Spectrum Efficiency and Security in Dynamic Spectrum Sharing

Sudeep Bhattarai

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
Electrical Engineering

Jung-Min (Jerry) Park, Chair
A. Lynn Abbott
Carl B. Dietrich
Yaling Yang
Danfeng Yao

February 22, 2018
Blacksburg, Virginia

Keywords: Dynamic Spectrum Access, Aggregate Interference, Dynamic Exclusion Zones, Spectrum Efficiency, 802.11ax, Operational Security.

Spectrum Efficiency and Security in Dynamic Spectrum Sharing

Sudeep Bhattarai

(ABSTRACT)

We are in the midst of a major paradigm shift in how we manage the radio spectrum. This paradigm shift in spectrum management from exclusive access to shared access is necessitated by the growth of wireless services and the demand pressure imposed on limited spectrum resources under legacy management regimes. The primary constraint in any spectrum sharing regime is that the incumbent users (IUs) of the spectrum need to be protected from harmful interference caused due to transmissions from secondary users (SUs). Unfortunately, legacy techniques rely on inadequately flexible and overly conservative methods for prescribing interference protection that result in inefficient utilization of the shared spectrum.

In this dissertation, we first propose an analytical approach for *characterizing the aggregate interference* experienced by the IU when it shares the spectrum with multiple SUs. Proper characterization of aggregate interference helps in defining incumbent protection boundaries—a.k.a. *Exclusion Zones (EZs)*[1]—that are neither overly aggressive to endanger the IU protection requirement, nor overly conservative to limit spectrum utilization efficiency. In particular, our proposed approach addresses the two main limitations of existing methods that use terrain-based propagation models for estimating the aggregate interference. First, terrain-based propagation models are computationally intensive and data-hungry making them unsuitable for large real-time spectrum sharing applications such as the spectrum access system (SAS)[2]. Second, terrain-based propagation models require accurate geo-locations of SUs which might not always be available, such as when SUs are mobile, or when their locations are obfuscated for location privacy concerns.

[1] An EZ is a spatial separation region around an IU where co-channel/adjacent channel SUs are not allowed to transmit

[2] The "Spectrum Access System" is a term used in recent Federal Communications Commission (FCC) notices and publications to denote a network of databases and supporting infrastructure deployed to enable dynamic spectrum sharing in the 3.5 GHz *Citizens Broadband Radio Service (CBRS)* band.

Our second contribution in this dissertation is the novel concept of *Multi-tiered Incumbent Protection Zones (MIPZ)* that can be used to prescribe interference protection to the IUs. Based on the aforementioned analytical tool for characterizing the aggregate interference, we facilitate a framework that can be used to replace the legacy notion of static and overly conservative EZs with multi-tiered dynamic EZs. MIPZ is fundamentally different from legacy EZs in that it dynamically adjusts the IU's protection boundary based on the radio environment, network dynamics, and the IU interference protection requirement. Our extensive simulation results show that MIPZ can be used to improve the overall spectrum utilization while ensuring sufficient protection to the IUs.

As our third contribution, we investigate the operational security (OPSEC) issue raised by the emergence of new spectrum access technologies and spectrum utilization paradigms. For instance, although the use of geolocation databases (GDB) is a practical approach for enabling efficient spectrum sharing, it raises a potentially serious OPSEC problem, especially when some of the IUs are federal government entities, including military users. We show that malicious queriers can readily infer the locations of the IUs even if the database's responses to the queries do not directly reveal such information. To address this issue, we propose a *perturbation-based optimal obfuscation strategy* that can be implemented by the GDB to preserve the location privacy of IUs. The proposed obfuscation strategy is optimal in the sense that it maximizes IUs' location privacy while ensuring that the expected degradation in the SUs' performance due to obfuscated responses does not exceed a threshold.

In summary, this dissertation focuses on investigating techniques that improve the utilization efficiency of the shared spectrum while ensuring adequate protection to the IUs from SU-induced interference as well as from potential OPSEC threats. We believe that this study facilitates the regulators and other stakeholders a better understanding of mechanisms that enable improved spectrum utilization efficiency and minimize the associated OPSEC threats, and hence, helps in wider adoption of dynamic spectrum sharing.

Spectrum Efficiency and Security in Dynamic Spectrum Sharing

Sudeep Bhattarai

(GENERAL AUDIENCE ABSTRACT)

Radio spectrum is a precious resource that enables wireless communications. On the one hand, the demand for wireless spectrum is skyrocketing due to the ever-increasing number of smartphones and other wireless devices. On the other hand, the total usable wireless spectrum is limited. As a result, we are at a stage where spectrum demand far exceeds the supply. Since spectrum is a finite resource, the only way to fulfill this demand is by sharing the spectrum dynamically among multiple users—i.e., by enabling "dynamic spectrum sharing" among different class of users and uses. In this dissertation, we seek to investigate methods and tools for improving the utilization efficiency of the shared spectrum as well as for ensuring the operational privacy and security of spectrum users in dynamic spectrum sharing. In doing so, we propose several novel approaches and demonstrate their efficacy in improving spectrum utilization efficiency and operational privacy by providing results from extensive simulations and relevant real-world case studies. We believe that studies of this kind facilitate the regulators and other stakeholders a better understanding of mechanisms that enable improved spectrum utilization efficiency and minimize the associated operational privacy and security threats—and hence, help in wider adoption of dynamic spectrum sharing.

Dedication

To my family...

parents, sister, wife,

for their unconditional love and support.

Acknowledgments

Throughout my graduate study, I have been fortunate to be blessed with the love, support and encouragement of many people including faculty, staff, colleagues, friends and family. It has been quite an eventful and enjoyable journey to finally arrive at this point. I would like to begin by thanking my loving family—my parents, sister and wife—whose unconditional love and support has always directed me towards a successful and meaningful life. This dissertation would not have been possible without their continuous encouragement, drive and support. Thank you for always being there for me.

I would like to express my sincere gratitude to my Ph.D. advisor, Dr. Jung-Min (Jerry) Park, for his generous support, great guidance and invaluable mentorship in my pursuit of academic excellence. I could not have made it to this point without his guidance and support. The academic and non-academic training that I have received under his supervision is the biggest asset I have ever earned, and I will cherish it forever. I would also like to thank Dr. A. Lynn Abbott, Dr. Carl Dietrich, Dr. Yaling Yang and Dr. Daphne Yao for being a part of my Ph.D. committee and for reviewing my work. Your helpful feedback during the preliminary exam were helpful in improving and balancing certain aspects of this dissertation.

My learning at graduate school has been further enriched with two valuable internship programs that I participated at AT&T Labs and Google. Both of these experiences have helped me understand the real-world perspective of my research. My sincere token to thanks goes to Dr. Jin Wang and Dr. Andrew Clegg for their passionate mentoring throughout these internship programs. I would also like to thank Dr. Preston Marshall for his continuous

motivation and encouragement throughout my internship at Google.

Next, I would like to offer a token of appreciation to my colleagues Behnam Bahrak, Vireshwar Kumar, Bo Gao, Abid Ullah, Seungmo Kim, Jinshan Liu, Gaurang Naik, Pradeep Vaka, He Li, Taiwo Oyedare and Dr. Hanif Rahbari from the ARIAS lab. You have played an important role in making some of my research ideas mature through group discussions, knowledge-sharing and feedback.

Lastly, I would like to thank all my friends and family in Blacksburg, who have made the last five years colorful, enjoyable and pleasantly memorable. Being far away from home is not easy, but you guys have helped me miss home less often. Finally, I am thankful to the entire Blacksburg community for so many great offerings and for witnessing the journey and experience of my graduate study. You will be in my memory, always.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Radio spectrum is a valuable resource. It is not only a key enabler of technological innovations in wireless communications, but it also plays an important role as an economic growth engine, as highlighted in the 2012 U.S. President's Council of Advisors on Science and Technology (PCAST) report,"*Realizing the full potential of government-held spectrum to spur economic growth*" [1]. The impact of spectrum on the national economy is expected to increase as the proliferation of wireless devices and applications of all types and for all uses accelerates[1]. This includes legacy and new users; communication and sensing applications; wide-area and local-area networks; commercial and government users; etc. As the demand for spectrum continues to skyrocket, it will become increasingly difficult, if not impossible, to meet that demand through the legacy spectrum policy based on the assignment of siloed, exclusive-use spectrum bands to particular applications. The legacy spectrum management regime is inadequately flexible, making it difficult to transition spectrum resources to new uses, users, and technologies as market conditions shift, further aggravating the spectrum scarcity associated with outmoded, legacy regulatory frameworks.

What is needed is a paradigm shift toward a world in which spectrum is shared more in-

[1]For instance, according to Cisco, there will be a ten-fold increase in U.S. mobile data traffic between 2014 and 2019 [2].

tensively and flexibly—or equivalently, dynamically—among all classes of users and uses. This includes both *Incumbent Users* (IUs), or those with legacy access rights to spectrum, and *Secondary Users* (SUs), or those who are seeking access to additional spectrum. Often the term *Dynamic Spectrum Sharing (DSS)* is used to describe this paradigm shift. DSS involves real-time adjustment of spectrum usage in response to changing circumstances and objectives such that the utility of spectrum is maximized. Realizing this paradigm shift requires the co-evolution of radio networks, wireless markets and business models, and the regulatory rules and mechanisms—or, regimes—that govern how spectrum is shared among all classes of IUs and SUs.

Enabling the shared use of spectrum is one of the key strategies for mitigating the spectrum shortage problem. Realizing this, the academia, the wireless industry, regulators, and other stakeholders in the U.S. and a number of other countries have undertaken initiatives to break-down the legacy silos of exclusive-spectrum usage models and address the technical and policy challenges in expanding spectrum sharing options. The Advanced Wireless Services (AWS)-3 auction[3], progress on enabling shared access to TV white spaces [4], ongoing progress in the FCC's 3.5 GHz and 5 GHz proceedings [5, 6, 7, 8, 9], standardization of Licensed Shared Access (LSA) [10, 11] in the Europe, etc. are some examples of such initiatives. In essence, these initiatives show a promise in advancing this vision of increased spectrum sharing in multiple bands, including between commercial and federal government users, such that the overall utilization efficiency of the spectrum is improved.

The utilization efficiency of shared spectrum depends mainly on the collection, analysis and sharing of information about the radio environment and spectrum usage among participating users. For instance, the knowledge of a user's geolocation, times of operation and radio capabilities helps other users to opportunistically and efficiently share the same spectrum without causing harmful interference to each other. However, much of this information has the potential to pose a threat to the operational privacy and security of spectrum users. In particular, unauthorized access to location, technical capabilities, or usage behavior of a particular set of users could pose a significant threat to users' strategic interests and privacy.

This privacy issue is of critical concern when some of the spectrum users include federal government and military users—such as the case in the U.S. 3.5 GHz band sharing [12, 6]. Motivated by this conflict, in this dissertation, we study the following two main issues in dynamic spectrum sharing: i) spectrum utilization efficiency, and ii) operational security (OPSEC). Study of this kind facilitates a better understanding of mechanisms that enable improved spectrum utilization efficiency and minimize the associated OPSEC threats, and hence, helps in wider adoption of dynamic spectrum sharing.

1.1 Spectrum Utilization Efficiency

The utilization efficiency of the shared spectrum depends on proper spectrum management and coordination among users that share the spectrum. For facilitating spectrum management, the Federal Communications Commission (FCC) has mandated the use of geolocation databases (GDBs) in the U.S. TV band [4] and the 3.5 GHz band [12, 6], and it is very likely to be adopted for other spectrum sharing applications as well. A GDB houses an up-to-date repository of incumbent users' spectrum usage information along with their operational attributes (e.g., location, times of operation, transmit spectral mask, receiver sensitivity, etc.), performs real-time aggregate interference computations using radio propagation models, and uses this information to determine spectrum availability at the locations of secondary users. For example, when an entrant SU requests access to the spectrum, the GDB first computes the estimated interference from the prospective SU to the IU, and then allows the SU to access the spectrum only if the interference experienced by the IU is below a threshold. The practical advantage of employing GDB-driven spectrum sharing compared to spectrum sensing-driven spectrum sharing is that the former enables SU devices to utilize spectrum more efficiently compared to the latter by reliably identifying fallow spectrum and minimizing the probability of interference events.

In spectrum sharing, it is important to limit the interference from SUs to the IU to an ac-

ceptable level. One popular approach is to define a geographic separation region around the IU where SUs are prohibited from operation. This region is termed as an *Exclusion Zone (EZ)* and is defined based on principles of radio propagation path loss—i.e., by estimating the aggregate interference power caused due to transmissions from multiple SUs at the IU. Thus, the accurate prediction of radio propagation path loss plays a crucial role in protecting IUs from harmful interference and also in improving the utilization of the spectrum. A propagation analysis that over-estimates path loss between the SU and the IU will under-estimate the potential for co-channel interference, providing inadequate interference protection for the IU. In contrast, an analysis that under-estimates the path loss will unnecessarily preclude SUs from taking advantage of fallow spectrum although doing so would not cause harmful interference to the IU. The deployment of such overly conservative EZs can significantly reduce the economic benefits of spectrum sharing, and may seriously hinder its adoption due to the lack of interest from potential SU wireless industry stakeholders.

Previous studies[2] have shown that the use of terrain-based propagation models, such as the Irregular Terrain Model (ITM) in point to point (PTP) mode, improves the efficacy of spectrum sharing because such models accurately estimate the radio propagation path loss in a communication link [13]. However, using ITM-PTP for characterizing aggregate interference caused by multiple SUs may not always be viable. First, ITM-PTP model is computationally intensive and data hungry due to the consideration of detailed terrain characteristics in path loss computations. When a large number of SUs share the spectrum with an IU, computing the aggregate interference from all SUs at the IU requires many ITM-PTP path loss computations, which is time consuming. Second, ITM-PTP requires accurate geo-locations of SUs which might not always be available (e.g., the precise locations of SUs might not be available when they are mobile, or when they obfuscate their geo-locations for achieving location privacy).

[2]In June 2015, the National Telecommunications and Information Administration (NTIA) published a report that shows that the EZ of IUs in the 3.5 GHz band can be reduced by up to 70% when legacy propagation models are replaced by the Irregular Terrain Model in point to point (ITM-PTP) mode. The ITM in PTP mode is one of the most popular terrain-based propagation model in use today.

Due to the aforementioned limitations of terrain-based propagation models, there is a need for an alternative approach, or an analytical approach, for characterizing the aggregate interference. Proper characterization of aggregate interference helps in defining incumbent protection boundaries that are neither overly aggressive to endanger the IU protection requirement, not overly conservative to limit spectrum utilization efficiency. Such an approach will be employed by a central spectrum management entity to perform real-time estimates of the SUs' aggregate interference power, which is the key parameter needed to perform spectrum access control—i.e., control which and how many SUs are allowed to access spectrum. The model should be able to accurately estimate the aggregate interference in a computationally efficient manner, and it should be effective even when precise geo-locations of SUs are not available.

In this dissertation, we first identify that the legacy EZs, as they are defined today, often result in an overly conservative approach for IU protection that unnecessarily limits the SUs' spectrum access opportunities. Motivated by this, we propose an analytical tool that can be employed by a central spectrum management entity (such as the Spectrum Access System (SAS)[3]) for performing real-time estimates of the SUs' aggregate interference power in a computationally efficient manner and without requiring information regarding the precise geolocations of SUs. We show that our proposed tool can be used to completely redefine the existing notion of overly conservative EZs by facilitating dynamic adjustment of the IU's protection boundary based on radio interference environment, network dynamics, density of SUs, and constraints imposed by the primary system performance requirements. Furthermore, our proposed framework can be used by spectrum regulators for quantitatively analyzing the incumbent protection zones to gain insights of and determine the trade-offs between interference protection and spectrum utilization efficiency.

[3]The term 'SAS" is used to refer to a system of databases and enabling infrastructure for facilitating spectrum management in the U.S. 3.5 GHz band

1.2 Security in Spectrum Sharing

The emergence of new spectrum access technologies and spectrum utilization paradigms raise new security challenges that have not been studied previously. For instance, although using GDBs for spectrum sharing has many pragmatic advantages, it raises a potentially serious *operational security* problem. In particular, SUs, through seemingly innocuous queries to the database, may be able to infer an IU's operational parameters, such as its geolocation, times of operation, protected contour, transmit power, antenna attributes, receiver sensitivity, etc. [14]. When IU systems are commercial systems, such as the case in the TV bands, OPSEC is not a major concern. However, in federal-commercial spectrum sharing, where some of the IUs are federal government systems including military and public safety communication systems (e.g., the IUs of the U.S. 3.5 GHz band include Department of Defense (DoD) radar systems), the information revealed by the databases may result in a serious breach of the IUs' OPSEC [15]. Devising techniques and policies for protecting the OPSEC of DoD entities while, at the same time, enabling the commercial SUs to effectively utilize fallow spectrum are key obstacles to realizing spectrum sharing in the 3.5 GHz band.

Recently, a number of research and standardization efforts have been launched to address the problem of OPSEC in GDB-driven spectrum sharing, specially in the context of federal-commercial spectrum sharing. In 2015, the Wireless Innovation Forum created the Spectrum Sharing Committee that serves as a common industry and government standards body to support the development and advancement of advanced spectrum sharing technologies [15]. The Security Requirements Working Group, which is one of the Working Groups within the Spectrum Sharing Committee, has been charged with defining the OPSEC requirements, including location privacy, as well as the communications security requirements for spectrum sharing ecosystems. Moreover, under the auspices of the Defense Advanced Research Projects Agency's (DARPA's) Shared Spectrum Access for Radar and Communications (SSPARC) program [16], research teams from industry and academia are developing techniques for addressing OPSEC, including location privacy, in the context of spectrum sharing between

military radars and commercial communications systems.

In this dissertation, we investigate one of the key aspects of OPSEC in GDB-driven federal-commercial spectrum sharing. In particular, we study the *location privacy* of IUs whose locations, along with other relevant information, are crucial in finding spectrum opportunities for the SUs. We show that an adversary, by masquerading as a legitimate SU, can make multiple queries to the database, collect responses and use them to effectively infer the IUs' locations. We call it a *location inference attack*. Unfortunately, the problem of IUs' location privacy cannot be fully or adequately addressed by tightly controlling access to the database because: (1) all SUs need access to the database for realizing spectrum sharing, and (2) identifying malicious SUs, merely on the basis of their queries to the database, is very difficult.

To address this issue, we propose a *perturbation-based optimal obfuscation strategy* than can be implemented by the GDB to preserve the location privacy of IUs. The GDB implements this strategy and responds to queries made from SUs with an obfuscated response. The proposed obfuscation strategy is optimal in the sense that it maximizes the IUs' location privacy while ensuring that the expected degradation in the SUs' performance due to obfuscated responses does not exceed a threshold. This report is one of the few reports that addresses the problem of preserving the location privacy of a group of users (IUs) from another group of users (malicious queriers) through a trusted database. Note that this is different from location privacy in location based services (LBS) [17] because in LBS, the database is regarded as an "honest-but-curious" adversary.

1.3 Contributions

In this dissertation, we study the two main aspects of dynamic spectrum sharing: i) spectrum utilization efficiency, and ii) operational security. In particular, we seek to answer the following questions pertaining to spectrum sharing:

- *How can we estimate the aggregate interference in a computationally efficient manner?*
- *How can we redefine the legacy notion of overly conservative mechanisms for protecting incumbents from harmful interference?*
- *How can new wireless protocols be standardized for improving the spectrum utilization efficiency?*
- *How can we safeguard users' operational information when access to such information is a key to enabling efficient spectrum sharing?*

The main contributions of this dissertation are summarized below:

1.3.1 A Comprehensive Literature Survey of Recent Spectrum Sharing Initiatives

This contribution is presented in Chapter 2 where we provide a comprehensive overview of the current status of significant regulatory initiatives underway globally to facilitate the transition toward a regime of dynamic shared spectrum. We particularly focus on database-driven models, which have been shown to offer promise a cost-effective and reliable approach for managing sharing among multiple classes of users with heterogeneous access rights and radio network technologies. We provide a current overview of major technological and regulatory reforms that are leading the way toward a global paradigm shift to more flexible, dynamic, market-based ways to manage and share radio spectrum resources. We focus on current efforts to implement database-driven approaches for managing the shared co-existence of users with heterogeneous access and interference protection rights, and discuss open challenges.

1.3.2 Characterization of Aggregate Interference

We discuss this contribution in Chapter 3 and propose an analytical tool that we refer to as *Tool for Enabling Spatial Spectrum Sharing Opportunities (TESSO)*. TESSO is a tool that can be employed by a central spectrum management entity (such as a Spectrum Access System (SAS)) to perform real-time estimates of the SUs' aggregate interference power, which is a key parameter needed to perform spectrum access control (i.e., control which and how many SUs are allowed to access the spectrum). TESSO is computationally efficient, and it can be implemented by a SAS ecosystem in real-time to compute the maximum number of SUs, say N, that can be safely allowed to co-exist with an IU in a given region. Unlike legacy methods, TESSO is computationally efficient and it does not require the precise geo-locations of the SUs. These two distinguishing characteristics make TESSO favorable to implement in real-time spectrum sharing systems such as the GDB-driven spectrum sharing. Results from our case studies show that the performance of TESSO, in terms of spectrum utilization and incumbent protection, is comparable to that of computationally intensive terrain-based propagation models, such as the Irregular Terrain Model in Point-to-Point mode.

1.3.3 Dynamic Exclusion Zones for Spectrum Sharing

We describe this contribution in Chapter 4. Here, we identify that the legacy notion of providing interference protection to the IUs by using static EZs is overly rigid, and often results in poor spectrum utilization efficiency. To address this, we propose a novel framework for prescribing interference protection for the IUs that addresses the aforementioned limitation of legacy EZs. Specifically, we introduce the concept of *Multi-tiered Incumbent Protection Zones (MIPZ)*, and show that it can be used to dynamically adjust the IU's protection boundary based on changes in the radio environment, network dynamics, and the IU interference protection requirement. The MIPZ framework can also be used as an analytical tool for quantitatively analyzing the incumbent protection zones to gain insights of and determine the trade-offs between interference protection and spectrum utilization efficiency.

Using results from extensive simulations, we show that MIPZ adapts to changing network conditions by adjusting the EZ boundary, provides the required interference protection to the IU, and improves the overall spectrum utilization.

1.3.4 Performance Analysis of 802.11ax

This contribution is presented in Chapter 5 where we provide a case-study of spectrum sharing in the unlicensed band. Legacy Wireless Fidelity (Wi-Fi) protocols are not good at coping with the traffic demands of users in a congested environment because their medium access technique, which is common to all legacy technologies, is sub-optimal in terms of spectrum utilization efficiency. To address this limitation, the next generation Wi-Fi technology—referred to as IEEE 802.11ax—introduces some key features, most notably the use of Multi-User Orthogonal Frequency Division Multiple Access (MU-OFDMA) technology in its medium access control (MAC) layer. MU-OFDMA allows multiple users to transmit simultaneously in smaller sub-channels (a.k.a. resource units (RUs)) in the uplink (UL) as well as the downlink (DL), thereby improving the 802.11ax MAC efficiency, especially when the network size is large. In our work, we first provide an analytical characterization of the MAC layer performance of the new MU OFDMA-based 802.11ax and summarize our findings. Second, we investigate the impact of different RU distributions on the network performance and devise an algorithm for optimal RU allocation such that the overall 802.11ax throughput is maximized. Third, we study how to share the airtime between legacy 802.11 and 802.11ax transmission in a fair manner when both categories of STAs are jointly served by a single access point (AP) that can support both 802.11ax and legacy Wi-Fi. From this case study, we are able to demonstrate that effective management of spectrum resources helps in efficiently serving multiple users and in maximizing the overall utilization of the spectrum.

1.3.5 Operational Security of Incumbent Users

We investigate the problem of operational security in GDB-driven spectrum sharing in Chapter 6. In particular, we describe a location inference attack and show that an adversarial SU can use Bayesian learning to readily infer the locations of IUs by making seemingly innocuous queries to the database. Unfortunately, existing techniques to mitigate location inference attacks in other applications, such as LBS, are not practical in spectrum sharing because they limit spectrum utilization opportunities for the non-adversarial SUs. To counter location attacks in spectrum sharing, we propose an optimal obfuscation strategy that maximizes the location privacy of IUs while ensuring that the degradation in SUs' spectrum utilization due to obfuscated responses does not exceed a threshold. Using simulation results, we demonstrate the effectiveness of the proposed strategy in thwarting location inference attacks.

The aforementioned contributions have resulted in the following publications.

- **Patent**

  1. J.-M. Park and **S. Bhattarai**, "Method and Apparatus for Defining Dynamic Separation Regions to Protect Primary Users from Interference in Dynamic Spectrum Sharing", *U.S. Provisional Patent (filed on October 2015).*

- **Journal Publications**

  1. **S. Bhattarai**, J.-M. Park and W. Lehr, "Dynamic Exclusion Zones for Protecting Primary Users in Database-Driven Spectrum Sharing", (manuscript under preparation for submission to *IEEE Transactions on Cognitive Communications and Networking*).
  2. **S. Bhattarai**, P.R. Vaka J.-M. Park, "Thwarting Location Inference Attacks in Database-Driven Spectrum Sharing", accepted to appear in *IEEE Transactions on Cognitive Communications and Networking.*

3. **S. Bhattarai**, J.-M. Park, Bo Gao, Kaigui Bian, William Lehr, "An Overview of Dynamic Spectrum Sharing: Ongoing Initiatives Challenges and a Roadmap for Future Research", *IEEE Transactions on Cognitive Communications and Networking*, vol. 2, no. 2, pp. 110-128, June 2016.

- **Conference Proceedings**

1. **S. Bhattarai**, G. Naik, J.-M. Park, "Performance of IEEE 802.11ax in a Heterogeneous Wi-Fi Network", under review in *ACM MobiHoc*, Los Angeles, USA, 2018.
2. **S. Bhattarai***, G. Naik*, J.-M. Park, "C-UORA: A Novel MAC Scheme for Uplink Multi-User OFDMA in Dense Wi-Fi Networks", under review in *IEEE ICC Workshop on 5G Ultra Dense Networks*, 2018. (* denotes equal contribution).
3. G. Naik*, **S. Bhattarai***, J.-M. Park, "Performance Analysis of Uplink Multi-User OFDMA in IEEE 802.11ax", accepted to appear in *IEEE ICC*, 2018. (* denotes equal contribution).
4. **S. Bhattarai***, P. R. Vaka*, J.-M. Park, "Co-existence of NB-IoT and Radar in Shared Spectrum: An Experimental Study", in *Proc. of IEEE GLOBECOM*, Singapore, 2017. (* denotes equal contribution).
5. **S. Bhattarai**, J.-M. Park, W. Lehr and B. Gao, "TESSO: An Analytical Tool for Characterizing Aggregate Interference and Enabling Spatial Spectrum Sharing", in *Proc. of IEEE DySPAN*, USA, 2017.
6. P. R. Vaka, **S. Bhattarai**, J.-M. Park, "Location Privacy of Non-Stationary Incumbent Systems in Spectrum Sharing", in *Proc. of IEEE GLOBECOM*, USA, 2016.
7. B. Gao, **S. Bhattarai**, J.-M. Park, Y. Yang, M. Liu, K. Zeng, Y. Dou, "Incentivizing Spectrum Sensing in Database-Driven Dynamic Spectrum Sharing", in *Proc. of IEEE INFOCOM*, USA, 2016.

8. **S. Bhattarai**, A. Ullah, J.-M. Park, J.H. Reed, D.Gurney, B. Gao, "Defining Incumbent Protection Zones on the Fly: Dynamic Boundaries for Spectrum Sharing", in *Proc. of IEEE DySPAN*, Sweden, 2015.
9. A. Ullah, **S. Bhattarai**, B. Bahrak, J.-M. Park, J.H. Reed, D.Gurney, K. Bian, "Multi-Tier Exclusion Zones for Dynamic Spectrum Sharing", in *Proc. of IEEE ICC*, London, U.K., 2015.
10. B. Bahrak, **S. Bhattarai**, A. Ullah, J.-M. Park, J.H. Reed, D.Gurney, "Protecting the Primary Users' Operational Privacy in Spectrum Sharing", in *Proc. of IEEE DySPAN*, USA, 2014. (Best Paper Award)

1.4 Organization of this Dissertation

The rest of this dissertation is organized as follows. In Chapter 2, we provide a comprehensive overview of the current status of significant regulatory initiatives underway globally to facilitate the paradigm shift in spectrum management towards dynamic spectrum sharing. Next, in Chapter 3, we describe an analytical tool that can be used to efficiently compute aggregate interference caused by multiple SUs to the IU in dynamic spectrum sharing networks. We present an analytical framework that facilitates the redefinition of legacy notion of conservative incumbent protection boundaries in Chapter 4. In Chapter 5, we provide a detailed analysis of the next-generation Wi-Fi technology that promises improved utilization of the spectrum by introducing key PHY and MAC layer features. This chapter serves as an illustration of how spectrum utilization efficiency can be improved in future wireless networks. Next, in Chapter 6, we motivate and investigate the problem of operational privacy and security in database-driven spectrum sharing and propose a mechanism that thwarts location inference attacks from malicious users. Finally, we conclude the dissertation by providing concluding remarks in Chapter 7.

Chapter 2

An Overview of Dynamic Spectrum Sharing

In this chapter, we provide a comprehensive overview of the current status of significant regulatory initiatives underway globally to facilitate the transition toward a regime of Dynamic Shared Spectrum, with a special focus on database-driven models, which have been shown to offer promise as a cost-effective and reliable approach for managing sharing among multiple classes of users with heterogeneous access rights and radio network technologies [18, 19, 20, 21]. In Section 2.1, we summarize some of the earlier literature on spectrum sharing and clarify some of our terminology. We follow this in Section 2.2 with a summary of the ongoing spectrum reform efforts within the U.S. and several other countries. In Section 2.3, we address, in general terms, a key concern of spectrum management—the need to manage interference among heterogeneous users and discuss how that challenge is changing as we move toward more dynamic sharing models. In Section 2.4, we discuss how the challenge is being addressed in several important spectrum bands. In Section 2.5, we consider another important challenge confronting dynamic spectrum management—the need to protect the confidentiality and security of spectrum users in light of management frameworks that require sharing significant information about the location and usage of spectrum resources. In

Section 2.6, we identify some of the open research questions. Section 5.8 provides summary conclusions.

2.1 Spectrum Access and Management Regimes

Spectrum resources are artificially scarce, in part, because static, legacy regulatory regimes inhibit the adoption of technologies and usage practices that would allow spectrum to be shared more intensively. Policymakers have recognized for many years that legacy management regimes need to be reformed to allow greater scope for market-forces to direct how spectrum resources are used and to create incentives and opportunities for the commercialization of innovative and more efficient radio technologies [22, 23].

The critical need for increasing commercial access to shared spectrum was emphasized in the *National Broadband Plan*, [24] which was unveiled by the U.S. Federal Communications Commission (FCC) in 2010. The subsequent U.S. Presidential Memoranda—*Unleashing the Wireless Broadband Revolution* [25] and *Expanding America's Leadership in Wireless Innovation* [26]—issued executive mandates to implement policies to expand access to shared spectrum. Under the auspices of the White House, the FCC and the National Telecommunications and Information Administration (NTIA) are taking aggressive steps to realize the vision outlined in the Presidential Memoranda. In the U.S., the recently completed Advanced Wireless Services (AWS)-3 auction [3], progress on enabling shared access to TV white spaces [4], and ongoing progress in the FCC's 3.5 GHz and 5 GHz proceedings [5, 27] show promise in advancing this vision of increased spectrum sharing in multiple bands, including between commercial and federal government users.

Regulatory bodies in other countries have also put in motion spectrum-related initiatives, and, in some cases, have established regulations with the aim of improving spectrum utilization efficiency through shared spectrum access. These efforts include the studies and initiatives undertaken by the United Kingdom's Office of Communications (Ofcom) [28, 29, 30],

Industry Canada [31, 32], Infocomm Development Authority of Singapore (IDA) [33, 34], China's IMT-2020[1] [35], Radio Spectrum Policy Group in Europe [36, 37, 38], and the European Communications Office [39].

In multiple ways, all of these initiatives represent progress toward enabling Dynamic Spectrum Access (DSA). In the engineering and technical standards literature, DSA is often used to refer to the "real-time adjustment of spectrum utilization in response to changing circumstances and objectives" [40], and is usually assumed to be enabled by or coincident to the use of Cognitive Radio (CR) and/or Software Defined Radio (SDR) capabilities or technologies. CR has been defined as "an approach to wireless engineering wherein the radio, radio network, or wireless system is endowed with awareness, reason, and agency to intelligently adapt operational aspects of the radio, radio network, or wireless system" [41]. SDRs implement radio functionality in software rather than hardware, thereby facilitating the adaptive functionality that characterizes CRs. In the full-blown scenario, CR-"smart" radio systems would collectively sense and analyze their local radio environment, negotiate optimal sharing arrangements, and then adapt their radio operating parameters (i.e., frequency, power, modulation, transmission timing, direction of transmission, and other waveform characteristics) to maximize shared use of local spectrum resources. The concept of shared/dynamic spectrum access represented by this vision is presented in Figure 2.1.

Although significant progress has been made in developing CR, SDR, and other smart radio technologies, we are still far from being able to actually realize the full-blown scenario described above. Realizing this vision depends on the commercial deployment of new radio technologies, the adoption of new spectrum access regime, and regulatory reforms. In the past five years, a number of surveys have been published that describe the current status of enabling technologies such as CRs and SDRs [42, 43], -or provide a taxonomy of the various ways in which spectrum may be managed so as to enable more extensive spectrum sharing

[1]IMT-2020 (5G) Promotion Group was jointly established in February 2013 by three ministries of China based on the original IMT-Advanced Promotion Group. The members include the main operators, vendors, universities, and research institutes in China. The Promotion Group is the major platform to promote 5G technology research in China and to facilitate international communication and cooperation.

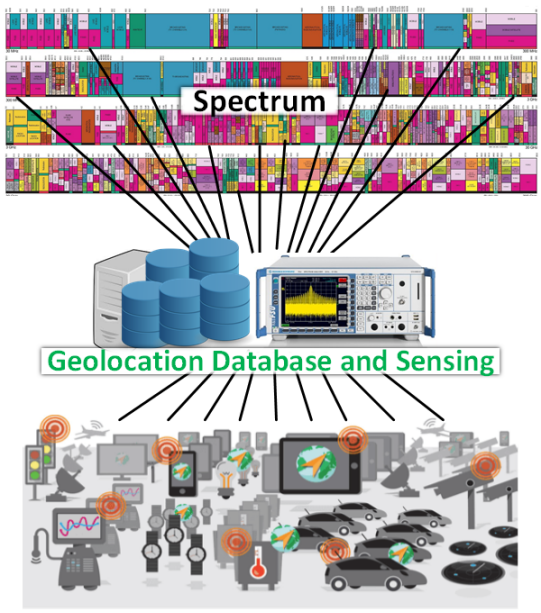


Figure 2.1: Dynamic spectrum sharing via geolocation databases and sensing.

