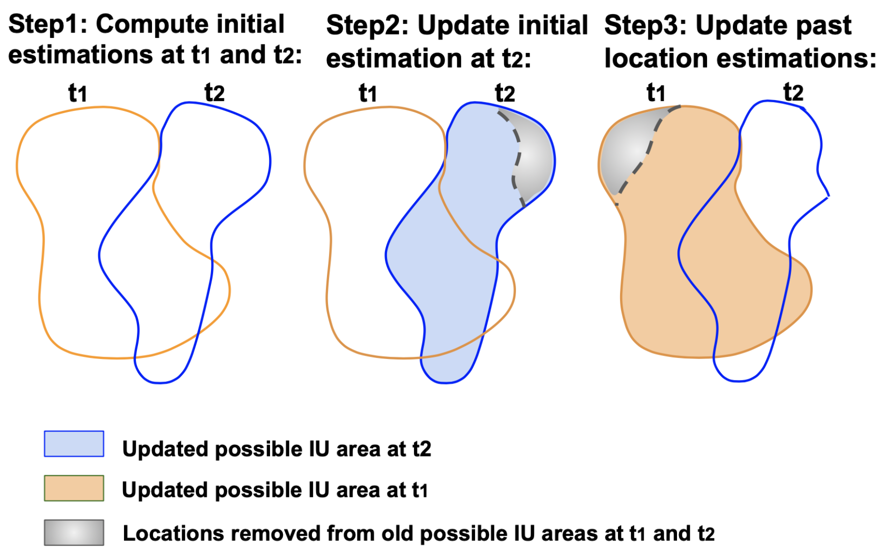

Figure 4.3: An example showing how adversary generates possible areas for moving IU.

Table 4.4: Procedure for adversary to generate possible areas for moving IU

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 4.1 in Section 4.3.
Step 2: /* update current Z_n by Z_{n-1} */
$Z_n = \{l_i \mid l_i \in Z_n$ and $\exists l_j \in Z_{n-1}$ such that $\lvert l_i - l_j \rvert \leq \Delta\}$
Step 3: /* Update past location trajectory based on Z_n*/
From $t_j = t_{n-1}$ to $t_j = t_1$:
$Z_j = \{l_k \mid l_k \in Z_j$ and $\exists l_u \in Z_{j+1}$ such that $\lvert l_k - l_u \rvert \leq \Delta\}$

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.

4.4.2 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:

$$opt\boldsymbol{\omega}_j, optPt_{j,j\in[1,n]} = \underset{\boldsymbol{\omega}_j, Pt_j, j\in[1,n]}{\arg\min} \sum_{j=1}^{n} \frac{1}{size(Z_j(\boldsymbol{\omega}_j, Pt_j))} \tag{4.14}$$

The algorithm in Table 4.5 compute the above Equation (4.14). Here, we assume the adversary will use the algorithm in Table 4.4 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.

4.4.3 Conceal IU's Real-time Location

Consider that an adversary is using the algorithm in Table 4.4 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:

$$opt\boldsymbol{\omega}_n, optPt_n = \underset{\boldsymbol{\omega}_n, Pt_n}{\arg\min} \frac{1}{size(Z_n(\boldsymbol{\omega}_n, Pt_n))} \tag{4.15}$$

An algorithm similar to the one in Section 4.4.2 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 (4.15) instead of Equation (4.14).

Table 4.5: Procedure for IU to maximize the number of possible traces

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 4.3 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 $\widetilde{Z}_i = \{Z_i(\boldsymbol{\omega}_{n_1}, Pt_{n_2})\vert \text{ for all } (\boldsymbol{\omega}_{n_1}, Pt_{n_2})\}$
Step 3: For every possible sequence of IU parameter tuning, which is denoted as $s = \{(\omega_{n_1}, Pt_{n_2})_i \vert i = 1...n\}$, retrieve the corresponding sequence of Z_i and narrow down these Z_i based on Step 2 and 3 in Table 4.4.
Step 4: Pick the best sequence S_{opt} that satisfies Equation (4.14) among all sequences.

4.5 Simulation Results

In this section, we simulate the static IU and the moving IU location privacy protection problem described in Section 4.3 and 4.4 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 4.4. 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 4.4, 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.

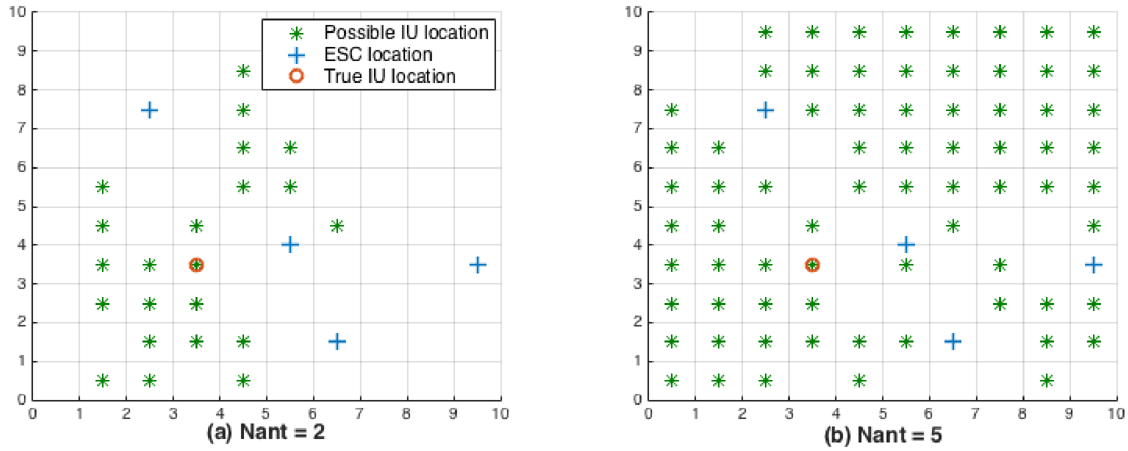

Figure 4.4: Examples showing maximized possible location area for static IU when $N_{ant} = 2$ and $N_{ant} = 5$.

In our simulation of mobile IUs, we set the speed of IU as between 0 to 2 (grid per time interval). Figure 4.5 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 4.6 (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.

The most dissimilar trace to the true IU route is presented in Figure 4.6 (b). Similarity between two traces is measured by:

$$dist = \sum_{t=t_1}^{t_n} \sqrt{(L1_t - L2_t)^2} \tag{4.16}$$

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 4.6, the existence of the possible traces that are far away from the true trace make preservation of moving IU's location privacy feasible.

Table 4.6 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

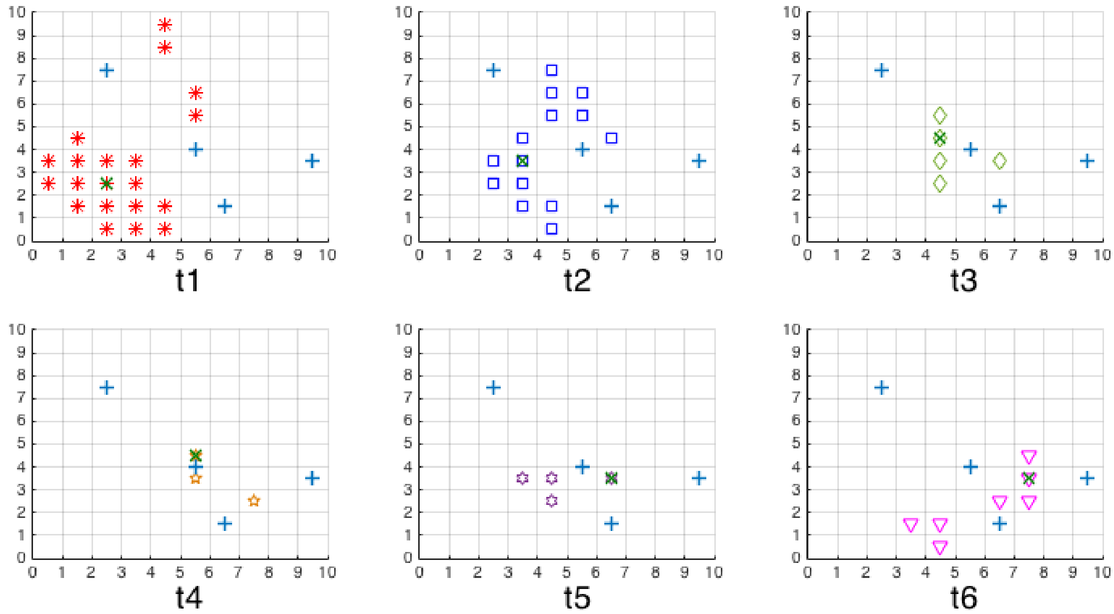

Figure 4.5: Maximal areas of possible IU locations at each point of time. The crosses in all sub-figures denote the true IU locations, the plus signs denote the ESC locations, and the other markers are computed possible IU locations.

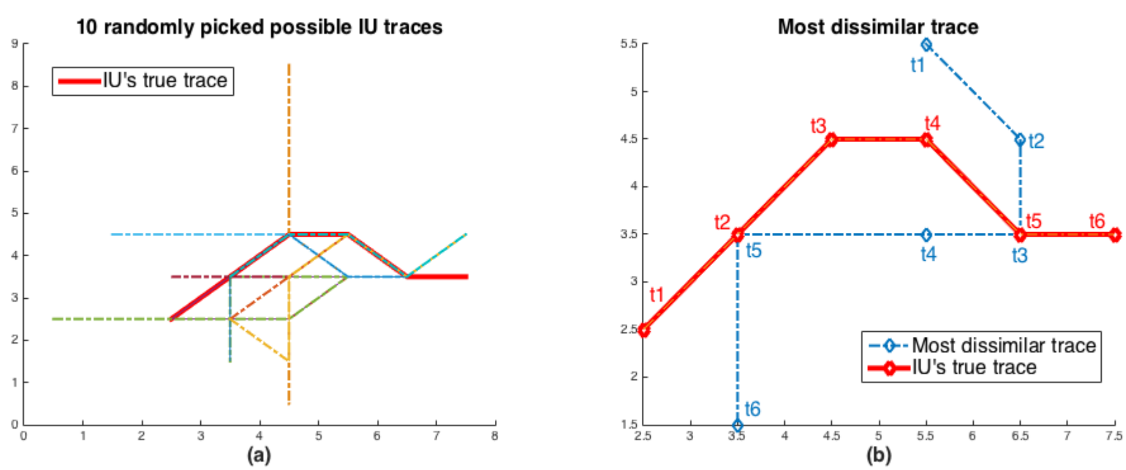

Figure 4.6: Sub-figure (a) shows 10 randomly picked possible IU traces in dash-dot lines and the IU's real route in a sold red line. Sub-figure (b) shows an example of the most dissimilar trace, $t_i, i \in [1, 6]$ denotes each time step.

computed by Equation (4.16). 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 $200m$.

Table 4.6: 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 4.7: Number of possible IU traces and current locations

<table>
<tr><th></th><th>δ</th><th>K</th><th>$N_{ant} = 2$</th><th>$N_{ant} = 5$</th></tr>
<tr><td rowspan="4">Possible IU traces</td><td rowspan="2">1 dB</td><td>4</td><td>40</td><td>6124905</td></tr>
<tr><td>6</td><td>14</td><td>4924908</td></tr>
<tr><td rowspan="2">2 dB</td><td>4</td><td>1389</td><td>10153583</td></tr>
<tr><td>6</td><td>186</td><td>9037580</td></tr>
<tr><td rowspan="4">Possible IU locations</td><td rowspan="2">1 dB</td><td>4</td><td>4</td><td>74</td></tr>
<tr><td>6</td><td>2</td><td>71</td></tr>
<tr><td rowspan="2">2 dB</td><td>4</td><td>12</td><td>89</td></tr>
<tr><td>6</td><td>8</td><td>86</td></tr>
</table>

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 the way. Three general trends in Table 4.7 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 4.2, and further reduce the l_i's probability of being regarded as a possible IU location.

4.6 Chapter Summary

Since IUs in the 3.5 GHz band are mostly military systems such as US naval radars, whose location privacy is highly sensitive, it is preferable to hide IU's true location under the detection of ESCs. In this chapter, 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.

Part III

Power Control Strategies in Distributed Dynamic Spectrum Access

Chapter 5

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

In this part, we focus on SU power control problem in distributed DSA. As mentioned previously, 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 for a system to ensure the QoS of both the IU and SUs while protecting IU operation security. In this chapter, we propose a novel distributed SU transmit power control algorithm to solve this challenge and achieve minimum energy consumption. Our scheme can enable SINR-guaranteed coexistence between SUs and IUs and protect IUs from harmful interference, while requiring no information directly from IUs. 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. Hence, we demonstrate that our algorithm satisfies the CBRS OPSEC requirements in 3.5 GHz band. Our scheme's convergence and stability properties, as well as its privacy-protection strength, are both theoretically analyzed and experimentally demonstrated through simulations.

5.1 Introduction

Due to the rapid growth in wireless communication demands, the frequency spectrum is becoming increasingly crowded. DSA is then proposed to enable the spectrum sharing between IUs and SUs in underutilized spectrum to mitigate the spectrum scarcity problem. This chapter 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 SAS and an ESC system [16]. 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 [22]. Centralized power control algorithms, such as those proposed in [82, 83], 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 [22, 23, 84], 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 chapter, 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 chapter, we will discuss our algorithm design using the following organization. Section 5.2 introduces the system model and the QoS requirements for SU and IU. Section 5.3 describes our power control algorithm for SUs to distributively adjust their transmit power. In Section 5.4, we demonstrate the convergence and stability properties of our algorithm under different conditions. Section 5.5 further shows how IU's interference requirement is statistically guaranteed. Section 5.6 analyzes that even when the ESC-supplied information is leaked, it is still difficult for adversaries to infer the true IU location. In Section 5.7, we present the evaluation of the proposed algorithm using simulations.

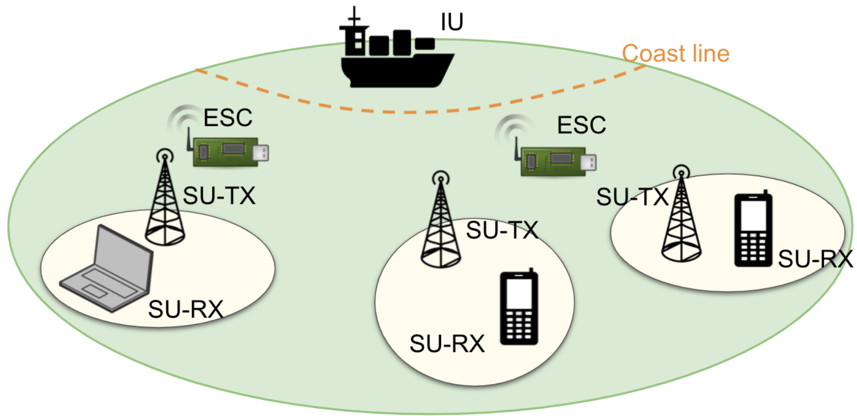

Figure 5.1: System model.

5.2 Problem Formulation

The system model in our algorithm is illustrated in Figure 5.1. 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 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:

$$\begin{cases} \frac{g_{ii}P_i}{\sum_{j \neq i} g_{ji}P_j + \varphi} - \tau_i = 0, i \in [1, n] & (a) \\ Prob(\sum_i g_{iI}P_i \leq T) \geq \chi & (b) \\ 0 \leq P_i \leq P_{max}, i \in [1, n] & (c), \end{cases} \tag{5.1}$$

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 (5.1) are straightforward, they are hard to guarantee directly. Due to privacy protection of IU's location information, g_{iI} in (5.1) 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 [18]. 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 5.5 for details). Hence, the constraint formulation in (5.1) is converted into:

$$\begin{cases} \frac{g_{ii}P_i}{\sum_{j\neq i} g_{ji}P_j+\varphi} - \tau_i = 0, i \in [1,n] \quad (a) \\ \sum_i g_{ie}P_i \leq T_e, e \in [i,m] \quad (b) \\ 0 \leq P_i \leq P_{max}, i \in [1,n] \quad (c), \end{cases} \tag{5.2}$$

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

Denote the set of SU power settings that satisfy (5.2) as the solution set $R := \{\mathbf{P}|\mathbf{P} \text{ satisfies } (5.2)\}$, 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 (5.2) does not exist (a.k.a. $R = \emptyset$), meaning that a power setting that satisfies all three constraints in (5.2) does not exist, our power control algorithm will converge to a stable point that guarantees IU's QoS requirement (5.2b), while the constraint (5.2a) 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.

5.3 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.

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

$$\omega_e = \frac{\xi_1(C_e - \xi_2 T_e)}{C_e}, \tag{5.3}$$

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 5.6. 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 5.5, 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 [85–87]. 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:

$$\Omega_e = f'(\omega_e) \cdot \lambda_e^2, \tag{5.4}$$
$$\Gamma_{min} = \min(-\omega_e), \tag{5.5}$$
$$\text{where } f(z) := \max(0, z). \tag{5.6}$$

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

$$\dot{\lambda}_e = \frac{d\lambda_e}{dt} = -\beta_e f(\omega_e) \cdot 2\lambda_e. \tag{5.7}$$

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

$$\lambda_e + \dot{\lambda}_e = \lambda_e - \beta_e f(\omega_e) \cdot 2\lambda_e > 0 \Rightarrow 0 < \beta_e < \frac{1}{2f(\omega_e)} \tag{5.8}$$

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:

$$\dot{P}_i = \frac{dP_i}{dt} = \dot{\widetilde{P}}_i + \sum_e g_{ie} \Omega_e \dot{\widetilde{P}}_i, \tag{5.9}$$
$$\text{where } \dot{\widetilde{P}}_i = \alpha_i \cdot \left(\frac{\tau_i}{SINR_i} - 1 \right) P_i, \tag{5.10}$$
$$\alpha_i = \alpha_i(\Gamma_{min}, g_{ie}, \Omega_e, SINR_i) \tag{5.11}$$

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 6.5.3. 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.

5.4 Convergence and Stability

To prove our algorithm's convergence, first note that theoretically, the aggregated SU interference at ESC e can be expressed as $C_e = \sum_i P_i g_{ie}$. Combining this with (5.3) (5.4) (5.7) (5.9) (5.10), the transmit power update algorithm at SU-TX i can be expressed as:

$$\dot{P}_i = \frac{dP_i}{dt} = \widetilde{\dot{P}}_i + \left[\sum_e f'(\sum_i P_i g_{ie} - \xi_2 T_e) g_{ie} \lambda_e^2\right] \widetilde{\dot{P}}_i, \tag{5.12}$$

$$\text{where } \widetilde{\dot{P}}_i = \alpha_i \left(\frac{\tau_i}{\frac{P_i g_{ii}}{\sum_{j \neq i} P_j g_{ji} + \varphi}} - 1 \right) P_i, \tag{5.13}$$

$$\dot{\lambda}_e = \frac{d\lambda_e}{dt} = -\beta_e f(\xi_1 \frac{\sum_i P_i g_{ie} - \xi_2 T_e}{\sum_i P_i g_{ie}}) \cdot 2\lambda_e. \tag{5.14}$$

According to (5.3) and (5.6), 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 we use $f'(\sum_i P_i g_{ie} - \xi_2 T_e)$ to represent $f'(\omega_e)$ in the following analysis. Essentially, in this section, we will examine the system's convergence to an SU transmit power allocation set $\widetilde{R}$ that is defined as $\widetilde{R} := \{\mathbf{P}|\mathbf{P}$ satisfies all the constraints in (5.15)$\}$:

$$\begin{cases} \frac{g_{ii} P_i}{\sum_{j \neq i} g_{ji} P_j + \varphi} - \tau_i = 0, i \in [1, n] \ (a) \\ \sum_i g_{ie} P_i \leq \xi_2 T_e, e \in [i, m] \ (b) \\ 0 \leq P_i \leq P_{max}, i \in [1, n] \ (c) \end{cases} \tag{5.15}$$

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 (5.15b).

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 (5.12) - (5.14) will never converge to a point that satisfies all the constraints in Equation (5.2) 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.

5.4.1 Part 1: Solution set $\widetilde{R}$ to (5.15) 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 (5.15), 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 (5.15)to get a new relaxed solution set $\widetilde{Z}$, such that all $\mathbf{P} \in \widetilde{Z}$ satisfies:

$$\begin{cases} \frac{g_{ii}P_i}{\sum_{j\neq i} g_{ji}P_j+\varphi} - \tau_i = 0, i \in [1,n] \ (a) \\ \sum_i g_{ie}P_i \leq \xi_2 T_e, e \in [i,m] \ (b) \\ P_i \geq 0, i \in [1,n]. \ (c) \end{cases} \tag{5.16}$$

   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.

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 1 demonstrates that our algorithm asymptotically converges to an invariant set $\widetilde{Z}$. Theorem 2 states that our algorithm will stabilize at a unique equilibrium point in $\widetilde{Z}$.

Theorem 1. *Starting from any initial state $P_i(0) > 0$, the system described in (5.12) to (5.14) 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:

$$\begin{cases} \dot{\widetilde{P_i}} = \alpha_i \left(\dfrac{\tau_i}{\frac{P_i^* g_{ii}}{\sum_{j\neq i} P_j^* g_{ji} + \varphi}} - 1 \right) P_i^* = 0 & (5.17a) \\ \dot{\lambda}_e = -\beta_e f(\xi_1 \dfrac{\sum_i P_i^* g_{ie} - \xi_2 T_e}{\sum_i P_i^* g_{ie}}) \cdot 2\lambda_e = 0 & (5.17b) \end{cases}$$

Since $\lambda_e > 0$ and $P_i g_{ie} - T_e \neq 0$, from (5.17b), it is clear that $f(\sum_i P_i^* g_{ie} - T_e) = 0$, which, based on $f(\cdot)$ definition in (5.6), means $\sum_i P_i^* g_{ie} - T_e < 0$. Based on (5.13), 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, (5.17a) and (5.17b) can be converted to:

$$\begin{cases} \frac{\tau_i}{\frac{g_{ii} P_i^*}{\sum_{j\neq i} g_{ji} P_j^* + \varphi}} = 1, \forall i \in [1,n] \\ \sum_i P_i^* g_{ie} \leq \xi_2 T_e, \forall e \in [1,m] \end{cases} \tag{5.18}$$

Clearly, (5.18) 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 (5.13), $\dot{\widetilde{P_i}}$ can be rewritten as:

$$\dot{\widetilde{P_i}} = \alpha \left(\frac{\tau_i}{g_{ii}} \sum_{j\neq i} g_{ji} P_j - P_i \right) + \alpha \frac{\tau_i}{g_{ii}} \varphi = \boldsymbol{A}\boldsymbol{P} + \boldsymbol{b}, \tag{5.19}$$

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 1 and 2 from existing literature [21, 88, 89].

Lemma 1. *: 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 [88].*

Lemma 2. *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 [89].*

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 (5.19), $\boldsymbol{AP}^* = -\boldsymbol{b}$. According to Lemma 1, all the eigenvalues of $\boldsymbol{A}$ have negative real parts. Thus, we can apply Lemma 2 and find a positive definite matrix $\boldsymbol{M}$ that solves $\boldsymbol{A}^\top \boldsymbol{M} + \boldsymbol{MA} = -\boldsymbol{Q}$ given any $\boldsymbol{Q} = \boldsymbol{Q}^\top > 0$. Hence, we can construct a Lyapunov function $V(\boldsymbol{P})$ for $\dot{\widetilde{P}}_i$ as

$$V(\boldsymbol{P}) := (\boldsymbol{P} - \boldsymbol{P}^*)^\top \boldsymbol{M}(\boldsymbol{P} - \boldsymbol{P}^*) \geq 0 \tag{5.20}$$

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

$$\dot{V}(\boldsymbol{P}) = \sum_i \frac{\partial V(\boldsymbol{P})}{\partial P_i} \dot{\widetilde{P}}_i = -(\boldsymbol{P} - \boldsymbol{P}^*)^\top \boldsymbol{Q}(\boldsymbol{P} - \boldsymbol{P}^*) \leq 0 \tag{5.21}$$

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 $\boldsymbol{Q} = \boldsymbol{H}^\top \boldsymbol{DH}$, 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:

$$\dot{V}(\boldsymbol{P}) = \sum_i \frac{\partial V(\boldsymbol{P})}{\partial P_i} \dot{\widetilde{P}}_i = \sum_i \delta_i {y_i}^2 \tag{5.22}$$

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

$$K(\boldsymbol{\lambda}, \boldsymbol{P}) := F(\boldsymbol{\lambda}, \boldsymbol{P}) - F(\boldsymbol{\lambda}^*, \boldsymbol{P}^*), \tag{5.23}$$

$$\text{where } F(\boldsymbol{\lambda}, \boldsymbol{P}) := \sum_e f\Big(W(\boldsymbol{P}) \sum_i g_{ie} - \xi_2 T_e\Big) {\lambda_e}^2, \tag{5.24}$$

$$W(\boldsymbol{P}) := V(\boldsymbol{P}) + \epsilon. \tag{5.25}$$

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:

$$W(\boldsymbol{P}) \sum_i g_{ie} - \xi_2 T_e = (V(\boldsymbol{P}) + \epsilon) \sum_i g_{ie} - \xi_2 T_e > 0. \tag{5.26}$$

Note this is possible because $V(\boldsymbol{P})$ is a definite positive function. Theorem 5 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

$$\begin{cases} P_i = P_i^* = \frac{\tau_i}{g_{ii}} \left(\sum_{j\neq i} g_{ji} {P_j}^* + \varphi\right), \forall i \in [1, n] \\ \sum_i P_i g_{ie} - \xi_2 T_e \leq 0, \forall e \in [i, m]. \end{cases} \tag{5.27}$$

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

Theorem 2. *$\widetilde{Z}$ 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 (5.19) can be assumed to be sufficiently random according to [21]. 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 1 and Theorem 2, we now can conclude that the system asymptotically converges to a unique equilibrium in $\widetilde{Z}$ when $\widetilde{Z} \neq \emptyset$.

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 $\boldsymbol{P}^* \in \widetilde{R}$.

5.4.2 Part 2: Solution set $\widetilde{R}$ to (5.15) 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 (5.12) - (5.14) 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.

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 $\sum_{i\in[1,n]} P_i^* g_{ie} \leq \xi_2 T_e, e \in [1,m]$ 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.

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 $\sum_i P_i^* g_{ie} \leq \xi_2 T_e, e \in [1,m]$.

This can be achieved by a step size control procedure that computes the feasible step size α_i in (5.9). The procedure need to ensure that the ESC's interference at any iteration to be smaller than its threshold T_e by enforcing :

$$\sum_{i\in[1,n]} (P_i + \dot{P}_i) g_{ie} < T_e, e \in [1,m] \tag{5.28}$$

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 (5.3) - (5.9), (5.28) can be rewritten as:

$$C_e + \sum_i \alpha_i (\frac{\tau_i}{SINR_i} - 1)(1 + \sum_e \Omega_e g_{ie}) P_i g_{ie} < T_e \tag{5.29}$$

To guarantee (5.29), we set α_i to make the following inequality hold $\forall i \in [1,n]$:

$$\alpha_i (\frac{\tau_i}{SINR_i} - 1)(1 + \sum_e \Omega_e g_{ie}) < \Gamma_{min}, \tag{5.30}$$

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.

5.5 ESC interference requirements

As discussed in Section 5.2, 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 (5.1) cannot be solved directly. Therefore, we estimate the interference from SU-TX to ESC instead and create problem formulation (5.2). In Section 5.4, we have proved that our algorithm asymptotically stabilize at an equilibrium that solves the problem in (5.2). 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 (5.2) is approximately also a solution to the problem in (5.1).

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:

$$U(\mathbf{T_E}) := Pr(I \leq T | C_e \leq T_e, \text{for all } e \in [1, m]) \geq \Psi \tag{5.31}$$

where the constant threshold $\Psi \in [0, 1]$ and $\Psi \approx 1$. The left side of (5.31), 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 5.5.1. In Section 5.5.2, we model the conditional statistical distribution of I, given ESC's local RSS of IU. Next, Section 5.5.3 solves (5.31) as a cumulative density function of a conditional normal distribution, and use this function to identify T_E that guarantees $U(\mathbf{T_E}) \geq \Psi$.

5.5.1 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:

$$Prob(g_{ie} \leq g) = 1 - Pr(d_{ie} \leq (\frac{g}{\eta})^{-\frac{1}{\upsilon}}) \tag{5.32}$$

$$\rho_{G_e}(g) = \frac{\partial Prob(g_{ie} \leq g)}{\partial g} = \frac{\eta^{\frac{1}{\upsilon}}}{\upsilon} g^{-\frac{1+\upsilon}{\upsilon}} \rho_{D_e}((\frac{g}{\eta})^{-\frac{1}{\upsilon}}) \tag{5.33}$$

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

$$\mu_e = \int_{\eta l^{-\upsilon}}^{\eta \epsilon_1^{-\upsilon}} \frac{2\eta^{\frac{2}{\upsilon}} g^{-\frac{2}{\upsilon}}}{\upsilon l^2} \mathrm{d}g, \quad \sigma_e^2 = \int_{\eta l^{-\upsilon}}^{\eta \epsilon_1^{-\upsilon}} (g - \mu_e)^2 \frac{2\eta^{\frac{2}{\upsilon}} g^{-\frac{2+\upsilon}{\upsilon}}}{\upsilon l^2} \mathrm{d}g \tag{5.34}$$

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

$$\hat{\mu}_e = \sum_{i=1}^{n} P_i \mu_e, \quad \hat{\sigma}_e^2 = \sum_{i=1}^{n} (P_i)^2 \sigma_e^2. \tag{5.35}$$

5.5.2 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 $\Xi_{PR}(P_r) = 1 - \exp(-\frac{P_r}{2r_e^2})$, where r_e^2 is the expectation of P_r, which can be measured by ESC sensor e. Therefore, the CDF of g_0 can be derived by:

$$\Xi_{G_0}(g_0) = 1 - \exp(-\frac{g_0 P_t}{2r_e^2}). \tag{5.36}$$

The CDF of d_0 is then computed by:

$$\Xi_{D_0}(d_0) = \exp(-\frac{\eta d_0^{-\upsilon} P_t}{2r_e^2}), \tag{5.37}$$

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

$$\rho_{D_0}(d_0) = \exp(-\frac{P_t \eta d_0^{-\upsilon}}{2r_e^2})\frac{\upsilon P_t \eta}{2r_e^2} d_0^{-\upsilon-1}. \tag{5.38}$$

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:

$$\rho_{D_I|D_0}(d_{iI}|d_0) = \begin{cases} \frac{2d_{iI}}{l^2}, & 0 \le d_{iI} \le l - d_0 \\ \frac{2d_{iI}}{\pi l^2} \arccos(\frac{d_0^2 + d_{iI}^2 - l^2}{2d_0 d_{iI}}), & l - d_0 < d_{iI} \le l + d_0. \end{cases} \tag{5.39}$$

Thus, combining (5.39) with (5.38), $\rho_{D_I}(d_{iI})$ can be computed by:

$$\rho_{D_I}(d_{iI}) = \begin{cases} \int_0^{l-d_{iI}} \frac{2d_{iI}}{l^2} \exp(-\frac{P_t \eta d_0^{-\upsilon}}{2r_e^2}) \cdot \quad \frac{\upsilon P_t \eta}{2r_e^2} d_0^{-\upsilon-1} \mathrm{d}d_0, \\ \qquad 0 \le d_{iI} \le l \\ \int_{d_{iI}-l}^{l} \frac{2d_{iI}}{\pi l^2} \arccos(\frac{d_0^2 + d_{iI}^2 - l^2}{2d_0 d_{iI}}) \cdot \quad \exp(-\frac{P_t \eta d_0^{-\upsilon}}{2r_e^2}) \\ \frac{\upsilon P_t \eta}{2r_e^2} d_0^{-\upsilon-1} \mathrm{d}d_0, \qquad l < d_{iI} \le 2l \end{cases} \tag{5.40}$$

The relation between d_{iI} and g_{iI} is the same as the relation between d_{ie} and g_{ie} in (5.33), the expectation μ_I and variance σ_I^2 of g_{iI} can be computed by:

$$\mu_I = \int_g \int_{d_0} \frac{\eta^{\frac{1}{\upsilon}}}{\upsilon} g^{-\frac{1}{\upsilon}} \rho_{D_I}((\frac{g}{\eta})^{-\frac{1}{\upsilon}}) \mathrm{d}d_0 \mathrm{d}g \tag{5.41}$$

$$\sigma_I^2 = \int_g \int_{d_0} \frac{(g - \mu_I)^2 \eta^{\frac{1}{\upsilon}}}{\upsilon} g^{-\frac{1+\upsilon}{\upsilon}} \rho_{D_I}((\frac{g}{\eta})^{-\frac{1}{\upsilon}}) \mathrm{d}d_0 \mathrm{d}g, \tag{5.42}$$

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

$$\hat{\mu}_I = \sum_{i=1}^n P_i \mu_I, \quad \hat{\sigma}_I^2 = \sum_{i=1}^n (P_i)^2 \sigma_I^2. \tag{5.43}$$

5.5.3 Determine ESCs' interference constraints

As discussed in Section 5.5.1 and 5.5.2,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 (5.31), which can be rewritten to:

$$U(\mathbf{T_E}) = Pr\big(\sum_{i\in[1,n]} P_i g_{iI} \leq T \big| \sum_{i\in[1,n]} P_i g_{ie} \leq T_e, \text{for all } e \in [1,m]\big) \geq \Psi. \quad (5.44)$$

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

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

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

$$Pr\left(I \leq T \,|C_e = T_e\right) \geq \Psi, \quad (5.45)$$

we know (5.44) must hold, which means IU's interference requirement is statistically satisfied.

According to the theory of conditional normal distribution [90], the conditional random variable $I|C_e = T_e$ is normally distributed, whose $\hat{\mu}_{Ie}$ and variance $\hat{\sigma}_{Ie}$ are:

$$\hat{\mu}_{Ie} = \hat{\mu}_I + \frac{\Sigma_{12}}{\Sigma_{22}}(T_e - \hat{\mu}_e), \quad (5.46)$$

$$\hat{\sigma}_{Ie} = \Sigma_{11} - \frac{\Sigma_{12}^2}{\Sigma_{22}}, \quad (5.47)$$

$$\text{where } \Sigma_{11} = cov(I, I), \Sigma_{12} = cov(I, C_e), \quad (5.48)$$

$$\Sigma_{22} = cov(C_e, C_e), \quad (5.49)$$

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

$$\mu_0 = T - \hat{\sigma}_{Ie}\Phi^{-1}(\Psi), \quad (5.50)$$

where $\Phi^{-1}(\cdot)$ is the quantile function of standard normal distribution. Then, based on (5.46), T_e can be computed by

$$T_e = (\mu_0 - \hat{\mu}_I)\frac{\Sigma_{22}}{\Sigma_{12}} + \hat{\mu}_e. \quad (5.51)$$

(5.51) is the formula that each ESC e uses to generate T_e independently as its interference requirement. Bring this T_e into (5.3), the IU's interference requirement is statistically guaranteed.

5.6 Analysis on IU privacy protection

In this section, we demonstrate that our algorithm is secure in the sense that, even if every message exchanged in the system is leaked, the location of incumbent activity still cannot be accurately estimated. Through this analysis on IU location privacy protection, we demonstrate that our power control algorithm meets the requirements for CBRS OPSEC.

The security threat model for the overall ESC/SAS is described in [91] including compromised CBSD, compromised SAS operator and compromised ESC operator, etc. WINNF document [66] gives a general threat model under consideration for CBRS OPSEC: "The threat model under consideration for CBRS OPSEC is where an Internet-connected device is able to probe the Spectrum Access Server (SAS) ecosystem through spectrum access queries and as a result learn information about military operations at a higher level of fidelity than can be reliably discovered from other Internet-connected sources such as news reports about naval activity."

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. Thus, in the threat model for our power control system, we assume ESCs are trustworthy so an adversary cannot know its raw measurement of IU RSS. However, an Internet-connected adversary can also probe the SAS to obtain the IU-related parameters. It is also possible for the adversary to eavesdrop the communication channel if he is somewhere near the SU network. The attacker will attempt to derive sensitive IU location data from information that they observed.

According to (5.3) - (5.11) and Section 5.5, 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 (5.3). 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 [92]. 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 [92]. 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 5.7.3, 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.

5.7 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 $20m/s$. Figure 5.2 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 $0.0001W$.

5.7.1 Stability analysis

The evaluation first examines the stability of our algorithm under different cases discussed in Section 5.4. We denote the case where solution set $\widetilde{R}$ to (5.15) 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 5.1. 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 5.2 and 5.3. In Table 5.2, 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.

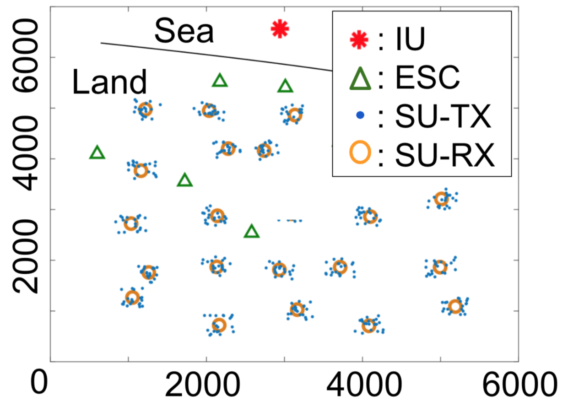

Figure 5.2: Example of our simulation settings.

Table 5.1: Parameter settings for Case 1, 2 and 3

Parameter	Case 1	2	3
number of SU BSs	9	16	25
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}

Case 1: Solution set $\widetilde{R}$ to (5.15) 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 5.3, 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.

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 5.1, 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 will not get its SINR satisfied despite its SU-TX using maximum transmit power, while other SU-RXs can maintain their SINR. Table 5.3's simulation results exactly match this expectation. In addition, Table 5.3

Table 5.2: 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 5.3: Simulation results for Case 1, 2 and 3 in Scenario 1 and 2

<table>
<tr><th></th><th></th><th>Fraction of time transmit power < the maximum</th><th>Fraction of time when SU's SINR $\geq \tau$</th><th>Fraction of time when SU interference to IU $\leq T$</th></tr>
<tr><td rowspan="3">Scen-ario 1</td><td>Case 1</td><td>1</td><td>0.9784</td><td>1</td></tr>
<tr><td>Case 2</td><td>0.5260</td><td>0.5840</td><td>1</td></tr>
<tr><td>Case 3</td><td>1</td><td>0.0422</td><td>1</td></tr>
<tr><td rowspan="3">Scen-ario 2</td><td>Case 1</td><td>1</td><td>0.9771</td><td>1</td></tr>
<tr><td>Case 2</td><td>0.5423</td><td>0.6267</td><td>1</td></tr>
<tr><td>Case 3</td><td>1</td><td>0.0531</td><td>1</td></tr>
</table>

shows that our scheme still ensure the IU's interference level is below the threshold in this case.

Case 3: $\widetilde{Z}$ is empty

In the third simulation, as shown in Table 5.1, 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 5.4.2, 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 5.3. 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 5.2, 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.

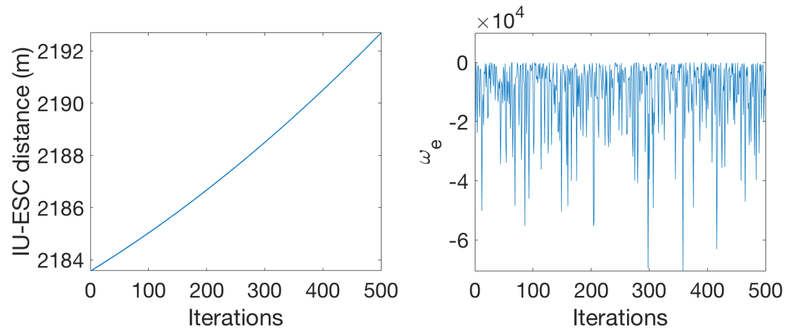

Figure 5.3: Left figure shows 500 iterations of one sequence of IU-ESC distances and right figure shows the corresponding ω_e sequence.

5.7.2 Efficiency evaluation

We compare our algorithm with the existing IU protection schemes [93, 94] in terms of network capacity under the same IU interference protection level. A geographic exclusion zone (GEZ) scheme in [93] calculates the minimum radius of the primary exclusion zone based on the primary outage constraint, and [94] 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.

5.7.3 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 5.3 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 [95], and the p-value is around 0.28 which is larger than 0.05 [92]. 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.

5.7.4 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 [57,58], 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.

5.8 Chapter Summary

Adaptive power control is a feasible way to enable successful coexistence between IUs and SUs. In this chapter, 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. To the best of our knowledge, our algorithm is the first power control algorithm that meets the CBRS OPSEC requirements in 3.5 GHz DSA. 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.

Chapter 6

Distributed and Secure Uplink Power Control in Dynamic Spectrum Access

Different from the previous chapter which presents an SU power control algorithm to achieve minimum power consumption, in this chapter, we develop another secure and distributed SU transmit power control algorithm aiming at optimal network utility in uplink. This algorithm enables optimal SU power control to maximize the sum of SU rates. The SINR-guaranteed coexistence between SUs and IUs are enabled to maintain effective communication, while no information is directly required from IUs. Local measurements of IU signals provided by ESCs also undergo a security masking process to ensure that IU location cannot be derived from its outputs. Convergence and stability properties of our algorithm, as well as its privacy-protection strength, are both theoretically analyzed and experimentally evaluated through simulations.

6.1 Introduction

Spectrum scarcity problem has been exacerbated due to the rapid growth in the demand for wireless communication. DSA has been proposed as a promising solution to mitigate the scarcity problem. The key form of the DSA recommended by NTIA [96] and FCC [97] is to share the licensed bands belonging to government incumbents with commercial wireless broadband devices. DSA systems deployed in 3.5 GHz band is one of the eminent DSA architectures. This architecture is composed of a SAS and an ESC system [6]. ESC system is a distributed network of sensors built to detect the IU's presence in 3.5 GHz band and inform SAS with its RSS of IU signals. SAS is responsible for granting and coordinating SUs' access to the spectrum based on the reported activities of both IUs and SUs. Specifically, SAS cannot allow any SU access the licensed channel unless it can be concluded from ESC-provided IU sensing results that no harmful interference to the IUs will be triggered by the SUs' transmission. Power control for secondary networks, thus, can be a feasible way to ensure an SU can obtain such transmission permission to coexist with IUs. in this chapter, we mainly focus on the uplink SU power control in 3.5 GHz DSA systems aiming at maximizing secondary network utility.