[44, 45]. One such example is illustrated in a figure reproduced from the METIS project [46], a recently concluded European project that was focused on developing technologies for 5G (see Figure 2.2).

Figure 2.2 lays out various regulatory rights regimes for managing spectrum access, ranging from exclusive licensed spectrum (used by cellular operators and television broadcasters) to unlicensed spectrum access (used by Wi-Fi and Bluetooth). In the exclusive licensed regime, a single operator manages how spectrum is shared among the spectrum users; whereas in the unlicensed regime, sharing is uncoordinated. These two models represent points on a continuum of potential sharing regimes, wherein different tiers of users may have different rights to access the spectrum and to protection from potential interference caused by other users. One sharing model that has the features of both of the aforementioned regimes is Licensed Shared Access (LSA). In LSA, an IU with previously exclusive-usage rights tolerates shared access from a new SU, who is allowed to share pursuant to a framework that ensures mutual protection from interference. Current implementations of this framework rely on a database-driven mechanism to enforce the sharing arrangement [45].

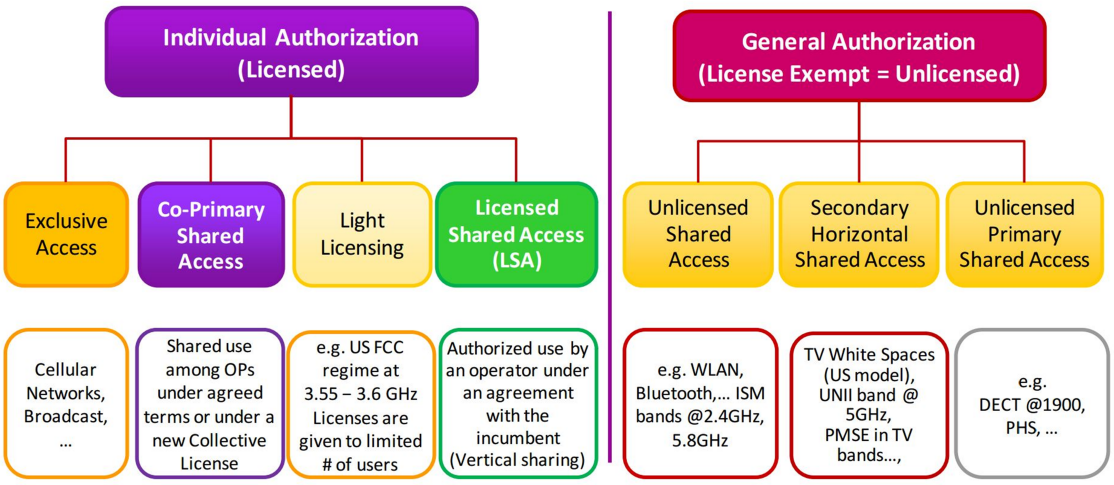


Figure 2.2: Spectrum access schemes and authorization regimes.

In these and other regulatory frameworks, DSA is more than just a technical vision. It also encompasses a framework for managing the spectrum access and usage rights, including protection from interference and other management rights (e.g., the right to exclude or pre-empt other users, the right to sub-lease or transfer management of the spectrum; as well as obligations to obey operating rules). A full-featured DSA management regime will have technical, regulatory, and business/market mechanisms in place to enable spectrum resources to be dynamically reallocated and shared across users (e.g., government and commercial) and uses (e.g., sensing and communications) on a more fine-grained and granular basis along any potential technical dimension (i.e., frequency, time, space, direction of transmission, etc.) and under a variety of differing rights models (e.g., real-time spectrum markets, administered sharing among multiple tiers of PU and SUs with changing usage rights, etc.). In this chapter, we use DSA more loosely to refer to the full range of business, regulatory, and/or technically enabled ways in which enhanced sharing models are being enabled. In so doing, we diverge from the technical literature that restricts DSA to refer to spectrum usage paradigms that require or make use of CR or SDR technologies or capabilities. As argued elsewhere, we need to evolve toward these expanded sharing models, and in so doing, will enhance the likelihood that CR, SDR, and other advanced radio technologies will be commercialized successfully

[47]. Our broader interpretation of what constitutes DSA is intended to highlight how the matrix of regulatory reforms and evolving sharing concepts discussed in subsequent sections are contributing to the expansion of options and capabilities for sharing spectrum more flexibly and dynamically. In the next section, we review some of the regulatory initiatives underway.

2.2 Recent Spectrum Initiatives

2.2.1 Spectrum Initiatives in the U.S.

TV band

In September 2010, the FCC issued final rules to allow low power unlicensed devices to operate on unused channels in the TV broadcast bands (often called the TV white spaces (TVWS)) in the U.S. [4]. Concerned about the technical capabilities of sensing and the risk of interference, the FCC mandated a database-driven approach, attesting to the challenges of Cognitive Radio (CR) systems, even when employed to detect the presence of high-power, high-site (TV transmitters with large HAAT (height above average terrain)), and fixed TV stations. The TVWS devices must register with a database that dictates how and when they can access the spectrum. To obtain spectrum availability information from the database, a TVWS device needs to submit a spectrum query to it that contains its operational parameters (e.g., type of device, location, etc.). Two IEEE standards, namely IEEE 802.22 and IEEE 802.11af, were developed to enable communications in the TVWS.

AWS-3 band

In January 2015, the FCC completed an auction of AWS-3 licenses in the $1695-1710$ MHz, $1755-1780$ MHz, and $2155-2180$ MHz bands (collectively called "AWS-3" bands) [3]. The

incumbents of this band are federal systems, including the federal meteorological-satellite (MetSat) systems. Cellular service providers will share this band with the incumbents based on manual coordination of protection zones to protect the federal systems [48].

3.5 GHz band

Per its recent *Report and Order and Second Further Notice of Proposed Rule Making* (FNPRM) [5], the FCC has opened up the 3.5 GHz ($3550 - -3700$ MHz) band to SU access. This band will now be home to the new Citizens Broadband Radio Service (CBRS). The entrant users will share the spectrum among themselves and incumbents through a three-tiered access model composed of the Incumbent Access (IA), Priority Access (PA) and General Authorized Access (GAA) tiers (see Figure 2.3). The harmonious coexistence among the three tiers of users is ensured through the employment of an automated frequency assignment and control database mechanism known as the *Spectrum Access System* (SAS). The FNPRM [5] also prescribes the use of a network of spectrum sensors, called *Environmental Sensing Capability* (ESC), to detect the presence of IUs and aid the SAS in assessing the spectrum environment.

IA users include authorized federal and grandfathered fixed satellite service users currently operating in the 3.5 GHz band. These users will be protected from harmful interference from PA and GAA users. The PA tier consists of Priority Access Licensees (PALs) that will be assigned using a competitive bidding process within the $3550 - 3650$ MHz portion of the band. Each PAL is defined as a non-renewable authorization to use a 10 MHz channel in a single census tract for up to three-years. At maximum, a total of seven PALs may be assigned in any given census tract with up to four PALs going to any single applicant. Applicants may acquire up to two-consecutive PAL terms in any given license area during the first auction. The GAA tier is licensed-by-rule to enable open, flexible access to the band for the widest possible group of potential users. GAA users are permitted to use any portion of the $3550 - 3700$ MHz band not assigned to a higher tier user and may also operate

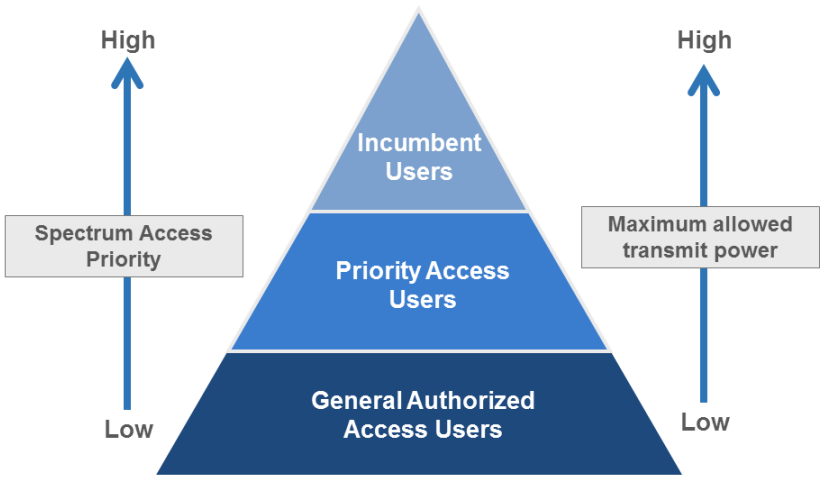


Figure 2.3: Three-tiered access model of the CBRS band.

opportunistically on unused PA channels.

The envisioned SAS for the U.S. 3.5 GHz-based CBRS band supports coexistence among heterogeneous wireless access technologies, specifically PAL and GAA users, in a centralized fashion. It maintains a registry of all coexisting devices in the band along with their geo-operational status. SAS acts as a highly automated spectrum access coordinator that facilitates coexistence among heterogeneous devices across the band and prevents interference events by enforcing the band's usage policy. It protects higher tier users from interference from lower tier users, while simultaneously seeking to ensure maximal spectrum availability for lower tier PAL and GAA users and their harmonious coexistence [5]. The SAS architecture will be designed based on the specific use-case scenario of the 3.5 GHz band to support a harmonious coexistence among heterogeneous wireless access technologies of similar/different spectrum access hierarchy.

5 GHz band

In 2013, the FCC, in its Notice of Proposed Rule Making (NPRM), announced that it intends to modify rules that govern the operation of Unlicensed National Information In-

frastructure (U-NII) devices and make available an additional 195 MHz of spectrum in the 5 GHz band [49]. The NPRM prescribed sharing the Intelligent Transportation System (ITS) band ($5.85 - 5.925$ GHz) with unlicensed devices and allow the latter (specifically 802.11ac/802.11ax systems) to have access to more wideband channels (80 MHz and 160 MHz). Later, in 2014, the FCC released *First Report and Order* [7] with the goal of increasing the utility of 5 GHz band by modifying certain U-NII rules and testing procedures that ensure that U-NII devices do not cause harmful interference to the IUs (Dedicated Short Range Communications (DSRC) systems) of these bands. Currently, the FCC is in the process of creating a new set of rules for this band which would be ultimately referred to as the U-NII-4 band. For more details of activities surrounding U-NII-4 band, specifically sharing between 802.11 and DSRC, readers are referred to [8].

In the ongoing proceedings for the 5 GHz band, there is a growing contention between unlicensed LTE (including License Assisted Access (LAA) and LTE-Unlicensed (LTE-U)) and Wi-Fi stakeholders for access to the band. Several industry entities, mainly Wi-Fi stakeholders, have raised concerns over the introduction of LTE-U/LAA in the unlicensed bands. Because of the ongoing, sometimes contentious, debate between the LTE and Wi-Fi communities regarding the coexistence of the two technologies, the FCC, in May 2015, formally sought comments on a range of topics related to the LTE-U/LAA technologies [9]. More recently, in August 2015, the LTE-U and Wi-Fi stakeholders held a meeting to discuss these coexistence issues [50]. We will provide more details on the coexistence issues between Wi-Fi and unlicensed LTE in Section 2.4.

Millimeter wave bands

In August of 2013, the FCC changed its rules in the $57 - 64$ GHz band, commonly known as the 60 GHz band, to improve the use of unlicensed spectrum for high-capacity, short-range outdoor backhaul, especially for small cells [51]. The 60 GHz band is allocated on a co-primary basis to the federal mobile, fixed, inter-satellite and radio-location services; and

to non-federal fixed, mobile and radio-location services. Under Part 18 of the new rules, industrial, scientific and medical (ISM) equipment may also operate in the 60 GHz band at 61.25 GHz ±250 MHz.

On October 16, 2003, the FCC adopted a *Report and Order* [52] establishing service rules to promote non-federal development and use of the millimeter wave spectrum in the $71-76$ GHz, $81-86$ GHz and $92-95$ GHz bands, which are allocated to non-federal government and federal government users on a co-primary basis. Specifically, the *Report and Order* permits the issuance of an unlimited number of non-exclusive, nationwide licenses to non-federal government entities for all 12.9 GHz of spectrum. It did not require prior coordination among non-federal government licensees asserting that interference is unlikely due to the "pencil-beam" nature of the transmissions in this service. However, realizing that this scheme will delay and perhaps hinder industry efforts to use the 70/80 GHz band as anticipated, the FCC, on March 3, 2005, issued *Memorandum Opinion and Order* [53] and changed the original decision. The new rules require non-federal government users to finish all interference analyses prior to equipment installation. Furthermore, the FCC recently issued an NPRM for seeking comments on authorizing mobile operations in the 28 GHz, 37 GHz, 39 GHz, and $64-71$ GHz bands [54].

As summarized above, the NTIA and the FCC have put into action several initiatives with the aim to expand wireless broadband use, increase sharing, and ultimately meet the 500 MHz goal specified in the 2010 Presidential Memorandum [25]. The NTIA's fifth interim progress report released in 2015 states, "Between October 2010 and September 2014, NTIA and the FCC formally recommended or otherwise identified for study for potential reallocation up to 589 MHz." [55]. This total includes 335 MHz in federal or shared bands and between $152-254$ MHz in non-federal bands. An additional 960 MHz is slated for potential future study for repurposing. All together, the NTIA and the FCC have made available or are investigating for potential re-purposing between $1,447$ and $1,549$ MHz of bandwidth under 6 GHz.

2.2.2 Spectrum Initiatives Outside the U.S.

European Commission

In November of 2012, the European Commission solicited opinions on spectrum sharing issues concerning LSA which is the key concept that has been studied for realizing spectrum sharing in various bands in Europe [56]. LSA ensures guarantees in terms of spectrum access and interference protection to the incumbent(s) as well to the LSA licensees, and hence provides a predictable quality of service to both parties [57]. Spectrum sharing via LSA can be realized across frequency, time, and geographical dimensions.

United Kingdom

As part of the 2015 World Radio Conference (WRC-15) preparatory process, the European Conference of Postal and Telecommunications Administrations (CEPT) analyzed possible sharing of Wi-Fi with incumbent users in $5350 - 5470$, $5725 - 5850$ and $5850 - 5925$ MHz bands in order to develop a European Common Position—i.e., defining a common set of rules for governing access to the 5 GHz band. In addition, Ofcom recently issued a call for inputs, which sought views on the bands that are to be discussed under WRC-15 agenda item 1.1 and sought views on the suitability of these bands for use by mobile or wireless broadband including the 5 GHz bands for Wi-Fi [58]. Furthermore, in February of 2015, Ofcom finalized its decision to allow SUs to access the unused parts of radio spectrum in the $470 - 790$ MHz band through dynamic sharing controlled by a spectrum database [59]. Under this plan, the spectrum that is not utilized by Digital Terrestrial Television (DTT) (including local TV) and PMSE services is shared with TVWS devices on a license-exempt basis.

France

In France, The Agence Nationale des Fréquences (ANFR) is considering sharing the 2.3 GHz, 5.8 GHz, $17.7 - 19.7$ GHz bands [11]. Incumbents of the 2.3 GHz bands are telemetry and other defense applications, and the expected secondary users are mobile/cellular service providers. ANFR is considering opening up this band in the regime of the LSA framework, which affords guaranteed access to spectrum and protection against harmful interference to both the incumbents as well as the LSA licensees. In the 5.8 GHz band, a geolocation-based approach is being considered to support the coexistence between the road tolling application and Intelligent Transportation Systems. The $17.7 - 19.7$ GHz band is being considered for spectrum sharing between fixed service microwave services (as IUs) and uncoordinated fixed satellite services (as SUs).

Canada

In 2012, Industry Canada (IC)—the government entity in charge of spectrum management in Canada—released its policy decision to enable access to TVWS [32]. In Feb. 2015, IC published a specification describing the technical and operational requirements for TVWS devices, which broadly follows the U.S. requirements in terms of equipment types and technical characteristics [60]. Currently, IC is in the process of defining rules for certifying the database and the TVWS devices.

Singapore

Singapore's IDA, in November 2014, approved the rules enabling access to TVWS based on a license-exempt basis provided that devices comply with the technical requirements specified by the IDA, contact a licensed database to obtain channel availability, and are registered with the IDA following a comprehensive validation process [34]. The device types and requirements are broadly in line with the U.S. model, although Singapore allows for

variable effective isotropic radiated power (EIRP) levels.

China

China is actively studying how much spectrum in which bands will be needed to support 5G in its domestic market. In 2013, a promotional group called IMT-2020 (5G) was established to define relevant standards and requirements and to facilitate the development of 5G systems in China. Its primary goal is to start the commercialization of 5G networks in China by 2020. So far, IMT-2020 has identified $450-470$ MHz, $698-806$ MHz and $3400-3600$ MHz bands as candidate bands for 5G development [35]. Several other bands in the range $6-100$ GHz are also being considered for further studies on channel measurements, modeling and coexistence.

New Zealand

Starting in November 2014, Radio Spectrum Management—the government entity in charge of spectrum in New Zealand—initiated a temporary arrangement for access to TVWS in New Zealand, which allows interested parties to obtain licenses for operation of TVWS devices at channels that will be specified in the license [61]. This TVWS access plan does not employ the database-driven spectrum sharing approach, but devices are required to be complaint with relevant regulatory standards which are similar to the ones adopted by the FCC.

Field Trials of LSA in Europe

In April of 2013, the first field trial of shared use of the 2.3 GHz band with a live LTE network was successfully demonstrated in Finland [62] by taking into consideration the inputs from all stakeholders including regulators, incumbents, mobile operators and equipment-supplying industries. Later, in May of 2015, Nokia performed another field trial using LTE network and LSA controller, and rebutted the potentials of LSA in realizing effective spectrum sharing

[10]. Altogether, it is expected that the $2.3 - 2.4$ GHz band will be one of the first bands to be opened up for LSA-based sharing in Europe. However, implementing LSA in this band will entail some challenges as the band is currently used for various incumbent applications, including government services as well as program making and special events (PMSE) services, in different European countries.

A timeline of spectrum initiatives, both inside and outside the U.S., is shown in Figure 2.4.

2.3 Protecting Incumbents

To ensure the viability of spectrum sharing, certain key requirements must be met. One of those requirements is managing radio interference. For wireless communications to work, receivers need to be able to disentangle their desired signals from background noise which may come from either unintentional (e.g., radiating power lines) or intentional transmitters operating either in the same (in-band) or other (out-of-band) frequencies. Historically, the basis for exclusive assignments was to ensure that the radio users of the spectrum would be protected from harmful interference from transmissions from unaffiliated intentional transmitters. The operator with exclusive access could be expected to manage in-band interference from its affiliated users, but needed protection from unaffiliated users transmitting in the spectrum as well as from out-of-band interference from users in other bands.

If the goal is to expand access to spectrum, then an important challenge is to ensure adequate protection both for IUs, the legacy rights holders and users of the spectrum, and the SUs, or new spectrum users who will be accessing the spectrum. Multiple schemes are feasible for managing multiple tiers of users. For example, public safety access may have the right to preempt other traffic, whether the public safety users are IUs or SUs in a particular band, and whether the other users are commercial or government users, etc. More typically, it is often assumed that the IUs have primary usage and interference protection rights by virtue of their legacy incumbency. They may have to tolerate interference from other co-primary

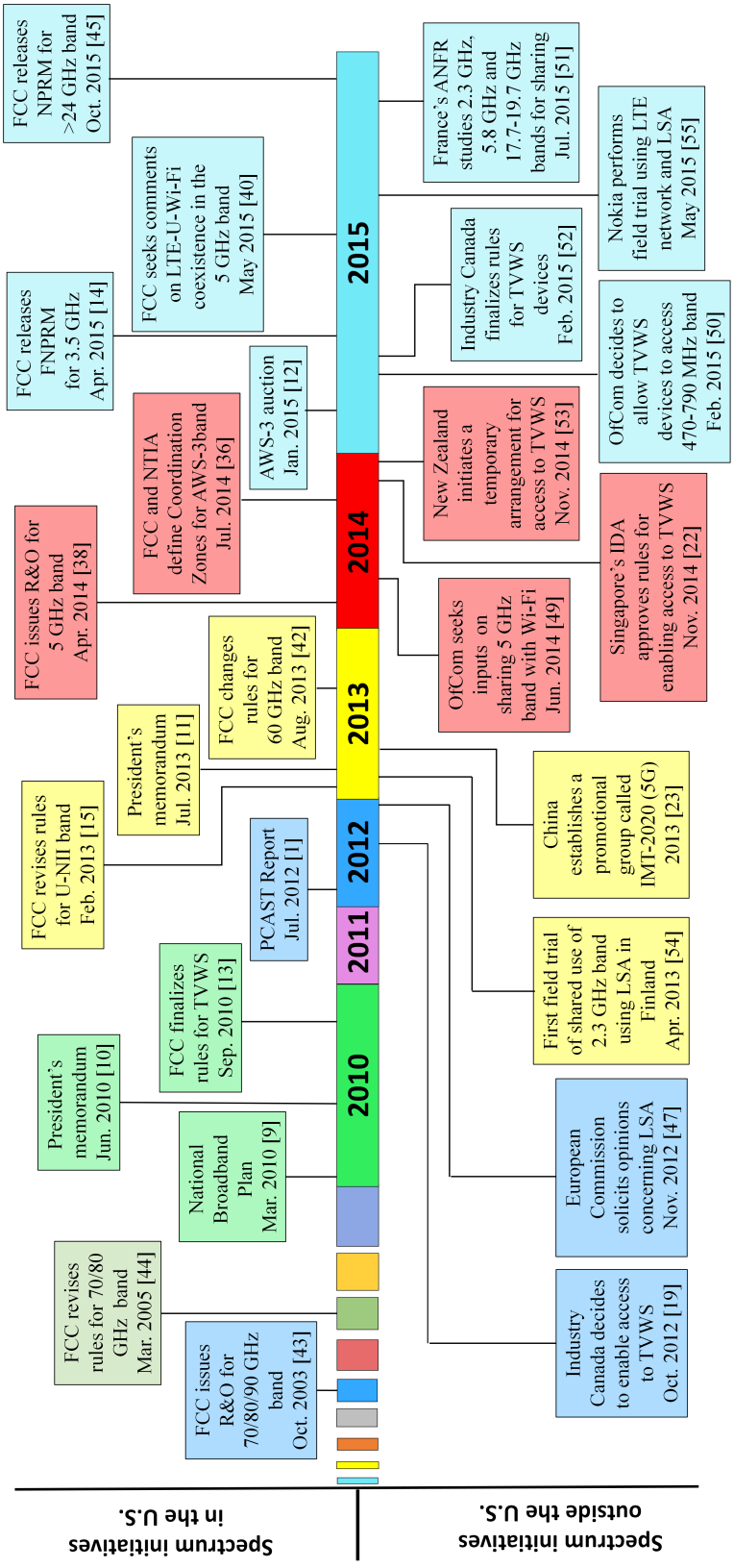


Figure 2.4: Timeline of spectrum initiatives.

IUs. The new users, or SUs, have secondary usage and interference protection rights. The SUs may access and use the spectrum so long as they do not interfere with the IUs, but may be protected from still lower-tier users and may need to tolerate interference from same-tier SUs.

In any case, the sharing framework that provides differing levels of interference protection to different classes of spectrum users needs to be enforced so that the rules are respected by all spectrum users. In general, mechanisms for interference protection protect incumbents (or higher-tier users in multi-tiered access models) from interference generated by lower-tier users. In general, mechanisms for incumbent protection can be classified into two categories: i) *ex ante* (a.k.a. preventive) mechanisms, ii) *ex post* (a.k.a. punitive) mechanisms [63, 64]. Ex ante mechanisms are designed to reduce the probability of occurrence of harmful interference events, while ex post mechanisms are designed to identify and/or adjudicate malicious or selfish behavior after harmful interference events have occurred. Ex ante and ex post approaches work in tandem (but not in isolation), and thus the choice of an ex ante approach affects how ex post enforcement is carried out [64].[2]

In the following sub-sections, we discuss various technical and regulatory approaches that have been employed to manage the collective interference environment, and will discuss ways in which enforcement mechanisms may change to enable more dynamic sharing models. To simplify the exposition, we will presume that IUs have a right to interference protection from SUs, whose right to access the spectrum is contingent on their compliance to the IU interference protection requirement.

[2]The characterization of ex post/ex ante mechanisms as preventive/punitive is an over-simplification to facilitate discussion. For example, today's ex post enforcement is tomorrow's ex ante enforcement; and "carrot" incentives may be viewed as negative penalties (e.g., credits for a history of non-interfering operations).

2.3.1 Ex Ante (Preventive) Approaches

Ex ante approaches are mechanisms used to prevent interference events to the IUs. Examples include the use of exclusion zones (EZs), policy based radios [65], secure radio middleware [66], tamper-resistance techniques [67], radio integrity assessment techniques [68] and hardware-based compliance modules [69]. Among these measures, exclusion zones (a.k.a. protection zones) is the primary ex ante spectrum enforcement scheme used by the regulators to protect IUs from SU-generated interference [70]. The legacy notion of an exclusion zone (EZ) is a static spatial separation region defined around an IU, where co-channel (and possibly also adjacent-channel) transmissions by SUs are not allowed. An EZ needs to achieve two, seemingly opposing, objectives: (i) protect IUs from interference caused by SUs; and (ii) enable efficient utilization of spectrum by the SUs. However, the legacy notion of EZs is inept at achieving those objectives, primarily due to the fact that it is overly conservative and static [64, 71, 70]. The notion of a static EZ implies that it has to protect incumbents from the union of likely interference scenarios, resulting in a worst-case and very conservative solution.

Legacy Notion of Incumbent Protection Zones

In order to protect incumbents (i.e., TV broadcast stations) operating in the TV bands, the U.S. FCC employs *F-curves* that define a protected service contour around an incumbent. An F-curve, $F(x, y)$, ensures a probabilistic guarantee that, inside the TV coverage region, the received TV signal is above a given threshold $x\%$ of the time in $y\%$ of the locations [72, 4]. Then, an appropriate safety margin is added to the protected service contour, often in the form of a minimum separation distance from the edge of the protected service contour, to derive appropriate EZs for both co-channel and adjacent-channel SU operations.

In the AWS-3 band, the NTIA recently prescribed *Coordination Zones* (CZs) for sharing these bands with wireless broadband systems (WBSs) [48]. A CZ is not an EZ where SUs

are prohibited, but it is the area inside which a WBS may operate provided that it meets the requirements for coordination with federal incumbents [73]. Specifically, NTIA's rules require each AWS-3 licensee, prior to its first operations in its AWS-3 licensed area, to reach a coordination arrangement with each Federal agency [74]. After a successful coordination arrangement, the AWS-3 licensee will be notified with operating conditions that specify the terms in which the licensee may begin operations, or denial of request. Even if an AWS-3 licensee is allowed to operate inside a CZ, it must tolerate possible interference from the IUs. For further details on coordination procedures in the AWS-3 band, readers are referred to [48].

The legacy protection zones, as they are defined today, often result in an overly conservative approach for incumbent protection that unnecessarily limits the SUs' spectrum access opportunities. A good example of this can be seen in the U.S. TV bands. To account for possible deep fades, the IEEE 802.22 working group specifications require detectors to have a sensitivity of -116 dBm which corresponds to a safety margin of roughly 20 dB (equivalent to an increased radius of an EZ up to 110 km) [75, 76]. However, in most situations, the probability of such deep fades is very low, and hence the specifications unnecessarily constrain spectrum access opportunities for the SUs. Another example can be seen in the proposed use of EZs to protect incumbents in the 3.5 GHz band. In [77], the NTIA proposed the use of EZs that cordoned off vast areas inland of the east and west coast of the U.S. to protect the navy's ship-borne radar systems. Some have estimated that nearly 60% of the U.S. population reside inside these EZs [64]. The deployment of such overly conservative EZs can significantly reduce the economic benefits of spectrum sharing, and may seriously hinder its adoption due to the lack of interest from potential SU wireless industry stakeholders.

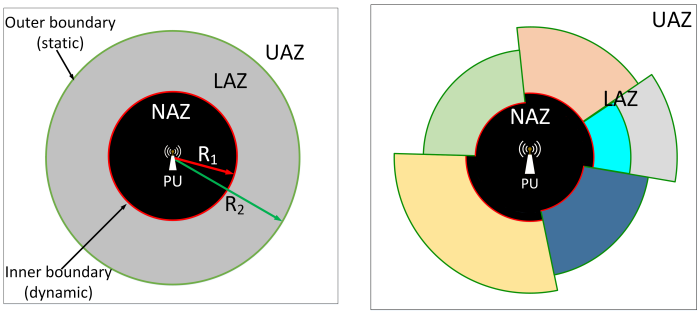
New Models for Incumbent Protection

To fully reap the benefits of spectrum sharing, there is a need to employ incumbent protection approaches that strike an optimal balance between two key objectives—viz., reliably protect

IUs from interference and maximize spectrum access opportunities for SUs. Achieving such a balance is not feasible with the legacy notion of EZs, and a more agile approach is needed. One such approach is the use of *multi-tiered dynamic incumbent protection zones* (MIPZ) proposed by Bhattarai et al. [70].

MIPZ is a novel framework for systematically designing an EZ that can adjust its boundaries by dynamically adapting to changes in the interference environment. MIPZ is designed for database-driven spectrum sharing (e.g., SAS), and it protects IUs by providing a probabilistic guarantee of interference protection. Specifically, MIPZ consists of three zones—(i) No Access Zone (NAZ) where SU operation is strictly prohibited, (ii) Limited Access Zone (LAZ) where only a "limited" number of SUs are allowed to operate, and (iii) Unlimited Access Zone (UAZ) where SUs have unencumbered access to the spectrum. Figure 2.5 shows a simplified (considering circular EZs), as well as a practical (considering irregular EZs), model of the MIPZ framework. For technical details pertaining to the computation of NAZ-LAZ (inner) and LAZ-UAZ (outer) boundaries, readers are referred to [70].

On one hand, stringent technical requirements and risks of interference to the IUs (especially passive IUs) have made spectrum sharing approaches that rely solely on sensing less popular recently [78]. On the other hand, experimental results from recent studies have shown that sharing approaches that rely solely on databases alone may offer inaccurate and stale information of spectrum availability [79, 80, 81]. State-of-the-art research has shown that incorporating real-time sensing data with a database-driven approach is more effective in maximizing spectrum access opportunities for SUs than using either a sensing or a database approach in isolation [78, 70, 79, 82, 83]. Hence, researchers proposed a concept called *Radio Environment Map* (REM) [80, 84, 85, 86], which incorporates a statistical fusion of multiple sources of incumbent characteristics and offers improved spectrum access opportunities for SUs. A recent study is the work of Bo et al. [21] who proposed a multi-tiered spectrum sharing framework, similar to MIPZ, that incorporates sensing results into a database-driven sharing approach and refines the EZ boundary to take advantage of the fallow spectrum that is not captured by database-driven sharing alone. Authors of [21] also studied strategies to



(a) Simplified model (b) Practical model

Figure 2.5: MIPZ framework

incentivize spectrum sensing that can be incorporated in their proposed framework.

Protecting Passive Incumbents

In the preceding paragraphs, we focused on protecting incumbents that actively emit RF energy. In this section, however, we focus on a very different scenario that involves spectrum sharing between passive sensing systems (as IUs) and active communication systems (as SUs). In this scenario, the IUs are receiver-only passive systems, such as systems for earth exploration satellite service (EESS), radio astronomy (RA), or remote sensing. Such passive systems strive to observe extremely faint signals that are emitted by distant non-coordinating transmitters. The signal-to-noise ratio (SNR) of the signal that needs to be detected can be as low as -60 dB [87]. This constraint forces the passive systems to use very sensitive receiver-antenna systems which, in turn, make them highly vulnerable to interference, much more so than active communication systems [88].

There are other issues that make spectrum sharing between active and passive systems different from sharing between active systems. For example, geographic separation does not apply to many EESS whose footprint covers a large area on the Earth's surface; frequency separation may not be applicable to RA systems because radio astronomers are often interested in a large swath of the radio spectrum as different physical processes produce electromagnetic

radiation at different frequencies; and time sharing may not be feasible for passive systems that require continuous sensing. Therefore, spectrum sharing between passive and active systems requires an understanding of the operational and functional nature of each passive system and identification of the most suitable dimension (in time, frequency, or space), which should be used to carry out spectrum sharing with active users.

One existing approach for protecting terrestrial passive systems is to locate them in an area that is far away from high population density areas and is devoid of industrial development (e.g., RA telescope at Green Bank, WV, USA). The majority of interference that is detected in such remote sites is due to extra-terrestrial sources, interference propagation through the ionosphere, or tropospheric scatter from remote transmitters [89]. To mitigate such interference, *unilateral* techniques such as excision, cancellation and anti-coincidence are often employed [90]. However, the efficacy of the legacy unilateral approaches is inherently limited by the lack of coordination with the active sources of interference. More importantly, such unilateral approaches are not conducive to efficient utilization of the spectrum.

To enable efficient sharing between incumbent passive systems and secondary active systems, a *bilateral* approach that considers coordination between the two parties is needed, and this coordination can be handled by a spectrum management entity such as a SAS. Cooperative interference mitigation techniques coordinate the timing and regional use of the radio spectrum in a more dynamic manner. Active systems can cooperate by briefly interrupting or synchronizing radio transmissions to accommodate the passive measurements whenever and wherever needed.

Another scenario in which time-sharing can be employed is the coexistence of EESS systems and active secondary systems. To protect low-orbit EESS systems, SAS can employ a *no access zone* (i.e., a region where no SUs are allowed to transmit) that moves in synchronization with the satellite footprint's movement, similar in concept to a dynamic exclusion zone. In essence, spectrum access is being coordinated through the SAS, and the IUs and the SUs are time-sharing the spectrum. This notion of time-sharing is possible because most pas-

sive sensing applications require access to particular segments of the spectrum for relatively short durations only, and these durations can be pre-scheduled based on the information about the satellite's spectrum usage, orbital path, velocity, and the location and size of its instantaneous footprint on the earth.

2.3.2 Ex Post (Punitive) Approaches

In general, ex post enforcement approaches involve one or more of the following four enforcement steps:

Monitoring/Logging Interference Events

This step involves collecting information about users' activities that can later be used in adjudication procedures, if deemed necessary. In essence, logging the details of interference events is equivalent to collecting *forensic evidence*, which cannot be repudiated by the suspected interferer, during the adjudication process.

Identifying Non-Complaint Transmitters

This step involves the reliable identification and, if possible, authentication of the interference source. In the literature, identification mechanisms at the upper layers of the protocol stack have been used to authenticate or uniquely identify transmitters. However, these approaches are of limited value in ex post enforcement, because the enforcement entity (e.g., FCC) may not know the upper layers of the protocol stack used by the interference source, and, as a consequence, is unable to decode the upper layer signaling needed to identify the interferer. For this reason, authentication or identification at the PHY-layer is the most appealing approach for ex post enforcement.

PHY-layer authentication is an active area of research, and several schemes have been pro-

posed, which can be broadly categorized into two classes: intrinsic and extrinsic approaches. The former utilizes the transmitter-unique "*intrinsic*" characteristics of the waveform as unique signatures to authenticate/identify transmitters. They include RF fingerprinting, and electromagnetic signature identification [91, 92, 93, 94]. Extrinsic schemes enable a transmitter to "*extrinsically*" embed an authentication signal (e.g., digital signature) in the message signal and enable a receiver to extract it. Such schemes include PHY-layer watermarking [95, 96, 97, 98] and transmitter authentication [99, 100, 101, 102, 103, 104, 105]. On one hand, the intrinsic approaches require the blind receiver to have only a little knowledge about the transmission parameters to authenticate the transmitter, but they are limited by their low robustness against noise and security attacks [106]. On the other hand, the extrinsic approaches can be made highly robust against noise and security threats, but they require the blind receiver to have complete knowledge about the transmission parameters.

In some ex post enforcement scenarios, the enforcement entity may not have knowledge of the PHY-layer parameters used by the rogue or mal-functioning transmitters. In such situations, conventional PHY-layer authentication schemes (e.g., [95, 96, 99, 100, 101, 102]) cannot be used, because in those schemes, the verifier needs to know all of the PHY-layer parameters to correctly authenticate the transmitter. Kumar et al. [107] recently addressed this important issue by proposing a scheme that realizes *blind transmitter authentication* (BTA). The authors coin the term BTA to refer to the problem of authenticating a transmitter by extracting its unique, identifiable information from the received signal with little or no knowledge of the PHY-layer transmission parameters.

Note that most of the aforementioned schemes can be readily circumvented if tamper-resistance or integrity protection mechanisms are not employed to thwart hackers from removing or incapacitating the authentication mechanism used by the transmitter. There are a number of prior studies that have attempted to address this issue [108, 67].

Furthermore, PHY level identification may pose a threat to privacy or security if access and use of the information is not appropriately secured and in compliance with higher-

layer (network or application layer) policies and protocols. Practical implementation of such techniques will need to consider such cross-layer design issues. (These issues are addressed further in Section VI.)

Localizing Non-Complaint Transmitters

Once the malicious or mal-functioning transmitter has been identified, the next step is to localize it. In database-driven spectrum sharing, SUs need to register with the database. Hence, it would be straightforward for the database to know a rogue transmitter's approximate location, assuming that the transmitter identification step has been successfully completed. The challenge is to find out the precise geo-location of the rogue transmitter because it is unlikely that the rogue transmitter would provide any cooperation for its location estimation. Thus, the localization in cognitive radio networks has to be achieved via a non-interactive technique, e.g., by using localizing techniques such as direction of arrival estimation, or by implementing sensors/receivers to measure the received signal strength (RSS) [109, 110, 111, 112]. The RSS is an indicator of the link distance between a transmitter and a receiver. Hence, the information about the distances measured between the rogue transmitter and a set of receivers through RSS measurements can be merged at the regulator to localize the rogue transmitter.

Adjudication and Resolution

In the final step of ex post enforcement, the non-compliant transmitter is adjudicated and penalized. Malicious users can be penalized by either restricting their access to the spectrum for a certain duration of time or by imposing economic penalties. The severity of the punishment should be proportional to the severity of the non-compliant act and the estimated cost of the harm [113, 114]. However, the implications of imperfect enforcement must also be taken into account when designing an ex post enforcement methodology. The primary goal of adjudication/penalization should be to encourage and, if possible, incentivize SUs

to self-regulate and obey access rules, and not to mete out heavy-handed punishments to misbehaving users.

In the U.S., the responsibility of interference resolution and spectrum enforcement is centralized in the Enforcement Bureau of the FCC. In carrying out its enforcement activities, the Enforcement Bureau has several punitive measures at its disposal, including imposing monetary forfeitures, issuing cease and desist orders, and revoking operating authority (e.g., a station license). Traditionally, the Enforcement Bureau has relied on a number of enforcement tools, one of which is call signs and related identifiers. Call signs or call letters have been used since the early days of wireless communications to uniquely identify transmitting stations. By listening to and deciphering the call letters or related identifiers of an interfering fixed (but not mobile) transmitter, a regulator can identify and, if the geographic coordinates associated with the transmitter are known, locate the transmitter. Another legacy enforcement tool is station licenses. To operate a station, an operator has to first file an application for a station license to the FCC. The station license authorizes the licensee to operate the station for a pre-determined period of time after which the license needs to be renewed. The threat of license revocation often acts as a strong incentive for operators to obey the FCC's rules. Another traditional tool worth mentioning is operator licenses. Traditionally, the FCC has required those who operate and maintain transmitter stations to be licensed.

Unfortunately, most, if not all, of the traditional enforcement tools mentioned above have little value in spectrum sharing scenarios [115]. For instance, the utility of traditional call signs for enforcement activities has dwindled away to almost nothing due to the widespread movement from analog transmitters to digital transmitters and from aural to data communications. Station licenses cannot be used as an enforcement tool because most SUs (who opportunistically access fallow spectrum) are unlicensed users in the envisioned SAS ecosystem. Further, operator licensing has been largely phased out in most services. This is due to the fact that, in modern systems, procedures for accessing channels are controlled by computer logic, and minimal or no expertise on the part of the operator is required to ensure

efficient operation and control interference.

The limitations of legacy approaches for enforcing access rules in spectrum sharing scenarios necessitate the development of a new set of enforcement tools. Interference resolution and enforcement is one of the fundamental requirements that must be met to enable government-commercial spectrum sharing. The willingness of government agencies to share spectrum on a more expanded and dynamic basis depends on their confidence that the applicable regulations and rules regarding interference will be effective and enforced in an appropriate time frame [115]. Also, the value of shared government spectrum to commercial entities depends on their confidence that the regulators have applicable rules and tools in place to effectively control the number of interference incidents and have the ability to resolve incidents promptly.

To enhance the efficiency of enforcement, it is important to consider the design of ex ante and ex post frameworks concurrently to ensure they are mutually re-enforcing so as to maximize the likelihood of compliant behavior and minimize the total costs imposed of ensuring such compliance. Creative approaches should be considered. For example, it may be feasible to have negative penalties as part of an ex post regime. Under these, radios which establish a record of good performance might be granted additional permissions or expanded access to spectrum resources as way to incentivize compliance with access and radio operation rules. Alternatively, crowd-sourcing and other techniques for distributing the costs and responsibilities for enforcement may augment and ease the enforcement burden falling on traditional regulatory institutions such as the FCC. How to integrate such novel techniques into existing rules and institutional management frameworks poses an open research challenge.

2.4 Coexistence between Heterogeneous Wireless Technologies

In the previous section, we focused on the general problem of interference protection as represented by the various mechanisms used to enforce coexistence between IUs and SUs. In this section, we discuss an equally important problem, viz., techniques for assuring harmonious sharing between *heterogeneous* wireless access technologies. Compared to IU-SU coexistence, SU-SU coexistence has attracted much less attention from the regulators as well as the research community. This may be partially due to the experience in the ISM bands, where diverse technologies, such as Wi-Fi and Bluetooth, coexist harmoniously, in most situations, without a common coexistence mechanism. However, the coexistence situation in the TV bands and other shared-access bands (e.g., 3.5 and 5 GHz bands) is more complex and challenging due to a number of reasons, including the use of devices with higher transmission power, disparity of PHY/MAC strategies employed by the secondary systems, and the competition among the commercial service providers that aim to augment their existing network capacity with additional capacity tapped from those bands.

2.4.1 TV Band: Coexistence among SUs

In order to address the coexistence issues among TVWS devices, industry stakeholders have undertaken active steps towards standardizing several TVWS technologies, including ECMA-392 [116], IEEE 802.19.1 [117], 802.22 [118], 802.11af [119], and 802.15.4m [120]. In addition, the DySPAN Standards Committee formed a new 1900.7 task group (TG) to create another standard for TVWS [121]. To address the problem of secondary network coexistence in TVWS, the 802.19.1 TG was formed [117, 122]. The purpose of the 802.19.1 standard is to enable the family of 802 wireless standards to most effectively use TVWS by providing standard coexistence methods among dissimilar or independently operated TVWS networks and dissimilar TVWS devices [123]. This standard addresses coexistence issues among IEEE

802 networks and devices and will also be useful for non-IEEE 802 networks and TVWS devices. It acts as an interface between coexisting networks, providing functionality related to identification of 802.19.1-compliant systems (e.g., via registration), obtaining/updating coexistence information (e.g., from databases), and using intelligent decision making algorithms to facilitate harmonious coexistence (e.g., decide which actions should be taken by networks to solve coexistence problems).

2.4.2 5 GHz Band: Coexistence between Wi-Fi and LTE-U

Recently, the 5 GHz bands have attracted significant interest for launching new wireless applications and services because of their favorable propagation characteristics and the relative abundance of spectrum therein (580 MHz in the U.S., $455 - 605$ MHz in Europe, 325 MHz in China [124]). There are proposals from multiple industry stakeholders such as Qualcomm and others to extend the deployment of LTE-Advanced (LTE-A) to the 5 GHz U-NII bands by exploiting a number of available technologies, such as carrier aggregation (CA) and supplemental downlink (SDL) [125, 126]. This so-called pre-standard LTE-U approach is applicable to regions that do not have a Listen Before Talk (LBT) requirement on accessing the U-NII bands (e.g., US, China, and South Korea). For instance, CA/SDL can be used in LTE FDD mode to augment the data-carrying capacity of the downlink from the LTE eNodeB to the LTE user equipment (UE), thus creating a fat downlink pipe. Control and management functions, as well as time-critical communications, are likely to continue to take place over the licensed ("anchor") channel. In other regions of the world (e.g., Europe, Japan), regulators require devices that wish to access the U-NII bands to execute the LBT procedure at the milliseconds scale. Ongoing 3GPP standardization efforts that aim to make LTE compatible with the LBT procedure are referred to as LAA. The introduction of LTE-U (or LAA) in the 5 GHz bands will require current and future Wi-Fi technologies operating in these bands to share spectrum with LTE-U (or LAA) devices.

Coexistence in the 5 GHz bands has been studied in several previous works, which focused

on different aspects, including channel interference, spectrum sharing, and scheduling. Part of the challenge is that technologies like Wi-Fi rely on distributed access control mechanisms whereas technologies like LTE take advantage of operator-centralized control, which proponents of distributed access models argue may give LTE-like technologies an unfair advantage in accessing the shared spectrum. An investigation of the performance of co-existing LTE and WLAN on the license-exempt band [127] shows that WLAN technologies hold their transmissions when channel interference is detected, while LTE reduces its transmission speed in order to increase the transmission robustness. Authors of [128] propose to apply the Request-to-Send/Clear-to-Send (RTS/CTS) protocol to LTE eNodeBs, so that the WLAN networks do not always yield to LTE transmissions. A large number of related works study spectrum sharing. Xing et al. [129] propose an adaptive spectrum sharing technique in which LTE should adjust its subframe configuration periodically to adapt to the traffic load of WLAN system. Authors of [130] propose spectrum sharing using a spectrum consumption model. This mechanism considers spectrum management policies, including existing users convey restrictions to new users, spectrum trading [131], service-level agreement [132], etc. Some works study the spectrum sharing in unlicensed band using game theory [133, 134]. Yun et al. [135] propose a new algorithm to decode two interfering cross technology Orthogonal Frequency Division Modulation (OFDM) signals without alignment in time or frequency. Although their algorithm allows LTE and Wi-Fi to transmit simultaneously, the proposed estimation and decoding technology must be applied to each receiver device.

Enabling a fair coexistence between LTE-U and Wi-Fi is challenging due to the disparity between their MAC protocols and the "greedy" nature of LTE-U. LTE-U adopts a schedule-based access approach, whereas Wi-Fi uses contention-based random access. Although LTE-U employs a number of coexistence techniques (e.g., carrier-sensing adaptive transmission (CSAT)), it still exhibits an inherently more aggressive approach in accessing the spectrum compared to Wi-Fi. Fairness is critically important in this case as the two coexisting technologies have the same spectrum access priority.

2.4.3 5 GHz Band: Coexistence between Wi-Fi and DSRC

Wi-Fi stakeholders in the U.S. have been lobbying the government for access to more spectrum in the 5 GHz bands in order to deploy their next-generation technologies, such as 802.11ac and 802.11ax. In response to the rapidly accelerating adoption of Wi-Fi, particularly the burgeoning 802.11ac standard, the FCC issued an NPRM in 2013 [27] that recommends adding 195 MHz of additional spectrum by opening up the ITS band ($5.850 - 5.925$ GHz), where DSRC users are the IUs, to unlicensed devices. Inclusion of the ITS band permits one additional 80 MHz and one additional 160 MHz channel for 802.11ac or 802.11ax. However, the realization of this scenario requires a careful design of the coexistence framework. The coexistence of ITS applications with Wi-Fi may severely degrade the performance of the former, especially safety applications that are very sensitive to communication latency [136]. Moreover, when the ITS band was first allocated in 1999, the FCC's original intention was for this band to support DSRC for ITS exclusively, and hence the ITS protocol stack or the relevant applications designed thereafter were not designed to coexist with unlicensed devices.

The coexistence of DSRC and Wi-Fi raises a totally different set of challenges than the ones discussed in Section 2.4.2. In this case, DSRC is the incumbent user, and Wi-Fi is the secondary user with lower priority. Incumbent protection is a major challenge because the incumbent users are highly mobile vehicular nodes that utilize spectrum in a dynamic manner in spatial and temporal dimensions. The difficulty of the problem is exacerbated by the fact that 802.11ac/802.11ax has a distinct advantage over DSRC in accessing the spectrum due to its shorter interframe space (IFS) values, which could have a very negative impact on the communication latency of DSRC safety applications.

2.4.4 Coexistence in Spectrum Bands above 6 GHz

Due to the scarcity of spectrum at frequencies below 6 GHz, the use of higher frequencies such as those in the mmWave bands has been proposed for 5G cellular systems. In general, mmWave communication systems cause less interference to neighboring cells operating in the same frequency bands compared to communication at lower frequencies [137]. The noise-limited behavior inherent in mmWave communication systems may allow them to share the spectrum without any prior coordination. However, the requirement of highly directional and adaptive transmissions, directional isolation between links, and significant possibilities of outage have strong implications on multiple access, channel structure, synchronization, and receiver design [138]. In this regard, several industry stakeholders and regulatory bodies, including IMT-2020 in China, OfCom in the UK and FCC in the US, have been actively seeking comments and proposals regarding coexistence mechanisms for bands above 6 GHz [35, 54].

2.5 Security and Privacy Issues

In the preceding two sections we discussed the important challenge of managing interference. Many of the mechanisms discussed relied on the collection, analysis, and sharing of information about the radio environment and spectrum usage in order to ensure efficient collective use of the spectrum. Much of this information has the potential to pose a threat to the confidentiality and privacy of spectrum users. For example, unauthorized access to the location, technical capabilities, or usage behavior of SUs or IUs could pose a significant threat to users strategic interests and privacy. In this section, we turn to another important challenge: the need to protect the privacy and confidentiality of information collected as a byproduct of spectrum management.

For example, the use of spectrum databases offers a pragmatic approach for enabling spectrum sharing between government (IU) and commercial users (SUs), but at the same time, it

incurs a number of security and privacy concerns by unintentionally facilitating the collection and aggregation of sensitive information by adversial SUs [139]. Examples include threats to the operational security (OPSEC) of the incumbents (e.g., Naval radar systems), privacy of the SUs (e.g., by potentially enabling location-tracking of individuals), and attacks targeting the SAS infrastructure.

2.5.1 OPSEC Threats to the Incumbents and Countermeasures

Although using geolocation databases is a practical and cost-effective approach for enabling spectrum sharing, it poses a potentially serious OPSEC problem. SUs (queriers), through seemingly innocuous queries to the database, can infer *operational attributes* (e.g., location, type, times-of-operation, antenna attributes, receiver sensitivity, etc.) of the incumbents, and thus compromise their OPSEC [139]. Figure 2.6 illustrates this threat, which is referred to as an *inference* attack. A malicious user can infer the sensitive data of incumbents even if the database does not directly reveal such information. When incumbents are federal government systems, including mission-critical military systems and public-safety entities, such as in the U.S. 3.5 GHz band, this breach of incumbents' OPSEC is a critical issue. Although potentially less serious, OPSEC concerns may arise among commercial users who may be concerned about access to strategically sensitive information by competitors or threats to the privacy of their customers from unauthorized access to database information.

The problem of incumbents' OPSEC cannot be adequately addressed by tightly controlling access to the database because: i) all SUs need to access the database to realize spectrum sharing, and ii) identifying malicious SUs is challenging, especially when they are *inside-attackers* (i.e., legitimate/authorized users performing illegitimate/unauthorized actions). A more viable approach may be to "obfuscate" the information revealed by the database in an intelligent manner such that a certain level of OPSEC is assured while supporting efficient use of the spectrum [63]. Several obfuscation schemes, such as perturbation, transfiguration, k-anonymity and k-clustering, are proposed in [139]. Differential privacy [140] is

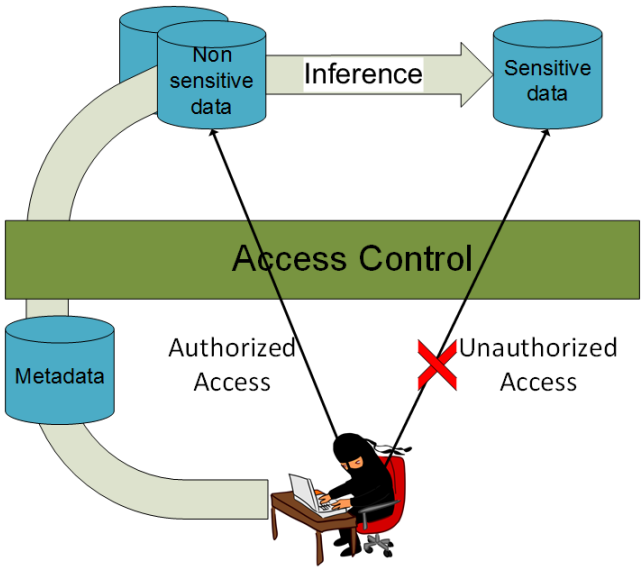


Figure 2.6: Indirect information access via inference channel.

another emerging privacy-preserving paradigm that provides a semantic privacy model with strong protection guarantees: it captures the amount of disclosure that occurs due to the publication of sensitive data in addition to mandating how the published data should look. A generalization of differential privacy, called "geo-indistinguishability", has been studied in [141, 142] for protecting the location privacy of users in the context of location based services.

2.5.2 Privacy Threats to the SUs and Countermeasures

Another issue in database-driven spectrum sharing is the privacy of SUs. Since SUs need to send their operational attributes (e.g., identity, location, antenna parameters, etc.) to the database for obtaining the spectrum availability information in their region, their privacy may be threatened by an untrustworthy/semi-trustworthy database. An example of such a database is a compromised SAS that is managed by a commercial entity, which provides accurate spectrum availability information but may misuse the querier's information for its own benefit. An untrustworthy or a compromised database can directly infer a SU's

information including its spectrum usage habits, device type, times of operation, mobility, etc. [143]. One way to counter this threat is to use a two-way authentication protocol between the SAS and the SU—it enables both the SAS and the SU to authenticate each other. Homomorphic encryption-based private information retrieval [144] is another approach for accessing data privately from an untrustworthy/semi-trusted database. Other techniques that have been studied in the context of LBS to preserve the users' location privacy include sending a space- or time-obfuscated version of the users' actual locations [145, 146], hiding some of the users' locations by using mix zones [147], sending fake queries, indistinguishable from real queries, issued from fake locations to the database [148], and applying k-anonymity [149] to location privacy.

2.5.3 Security Threats to the SAS and Remedies

In addition to aforementioned threats to the security and privacy of the IUs and the SUs, there are other security concerns associated with database-driven spectrum sharing. One such concern is the threats against the infrastructure that govern spectrum access and sharing (i.e., SAS or SAS-like infrastructure). Similar to the Internet's DNS (Domain Name System), it is expected that several physical SASs will be networked together to form a region-wide infrastructure. Therefore, some of the security threats against DNS servers may be applicable to the SAS as well. A malicious user may modify its own device to masquerade as another certified device. An attacker can spoof a spectrum database and can modify/jam the query sent by another device or modify/jam the database-response that was intended for some other legitimate device. Adversaries can maliciously alter the contents of the SAS (a.k.a. SAS poisoning). Malicious groups may redirect a legitimate SAS's traffic to another bogus server (a.k.a. SAS pharming). Similarly, denail-of-service to the legitimate SUs can be caused by bombarding a large number of bogus queries to the SAS [63].

Most of the aforementioned security threats may be addressed by implementing a *two-way encrypted authentication* between the SAS and the SU (querier). Authentication thwarts

masquerade and database spoofing attacks. Cryptography-based integrity protection mechanisms (e.g., message authentication codes) prevent adversaries from modifying spectrum queries/responses without being detected, and the same applies to the unauthorized modification of the SAS contents. In terms of countering threats to the availability of SAS, maintaining redundancy in the SAS's contents is one straightforward technique. The efficacy of this technique has been demonstrated in several attack incidents of the past, including the distributed-denial-of-service (DDoS) attack that was launched against DNS root servers in October of 2007 [150].

2.6 Open Problems and Research Challenges

While radio and networking technical capabilities have improved substantially and while promising reform initiatives are underway enabling progress toward realization of the DSA vision articulated earlier, much remains to be done. New radio capabilities breed new demands for access to spectrum, and the continuing process of technical, market, and policy innovations is continuously creating new SUs seeking access to spectrum. There are a number of open challenges in both the technological and policy domains. Some of these are discussed in the following subsections and summarized in Table 2.1.

2.6.1 Spectrum Efficiency and Access

One of the key challenges in dynamic spectrum sharing is the effective management of spectrum resources. It requires advancements in allocation and assignment mechanisms that not only facilitate spectrum sharing, but also support measurement and dynamic assessment of the costs and benefits of sharing. It is a multidisciplinary challenge that requires a joint engagement of technical, economic and policy perspectives [151]. Further research is needed to develop and advance our ability to quantify spectrum efficiency, harmful interference, spectrum value and fair access to the spectrum.

Table 2.1: Open problems and research challenges in dynamic spectrum sharing

Category	**Open Problems and Research Challenges**
1. Spectrum allocation/assignment and spectrum management	• New access paradigms and protocols for efficient spectrum use. • Models that incentivize incumbents to share their licensed spectrum or to relocate to other bands. • Sharing between commercial and non-commercial users (e.g., federal-commercial sharing). • Models and techniques, including dynamic spectrum markets/auctions, for assignment of spectrum. • Frameworks for defining dynamic and flexible incumbent protection zones. • Approaches for incorporating real-time sensing results with database-driven spectrum sharing.
2. Metrics to quantify spectrum usage	• Quantifying spectrum efficiency, value of spectrum and fair access to the spectrum. • Defining techniques and standards for spectrum measurement. • Quantitative definition of harmful interference, and its applications. • Quantifying receiver performance in real-world spectrum sharing environment. • Tools for evaluating the economic and technical trade-offs in spectrum sharing.
3. Interference management and coexistence	• Techniques for enabling harmonious coexistence between heterogeneous wireless technologies. • Adaptive modulation schemes to enable coexistence and interference mitigation. • Realistic propagation models for frequencies that are being considered for new applications. • Mathematical models of interference and techniques for mitigating interference. • Models for radio system performance with trade-off assessment capabilities. • Interference-tolerant waveforms and protocols. • Techniques and policies for protecting passive IUs.

Category	**Open Problems and Research Challenges**
4. Security and enforcement	• Vulnerability studies of flexible spectrum access systems and development of countermeasures. • Investigating the trade-off between OPSEC and implementation complexity in spectrum sharing. • Hardware and software technologies for enforcing spectrum sharing rules. • Techniques and policies for identifying, adjudicating and punishing non-compliant radio devices. • Defining property rights, and mechanisms to enforce those rights. • Automated enforcement mechanisms and compliance certification methods.
5. Radio hardware and software	• Reconfigurable radio hardware, including antennas, amplifiers, filters, tuners, etc. • Improvements in smart radio architectures that support high dynamic range for wideband operation. • Radio hardware that supports operation in the millimeter wave band. • Designing low-power or energy-harvesting devices for sustainability. • Hardware that provide improved geolocation, direction-finding and interference nulling capabilities. • Clearly defined metrics for quantifying advances in radio hardware and software.
6. Protocols and standards	• Frequency-, space-, and time-cognizant protocols that dynamically leverage multi-functional radio hardware and software. • Standards that support pre-emptive spectrum access for emergency services. • Protocols and standards for carrier aggregation. • Database-access-protocols for database-driven sharing. • Standards for radio propagation measurement for different bands.

Category	**Open Problems and Research Challenges**
7. Experimentation, testing and standardization	• Development of advanced and adaptable test beds using advances in hardware, software and policy. • Virtual test beds, including the use of computer simulations, to model and assess coexistence techniques in large-scale spectrum sharing scenario. • Proofs-of-concept demonstrations covering a variety of bands, applications and geographical areas. • Standardization of current/future test beds.
8. Policy, regulatory and economic issues	• Service level agreements for negotiated sharing. • Understanding the possible impact of new radio technologies on health and environment. • Risk assessment techniques for evaluating when and how to share the spectrum between users. • Strategies for designing dynamic spectrum auctions and markets. • Assessment of economic trade-offs in incentivizing spectrum sharing under multiple scenarios. • Strategies to inventivize spectrum sensing. • Devising economic models and processes that can operate on huge datasets of wireless feedback, rapidly assess spectrum usage, and adjust spectrum sharing parameters in real-time.

To increase the resolution of spectrum availability and utilization, there is a need to augment the spectrum database content with real-time sensing results [152]. Advanced spectrum sensing techniques are needed to quickly and accurately identify transmission opportunities over a very wide spectrum pool that may host a large number of different wireless services. However, designing a framework that enables the marriage of database-driven and sensing-driven spectrum sharing approaches remains an open problem. Furthermore, sharing between users with different access-priorities confront novel challenges that demand study of new access paradigms and protocols, dynamic and flexible incumbent protection zones, and adaptive models for spectrum allocation and assignment. We summarize open research challenges related to spectrum efficiency and access in Category 1 and 2 of Table 2.1.

2.6.2 Coexistence and Interference Management

Facilitating harmonious coexistence among heterogeneous wireless technologies is another challenge in dynamic spectrum sharing (see Category 3 of Table 2.1). First and foremost, specific metrics need to be established for assessing how well devices are coexisting together. There is also a need to develop modulation schemes that adapt in concert with other system components to enable interference mitigation/avoidance. Realistic propagation models, including inferential models (models that allow the prediction of signal loss at one frequency from measurements at other), for frequencies that are being considered for new applications enable regulators and policy makers to foresee the merits of coexistence in both technological and non-technological aspects.

Future spectrum sharing scenarios require coexistence among secondary users of the spectrum (e.g., LTE-U and Wi-Fi in the 5 GHz band). Facilitating SU-SU coexistence requires the development of techniques that have not been studied before. For example, even with TV white space systems using database approaches, the issue of how multiple white space networks might co-exist and coordinate with each other is yet to be explored [117]. The databases inform the radios which TV channels are available—they say nothing about other

data networks that might be trying to use the available TV channels.

Moreover, spectrum coordination or cooperation between disparate networks, such as a government network as an IU and a commercial mobile network as a SU, as required in U.S. 3.5 GHz band, is just in the beginning phase. Sharing between government and commercial entities will require innovations in technology as well as in business, administrative, and market institutions and practices. Special-purpose wireless systems may be difficult to accommodate within bold new spectrum-use models because of fundamental limitations on frequency agility due to basic operational requirements, extreme sensitivity to interference, or potentially drastic consequences due to failure of a radio frequency link. Innovative solutions for accommodating such systems are needed. These systems may include medical devices, surveillance, remote sensing, and passive systems such as radio telescopes. Furthermore, coexistence with legacy systems is an additional challenge because of backward and forward inter-operability and compatibility.

2.6.3 Hardware, Software, Protocols and Standards

Improving spectral efficiency and radio configurability for hardware and software-defined radios is crucial for enabling the commercialization of appropriate spectrum sharing customer and network equipment. This requires advancements in smart radio architectures that support high dynamic range for wideband operation. New technologies and applications above 6 GHz are a promising emerging area. Designing power efficient radios that support high bandwidth and multi-antenna applications is another challenging problem that needs to be addressed.

New advances in the areas of radio hardware, software, signal processing, protocols and access theory need to be developed such that they will work in concert, flexibly and over time to support wireless technologies of diverse needs. Fundamental limits in these areas also need to be explored. There is also a need to design hardware that provide improved geolocation capabilities for indoor applications, direction-finding and interference-nulling capabilities.

For sustainability, research should focus on designing low power energy-harvesting devices.

Besides hardware, there is a need to develop simulation tools and software for evaluating the efficiency and scalability of newly proposed architectures. Frequency-, space-, and time-cognizant protocols need to be developed for improving the spectral efficiency. Standards need to be defined for technologies such as carrier aggregation, database-access-protocol and radio propagation measurement for different bands. These issues are outlined in Category 5 and 6 of Table 2.1.

2.6.4 Security and Enforcement

The successful deployment of new spectrum access technologies, such as cognitive radios, and the realization of their benefits will partly depend on the placement of essential security mechanisms in sufficiently robust form to resist misuse of the technologies. The emergence of new spectrum access technologies and spectrum utilization paradigms raise new security challenges that have not been studied previously. Vulnerability studies of flexible spectrum access systems and development of countermeasures is central to realizing effective spectrum sharing.

There is a need to study obfuscation techniques that meet the OPSEC requirements of incumbent users, especially military users, while enabling efficient spectrum utilization. Studies must also focus on thwarting threats against the infrastructure that govern spectrum access and sharing. Furthermore, regulators and policy makers need to understand what data from spectrum usage can be collected and analyzed to assess spectrum utilization without infringing on the users' privacy. Note that more reliable and effective enforcement regimes often result in greater infringement of the user's privacy rights. Multidisciplinary research efforts are needed to study this issue, and to explore the technical and sociological solution approaches for balancing the two, seemingly opposing, goals of enforcement and privacy.

Frequency agile radios combined with compliance and enforcement requirements necessitate

research in the following areas: (i) automating the detection and identification of interference sources; (ii) creating mechanisms for rapidly enforcing policy changes on radio devices; (iii) evaluating the sociology of privacy, enforcement mechanisms, and potential penalties; and (iv) evaluating the economic trade-offs in ex-ante and ex-post mechanisms. As wireless systems become more advanced, certifying new wireless devices (especially those which are based on software defined radio) for compliance becomes non-trivial because of the radio's reconfigurable and frequency-agile nature [153, 154, 155]. Beyond certification, monitoring will be needed to ensure that deployed systems are in compliance, and when they are not, enforcement procedures will be needed to remedy the problems. Some of the open problems and research challenges related to spectrum enforcement, compliance and security are enumerated in Category 4 of Table 2.1.

2.6.5 Experimentation, Testing and Standardization

To ensure that the new technologies will not cause harm to legacy systems, are robust and secure, and are efficient users of the spectrum, testing of new technology through large-scale experimentation is essential. Such testing will also prove helpful in raising stakeholder trust that the new sharing approaches will work as promised. This requires new tests, measurement solutions, standards and regulatory validation. Measurements and metrics to establish existing and future levels of spectrum occupancy and efficiency will also be required. Development of advanced and adaptable test beds using advances in hardware, software and policy; proof-of-concept demonstrations; and standardization of current/future test beds are imperative to assess the performance of new technologies. Open problems related to experimentation, testing and standardization are listed in Category 7 of Table 2.1.

2.6.6 Regulatory and Policy Challenges

Beyond technical issues, there are also policy-domain challenges in dynamic spectrum sharing. Future sharing systems may employ dynamic spectrum markets in which primary licensees can sell spectrum access to SUs on a temporary basis. There exists a need for interdisciplinary research in the areas of market- and non-market-based mechanisms for spectrum access and usage to efficiently organize the sharing of scarce spectrum resources. For spectrum markets to work efficiently, there has to be sufficiently liquid supply and demand of spectrum resources to make it worthwhile incurring the transaction costs associated with administering and making use of the markets. Thus, it is also important to consider how to enhance the value of spectrum to SUs. For instance, sharing might only be of a little value if an IU needs arbitrary access to the spectrum because this prevents SUs from predicting the availability of spectrum.

Market barriers (e.g., transaction costs, lack of incentives, strategic concerns) and limited availability of information (e.g., unavailability of federal-IUs' operational parameters) all pose policy challenges for realizing the potential of spectrum sharing. Other challenges include authorization constraints (e.g., regulatory and policy requirements); and lack of incentives for incumbents to share (e.g., incumbents may see future spectrum sharing only as a threat to their own use) [11]. Also, there are issues related to health and environmental ramifications of emerging technologies. Interdisciplinary collaboration among researchers of diverse backgrounds is crucial in addressing these challenges.

Finally, the design of radio systems is inherently cross-disciplinary since the technologies are only a part of the larger system which includes the stakeholders, markets, and institutional frameworks within which those technical systems operate and evolve. The technologies, business models, markets, and regulatory frameworks need to co-evolve. Category 8 of Table 2.1 outlines some of the policy, regulatory and economic challenges in dynamic spectrum sharing.

2.7 Chapter Summary

This chapter has provided a comprehensive review of important trends, regulatory reform initiatives, and research challenges that are part of the ongoing systematic efforts to bring about fundamental changes to how we manage and utilize radio spectrum. Most of the legacy spectrum regimes employed throughout the world are overly static and inflexible, making it difficult, if not impossible, to utilize spectrum to its full potential in an efficient manner. Dedicated exclusive-use assignments, premised on archaic notions of radio technology, reduced incentives to use spectrum efficiently and contributed to problems of artificial scarcity, thereby impeding growth and innovation in wireless services and technologies. The future needs to embrace more dynamic models of spectrum sharing, or Dynamic Spectrum Access (DSA), in which spectrum may be shared along multiple technical dimensions (e.g., frequency, time, space, and direction) and across multiple usage contexts (e.g., commercial/government, legacy/new, licensed/unlicensed, or multiple classes of spectrum rights holders). Realizing this DSA vision requires the co-evolution of technical, regulatory, and business models for managing how spectrum usage rights are administered and enforced. Rendering traditional mechanisms such as static exclusion zones more dynamic [70], incorporating database technologies, and augmenting those with sensing capabilities represent distinct but complementary steps on the path to dynamic spectrum sharing.