One crucial challenge of designing optimal power control schemes for the above DSA system is that some IU information (e.g. IU location information) required in making an optimal power allocation is sensitive and cannot be revealed to any other user. Essentially, when making an optimal power assignments, all SUs need to be jointly coordinated to optimize the network utility, which traditionally requires a centralized controller with global knowledge of the entire network (including both IUs and SUs). However, centralized optimal power allocation is not feasible considering IU privacy protection and the inevitably heavy computational overheads on the controller. A practical scheme, thus, has to be distributed without requiring any sensitive information exchange between users .

Several existing works attempt to partially address the optimal SU power control problem, and we will discuss them in three categories: centralized optimization algorithms, distributed power control algorithms for SUs only and distributed power control algorithms for all tiers of users. Centralized optimization algorithms, such as those proposed in [19,20], 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 SU power control strategies, such as [21–23], 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. Distributed power control algorithms for all tiers of users, such as [24,25], do not share the IU's information with SUs, but they assume that all users (including both SUs and IUs) will participate in the power adaptation procedure simultaneously. Such assumption is also not feasible in 3.5 GHz DSA since IU operations in this band, which are satellite and radar, are independent to SU operations and classified.

To fill in the void of existing works, in this chapter, we formulate the uplink power control problem in DSA scenarios as a utility maximization problem, which is then solved using a proposed distributed and secure algorithm. Downlink power control problem in 3.5 GHz DSA is studied in our previous work. We theoretically prove the uplink power control algorithm's convergence at the maximum of network utility, and also show that both IU's interference constraint and SU's power limit and minimum SINR requirement are satisfied at the optimal stable point whenever the formulated uplink optimization problem is feasible. When the optimization problem is infeasible, our algorithm can still converge to a sub-optimal point where all requirements are satisfied except some SU's minimum SINR constraints. In this case, SINR of SUs is sacrificed due to IU's interference protection or SU's power limit. This is reasonable because in DSA, FCC regulation demands that IU's performance has to be guaranteed and SU's maximum power limit cannot be exceeded. Furthermore, no exchange of sensitive IU operation information (e.g. IU's location or its received interference level) is required in the algorithms. Instead of directly sharing the raw IU signal strength sensed by ESC, we proposed a geometry-based model so that the algorithm only requires some ESC processed values related to IU signal strength. Our algorithm ensures that accurate operation information of IU cannot be derived from the masked information exchanged in this system.

The remainder of this chapter is organized as follows. Section 6.2 introduces the system model and formulates the uplink power control problem in the DSA system. Section 6.3 provides a brief introduction on D.C. programming as a preliminary to our algorithm. Section 6.4 describes how each SU uses our uplink power control algorithm to distributively adjust its transmit power, and the convergence and stability properties of the uplink algorithm are demonstrated in Section 6.5. Section 6.6 further shows how IU's interference requirement is statistically guaranteed based on geometry modeling. Section 6.7 analyzes that even when the ESC-supplied information is leaked, it is still difficult for adversaries to infer the true IU location. Evaluations are provided in Section 6.8.

6.2 Problem Formulation

The system model considered in the paper is illustrated in Figure 6.1. Specifically, we assume that m_1 IUs, m_2 ESC sensors, and n pairs of SUs and BSs are distributed in an area. Both the IUs and SUs can be mobile. In uplink, all SUs transmit on the same frequency band. We assume an SU i ($i \in [1, n]$) only transmits towards a BS i. Note that a BS that receives messages from multiple SUs can be simply modeled as multiple co-located BSs, each communicating with one SU.

6.2.1 Uplink Power Control Problem

One typical objective of an uplink power control problem is to find the optimal power allocation that maximizes the sum of individual rates in uplink. To formulate the problem, denote the transmit power of SU i as P_i. The path attenuation from SU i to BS j is denoted by g_{ij}. φ_i denotes the environmental noise between SU i and BS i including the additive receiver noise. The SINR of SU i, thus, can be expressed by $SINR_i = \frac{P_i g_{ii}}{\sum_{j \neq i} P_j g_{ji} + \varphi_i}$. Since the QoS requirements of IU and SUs need to be satisfied, the uplink power control problem can be formulated as:

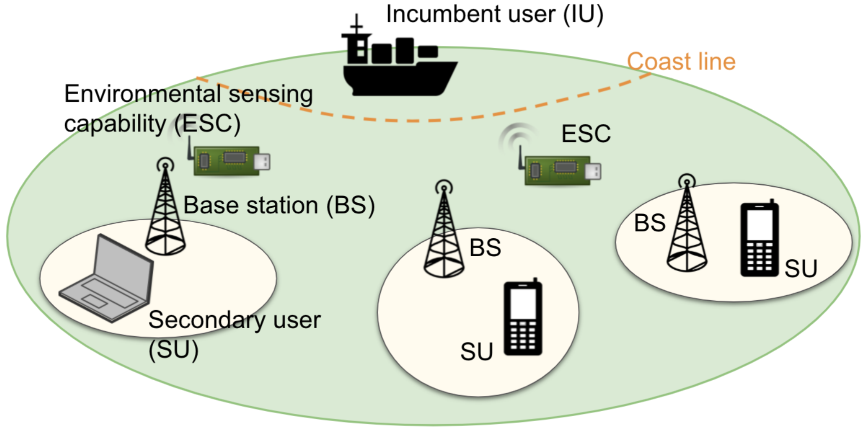

Figure 6.1: System model.

$$\max_{\mathbf{P}} \quad \sum_{i=1}^{n} log_2\Big(\frac{P_i g_{ii}}{\sum_{j\neq i} P_j g_{ji} + \varphi_i} + 1\Big)$$

$$s.t. \quad \frac{P_i g_{ii}}{\sum_{j\neq i} P_j g_{ji} + \varphi_i} \geq \tau, i \in [1, n] \tag{6.1a}$$

$$Pr\Big(\sum_i g_{iI} P_i \leq T\Big) \geq \Lambda \tag{6.1b}$$

$$0 \leq P_i \leq P_{max}, i \in [1, n] \tag{6.1c}$$

The objective is to maximize the sum of SU rates. τ denotes the minimum required SINR level for SU to maintain effective communications as shown by constraint (6.1a). Note that the constraints in (6.1a) are actually the linear constraints. Constraint (6.1b) shows the IU's interference requirement. g_{iI} represents the signal attenuation from SU i to the IU, and T denotes the IU's interference tolerance threshold. Constraint (6.1b) in essence states that the probability that the aggregated SU interference received at IU is no larger than the IU's interference requirement T must be no smaller than an acceptable threshold Λ. Constraint (6.1c) shows that SUs' transmit power P_i is not allowed to exceed its maximum P_{max}.

Though the constraints in problem (6.1) are straightforward, it is hard to guarantee them directly. Due to IU's location privacy protection, g_{iI} in problem (6.1) should not be revealed to any SU/BS/ESC. Thus, neither the direct measurement nor the theoretical estimate of interference suffered by IU is feasible. In addition, an IU in 3.5GHz band usually does not have real-time communications with any SU/BS/ESC. Thus, it is also impossible to expect IU to inform SU about its local interference level.

Our solution is to translate the constraints on IU's received interference to the restrictions on ESC's received interference, which can then be directly measured or theoretically estimated by ESC since ESCs' location information can be found publicly according to FCC regulation in 3.5GHz [18]. Specifically, we propose that once an ESC e has detected the existence of IU, it uses the sensing results of IU to derive its local requirement on the maximum allowable SU interference, denoted as T_e. The computation of T_e demonstrates that the aggregated SU signals at IU is likely to be constrained below T if every ESC's received interference from SUs does not exceed T_e (See Section 6.6 for details). Thus, the problem formulation in (6.1) is converted into (6.2):

$$\max_{\mathbf{P}} \quad \sum_{i=1}^{n} log_2(\frac{P_i g_{ii}}{\sum_{j\neq i} P_j g_{ji} + \varphi_i} + 1) \tag{6.2}$$

$$s.t. \quad \frac{P_i g_{ii}}{\sum_{j\neq i} P_j g_{ji} + \varphi_i} \geq \tau, i \in [1, n] \tag{6.2a}$$

$$\sum_{i} P_i g_{ie} \leq T_e, e \in [i, m_2] \tag{6.2b}$$

$$0 \leq P_i \leq P_{max}, i \in [1, n] \tag{6.2c}$$

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

Denote the SU power assignments that solve the optimization problem in formulation (6.2) as a solution set $S := \{\mathbf{P}|\mathbf{P} \text{ solves } (6.2)\}$, where $\mathbf{P}$ is a column vector and $\mathbf{P} = \{P_i, i \in [1, n]\}$. Note that S exists only when constraints (6.2a)-(6.2c) can be guaranteed together. In the following sections, we will present our distributed uplink power control algorithm and analyze the convergence and stability of our algorithm. When the solution set S exists, meaning that constraints (6.2a)-(6.2c) can be satisfied together, our algorithm successfully converges at the optimal stable point in S. When a solution to (6.2) does not exist (a.k.a. $S = \emptyset$), meaning that a power setting satisfying all three constraints in (6.2) does not exist, our algorithm will converge to a sub-optimal point that guarantees IU's QoS requirement (6.2b) and SU's upper power limit constraint (6.2c), while the constraint (6.2a) may be violated. We believe this to be a desirable feature of our algorithm because in DSA system, 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.

6.3 D.C. Programming

The uplink power control problem in (6.2) has a non-convex objective, and thus can be hard to solve. Fortunately, D.C. programming is extensively developed to cover almost all non-convex global optimization problems. Among the general D.C. approaches, DCA is a robust and efficient method to solve large-scale DC programs [62].

Based on DC programming, rewrite (6.2) as:

$$\begin{aligned} \max_{\mathbf{P}} \quad & h_1(\mathbf{P}) - h_2(\mathbf{P}) \\ s.t. \quad & (2a), (2b), (2c) \end{aligned} \tag{6.3}$$

where $h_1(\mathbf{P}) = \sum_{i=1}^{n} log_2(\sum_j P_j g_{ji} + \varphi_i)$ and $h_2(\mathbf{P}) = \sum_{i=1}^{n} log_2(\sum_{j \neq i} P_j g_{ji} + \varphi_i)$ are concave functions.

As presented in [62], DCA iteratively locates the global optimal solution of (6.3) by generating a sequence $\{\bar{\mathbf{P}}^{(t)}, t = 0, 1, 2, ...\}$ of improved feasible solutions. Specifically, initialized from a feasible starting point $\bar{\mathbf{P}}^{(0)}$, $\bar{\mathbf{P}}^{(t+1)}$ is computed as the optimal solution to the t-th convex sub-problem, which is formulated as:

$$\begin{aligned} \max_{\mathbf{P}} \quad & h_1(\mathbf{P}) - h_2(\bar{\mathbf{P}}^{(t)}) - \nabla h_2(\bar{\mathbf{P}}^{(t)})^{\top}(\mathbf{P} - \bar{\mathbf{P}}^{(t)}) \\ s.t. \quad & (2a), (2b), (2c) \end{aligned} \tag{6.4}$$

where $\nabla h_2(\bar{P}_i^{(t)})$ is the gradient of $h_2(\bar{\mathbf{P}}^{(t)})$ at each $\bar{P}_i^{(t)}$, as expressed as:

$$\nabla h_2(\bar{P}_i^{(t)}) = \frac{1}{\ln 2} \sum_{j \neq i} \frac{g_{ij}}{\sum_{k \neq j} \bar{P}_k^{(t)} g_{kj} + \varphi_j} \tag{6.5}$$

Since (6.4) is a convex problem, whenever the global optimal solution $\bar{\mathbf{P}}^{(t+1)}$ to (6.4) exists, it must be unique.

Also, it has been proved in [62] that the sequence $\{\bar{\mathbf{P}}^{(t)}, t = 0, 1, 2, ...\}$ of improved solutions always converges in finite iterations. The iterative process can be terminated at $|\bar{\mathbf{P}}^{(t)} - \bar{\mathbf{P}}^{(t-1)}| \leq \epsilon_0$ or $|\sum_i \bar{P}_i^{(t)} g_{ij} - \sum_i \bar{P}_i^{(t-1)} g_{ij}| \leq \epsilon_0$, where $\epsilon_0 > 0$ is some threshold. Note that DCA is designed only based on its local characteristics, it cannot theoretically guarantee the globality of converged solutions for general DC programs. However, in practice, DCA converges quite often to a global solution, and is proved to be more robust and more efficient than related standard methods [98–100]. In Section 6.8, we compare the performance of DCA and a global optimizer, which shows that DCA indeed performs better in our case.

Essentially, the procedure of DCA can be regarded as a nested loop. The inner loops are responsible for computing each $\bar{\mathbf{P}}^{(t)}$ as the solution to every $(t-1)$-th convex sub-problem (6.4) to form the sequence of improved solutions $\{\bar{\mathbf{P}}^{(t)}, t = 0, 1, 2, ...\}$, so that the outer loop (envelope) can approach the optimal solution to the original non-convex problem (6.3) (i.e., problem (6.2)) based on the sequence $\{\bar{\mathbf{P}}^{(t)}, t = 0, 1, 2, ...\}$. DCA provides a theoretical idea to find the global optimum of D.C. problems efficiently. However, it cannot be directly applied to the scenario of uplink power control in 3.5 GHz DSA systems, because it does not have any indication on a practical way to solve the sub-problems (6.4) in such scenario. In our proposed SU transmit power control algorithm, presented in the following sections, we adopt the general idea of DCA and demonstrate that our algorithm can solve the sub-problem (6.4) in a practical and distributed manner repeatedly to generate the sequence of improved solutions, and thus the optimal solution to original problem (6.2) can be approached iteratively and distributively.

6.4 Our Distributed Uplink Power Control Algorithm

In this section, we present our distributed uplink power control algorithm. As discussed, the procedure of DCA is a nested loop. Thus, our algorithm also contains an outer loop and several inner loops. Similar to DCA, our algorithm will generate the sequence of improved solutions $\{\bar{\mathbf{P}}^{(t)}, t = 0, 1, 2, ...\}$ which construct the envelope, and each element $\bar{\mathbf{P}}^{(t)}$ inside the sequence is essentially the converged SU transmit power of each $(t-1)$-th inner loop and is also the initial transmit power of t-th inner loop. In our algorithm, the solution $\bar{\mathbf{P}}^{(t)}$ to every convex sub-problem (6.4) will be distributively computed, and hence the optimal power allocation of original problem (6.2) can also be gradually approached in a distributed way. The algorithm can be divided into four parts: the ESC update algorithm, the SAS update algorithm, the BS update algorithm, and the SU update algorithm. The procedure of our algorithm is presented in Table 6.1, and the details of each part and each parameter will be described in the following.

Table 6.1: Our distributed uplink power control algorithm

Our distributed uplink power control algorithm:
For each iteration t in outer loop **do**
Each BS j **(**$j \in [1, n]$**):** a) compute $\Gamma_j^{(t)}$
b) broadacst $\Gamma_j^{(t)}$ to SUs
For each iteration k in inner loop **do**
Each ESC e **(**$e \in [1, m_2]$**):** a) compute Δ_e based on (6.6)
b) forward Δ_e to SAS
SAS: a) compute Δ based on SAS update algorithm
b) forward Δ to BSs
Each BS j **(**$j \in [1, n]$**):** a) for every associated SU i,
compute f_i', and λ_i based on (6.7)-(5.8)
b) broadcast Ω_j, Δ, and $f_i'\lambda_i^2$ for all i to SUs
Each SU i **(**$i \in [1, n]$**):** update transmit power P_i based on (5.12)
end
end

ESC update algorithm: As in Table 6.1, each ESC e measures its local aggregated SU interference, denoted as C_e, and then updates SAS in every iteration inside each inner loop with

$$\Delta_e = (\eta_2 T_e - C_e)\eta_1, \tag{6.6}$$

Here, η_1 and η_2 are two random numbers in the range of $(0,1]$. Both η_1 and η_2 take different values for each Δ_e computation to increase the variations in the value of Δ_e to ensure privacy-protection of IU. The detailed analysis for IU location protection can be found in Section 6.7. 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 6.6, we will discuss the details of T_e generation.

In the ESC update algorithm, we assumes ESC to be able to differentiate IU signals from SU signals based on the dissimilarities in their signal characteristics (e.g. modulation schemes). Such signal classification can be realized through many existing approaches [85–87]. Most of current and proposed ESC design proposals already have this capability.

SAS update algorithm: SAS calculates the minimum value of ESC-supplied Δ_es, denoted by Δ, which is computed by $\Delta = \min(\Delta_e, e \in [1, m_2])$, and then forwards Δ to all BSs in every iteration within each inner loop.

BS update algorithm: As in Table 6.1, at every t-th point of the outer loop, BS j will broadcast a parameter $\Gamma_j^{(t)}$ which is the sum of its received SU interference and environmental noise level. While in each iteration of the inner loops, BS j will broadcast a set of parameters including Δ, and $f_i'\lambda_i^2$ and Ω_j for each associated SU i. We will explain the details of each parameter in the following.

In the inner loops, the BS's parameter f_i' for its associated SU i is computed as follows:

$$f_i' := f'(\tau - SINR_i) = \begin{cases} 1, & SINR_i < \tau \\ 0, & SINR_i > \tau \end{cases} \tag{6.7}$$

$$\text{where } f(z) := \max(0, z). \tag{6.8}$$

In addition, for each associated SU i, λ_i is a non-zero positive time dependent variable that is updated by the following differential equation:

$$\dot{\lambda}_i = \frac{d\lambda_i}{dt} = \beta_i f(\tau - SINR_i) 2\lambda_i. \tag{6.9}$$

where β_i is a positive number. β_i is designed to always guarantee $\lambda_i \leq \lambda_{max}$, where λ_{max} is a very large number. β_i is updated by ensuring:

$$\begin{aligned} &\lambda_i + \dot{\lambda}_i = \lambda_i + \beta_i f(\tau - SINR_i) 2\lambda_i \leq \lambda_{max} \\ &\Rightarrow 0 < \beta_i \leq \frac{\lambda_{max} - \lambda_i}{2\lambda_i f(\tau - SINR_i)} \end{aligned} \tag{6.10}$$

Note that the initial $\lambda_i(0)$ must be positive and satisfy $\lambda_i(0) \ll \lambda_{max}$ to ensure λ_i and β_i to be non-negative. And it is easy to achieve because $\lambda_i(0)$ can be determined by BS itself.

In the inner loops, BS j also computes its total received signal and noise strength, denoted as Ω_j, which is the sum of its received signal level and environmental noise level. BS j then broadcasts Ω_j in every iteration of every inner loop.

Thus, each BS j broadcasts the parameter $\Gamma_j^{(t)}$ at the each t-th point of the outer loop, and it also broadcasts the global parameters Δ, Ω_j, $f_i'\lambda_i^2$ for $i \in [1, n]$ to its associated SUs in every iteration within each inner loop. The update frequency and information exchange rate between BS j and its associated SUs is evaluated in Section 6.8.

The SU update algorithm: SU i adapts its transmit power P_i in every iteration inside each inner loop by:

$$\dot{P}_i = \alpha_i \chi_i \tag{6.11}$$

$$\chi_i = [\sum_k \frac{g_{ik}}{\Omega_k} - \sum_{k \neq i} \frac{g_{ik}}{\Gamma_k^{(t)}} - f_i'\lambda_i^2 g_{ii} + \sum_{k \neq i} f_k'\lambda_k^2 \tau g_{ik}]P_i \tag{6.12}$$

$$\text{where } \alpha_i \leq \Delta|\frac{1}{n\chi_i g_{ie}}| \tag{6.13}$$

In the above adaption algorithm, as mentioned, Δ, Ω_j, $f_i'\lambda_i^2$ ($i \in [1, n], j \in [1, n]$) are broadcasted by BSs at every iteration of each inner loop, while $\Gamma_j^{(t)}$ is broadcasted by BSs at each outer loop iteration and remains the same during the entire inner loop. Channel gain g_{ik} from SU i to BS k can be measured by SU i using downlink reference (e.g. beacon signal). For example, in time-division duplex (TDD) systems, BSs will broadcast beacon signals at a fixed reference power once or twice within each frame. Due to channel reciprocity in TDD systems, SUs can measure its uplink channel gain to various BSs based on these downlink reference signals [101,102]. SU i can estimate its channel gain g_{ie} to 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 5.4.2. The step size value depends on both locally observable and measurable parameters g_{ie} and χ_i, and a global scalar parameter Δ from BS's broadcasts.

In our algorithm, only locally observable and measurable information and some insensitive aggregated information broadcasted by BSs are required for each SU to update its transmit power distributively. The broadcasted information from BSs reveals no IU location or IU interference levels. Also, accurate IU location or interference level can not be derived using the information transmitted from ESC to BS. The computation in BS side is not difficult and requires no privacy sensitive information from IU. In Section 6.5, we prove that our system will asymptotically converge into an optimal stable point in the set S whenever S is nonempty. Then, we will demonstrate how the system stabilizes when S is empty.