Chapter 3

TESSO: An Analytical Framework for Exploring Spatial Sharing Opportunities

3.1 Introduction

The accurate prediction of radio propagation path loss plays a crucial role in realizing effective spatial spectrum sharing, particularly in the context of geolocation database (GDB)-driven spectrum sharing. In GDB-driven spectrum sharing, such as sharing dictated by a Spectrum Access System (SAS)[1], a spectrum management entity first computes the expected co-channel interference that a prospective SU may cause to the IU. To compute the expected interference, the SAS uses an appropriate radio propagation path loss model[2] as well as information such as the SU's and the IU's geo-locations, their antenna parameters and the SU's transmit power. The result of this analysis is then combined with informa-

[1]The Spectrum Access System is the term used in the recent FCC and NTIA documents to denote a network of databases and spectrum managers deployed to enable dynamic spectrum sharing.

[2]A radio propagation model is an empirical mathematical formulation for the characterization of radio propagation path loss as a function of frequency, distance and other parameters.

tion about the IU's interference protection criteria to compute spectrum availability at the prospective SU's location. If the estimated aggregate interference to the co-channel IU is below its interference tolerance threshold, the SU is allowed to transmit in the co-channel; otherwise not. To fully reap the benefits of spectrum sharing, an accurate propagation analysis is desired. A propagation analysis that over-estimates path loss between the SU and the IU will under-estimate the potential for co-channel interference, providing inadequate interference protection for the IU. In contrast, an analysis that under-estimates the path loss will unnecessarily preclude SUs from taking advantage of fallow spectrum.

Often times, in spectrum sharing, multiple SUs share the spectrum with an IU. For example, in the three-tiered sharing architecture of the U.S. 3.5 GHz band, multiple Priority Access Licensed (PAL) users and General Authorized Access (GAA) users share the band with an incumbent ship-borne radar [5]. Here, the interference power received at the IU is not just the interference caused by a single SU, but in fact, it is the *aggregate interference* caused by multiple SUs. To ensure harmonious coexistence, the spectrum manager of a purely GDB-driven spectrum sharing ecosystem should estimate the aggregate interference, and allow an entrant SU to transmit in the co-channel only if doing so does not cause harmful interference to the IU.

Studies have shown that the use of terrain-based propagation models, such as Irregular Terrain Model (ITM) in point to point (PTP) mode[3], improves the efficacy of spectrum sharing because such models accurately estimate the path loss in a communication link [156]. For example, in June 2015, the National Telecommunications and Information Administration (NTIA) published a report that shows that the exclusion zone[4] of IUs in the 3.5 GHz band can be reduced by up to 70% when legacy propagation models are replaced by terrain-based propagation models such as ITM-PTP model [13]. However, using ITM-PTP for characterizing aggregate interference caused by multiple SUs might not be viable for several reasons.

[3]The ITM in PTP mode is the most popular terrain-based propagation model in use today.

[4]An exclusion zone is the area around an IU where co-channel/adjacent-channel transmissions from SUs are prohibited.

First, ITM-PTP model is computationally intensive and data hungry due to the consideration of detailed environmental parameters in path loss computations. Therefore, when N SUs are likely to share the spectrum with an IU—i.e., when N interferers possibly contribute to the aggregate interference at the IU—computing the aggregate interference requires N ITM-PTP path loss computations, which requires very long processing time when N is large. Second, ITM-PTP requires accurate geo-locations of SUs which might not be available in some spectrum sharing scenarios (e.g., the precise locations of SUs might not be available when they are mobile, or when they obfuscate their geo-locations for achieving location privacy).

Due to the aforementioned limitations of ITM-PTP, an alternative approach, or an analytical tool, for characterizing the aggregate interference is desirable in some spectrum sharing scenarios. The tool should be able to accurately estimate the aggregate interference in a computationally efficient manner, and it should be effective even when precise geo-locations of SUs are not available. In this chapter, we propose an analytical tool that we refer to as *Tool for Enabling Spatial Spectrum Sharing Opportunities (TESSO)*. TESSO is a tool that can be employed by a central spectrum management entity (such as a SAS) to perform real-time estimates of the SUs' aggregate interference power, which is the key parameter needed to perform spectrum access control (i.e., control which and how many SUs are allowed to access spectrum). The main features of TESSO are summarized below:

- TESSO enables us to analytically model the aggregate interference caused by SUs (as measured at an IU). Using the mathematical model for aggregate interference, TESSO effectively facilitates GDBs to identify spatial spectrum sharing opportunities around an IU.

- TESSO is computationally efficient, and it can be implemented by a SAS ecosystem in real-time to compute the maximum number of SUs, say N, that can be safely allowed to co-exist with an IU. To compute N, TESSO does not require the precise geo-locations of the SUs.

- The performance of TESSO, in terms of spectrum utilization and incumbent protection, is comparable to that of computationally intensive terrain-based propagation models, such as ITM-PTP.

The road map of the rest of the chapter is as follows. In Section 3.2, we discuss the preliminaries. In Section 3.3, we demonstrate the effectiveness of terrain-based propagation model in enabling spatial spectrum sharing opportunities and illustrate how ITM-PTP mode ensures the protection of IU from aggregate interference caused due to SUs. Later, in Section 3.4, we introduce and provide details of TESSO. Case studies for evaluating the performance of TESSO are presented in Section 6.6. Finally, Section 5.8 concludes the chapter.

3.2 Preliminaries

3.2.1 Irregular Terrain Model

The ITM is a radio propagation model, which predicts tropospheric radio transmission loss over irregular terrain for a radio link [157]. It is designed for use at frequencies between 20 MHz and 20 GHz, and for path lengths between 1 km and 2000 km. ITM estimates radio propagation loss as a function of distance and other system and environmental factors such as variables in time and space. Radio propagation loss is computed based on electromagnetic theory, and signal loss variability expressions are derived from comprehensive sets of measurements. ITM is both data and computationally intensive. There are two modes of operation of ITM: (i) Area prediction (ITM-AP) mode, and (ii) Point-to-point (ITM-PTP) mode.

In the ITM-AP mode, the term "area" is described by the terrain irregularity parameter, Δh, and the effective antenna heights of the system. The suggested values of Δh for different terrains are given in [158]. Based on Δh and other parameters, the ITM-AP mode predicts the path loss between any two given points. In contrast, the ITM-PTP mode takes into

account the actual obstructions between the transmitter and the receiver. To make its predictions, the ITM-PTP mode incorporates the principal determinants of radio propagation over irregular terrain paths, which include [159]:

- the amount by which the direct ray clears terrain prominences or is blocked by them;
- the position of terrain obstacles along the path;
- the strong influence of the degree of roundness of these terrain features; and
- the apparent earth flattening due to atmospheric refraction.

The ITM-PTP mode relates the statistical variance of terrain elevations to classical diffraction theory, and predictions made by the model agree closely with the measured data. Comparison with actual propagation measurements validates that path loss values calculated by the ITM-PTP mode are quite accurate; and moreover that the accuracy of the ITM-PTP mode is as good as or better than that achieved by alternative procedures [159]. In this chapter, we synonymously use the term *terrain-based propagation model* to refer to the ITM-PTP model.

3.2.2 Aggregate Interference

When multiple SUs share the spectrum with an IU, the interference power received at the IU is not just the interference caused by a single SU, but it is the aggregate interference caused by multiple SUs. A successful design and deployment of dynamic spectrum access, therefore, requires an accurate model for characterizing the aggregate interference. This characterization feeds into the design of transmission policies for SUs and protects IUs from SU-generated interference.

To characterize the performance of IUs in dynamic spectrum access, a detailed analysis of the aggregate interference needs to be done. In practical networks, a multitude of factors must

be considered together in order to arrive at an accurate statistical model for the aggregate interference. Aggregate interference depends on propagation characteristics of the channels between the SUs and the IU, such as path loss, shadowing and fading, and also on the transmit power control scheme used by the SUs. Terrain characteristics in the link between the SUs and the IU also affect the distribution of aggregate interference. Furthermore, the number of SUs that transmit and their locations, themselves are random variables and affect the aggregate interference.

Given the importance of aggregate-interference modeling in dynamic spectrum access, researchers have studied this topic extensively in the past few years. Some works focus on developing statistical interference models, while others provide exact analysis and performance bounds. For example, Bhattarai et. al. in [160] derived an expression for the aggregate interference by considering a path loss model that is based on exponential path loss and log-normal shadowing. They showed that the aggregate interference from a fixed number of SUs, distributed uniformly over a region, can be modeled as a log-normal random variable. In [161], the authors used the method of log-cumulants to approximate the distribution parameters of the aggregate interference. Ghasemi and Sousa, in [162], developed a statistical model of interference aggregation in spectrum-sensing cognitive wireless networks by explicitly taking into account the random variations in the number, location and transmitted power of SUs as well as the propagation characteristics. The authors of [163] suggest that, for arbitrarily-shaped network regions, the shifted log-normal distribution provides the overall best approximation for the aggregate interference, especially in the distribution tail region. In general, these models for aggregate interference are useful not only in characterizing the performance of dynamic spectrum access networks, but also in designing protection zones around an IU [160, 164], deploying cognitive radios [165], managing spectrum access control, etc.

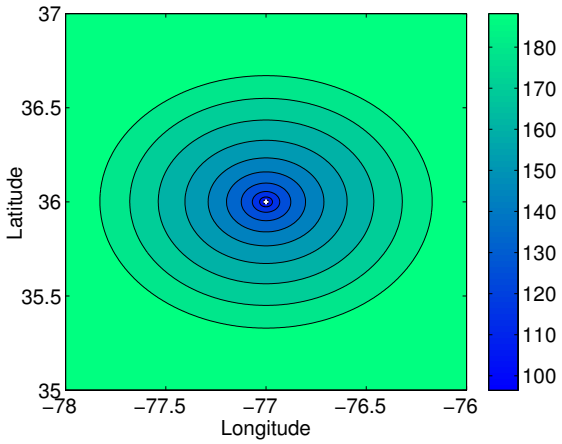
3.2.3 Exclusion Zones

The notion of an exclusion zone (EZ) is a static spatial separation region defined around an IU, where co-channel and/or adjacent-channel transmissions by SUs are prohibited. EZs are the primary ex-ante mechanism employed by regulators to protect IUs from harmful interference caused by transmissions from SUs. The legacy EZs are conservative and static. The notion of a static exclusion zone implies that it has to protect IUs from the union of all likely interference scenarios, resulting in a worst-case and very conservative solution [160]. Since SU operations are prohibited inside an EZ, the conservative design of EZs unnecessarily limits the SUs' spatial spectrum-access opportunities.

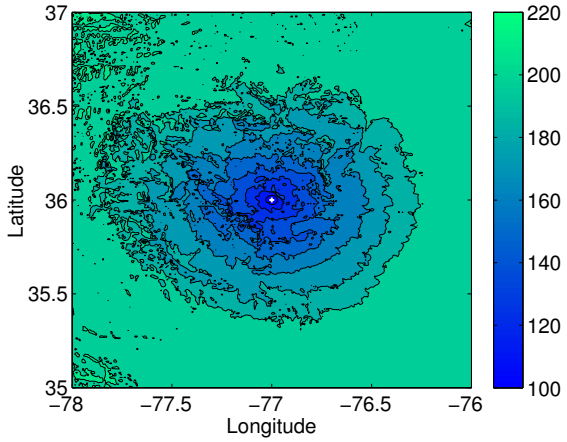
In its Notice of Proposed Rule Making (NPRM) [166], the Federal Communications Commission (FCC) acknowledged that the size of an EZ could be significantly reduced if a realistic propagation model could be used in conjunction with a mechanism to monitor the aggregate interference caused by SU transmissions. In June of 2015, the NTIA published a technical report summarizing their preliminary analysis on redefining the EZ boundaries for ship-borne radars in the 3.5 GHz band [13]. Their results show that the size of EZs can be reduced by up to 70% when legacy propagation models are replaced by terrain-based propagation models such as the ITM-PTP model.

3.3 Illustrative Example of ITM-PTP Mode

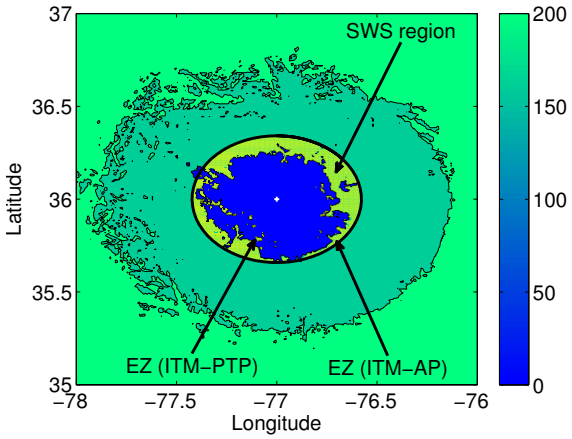
Before introducing TESSO in the next section, here, we provide an illustrative example to demonstrate the effectiveness of a terrain-based propagation model in discovering spatial spectrum sharing opportunities. Specifically, we compare ITM-PTP mode—a terrain-based propagation model— against the ITM-AP mode—a model that does not use details of terrain in the path loss computations. Later, in Section 6.6, we use these results as a benchmark to evaluate the relative effectiveness of TESSO in identifying spatial spectrum sharing opportunities.



(a) Path loss map (in dB) using ITM-AP mode



(b) Path loss map (in dB) using ITM-PTP mode



(c) Using ITM-PTP to discover SWSs.

Figure 3.1: Use of ITM-PTP for discovering SWSs in case study 1. The white dot at the center represents the IU location. The color map represents the ITM path loss.

Table 3.1: ITM parameters used in our analysis.

Radio frequency, f	3550 MHz
Polarization	Vertical
Surface refractivity	301 N-units
Dielectric constant of ground	15
Conductivity of ground	0.0005 S/m
Radio climate	Continental temperature

Let us define an analysis area of approximately $40,000$ square kilometers centered at ($36°$, $-77°$) latitude-longitude as shown in Figure 3.1(a). An IU, operating in the 3550 MHz band, is located at the center of the analysis area. Let us divide the analysis area into square grids, each with a side length of $0.01°$ (roughly 1 km). Now, using ITM-AP mode along with the parameters listed in Table 3.1, radio propagation loss is computed from the center of each grid to the IU. For computing the ITM-AP path loss, we use the terrain irregularity parameter, $\Delta h = 90$ m. The resulting path loss map (in dB) is shown in Figure 3.1(a). The oval shape of the path loss contours is attributed to the fact that ITM-AP mode does not consider the exact details of terrain to compute the path loss in the point to point link. Rather, it uses the average terrain characteristics—defined by Δh—for path loss computations. For a given Δh, path loss from a grid to the IU is a function of distance, but not of the actual terrain in the link connecting the two points.

Figure 3.1(b) shows the path loss contours when ITM-PTP mode is used to compute the propagation loss for the same map. We used the same parameters as outlined in Table 3.1. For extracting the terrain details in the path loss computations, we used the Global Land One-km Base Elevation (GLOBE) database [167]. GLOBE is an internationally designed, developed, and independently peer-reviewed global digital elevation model, at a latitude-longitude grid spacing of 30 arc-seconds ($3''$). Unlike ITM-AP mode, the path loss contours obtained by using ITM-PTP mode are highly irregular in shape. The irregularities occur from the fact that specific terrain details in the point to point link are considered while computing the propagation loss. Furthermore, the path loss predicted by the ITM-PTP mode is often larger and more accurate than that predicted by the ITM-AP mode. By

comparing Figures 3.1(a) and 3.1(b), it is evident that ITM-PTP mode's ability to produce accurate path loss estimates can be utilized to identify spatial sharing opportunities, albeit such an approach would incur a high computational cost.

Suppose that a SU transmits with power $P_{ts} = 30$ dBm, the receiver antenna gain of the IU is $G_r = 0$ dB, the transmitter antenna gain of the SU is $G_t = 0$ dB, and the interference tolerance threshold of the IU is $I_{th} = -120$ dBm, then the minimum required path loss, $P_{L_{min}}$, for protecting the IU from interference caused by a single SU, I_{SU}, is computed as,

$$P_{L_{min}} = P_{ts} + G_t + G_r - I_{th} = 140 \text{ dB}.$$

In general, multiple SUs may operate around an IU. In order to ensure that the aggregate interference caused by multiple concurrently-transmitting SUs does not exceed I_{th}, a conservative margin of $\Delta P_L = 10 - 20$ dB is often added to $P_{L_{min}}$ [168]. For example, using $\Delta P_L = 20$ dB with the aforementioned parameters results in $P_{L_{min}} = 160$ dB. Then, using $P_{L_{min}}$, an EZ can be defined around an IU where SU transmissions are prohibited. Figure 3.1(c) shows the resulting EZ. The black oval represents the EZ when the ITM-AP mode is used to estimate the path loss, whereas the irregular blue contour represents the EZ when ITM-PTP mode is used. We refer to the spatial region that is inside the EZ defined by the ITM-AP mode, but outside the EZ defined by the ITM-PTP mode as the *spatial white space* (SWS). Based on the assumptions that were made above, an ITM-PTP mode can safely allow a limited number of SUs, say N, to operate inside a SWS without violating the IU's interference protection requirement (i.e., the aggregate interference power received by the IU does not exceed the interference tolerance threshold).

Now, let us assume that the IUs can operate without noticeable performance degradation if they are ensured a *probabilistic guarantee of interference protection*—i.e., an IU's interference protection is prescribed as follows: the aggregate interference, I_{agg}, from SUs is below I_{th} for

$(1-\epsilon)$ fraction of the time, where ϵ is the probability that $I_{agg} > I_{th}$. That is,

$$P\left(I_{agg} \leq I_{th}\right) \geq 1-\epsilon. \tag{3.1}$$

Since radio signal propagation is inherently stochastic, the notion of a probabilistic guarantee for interference protection is widely accepted. For example, the coverage regions of TV stations are based on F-curves, which provide a probabilistic guarantee that the signal reception is above a threshold [169].

Algorithm 1 Evaluating spatial sharing opportunities in SWSs using ITM-PTP path loss model.

Require: Parameters listed in Table 3.1, IU's location, GLOBE data, I_{th}, ϵ, P_{ts}, and SU queries from the SWS region.

Ensure: N.

Initialize $I_{agg} = 0$, and $N = 0$.
for each SU query i **do**
  if SU-SU coexistence criteria is satisfied **then**
    Compute ITM-PTP path loss, $P_{L_{ITM}}$, using IU's location, SU's location, GLOBE data and parameters listed in Table 3.1.
    Compute $I_{SU} = P_{ts} + G_t + G_r - P_{L_{ITM}}$, and $I_{agg} = I_{agg} + I_{SU}$.
    if $I_{agg} < I_{th}$ **then**
      Allow the i^{th} SU to transmit.
      Update $N = N + 1$.
    else if $I_{agg} > I_{th}$ **then**
      Generate a random number, u, between 0 and 1.
      if $u \leq \epsilon$ **then**
        Allow the i^{th} SU to transmit.
        Update $N = N + 1$.
        return N.
      else
        Deny the i^{th} SU's request to transmit.
        return N.
      end if
    end if
  end if
end for

Before introducing TESSO in the next section, let us discuss a methodology, described by

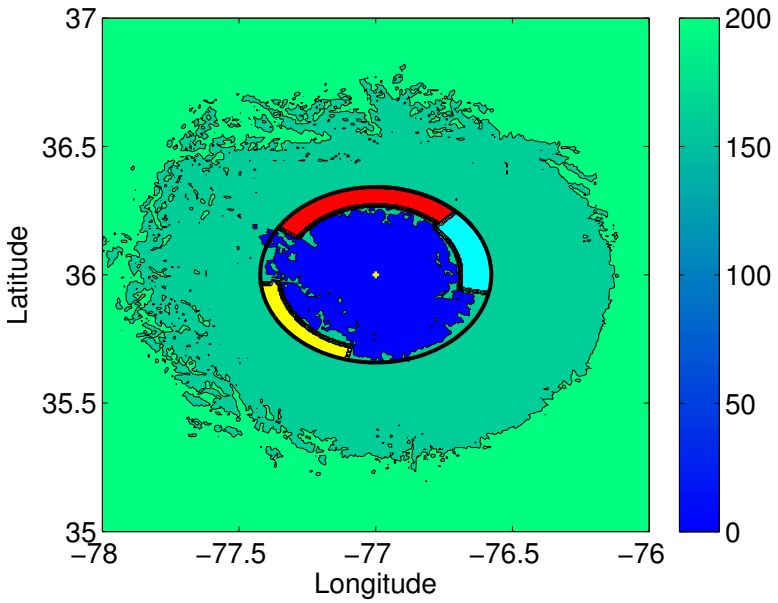


Figure 3.2: Modeling a SWS region as annular sectors in case study 1. The color map represents ITM-PTP path loss.

Algorithm 1, that can be employed by a SAS for evaluating spatial sharing opportunities in the SWS region. The proposed methodology is an approach for computing the maximum number of SUs that can be safely allowed to operate in the SWS region while satisfying Inequality (3.1). Algorithm 1 is based on the computationally intensive ITM-PTP model that requires the precise locations of SUs. Despite its high computational cost, the use of ITM-PTP model for path loss computations makes Algorithm 1 effective in accurately identifying the spatial spectrum sharing opportunities around an IU. In our analysis, the solution produced by Algorithm 1 represents the ground truth—i.e., it represents the true number of SUs that can be safely allowed in the SWS region. Later, in Section 6.6, we use the solution produced by Algorithm 1 as a benchmark for comparing the relative effectiveness of TESSO.

The methodology described in Algorithm 1 is as follows. When an entrant SU requests for spectrum access, the SAS uses ITM-PTP path loss model to predict the interference that is likely to be caused by the SU at the IU and checks if the aggregate interference caused by SUs is below the IU's interference tolerable threshold. For computing the interference,

the SAS uses a querying SU's location and other transmission parameters; IU's location and interference protection requirement; terrain information; and the ITM-PTP propagation model. The SAS positively acknowledges an entrant SU's request for spectrum access only if the I_{agg} caused by all co-channel SUs, including the requesting SU, in the SWS region does not violate the IU's protection requirement. According to Algorithm 1, the SAS allows at most N SUs to concurrently transmit in the SWS region. The value of N will be different for each instance of Algorithm 1 as it depends on SU query locations, corresponding path loss values and the instantaneous value of the aggregate interference.

3.4 TESSO: A Tool for Enabling Spatial Spectrum Sharing Opportunities

The use of realistic terrain-based propagation models is effective for identifying expanded SWS opportunities, while still providing IUs with appropriate interference protection. However, the computational complexity inherent in terrain-based propagation models and the requirement of precise geo-locations of SUs makes it challenging to implement them in real time systems, such as SAS-driven spectrum sharing. In this section, we describe an analytical tool—namely, TESSO—which is a mathematical framework for discovering SWS opportunities in a computationally efficient manner, while satisfying the IU's protection requirement. TESSO is based on a simplified propagation model whose parameters are derived by characterizing the statistical properties of the radio propagation environment.

From Figure 3.1(c), we can notice that the SWS region is highly irregular in shape. In order to consider the irregularity of the SWS region while making TESSO analytically tractable, let us model the SWS region as a union of multiple annular sectors of an oval as shown in Figure 3.2. We define the term "SWS sector" to refer to each of these sectors. This sectorized SWS model strikes an appropriate compromise between modeling a realistic SWS region and limiting modeling complexity. Recall that the EZ boundary indicated by the black oval is

conservative because it is computed using a propagation model (ITM-AP mode) that does not consider terrain details in the path loss computations. Therefore, the interference emanated by SUs operating outside this conservative EZ boundary can be safely ignored. However, in the SWS sectors, it needs to be ensured that the statistics of aggregate interference caused by multiple SU transmissions does not violate the IU interference protection requirement. TESSO protects the IUs by enabling a SAS to carefully control the number of SUs that are allowed to transmit concurrently in the SWS sectors.

3.4.1 Interference from a Single SU

In order to analyze the interference caused by a single SU, I_{SU}, at the IU, let us consider a SU operating inside a SWS sector. Also assume that SUs are uniformly distributed inside the SWS sector. Note that, in practical scenarios, SUs might be distributed non-uniformly, and such scenarios can be approximated by considering different SU densities in each SWS sector.

Let us consider a simplified propagation model with exponential path loss and log-normal shadowing. The path loss exponent, γ, and the variance of log-normal shadowing, σ^2, for each sector can be estimated using a number of approaches; e.g., by using measurement data or by using estimates from more accurate propagation models. Using a simplified propagation model, the path loss, P_L, to the IU from a SU located d meters away can be expressed as:

$$P_L = a + b \log_{10} d + \psi, \tag{3.2}$$

where, $a = P_{L_{d_0}} - b \log_{10} d_0$, $P_{L_{d_0}}$ is the path loss at a reference distance, d_0, in dB, $b = 10\gamma$, and ψ denotes the shadowing coefficient which is log-normally distributed with mean = 0 and variance = σ^2.

Now, if P_{ts} denotes the transmit power of SU in dBm, then the interference power received

by the IU receiver due to transmission from a SU is

$$I_{SU} = P_{ts} - P_L = P_{ts} - (a + b\log_{10} d + \psi). \tag{3.3}$$

When SUs are uniformly distributed in an annular sector, that is defined by R_1 and R_2 (the inner and the outer radius respectively), with the IU at the center, the distance between a SU and the IU is a random variable D whose probability density function (PDF) is given by Equation (4.3) [170].

$$f_D(d) = \frac{2d}{R_2^2 - R_1^2}, \qquad R_1 \leq d \leq R_2. \tag{3.4}$$

Strictly speaking, the outer and inner boundaries of a SWS sector are defined by arcs of concentric-ovals (because the Earth is not a perfect sphere), but, for simplicity, we approximate them as arcs of concentric-circles.

Finally, using transformation of random variables, the PDF of I_{SU}, denoted as $f_{I_{SU}}(i_{su})$, can be derived as [160]:

$$f_{I_{SU}}(i_{su}) = Ke^{\left(\frac{2(P_{ts}-i_{su}-a)\ln 10}{b}\right)} \left\{erf(B) - erf(A)\right\}, \tag{3.5}$$

$$\begin{aligned}
\text{where } K =& \frac{\ln 10}{b(R_2^2 - R_1^2)} e^{\frac{2(\ln 10)^2\sigma^2}{b^2}} \\
A =& \frac{1}{\sqrt{2}\sigma}\left(P_{ts} - i_{su} - a - b\log_{10} R_2 + \frac{2\sigma^2 \ln 10}{b}\right) \\
\text{and } B =& \frac{1}{\sqrt{2}\sigma}\left(P_{ts} - i_{su} - a - b\log_{10} R_1 + \frac{2\sigma^2 \ln 10}{b}\right).
\end{aligned}$$

Equation (4.7) is valid for any SU operating in any SWS sector. When specific values of a, b, P_{ts}, σ, R_1 and R_2 pertaining to the i^{th} SU operating in the j^{th} SWS sector are plugged into Equation (4.7), the PDF of $I_{SU_{i,j}}$ is obtained. Here, $I_{SU_{i,j}}$ denotes the interference power at the IU induced by transmission from the i^{th} SU operating in a randomly chosen location inside the j^{th} SWS sector.

Theorem 3.1. *For small ω, where $\omega = \frac{R_2}{R_1}$, the PDF of I_{SU} can be approximated as a*

log-normal distribution. The error in approximation increases monotonically with ω.

Proof. Let us rewrite Equation (4.7) as follows,

$$f_{I_{SU}}(i_{su}) = K' g_1(i_{su}) g_2(i_{su}), \tag{3.6}$$

where $g_2(i_{su}) = erf(g_3(i_{su})) - erf\left(g_3(i_{su}) - \frac{b \log_{10} \omega}{\sqrt{2}\sigma}\right)$, and $g_3(i_{su})$ and $g_1(i_{su})$ are linear and exponential functions of i_{su} respectively. Here, K' is a non-negative constant.

From the definition of the erf function, the plot of $g_2(i_{su})$ can be approximated as a Gaussian PDF. This approximation is fairly accurate when $\frac{b \log_{10} \omega}{\sqrt{2}\sigma}$ is small. Restating this in terms of ω, the Gaussian approximation holds true only for small values of ω. Finally, because the product of an exponential kernel ($g_1(i_{su})$ has the kernel of an exponential distribution) and a Gaussian kernel ($g_2(i_{su})$ can be approximated to have the kernel of a Gaussian distribution) results in another Gaussian kernel, $f_{I_{SU}}(i_{su})$ is a Gaussian PDF. □

In most spectrum sharing scenarios, ω is small because most of the SWSs are located near the R_2 boundary. Per Theorem 3.1, the distribution of I_{SU} can be approximated as a log-normal distribution in such cases.

3.4.2 Aggregate Interference

To adequately protect IUs from the interference from multiple SUs, we must consider the distribution of I_{agg}, which is the summation of random variables, $I_{SU_{i,j}}$, and is defined as

$$I_{agg} = \sum_{j=1}^{\mathcal{S}} \sum_{i=1}^{N^{(j)}} I_{SU_{i,j}}, \tag{3.7}$$

where, $\mathcal{S}$ denotes the total number of SWS sectors, and $N^{(j)}$ is the total number of SUs in the j^{th} SWS sector.

Since $I_{SU_{i,j}}$ can be approximated as a log-normal distribution, I_{agg} is the summation of log-normal random variables. It has been shown that the summation of log-normal random variables can be approximated by another log-normal random variable. Among existing approximation methods [171, 172, 173, 174], the Fenton-Wilkinson (FW) method [172] is a simple and computationally efficient algorithm for approximating the mean and variance of the resulting log-normal distribution. It provides a very good approximation in the tail region of the resulting complementary cumulative distribution function (CCDF) curve [175]. We employ the FW technique to approximate I_{agg} because for very small values of ϵ (e.g., $0 \leq \epsilon \leq 0.1$), Inequality (3.1) represents the tail region of the CCDF of I_{agg}. Recall that we are interested in the tail region of the I_{agg} distribution as dictated by Inequality (3.1).

The closed-form solutions provided by FW approximation are given in Equation (3.8) [172]:

$$\begin{aligned} \sigma^2_{agg} &= \ln\left(\frac{\sum_{j=1}^{\mathcal{S}}\sum_{i=1}^{N_j}\left(e^{2\mu_{i,j}+\sigma^2_{i,j}}(e^{\sigma^2_{i,j}}-1)\right)}{\sum_{j=1}^{\mathcal{S}}\sum_{i=1}^{N_j}\left(e^{\mu_{i,j}+\frac{\sigma^2_{i,j}}{2}}\right)}+1\right) \\ \mu_{agg} &= \ln\left(\sum_{j=1}^{\mathcal{S}}\sum_{i=1}^{N_j}\left(e^{\mu_{i,j}+\frac{\sigma^2_{i,j}}{2}}\right)\right)-\frac{\sigma^2_{agg}}{2}, \end{aligned} \tag{3.8}$$

where $\mu_{i,j}$ and $\sigma^2_{i,j}$ denote the mean and variance of individual summand. Similarly, μ_{agg} and σ^2_{agg} are mean and variance of the resulting I_{agg} distribution.

The above equations are valid for the natural logarithm, and they must be scaled appropriately when working with logarithms to the base of different values ($\log_{10}$ in our case).

3.4.3 Maximum Number of Permissible SUs

Here, we formulate an optimization problem that allows TESSO to compute the maximum number of SUs that can be safety allowed to operate in each SWS sector. While the objective is to maximize the spatial sharing opportunities for SUs, there are two primary constraints

that need to be satisfied: (i) IU interference protection criterion, and (ii) SU-SU coexistence criterion.

For guaranteeing IU interference protection, TESSO uses properties of the distribution of I_{agg} to satisfy Inequality (3.1). For facilitating SU-SU coexistence, suppose that a maximum of $N_{\max}^{(j)}$ SUs can co-exist in the j^{th} SWS sector. From here onwards, we refer SU to denote a cell, such as an LTE cell. In practice, $N_{\max}^{(j)}$ is computed using SU's coverage area, its transmit power, required signal to noise and interference ratio at the SU receiver, terrain, antenna parameters, etc. However, for simplicity, we assume that SU-SU co-existence is a function of the total area available for SUs and the area of each SU cell. Particularly, if $A^{(j)}$ and a_{su} denote the total area of the j^{th} SWS sector and the area of a SU cell, respectively, then the maximum number of SUs, $N_{\max}^{(j)}$, that can harmoniously coexist in the j^{th} SWS sector can be computed as

$$N_{\max}^{(j)} = \left\lfloor \frac{A^{(j)}}{a_{su}} \right\rfloor. \tag{3.9}$$

Using Equation (3.9), TESSO enables SU-SU coexistence by enforcing an upper bound on the maximum number of SUs that can operate in each SWS sector. Finally, TESSO formulates the optimization problem defined by Equation (4.20) to find the optimum value of $N^{(j)}$ for each SWS sector.

$$\begin{aligned} \text{Maximize}: \; & N = \sum_{j=1}^{\mathcal{S}} N^{(j)} \\ \text{subject to}: \; & P\left(\sum_{j=1}^{\mathcal{S}} \sum_{i=1}^{N^{(j)}} I_{SU_{i,j}} \leq I_{th} \right) \geq 1 - \epsilon \\ & 0 \leq N^{(j)} \leq N_{\max}^{(j)}, \quad j = 1 \ldots \mathcal{S} \end{aligned} \tag{3.10}$$

The above optimization problem can be readily solved using Genetic Algorithms [176].

Recall that Algorithm 1 and TESSO are two different approaches for identifying and evaluating the spatial sharing opportunities around an IU. While Algorithm 1 is computationally expensive (because it is based on ITM-PTP model) and requires the precise geolocations of SUs, TESSO is computationally efficient and works effectively even when the precise geoloca-

tions of SUs are not available. We shall provide a detailed comparison of the computational complexity of Algorithm 1 and TESSO in Section 3.5.3.

3.5 Evaluation of TESSO

In this section, we conduct two independent case studies to evaluate TESSO. In both studies, we analyze the performance of TESSO in identifying spatial spectrum sharing opportunities around an IU while ensuring protection of the IU from aggregate interference caused due to SUs. To evaluate the relative effectiveness of TESSO, we compare it against Algorithm 1, which is an approach for identifying spatial spectrum sharing opportunities in the SWS region based on the computationally intensive ITM-PTP model that requires the precise locations of SUs. In our analysis, the solution produced by Algorithm 1 represents the ground truth; it accurately computes the maximum number of SUs that can be safely allowed to transmit in the SWS region. On the other hand, TESSO estimates this value in a much more computationally efficient manner without requiring knowledge of the precise locations of SUs.

The set-up for our case studies is as follows. Case study 1 represents a scenario where an IU is located at $(36°, -77°)$ near Norfolk, Virginia. Case study 2 represents a scenario in which an IU is located at $(27.5°, -81.8°)$ near Fort Green, Florida. In each of these studies, we evaluate spectrum sharing opportunities around the IU's location. In both cases, the terrain around the IU is devoid of high mountains but is not completely flat. In terms of clutter—which is one of the key factors that characterize the propagation of radio signals—, these two case studies represent two different scenarios. The first case study considers an area that has high clutter due to the presence of dense forests in the vicinity of the IU, whereas in the second case study, the region around the IU has much lower clutter due to the lack of vegetation.

Henceforth, a SU refers to a square SU cell of side 2 km with a transmitter at the center and

a receiver at the edge of the cell. To compute the link capacity of a SU in units of bps/Hz, we use Shannon's channel capacity formula:

$$C_{SU_{i,j}} = \log_2(1 + \mathrm{SINR_{i,j}}). \tag{3.11}$$

where, $C_{SU_{i,j}}$ and $\mathrm{SINR_{i,j}}$ denote the link capacity in bps/Hz and the signal to interference and noise ratio of the i^{th} SU that operates in the j^{th} SWS sector. Here, the term "interference" refers to the sum of all other inferring signals, including those from co-channel IU transmitter and other co-channel SU transmitters, at the SU receiver of interest.

Finally, we use a metric called Area Sum Capacity (ASC) for quantifying spectrum utilization efficiency. ASC represents the sum of $C_{SU_{i,j}}$ for all N SUs that harmoniously coexist with the IU in the same channel.

$$\mathrm{ASC} = \sum_{j=1}^{\mathcal{S}} \sum_{i=1}^{N(j)} C_{SU_{i,j}}. \tag{3.12}$$

In both case studies, we follow the following steps:

i Define a SWS region based on the path loss map around the IU.

ii Run multiple instances of Algorithm 1 and calculate average values of N and ASC. These values serve as a benchmark against which we shall later compare the performance of TESSO.

iii Model the SWS region as a union of multiple annular sectors of a circle, and use TESSO to analytically compute N and ASC.

iv Compare N and ASC values obtained from TESSO against the benchmark values obtained in step ii. Check whether TESSO's solution satisfies the IU's interference protection requirement.

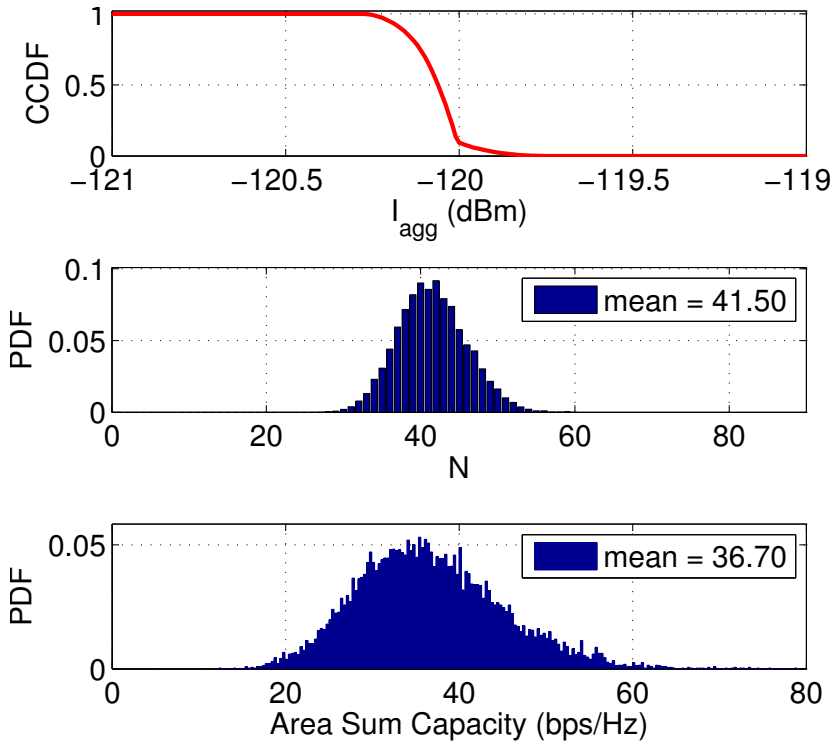


Figure 3.3: Distributions obtained by using ITM-PTP for case study 1.

3.5.1 Case Study 1: Norfolk Region

As explained above, first, we use Algorithm 1 to compute the total number of SUs, N, that can be safely allowed to transmit in the SWS region shown in Figure 3.1(c). The IU protection criteria is defined by Inequality (3.1) where $I_{th} = -120$ dBm and $\epsilon = 0.1$. Then, multiple instances of Algorithm 1 are run to obtain the empirical distributions of I_{agg}, N, and ASC. Figure 3.3 summarizes the results. As expected, the distribution of I_{agg} shows that the probabilistic guarantee of interference protection to the IU is satisfied. From the plots, we can also observe that N and ASC have skewed Gaussian distributions with mean values of 41.50 and 36.70 bps/Hz respectively.

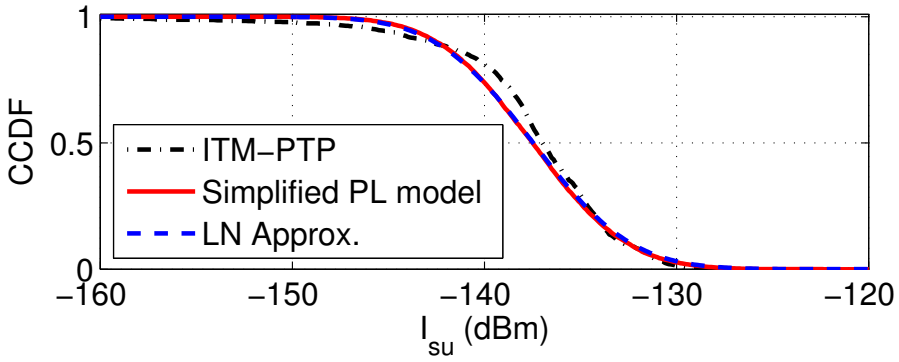
Next, we evaluate the performance of TESSO in finding the spatial sharing opportunities in the SWS sectors. Let us define a sectorized SWS as shown in Figure 3.2 which approximately covers the SWS region of Figure 3.1(c). First, we use Equation (4.7) to characterize the

distribution of I_{SU} in each SWS sector. The values of γ and σ for each SWS sector are estimated by using samples of the true path loss values (in the absence of measurement data, we assume that ITM-PTP path loss is the true path loss). Then, the distribution of I_{SU} is approximated as a log-normal distribution. Finally, the optimization problem defined in (4.20) is solved to obtain an optimal value of N using Matlab's genetic algorithm solver.

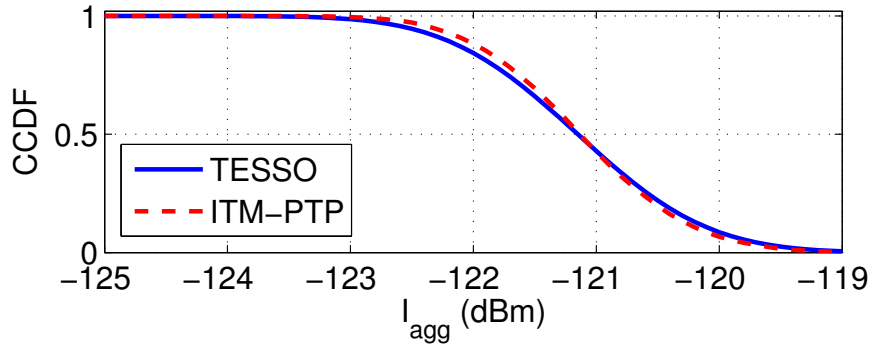
Figure 3.4(a) shows that the log-normal approximation for the distribution of I_{SU} in a SWS sector closely resembles its true distribution (obtained by using ITM-PTP path loss values). The log-normal approximation for I_{SU} distribution is obtained by first finding the weighted least-squares (WLS) values of γ and σ (parameters of the simplified path loss model) using the true path loss samples, and then using Theorem 3.1. For computing γ and σ using WLS, TESSO assigns large weights to smaller path loss values. Doing so ensures that the log-normal approximation matches the tail region of the true distribution of I_{agg}.

In Figure 3.4(b), we compare the true distribution of I_{agg} against the one predicted by TESSO. The true distribution is obtained by using the solution of optimization problem given in Equation (4.20) and the true path loss values (obtained from the ITM-PTP model). The plots show that TESSO accurately approximates the true distribution. More importantly, TESSO satisfies the IU's protection requirement.

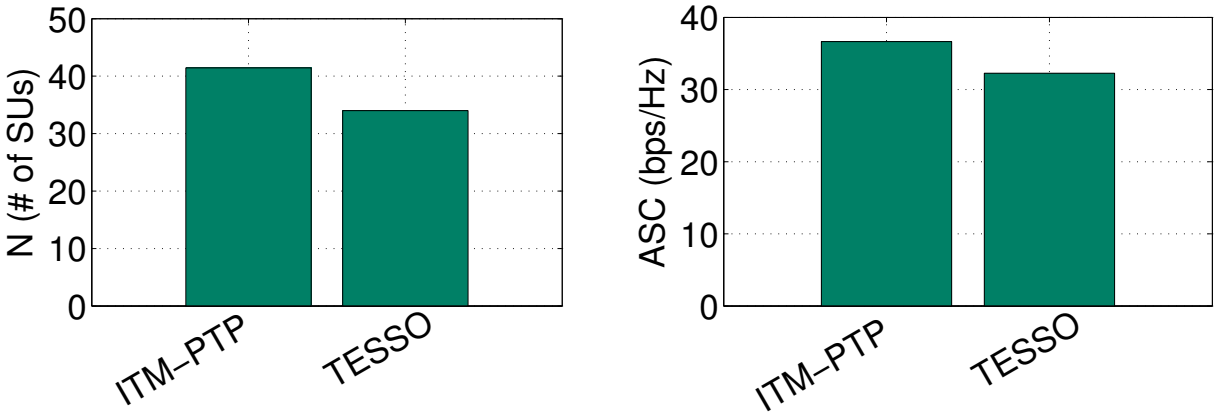
Figure 3.4(c) demonstrates the effectiveness of TESSO in identifying SWS opportunities. To make a fair comparison between TESSO and the ITM-PTP model, we add an additional constraint in (4.20) that ensures the same density of SUs in all SWS sectors. On average, TESSO identifies spatial sharing opportunities (N) almost as effectively as the ITM-PTP mode (Algorithm 1). Furthermore, comparing the performance in terms of ASC, the plot shows that the ASC achieved by TESSO is comparable to that achieved by the ITM-PTP model. The difference in the performances between TESSO and the ITM-PTP model is mainly because the ITM-PTP model exploits sharing opportunities throughout the SWS region (see Figure 3.1(c)), whereas TESSO identifies SWS opportunities only inside the SWS sectors (see Figure 3.2). Despite this slight disadvantage, TESSO's lighter computational



(a) Distribution of I_{SU}.

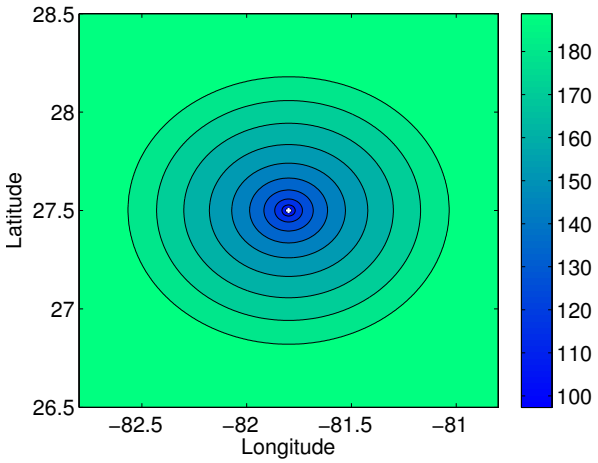


(b) Distribution of I_{agg}.

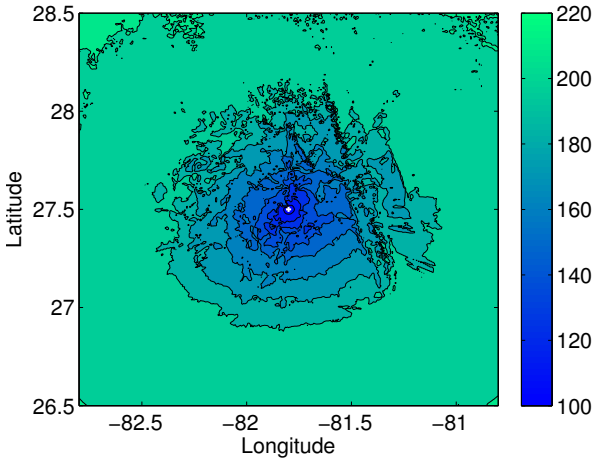


(c) SWS opportunities.

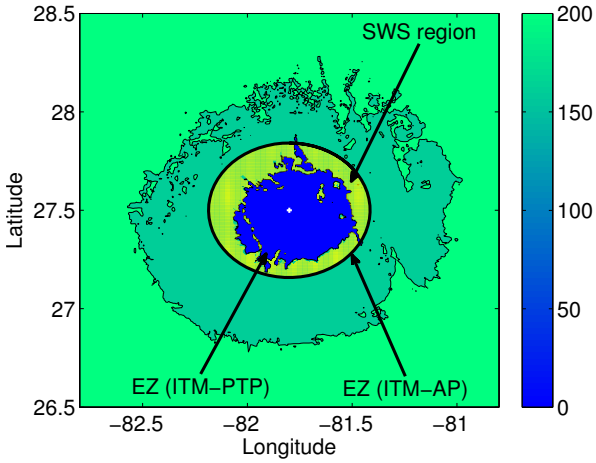
Figure 3.4: Comparison between TESSO and ITM-PTP in case study 1.



(a) Path loss map (in dB) using ITM-AP mode



(b) Path loss map (in dB) using ITM-PTP mode



(c) Using ITM-PTP to discover SWSs.

Figure 3.5: Use of ITM-PTP for discovering SWSs in case study 2. The white dot at the center represents the IU location. The color map represents the ITM path loss.

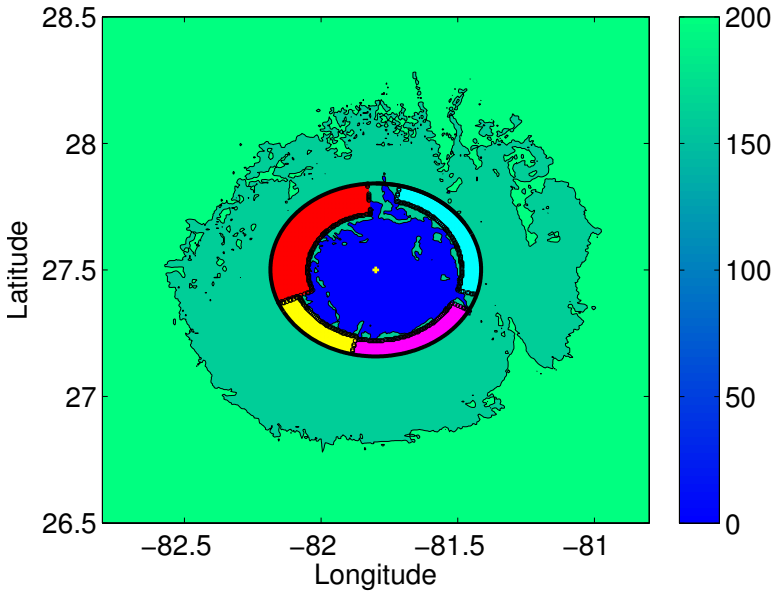


Figure 3.6: Modeling a SWS region as annular sectors in case study 2. The color map represents the ITM-PTP path loss.

cost makes it a favorable choice in applications where the geolocations of SUs are not precisely known, and the computation of aggregate interference power needs to be performed in real time for facilitating spectrum access control—such as the case in SAS-driven spectrum sharing.

3.5.2 Case Study 2: Fort Green Region

We continue to evaluate TESSO by repeating our analysis in case study 2. Similar to case study 1, first, we generate path loss maps and define the SWS region, as shown in Figures 3.5(a), 3.5(b) and 3.5(c). Then, Algorithm 1 is implemented to compute N and ASC while satisfying IU's protection requirement. Here, we set I_{th} to a different (compared to case study 1), but arbitrarily chosen, value of -118 dBm. Note that we chose different I_{th} values in these case studies for representing two different incumbent protection requirements. All other parameters remain the same as in case study 1. The results of Algorithm 1 are summarized in Figure 3.7. As expected, the plot of I_{agg} shows that the IU's protection criteria is satisfied.

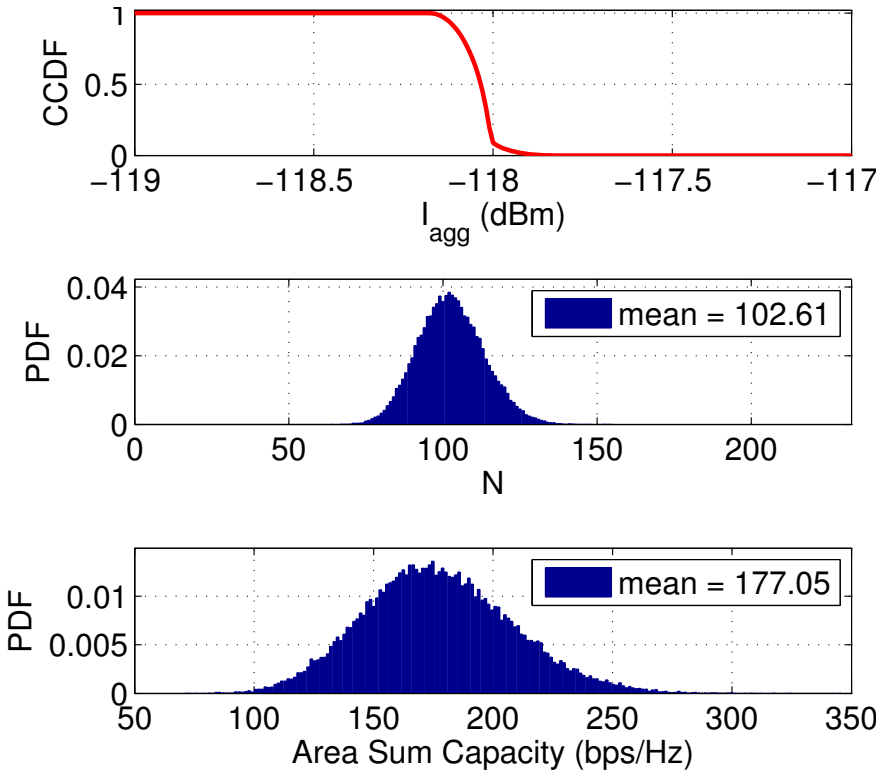


Figure 3.7: Distributions obtained by using ITM-PTP in case study 2.

The mean values of N and ASC obtained by Algorithm 1 are 102.61 and 177.05 bps/Hz respectively.

Next, SWS sectors are defined (see Figure 3.6) which approximately cover the SWS region of Figure 3.5(c). Then, using samples of true path loss values, the parameters γ and σ for each sector are estimated, and the distribution of I_{SU} is approximated as a log-normal distribution. Finally, TESSO optimization problem defined by Equation (4.20) is formulated and solved. The results are summarized in Figure 3.8.

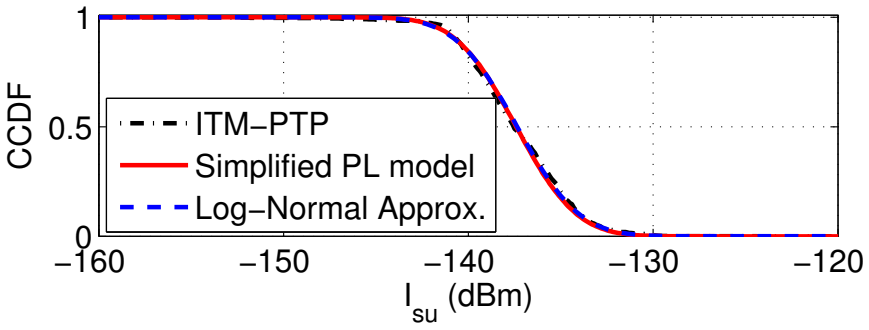
Plots in Figure 3.8(a) show that the distribution of I_{SU} can be approximated as a log-normal distribution. This approximated distribution is used by TESSO to characterize I_{agg} and to evaluate spatial sharing opportunities. Figure 3.8(b) shows that TESSO predicts I_{agg} fairly accurately and protects the IU from aggregate interference caused due to SUs. The IU protection requirement of $I_{agg} = -118$ dBm and $\epsilon = 0.1$ is reliably met.

The effectiveness of TESSO in enabling spatial sharing opportunities can be observed in Figure 3.8(c). The performance of TESSO in estimating N and ASC, is comparable to that of Algorithm 1 (which uses ITM-PTP). As explained in case study 1, the slight difference in the performances of TESSO and Algorithm 1 is mainly because the latter enables spectrum sharing in the entire SWS region, whereas the former enables spectrum sharing only in the SWS sectors. In other words, TESSO slightly under-performs Algorithm 1 because the total area of the SWS sectors is smaller than the total area of the SWS region.

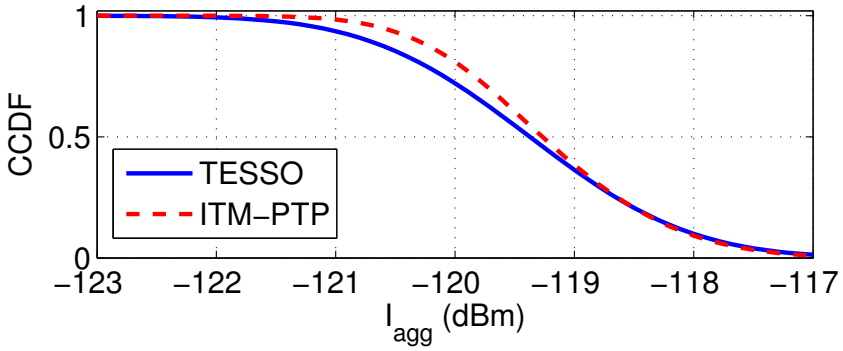
3.5.3 Computational Complexity

Note that Algorithm 1, on average, requires N ITM-PTP path loss computations. Therefore, the time complexity of Algorithm 1 is $O(N \times \tau)$, where $O(\tau)$ is the time complexity of each ITM-PTP path loss computation (approx. 100 milliseconds in our implementation). On the other hand, TESSO's time complexity is constant, and it is the time taken to solve the optimization problem given by (4.20). In general, time complexity of a genetic algorithm is difficult to express mathematically as it depends on several factors such as population size, crossover type, fitness function, etc. In our simulations, we observed that it takes approximately one second to solve the optimization problem given in (4.20) using Matlab's genetic algorithm solver.

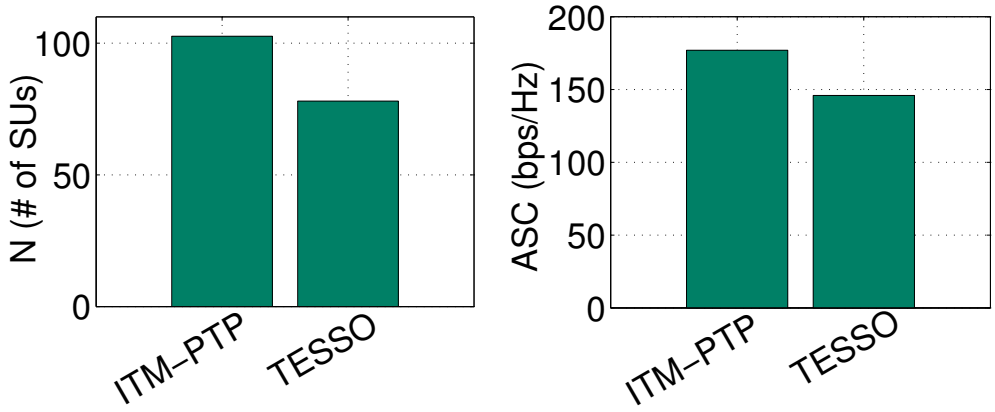
TESSO has a clear advantage over Algorithm 1 in terms of computation overhead, especially in cases when N is large. For instance, TESSO takes one second, on average, to solve the optimization problem given in Equation (4.20), whereas Algorithm 1 takes $0.1 \times N$ seconds. The value of N can be significantly large when IU does not have a very stringent interference protection requirement and SUs' transmit power is low (e.g., IoT applications, femtocells, etc.). Apart from this computational advantage, TESSO, unlike Algorithm 1, does not require knowledge of the precise locations of SUs in its computations. As long as TESSO knows that the SUs operate inside a given SWS sector, TESSO can evaluate spatial spectrum sharing opportunities reliably.



(a) Distribution of I_{SU}.



(b) Distribution of I_{agg}.



(c) SWS opportunities.

Figure 3.8: Comparison between TESSO and ITM-PTP in case study 2.

3.6 Chapter Summary

In this chapter, we proposed an analytical tool—namely TESSO—that can be used for characterizing the SUs' aggregate interference and identifying SWS opportunities in dynamic spectrum sharing. TESSO identifies SWS opportunities in a computationally efficient manner without requiring precise geo-locations of secondary users. Our detailed analysis provides the following important insight: *An analytical tool, such as TESSO, can be used to exploit SWS opportunities almost as effectively as the terrain-based models, such as the ITM-PTP model. TESSO is computationally efficient, and it provides the same level of interference protection guarantee to the IU compared to that offered by the ITM-PTP model.*

Chapter 4

Dynamic Exclusion Zones for Spectrum Sharing

4.1 Introduction

To ensure interference protection to the IU, a static spatial separation region is defined around the IU where no co-channel and/or adjacent-channel transmission is allowed. This protected region is often called an *Exclusion Zone* (EZ). The EZ is the primary *ex-ante* (i.e., preventive) spectrum enforcement method that the Federal Communications Commission (FCC) and the National Telecommunications and Information Administration (NTIA) employ to protect non-federal and federal government PUs.

Defining the EZ boundary, inside which a IU enjoys exclusive access rights to the spectrum, is considered to be a challenging problem in spectrum sharing. The difficulty of the problem arises because of the following two conflicting requirements. On one hand, the area defined by the EZ must be sufficiently large to protect the PU from SU-induced interference. On the other hand, the EZ should not unnecessarily limit SUs spectrum access opportunities [177], otherwise the economic viability of spectrum sharing itself is undermined. Furthermore,

when computing the EZ boundary, the effect of irregular terrain must also be considered in the path loss computations [178], which significantly increases the complexity of the already difficult problem.

Most of the existing methods, such as *F-curves* [179], tend to overly emphasize the first requirement, i.e., interference protection to the PUs [180], [181]. A good example of this can be seen in the TV bands. For example, to account for possible deep fades, the IEEE 802.22 working group specifications require detectors to have a sensitivity of -116 dBm which corresponds to a safety margin of roughly 20 dB (equivalent to an increase in the radius of the EZ by 110 km) [182], [168]. However, in most situations, detectors do not face such severe fading, and hence the SUs are unnecessarily prohibited from using the band in question even though the probability of causing harmful interference to the PUs is extremely small. Such overly conservative designs of EZs significantly reduce the economic benefits of spectrum sharing [183] and, in some cases, may hinder its adoption due to lack of interest from the wireless industry stakeholders.

With the realization that opening up more spectrum to commercial applications has tremendous potential to spur economic growth and technological innovations [183], regulatory bodies, the wireless industry, and other stakeholders have taken active steps to address the technical as well as the policy challenges for realizing spectrum sharing. Among these challenges, two issues are especially critical in Federal-commercial spectrum sharing: (i) spectrum (rule) enforcement [184], [185], [186] and (ii) security and privacy [187], [14]. Spectrum enforcement involves employing technical and policy solutions for protecting incumbents from interference induced by lower-tier users as well as ensuring the spectrum access privileges of the lower-tier users. On the other hand, security and privacy issues in spectrum sharing include the incumbents' operational privacy/security [14] and their communications/cyber security [187], [14]. This chapter focuses on the spectrum enforcement issue, more specifically *ex-ante* (i.e., preventive) enforcement.

EZs are the primary ex-ante spectrum enforcement method used by regulators to protect

the incumbents from SU-induced interference. Several definitions of EZs have been studied. A recent advancement in this direction is the use of *Spectrum Coordination Zones* (CZs) in the AWS-3 bands (specifically $1675 - 1710$ MHz and $1755 - 1780$ MHz) [186], [188]. We will describe CZs in Section 4.2. Similarly, *Geolocation Database (GDB)-driven* spectrum sharing has received considerable attention ever since its adoption in the TV bands, and it has also been proposed for enabling the three-tiered spectrum sharing model in the 3.5 GHz band [166], [12]. The network of GDBs and supporting infrastructure for enabling spectrum sharing in the 3.5 GHz band—sometimes referred to as the *Spectrum Access System* (SAS) [166]—is envisioned to house a repository of incumbents' spectrum usage information, and perform real-time aggregate interference computations by using the geolocations of PUs and SUs. The consideration of realistic propagation effects, including terrain details, in the aggregate interference computation is one of the key techniques for reducing the size of EZs.

In this chapter, we propose a novel framework for implementing ex-ante enforcement that addresses some of the problems of legacy EZs. Specifically, we introduce the concept of *Multi-tiered Incumbent Protection Zones (MIPZ)*, and show that it can be used to dynamically adjust the PU's protection boundary based on changes in the radio environment, network conditions, and the PU interference protection requirement. The MIPZ framework can be used as an analytical tool for quantitatively analyzing the incumbent protection zones to gain insights of and determine the tradeoffs between interference protection and spectrum utilization efficiency. The following bullets summarize the core contributions of this chapter:

- The proposed framework provides a systematic framework, based on sound mathematical models, for determining the boundary of spatial separation regions used for protecting PUs. Moreover, it provides valuable insights on the interplay and tradeoff between the two primary requirements of spectrum sharing—interference protection and spectrum utilization efficiency.

- MIPZ is fundamentally different from the legacy EZs in that it has been designed to be dynamically adjustable based on changes in the interference environment, network

conditions, or interference protection requirements.

- MIPZ adopts the concept of probabilistic guarantee of interference protection to the incumbents, which is grounded on solid mathematical formulations, for significantly improving the spectrum utilization.
- Our framework, MIPZ, enables a seamless integration of two spectrum sharing approaches: database-driven and spectrum sensing-driven spectrum sharing.
- Our closed-form solution approach significantly reduces the computational burden of the geolocation database, such as the SAS, in real-time.
- Using results from extensive simulations, we show that MIPZ adapts to changing network conditions by adjusting its boundary. Results also show that the proposed framework offers a significant gain in spectrum utilization as compared to the conventional EZs.

Note that the term "*Protection Zone (PZ)*" is used in this chapter in a general sense to refer to a spatial separation region defined for protecting PUs from SU-generated interference; it can be used to refer to the legacy exclusion zones, protection zones, or coordination zones [186], [189], [185], [190]. Also, in this chapter, we are using the term "*SAS*" in a general sense to refer to a network of geolocation databases and supporting infrastructure that are deployed to dictate the SUs' spectrum access.

The rest of the chapter is organized as follows. In Section 4.2, we provide a brief overview of methods used for defining the conventional EZ boundaries. In Section 4.3, we describe our proposed framework. The closed-form expression for the aggregate interference power is derived in Section 4.4. In Section 4.5, we formulate a stochastic optimization problem for defining the dynamic EZ boundaries. Through simulation results, we demonstate the performance of our framework in Section 4.6. Finally, Section 5.8 concludes the chapter.

4.2 Conventional Exclusion Zones

4.2.1 TV Band

In order to protect TV system incumbents in the U.S. TV bands, the protected service contours of the TV transmitter are computed using F-curves. A F-curve, $F(x, y)$, ensures a probabilistic guarantee that, inside the TV coverage region, the received TV signal is above a given threshold $x\%$ of the time in $y\%$ of the locations [179], [191]. Then, an appropriate interference protection ratio is applied, often in the form of a minimum separation distance from the edge of the computed TV protected service contour, to derive the appropriate EZs for both co-channel and adjacent channel SU operation. Furthermore, to avoid the detectors from detecting false positive spectrum opportunities due to possible severe multipath and deep fading, a conservative margin of 10 to 20 dB is added in the computation of EZs, which significantly increases the size of the TV EZs [168]. Several other incumbents also exist in the TV bands, and they are also protected through similar EZ computation methods.

4.2.2 AWS-3 Band

In AWS-3 band, the NTIA recently defined *Coordination Zones* (CZs) for sharing these bands with Wireless Broadband Systems (WBSs) [186]. The CZs are based on interference between satellite earth stations and WBSs. A CZ is not an EZ where SUs are not allowed to operate, but it is the area beyond which the earth station will not get interference from WBSs [188]. WBSs have unencumbered access to the co-channel outside the CZ, but the ones that are willing to operate inside the CZ must trigger coordination with the federal incumbent. Coordination process is initiated by WBS by submitting the detailed technical operating parameters to the federal point-of-contact who will respond to the request after assessing the possible interference caused at the incumbent. The WBS may or may not operate inside the CZ based on the response. Even if a WBS is allowed to operate inside the

CZ, it must tolerate the possible harmful interference from the incumbents.

CZs are computed based on several factors, such as transmit power of both SU and PU, antenna gains in the direction of interference, time variations of antenna gains in the case of earth station operating with non-geostationary satellite systems, receiver susceptibility to interference, propagation effects of radio waves, mobility of earth station, etc. If the WBS can be shielded from the interference generated by the satellite earth station, then the size of the CZ is based on interference mitigation techniques at the WBS (e.g., using directional antennas to avoid interference to the incumbent).

4.3 Proposed Framework: Multi-tiered Incumbent Protection Zones (MIPZ)

One of the main problems with conventional EZs is that they are overly large. The EZ boundary is defined conservatively so that the PUs are protected from interference even in the worst-case scenario. PUs experience higher interference when there is an interferer operating in a line-of-sight (LoS) region, and such interference is difficult to predict when the channel has small-scale fading characteristics.

The conservative approach for defining the conventional EZ boundary is also backed up by the following fact. Outside the EZ, the existing spectrum sharing model does not specify the limit on the number of simultaneous co-channel secondary transmissions — i.e., any SU can transmit in the co-channel as long as it is outside the PU's EZ, and can co-exist with other SUs in the same band. Thus, the interference power received at the PU is not just the interference caused by a single SU, but in fact, it is the aggregate interference caused by multiple (theoretically infinite) SUs. In the absence of a spectrum access controller, it is quite understandable that regulators have to conservatively set the EZ boundary so that the PUs are protected from the worst-case aggregate interference.

The FCC in its Notice for Proposed Rule Making (NPRM) [166] acknowledges that the size of the EZ could be significantly reduced if there were a mechanism to control the number of SU transmissions outside the EZ. Regulators have stepped towards this direction by introducing database-driven spectrum sharing models where GDB, such as SAS in the 3.5 GHz band, acts as a spectrum controller. In a GDB-driven spectrum sharing, a SU queries the database, and accesses the channel only if the database responds with a spectrum access grant. Motivated by this, we propose MIPZ framework for GDB-driven spectrum sharing. MIPZ allows the spectrum controller to adjust the size of the PZ dynamically based on instantaneous interference conditions, and hence, allows SUs to exploit more spectrum opportunities than the legacy EZs.