6.5 Convergence and Stability of Our Uplink Power Control Algorithm

In this section, we prove the convergence of our uplink power control algorithm. Note that theoretically, the aggregated SU interference at ESC e can be expressed as $C_e = \sum_i P_i g_{ie}$, the total received signal and noise strength Ω_j at BS j can be written as $\Omega_j = \sum_k P_k g_{kj} + \varphi_j$, and the received SU interference and noise level $\Gamma_j^{(t)}$ at BS j is expressed as $\Gamma_j^{(t)} = \sum_{k \neq j} \bar{P}_k^{(t)} g_{kj} + \varphi_j$. The value of $\Gamma_j^{(t)}$ will not change during inner loop iterations.

Combining this with (6.9), (6.11) and (6.12), transmit power update algorithm at SU i in essence can be re-expressed as:

$$\dot{P}_i = \alpha_i [\widetilde{\dot{P}_i} - f_i' \lambda_i^2 g_{ii} + \sum_{k \neq i} f_k' \lambda_k^2 \tau g_{ik}] P_i, \tag{6.14}$$

$$\text{where } \widetilde{\dot{P}_i} = \sum_j \frac{g_{ij}}{\sum_k P_k g_{kj} + \varphi_j} - \sum_{j \neq i} \frac{g_{ij}}{\sum_{k \neq j} \bar{P}_k^{(t)} g_{kj} + \varphi_j}, \tag{6.15}$$

$$\dot{\lambda}_i = \beta_i f[-(P_i g_{ii} - \tau(\sum_{k \neq i} P_k g_{ki} + \varphi_i))] 2\lambda_i. \tag{6.16}$$

Since $f(z)$ in (5.6) is not differentiable at $z = 0$, we only consider the convergence of the algorithm in the domain where $P_i g_{ii} > \tau(\sum_{k \neq i} P_k g_{ki} + \varphi_i), i \in [1, n]$ to ensure the existence of f_i' over $[0, P_{max}]$. Essentially, in this section, we will examine the system's convergence to an uplink transmit power allocation set $\widetilde{S}$ that is defined as $\widetilde{S} := \{\mathbf{P} | \mathbf{P} \text{ solves (6.17)}\}$:

$$\max_{\mathbf{P}} \quad \sum_{i=1}^{n} log_2 (\frac{P_i g_{ii}}{\sum_{k \neq i} P_k g_{ki} + \varphi_i} + 1) \tag{6.17}$$

$$s.t. \quad \frac{P_i g_{ii}}{\sum_{k \neq i} P_k g_{ki} + \varphi_i} > \tau, i \in [1, n] \tag{6.17a}$$

$$(2b), (2c)$$

Comparing $\widetilde{S}$ to the solution set S to problem (6.2), we have $\widetilde{S} \subset S$. Thus, once the system converges into $\widetilde{S}$, it also converges into S and solve problem (6.2). We will prove that whenever $\widetilde{S}$ is nonempty, our algorithm will stabilize at it and hence maximizes the sum of SU rates in uplink as well as satisfies both IU and SUs' requirements. Even when an optimal solution does not exist (i.e. $\widetilde{S} = \emptyset$, all three constraints cannot be guaranteed together), the system will asymptotically converge to a sub-optimal stable point which always satisfies the ESC's interference constraint (6.2b) and SU's maximum power constraint (6.2c).

As mentioned, our algorithm should converge to an optimal solution $\bar{\mathbf{P}}^{(t+1)}$ of the convex sub-problem (6.4) during the inner loop inside the t-th iteration of the outer loop, such that the improved sequence $\{\bar{\mathbf{P}}^{(t)}, t = 0, 1, 2, ...\}$ is gradually generated, and the optimal power allocation of problem (6.17) can be asymptotically approached. Note that the constraints of problem (6.17)'s corresponding convex sub-problem are also (6.17a), (6.2b) and (6.2c).

Our proof includes four stages and a special case. We only consider the case where (6.17) is feasible (i.e., $\widetilde{S}$ is not empty) in the four stages. Convergence in the special case where $\widetilde{S} = \emptyset$ is analyzed in Section 6.5.5.

For $\widetilde{S} \neq \emptyset$, in stage 1, we first consider a simplified optimization problem by removing SU's SINR constraint (6.17a), its upper power limit (6.2c) and IU's interference constraint (6.2b) in sub-problem (6.4). Through the relaxed problem, we derive the first condition that an optimal power allocation must satisfy to maximize the objective of (6.4). In the next stage, constraint (6.17a) is reconsidered. We prove the system's convergence at a point satisfying both the optimal condition derived in stage 1 and the constraint (6.17a). In stage 3, a step size control method is proposed to guarantee ESC's interference constraint (6.2b). In stage 4, we show how SU's maximum power constraint (6.2c) is guaranteed with a simple stop criterion. Since IU's interference constraint should be treated with higher priority than SU's SINR requirement, we prove that by using this algorithm, IU's requirement is satisfied in any cases even when SUs' and IUs' requirements cannot be satisfied simultaneously (i.e. $\widetilde{S} = \emptyset$).

6.5.1 Stage 1: A relaxed problem

To derive the first condition for the optimal solution of convex sub-problem (6.4), let's consider a simplified problem by removing SU's constraints (6.17a) and (6.2c) and IU's interference constraint (6.2b). The problem now becomes:

$$\begin{aligned} \max_{\mathbf{P}} \quad & h_1(\mathbf{P}) - h_2(\bar{\mathbf{P}}^{(t)}) - \nabla h_2(\bar{\mathbf{P}}^{(t)})^\top(\mathbf{P} - \bar{\mathbf{P}}^{(t)}) \\ \text{where } & h_1(\mathbf{P}) = \sum_{i=1}^{n} log_2(\sum_j P_j g_{ji} + \varphi_i), \\ & h_2(\bar{\mathbf{P}}^{(t)}) = \sum_{i=1}^{n} log_2(\sum_{j \neq i} P_j^{(t)} g_{ji} + \varphi_i). \end{aligned} \tag{6.18}$$

Since it is a convex problem, the unique optimal solution to (6.18) is given by:

$$\frac{1}{\ln 2} \sum_j \frac{g_{ij}}{\sum_k P_k g_{kj} + \varphi_j} - \nabla h_2(\bar{P_i}^{(t)}) = 0, i \in [1, n] \tag{6.19}$$

Essentially, the optimal power allocation solution for (6.17) must satisfy (6.19), meaning that the equilibrium of our power control algorithm must first satisfy (6.19).

6.5.2 Stage 2: Proof of system convergence at a point satisfying (6.19) and (6.17a)

In this subsection, we take SU's SINR constraint (6.17a) into account. We prove that the system will stabilize at a unique point satisfying both the optimal condition (6.19) derived in Section 6.5.1 and constraint (6.17a), such that the objective in (6.4) is maximized and SUs' SINR requirements are guaranteed.

For ease of notation, denote the power setting meeting the optimal condition (6.19) and SUs' SINR constraint (6.2a) as a column vector $\widetilde{Z} := \{\mathbf{P}|\mathbf{P}$ satisfies (6.19) and (6.17a)$\}$.

Theorem 3. *Starting from any initial state* $0 < P_i(0) < P_{max}$*, the system described in* (6.14) *to* (6.16) *asymptotically converges to an optimal power allocation setting* $\widetilde{Z}$*.*

Proof. The proof includes two steps. At step 1, we prove that the power setting $\widetilde{Z}$ is a saddle point of our algorithm. At step 2, by constructing a Lyapunov function, we prove that the system is asymptotically stable at $\widetilde{Z}$.

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

$$
\begin{cases}
\dot{P}_i = \alpha_i[\dot{\widetilde{P}}_i - f_i'\lambda_i^2 g_{ii} + \sum\limits_{k\neq i} f_k'\lambda_k^2\tau g_{ik}]P_i^* = 0 & \text{(6.20a)}\\
\dot{\widetilde{P}}_i = \sum\limits_j \dfrac{g_{ij}}{\sum_k P_k^* g_{kj} + \varphi_j} - \sum\limits_{j\neq i} \dfrac{g_{ij}}{\sum_{k\neq j} \bar{P}_k^{(t)} g_{kj} + \varphi_j} & \text{(6.20b)}\\
\dot{\lambda}_i = f[-(P_i^* g_{ii} - \tau(\sum\limits_{k\neq i} P_k^* g_{ki} + \varphi_i))]2\lambda_i = 0 & \text{(6.20c)}
\end{cases}
$$

Since $\lambda_i > 0$, from (5.17b), it is clear that $f[-(P_i^* g_{ii} - \tau(\sum_{k\neq i} P_k^* g_{ki} + \varphi_i))] = 0$, which, based on $f(\cdot)$ definition in (5.6), means $\frac{P_i^* g_{ii}}{\sum_{k\neq i} P_k^* g_{ki} + \varphi_i} > \tau$. Hence, $f_i' = 0, \forall i \in [i, n]$, and $\dot{P}_i = 0$ becomes equivalent to $\dot{\widetilde{P}}_i = 0$. Thus, (6.20a) to (6.20c) can be converted to:

$$
\begin{cases}
\sum_j \frac{g_{ij}}{\sum_k P_k^* g_{kj} + \varphi_j} = \sum_{j\neq i} \frac{g_{ij}}{\sum_{k\neq j} \bar{P}_k^{(t)} g_{kj} + \varphi_j},\\
\frac{P_i^* g_{ii}}{\sum_{k\neq i} P_k^* g_{ki} + \varphi_i} > \tau, \forall i \in [1, n]
\end{cases}
\tag{6.21}
$$

Based on (6.5) and (6.19), clearly (6.21) is equivalent to the definition of $\widetilde{Z}$. Hence, $\widetilde{Z}$ equals the saddle point $\boldsymbol{P}^*$ for the system.

Step 2: Given the system's saddle point $\widetilde{Z}$, now we will prove that $\widetilde{Z}$ is the equilibrium point of the system and the system converges at $\widetilde{Z}$ by constructing a Lyapunov function $K(\boldsymbol{\lambda}, \boldsymbol{P})$

for the system as

$$
\begin{aligned}
K(\boldsymbol{\lambda}, \boldsymbol{P}) :=& V(\boldsymbol{\lambda}, \boldsymbol{P}) + F(\boldsymbol{\lambda}, \boldsymbol{P}), \\
\text{where } V :=& \sum_j \ln(\sum_k P_k g_{kj} + \varphi_j) - \sum_j \nabla h_2(\bar{P_j}^{(t)}) P_j \ln 2, \\
F :=& \sum_j f[\tau(\sum_{k \neq j} P_k g_{kj} + \varphi_j) - P_j g_{jj}] \lambda_j^2.
\end{aligned} \tag{6.22}
$$

Theorem 4. *$K(\boldsymbol{\lambda}, \boldsymbol{P})$ defined in (6.22) is a Lyapunov function for the system defined in (6.14) - (6.16). In addition, $\dot{K} = 0$ if and only if $\boldsymbol{P}^* = \widetilde{Z}$.*

Proof: The partial derivative of $V(\boldsymbol{\lambda}, \boldsymbol{P})$ in (6.22) over P_i is derived as:

$$
\begin{aligned}
\frac{\partial V}{\partial P_i} &= \sum_j \frac{g_{ij}}{\sum_k P_k g_{kj} + \varphi_j} - \sum_{j \neq i} \frac{g_{ij}}{\sum_{k \neq j} \bar{P_k}^{(t)} g_{kj} + \varphi_j} \\
&= \widetilde{\dot{P}_i}
\end{aligned} \tag{6.23}
$$

Similarly, the partial derivative of $F(\boldsymbol{\lambda}, \boldsymbol{P})$ in (6.22) over P_i and λ_i are derived as:

$$
\frac{\partial F}{\partial P_i} = -f_i' \lambda_i^2 g_{ii} + \sum_{k \neq i} f_k' \lambda_k^2 \tau g_{ik}, \tag{6.24}
$$

$$
\begin{aligned}
\frac{\partial F}{\partial \lambda_i} &= f[\tau(\sum_{k \neq i} P_k g_{ki} + \varphi_i)) - P_i g_{ii}] 2\lambda_i \\
&= \dot{\lambda}_i / \beta_i
\end{aligned} \tag{6.25}
$$

Then we prove that $K(\cdot)$ is a Lyapunov function for the system described by (6.14) - (6.16). Since we are discussing a maximization problem, the convergence condition are $\dot{K} \geq 0$ and $K(\cdot)$ is upper bounded, and $\dot{K} = 0$ if and only if $\boldsymbol{P}^* = \widetilde{Z}$.

Firstly, we show that $K(\cdot)$ is upper bounded. The function $K(\cdot)$'s second order partial derivative over P_i satisfies $\frac{\partial^2 K}{\partial P_i^2} < 0$, thus, $K(\cdot)$ is concave over P_i. From (6.10) we can see that $\lambda_i \leq \lambda_{max}$ is always true. Thus, $K(\cdot)$ is also upper bounded over λ_i.

Next, the time derivative of $K(\cdot)$ is computed by

$$
\dot{K} = \sum_i \frac{\partial K}{\partial P_i} \dot{P}_i + \sum_i \frac{\partial K}{\partial \lambda_i} \dot{\lambda}_i \tag{6.26}
$$

Based on (6.25), the value of $\sum_i \frac{\partial K}{\partial \lambda_i} \dot{\lambda}_i$ can be calculated as following:

$$\sum_i \frac{\partial K}{\partial \lambda_i}\dot{\lambda}_i = \sum_i \dot{\lambda}_i^{\,2}/\beta_i \geq 0, \tag{6.27}$$

and $\sum_i \frac{\partial K}{\partial \lambda_i}\dot{\lambda}_i = 0$ if and only if $\frac{P_i g_{ii}}{\sum_{k\neq i} P_k g_{ki} + \varphi_i} > \tau, i \in [1, n]$. In this case, $f_i' = 0, i \in [1, n]$.

Next step is to compute $\sum_i \frac{\partial K}{\partial P_i}\dot{P}_i$. Given (6.14), (6.15), (6.23) and (6.24),

$$\sum_i \frac{\partial K}{\partial P_i}\dot{P}_i = \sum_i (\frac{\partial V}{\partial P_i} + \frac{\partial F}{\partial P_i})\dot{P}_i = \sum_i \frac{1}{\alpha_i P_i}\dot{P}_i^{\,2} \geq 0 \tag{6.28}$$

Hence, $\sum_i \frac{\partial K}{\partial P_i}\dot{P}_i = 0$ if and only if $\dot{P}_i = 0$. Since $f_i' = 0$, $\boldsymbol{P}^* = \widetilde{Z}$. $K(\cdot)$ is proved to be a Lyapunov function of our system.

□

6.5.3 Stage 3: Step size control for IU's interference constraint

So far we only consider the constraints (6.17a) in the problem (6.17). In this section, the ESC's interference constraint (6.2b) is taken into account. We show that the IU's interference requirement (ESC's interference constraint) can be guaranteed in any case by proposing a step size control method.

The step size control method need to ensure that the ESC's interference at any iteration to be smaller than its threshold T_e by enforcing:

$$\sum_{i\in[1,n]} (P_i + \dot{P}_i) g_{ie} \leq T_e, e \in [1, m_2] \tag{6.29}$$

In this way the requirement $\sum_i P_i^* g_{ie} \leq T_e$ can be guaranteed. Since $C_e = \sum_i P_i g_{ie}$, given (6.11), we can have:

$$\sum_i \dot{P}_i g_{ie} = \sum_i \alpha_i \chi_i g_{ie} \leq \sum_i \alpha_i |\chi_i| g_{ie} \leq T_e - C_e \tag{6.30}$$

Since $T_e - C_e \geq \Delta_e \geq \Delta$, (6.30) must hold if the following inequality (6.31) is satisfied:

$$\sum_i \alpha_i |\chi_i| g_{ie} \leq \Delta. \tag{6.31}$$

Thus, our algorithm limits α_i, $\forall i \in [1, n]$ setting by:

$$\alpha_i \leq \Delta |\frac{1}{n\chi_i g_{ie}}|. \tag{6.32}$$

Essentially, each SU i tunes the step size α_i in each iteration based on the above inequality, which ensures the ESC's interference requirements will not be exceeded at any time.

6.5.4 Stage 4: Stopping criterion

Finally, we handle the maximum power constraint (6.2c) of SUs. There are cases when the transmit power P_i of SU i already reaches P_{max}, while the optimal solution has not been achieved. In this case, SU 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 SUs keep on updating their transmit power until the convergence of the system. Now, we have proved that our algorithm will asymptotically converge to the optimal solution $\bar{\mathbf{P}}^{(t+1)}$ of sub-problem (6.4) through the inner loop at every t-th outer loop iteration. Hence, the optimal power allocation of problem (6.17) can be gradually approached based on the constructed sequence $\{\bar{\mathbf{P}}^{(t)}, t = 0, 1, 2, ...\}$ of improved solutions.

6.5.5 Special case: $\widetilde{S} = \emptyset$

There are cases where all three constraints in (6.17) cannot be guaranteed together (i.e., $\widetilde{S} = \emptyset$). In such a case, our algorithm chooses a rational step size based on (6.32) to ensure at least IU' interference requirement is always satisfied. Moreover, the stopping criterion is applied to guarantee that SU's transmit power is within the allowable range. Note that in this case, the algorithm sacrifices the SINR of SUs. Thus, the constraint (6.2a) may be violated. This is reasonable because in DSA, FCC regulation demands that IU's performance has to be guaranteed and SU's maximum power limit cannot be exceeded. Therefore, in this special case, some SUs have to fix their transmit power due to ESC's interference requirement or SU's transmit power limit unless the algorithm guides them to update the transmit power, while other SUs keep on updating their transmit power until the convergence of the system.

6.6 ESC interference requirements

As discussed in Section 6.2, due to the sensitivity in IU's location privacy, the interference from SUs to an IU cannot be directly measured and thus the uplink problem formulation in (6.1) cannot be solved directly. Therefore, we estimate the interference from SU to ESC instead and create problem formulation (6.2). In Section 6.5, we have proved that our uplink power control algorithm asymptotically stabilize at an equilibrium that solves the respective optimization problems with ESCs' requirements. In this section, we describe how our algorithm computes ESC's interference constraint T_e and verify that using this T_e computation, the solution to the uplink problem in (6.2) is approximately also a solution to (6.1).

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

$$U(\mathbf{T_E}) := Pr(I \leq T | C_e \leq T_e, \text{for all } e \in [1, m_2]) \geq \Psi \tag{6.33}$$

where Ψ is a constant threshold satisfying $\Psi \in [0,1]$ and $\Psi \approx 1$. We denote the left side of the inequality as $U(\mathbf{T_E})$, which represents the conditional probability that the aggregated SU interference I at IU does not exceed its requirement T given that the SU interference C_e received at each ESC e is bounded by $\mathbf{T_E}$. The formula essentially means that ESCs should choose a proper $\mathbf{T_E}$ to ensure the probability on the left side to be close to 1.

In the next sections, we derive the explicit expression of $U(\mathbf{T_E})$. To achieve this, we first present the geometric model of our system in Section 6.6.1. Based on the model, we derive the statistical distribution of C_e in Section 6.6.2. In Section 6.6.3, we model the conditional statistical distribution of I. Next, in Section 6.6.4, (6.33) is solved as a cumulative density function (CDF) of a conditional normal distribution, and use this CDF to determine T_E that guarantees $U(\mathbf{T_E}) \geq \Psi$.

6.6.1 Geometry-based heterogeneous network modeling

The network architecture used in our model is shown in Figure 6.2. Here we consider a heterogeneous network containing different tiers of SUs. The IU is denoted by a green triangle. In this section, we take one IU case as an example for detailed explanation. The case of multiple IUs is discussed in Section 6.6.5. All SUs are denoted by the red crosses. SUs inside each orange area form a cluster, and are regarded as the small cell users (hotspot users). The average number of hotspot SUs per cluster is n_s. The center of clusters, denoted by blue dots in Figure 6.2, are modeled as a homogeneous Poisson Point Process (PPP) with the density of ρ_1. Hotspot SUs are distributed around cluster centers according to a Gaussian distribution (a.k.a. Thomas cluster process [103]) with a scattering variance of σ_s^2. SUs outside the clusters are the macro cell users. The locations of macro cell SUs are also modeled as a homogeneous PPP with the density of ρ_2. ESC is denoted by a black square. 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. Thus, the average number of hotspot SUs in the given area is $\rho_1 n_s \pi l^2$, and the average number of macro cell SUs is $\rho_2 \pi l^2$.

6.6.2 Distribution of C_e

To derive the statistical distribution of C_e for ESC sensor e, the path attenuation between SU i and ESC e needs to be estimated. Since SU locations are usually not known to an ESC due to SU's location privacy protection, we can not measure or compute the channel gain directly. Thus, we establish a statistical model of channel gain between SU and ESC. According to Section 6.6.1, the SUs are categorized into macro cell users and hotspot users. Thus, we model the distribution of distance between hotspot SU and ESC, denoted as u_1, and the distribution of distance between macro cell SU and ESC denoted as u_2, respectively. in this chapter, we adopt the simplified path loss model $P^r(d) = P^t c d^{-\iota}$ for analysis since it

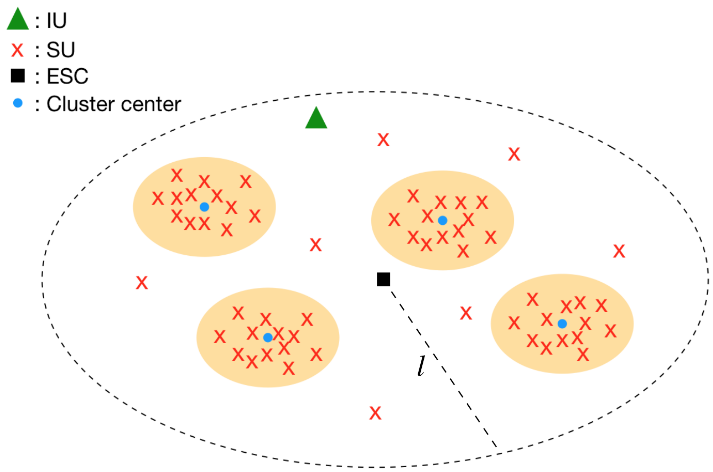

Figure 6.2: Network of SUs and IUs in the two-tier user-centric deployed HetNets, where the clusters with high user density are regarded as hotspots.

captures the main characteristics of ray tracing. Here, $P^r(d)$ denotes the received power at distance d and P^t denotes the transmit power. c is a constant which is given by $c = \frac{P^r(\bar{d})\bar{d}^{\iota}}{P^t}$, $\bar{d}$ is a reference distance, and ι is the path loss exponent. Hence, the channel gain between an ESC and a hotspot SU can be computed by $g_{u_1} = c{u_1}^{-\iota}$, and similarly $g_{u_2} = c{u_2}^{-\iota}$. Next, we examine the statistical distributions of u_1 and u_2, which are used for modeling g_{u_1} and g_{u_1}.

Distribution of distance u_1 between hotspot SU and ESC

We assume that the centers of SU clusters follow a homogeneous PPP, and hotspot SUs are normally distributed inside its cluster. The relation among hotspot SU, ESC and cluster center is illustrated in Figure 6.3, x_0 denotes the distance between cluster center and ESC.

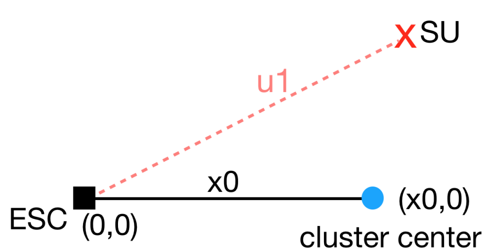

Figure 6.3: The relation among SU, ESC and cluster center.

According to [104], conditioned on the distribution of a cluster center, the distance u_1 from

$$\bar{g}_{u_1} = \int_{l^{-\iota}}^{\epsilon_1^{-\iota}} \int_0^l \frac{2x_0 c^{\frac{2}{\iota}} g^{-\frac{2}{\iota}}}{\iota \sigma_s^2 l^2} \exp(-\frac{(\frac{g}{c})^{-\frac{2}{\iota}} + x_0^2}{2\sigma_s^2}) \cdot I_0(\frac{c^{\frac{1}{\iota}} g^{-\frac{1}{\iota}} x_0}{\sigma_s^2}) \mathrm{d}x_0 \mathrm{d}g \tag{6.38}$$

$$\sigma_{g_{u_1}}^2 = \int_{l^{-\iota}}^{\epsilon_1^{-\iota}} \int_0^l (g - \bar{g}_{u_1})^2 \frac{2x_0 c^{\frac{2}{\iota}} c^{\frac{2}{\iota}} g^{-\frac{2}{\iota}-1}}{\iota \sigma_s^2 l^2} \exp(-\frac{(\frac{g}{c})^{-\frac{2}{\iota}} + x_0^2}{2\sigma_s^2}) \cdot I_0(\frac{c^{\frac{1}{\iota}} g^{-\frac{1}{\iota}} x_0}{\sigma_s^2}) \mathrm{d}x_0 \mathrm{d}g \tag{6.39}$$

ESC to an SU follows the Rician distribution, and the conditioned probability density function (PDF) can be written as:

$$\xi_{U_1|X}(u_1|x_0) = \frac{u_1}{\sigma_s^2} \exp(-\frac{u_1^2 + x_0^2}{2\sigma_s^2}) \cdot I_0(\frac{u_1 x_0}{\sigma_s^2}) \tag{6.34}$$

where $I_0(\cdot)$ is the modified Bessel function with order zero and σ_s^2 is the scattering variance. Since cluster centers are uniformly distributed, and the PDF is given by $\xi_X(x_0) = \frac{2x_0}{l^2}$. Thus, the PDF of u_1 can be computed as following:

$$\begin{aligned} \xi_{U_1}(u_1) &= \int_{x_0} \xi_{U_1|X}(u_1|x_0) \xi_X(x_0) \mathrm{d}x_0 \\ &= \int_0^l \frac{2x_0 u_1}{\sigma_s^2 l^2} \exp(-\frac{u_1^2 + x_0^2}{2\sigma_s^2}) \cdot I_0(\frac{u_1 x_0}{\sigma_s^2}) \mathrm{d}x_0 \end{aligned} \tag{6.35}$$

Distribution of distance u_2 between macro cell SU and ESC

As discussed, we assume that macro cell SUs are uniformly distributed inside the given area. The PDF of u_2, denoted as $\xi(u_2)$, can be expressed as $\xi_{U_2}(u_2) = \frac{2u_2}{l^2}$.

Distribution of g_{u_1}, g_{u_2} and C_e

So far we have derived the PDFs for distance u_1 and u_2, and the distributions of their corresponding channel gain g_{u_1} and g_{u_2} can be derived based on the following equations:

$$Pr(g_{u_1} \leq g) = Pr(u_1 \geq (\frac{g}{c})^{-\frac{1}{\iota}}) = 1 - Pr(u_1 \leq (\frac{g}{c})^{-\frac{1}{\iota}}) \tag{6.36}$$

$$\xi_{g_{u_1}}(g) = \frac{\partial Pr(g_{u_1} \leq g)}{\partial g} = \frac{c^{\frac{1}{\iota}}}{\iota} g^{-\frac{1+\iota}{\iota}} \xi_{U_1}(c^{\frac{1}{\iota}} g^{-\frac{1}{\iota}}) \tag{6.37}$$

Furthermore, the expectation $\bar{g}_{u_1}$ and variance $\sigma_{g_{u_1}}^2$ of g_{u_1} can be expressed as in (6.38) and (6.39), where ϵ_1 is the minimum distance between an SU and ESC.

The PDF of g_{u_2} is derived in the same way as in equation (6.37), and the expectation and variance of g_{u_2}, denoted as $\bar{g}_{u_2}$ and $\sigma^2_{g_{u_2}}$, can be calculated based on:

$$\bar{g}_{u_2} = \int_{l^{-\iota}}^{\epsilon_1^{-\iota}} \frac{2c^{-\frac{2}{\iota}} g^{-\frac{2}{\iota}}}{\iota l^2} \mathrm{d}g \tag{6.40}$$

$$\sigma^2_{g_{u_2}} = \int_{l^{-\iota}}^{\epsilon_1^{-\iota}} (g - \bar{g}_{u_2})^2 \frac{2c^{-\frac{2}{\iota}} g^{-\frac{2+\iota}{\iota}}}{\iota l^2} \mathrm{d}g \tag{6.41}$$

Since all hotspot and macro cell SUs are independent, g_{u_1} is i.i.d. and g_{u_2} is also i.i.d.. C_e is then re-expressed as $C_e = \sum_{i=1}^{\rho_1 n_s \pi l^2} P_i^h g_{u_1} + \sum_{i=1}^{\rho_2 \pi l^2} P_i^m g_{u_2}$, where P_i^h and P_i^m denote the transmit power of hotspot SU and macro cell SU, respectively. Given the number of hotspot SUs $\rho_1 n_s \pi l^2$ and the number of macro cell SUs $\rho_2 \pi l^2$ in the model, when $\rho_1 n_s \pi l^2$ and $\rho_2 \pi l^2$ increase, using the Central Limit Theorem and the Law of Large Numbers, C_e can be approximated by a summation of two normal distributions which is still a normal distribution, $C_e \sim N(\mu_e, \sigma_e^2)$, where

$$\begin{aligned} \mu_e &= \sum_{i=1}^{\rho_1 n_s \pi l^2} P_i^h \bar{g}_{u_1} + \sum_{i=1}^{\rho_2 \pi l^2} P_i^m \bar{g}_{u_2}, \\ \sigma_e^2 &= \sum_{i=1}^{\rho_1 n_s \pi l^2} (P_i^h)^2 \sigma^2_{g_{u_1}} + \sum_{i=1}^{\rho_2 \pi l^2} (P_i^m)^2 \sigma^2_{g_{u_2}}, \end{aligned} \tag{6.42}$$

6.6.3 Distribution of I

In this section, we model the statistical distribution of the IU's received SU interference I. Denoting g_{v_1} as the path loss from a hotspot SU to the IU and g_{v_2} as the path loss from a macro cell SU to the IU, we again re-express I as $I = \sum_{i=1}^{\rho_1 n_s \pi l^2} P_i^h g_{v_1} + \sum_{i=1}^{\rho_2 \pi l^2} P_i^m g_{v_2}$. Same as C_e, to model I, we again need to derive g_{v_1} and g_{v_2}'s statistical distribution while IU's location is not explicitly known due to IU location privacy protection.

The first step for modeling g_{v_1} and g_{v_2} is to to establish the statistical model of IU's location range to ESC, denoted as d_0, given ESC's local measurement of IU signal strength. Then, based on this model, each ESC independently estimate d_0, which leads to the derivation of g_{v_1} and g_{v_2} as well as the distribution of I and $U(\boldsymbol{T_E})$ in (6.33). It is important to note that this calculation process satisfies FCC's security regulation, which demands that ESCs must not share any IU's location-related information. In our algorithm, ESC only uses local information and there is no exchange of any IU-related information with other ESC or other parties in the system.

Distribution of d_0 based on ESC's local IU signal strength

We assume IU's transmit power P^t_{IU} is known since the general transmit power of 3.5GHz IU transmitters, such as radar systems, is easily found [105]. Hence, given the received IU signals, denoted as P^r_{IU}, an ESC can roughly model the distribution of its channel gain to IU as g_0 through a path loss formula $g_0 = P^r_{IU}/P^t_{IU}$. Thus, the distance between ESC and IU, denoted as d_0, is given by $d_0 = (\frac{g_0}{c_0})^{-\frac{1}{\iota}}$ where c_0 is a constant. Assuming IU's signal is transmitted through a Rayleigh fading channel, the CDF of P^r_{IU} can be modeled as $\Xi_{PR}(P^r_{IU}) = 1 - \exp(-\frac{P^r_{IU}}{s_e})$, where s_e is the expectation of P^r_{IU}, which can be measured by ESC e. Therefore, the CDF of g_0 can be derived by:

$$\begin{aligned}\Xi_{G_0}(g_0) &= Pr(G_0 \leq g_0) = Pr(P^r_{IU} \leq g_0 P^t_{IU}) \\ &= \Xi_{PR}(g_0 P^t_{IU}) = 1 - \exp(-\frac{g_0 P^t_{IU}}{s_e})\end{aligned} \tag{6.43}$$

The CDF of d_0 is then computed by:

$$\begin{aligned}\Xi_{D_0}(d_0) &= Pr(D_0 \leq d_0) = Pr(g_0 \geq c_0 d_0^{-\iota}) \\ &= 1 - \Xi_{G_0}(c_0 d_0^{-\iota}) = \exp(-\frac{c_0 d_0^{-\iota} P^t_{IU}}{s_e})\end{aligned} \tag{6.44}$$

Furthermore, the PDF of d_0 is expressed as:

$$\xi_{D_0}(d_0) = \exp(-\frac{c_0 P^t_{IU} d_0^{-\iota}}{s_e})\frac{\iota c_0 P^t_{IU}}{s_e} d_0^{-\iota-1} \tag{6.45}$$

Distribution of distance v_1 between hotspot SU and IU

The relation among IU, ESC, SU and cluster center is illustrated in Figure 6.4. From an ESC's perspective, the possible location of IU is uniformly distributed on a circle that is centered at itself and has a radius of d_0. As in Figure 6.4, r denotes the distance from cluster center to IU, and θ denotes the angle between d_0 and x_0.

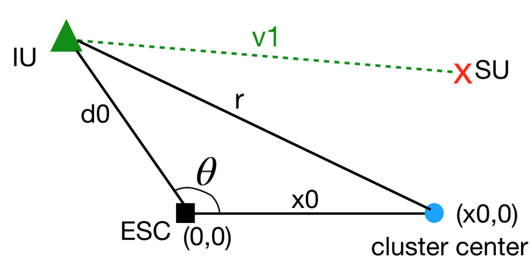

Figure 6.4: The relation among IU, ESC, SU and cluster center.

$$\Xi_R(r) = \int_0^l \frac{2x_0}{l^2} \int_0^l \frac{1}{\pi} \arccos \frac{d_0^2 + x_0^2 - r^2}{2d_0 x_0} \left[\exp(-\frac{c_0 P_{IU}^t d_0^{-\iota}}{s_e}) \frac{\iota c_0 P_{IU}^t}{s_e} d_0^{-\iota-1} \right] \mathrm{d}d_0 \mathrm{d}x_0 \quad (6.47)$$

$$\xi_R(r) = \frac{\mathrm{d}}{\mathrm{d}r}\Xi_R(r) = \int_0^l \frac{2r}{\pi l^2} \int_0^l \frac{1}{\sqrt{1-(\frac{d_0^2+x_0^2-r^2}{2d_0x_0})^2}} \left[\exp(-\frac{c_0 P_{IU}^t d_0^{-\iota}}{s_e}) \frac{\iota c_0 P_{IU}^t}{s_e} d_0^{-\iota-2} \right] \mathrm{d}d_0 \mathrm{d}x_0 \quad (6.48)$$

To derive the distribution of v_1, we need to compute the distribution for r. Clearly, r satisfies $r^2 = d_0^2 + x_0^2 - 2d_0x_0 \cos\theta$. Thus, the CDF of r, denoted by $\Xi_R(r)$, is given by:

$$\begin{aligned} \Xi_R(r) &= Pr(R \le r) \\ &= Pr(\sqrt{d_0^2 + x_0^2 - 2d_0x_0\cos\theta} \le r) \\ &= \int\int\int_{\sqrt{d_0^2+x_0^2-2d_0x_0\cos\theta \le r}} \xi_{X_0,\Theta,D_0}(x_0,\theta,d_0)\mathrm{d}x_0\mathrm{d}\theta\mathrm{d}d_0 \end{aligned} \quad (6.46)$$

Since x_0, θ, d_0 are independent, and the PDF of θ is $\xi_\Theta(\theta) = \frac{1}{\pi}$, $\Xi_R(r)$ can be computed based on (6.47). Thus, r's PDF $\xi_R(r)$ is derived as in (6.48).

Having $\xi_R(r)$, the next step is to compute the PDF of v_1. Similarly, conditioned on the distance r between an IU and a cluster center, the distance v_1 from IU to the SU, who is in a Thomas cluster process, is also Rician distributed, and the conditioned PDF is given by (6.49).

$$\xi_{V_1|R}(v_1|r) = \frac{v_1}{\sigma_s^2}\exp(-\frac{v_1^2+r^2}{2\sigma_s^2})I_0(\frac{v_1 r}{\sigma_s^2}) \quad (6.49)$$

Then the PDF of v_1 can be derived by (6.50).

$$\begin{aligned} \xi_{V_1}(v_1) = \int_0^{2l} \frac{v_1}{\sigma_s^2}\exp(-\frac{v_1^2+r^2}{2\sigma_s^2})I_0(\frac{v_1 r}{\sigma_s^2}) \int_0^l \frac{2r}{\pi l^2} \int_0^l \frac{1}{\sqrt{1-(\frac{d_0^2+x_0^2-r^2}{2d_0x_0})^2}} \cdot \\ \left[\exp(-\frac{c_0 P_{IU}^t d_0^{-\iota}}{s_e}) \frac{\iota c_0 P_{IU}^t}{s_e} d_0^{-\iota-2} \right] \mathrm{d}d_0 \mathrm{d}x_0 \mathrm{d}r \end{aligned} \quad (6.50)$$

$$\xi_{V_2}(v_2) = \begin{cases} \int_0^{l-v_2} \frac{2v_2}{l^2} \exp(-\frac{c_0 P_{IU}^t d_0^{-\iota}}{s_e}) \frac{\iota c_0 P_{IU}^t}{s_e} d_0^{-\iota-1} \mathrm{d}d_0, & 0 \le v_2 \le l \\ \int_{v_2-l}^{l} \frac{2v_2}{\pi l^2} \arccos(\frac{d_0^2+v_2^2-l^2}{2d_0 v_2}) \exp(-\frac{c_0 P_{IU}^t d_0^{-\iota}}{s_e}) \frac{\iota c_0 P_{IU}^t}{s_e} d_0^{-\iota-1} \mathrm{d}d_0, & l < v_2 \le 2l \end{cases} \tag{6.52}$$

$$\begin{aligned} \bar{g}_{v_1} = \int_{\frac{1}{(2l)^\iota}}^{\epsilon_2^{-\iota}} \int_0^{2l} \int_0^{l} \int_0^{l} & \frac{2rc^{\frac{2}{\iota}} g^{-\frac{2}{\iota}} I_0(\frac{(\frac{g}{c})^{-\frac{1}{\iota}} r}{\sigma_s^2})}{\iota \sigma_s^2 \pi l^2 \sqrt{1-(\frac{d_0^2+x_0^2-r^2}{2d_0 x_0})^2}} \exp(-\frac{c^{\frac{2}{\iota}} g^{-\frac{2}{\iota}} + r^2}{2\sigma_s^2}) \cdot \\ & \left[\exp(-\frac{c_0 P_{IU}^t d_0^{-\iota}}{s_e}) \frac{\iota c_0 P_{IU}^t}{s_e} d_0^{-\iota-2}\right] \mathrm{d}d_0 \mathrm{d}x_0 \mathrm{d}r \mathrm{d}g \end{aligned} \tag{6.53}$$

Distribution of distance v_2 between macro cell SU and IU

From an ESC's perspective, once the value of d_0 is determined, the possible location of IU should be uniformly distributed in a circle that is centered at itself and has a radius of d_0. Denote v_2 as the distance between a macro cell SU and IU. The PDF of v_2 conditioned on d_0, denoted as $\xi_{V_2|D_0}(v_2|d_0)$, is expressed as:

$$\xi(v_2|d_0) = \begin{cases} \frac{2v_2}{l^2}, & 0 \le v_2 \le l - d_0 \\ \frac{2v_2}{\pi l^2} \arccos(\frac{d_0^2+v_2^2-l^2}{2d_0 v_2}), & l - d_0 < v_2 \le l + d_0 \end{cases} \tag{6.51}$$

Thus v_2's PDF can be computed based on (6.52).

Distribution of g_{v_1}, g_{v_2} and I

Given the derived the PDFs for distance v_1 and v_2, the corresponding PDFs of channel gain g_{v_1} and g_{v_2} can be derived in the same way as shown in equations (6.36) and (6.37).

The expectation $\bar{g}_{v_1}$ and variance $\sigma_{g_{v_1}}^2$ of g_{v_1} are calculated following equations (6.53) and (6.54). Similarly, g_{v_2}'s expectation $\bar{g}_{v_2}$ and variance $\sigma_{g_{v_2}}^2$ are given by equations (6.55) and (6.56), where ϵ_2 is the minimum distance between an SU and IU.