First, we describe our framework assuming that the PU has a co-located transmitter (Tx) and receiver (Rx). Examples of co-located PUs are satellite earth stations, radar systems, etc. Then, in Section 4.5, we provide some high-level insights on how to adapt our model for the non-colocated PUs. Our framework consists of the following three access zones.

4.3.1 No Access Zone (NAZ)

NAZ is the spatial separation region defined in the immediate vicinity of the PU where access to the spectrum is allowed only to the licensed incumbents. In our model, NAZ is a circle centered at the PU-Rx, and its boundary is computed dynamically based on the instantaneous radio and network conditions. The lower bound on the NAZ boundary is computed by considering interference in both directions: from SU to PU and from PU to SU.

4.3.2 Limited Access Zone (LAZ)

LAZ is a disk shaped annular region that lies just outside the NAZ. It shares its inner boundary with NAZ and the outer boundary with Unlimited Access Zone (which will be

discussed shortly). Unlike the area outside conventional EZ, LAZ is the region which allows a limited number of co-channel SUs, say N, to transmit simultaneously. The upper bound on N is carefully computed, which we shall discuss in detail in Section 4.5. For a SU querying from LAZ region, the response of the spectrum database depends on the instantaneous number of other co-channel transmissions in the region. If the cardinality of other co-channel SUs operating in the LAZ is less than the upper bound of N, the querying SU is allowed to transmit in the co-channel, otherwise not. The outer boundary of the LAZ is computed using a propagation model such that the transmissions outside the LAZ cause negligible interference to the PU because of large path loss, hence, their contribution to aggregate interference can be ignored.

4.3.3 Unlimited Access Zone (UAZ)

UAZ is the region that lies outside the outer boundary of LAZ. In spirit, this region is similar to the area outside the conventional EZs where any number of SUs can transmit in the co-channel. Therefore, SUs have unencumbered access to the co-channel in the UAZ. The SU co-existence issues in the UAZ region is out of the scope of this chapter.

Figure 4.1 shows our MIPZ framework. The outer rectangle denotes the analysis area that encompasses a co-located PU at the center. The NAZ is shown as a solid black area inside the inner boundary, where the black color signifies the absence of white space (spectrum opportunities) in that region. The gray disk between the inner and outer boundaries is the LAZ region, where the gray color signifies that only a limited number of white spaces are available. Outside the LAZ is the UAZ shown in white color, where the white color signifies that this region is affluent in white spaces.

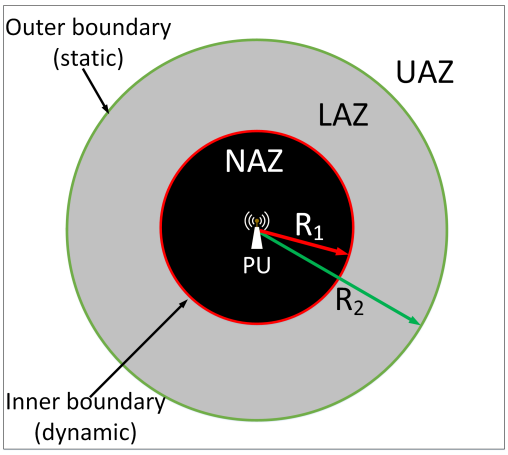


Figure 4.1: Concept of NAZ, LAZ and UAZ.

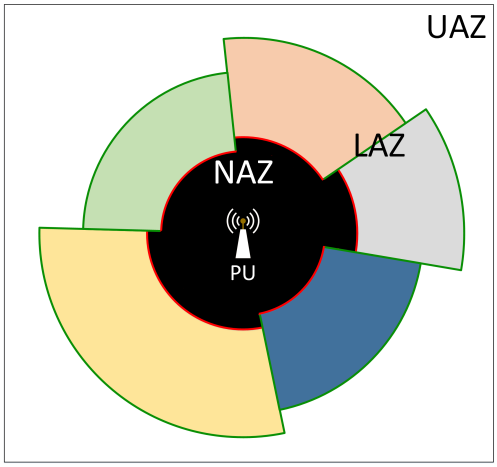


Figure 4.2: Realizing irregular PZs using annular sectors.

4.3.4 Practical Considerations

In practice, the zone boundaries will not always be perfect circles as shown in Figure 4.1. Terrain variations, environmental effects, antenna radiation pattern, etc. cause the signal to attenuate differently in different directions resulting in irregular zone boundaries. To consider the irregularity of the zone boundaries, we realize a sectorized model as shown in Figure 4.2. This model strikes an appropriate compromise between modeling realistic interference conditions and limiting modeling complexity. Here, each annular sector is a part of LAZ while the black irregular shape represents the NAZ. The inner boundary, as well as the upper bound on the number of SUs, needs to be defined for each LAZ sector.

Recall that no SU is allowed to operate inside the NAZ and SUs in UAZ do not contribute to the aggregate interference. Thus, in order to ensure that the aggregate interference power received by the PU is below its interference tolerance threshold (I_{th}), a centralized server/controller, such as the SAS, should govern the SU operations in the LAZ. The SAS should continuously monitor the instantaneous aggregate interference, and allow a new transmission inside LAZ only if the aggregate interference is lower than I_{th}. However, the computational complexity of accurately monitoring the instantaneous aggregate interference in real-time is very challenging [192], and this makes such an approach impractical for applications such as the SAS.

To address the complexity of monitoring the instantaneous aggregate interference in real-time, we relax the system requirement by making the following assumption. Let us assume that the PUs can operate without significant performance degradation if they are ensured a *probabilistic guarantee of interference protection*. In other words, a PU may achieve its desired *quality of service (QoS)* if the aggregate interference (I_{agg}) from SUs is below I_{th} for $(1-\epsilon)$ fraction of the time, where ϵ is the probability that $I_{agg} > I_{th}$.

$$P\left(I_{agg} \leq I_{th}\right) \geq 1 - \epsilon \tag{4.1}$$

Because of unpredictable nature of signal propagation, the notion of probabilistic guarantee is quite common in wireless applications. For example, the coverage regions of TV stations are based on F-curves which provide probabilistic guarantees that the signal reception is above a threshold.

4.4 Aggregate Interference Characterization

In this section, we first derive a closed-form expression for the probability distribution of co-channel interference caused at the PU by a single SU operating in a LAZ sector. This expression is valid for a SU transmitting in any LAZ sector provided that the relevant propagation parameters are available for that particular sector. Finally, in section 4.4.3, an expression for the probability distribution of aggregate interference is derived.

4.4.1 Interference from a Single SU

Let us consider a single SU operating inside a LAZ sector. We assume that SUs are uniformly distributed in space, therefore, the location of a SU is a two-dimensional uniform random variable. At first, this assumption might seem unreasonable as several studies have shown that mobile users tend to be clustered due to geographical factors, social gatherings, etc [193]. However, with multiple LAZ sectors, our framework can approximate the non-uniform SU distribution even if we consider uniform SU distribution in each sector. This can be achieved by considering different SU density in each sector.

In order to compute the path loss between SU and PU, let us consider a simplified propagation model with exponential path loss and shadowing. We choose this path loss model for the following two reasons: i) it is a popular path loss model for modeling large-scale outdoor channels, and has also been extensively used in prior 3GPP standards bodies [194], and ii) it facilitates us in deriving a closed-form analytical expression for the aggregate interference.

Beyond a reference distance d_0, the dB path loss (P_L) in the channel that links the SU and the PU is,

$$P_L = a + b\log_{10} d + \psi, \tag{4.2}$$

where $a = P_L(d_0) - b\log_{10} d_0$, $P_L(d_0)$ is the path loss at the reference distance in dB, $b = 10\gamma$, γ is the path loss exponent, d is the distance between a SU and the PU in meters, and ψ is the log-normal (normal in dB scale) shadowing coefficient with zero mean and variance $= \sigma^2$. From here onwards, we shall consider all computations in dB unless explicitly stated otherwise; therefore, whenever we say normal distribution, it is actually a normal distribution in the log scale.

Suppose that SUs are uniformly distributed in an annular sector with the PU at the center. Then the distance between a SU and the PU can be represented with a random variable D whose *probability density function (pdf)* is given by equation (4.3) [170].

$$f_D(d) = \frac{2d}{R_2^2 - R_1^2}, \qquad R_1 \leq d \leq R_2. \tag{4.3}$$

Here, R_1 and R_2 represent the radii of the inner and outer concentric circles, respectively, which combinedly define the annular LAZ sector.

Now, let us calculate the pdf of the second term of equation (4.2). This is basically a transformation of the random variable D to Y, $y = b\log_{10} d = g(d)$. We proceed as,

$$\begin{aligned} f_Y(y) =& f_D(g^{-1}(y)) \left| \frac{\partial g^{-1}(y)}{\partial y} \right| \\ =& \frac{2\ln(10)10^{2y/b}}{b(R_2^2 - R_1^2)}, \quad b\log_{10} R_1 \leq y \leq b\log_{10} R_2. \end{aligned}$$

Since we consider normal shadowing, the pdf of third term of equation (4.2) is,

$$f_\psi(\psi) = \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{\psi^2}{2\sigma^2}}.$$

Now that we know the pdf of the second and the third terms of equation (4.2), the resulting pdf of $Z = Y + \psi$ is given by the following convolution integral [195],

$$\begin{aligned} f_Z(z) &= \int_{-\infty}^{\infty} f_\psi(\psi) f_Y(z-\psi) d\psi \\ &= \int_{A_1}^{B_1} \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{\psi^2}{2\sigma^2}} \frac{2\ln(10) 10^{2(z-\psi)/b}}{b(R_2^2 - R_1^2)} d\psi, \end{aligned}$$

where $A_1 = z - b\log_{10} R_2$ and $B_1 = z - b\log_{10} R_1$.

Let $K_1 = \sqrt{\frac{2}{\pi}} \frac{\ln 10}{\sigma b(R_2^2 - R_1^2)}$ and proceed.

$$\begin{aligned} f_Z(z) &= K_1 \int_{A_1}^{B_1} e^{-\frac{\psi^2}{2\sigma^2}} e^{\frac{2(z-\psi)\ln 10}{b}} d\psi \\ &= K_1 e^{\left(\frac{2z\ln 10}{b} + \frac{2(\ln 10)^2\sigma^2}{b^2}\right)} \int_{A_2}^{B_2} e^{-\frac{1}{2}\frac{k^2}{\sigma^2}} dk, \end{aligned} \tag{4.4}$$

where $k = \psi + \frac{2\sigma^2 \ln 10}{b}$, $A_2 = z - b\log_{10} R_2 + \frac{2\sigma^2 \ln 10}{b}$ and $B_2 = z - b\log_{10} R_1 + \frac{2\sigma^2 \ln 10}{b}$.

Letting $p = \frac{k}{\sqrt{2}\sigma}$ and $K_2 = K_1\sqrt{\frac{\pi}{2}}\sigma e^{\frac{2(\ln 10)^2\sigma^2}{b^2}}$, equation (4.4) becomes,

$$\begin{aligned} f_Z(z) =& \frac{2}{\sqrt{\pi}} K_2 e^{\left(\frac{2z\ln 10}{b}\right)} \int_{A_3}^{B_3} e^{-p^2} dp \\ =& K_2 e^{\left(\frac{2z\ln 10}{b}\right)} \left\{erf(B_3) - erf(A_3)\right\}, \end{aligned}$$

$$\text{where } erf(x) = \frac{2}{\sqrt{\pi}} \int_0^x e^{-p^2} dp,$$
$$A_3 = \frac{1}{\sqrt{2}\sigma} \left(z - b \log_{10} R_2 + \frac{2\sigma^2 \ln 10}{b} \right), \text{ and}$$
$$B_3 = \frac{1}{\sqrt{2}\sigma} \left(z - b \log_{10} R_1 + \frac{2\sigma^2 \ln 10}{b} \right).$$

Finally, the pdf of P_L in equation (4.2) is,

$$f_{P_L}(p_l) = K_2 e^{\left(\frac{2(p_l - a)\ln 10}{b}\right)} \left\{ erf(B_4) - erf(A_4) \right\}, \tag{4.5}$$

$$\text{where } A_4 = \frac{1}{\sqrt{2}\sigma} \left(p_l - a - b \log_{10} R_2 + \frac{2\sigma^2 \ln 10}{b} \right), \text{ and}$$
$$B_4 = \frac{1}{\sqrt{2}\sigma} \left(p_l - a - b \log_{10} R_1 + \frac{2\sigma^2 \ln 10}{b} \right).$$

Let P_{ts} denote the transmit power of SU in dBm. Then, the interference power received by the PU receiver is,

$$I_{SU} = P_{ts} - P_L. \tag{4.6}$$

Using equations (4.5) and (4.6), the pdf of I_{SU} is,

$$f_{I_{SU}}(i_{su}) = K_2 e^{\left(\frac{2(P_{ts} - i_{su} - a)\ln 10}{b}\right)} \left\{ erf(B_5) - erf(A_5) \right\}, \tag{4.7}$$

$$\text{where } A_5 = \frac{1}{\sqrt{2}\sigma} \left(P_{ts} - i_{su} - a - b \log_{10} R_2 + \frac{2\sigma^2 \ln 10}{b} \right)$$
$$\text{and } B_5 = \frac{1}{\sqrt{2}\sigma} \left(P_{ts} - i_{su} - a - b \log_{10} R_1 + \frac{2\sigma^2 \ln 10}{b} \right)$$

As mentioned before, Equation (4.7) is valid for any SU operating in any LAZ sector. When specific values of a, b, P_{ts}, σ, R_1 and R_2 pertaining to i^{th} SU operating in j^{th} LAZ sector are plugged into Equation (4.7), the pdf of $I_{SU_{i,j}}$ is obtained. Here, $I_{SU_{i,j}}$ denotes the pdf

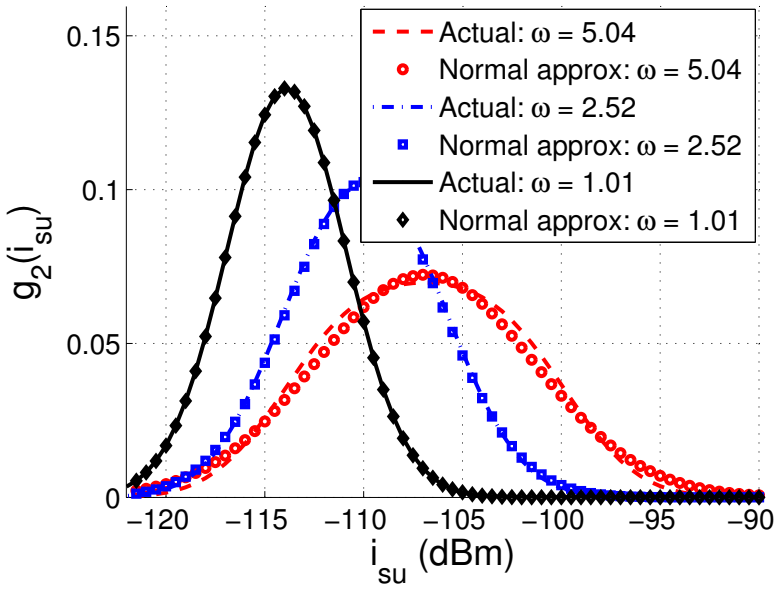


Figure 4.3: $g_2(i_{su})$ versus i_{su} for different values of ω.

of interference power at the PU receiver due to the transmission from i^{th} SU operating in a randomly chosen location inside the j^{th} LAZ sector.

4.4.2 Approximating I_{SU} Distribution as a Normal

The pdf in equation (4.7) looks notoriously complex as its kernel cannot be recognized as that of any of the standard pdfs. This poses as a major road-block in our quest of finding the closed form expression for aggregate interference, I_{agg}. Let us rewrite equation (4.7) as follows,

$$f_{I_{SU}}(i_{su}) = \frac{K_3}{\omega^2 - 1} g_1(i_{su}) g_2(i_{su}), \tag{4.8}$$

where $g_2(i_{su}) = erf(g_3(i_{su})) - erf\left(g_3(i_{su}) - \frac{b \log_{10} \omega}{\sqrt{2}\sigma}\right)$, $\omega = R_2/R_1$, $g_3(i_{su})$ and $g_1(i_{su})$ are linear and exponential functions of i_{su} respectively. K_3 is a non-negative constant.

From the definition of the erf function, the plot of $g_2(i_{su})$ can be approximated as a Gaussian pdf. This approximation is fairly accurate when $\frac{b \log_{10} \omega}{\sqrt{2}\sigma}$ is small. Since $b = 10\gamma$ (γ is the path

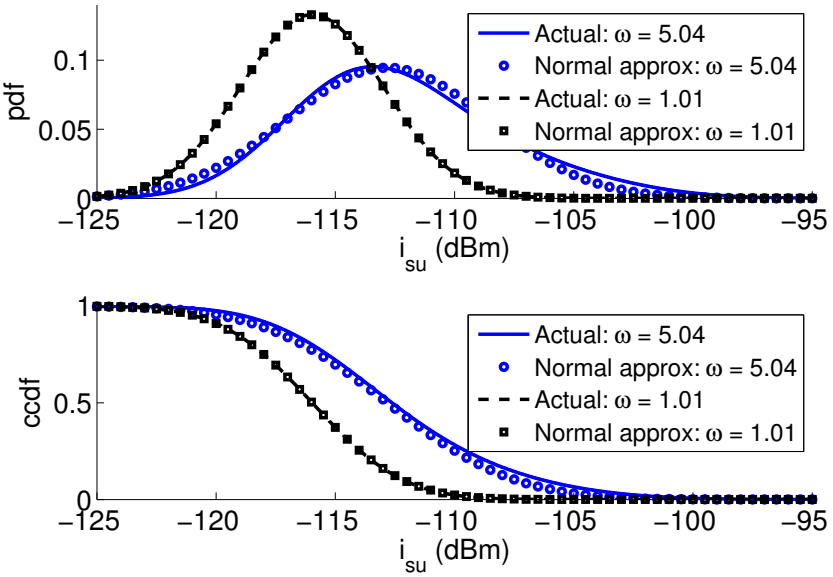


Figure 4.4: pdf and ccdf of I_{SU}: actual vs. approximation.

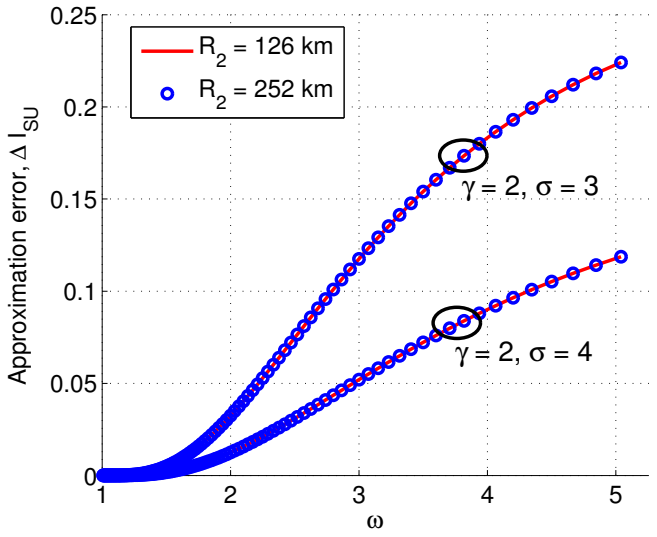


Figure 4.5: Error in normal approximation of I_{SU}.

loss exponent) and σ (standard deviation of shadow fading) are channel characteristics, a wireless system designer has no control over them. Therefore, the accuracy of the Gaussian approximation for the plot of $g_2(i_{su})$ depends on ω, where $\omega > 1$ (since $R_2 > R_1$). The approximation is highly accurate when ω is small. As ω becomes larger, the bell shaped curve of $g_2(i_{su})$ starts deviate from the Gaussian pdf. Figure 4.3 shows the comparative plots of $g_2(i_{su})$ against the closest normal pdf for different values of ω.

The function $g_1(i_{su})$ has the kernel of an exponential distribution. Using the fact that the product of an exponential kernel and a Gaussian kernel results in an another Gaussian kernel, $f_{I_{SU}}(i_{su})$ is a Gaussian pdf. Note that this approximation is accurate only when ω is small. Large value of ω causes $g_2(i_{su})$ (and hence $f_{I_{SU}}(i_{su})$) to deviate from the normal pdf resulting in a non-zero approximation error (ΔI_{SU}). We define ΔI_{SU} as the *Euclidean norm* of the difference between actual and approximated distributions of I_{SU}.

In Figure 4.4, the actual plots of $f_{I_{SU}}(i_{su})$ from Equation (4.7) and its *complementary cumulative distribution function* (ccdf) are compared against the pdf and the ccdf of normal approximation respectively. For generating these plots, typical practical values were plugged in for all other variables ($a = 37$ dB, $b = 20$, $\sigma = 3$, $P_{ts} = 23$ dBm, $R_2 = 126$ km). Then, the parameters of the normal approximation are obtained by fitting a least squares normal curve to the samples of $f_{I_{SU}}(i_{su})$. We can observe a close similarity between the two pdfs, especially when ω is small. The plot of ΔI_{SU} in Figure 4.5 shows that ΔI_{SU} increases with increase in ω. As expected, the plot also shows that the approximation error is a function of ω but not of the actual values of R_1 and R_2. Another important observation is that for any ω, ΔI_{SU} increases as the ratio γ/σ increases.

In our framework, ω is not significantly large. As we shall discuss in Section 4.5, typical value of R_2 is 126 km and R_1 ranges from 50 km to 126 km, which implies ω ranges from 1 to 2.52. At this value, ΔI_{SU} is fairly negligible. Therefore, we conclude that I_{SU} can be approximated as a normal distribution. This allows us to obtain the closed-form expression for the pdf of I_{agg}. Later, we shall further justify this approximation by showing that it has

negligible effect on the overall performance of PU and SU networks.

4.4.3 Aggregate Interference

The next step is to find the distribution of I_{agg}, which is the summation of random variables, $I_{SU_{i,j}}$.

$$I_{agg} = \sum_{j=1}^{T} \sum_{i=1}^{N_j} I_{SU_{i,j}}. \tag{4.9}$$

Here, T denotes the total number of LAZ sectors and N_j is the total number of SUs operating in the j^{th} LAZ sector. Note that equation (4.9) is valid only in standard units (Watts or milliWatts), but not in dB units. Since the distribution of $I_{SU_{i,j}}$ (in standard units) is log-normal, I_{agg} has the distribution of summation of log-normal random variables.

It has been shown that the summation of log-normal random variables can be approximated by another log-normal [196]. Several approximation techniques have been proposed [196], [171]. The most widely used approximations are the ones proposed by Fenton-Wilkinson [172], Schwartz-Yeh [173] and Mehta et. al. [174]. Fenton-Wilkinson is a simple and computationally efficient algorithm for approximating the mean and variance of the resulting log-normal distribution. While it provides a very good approximation in the tail region of the cdf curve, Fenton-Wilkinson is usually bad in the body region. Schwartz-Yeh provides a good approximation in the body region at the cost of added computational complexity, but unlike Fenton-Wilkinson, it doesn't do well in the tail region. Mehta et. al. provide a flexible mechanism that allows a user to choose the focus of the approximation. However, its computational complexity increases exponentially with the increase in the number of random variables being summed, which makes it the least favorable for using in real-time high traffic applications like the SAS.

In order to provide probabilistic guarantee of interference protection to the PU, the following

inequality must be satisfied.

$$\begin{aligned} & P\left(I_{agg} \leq I_{th}\right) \geq 1-\epsilon \\ \text{i.e.,} \quad & P\left(\sum_{j=1}^{T}\sum_{i=1}^{N_j} I_{SU_{i,j}} \leq I_{th}\right) \geq 1-\epsilon. \end{aligned} \tag{4.10}$$

From inequality (4.10), it is clear that we are interested in the tail portion of the complementary cdf of I_{agg}. Fenton-Wilkinson fits our purpose because it provides a log-normal approximation that is most accurate in the tail region [175]. Moreover, it performs well even with the summation of non-identically distributed log-normal variables (summands). This is desired in our case because the distribution of I_{SU} might be different for different LAZ sectors when sectors have different sets of parameters such as γ, P_{ts} and σ. Furthermore, Fenton-Wilkinson provides a closed-form solution for the mean and variance of the resulting log-normal distribution, making it easier to implement in the SAS. The closed-form solutions are given in equations (4.11) and (4.12) [172].

$$\sigma^2_{agg} = \ln\left(\frac{\sum_{j=1}^{T}\sum_{i=1}^{N_j}\left(e^{2\mu_{i,j}+\sigma^2_{i,j}}\left(e^{\sigma^2_{i,j}}-1\right)\right)}{\sum_{j=1}^{T}\sum_{i=1}^{N_j}\left(e^{\mu_{i,j}+\frac{\sigma^2_{i,j}}{2}}\right)}+1\right) \tag{4.11}$$

$$\mu_{agg} = \ln\left(\sum_{j=1}^{T}\sum_{i=1}^{N_j}\left(e^{\mu_{i,j}+\frac{\sigma^2_{i,j}}{2}}\right)\right) - \frac{\sigma^2_{agg}}{2}, \tag{4.12}$$

where $\mu_{i,j}$ and $\sigma^2_{i,j}$ denote the mean and variance of individual summand. Similarly, μ_{agg} and σ^2_{agg} are mean and variance of the resulting log-normal distribution; I_{agg} in our case.

The above equations are valid for natural logarithm, and they must be scaled appropriately when working with other logarithms ($\log_{10}$ in our case).

4.5 Determining the MIPZ Boundaries

Our framework defines NAZ, LAZ and UAZ regions based on two boundaries: outer boundary and inner boundary (Figure 4.1). The details of the boundary definitions are described in the next two sub-sections. In the following discussions, it is assumed that the PU's Tx and Rx are colocated. The non-colocated scenario will be discussed briefly at the end of the section.

4.5.1 Static Outer Boundary

The spectrum sharing etiquette in the UAZ region is exactly the same as that in the region outside conventional EZ. The SAS provides unencumbered access to the co-channel in the UAZ which forces us to define the outer boundary conservatively, just like the conventional EZ boundary. Otherwise, the PU may not be guaranteed an adequate interference protection either due to LoS interference from peak points in some terrain areas, or due to the aggregate interference from SUs. On the other hand, there are some possible spectrum opportunities near the conventional EZ boundary which are unnecessarily thwarted because of conservative boundary definition. To exploit such opportunities, we leverage the conventional EZ boundary definition as a starting point and use it as the outer boundary of our framework, and then explore spectrum opportunities inside it. This also allows us to make a direct comparison between the conventional EZ and our framework in terms of spectrum utilization.

We define the outer boundary of our framework in the same way as the regulators define the conventional EZ boundary, i.e., based on the maximum distance at which the PU can get interference from the SUs. The maximum distance depends on several factors such as SU transmit power, type of modulation and coding, PU Rx antenna gain, PU's interference protection and QoS requirement, etc. The Longley-Rice propagation model in point-to-point is used for pathloss calculations in determining the outer boundary. Furthermore, the outer

boundary is static because it is computed based on the worst-case interference conditions rather than the instantaneous radio conditions. As a specific example, a CZ of radius 126 km is defined for a satellite Earth Station in AWS-3 band, located in Patuxent River, Maryland, USA.

4.5.2 Dynamic Inner Boundary

The inner boundary separates the NAZ and LAZ regions. It is clear from Section 4.3 that the SAS allows only a limited number of SUs to operate in the LAZ region. Usually, the wireless network conditions are dynamic. For example, at peak times of the day, more SUs want to access the channel, while in the maintenance hours, only a few of them do so. To cope with the changing network conditions, it is desired that the size of the LAZ be dynamic so that the spectrum resources can be allocated on the fly. Note that the size of the LAZ plays a major role in determining the number of available spectrum resources in the region. In the previous subsection, we discussed that the outer boundary is static. Therefore, we define the inner boundary based on instantaneous network conditions, and make the LAZ region dynamic in size.

First, let us define the upper and lower bounds on R_1, the inner boundary. Clearly, the upper bound on R_1 is the outer boundary R_2. When $R_1 = R_2$, our model becomes equivalent to the conventional EZ. When $R_1 < R_2$, there is a non-zero area available in the LAZ region. This is where the SAS allows a limited number of SUs, say N, to operate. Small R_1 implies large area in the LAZ region, and apparently, it seems that this translates to a higher value of N. However, small R_1 has two major implications. The first issue with small R_1 is that it results in large ΔI_{SU}. Figure 4.4 shows that our appoximation predicts lower probability of interference in the tail region as compared to that given by the exact closed-form expression of I_{SU}. As R_1 gets small, the difference increases. The implication is that when R_1 is small and our approximation is used to compute the available number of spectrum resources in the LAZ, it computes N that is larger than the actual N permitted in the LAZ. This endangers

the PU's interference protection, and therefore, forces us to define a lower bound on R_1, say $R_{1_{lb}}^{(1)}$. $R_{1_{lb}}^{(1)}$ is computed based on the maximum tolerable ΔI_{SU}.

Another issue with small R_1 is that it brings the LAZ region closer to the PU. Referring to Figure 4.4, small R_1 causes the I_{SU} ccdf to shift to the right, and increases the probability that $I_{SU} > I_{th}$. This forces us to define another lower bound on R_1, say $R_{1_{lb}}^{(2)}$, based on the interference protection requirement of the PU. $R_{1_{lb}}^{(2)}$ is the distance at which a single SU endangers the protection requirement of the PU, as this forms a sort of lower bound. It is calculated using I_{th}, ϵ and pathloss equations.

When PU-Tx and PU-Rx are colocated, $R_{1_{lb}}^{(2)}$ depends on the interference from SU for a desired interference protection requirement of the PU. We define the interference tolerance level of PU in terms of outage probability, which is the probability that the received signal power coming from a co-channel SU is greater than a predefined interference threshold. The outage probability at the PU due to interference from a co-channel SU located at $R_{1_{lb}}^{(2)}$ in a shadow fading channel with variance $= \sigma^2$ is calculated as follows,

$$\epsilon = P\left(I_{SU} \geq I_{th}\right) = Q\left(\frac{I_{th} - \bar{I}_{SU}}{\sigma}\right) \tag{4.13}$$

where $Q(.)$ is the Gaussian Q function, and $\bar{I}_{SU}$ is the mean interference power which is given by,

$$\bar{I}_{SU} = P_{ts} - a - 10\gamma \log_{10} R_{1_{lb}}^{(2)}, \tag{4.14}$$

where $a = 10\gamma log_{10}\left(\frac{4\pi f}{c}\right)$, f is the radio frequency and c is the speed of propagation of the radio wave through the medium. Plugging (4.14) in (4.13) and rearranging gives $R_{1_{lb}}^{(2)}$.

$$R_{1_{lb}}^{(2)} = 10^{\left(\frac{\sigma Q^{-1}(\epsilon) + P_{ts} - a - I_{th}}{10\gamma}\right)}. \tag{4.15}$$

The co-located PUs, such as radars and satellite earth stations, have significantly higher transmit power (upto 90 dBm) compared to the SUs (20 – 33 dBm for the small cell LTE

base stations) [197]. When there is a large power discrepancy between the PU and SU, the interference from the PU to SU is a concern. To address this, we introduce a third lower bound on R_1, say $R_{1_{lb}}^{(3)}$. $R_{1_{lb}}^{(3)}$ is the minimum distance from the PU at which a SU can achieve its desired QoS level. If the QoS of the SU is also defined in terms of probabilistic guarantee of interference protection, $R_{1_{lb}}^{(3)}$ is given by equation (4.15) when I_{th} and ϵ are replaced with the interference threshold and outage probability of the SU, and P_{ts} is replaced with the transmit power of the PU.

The smallest R_1 that satisfies all three bounds is R_m.

$$R_m = \max\left(R_{1_{lb}}^{(1)}, R_{1_{lb}}^{(2)}, R_{1_{lb}}^{(3)}\right).$$

Apart from many advantages of GDB-driven spectrum sharing, it is often argued that the database might, at times, contain the stale information. While sensing-driven spectrum sharing provides real-time spectrum availability information, the cost of cooperation among the sensing nodes is extremely high. Recently, studies have shown that a fusion of GDB-driven and sensing-driven spectrum sharing can provide a better spectrum sharing experience [198], [199]. We allow our framework to enable the marriage of database-driven and sensing-driven spectrum sharing approaches by adding a value α to R_m, where α, which can be negative or positive, is determined by the sensing results. Adding α to R_m allows the database to refine the inner zone boundary based on real-time sensing results. Moreover, incorporating sensing results enhances the performance of MIPZ framework in finding the spectrum opportunities that are left uncaptured by the simplified propagation model used in the analytical analysis. The details pertaining to the computation of α is, however, out of the scope of this chapter. We shall pursue the detailed study of the tuning parameter, α, and the problem of combining the database contents with the sensing results in our future work.

$$R_{min} = \alpha + \max\left(R_{1_{lb}}^{(1)}, R_{1_{lb}}^{(2)}, R_{1_{lb}}^{(3)}\right). \tag{4.16}$$

On the other hand, when R_1 is large, the LAZ region lies far from the PU-Rx. The ccdf curve of Figure 4.4 shifts to the left. From this, we expect to achieve large N. However, large R_1 means small area for spectrum sharing in the LAZ region, and to addresss the co-existence issues among SUs, N should be small. These conflicting requirements make the problem of defining the inner boundary challenging.

Let λ denote the total number of spectrum requests coming from uniformly distributed SUs in an area between R_{min} and R_2 of a LAZ sector. Then, the total number of spectrum requests in an annular region between R_1 and R_2, λ_{LAZ}, is,

$$\lambda_{LAZ} = \frac{\lambda(R_2^2 - R_1^2)}{(R_2^2 - R_{min}^2)}. \tag{4.17}$$

When multiple SUs co-exist in a band, the co-existence among the SUs is also an issue. Suppose that a maximum of ρ SUs can co-exist in the area between R_{min} and R_2. From here onwards, we use SU to refer to a SU cell with a Tx at the center and a single Rx at the cell edge. ρ is computed by using SU's coverage area, its transmit power, required Signal-to-Noise-and-Interference-Ratio (SINR) at the SU-Rx, antenna parameters, path loss exponent and shadow fading environment. For simplicity, let us assume that co-existence is a function of the total area available for SUs and the area of each SU cell, i.e., $\rho = \frac{(R_2^2 - R_{min}^2)}{r_{su}^2}$, where r_{su} is the cell radius of the SU. Then, the total number of SUs that can co-exist in an area between R_1 and R_2, ρ_{LAZ}, is,

$$\rho_{LAZ} = \frac{(R_2^2 - R_1^2)}{r_{su}^2}. \tag{4.18}$$

Ideally, the desired number of SUs in the LAZ region is the minimum of λ_{LAZ} and ρ_{LAZ}. Assuming R_1 and R_2 are already defined, there is no incentive in allowing more than λ_{LAZ} SUs because only λ_{LAZ} SUs are requesting access to the co-channel. Also, allowing more than ρ_{LAZ} SUs causes unnecessary co-existence interference among the SUs.