Because all hotspot and macro cell SUs are independent, g_{v_1} is i.i.d. and g_{v_2} are also i.i.d.. When the number of hotspot SUs and the number of macro cell SUs increase, using the

$$\begin{aligned} \sigma_{g_{v_1}}^2 = \int_{\frac{1}{(2l)^\iota}}^{\epsilon_2^{-\iota}} \int_0^{2l} \int_0^{l} \int_0^{l} & \frac{2r(g-\bar{g}_{v_1})^2 c^{\frac{2}{\iota}} g^{-\frac{2}{\iota}-1} I_0(\frac{(\frac{g}{c})^{-\frac{1}{\iota}} r}{\sigma_s^2})}{\iota \sigma_s^2 \pi l^2 \sqrt{1-(\frac{d_0^2+x_0^2-r^2}{2d_0 x_0})^2}} \exp(-\frac{(\frac{g}{c})^{-\frac{2}{\iota}} + r^2}{2\sigma_s^2}) \cdot \\ & \left[\exp(-\frac{c_0 P_{IU}^t d_0^{-\iota}}{s_e}) \frac{\iota c_0 P_{IU}^t}{s_e} d_0^{-\iota-2}\right] \mathrm{d}d_0 \mathrm{d}x_0 \mathrm{d}r \mathrm{d}g \end{aligned} \tag{6.54}$$

$$\bar{g}_{v_2} = \int_{l^{-\iota}}^{\epsilon_2^{-\iota}} \int_0^{l-(\frac{g}{c})^{-\frac{1}{\iota}}} \frac{2c^{\frac{2}{\iota}}g^{-\frac{2}{\iota}}}{l^2} \exp(-\frac{c_0 P_{IU}^t d_0^{-\iota}}{s_e}) \frac{\iota c_0 P_{IU}^t}{s_e} d_0^{-\iota-1} \mathrm{d}d_0 \mathrm{d}g$$
$$+ \int_{\frac{1}{(2l)^\iota}}^{l^{-\iota}} \int_{(\frac{g}{c})^{-\frac{1}{\iota}}-l}^{l} \frac{2c^{\frac{2}{\iota}}g^{-\frac{2}{\iota}}}{\pi l^2} \arccos(\frac{d_0^2 + c^{\frac{2}{\iota}}g^{-\frac{2}{\iota}} - l^2}{2d_0(\frac{g}{c})^{-\frac{1}{\iota}}}) \exp(-\frac{c_0 P_{IU}^t d_0^{-\iota}}{s_e}) \frac{\iota c_0 P_{IU}^t}{s_e} d_0^{-\iota-1} \mathrm{d}d_0 \mathrm{d}g \tag{6.55}$$

$$\sigma_{g_{v_2}}^2 = \int_{l^{-\iota}}^{\epsilon_2^{-\iota}} \int_0^{l-(\frac{g}{c})^{-\frac{1}{\iota}}} (g - \bar{g}_{v_2})^2 \frac{2c^{\frac{2}{\iota}}g^{-\frac{2}{\iota}-1}}{l^2} \exp(-\frac{c_0 P_{IU}^t d_0^{-\iota}}{s_e}) \frac{\iota P_{IU}^t}{s_e} d_0^{-\iota-1} \mathrm{d}d_0 \mathrm{d}g$$
$$+ \int_{\frac{1}{(2l)^\iota}}^{l^{-\iota}} \int_{(\frac{g}{c})^{-\frac{1}{\iota}}-l}^{l} (g - \bar{g}_{v_2})^2 \frac{2c^{\frac{2}{\iota}}g^{-\frac{2}{\iota}-1}}{\pi l^2} \arccos(\frac{d_0^2 + c^{\frac{2}{\iota}}g^{-\frac{2}{\iota}} - l^2}{2d_0(\frac{g}{c})^{-\frac{1}{\iota}}}) \exp(-\frac{c_0 P_{IU}^t d_0^{-\iota}}{s_e}) \frac{\iota c_0 P_{IU}^t}{s_e} d_0^{-\iota-1} \mathrm{d}d_0 \mathrm{d}g \tag{6.56}$$

Central Limit Theorem and the Law of Large Numbers, $I = \sum_{i=1}^{\rho_1 n_s \pi l^2} P_i^h g_{v_1} + \sum_{i=1}^{\rho_2 \pi l^2} P_i^m g_{v_2}$ can be approximated by a normal distribution, $I \sim N(\mu_I, \sigma_I^2)$, where

$$\begin{aligned} \mu_I &= \sum_{i=1}^{\rho_1 n_s \pi l^2} P_i^h \bar{g}_{v_1} + \sum_{i=1}^{\rho_2 \pi l^2} P_i^m \bar{g}_{v_2}, \\ \sigma_I^2 &= \sum_{i=1}^{\rho_1 n_s \pi l^2} (P_i^h)^2 \sigma_{g_{v_1}}^2 + \sum_{i=1}^{\rho_2 \pi l^2} (P_i^m)^2 \sigma_{g_{v_2}}^2. \end{aligned} \tag{6.57}$$

6.6.4 Determine ESCs' interference constraints

In Section 6.6.2 and 6.6.3, we approximate C_e and I by normal distributions. The remaining problem to solve $U(\mathbf{T_E}) \geq \Psi$ in (6.33) is how each ESC e independently chooses a proper value of T_e. To achieve this, we rewrite (6.33) to:

$$U(\mathbf{T_E}) = Pr\Big(\sum_{i=1}^{\rho_1 n_s \pi l^2} P_i^h g_{v_1} + \sum_{i=1}^{\rho_2 \pi l^2} P_i^m g_{v_2} \leq T \Big| \sum_{i=1}^{\rho_1 n_s \pi l^2} P_i^h g_{u_1} + \sum_{i=1}^{\rho_2 \pi l^2} P_i^m g_{u_2} \leq T_e, \forall e \in [1, m_2] \Big) \geq \Psi. \tag{6.58}$$

Given that g_{u_1}, g_{u_2}, g_{v_1} and g_{v_2} are all positive, and $I = \sum_{i=1}^{\rho_1 n_s \pi l^2} P_i^h g_{v_1} + \sum_{i=1}^{\rho_2 \pi l^2} P_i^m g_{v_2}$ and $C_e = \sum_{i=1}^{\rho_1 n_s \pi l^2} P_i^h g_{u_1} + \sum_{i=1}^{\rho_2 \pi l^2} P_i^m g_{u_2}$, we have:

$$\begin{aligned}&Pr\left(I \le T\left|C_e \le T_e, \text{for all } e\right.\right)\\ \ge &Pr\left(I \le T\left|C_e \le T_e, \text{for some } e\right.\right)\\ \ge &Pr\left(I \le T\left|C_e = T_e, \text{for some } e\right.\right)\end{aligned} \tag{6.59}$$

Thus, so long as each ESC sensor e independently computes a T_e that satisfies the following inequality:

$$Pr\left(I \le T\left|C_e = T_e\right.\right) \ge \Psi, \tag{6.60}$$

we know (6.58) must hold, meaning that IU's interference requirement is statistically guaranteed.

Based on the theory of conditional normal distribution [90], the conditional random variable $I|C_e = T_e$ is also normally distributed, with expectation μ_{Ie} and variance σ_{Ie} computed by:

$$\mu_{Ie} = \mu_I + \frac{\Sigma_{12}}{\Sigma_{22}}(T_e - \mu_e), \tag{6.61}$$

$$\sigma_{Ie} = \Sigma_{11} - \frac{\Sigma_{12}^2}{\Sigma_{22}}, \tag{6.62}$$

$$\text{where } \Sigma_{11} = cov(I, I), \Sigma_{12} = cov(I, C_e), \tag{6.63}$$

$$\Sigma_{22} = cov(C_e, C_e), \tag{6.64}$$

where function $cov(\cdot)$ calculates the covariance of the two input distributions. Since the distribution of $I|C_e = T_e$ is known, given a Ψ, the value of μ_{Ie}, denoted as μ_0, that makes $Pr\left(I \le T\left|C_e = T_e\right.\right) \ge \Psi$ can be computed as:

$$\mu_0 = T_e - \sigma_{Ie}\Phi^{-1}(\Psi), \tag{6.65}$$

Here, $\Phi^{-1}(\cdot)$ is the quantile function of standard normal distribution. Thus, based on (6.61), T_e can be calculated by

$$T_e = (\mu_0 - \mu_I)\frac{\Sigma_{22}}{\Sigma_{12}} + \mu_e. \tag{6.66}$$

(6.66) is the formula used by each ESC e to generate T_e locally as its interference requirement. By using a proper T_e in the adaptive algorithm described in (6.6), the IU's interference requirement is statistically guaranteed.

6.6.5 Multiple IU Cases

So far only the scenario with one IU is considered. However, the way to handle multiple IUs in ESC requirement computation is straightforward. If an ESC e detects the existence of multiple IUs, it can simply compute the constraint threshold for each IU and choose the minimum one as final T_e, such that (5.44) is guaranteed for every IU.

6.7 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 ESCs are responsible for detecting an IU's existence in the spectrum and measuring the average received IU signal strength. ESCs are the only entities that obtain 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, BSs, SUs or the communication channel. The attacker will attempt to derive sensitive IU location data from information that they observed.

According to (6.6) - (6.13) and Section 5.5, each ESC e uses the average detected IU signal strength s_e to generate its interference requirement T_e and computes Δ_e to be sent to SAS. The minimum value Δ of Δ_es is then forwarded to SUs. From the adversary's perspective, since Δ's and Δ_e's computation are both based on T_e, which are again related to the distance between IU and ESC e, Δ_e and Δ may carry some IU location information and can be used to infer the changes in IU's true location.

In this section, we mainly focus on the case with one IU to analyze the strength of Δ_e on IU location protection. If the attacker cannot infer IU location changes from Δ_es in this simple case, neither can he derive the IU location changes from Δ or in multiple IU cases. This is because Δ is the minimum value of $\Delta_e, e \in [1, m_2]$. Thus, it contains no additional information regarding IU locations comparing to Δ_es. In multiple IU cases, Δ_es calculated by ESC e in different iterations may not match to the same IU. Thus, Δ_e in this case may not have the consecutive location information of any IU, which makes deriving a single IU location change even harder comparing to a single IU case.

Consider a single IU case. To ensure that IU-ESC distance changes cannot be discovered in a sequence of Δ_e, our method increases the randomness in the value of Δ_e by using random numbers η_1 and η_2 in the generation of Δ_e as shown in equation (6.6). To analyze if the variations in Δ_e are related with the changes in IU's location, one can calculate the correlation and p-value between the sequence of Δ_e and the IU-ESC distances [92]. Correlation coefficient and p-value are often used together to measure the strength of the relationship between two variables. A lower p-value can be interpreted as a stronger relation between two sets of data, and a p-value higher than 0.05 means that the correlation is not statistically significant [92]. If the sequences of Δ_e and IU-ESC distances have a low correlation coefficient with a large p-value, we can say that the correlation between Δ_es and IU-ESC distances is not statistically significant, and the attacker can hardly use Δ_es to infer the IU's true location. Using this method, in evaluation section 6.8.3, we compute the correlation coefficient and p-value through 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 from Δ_e sequence.

6.8 Evaluation

In this section, we evaluate the performance of the proposed uplink power control algorithm by simulation. The simulation platform is MATLAB 2018a on a macOS Sierra with 2.7 GHz Intel Core i5 processor. Evaluation for the proposed algorithm is divided into two sets. The first set considers the scenario with static SUs and IUs, and the second set assumes the mobility of SUs and IUs. Both sets examine the secondary network utility, convergence speed of SU transmit power, SINR of SUs and the SU interference received at IU.

Figure 6.5 shows an example of our simulation setting. Both IUs and SUs can be mobile in the simulation, and cases with different speeds of IU and SU are evaluated in the second set of the simulation. In terms of parameter settings, the number of macro cell BS is set to $\{2, 5, 10\}$, the number of small cell BS is set to $\{2, 4, 6\}$, the number of SUs communicating with each BS is set to 15, and the ESC number is chosen from 2 to 4. The range of SU's minimum required SINR τ is selected from 30 to 100, and IU's maximum allowable interference T is set to $\{10^{-7}W, 10^{-6}W, 10^{-5}W\}$. Each ESC senses the interference from both SUs and IU 100 times per second. Each BS broadcasts the required information per 10 millisecond. We assume that in our algorithm the messages transmitted between entities are all 16-bit floating point numbers. By using time series compression with delta encoding [106, 107], the data transmission rate of each BS to its SUs is around 7 Mbps. Each SU reads its location information at a rate of 10Hz from a GPS sensor. A standard path loss model is applied for each SU. The path loss exponent ι is set to 4. The maximum SU transmit power is $1W$. The environment interference φ_i to BS i includes both the receiver noise and other environment noises, and is set to $-80dbm$. The parameters used by ESC to theoretically estimate its interference threshold are shown in Table 6.2.

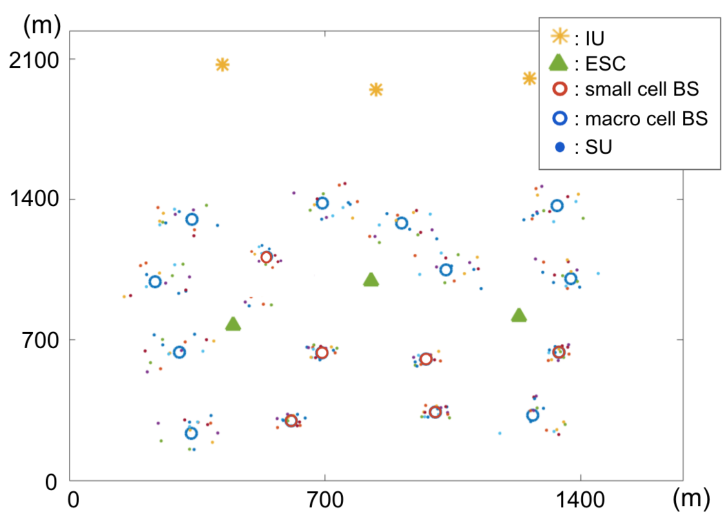

Figure 6.5: Example of our simulation settings.

Table 6.2: Parameter settings

Parameter	Description	Value
ρ_1	Density of cluster centers	$5 \times 10^{-6}/m^2$
ρ_2	Density of macro cell SUs	$1 \times 10^{-5}/m^2$
n_s	Avg. No. of hotspot SUs	15
σ_s	Scattering variance	$40m$
l	ESC sensing range	$1000m$
P_{IU}^t	IU's transmit power	$1000W$

6.8.1 Stability analysis

Case with static IU and SU

In the first set of simulation, we examine the algorithm's performance given static IU and SU.

Table 6.3 shows the average convergence speed of SU's transmit power. In this case, $\tau = 50$, $T = 10^{-6}W$, $numESC = 3$. The system is assumed to be stable when the fluctuations in transmit power are smaller than $0.0001W$. It can be observed that SU's transmit power converges quickly in less than 200 iterations. Only a slight increase in the convergence speed is observed as the total number of SU increases from 60 to 240, which indicates the good scalability of our algorithm.

Table 6.3: Average convergence speed of SU's transmit power

SU number	60	135	240
Avg. iterations used for convergence	139.2122	146.0846	151.3658

Next, we evaluate our algorithm's performance in achieving the maximum network utility (sum of SU rates) with a optimization solver called Global Search [108]. Global Search uses a multi-start framework designed to find global optima for pure and mixed integer nonlinear problems with many constraints and variables. We randomly generate 100 simulation settings for the comparison. Table 6.4 presents the ratio that the maximum network utility obtained by our algorithm is larger than the utility obtained by Global Search algorithm. We can see that our algorithm outperforms Global Search almost in every test. As mentioned, DCA converges quite often to a global solution in practice, Table 6.4 at least demonstrates that our algorithm performs better than a commonly used global solver in finding the global optima of the given uplink power control problem. Moreover, for each setting, the average running time of our algorithm for convergence is around 3.5 seconds, and it is much smaller than the running time of the Global Search algorithm which is around 70.5 seconds.

Table 6.5 shows the average percentage of SU satisfying its SINR requirement given different

Table 6.4: Comparison between our algorithm and global search

SU number	60	135	240
ratio	1	1	0.99

number of SUs and SU SINR requirements. We can observe that the amount of SUs who have their SINR guaranteed is gradually decreasing as the minimum required SINR grows. This is intuitive since it becomes more difficult to meet every SU's required SINR when all SUs are demanding for higher SINR. However, given a certain SINR, there is only a slight decrease in the percentage as the total SU number increases, which also indicates the good scalability of our algorithm.

Table 6.5: Ratio of SU satisfying its SINR requirement

total SU number / minimum SINR	60	135	240
30	0.9973	0.9876	0.9780
50	0.9324	0.9249	0.9203
70	0.8822	0.8625	0.8581
100	0.8112	0.8075	0.7898

We also calculate the ratio of IU satisfying its interference requirement under different parameter settings, where the number of SU ranges from 60 to 240, the number of ESC ranges from 2 to 4 and the IU's interference requirement is set to $\{10^{-7}W, 10^{-6}W, 10^{-5}W\}$. We observe from the results that the interference received by IU is guaranteed 100% of time to be below their requirements under all the above settings.

Case with mobile IU and SU

The second set of simulations takes the mobility of IU and SU into consideration. Each simulation lasts for 10 minutes (i.e. 60000 iterations). In the simulation, both ESC and BS broadcast their information per 10 ms, and SU updates its location information 10 times per second. The number of macro cell BS is set to 10 and the number of small cell BS's is 6. ESC number is set to 3 in this case.

We first set IU's moving speed to $10m/s$ and SU's moving speed to $1m/s$. In Table 6.6, it can be seen that each SU only takes around 2% of its total operation time in the convergence process through processing all the SUs' data. We can also observe that the average amount of time during which the SU's SINR is satisfied is gradually decreasing as the minimum required SINR grows, since it becomes more difficult to guarantee the SUs' target SINR if they are requiring for higher SINR. However, IU's interference requirement is satisfied 100%

of time, because our algorithm treats IU's interference constraint with higher priority than SU's SINR requirement. By using this algorithm, IU's interference requirement is statistically guaranteed by ESC's interference threshold in any case even when SUs' and IUs' constraints cannot be satisfied simultaneously (i.e. $\widetilde{S} = \emptyset$).

Table 6.6: Our algorithm's performance under different minimum SINR

minimum SINR	30	50	100
Ratio of time used for convergence per SU	0.0249	0.0251	0.0244
Ratio of time when SU's SINR is satisfied	0.9765	0.9221	0.7886
Ratio of time when IU's QoS is satisfied	1	1	1

Figure 6.6 shows our algorithm's convergence under different IU's and SU's moving speeds. In this case, the required SU SINR is set to 50. In the left figure of Figure 6.6, SU's moving speed is set to $1m/s$ and IU's moving speed varies from $1m/s$ to $30m/s$. We can see that the system's convergence time is not obviously influenced by the changes in IU's speed, because IU's location only affects the calculation of ESC's interference requirement which only provides an upper bound on SU's power adaptation step size. In the right figure of Figure 6.6, IU's moving speed is fixed to $10m/s$ and SU's moving speed ranges from $1m/s$ to $20m/s$ (e.g., from walking speed to freeway speed). It can be seen that the average convergence time per SU slightly increases as the SU's moving speed increases. It is intuitive because when an SU's speed increases, its movement within an iteration becomes larger and it becomes harder to converge. However, the observed increase is relatively small, which means our algorithm is not very sensitive to the SU's moving speed. In addition, by processing all the results, we also observe that IU's interference requirement is always guaranteed under different moving speeds of both SUs and IUs.

6.8.2 Efficiency evaluation

We compare our algorithm with the existing primary user (PU) protection schemes [93,94] in terms of network throughput under the same IU interference protection level. A geographic exclusion zone (GEZ) scheme in [93] calculates the minimum radius of the primary exclusion zone based on the primary outage constraint, and [94] 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 IU's interference requirement equal to $10^{-8}W$ and the number of SUs equal to 240, the minimum radius of exclusion zone in GEZ ends up to be 1000m and the number of SUs being switched off in DEZ becomes 70. Under these settings, our scheme can improve the total SU capacity by 56% over GEZ and by 48% over DEZ on average.

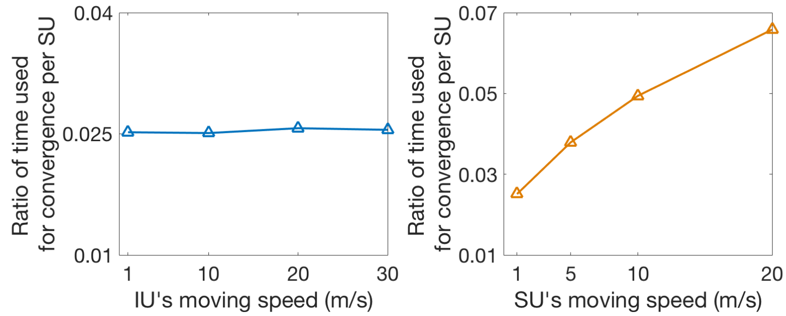

Figure 6.6: Left figure shows the ratio of time used for convergence per SU given different IU's moving speed, and the SU's speed is set to $1m/s$. Right figure shows the ratio of time used for convergence per SU given different SU's moving speed, and the IU's speed is set to $10m/s$

We also compare our algorithm with three power control algorithms all aiming at throughput maximization subjected to satisfying a minimum target SINR for all SUs. [62] developed an efficient centralized DC algorithm that achieves the global optimal throughput. A binary power control algorithm is proposed in [69] to maximize the total SU throughput in a CRN while limiting the interference to the PU within an acceptable range. [71] proposed a distributed algorithm aiming at maximizing the throughput with minimum power consumption.

In the evaluation, we assume 9 to 36 pairs of SU transmitters and receivers are distributed in a $500m \times 500m$ square. Note that because the formulation of [62] and [71] do not consider PU(IU) interference constraint, we assume the PU(IU) locates far enough from SU network, and hence the PU(IU) will not be affected by the SUs, the PU(IU) interference requirement in our algorithm and [69] will not be violated even when all SUs transmit at the maximum power simultaneously. 100 simulation settings are randomly generated for each number of SU pair. The average throughput of each algorithm is measured. From Figure 6.7, we can see that our algorithm outperforms binary algorithm [69] and the algorithm for energy efficiency and throughput maximization [71]. The average throughput achieved by our algorithm and centralized DC algorithm [62] are almost the same. This is because our algorithm and [62] both refer to Frank and Wolfe feasible direction algorithm [109] to locate the global optimal solution to the formulated non-convex problem.

6.8.3 Evaluation on IU location protection

In the evaluation of IU location protection, we randomly generate 500 settings of the locations of a moving IU, 3 ESCs and 240 static SUs. Each simulation with one setting lasts for 60000 iterations. Figure 6.8 zooms in for the 500 iterations of example sequences of IU-ESC distances and Δ_es. The average correlation coefficient between the sequences of IU-ESC distances and Δ_es is around 0.07 which can be considered negligible [95], and the p-value is

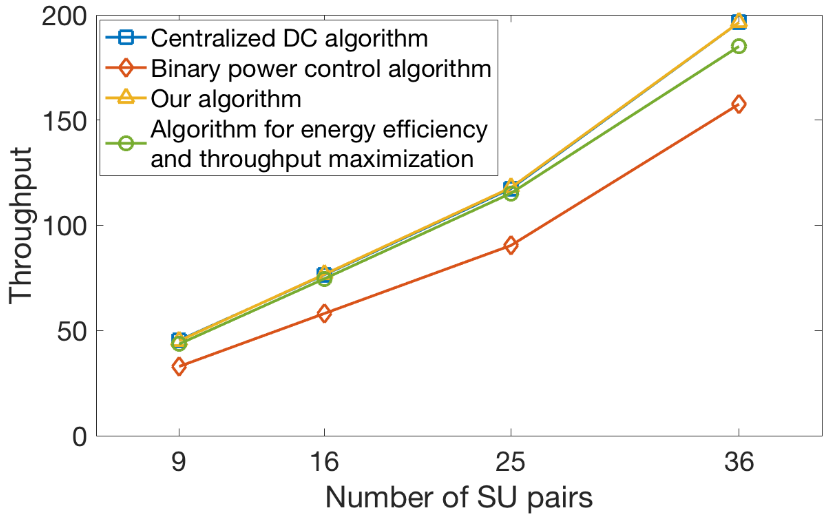

Figure 6.7: Comparison between our algorithm and three power control algorithms on throughput

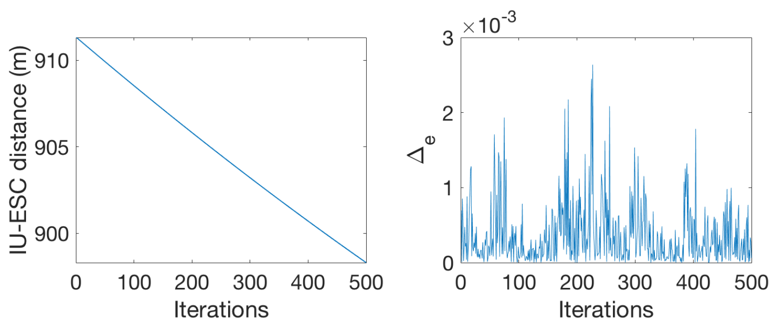

Figure 6.8: Left figure shows 500 iterations of one sequence of IU-ESC distances and right figure shows the corresponding Δ_e sequence.

around 0.31 which is much larger than 0.05 [92]. Hence, we can conclude that the correlation is not statically significant. Such low correlation indicates that it is difficult for an attacker to infer IU's true location from Δ_es.

6.9 Chapter Summary

In this chapter, we studied the uplink power control problem in 3.5 GHz DSA systems with the objective of utility maximization subject to SU's transmit power limit and SINR constraints and IU's interference constraints. Due to security considerations, the proposed distributed SU transmit power control algorithm does not depend on any sensitive information from IU. IU's interference requirement is proved to be guaranteed by our algorithm in any case. Each SU only requires locally observable measurements with aggregated insensitive information provided by ESCs and BSs to adjust its transmit power distributively. Our algorithm satisfies the CBRS OPSEC requirements for 3.5 GHz DSA. Through the analysis on the algorithm's convergence and stability properties, we demonstrate that our algorithm will converge to a stable optimal point which always satisfies the IU's interference constraint. SUs' SINR requirements will also be satisfied whenever the utility maximization problem is feasible. Finally, the simulation results demonstrate the effectiveness of our proposed algorithm.

Part IV

Future Work and Conclusions

Chapter 7

Future Work

As a future work, we are going to conduct two field experiments for validating the practical feasibility of the two algorithms proposed in III.

7.1 Field Experiment for Crowdsourcing-based Spectrum Monitoring

First, we are going to implement a crowdsouring based spectrum monitoring platform using the fast heuristic algorithm proposed in Section 3.3.2 with software defined radio (GNU Radio) and hardware (multiple USRP N210s and laptops), to verify the feasibility of the proposed crowdsouring spectrum monitoring algorithm.

The experiment setup of the spectrum monitoring field test is shown in Figure 7.1, which includes:

- A central controller: A Dell Inspiron personal computer. It is responsible for making the monitoring task assignments for SUs through the proposed Fast Heuristic algorithm.
- Multiple PUs: multiple WLAN routers located in Virginia Tech's Durham hall. In the experiment, the routers are selected to act as PUs which should not be mutually interfered when they are transmitting.
- Multiple SUs: two Ettus Research USRP (Universal Software Radio Peripheral) N210s. Two USRPs are used as SUs. They will be controlled by the proposed Fast Heuristic Spectrum monitoring algorithm. GNU Radio is selected as the software of choice to implement the spectrum monitoring scheme with the USRPs.

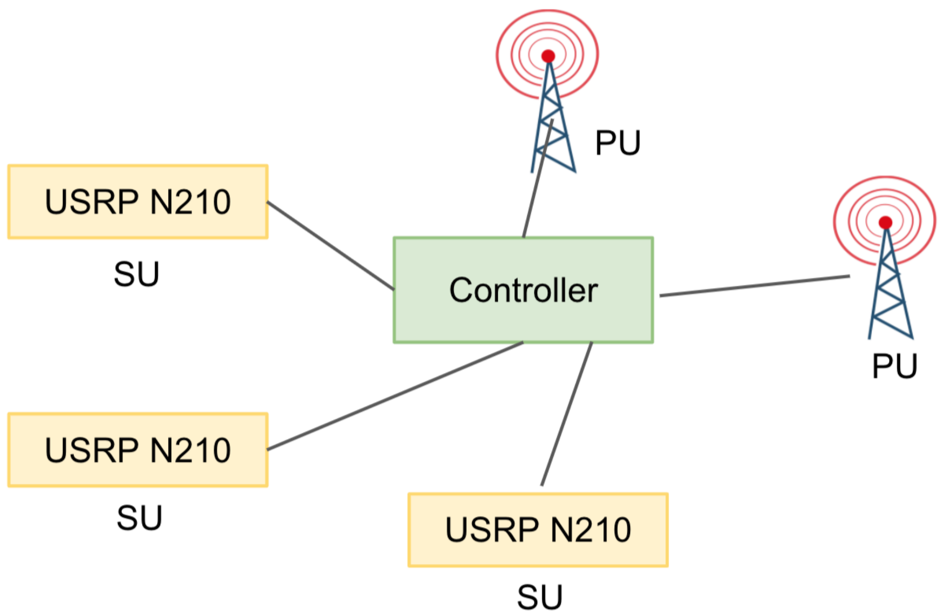

Figure 7.1: Experiment setting for crowdsourcing spectrum monitoring field test.

The reasoning behind choosing the USRP as the hardware of choice and GNU Radio as the software of choice has been covered in later subsections.

7.1.1 USRP and GNU Radio

The hardware devices that are going to be used in this spectrum monitoring field test are USRP N210s. USRP devices, which are developed by Ettus Research, are designed to work along with or support the open source SDR platform known as GNU Radio [110]. The USRP is perfect for implementations such as DSA schemes because of its high dynamic range processing capability. Typically a USRP consists of a motherboard for signal processing, multiple daughter boards, multiple extension sockets, an FPGA, ADCs, DACs and a Gigabit ethernet interface. Via this ethernet interface, the USRPs can connect to the host computer or central controller.

Specifically, the USRP N210 has several components including two 100 MSamples/second 14-bit ADCs and a FPGA [111]. These ADCs are used to down convert and demodulate the signals captured by the daughterboards. The FPGA is used to send the discrete signal samples to the host computer through the ethernet interface after converting them from continuous signals. One of the advantages of the N210 family of USRP devices (part of the Networked Series products developed by Ettus Research) is that it offers a Multiple Input Multiple Output (MIMO) capability, so that users can simultaneously use this device as a transmitter and a receiver.

GNU radio is one of the open source software toolkit that is able to work with USRP N210. The reason for choosing GNU radio is that all the modules for both transmitters and receivers in GNU radio are defined by software, and hence provide the users with a great deal of flexibility and convenience.

7.2 Field Experiment for IU Location Privacy Protection

To address the feasibility of the proposed IU location privacy protection algorithm (Section 4.3 and 4.4) in real world, we will implement the scenario of IU location privacy preservation in 2.4 GHz band. Since 3.5 GHz band is mainly registered for military and governmental use, we are not authorized to conduct the experiment on this frequency band, instead, we are going to build our prototype with the techniques in 2.4 GHz band which will also demonstrate our algorithm's feasibility in terms of real world application.

Our hardware platform will include a router playing the role of IU transmitter, a Yagi directional antenna attached to the router, a rotating plate which helps rotate the antenna, four laptops as the malicious ESCs, and a grid area. The router has a transmit power ranging from 0 dB to 30 dB, the directional antenna provides the antenna gain of 15 dBi with -3 dB beamwidth of 30 degree. Due to the hardware limitation, we cannot change the antenna gain of this antenna. Hence, instead of tuning the antenna gain and the router's transmit power independently, we decide to only tune the router's transmit power to control the final output power which is the sum of those two parameters in this experiment. Four laptops record the RSSI readings from the router with antenna. From Equation 4.4 and 4.5, we assume a transmitter with a rotating directional antenna is able to change its transmit power and antenna gain to the optimal values every time it faces with an ESC. To achieve this, in this experiment, we will manually rotate the antenna in the direction of a laptop before the laptop starts to record the RSSI readings. The RSSI is set to update at every 0.5 seconds, with a total length of 20 seconds. Then the average value is used as the final RSSI. The size of the grid area is decided as 5m $\times$ 4m so far, and it is uniformly divided into the grids with 0.5m $\times$ 0.5m in size.

Several adjustments should be done to guarantee the repeatability of the experiment and reduce the experimental error. Due to the small size of the predetermined grid area, pathloss vectors will be influenced by the locations of the antenna and laptops in vertical direction, and the RSSI readings will be further affected. Hence, we need to place the antenna and the laptop on the same horizontal plan. Note that in the DSA scenario, the distance between IU and ESC is much larger than the distance in our field test, RSSI error caused by vertical difference between IU and ESC's locations is negligible. In the field test, to ensure that the antenna is accurately faced with the laptop, we will determine the antenna's output direction to be perpendicular to the back of the laptop. Moreover, we will fix a laser pointer on the center of upper surface of the antenna so that we can make sure the antenna always target the same point at one laptop precisely.

According to the theoretical analysis in Section 4.4 and the proposed heuristic algorithm in Table 4.3, temporarily we design the experiment procedure as following, which is divided into three steps:

1. Step 1: Given a setting of receiver laptop placement and the router's predetermined trace, we calculate the optimal transmit power $Ptw\_opt(t)$ for the router at each time step in the simulation, based on Table 4.5.

2. Step 2: According to the algorithm in Table 4.3, for every grid, we determine if it is a possible location of the router whose transmit power is set to the simulated optimal power $Ptw\_opt(t)$ from Step 1.

3. Step 3: Last, we narrow down these $Z(Ptw\_opt(t))$ based on Step 2 and 3 in Table 4.4.

Through this procedure, we are able to obtain the maximized possible locations of the router at each time step based on field test results.

7.3 Fairness Considerations in distributed SU power control

Efficiency and user fairness are two mostly concerned metrics for power control algorithms. In the two proposed power control algorithms, we did not take user fairness into consideration. Hence, in the future work, we will add SUs' SINR fairness into problem formulation. Some commonly seen SINR fairness definitions include $\alpha-$fairness, max-min fairness and weighted sum-SINR fairness, etc. Moreover, the scenario with selfish users where each SU competes to maximize its own utility would be another project to work on.

Chapter 8

Conclusions

DSA is a powerful approach to solve the spectrum scarcity problem caused by rapid increase in wireless communication demands. Based on architecture design, DSA systems can be classified as centralized and distributed. In this dissertation, we study the spectrum management issues in both types of systems, particularly the spectrum sensing issues with IU location privacy issues in centralized DSA, and the spectrum sharing problems in distributed DSA systems.

First, Part I including Chapter 1 and Chapter 2 provides the introduction and background related to the dissertation topics.

In Part II, we focus on the spectrum sensing issues in centralized DSA.

For the topic of centralized spectrum monitoring, a novel crowdsourcing based spectrum monitoring system is presented in Chapter 3 in Part II. To improve efficiency and reduce the cost for complicated infrastructure, our algorithm intelligently schedules the monitoring tasks for masses of portable mobile devices, by leveraging the practical spectrum usage data. We propose two algorithms based on the uneven distribution of the intervals between occurrences of each PU pattern, which can be learnt from history. One of the algorithms is for existing pattern monitoring and another aims at unknown pattern monitoring. Simulation results show that our system achieves a high spectrum monitoring coverage. Our system is also capable of running efficiently even when no historical spectrum information is available.

Since the central controller usually requires IU presence information obtained during spectrum sensing to efficiently coordinate SU access, IU privacy protection becomes a big concern in spectrum management. In Chapter 4 in Part II, 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 enhances the IU's location privacy protection even in the worst case where all ESCs are compromised.

In Part III, we study the spectrum sharing issues in distributed DSA, particularly the power control problems with different objectives.

As mentioned, in a DSA system, SUs can only be permitted to access the licensed bands if these SUs will not cause any harmful interference to the IUs. Hence, adaptive SU power control can be a viable way to ensure an SU can obtain such transmission permission to coexist with IUs. In Chapter 5 in Part III, we proposed a distributed SU transmit power control algorithm aiming at minimizing the system's power consumption, subject to IU's interference requirement and SU-TXs' SINR requirements and upper power constraints. To meet the CBRS OPSEC requirements, our algorithm does not require IUs' location information or IUs' participation in the power control in SU networks. 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.

Chapter 6 in Part III investigates the uplink power control problem in 3.5 GHz DSA systems. This problem is similar to the power control problem in Chapter 5, but with a totally different objective. The objective function of this problem is uplink utility maximization subjected to SU's transmit power limit and the minimum required SINR and IU's interference requirements. Due to security considerations, the proposed distributed SU transmit power control algorithm does not depend on any sensitive information from IU. To adjust the transmit power distributively, each SU only requires locally observable measurements with some insensitive IU information which undergoes a security masking process. Through the analysis on the algorithm's convergence and stability properties, we demonstrate that our algorithm will converge to a stable optimal point which satisfies the IU's interference requirement in any case. SUs' SINR requirements will also be satisfied whenever the utility maximization problem is feasible. The effectiveness of our proposed algorithm is demonstrated through simulations. Since only masked values are shared among participating entities in our algorithm, even if the information is leaked, an adversary will not be able to infer sensitive information of the IU.

Finally, Part IV discussed the future work and concludes this dissertation.

Bibliography

[1] *United states frequency allocations: The radio spectrum.*, 2016.

[2] S Roy, K Shin, A Ashok, M McHenry, G Vigil, S Kannam, and D Aragon. Cityscape: A metro-area spectrum observatory. In *Computer Communication and Networks (ICCN), 2017 26th International Conference on*, pages 1–9. IEEE, 2017.

[3] Min Song, Chunsheng Xin, Yanxiao Zhao, and Xiuzhen Cheng. Dynamic spectrum access: from cognitive radio to network radio. *IEEE Wireless Communications*, 19(1), 2012.

[4] Sudeep Bhattarai, Jung-Min Jerry Park, Bo Gao, Kaigui Bian, and William Lehr. An overview of dynamic spectrum sharing: Ongoing initiatives, challenges, and a roadmap for future research. *IEEE Transactions on Cognitive Communications and Networking*, 2(2):110–128, 2016.

[5] Pradeep Reddy Vaka, Sudeep Bhattarai, and Jung-Min Park. Location privacy of non-stationary incumbent systems in spectrum sharing. In *Global Communications Conference (GLOBECOM), 2016 IEEE*, pages 1–6. IEEE, 2016.

[6] 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.

[7] Kang G Shin, Hyoil Kim, Alexander W Min, and Ashwini Kumar. Cognitive radios for dynamic spectrum access: from concept to reality. *IEEE Wireless Communications*, 17(6), 2010.

[8] Gbenga Salami, Olasunkanmi Durowoju, Alireza Attar, Oliver Holland, Rahim Tafazolli, and Hamid Aghvami. A comparison between the centralized and distributed approaches for spectrum management. *IEEE Communications Surveys & Tutorials*, 13(2):274–290, 2010.

[9] Ian F Akyildiz, Won-Yeol Lee, Mehmet C Vuran, and Shantidev Mohanty. A survey on spectrum management in cognitive radio networks. *IEEE Communications magazine*, 46(4):40–48, 2008.

[10] Hao Song. *Spectrum Management in Dynamic Spectrum Access: A Deep Reinforcement Learning Approach*. PhD thesis, Virginia Tech, 2019.

[11] Yousi Lin, Yuxian Ye, and Yaling Yang. Crowdsourcing-based spectrum monitoring at a large geographical scale. In *2019 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*, pages 1–10. IEEE, 2019.

[12] Jeff Howe. *Crowdsourcing: How the power of the crowd is driving the future of business*. Random House, 2008.

[13] Lixin Shi, Paramvir Bahl, and Dina Katabi. Beyond sensing: Multi-ghz realtime spectrum analytics. In *NSDI*, pages 159–172, 2015.

[14] Yanzhi Dou, Kexiong Curtis Zeng, He Li, Yaling Yang, Bo Gao, Chaowen Guan, Kui Ren, and Shaoqian 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*, pages 321–330. ACM, 2016.

[15] S Joshi, KBS Manosha, M Jokinen, T Hänninen, Pekka 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.

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

[17] Jonathan R Agre and Karen D Gordon. Summary of recent federal government activities to promote spectrum sharing, 2015.

[18] 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.

[19] 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.

[20] 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.

[21] 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.

[22] 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.

[23] 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.

[24] Liang Zheng, Chee Wei Tan, et al. Cognitive radio network duality and algorithms for utility maximization. *IEEE Journal on Selected Areas in Communications*, 31(3):500–513, 2013.

[25] Chee Wei Tan. Optimal power control in rayleigh-fading heterogeneous wireless networks. *IEEE/ACM Transactions on Networking*, 24(2):940–953, 2015.

[26] Mohamed Medhat Tawfik Abdelraheem. *Spectrum-efficient Cooperation and Bargaining-based Resource Allocation for Secondary Users in Cognitive Radio Networks*. PhD thesis, Virginia Tech, 2015.

[27] Qing Zhao and Brian M Sadler. A survey of dynamic spectrum access. *IEEE signal processing magazine*, 24(3):79–89, 2007.

[28] Tevfik Yucek and Huseyin Arslan. A survey of spectrum sensing algorithms for cognitive radio applications. *IEEE communications surveys & tutorials*, 11(1):116–130, 2009.

[29] Berk Canberk, Ian F Akyildiz, and Sema Oktug. Primary user activity modeling using first-difference filter clustering and correlation in cognitive radio networks. *IEEE/ACM Transactions on Networking*, 19(1):170–183, 2010.

[30] Chowdhury Shahriar, Shabnam Sodagari, and T Charles Clancy. Physical-layer security challenges of dsa-enabled td-lte. In *Proceedings of the 4th International Conference on Cognitive Radio and Advanced Spectrum Management*, pages 1–6, 2011.

[31] Tanuja S Dhope. *Cognitive radio networks optimization with spectrum sensing algorithms*, volume 44. River Publishers, 2015.

[32] Chao Zou and Chunxiao Chigan. On game theoretic dsa-driven mac for cognitive radio networks. *Computer Communications*, 32(18):1944–1954, 2009.

[33] Qing Zhao, Lang Tong, and Ananthram Swami. Decentralized cognitive mac for dynamic spectrum access. In *First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005.*, pages 224–232. IEEE, 2005.

[34] Jian Chen, Hewu Li, Jianping Wu, and Rui Zhang. Starp: a novel routing protocol for multi-hop dynamic spectrum access networks. In *Proceedings of the 1st ACM workshop on Mobile internet through cellular networks*, pages 49–54, 2009.

[35] Lei Ding, Tommaso Melodia, Stella N Batalama, and John D Matyjas. Distributed routing, relay selection, and spectrum allocation in cognitive and cooperative ad hoc networks. In *2010 7th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON)*, pages 1–9. IEEE, 2010.

[36] Lei Ding, Tommaso Melodia, Stella Batalama, and Michael J Medley. Rosa: distributed joint routing and dynamic spectrum allocation in cognitive radio ad hoc networks. In *Proceedings of the 12th ACM international conference on Modeling, analysis and simulation of wireless and mobile systems*, pages 13–20, 2009.

[37] Snehal Chitnavis and Andres Kwasinski. Cross layer routing in cognitive radio networks using deep reinforcement learning. In *2019 IEEE Wireless Communications and Networking Conference (WCNC)*, pages 1–6. IEEE, 2019.

[38] Haoyi Xiong, Daqing Zhang, Leye Wang, J Paul Gibson, and Jie Zhu. Eemc: Enabling energy-efficient mobile crowdsensing with anonymous participants. *ACM Transactions on Intelligent Systems and Technology (TIST)*, 6(3):39, 2015.

[39] Ana Nika, Zengbin Zhang, Xia Zhou, Ben Y Zhao, and Haitao Zheng. Towards commoditized real-time spectrum monitoring. In *Proceedings of the 1st ACM workshop on Hot topics in wireless*, pages 25–30. ACM, 2014.