Based on the above discussions, we formulate the following stochastic optimization problem

for finding optimum R_1 that maximizes N while minimizing ω, and also satisfies the PU's protection criteria. Recall that minimizing ω ensures that the approximation error, ΔI_{SU}, is minimized. In this formulation, it is assumed that there is a single LAZ sector and all SUs operating in the LAZ have same transmission parameters, resulting in same distribution of I_{SU} for all SUs.

$$\begin{aligned} \text{Maximize}: \quad & N - \omega \\ \text{subject to}: \quad & P\left(\sum_{i=1}^{N} I_{SU_i} \leq I_{th}\right) \geq 1 - \epsilon \\ & R_{min} \leq R_1 \leq R_2 \\ & 0 \leq N \leq \min(\lambda_{LAZ}, \rho_{LAZ}). \end{aligned} \tag{4.19}$$

Now, let us extend the above problem formulation to the case when there are T LAZ sectors. Suppose $N^{(j)}$, $R_{min}^{(j)}$, $R_1^{(j)}$, $R_2^{(j)}$, $\lambda_{LAZ}^{(j)}$, $\rho_{LAZ}^{(j)}$ and I_{SU_j} denote the number of SUs, R_{min}, R_1, R_2, λ_{LAZ}, ρ_{LAZ} and I_{SU} of j^{th} sector respectively. Then, the optimization problem (4.19) can be reformulated as (4.20).

$$\begin{aligned} \text{Maximize}: & \sum_{j=1}^{T} \left(\eta^{(j)} N^{(j)} - \omega\right) \\ \text{subject to}: & P\left(\sum_{j=1}^{T}\sum_{i=1}^{N^{(j)}} I_{SU_j} \leq I_{th}\right) \geq 1 - \epsilon \\ & R_{min}^{(j)} \leq R_1^{(j)} \leq R_2^{(j)}, \qquad j = 1 \ldots T \\ & 0 \leq N^{(j)} \leq \min(\lambda_{LAZ}^{(j)}, \rho_{LAZ}^{(j)}), \qquad j = 1 \ldots T, \end{aligned} \tag{4.20}$$

When all SUs within a LAZ sector have the same link capacity (Mbps/Hz), the weights $\eta^{(j)}$ correspond to the relative spectral capacities (or relative spectral efficiencies) of SUs in different LAZ sectors. A higher number of SUs is desired in the sector that has higher link capacity for each SU. Link capacities can be different when different types of SUs (e.g., LTE, WiFi, etc.) or SUs with different operating parameters (e.g., P_{ts}, r_{su}, etc.) operate in different LAZ sectors. Terrain characteristics, which might be different in different LAZ

sectors, affect the propagation characteristics, γ and σ, which in turn affect the link capacities of SUs. However, if all LAZ sectors have SUs with the same link capacity, then $\eta^{(j)} = 1$ for all j, and the objective function in (4.20) simplifies to a regular sum of $(N^{(j)} - \omega)$.

Optimization problems (4.19) and (4.20) are mixed-integer nonlinear programming problems because they require $N_j, j = 1 \dots T$ to be integers, and the interference constraint is nonlinear. Several algorithms such as cutting-plane [200] and branch-and-bound [201] can be used to solve this kind of problems. But often, due to their computational complexity, *Genetic Algorithm* (GA) is preferred. A GA is a heuristic search algorithm for solutions of optimization problems that starts from a random initial guess and attempts to find the best solution under some criteria [176]. Problems (4.19) and (4.20) can be easily solved using GAs.

In practice, both λ and ρ vary with time. The query requests arriving at the SAS is high during peak hours, while it is quite low during maintenance hours. Similarly, ρ changes when the SUs change their coverage area, transmit power, etc. Changes in these parameters and other operating parameters of the PU and the SUs also changes the distribution of I_{SU_j} and hence I_{agg}. Assuming that all these parameters are available to the SAS beforehand, it solves the optimization problem (4.20) whenever it expects these parameters to change. The SAS then responds to the spectrum queries coming from the SUs based on the solution of problem (4.20) — i.e., it allows a maximum of N spectrum access grants inside the LAZ at any given time.

Until now, we assumed that the PU has colocated Tx and Rx; while in practice, PUs may have non-colocated Tx and Rx. Examples of non-colocated PUs are TV stations and any other broadcast systems. Our derivations can be easily extended to a non-colocated PU by adding a margin, ΔI, to the I_{th} of the PU, where ΔI is a function of the path loss between PU-Tx and PU-Rx located at the edge of the coverage area.

4.6 Simulation Results

In this section, we present simulation results for demonstrating the performance of our proposed framework. In the first half of this section, we compare the results from our analytical solution with those from Monte-Carlo simulations, and justify that the normal approximation for characterizing the pdf of I_{SU} has negligible impact on the PU's interference protection. Then, in the later half, we present results to show that our framework dynamically adjusts the size of LAZ, computes the allowed number of SUs in the LAZ based on dynamic network conditions, and maximizes the overall spectrum utilization.

Let us define the database coverage area as a 300 km by 300 km square with a co-located PU at the center. The PU considered for this simulation study is an actual MetSat earth station in the AWS-3 band located at Petuxant River, Maryland, USA. For this PU, regulators have defined a circular EZ of radius 126 km, and therefore we set $R_2 = 126$ km. The area outside R_2 is the UAZ region, and we divide it into square grids of side $2r_{su}$ km, each of which hosts a SU cell with radius r_{su}. We do not have access to the specific operating parameters of the PU, so, let us assume its transmit power, I_{th} and ϵ as 60 dBm, -100 dBm and 0.1 respectively unless otherwise explicitly stated. For the LTE based SUs, measurements have shown that there is no influence on the SU throughtput when the radar interference power is below -50 dBm [202]. Therefore, we assume that for proper operation of SUs, the interference from the incumbent should be below -50 dBm at least 0.9 fraction of the time. For simplicity, let us assume that the LAZ consists of a single sector, and has the same propagation environment (γ and σ) as the UAZ region. Also, the SUs in UAZ and LAZ have identical transmission parameters as outlined in Table 4.1. Furthermore, we assume that sensing results are not available to the database; therefore α in equation (4.16) is set to zero. Using these parameters, the SAS solves the optimization problem (4.19), and computes the optimum values of R_1 and N. We use those results to study the performance of the primary and secondary networks in terms of interference protection and spectrum utilization respectively.

Table 4.1: Sample parameters for simulations

Radio frequency, f	1755 MHz
Radiation pattern	Omnidirectional
SU transmit power, P_{ts}	23 dBm
SU cell size, r_{su}	2 km
Total spectrum requests from SUs, λ	$10,000$
Channel bandwidth (W_s)	15 MHz
Path loss exponent, γ	2
Standard deviation of shadow fading, σ	3 dB

Table 4.2: Four scenarios considered in Figure 4.6

Scenario	γ	σ (dB)	P_{ts} (dB)
1	2.5	4	35
2	2.5	7	35
3	2	4	23
4	2	7	23

4.6.1 PU Interference Protection: Our Approximation versus Monte-Carlo Simulations

The closed-form expression for I_{agg} was derived based on the following two approximations: i) pdf of I_{SU} (in standard units) is log-normal, and ii) sum of log-normals is another log-normal. In order to justify that the PU's interference protection is not compromised by making such approximations, we perform a Monte-Carlo (MC) based simulation study. First, the optimization problem in (4.19) is solved by making the aforementioned approximations to obtain N and R_1. Using these results and equations (4.11) and (4.12), we obtain the ccdf plot of I_{agg}.

For performing the MC simulations, N SUs are uniformly distributed in the area between R_1 and R_2, and the aggregate interference power received at the PU is calculated using equations (4.2), (4.6) and (4.9). Then, we perform $50,000$ MC iterations, and compare the empirical ccdf of I_{agg} against the ccdf obtained from closed-form expressions. Figure 4.6 shows a close similarity between the two plots for different scenarios outlined in Table 4.2. This verifies that our approximation does not compromise the interference protection of the

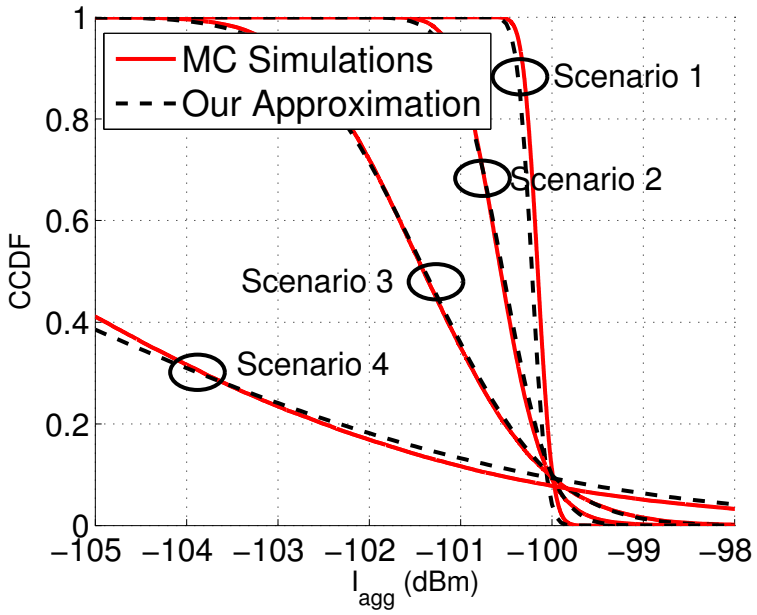


Figure 4.6: ccdf of aggregate interference experienced by PU

PU—the probabilistic guarantee of interference protection, $P(I_{agg} \leq -100 \text{ dBm}) \geq 0.9$, is always achieved. Our approximation slightly underestimates I_{agg} for large γ and small σ values, and slightly overestimates it for small γ and large σ values.

4.6.2 Spectrum Utilization: Adapting to Dynamic Network Conditions

To study the effect of model parameters on the secondary spectrum utilization, we define spectrum utilization in terms of *Area Sum Capacity* (ASC). ASC is the sum of channel capacity values of each co-existing SU within the SAS coverage area. Throughout the simulations, we assume that SU is a cell of radius r_{su}, which consists of a single Tx at the center and a single Rx at the cell edge. The channel capacity (C_{SU}) of a SU operating in a channel of bandwidth W_s is calculated using the Shannon capacity formula.

$$C_{SU} = W_s log_2(1 + \text{SINR}) \tag{4.21}$$

Here, the SINR at the SU-Rx is given by,

$$\text{SINR} = \frac{P_{ts}/P_L(r_{su})}{n_s W_s + I_{P2S} + I_{S2S}} \tag{4.22}$$

where, $P_L(r_{su})$ is the path loss between the SU-Tx and SU-Rx, n_s is the thermal noise power at the SU-Rx, I_{P2S} is the PU to SU interference and I_{S2S} is the aggregate interference power at the SU from other co-existing SUs.

Now, if we assume all SUs use the same bandwidth, the SU ASC (units = bits per second) is computed as,

$$ASC = W_s \sum_{i=1}^{N_T} log_2(1 + \text{SINR}_i) \tag{4.23}$$

where, N_T represents the total number of SUs in the system (both LAZ and UAZ), and SINR_i denotes the SINR at the i^{th} SU-Rx.

Effect of I_{th}

The effect of I_{th} on N, R_1 and ASC is shown in Figure 4.7. As I_{th} increases, the SAS extends LAZ towards the PU by making R_1 smaller until it becomes equal to R_{min}. Increased area in the LAZ and high I_{th} implies that more SUs (increased N) can be accomodated in the LAZ. Although the increased number of SUs in the LAZ lowers the SINR of existing SUs in both UAZ and LAZ regions due to increased I_{S2S} and decreases their capacity, Figure 4.7(c) shows that the ASC gain from added SUs is significant enough to overcome the loss. Next observation in Figure 4.7(b) is that around $I_{th} = -76$ dBm, R_{min} kicks in and does not allow R_1 to decrease further even when I_{th} increases. Also, since the upper bound of N depends on R_1 (recall equations (4.17) and (4.18)), N saturates and so does ASC. Another important observation in Figure 4.7(a) is the low sensitivity of N on ϵ. When ϵ is large, the SAS packs more SUs in the LAZ region by increasing the size of the LAZ. But when the size of LAZ increases (i.e., R_1 decreases), the distribution of I_{SU} also changes. For small R_1, the ccdf of I_{SU} moves towards higher values of i_{su} (see Figure 4.4) which increases the probability that

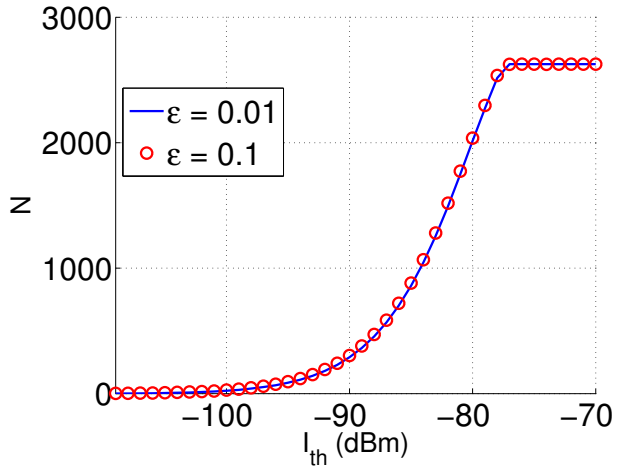
a SU causes interference to the PU. Because this change in I_{SU} applies to all SUs in the LAZ, N cannot be increased by a huge factor without violating the PU interference criteria. Therefore, we do not see a significant increase in N even when ϵ increases by an order of magnitude.

Effect of λ

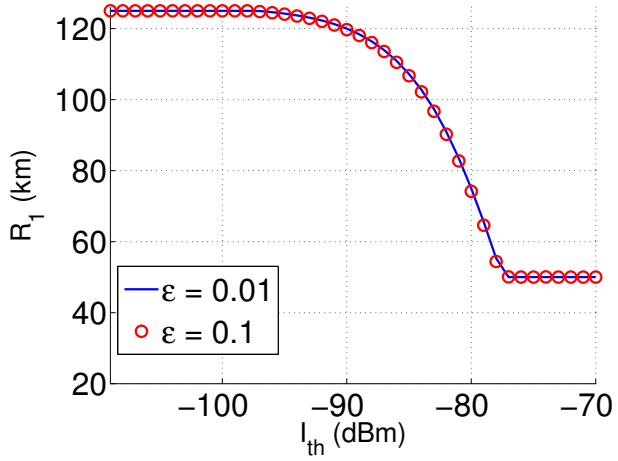
The effect of λ on N, R_1 and ASC is shown in Figure 4.8 for different I_{th} values at $\epsilon = 0.1$. When there are less number of SU requests, the SAS maximizes N by increasing the size of the LAZ, i.e., making R_1 smaller. Small λ implies small λ_{LAZ}, therefore, the upper bound on N is λ_{LAZ} but not ρ_{LAZ} (recall the last constraint of (4.19)). Consequently, increasing λ_{LAZ} by decreasing R_1 maximizes N, and hence, the ASC. However, the lower bound on R_1 prevents the SAS from decreasing it beyond R_{min} as noticed in Figure 4.8(b) for $I_{th} = -90$ dBm. Another observation from Figure 4.8(b) is that $R^{(2)}_{1_{lb}}$ for sensitive PUs (having small I_{th}) is large, and this results in large R_{min}. Large R_{min} decreases λ_{LAZ} which ultimately results in smaller N, and hence, a smaller gain in ASC as compared to the less sensitive PUs.

Effect of r_{su}

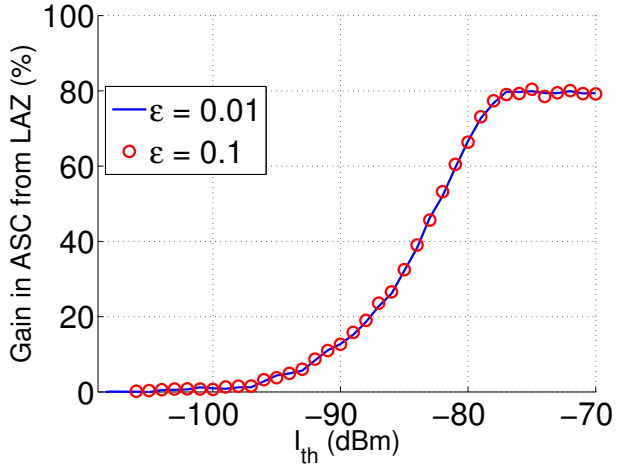
Figure 4.9 shows that our framework adapts to the change in SU cell size, and addresses the co-existence among SUs in the LAZ. From equation (4.18), ρ_{LAZ} decreases when r_{su} increases for any I_{th} value. When λ and I_{th} both are large, ρ_{LAZ} dictates the upper bound on N. So, in order to maximize N, SAS increases the size of the LAZ by decreasing R_1. However, for sensitive PUs, LAZ cannot be increased by a huge factor, otherwise the PU interference criteria may not be satisfied. Therefore, N is small when I_{th} is small. As N decreases with increasing r_{su}, a decrease in ASC gain is observed. Recall our assumption that the SU cell consists of a single Tx at the center and a single Rx at the cell edge. Large SU cell size implies reduced SINR at the SU-Rx, which causes the ASC gain to decline sharply even



(a) N versus I_{th}.

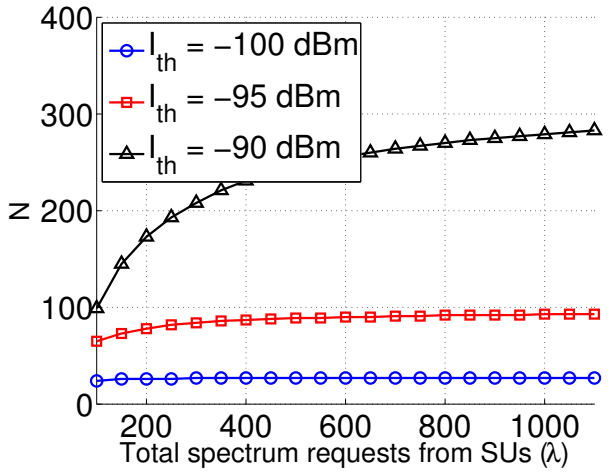


(b) R_1 versus I_{th}.

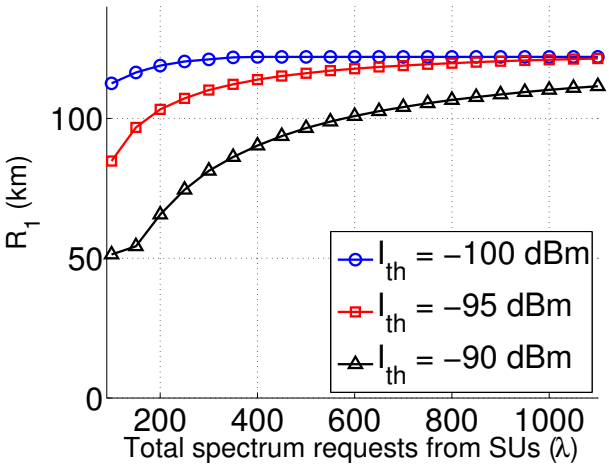


(c) ASC versus I_{th}.

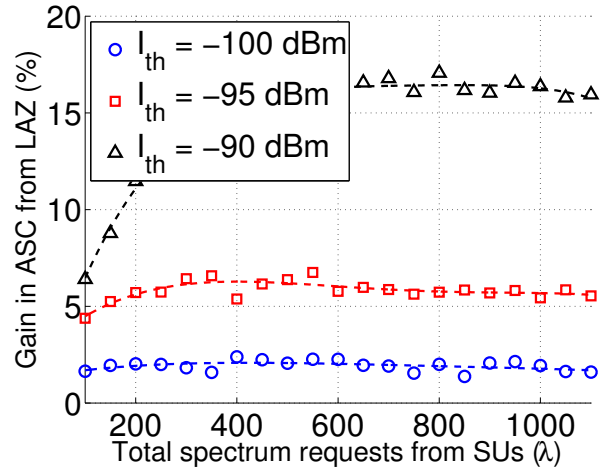
Figure 4.7: Effect of PU interference threshold, I_{th}, on N, R_1 and ASC



(a) N versus λ



(b) R_1 versus λ



(c) ASC versus λ

Figure 4.8: Effect of SU requests, λ, on N, R_1 and ASC

when N does not.

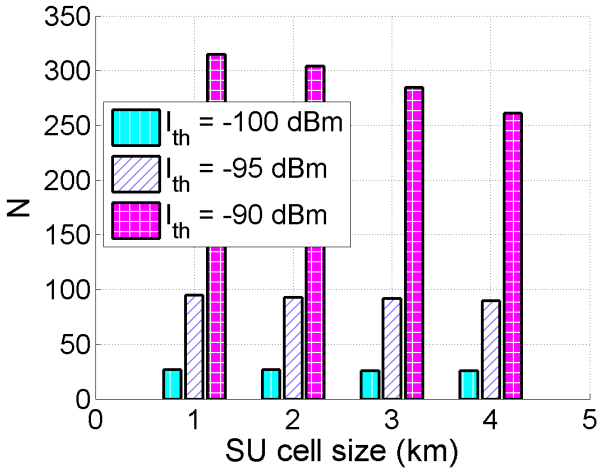
Effect of P_{ts}

Our framework also adapts to the change in SU transmit power in the LAZ. The results are summarized in Figure 4.10. When P_{ts} is large, the SAS reduces the size of LAZ by increasing R_1 to protect the PU from interference. Large R_1 implies small λ_{LAZ} and ρ_{LAZ}, the upper bounds on N. As a result, N is small. Nevertheless, this decrease in N does not necessarily reduce the ASC. With high P_{ts}, SU Rxs in the LAZ experience increased SINR which results in a gain in ASC. This gain overcomes the loss in ASC due to decreased N, specially when N is large, such as for $I_{th} = -95$ dBm and $P_{ts} = 16$ dBm in Figure 4.10(c). However, when N is very small, such as for $I_{th} = -100$ dBm and $P_{ts} = 23$ dBm in Figure 4.10(c), the ASC loss due to decreased N is higher than the gain achieved from increased SINR, and hence, the overall ASC gain from LAZ is small. This provides us a valuable insight that P_{ts} can be optimized for maximizing the ASC.

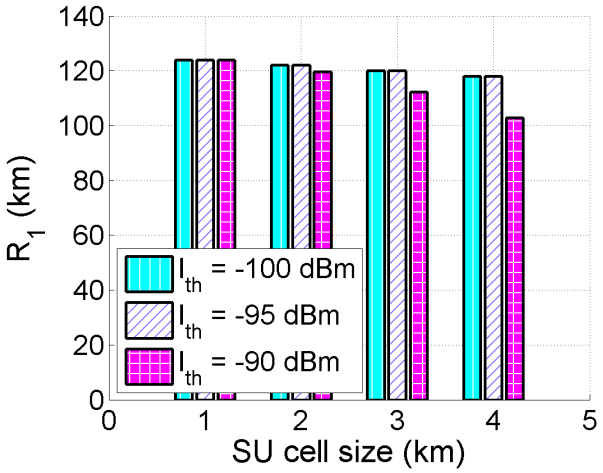
4.6.3 Economic Merit of MIPZ

In Figure 4.11, we illustrate the possible economic merit of implementing our proposed framework. The outer boundary represents the current EZ defined by NTIA [186] for a AWS-3 based MetSat Earth station, and the green annular region is the LAZ region defined by our model for a realistic set of parameters. The introduction of the LAZ region serves approximately 10 million people of Richmond, VA, Washington D.C. and Baltimore, MD, which would otherwise lie in the NTIA-defined EZ. With a bandwidth of 15 MHz, this area represents about 150 million MHz-POPs for a wireless operator. Using Verizon's valuation of the nearby AWS band in their proposed spectrum swap, this is worth approximately $132 million per auction period [177], [203].

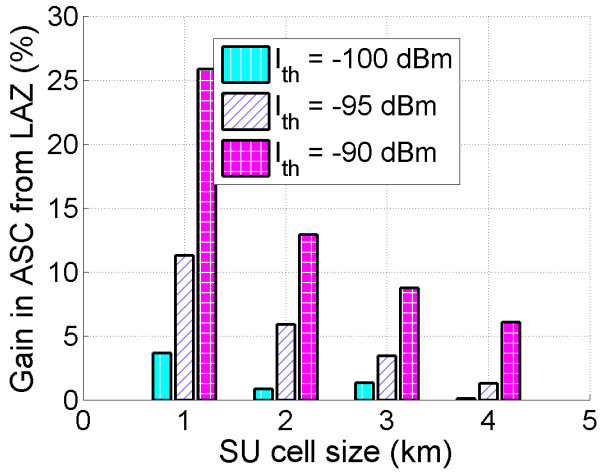
Although we analyzed the economic merit of MIPZ for this particular incumbent, similar



(a) N versus r_{su}

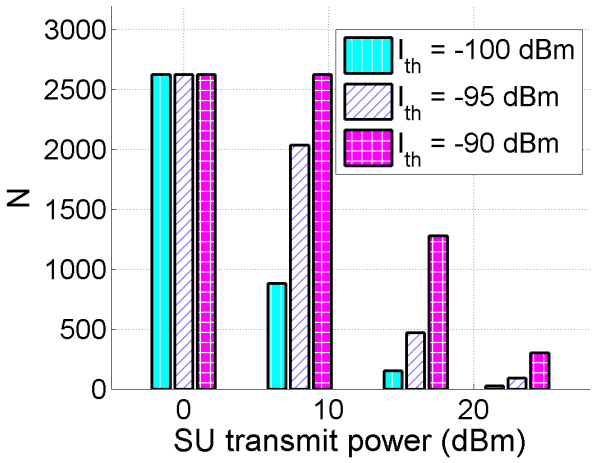


(b) R_1 versus r_{su}

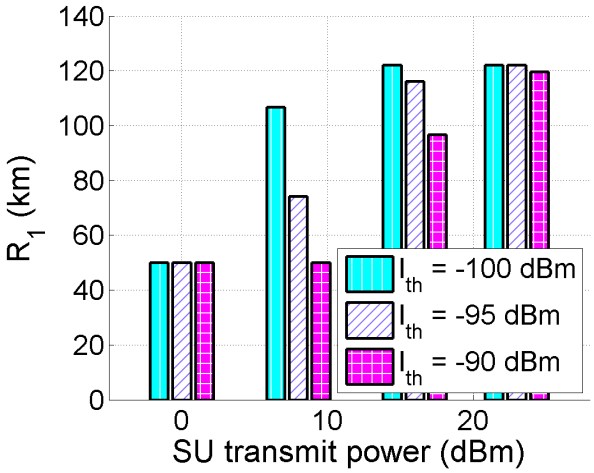


(c) ASC versus r_{su}

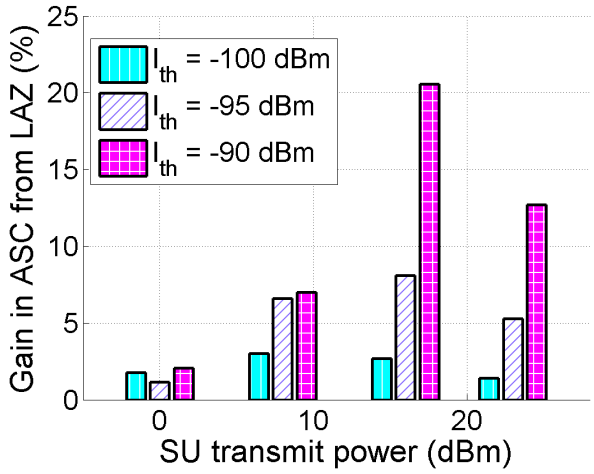
Figure 4.9: Effect of SU cell size, r_{su}, on N, R_1 and ASC



(a) N versus P_{ts}



(b) R_1 versus P_{ts}



(c) ASC versus P_{ts}

Figure 4.10: Effect of SU transmit power, P_{ts}, on N, R_1 and ASC

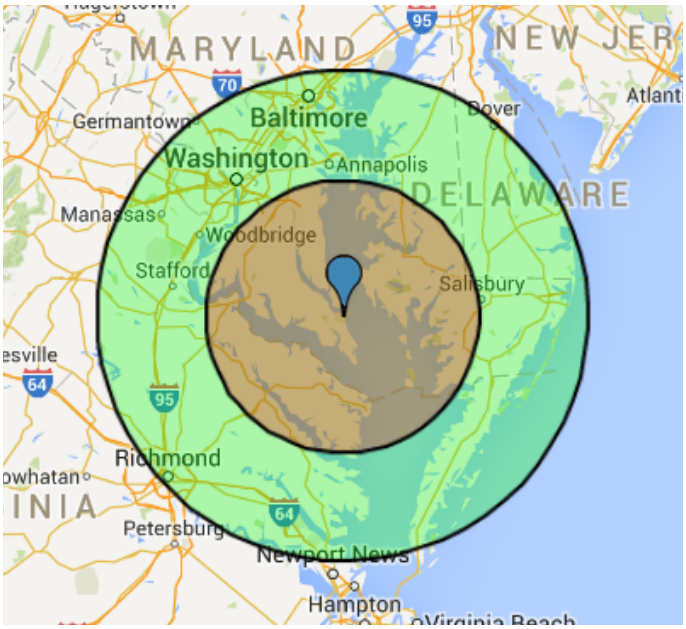


Figure 4.11: A map showing the service area of the LAZ region

analysis can be done for other incumbents as well. The economic merit varies based on the location of the incumbent on the map.

4.7 Chapter Summary

In this chapter, we introduced the concept of multi-tiered dynamic PZs for ex-ante spectrum enforcement in GDB-driven spectrum sharing. The proposed framework allows a limited number of SUs to operate closer to the PU, and improves the overall spectrum utilization while ensuring a probabilistic guarantee of interference protection to the PUs. By making some reasonable assumptions, we derived a closed-form expression of the aggregate interference power received by the PU, and used it to dynamically adjust the size of the PZ boundary. Using extensive simulation results, we showed that our framework can effectively adapt to the changing interference environment to increase spectrum utilization efficiency.

Chapter 5

Performance Analysis of 802.11ax

5.1 Introduction

Wireless Fidelity (Wi-Fi) has experienced tremendous growth in the past two decades and has become ubiquitous in today's home and enterprise networks. It has been estimated that the global worth of the Wi-Fi market will reach USD 33.6 billion by 2020 [204]. This huge success of Wi-Fi has, however, at the same time, led to a degradation in its performance, particularly in dense deployment scenarios. For instance, a Wi-Fi hotspot in a crowded street (e.g., Times Square), an airport, a stadium or a concert offers poor performance because of severe collisions arising due to channel contention from a large number of associated Wi-Fi stations (STAs). Motivated by the growing need for improved performance, the IEEE standardization committee has actively continued to release new protocols for Wi-Fi starting from 802.11a to the most recent 802.11ac. Additionally, to take Wi-Fi a step further, in 2014, the High Efficiency Wireless Local Area Network (HE-WLAN) task group (a.k.a. TGax) was formed with an objective of developing standards for the next generation Wi-Fi, namely IEEE 802.11ax [205]. According to its functional requirements, 802.11ax should support a ten-fold increase in the number of supported users over the same unlicensed spectrum, increase average user throughput by four times, and improve outdoor and multi-path signal

robustness [206].

Although most of the previous 802.11 amendments have improved the physical (PHY) layer throughput by adopting advanced techniques, such as higher order modulation and coding schemes, orthogonal frequency division multiplexing (OFDM), multiple input multiple output (MIMO), etc., the MAC layer protocol used in all amendments has been fairly similar to each other. Admittedly, the MAC protocols of 802.11 have been unable to keep up with the progress made at its PHY layer. Therefore, the inefficiency of the MAC layer presents a major bottleneck in translating the high PHY layer throughput into high throughput at the transport and application layers in real-world scenarios, particularly when the Wi-Fi deployment is dense [207]. To address this issue, the 802.11ax TGax is set to introduce several modifications to the 802.11 MAC layer protocol. The most notable feature is the adoption of orthogonal frequency division multiple access (OFDMA) in both the uplink (UL) (i.e., from STAs to the AP) and the downlink (DL) (i.e., from the AP to STAs). OFDMA divides the available physical resource, i.e., spectrum, into multiple orthogonal sub-channels—referred to as a resource unit (RU) in the 802.11ax terminology. The 20 MHz, 40 MHz, 80 MHz and 160 MHz Wi-Fi channels can be divided into 9, 18, 37 and 74 RUs, respectively. These RUs can then be allocated to different users as per their traffic demands, thereby enabling concurrent multi-user (MU) transmissions. This is in contrast to previous Wi-Fi standards wherein all devices transmit, one at a time, in the entire channel bandwidth.

For facilitating MU transmissions, the 802.11ax capable AP serves as a central controller and triggers the MU OFDMA mode by transmitting a *Trigger Frame* (TF) [208]. A TF is an 802.11ax frame structure that contains fields related to RU allocation for STAs, associated power control and transmission timing information. In the DL, the AP has the global knowledge of the packet queue status for each associated STA. Therefore, 802.11ax provisions purely schedule-based transmissions in the DL; one or more RUs are dedicated for packet transmission to a particular STA. However, in the UL, the STAs must explicitly communicate their traffic requirements to the AP by transmitting regular buffer status report (BSR). BSR information can either be elicited by the AP or piggybacked by STAs in certain transmitted

packets. 802.11ax supports two modes in which packets can be transmitted in the UL: i) scheduled access (SA), in which the AP schedules a set of STAs to transmit on dedicated contention-free RUs, and ii) random access (RA) in which, multiple STAs contend to transmit their packet using the exponential backoff-based distributed coordination function (DCF), similar to the one used in legacy[1] 802.11 MAC.

SA mode preempts channel contention from STAs and helps in improving the overall 802.11ax throughput. On the other hand, RA mode facilitates 802.11ax network in allowing transmissions from those STAs whose BSR information is not available at the AP. For example, newly joined STAs that have control frames to transmit or other STAs who haven't transmitted any packets for a while may not be scheduled in any SA RUs by the AP because of the unavailability of their BSR information. However, using RA mode, such STAs can contend and transmit their packets (along with piggybacked BSR information) in RA RUs. Thus, the use of RA RUs not only allows STAs to transmit their packets but also provides the required information to the AP so that the AP can schedule SA RUs to those STAs in the subsequent TFs. Therefore, in all practical implementations of 802.11ax, the AP dynamically allocates some of the RUs as SA RUs and the remaining ones as RA RUs such that it can collect enough BSRs for scheduling STAs in the SA RUs. It is important to note that maintaining a balance between RA RUs and SA RUs is a key to meet 802.11ax's functional requirements. In this chapter, we investigate this resource allocation problem in detail and devise an algorithm that facilitates the dynamic and optimized allocation of RUs such that the 802.11ax network throughput is maximized in different deployment scenarios.