[40] Ana Nika, Zhijing Li, Yanzi Zhu, Yibo Zhu, Ben Y Zhao, Xia Zhou, and Haitao Zheng. Empirical validation of commodity spectrum monitoring. In *Proceedings of the 14th ACM Conference on Embedded Network Sensor Systems CD-ROM*, pages 96–108. ACM, 2016.

[41] Mariya Zhivkova Zheleva, Ranveer Chandra, Aakanksha Chowdhery, Paul Garnett, Anoop Gupta, Ashish Kapoor, and Matt Valerio. Enabling a nationwide radio frequency inventory using the spectrum observatory. *IEEE Transactions on Mobile Computing*, 17(2):362–375, 2018.

[42] Fulong Ma, Xiao Liu, Anfeng Liu, Ming Zhao, Changqin Huang, and Tian Wang. A time and location correlation incentive scheme for deep data gathering in crowdsourcing networks. *Wireless Communications and Mobile Computing*, 2018, 2018.

[43] Dejun Yang, Guoliang Xue, Xi Fang, and Jian Tang. Crowdsourcing to smartphones: Incentive mechanism design for mobile phone sensing. In *Proceedings of the 18th annual international conference on Mobile computing and networking*, pages 173–184. ACM, 2012.

[44] Juong-Sik Lee and Baik Hoh. Sell your experiences: a market mechanism based incentive for participatory sensing. In *2010 IEEE International Conference on Pervasive Computing and Communications (PerCom)*, pages 60–68. IEEE, 2010.

[45] Chi Harold Liu, Bo Zhang, Xin Su, Jian Ma, Wendong Wang, and Kin K Leung. Energy-aware participant selection for smartphone-enabled mobile crowd sensing. *IEEE Systems Journal*, 11(3):1435–1446, 2017.

[46] Chi Harold Liu, Jun Fan, Pan Hui, Jie Wu, and Kin K Leung. Toward qoi and energy efficiency in participatory crowdsourcing. *IEEE Transactions on Vehicular Technology*, 64(10):4684–4700, 2014.

[47] Wendong Wang, Hui Gao, Chi Harold Liu, and Kin K Leung. Credible and energy-aware participant selection with limited task budget for mobile crowd sensing. *Ad Hoc Networks*, 43:56–70, 2016.

[48] Yu Zhang and Mihaela van der Schaar. Robust reputation protocol design for online communities: A stochastic stability analysis. *IEEE Journal of Selected Topics in Signal Processing*, 7(5):907–920, 2013.

[49] Leydy Johana Hernández Viveros, Danilo Alfonso López Sarmiento, and Nelson Enrique Vera Parra. Modeling and prediction primary nodes in wireless networks of cognitive radio using recurrent neural networks. 2018.

[50] Mariya Zheleva, Ranveer Chandra, Aakanksha Chowdhery, Ashish Kapoor, and Paul Garnett. Txminer: Identifying transmitters in real-world spectrum measurements. In *Dynamic Spectrum Access Networks (DySPAN), 2015 IEEE International Symposium on*, pages 94–105. IEEE, 2015.

[51] Cengis Hasan and Mahesh K Marina. Channel vacancy forecasting for communication-free inter-operator spectrum sharing in small cell networks.

[52] Jae-Chern Yoo and Tae Hee Han. Fast normalized cross-correlation. *Circuits, systems and signal processing*, 28(6):819, 2009.

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

[54] 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.

[55] 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.

[56] 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 *Distributed Computing Systems (ICDCS), 2017 IEEE 37th International Conference on*, pages 2486–2493. IEEE, 2017.

[57] 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.

[58] 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.

[59] Han Xiao, Hao Zhang, Zengfeng Wang, and T Aaron Gulliver. An rssi based dv-hop algorithm for wireless sensor networks. In *Communications, Computers and Signal Processing (PACRIM), 2017 IEEE Pacific Rim Conference on*, pages 1–6. IEEE, 2017.

[60] Jiang Xiao, Zimu Zhou, Youwen Yi, and Lionel M Ni. A survey on wireless indoor localization from the device perspective. *ACM Computing Surveys (CSUR)*, 49(2):25, 2016.

[61] Ting Wang and Yaling Yang. Analysis on perfect location spoofing attacks using beamforming. In *INFOCOM, 2013 Proceedings IEEE*, pages 2778–2786. IEEE, 2013.

[62] Ha Hoang Kha, Hoang Duong Tuan, and Ha H Nguyen. Fast global optimal power allocation in wireless networks by local dc programming. *IEEE Transactions on Wireless Communications*, 11(2):510–515, 2011.

[63] Saeed Ashrafinia, Udit Pareek, Muhammad Naeem, and Daniel Chonghwan Lee. Binary artificial bee colony for cooperative relay communication in cognitive radio systems. In *2012 IEEE International Conference on Communications (ICC)*, pages 1550–1554. IEEE, 2012.

[64] Liang Zheng and Chee Wei Tan. Maximizing sum rates in cognitive radio networks: Convex relaxation and global optimization algorithms. *IEEE Journal on Selected Areas in Communications*, 32(3):667–680, 2013.

[65] E Kayalvizhi and Balamurugan Gopalakrishnan. Estimation of optimal channel gain in cognitive radio networks using bisectional algorithm. *International Journal of Advanced Networking and Applications*, 11(1):4171–4176, 2019.

[66] Wireless Innovation Forum. Cbrs operational security. *WINNF-15-S-0071*, October 1, 2016.

[67] Yongjun Xu and Xiaohui Zhao. Robust power control for multiuser underlay cognitive radio networks under qos constraints and interference temperature constraints. *Wireless personal communications*, 75(4):2383–2397, 2014.

[68] Yongjun Xu and Xiaohui Zhao. Distributed power control for multiuser cognitive radio networks with quality of service and interference temperature constraints. *Wireless Communications and Mobile Computing*, 15(14):1773–1783, 2015.

[69] Dharati Nakhale and Mohammed Zafar Ali Khan. Fast binary power allocation for uplink distributed cognitive radio networks. In *2018 10th International Conference on Communication Systems & Networks (COMSNETS)*, pages 435–438. IEEE, 2018.

[70] 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.

[71] Rojin Aslani and Mehdi Rasti. A distributed power control algorithm for energy efficiency maximization in wireless cellular networks. *IEEE Wireless Communications Letters*, 9(11):1975–1979, 2020.

[72] Fatemeh Shah-Mohammadi, Hatem Hussein Enaami, and Andres Kwasinski. Neural network cognitive engine for autonomous and distributed underlay dynamic spectrum access. *IEEE Open Journal of the Communications Society*, 2:719–737, 2021.

[73] Federal Communication Commission. Facilitating shared use in the 3.1-3.55 ghz band. February 24, 2021.

[74] Federal Communication Commission. 47 cfr part 96 - citizens broadband radio service. October 1, 2016.

[75] Hubert Schreier, Jean-José Orteu, and Michael A Sutton. *Image correlation for shape, motion and deformation measurements*. Springer US, 2009.

[76] Michal Piorkowski, Natasa Sarafijanovic-Djukic, and Matthias Grossglauser. CRAWDAD dataset epfl/mobility (v. 2009-02-24). Downloaded from https://crawdad.org/epfl/mobility/20090224/cab, February 2009. traceset: cab.

[77] Daniel T Wagner, Andrew Rice, and Alastair R Beresford. Device analyzer: Understanding smartphone usage. In *International Conference on Mobile and Ubiquitous Systems: Computing, Networking, and Services*, pages 195–208. Springer, 2013.

[78] Roberto Vescovo. Pattern synthesis with null constraints for circular arrays of equally spaced isotropic elements. *IEE Proceedings-Microwaves, Antennas and Propagation*, 143(2):103–106, 1996.

[79] D Oo North. An analysis of the factors which determine signal/noise discrimination in pulsed-carrier systems. *Proceedings of the IEEE*, 51(7):1016–1027, 1963.

[80] Neelakantan Nurani Krishnan, Ratnesh Kumbhkar, Narayan B Mandayam, Ivan Seskar, and Sastry Kompella. Coexistence of radar and communication systems in cbrs bands through downlink power control. In *MILCOM 2017-2017 IEEE Military Communications Conference (MILCOM)*, pages 713–718. IEEE, 2017.

[81] Frank H Sanders, Robert L Sole, Brent L Bedford, David Franc, and Timothy Pawlowitz. Effects of rf interference on radar receivers. *NTIA Report TR-06-444*, 2006.

[82] 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.

[83] 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.

[84] 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.

[85] 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.

[86] 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.

[87] 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.

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

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

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

[91] Wireless Innovation Forum. Cbrs threat model technical report. *WINNF-15-P-0089*, 11 May 2016.

[92] 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.

[93] 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.

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

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

[96] Gary Locke and L Strickling. Plan and timetable to make available 500 megahertz of spectrum for wireless broadband. *US Department of Commerce, Washington, DC, USA*, 2010.

[97] P Kolodzy and I Avoidance. Spectrum policy task force federal commun. comm. 2002.

[98] Nalan Gulpinar, Le Thi Hoai An, and Mahdi Moeini. Robust investment strategies with discrete asset choice constraints using dc programming. *Optimization*, 59(1):45–62, 2010.

[99] Le Thi Hoai An. An efficient algorithm for globally minimizing a quadratic function under convex quadratic constraints. *Mathematical programming*, 87:401–426, 2000.

[100] Pham Dinh Tao and Le Thi Hoai An. A dc optimization algorithm for solving the trust-region subproblem. *SIAM Journal on Optimization*, 8(2):476–505, 1998.

[101] Senay Haile. Investigation of channel reciprocity for ofdm tdd systems. Master's thesis, University of Waterloo, 2009.

[102] Nicholas William Anderson. Uplink resource allocation to control intercell interference in a wireless communication system, September 20 2011. US Patent 8,023,955.

[103] Radha Krishna Ganti and Martin Haenggi. Interference and outage in clustered wireless ad hoc networks. *IEEE Transactions on Information Theory*, 55(9):4067–4086, 2009.

[104] Mehrnaz Afshang and Harpreet S Dhillon. Poisson cluster process based analysis of hetnets with correlated user and base station locations. *IEEE Transactions on Wireless Communications*, 17(4):2417–2431, 2018.

[105] Paul Hale, Jeffrey Jargon, Peter Jeavons, M Lofquist, M Souryal, and A Wunderlich. 3.5 ghz radar waveform capture at point loma. *NIST TN 1954*, 2017.

[106] Tuomas Pelkonen, Scott Franklin, Justin Teller, Paul Cavallaro, Qi Huang, Justin Meza, and Kaushik Veeraraghavan. Gorilla: A fast, scalable, in-memory time series database. *Proceedings of the VLDB Endowment*, 8(12):1816–1827, 2015.

[107] Jeffrey C Mogul, Fred Douglis, Anja Feldmann, and Balachander Krishnamurthy. Potential benefits of delta encoding and data compression for http. In *Proceedings of the ACM SIGCOMM'97 conference on Applications, technologies, architectures, and protocols for computer communication*, pages 181–194, 1997.

[108] Zsolt Ugray, Leon Lasdon, John Plummer, Fred Glover, James Kelly, and Rafael Martí. Scatter search and local nlp solvers: A multistart framework for global optimization. *INFORMS Journal on Computing*, 19(3):328–340, 2007.

[109] Pierre Apkarian and Hoang Duong Tuan. Robust control via concave minimization local and global algorithms. *IEEE Transactions on Automatic Control*, 45(2):299–305, 2000.

[110] D Casey Tucker and Gene A Tagliarini. Prototyping with gnu radio and the usrp-where to begin. In *IEEE Southeastcon 2009*, pages 50–54. IEEE, 2009.

[111] Ettus Research. Uhd - general application notes. `http://files.ettus.com/uhd_docs/manual/html/general.html`.

[112] Zhi-Quan Luo, Wing-Kin Ma, Anthony Man-Cho So, Yinyu Ye, and Shuzhong Zhang. Semidefinite relaxation of quadratic optimization problems. *IEEE Signal Processing Magazine*, 27(3):20–34, 2010.

Appendix A

A.1 Proof of Claim 1

To prove the feasibility of the problem in Table 4.2, let us consider a sub-problem, which is to determine whether a single l_i is a possible IU location:

Table A.1: Sub-problem

sub-problem:
find any $\boldsymbol{\omega}$, Pt, $\widehat{\boldsymbol{\omega}}$, $\widehat{Pt}$
that satisfy: $SINR \geq SNR_{min}$
$\left\| 10log_{10}\frac{\widehat{Pt}\left\|\widehat{\boldsymbol{\omega}}^H\widehat{\boldsymbol{h}_k}\right\|^2}{(\frac{4\pi}{\lambda}\widehat{d}_k)^2} - 10log_{10}\frac{Pt\left\|\boldsymbol{\omega}^H\boldsymbol{h_k}\right\|^2}{(\frac{4\pi}{\lambda}d_k)^2}\right\| \leq \delta$
$\forall k = 1, 2, \cdot, K$
$\Leftrightarrow \frac{1}{\delta'} \leq \left\| \frac{\widehat{Pt}\left\|\widehat{\boldsymbol{\omega}}^H\widehat{\boldsymbol{h}_k}\right\|^2}{(\frac{4\pi}{\lambda}\widehat{d}_k)^2} / \frac{Pt\left\|\omega^H\boldsymbol{h_k}\right\|^2}{(\frac{4\pi}{\lambda}d_k)^2}\right\| \leq \delta'$

In Table A.1, SINR at a radar receiver is computed using Equation (6.2a), SNR_{min} is calculated based on Equation (4.6) 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 A.2.

The relaxed sub-problem is feasible if and only if the solution t^* to complementary problem in Table A.2 satisfies $t^* \geq \frac{1}{\delta'}$ and it is infeasible if and only if $t^* < \frac{1}{\delta'}$. Conversely, assume

Table A.2: Complementary problem and equivalent problem

complementary problem:
$\max\limits_{\boldsymbol{\omega}, Pt, \widehat{\boldsymbol{\omega}}, \widehat{Pt}} \ t = \min\limits_{k} \left\{ \frac{\widehat{Pt}\left\|\widehat{\boldsymbol{\omega}}^H \widehat{\boldsymbol{f}_k}\right\|^2}{Pt\|\boldsymbol{\omega}^H \boldsymbol{f_k}\|^2} \right\}_{k=1}^{K}$
s.t. $\frac{\widehat{Pt}\left\|\widehat{\boldsymbol{\omega}}^H \widehat{\boldsymbol{f}_k}\right\|^2}{Pt\|\boldsymbol{\omega}^H \boldsymbol{f_k}\|^2} \leq \delta'$, $k = 1, 2, \cdot, K$.
equivalent problem:
find any $\boldsymbol{\omega}$, Pt, $\widehat{\boldsymbol{\omega}}$, $\widehat{Pt}$
that satisfy: $\eta \leq \frac{\widehat{Pt}\left\|\widehat{\boldsymbol{\omega}}^H \widehat{\boldsymbol{f}_k}\right\|^2}{Pt\|\boldsymbol{\omega}^H \boldsymbol{f_k}\|^2} \leq \delta'$
$\forall k = 1, 2, \cdot, K$

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 A.2 in polynomial time.

Comparing two problems in Table A.2, 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 A.2 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 A.2. 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 A.2 to problem in Table A.1 is also polynomial. Hence, to prove that relaxed sub-problem is NP-hard, we can first show complementary problem in Table A.2 is NP-hard.

Now consider the case where the solution to complementary problem in Table A.2 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 A.3.

Table A.3: Equivalent problem

$\max\limits_{\boldsymbol{\omega}, Pt, \widehat{\boldsymbol{\omega}}, \widehat{Pt}} \frac{\widehat{Pt}\left\|\widehat{\boldsymbol{\omega}}^H \widehat{\boldsymbol{f}_k^*}\right\|^2}{Pt\left\|\boldsymbol{\omega}^H \boldsymbol{f_k^*}\right\|^2}$
s.t. $\frac{\widehat{Pt}\left\|\widehat{\boldsymbol{\omega}}^H \widehat{\boldsymbol{f}_k}\right\|^2}{Pt\|\boldsymbol{\omega}^H \boldsymbol{f_k}\|^2} \leq \delta'$
$\frac{\widehat{Pt}\left\|\widehat{\boldsymbol{\omega}}^H \widehat{\boldsymbol{f}_k}\right\|^2}{Pt\|\boldsymbol{\omega}^H \boldsymbol{f_k}\|^2} \geq \frac{\widehat{Pt}\left\|\widehat{\boldsymbol{\omega}}^H \widehat{\boldsymbol{f}_k^*}\right\|^2}{Pt\left\|\boldsymbol{\omega}^H \boldsymbol{f_k^*}\right\|^2}$

To 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 A.4.

Table A.4: A multivariate optimization problem

$$\max_{\boldsymbol{\omega}, Pt, \widehat{\boldsymbol{\omega}}, \widehat{Pt}} \; log\ \widehat{Pt} - log\ Pt + log\ \left|\widehat{\boldsymbol{\omega}}^H \widehat{\boldsymbol{f}}_k\right|^2 - log\ \left|\boldsymbol{\omega}^H \boldsymbol{f_k}\right|^2$$

$$\text{s.t. } \frac{\widehat{Pt}\left|\widehat{\boldsymbol{\omega}}^H \widehat{\boldsymbol{f}}_k\right|^2}{Pt\left|\boldsymbol{\omega}^H \boldsymbol{f_k}\right|^2} \leq \delta'$$

$$\frac{\widehat{Pt}\left|\widehat{\boldsymbol{\omega}}^H \widehat{\boldsymbol{f}}_k\right|^2}{Pt\left|\boldsymbol{\omega}^H \boldsymbol{f_k}\right|^2} - \frac{\widehat{Pt}\left|\widehat{\boldsymbol{\omega}}^H \widehat{\boldsymbol{f}}_k^*\right|^2}{Pt\left|\boldsymbol{\omega}^H \boldsymbol{f}_{\boldsymbol{k}}^*\right|^2} \geq 0$$

$$\Leftrightarrow \widehat{\boldsymbol{\omega}}^H \left(\frac{\widehat{Pt}}{Pt\left|\boldsymbol{\omega}^H \boldsymbol{f}_{\boldsymbol{k}}^*\right|^2} \boldsymbol{f}_{\boldsymbol{k}}^* \boldsymbol{f}_{\boldsymbol{k}}^{*H} - \frac{\widehat{Pt}}{Pt\left|\boldsymbol{\omega}^H \boldsymbol{f_k}\right|^2} \boldsymbol{f_k} \boldsymbol{f_k}^H\right) \widehat{\boldsymbol{\omega}} \leq 0$$

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 A.4 is NP-hard too.

As observed in Table A.4, $\boldsymbol{f_k} \boldsymbol{f_k}^H$ now becomes a Hermitian positive semi-definite matrix and

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

is an indefinite matrix. Thus, the reduced problem is a non-convex quadratically constrained quadratic programming (QCQP) problem, which is NP-hard in general [112]. Thus, complementary problem in Table A.2 is NP-hard in general and so is sub-problem in Table A.1. Since the sub-problem should be computed for each l_i in order to solve the problem in Table 4.2, clearly problem in Table 4.2 is also NP-hard in general.

Appendix B

Theorem 5. *$K(\boldsymbol{\lambda}, \boldsymbol{P})$ defined in* (5.23) *is a Lyapunov function for the system defined in* (5.12) - (5.14). *In addition, $\dot{K} = 0$ if and only if $\boldsymbol{P} = \boldsymbol{P^*}$ and $\sum_i P_i g_{ie} < T_e$.*

Proof: The partial derivative of $F(\boldsymbol{\lambda}, \boldsymbol{P})$ in (5.23) over P_i and λ_e are derived as:

$$\frac{\partial F}{\partial P_i} = \frac{\partial F}{\partial W} \cdot \frac{\partial W}{\partial P_i} = \frac{\partial F}{\partial W} \cdot \frac{\partial V}{\partial P_i} \tag{B.1}$$

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

$$\frac{\partial F}{\partial \lambda_e} = f(W \sum_i g_{ie} - \xi_2 T_e) \cdot 2\lambda_e > 0 \tag{B.3}$$

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 (5.8) and (5.14) 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 (5.20). Moreover, given (5.24) and (5.25), 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

$$\dot{K} = \sum_i \frac{\partial K}{\partial P_i}\dot{P}_i + \sum_e \frac{\partial K}{\partial \lambda_e}\dot{\lambda}_e \tag{B.4}$$

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

$$\sum_e \frac{\partial K}{\partial \lambda_e}\dot{\lambda}_e = \sum_e \frac{\partial F}{\partial \lambda_e} 2\lambda_e \beta_e \left(-f(\sum_i P_i g_{ie} - \xi_2 T_e) \right) \leq 0, \tag{B.5}$$

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 (5.21), (5.22), (B.1),

$$\begin{aligned} \sum_i \frac{\partial K}{\partial P_i}\dot{P}_i &= \sum_i \frac{\partial F}{\partial P_i} \left(\tilde{\dot{P}}_i + \sum_e \Omega_e g_{ie} \tilde{\dot{P}}_i \right) \\ &= \sum_i \frac{\partial F}{\partial W} \left(1 + \sum_e \Omega_e g_{ie} \right) \delta_i {y_i}^2 \leq 0 \end{aligned} \tag{B.6}$$

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.