Furthermore, we envision that at least during the initial deployments of 802.11ax networks, an 802.11ax capable AP would need to simultaneously serve both legacy 802.11 and 802.11ax STAs. Although 802.11ax devices are backward compatible with legacy 802.11 protocols, legacy STAs cannot understand and support MU OFDMA transmissions. They can only decode transmissions done on the entire 20 MHz channel. Therefore, in order to jointly

[1]Throughout the chapter, we use the terms "legacy Wi-Fi" and "legacy 802.11" interchangeably to refer to all previous versions of Wi-Fi including 802.11a/b/g/n/ac.

serve both legacy 802.11 and 802.11ax STAs, the AP has to allocate different fractions of airtime for single-user (to support legacy STAs) and multi-user (to support 802.11ax STAs) transmission modes. In this chapter, we study the issue of fair distribution of airtime between legacy 802.11 and 802.11ax transmissions when they operate in networks with different traffic requirements.

The core contributions of this chapter are summarized in the following bullets:

- We describe the novel MU-OFDMA based 802.11ax MAC that is being studied for 802.11ax in the TGax. We provide a detailed analysis of the MAC protocol and derive an expression for throughput achieved at the MAC layer.
- We investigate the impact of different distributions of RA RUs and SA RUs on the overall performance of 802.11ax MAC. Based on our findings, we devise an algorithm for the optimal allocation of RUs as SA RUs and RA RUs that maximizes the overall throughput of an 802.11ax network in all use-case scenarios.
- We envision that during the initial deployments of 802.11ax, an 802.11ax capable AP would need to serve both legacy 802.11 and 802.11ax STAs. In such settings, we analyze how to fairly distribute the airtime for jointly serving legacy 802.11 and 802.11ax STAs in networks with different traffic requirements.
- We enhance several PHY and MAC layer modules of NS-3 for supporting MU OFDMA transmissions as described in the latest TGax documents. We validate our analyses by comparing the performance of an 802.11ax network obtained from theoretical results with those obtained from extensive NS-3 simulations.
- Our results from NS-3 simulations indicate the existence of a unique problem in a heterogeneous Wi-Fi network (comprising of 802.11ax and legacy STAs)—i.e., the *artificial hidden node problem*, wherein some legacy STAs fail to detect transmissions from 802.11ax STAs, leading to collisions. We analyze the impact of this issue on the aggregate throughput performance of 802.11ax.

5.2 Related Work

The performance of 802.11-based networks has been extensively studied in the literature. The foundation of such analyses was laid by Bianchi in [209], where the author proposes a two-dimensional Markov chain model to characterize the throughput performance (in saturated conditions) of the 802.11 Distributed Coordination Function (DCF). Extensions to this model have been proposed for 802.11ax networks, particularly for the UL MU OFDMA mode of operation. For example, Bellalta et al. [210] compute the 802.11ax saturated throughput when the 802.11ax AP uses both, MU MIMO as well as MU OFDMA transmissions. The authors show that there exists an optimal number of active users that maximizes the aggregate network throughput. Additionally, Lanante et al. [211] compute the saturated throughput in the UL under the assumption that UL OFDMA-based RA (UORA)[2] is the only mechanism for transmitting UL packets. On the other hand, DL throughput in 802.11ax is essentially deterministic (under saturated assumptions), which is verified by the authors in [212].

The existing literature on 802.11ax provide deeper insights on 802.11ax performance. However, each of the aforementioned works restrict their focus on a sub-problem of the overall network performance. For example, the authors in [210] and [212] do not consider UORA – that enables stations to contend over a subset of the total RUs. The authors in [211] consider an RA-only UL system, thus failing to capture the behavior of a practical 802.11ax network which uses both RA and SA mechanisms simultaneously. Note that the RA mechanism informs BSR information to the AP and facilitates SA transmissions. Hence, we argue that a study that does not consider RA and SA transmissions jointly is incomplete and does not reflect the practical behavior of 802.11ax networks. In addition, the existing works focus on performance of an 802.11ax-only network and do not study the network performance in the presence of legacy 802.11 users. We believe that the later is a more practical scenario, at least in the initial phases of 802.11ax deployments.

In this chapter, we consider a system model that is accurate as per the latest TGax submis-

[2]We describe the UORA scheme in Sec. 5.3

sions, and consider a scenario where UORA is used in conjunction with SA, i.e., when the AP transmits a TF, it provides scheduling information for STAs on a subset of RUs, while the remaining RUs are used for RA. Along with the saturated system throughput, we characterize 802.11ax performance in terms of *BSR delivery rate*—a metric that is important in dynamic network environments. Furthermore, we study the 802.11ax system performance under different use-case scenarios where the traffic requirements in the UL and DL are asymmetric. Finally, we analyze the performance of a heterogeneous network comprising of legacy 802.11 as well as 802.11ax STAs, both of which are jointly served by a single 802.11ax-capable AP.

5.3 MAC Scheme for 802.11ax

In this section, we describe the new MAC scheme that has been proposed in the current TGax documents [205] as a part of the 802.11ax standardization process. Introduction of multiple other features—such as Dynamic Sensitivity Control (DSC), Basic Service Set (BSS) coloring, etc.—for improving the efficiency of the 802.11ax MAC layer are equally interesting topics. However, in the interest of space, we shall limit our discussions to MU OFDMA.

The granularity of a frequency resource in the legacy 802.11 standards is a 20 MHz-wide channel that is composed of 64 OFDM sub-carriers, each of which is 312.5 kHz wide. This is set to change in 802.11ax, where the sub-carrier width will be reduced by a factor of four to 78.125 kHz. This improves the robustness of 802.11ax against multi-path fading in outdoor environments. Further, a block of 26 sub-carriers constitutes the smallest unit of frequency resource—i.e., RU—that can be assigned independently to different users, thereby enabling multiple concurrent transmissions, also known as MU OFDMA transmissions. Thanks to MU OFDMA, a 20 MHz-wide channel can support a maximum of 9 parallel transmissions, while the 40, 80 and 160 MHz wide channels can support up to 18, 37 and 74 concurrent transmissions, respectively.

802.11ax will support MU OFDMA in the UL as well as DL. In both cases, the MU OFDMA

mode of operation is initiated when the AP broadcasts a TF. Since all DL traffic is routed to the STAs through the AP, the AP can transmit packets concurrently to multiple STAs over different RUs while taking into consideration performance requirements (such as latency, throughput etc.) of individual STAs. On the other hand, efficient allocation of RUs to the STAs in UL requires the AP to have a knowledge of the buffer occupancy status of the associated STAs. This is facilitated in 802.11ax using a buffer status report (BSR) frame that is sent by the STAs to the AP to notify the current occupancy status of their transmit buffers. BSR delivery to the AP can be AP-invoked (where the AP explicitly requests BSRs from its STAs) or unelicted (when the STAs transmit their BSRs without the AP's request). For the former case, any Quality of Service (QoS)-enabled frame can act as the BSR where the transmission opportunity (TXOP) field in the QoS Control sub-frame is re-used (when the network operates in MU OFDMA mode) as the BSR. In the latter case, STAs transmit their BSR information by piggybacking it along with their regular payload packets.

The UL MU OFDMA mode in 802.11ax will provision two types of RUs—SA RUs, on which the AP specifies (using the TF) an exact sub-set of STAs that can transmit in the UL without any contention, and RA RUs, on which those STAs can contend that have packets to transmit, but are not scheduled to transmit in the current MU OFDMA cycle because their BSR information is not available at the AP[3]. A TF that supports at least one RA RU is referred to as a Trigger Frame-Random Access (TF-R). In a TF-R, RA RUs are identified by a value 0 in the Association ID (AID) field, while each SA RU is identified by a non-zero AID value (corresponding to the AID of the STA that is scheduled to transmit on that particular RU). RA RUs can be used by: i) STAs that seek to join the network (to send control frames such as Association Requests), or ii) STAs that have recently joined the network or have just woken from a sleep state and have not been scheduled by the AP for transmissions in the UL (to send their BSR information).

The contention process used by STAs for transmitting their packets on RA RUs is referred

[3]In our work, we assume that STAs who have successfully reported their BSR information to the AP but are not scheduled for transmission in the current MU OFDMA cycle do not contend for RA RUs.

to as UORA. Note that UORA occurs in conjunction with the SA procedure in the UL OFDMA mode of 802.11ax. Each contending STA picks a random integer—the OFDMA Backoff Counter (OBO) uniformly in the range [0, OCW−1], where OCW stands for OFDMA Contention Window. On reception of the TF-R, STAs that have not been assigned to SA RUs but have a packet to transmit contend for transmission on the RA RUs. Every contending STA decrements its OBO by the number of advertised RA RUs (N_{RA}). If the OBO decrements to zero, the packet is transmitted on a randomly chosen RA RU. If not, the contention process is ceased until the reception of next TF-R. Much alike the contention procedure used in legacy 802.11 standards, OCW is reset to OCW_{min} following a successful transmission, and is doubled for every collision until the OCW reaches OCW_{max}. We assume that STAs that contend on RA RUs transmit their respective payload frames with the TXOP field in the QoS Control sub-frame set to indicate their respective transmit buffer occupancy status. Once an STA successfully transmits a packet (along with piggybacked BSR), it does not contend on RA RUs until the AP assigns enough SA RUs for the STA to be able transmit all the packets reported in its latest BSR. Note that once the AP knows BSR information of an STA, the former will allocate required resources to the later based on its quality of service (QoS) requirements such as latency, throughput, etc. Fig. 5.1 provides an illustrative example of UORA operation in conjunction with SA in 802.11ax UL OFDMA.

Transmissions shown in Fig. 5.1 correspond to one cycle of UL MU OFDMA transmissions. Throughout the chapter, we refer to this cycle as *TF cycle*. The AP can assign RUs for SA in the TF-R because it is aware of the transmission queue status of STAs 1 and 2. On the completion of the TF cycle, the AP has knowledge of STA 7's buffer status, and can assign STA 7 SA RUs in subsequent TF cycles.

Throughout this chapter, we assume that the only mechanism for BSR delivery available at the STAs is by piggybacking the BSR information on payload frames. We make this assumption because although a null QoS frame (i.e. a QoS frame with no payload) can be used to convey the BSR to the AP, if the TF-R assigns any of the RUs for SA, the time taken for the completion of TF cycle will depend on the time taken for the STAs that are assigned

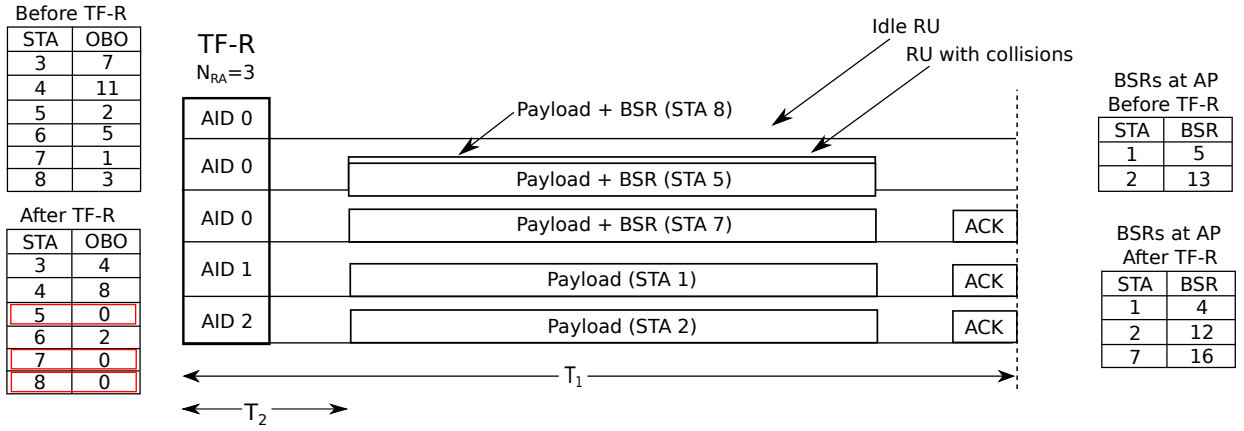


Figure 5.1: UORA used jointly with SA transmissions. STAs 1 and 2 are assigned RUs for SA, while the remaining STAs contend for transmissions on the three RA RUs. STAs 5, 7 and 8 decrement their OBOs to zero, and transmit on randomly selected RUs. This leads to a collision on the second RA RU, and successful transmission on the third RA RU; the first RA RU remains idle.

SA RUs to complete their payload transmissions. By transmitting the null QoS frame, remainder of the air-time in the TF cycle is wasted even if the transmission is successful. The only pragmatic use-case where the null QoS frame can be used for BSR delivery is when all RUs are assigned for RA. In such circumstances, it is advantageous to use a null QoS frame because if transmissions on all RUs collide, then the air-time wasted is small. This procedure is similar in spirit to the use of RTS/CTS frame in legacy transmissions whereby payload transmissions can be preceded by RTS/CTS exchange so that if the RTS/CTS frames collide, the wasted air-time is minimized.

Furthermore, we assume that only the RA RUs are used for BSR transmissions. This is becuase the sub-field (TXOP duration) in the QoS Control sub-frame that is used for conveying the BSR can have different interpretations based on the mode in which the 802.11ax AP operates. The TXOP sub-field is normally used by the STAs to request a specific TXOP duration for subsequent transmissions. However, the 802.11ax standard requires the AP to interpret the TXOP sub-field as the BSR of the corresponding STA when the network operates in MU OFDMA mode. Although BSRs can be transmitted piggybacked on payload frames on SA RUs, STAs can potentially use the TXOP field in the regular context.

Therefore, the AP can be certain of TXOP sub-field intepretation (as a BSR) only when the BSR is delivered on one of the RA RUs.

From the aforementioned discussions, it is clear that the AP can schedule UL MU OFDMA transmissions effectively only if the STAs are successful in delivering their respective BSRs over the RA RUs. Consequently the choice of division of RUs between RA and SA RUs is a critical factor influencing the overall network performance. We look at the impact of this design choice in the next section.

5.4 Performance Analysis of 802.11ax

In this section, we analyze the performance of the MU OFDMA scheme described in the previous section. In particular, we derive expressions for the following two key performance metrics: i) Throughput, and ii) BSR delivery rate.

Let us consider an 802.11ax network consisting of a single AP and n STAs. Assume a saturated network, where the transmission queue of every STA is always non-empty. Nevertheless, STAs still need to inform the AP about their BSR information because the AP only schedules those STAs in the UL SA RUs whose BSR is known to it. Since MU transmissions is one the characteristic features of 802.11ax MAC, we assume that the AP as well as all STAs support MU transmissions in both UL and DL. However, since the DL MU OFDMA is based on purely schedule-based transmissions, the DL throughput is invariant to network parameters and we will discuss it briefly towards the end of the section. First, we focus our attention on the UL throughput of the 802.11ax MAC.

Suppose that the 802.11ax channel is divided into N_{RU} RUs, where N_{RA} RUs are allocated for RA and the remaining $N_{\mathrm{SA}} = N_{\mathrm{RU}} - N_{\mathrm{RA}}$ RUs are allocated for SA. Since there is one STA assigned to each N_{SA} RU in a TF cycle, the remaining $n_{\mathrm{ra}} = n - N_{\mathrm{SA}}$ STAs contend for transmission on N_{RA} RUs. Similar to many previous works on 802.11, let us assume that all nodes can hear transmissions from other nodes; i.e., there are no hidden nodes. Also, we

assume that channel conditions are ideal, i.e. there are no PHY layer impairments. Thus, in our model, packet errors occur only when multiple STAs transmit at the same time in the same RU.

Let us use the notation $W_i = 2^i W$ to denote the size of the OCW, where W_i denotes the OCW for back-off state i and W denotes the OCW_{min}. Let m be the maximum back-off state and $W_{\text{max}} = 2^m W$ be OCW_{max}. An STA transmits a frame when its OBO decrements to 0. As opposed to the back-off procedure in legacy 802.11, in 802.11ax, the OBO is decremented by N_{RA} after receiving the TF. The back-off process can then be modeled by a two-dimensional Markov chain, and the probability that an STA transmits its BSR in any of the N_{RA} RUs can be computed as follows [209, 213],

$$\tau = \frac{2(1-2p)}{(1-2p)\left(\frac{W}{N_{\text{RA}}}+1\right) + p\frac{W}{N_{\text{RA}}}(1-(2p)^m)}. \tag{5.1}$$

where, p denotes probability that a transmitted packet collides.

Similar to legacy 802.11, there is only one contention process running in the 802.11ax MAC. However, there are N_{RA} RA RUs, and collision among transmissions from multiple STAs occur only when they transmit at the same time on the same RA RU. Assuming that a packet is transmitted on a randomly chosen RA RU among N_{RA} available RA RUs, the probability that a transmitted packet results in a collision can be computed as,

$$p = 1 - \left(1 - \frac{\tau}{N_{\text{RA}}}\right)^{n_{\text{ra}}-1}. \tag{5.2}$$

Equations (5.1) and (5.2) can be solved using numerical methods for given values of W, m, N_{RA} and n_{ra}. Using the values of τ and p, we can compute the probability that at least one STA transmits in a considered RA RU during the TF as follows,

$$P_{tr} = 1 - \left(1 - \frac{\tau}{N_{\text{RA}}}\right)^{n_{\text{ra}}}. \tag{5.3}$$

Now, the probability P_s that a transmission in an RA RU is successful is given by the probability of exactly one transmission given that there has been a transmission on the considered RA RU.

$$P_s = \frac{n_{\text{ra}} \frac{\tau}{N_{\text{RA}}} \left(1 - \frac{\tau}{N_{\text{RA}}}\right)^{n_{\text{ra}}-1}}{1 - \left(1 - \frac{\tau}{N_{\text{RA}}}\right)^{n_{\text{ra}}}}. \tag{5.4}$$

Similarly, the probability P_{idle} that all RA RUs are idle because none of the STAs were able to complete their back-off procedure is given as,

$$P_{\text{idle}} = (1 - P_{tr})^{N_{\text{RA}}}. \tag{5.5}$$

Next, we define the following two time periods T_1 and T_2 (see Equation (5.6)) based on the TF cycle of Figure 5.1.

$$\begin{aligned} T_1 &= T_H + (T_{\text{TF}} + \text{SIFS} + T_\delta) + (T_P + \text{SIFS} + T_\delta) + (T_{\text{ACK}} + \text{SIFS} + T_\delta) \\ T_2 &= T_H + (T_{\text{TF}} + \text{AIFS} + T_\delta) \end{aligned} \tag{5.6}$$

where, T_H and T_δ refer to the time taken to transmit frame header bits and the propagation delay respectively.

- T_1**:** T_1 represents the time spanned by a TF cycle when there is at least one RU on which a packet is transmitted. This includes two cases: i) a TF cycle that allocates at least one RU as SA RU (this case always results in transmissions in the allocated SA RUs), and ii) a TF cycle that allocates all RUs as RA RUs and there is at least one STA that transmits on an RA RU. In either case, the duration of a TF cycle is T_1.

- T_2**:** T_2 denotes the time duration of a TF cycle for which all RUs are assigned as RA RUs (i.e., $N_{RA} = N_{RU}$) but none of the STAs transmits a packet due to non-zero OCW values. In this case, the AP can transmit a new TF with same/different RU assignments after sensing the channel idle for an AIFS duration.

Based on the allocation of RUs as RA RUs and SA RUs in a TF cycle, the following throughput expressions can be derived.

1. $1 \leq N_{\text{SA}} \leq N_{\text{RU}}$ (at least one RU assigned for SA and the rest are assigned for RA):
   When a TF comprises of at least one SA RU, irrespective of whether transmissions occur in RA RUs, the AP must reserve the channel for T_1 duration to allow transmissions in the SA RUs. In this case, the throughput is computed as,

$$S_{ul} = \frac{(N_{\text{SA}} + N_{\text{RA}} P_{tr} P_s) E[P]}{T_1}. \tag{5.7}$$

   where, $E[P]$ denotes the expected packet size in bits.

2. $N_{\text{RA}} = N_{\text{RU}}$ (all RUs are assigned as RA RUs):
   This case includes two sub-cases: i) none of the STAs are able to finish their respective back-off procedure, resulting in no packets being transmitted on any of the RA RUs (this event occurs with probability P_{idle}), and ii) at least one STA completes its back-off procedure and transmits on an RA RU. Combining these mutually-exclusive events, the throughput of a TF cycle can be computed.

$$S_{ul} = \frac{N_{\text{RA}} P_{tr} P_s E[P]}{(1 - P_{\text{idle}}) T_1 + P_{\text{idle}} T_2}. \tag{5.8}$$

Finally, let us use the notation S_{dl} to denote the downlink throughput of 802.11ax. Since 802.11ax DL transmissions are purely schedule-based, S_{dl} is independent of n and is computed as $S_{dl} = \frac{N_{\text{RU}} E[P]}{T_1}$. Note that each TF cycle used for DL transmissions delivers N_{RU} packets whereas each TF cycle designated for UL transmissions delivers $(P_{tr} P_s N_{RA} + N_{SA})$ packets on average. Therefore, if the the DL to UL traffic/packet ratio in an 802.11ax network is $\eta : 1$, then the aggregate 802.11ax throughput can be computed using Equation (5.9).

$$S_{11ax} = \frac{\eta (P_{tr} P_s N_{RA} + N_{SA}) S_{dl} + N_{RU} S_{ul}}{\eta (P_{tr} P_s N_{RA} + N_{SA}) + N_{RU}} \tag{5.9}$$

Consider a highly dense and dynamic use-case scenario for 802.11ax, such as a wireless hot-spot in a crowded street (e.g., Times Square in New York city)[4]. In such settings, due to severe contention on RA RUs, many STAs might fail to successfully report their BSR information to the AP. Thus, the AP cannot schedule them in the SA RUs of subsequent TF cycles. This effect is more pronounced for STAs that need to join (by sending control packets on an RA RU) or have just joined the network but haven't reported their BSR to the AP. In order to assess how well an 802.11ax network supports such STAs in dense and dynamic use-cases, quantifying the UL throughput itself is not sufficient. Rather, the efficiency of the MAC layer in terms of the average number of BSRs collected per TF cycle must be analyzed. We coin a new metric, namely *BSR delivery rate*, denoted by β for facilitating this measurement. In particular, β can be calculated using Equation (5.10).

$$\beta = N_{\mathrm{RA}} P_{tr} P_s. \tag{5.10}$$

Ideally, an 802.11ax network delivers best performance to STAs by simultaneously offering high throughput and β. However, we must note that these two are conflicting requirements in the UL. If the goal is to maximize the UL throughput, the AP must allocate all RUs as SA RUs, but that will lead to $\beta = 0$. When $\beta = 0$, the AP cannot schedule enough STAs in the subsequent TF cycles, thus lowering the throughput. On the other hand, if the objective is to maximize β, i.e., maximally support new STAs for reducing their latency, then all RUs should be allocated as RA RUs. However, this would reduce the UL throughput because the efficiency of RA RUs in successfully transmitting a packet is significantly low due to contention. Clearly, an optimal balance between throughput and β can be achieved by carefully allocating RA RUs and SA RUs. We study this issue in detail in the next section.

[4]We use the term "dynamic" to refer to a network use-case scenario where STAs join/leave the network frequently.

5.5 Optimal RU Allocation Scheme

As discussed in the previous section, striking an optimal balance between N_{SA} and N_{RA} is critical in achieving a stable UL throughput in 802.11ax networks. On one hand, in order to increase the aggregate throughput, the AP can choose to assign a large fraction of the RUs as SA RUs—as contention-free transmissions on the SA RUs provide the maximum possible throughput. On the other hand, the AP cannot assign STAs for schedule-based transmissions unless it knows the BSRs of the corresponding STAs. Since we assume that the only mechanism for BSR delivery is through contention on the RA RUs (recall this discussion from Sec. 5.3), the AP must select N_{SA} and N_{RA} such that it never runs out of BSR values. An arbitrarily chosen division of RUs may imply that the network either lacks enough resources to meet STAs' demand for transmission (when it assigns a larger N_{RA} than is required). It may also imply that the network wastes some resources because of unavailability of STAs' BSR information (when it assigns small N_{RA}).

If the objective is to maximize the throughput, the AP must select N_{SA} and N_{RA} such that BSRs are collected from STAs at exactly the same rate at which these STAs can be scheduled on SA RUs, at least on an average sense. We refer to such a system state as the *steady state* of the system. We now outline the requirement for a system to be in steady state. Suppose that the AP uses N_{RA} RA RUs and, on an average, successfully collects BSR information from $\beta = P_{tr}P_sN_{RA}$ STAs in each TF cycle. The AP allocates the remaining N_{SA} SA RUs for serving the UL traffic demand of STAs whose BSR information is known to the AP.

We assume that STAs report BSRs to the AP in terms of the number of available packets in its transmit buffer. Further, we assume that the mean length of the BSR field is λ. This implies that if one SA RU allocation to an STA results in transmission of one packet, then that STA must be scheduled in λ TF cycles before its UL buffer is empty. Further, if an STA s reports a BSR of λ_s, we assume that the STA will not contend for transmissions on RA RUs until it is scheduled for transmitting λ_s packets in the subsequent UL TF cycles by the AP. We claim that this assumption is pragmatic because the AP has a knowledge

of at least λ_s packets available in the buffer of STA s. Therefore, any further transmission attempt from the same STA on RA RUs will only increase the overall contention.

Given this, for an 802.11ax network to be stable, the demand from STAs—i.e., $\beta \times \lambda$ packet transmission requests—must be equal to the supply—i.e., N_{SA} packet transmission opportunities. If this condition is not satisfied, either the AP collects BSR information from a larger number of STAs on average than can be assigned using the available SA RUs, or there might a fewer number of STAs for which the AP knows the BSR information than the available SA RUs. Equation (5.11) concisely characterizes the mathematical representation of a stable 802.11ax network.

$$N_{SA} = \lambda\beta \implies N_{SA} = \lambda P_{tr} P_s N_{RA} \tag{5.11}$$

Given that a system is in the steady state, on an average, the AP knows the BSR values of exactly as many STAs that are assigned SA RUs for transmissions. Equation (5.11) further implies that, on an average, the AP only knows the BSR information of N_{SA} STAs. Thus, if there are a total of n nodes, in the steady state, $n - N_{SA}$ nodes contend for transmission on N_{RA} RA RUs and N_{SA} nodes transmit on contention-free SA RUs.

From Equation (5.11), it is clear that the optimal values of N_{SA} and N_{RA} depend on λ. Further, since P_{tr} and P_s depend on the network size (n), the optimal N_{SA} and N_{RA} also depend on n. In practical 802.11ax networks, λ for each STA might be different and change with respect to time. Generally speaking, the AP may not be able to track this information for all associated STAs. Consequently, although an optimal N_{RA} can be computed theoretically by jointly solving Equations (5.1), (5.2) and (5.11), a real-world AP does not have this luxury. Therefore, an AP must be able to learn the changing network dynamics on the fly and arrive at the steady state regardless of n and the distribution of λ across STAs. Towards this objective, we now describe an algorithm, Algorithm 1, that can be implemented at an 802.11ax AP for achieving the optimal distribution of SA RUs and RA RUs.

In Algorithm 1, Ψ denotes the set of STAs whose non-zero BSRs are known at the AP. Further, in a given TF cycle, let ϕ and ψ denote the set of STAs that have been assigned SA RUs and the set of STAs that successfully deliver a BSR to the AP, respectively.

Algorithm 2 Algorithm for optimal allocation of RU in 802.11ax.

Initialize: $\Psi \leftarrow \{\}$
while true **do**
  Compute $N_{\mathrm{SA}} = \min(|\Psi|, N_{\mathrm{RU}})$
  Sort BSRs in descending order
  Select N_{SA} STAs with largest BSRs in Ψ
  BSR[s] = BSR[s] - #scheduled_packets $\forall s \in \phi$
  if BSR[s] $= 0, \quad \forall s \in \Psi$ **then**
    $\Psi = \Psi \setminus \{s\}$
  end if
  Allocate $N_{\mathrm{RA}} = N_{\mathrm{RU}} - N_{\mathrm{SA}}$ RUs for random access
  Transmit Trigger Frame
  if $N_{\mathrm{RA}} > 0$ and BSR received on RA RU k **then**
    $\Psi \cup \{k\} \quad \forall k \in \psi$
    Update BSR[k] $\forall k \in \psi$
  end if
end while

In each TF cycle, the AP updates the BSR values of all scheduled STAs by decrementing their respective BSR values by the number of scheduled packets. Further, following the successful reception of BSR(s) from contending STA(s) on one or more of the RA RUs, BSR values of the corresponding STA(s) are updated.

The core idea used in Algorithm 1 is that as long as the AP is aware of the BSR information of N_{RU} STAs, the AP assigns all RUs for schedule-based transmissions, one for each STA. If not, the AP assigns an SA RU, one for each of those STAs whose BSR information is available at the AP, while the remaining RUs are assigned for RA. BSRs, once delivered, are valid at the AP until λ packets are scheduled in the UL. Thus, after λ packets have been scheduled in the UL for a particular STA, the AP no longer knows its buffer status. In Algorithm 1, $N_{\mathrm{RA}} > 0$ only when there are fewer than N_{RU} BSRs are known to the AP. These conditions ensure that the AP collects just the right number of BSRs that it can

schedule on the SA RUs. In Section 5.7, we evaluate the performance of Algorithm 1 by implementing it in NS-3 and performing simulations therein.

5.6 Airtime Distribution between Legacy Wi-Fi and 802.11ax

In this section, we leverage the analysis presented in previous sections and study a key practical issue in 802.11ax deployments—i.e., the appropriate distribution of airtime between legacy Wi-Fi and 802.11ax when both categories of STAs are jointly served by a single AP. Consider a scenario where a single 802.11ax capable AP needs to serve both legacy Wi-Fi as well as 802.11ax STAs. This will indeed be the case during the initial deployments of 802.11ax where the newly introduced devices will be 802.11ax capable whereas the existing devices will not support MU-OFDMA based 802.11ax transmissions. Therefore, in order to support both categories of devices, an 802.11ax capable AP needs to facilitate two disjoint operation modes: i) single-user mode, which allows transmissions to/from legacy Wi-Fi devices, and ii) multi-user mode intended for 802.11ax devices.

In single-user mode, transmission from each STA occurs over the entire channel bandwidth. Since 802.11ax devices are backward compatible with legacy 802.11 protocols, the former can decode the legacy 802.11 packet headers and back-off their transmissions. More specifically, 802.11ax devices can decode the network allocation vector (NAV) field in the MAC header and enter into power-saving mode. Note that there have been discussions in the TGax on whether to allow 802.11ax devices to contend for the channel during both single-user and multi-user modes of operation[5]. Permitting 802.11ax STAs to contend during both single-user and multi-user modes of operations allows them to transmit more frequently leading to fairness issues. Therefore, the TGax discussions advocate permitting only legacy 802.11

[5]Since 802.11ax STAs can also operate in legacy mode (i.e., single-user mode), they can contend for the entire channel if permitted to do so during the single-user mode.

STAs to contend for the channel when the AP provisions single-user mode of operation. Therefore, we establish our subsequent discussions based on the same assumption.

The single-user and multi-user modes operate dis-jointly and facilitate transmissions from legacy and 802.11ax STAs, respectively. In such settings, throughput and fairness are the key performance metrics that need to be considered while designing the system. It is often desired that the overall throughput of the network be maximized, but such a throughput maximization scheme might not be fair for all users. For instance, in a network composed of legacy and 802.11ax STAs, allowing the network to operate only in multi-user mode maximizes the overall network throughput, but doing so will be unfair to legacy STAs. Also, it has been shown that systems employing throughput fairness—i.e., each STA transmits the same number of packets on average—reduces the overall throughput of the network when some STAs (e.g., legacy STAs) only support lower rates. For example, a STA with very low rate occupies the channel most of the time, thereby lowering the aggregate network throughput. Research have shown that Airtime Fairness (AF)—a fairness scheme that allows an equal fraction of air time to each STA—achieves a proper balance between throughput maximization and fairness consideration in 802.11 networks. In particular, it has been shown both analytically and experimentally that: i) traditional notion of proportional fairness [214] translates to airtime fairness in CSMA/CA based system such as Wi-Fi [215], and ii) airtime fairness improves the aggregate performance of the network [216].

Let us assume there are n_{leg} legacy and n_{11ax} 802.11ax STAs associated to a single 802.11ax capable AP. Denote the total MAC-layer throughput of a purely legacy network having n_{leg} nodes by S_{leg} and that of a purely 802.11ax network having n_{11ax} nodes by S_{11ax}. Suppose that the AP operates in single-user mode for α fraction of time and multi-user mode for the remaining $(1-\alpha)$ fraction. Then, the throughput fairness between legacy Wi-Fi transmissions and 802.11ax transmissions in a heterogeneous Wi-Fi network is achieved

if the airtime distribution satisfies Equation (5.12).

$$\frac{\alpha S_{leg}}{n_{leg}} = \frac{(1-\alpha)S_{11ax}}{n_{11ax}} \implies \alpha = \frac{n_{leg}S_{11ax}}{n_{leg}S_{11ax} + n_{11ax}S_{leg}} \tag{5.12}$$

Similarly, airtime fairness between legacy Wi-Fi transmissions and 802.11ax transmissions is achieved if the airtime distribution satisfies Equation (5.13).

$$\frac{\alpha}{n_{leg}} = \frac{(1-\alpha)}{n_{11ax}} \implies \alpha = \frac{n_{leg}}{n_{leg} + n_{11ax}} \tag{5.13}$$

Consequently, the aggregate throughput achieved by a heterogeneous network consisting of both legacy and 802.11ax STAs is given by Equation (5.14).

$$S_{agg} = \alpha S_{leg} + (1-\alpha)S_{11ax} \tag{5.14}$$

We shall discuss the implications of Equation (5.14) for different network deployment scenarios in the next section.

5.7 Results and Discussions

In this section, we investigate the MAC layer performance of 802.11ax by applying the analysis presented in previous sections. We then validate our analysis by implementing the MU OFDMA based 802.11ax MAC in NS-3 and comparing analytical results with those obtained from extensive NS-3 simulations for various use-case scenarios. Finally, based on our results, we provide key insights on some practical issues that might arise during the initial deployments of 802.11ax. Henceforth, unless explicitly stated otherwise, we use the following set of parameters (see Table 5.1) for all of our simulations.

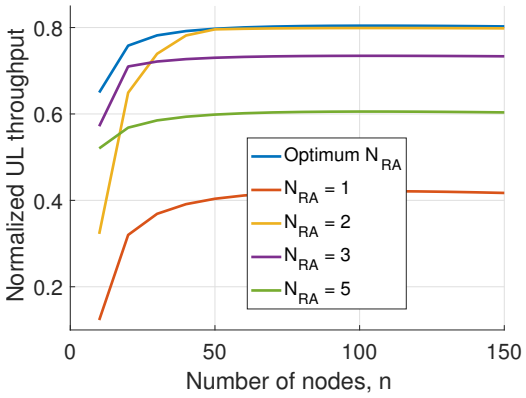
Throughout this section, results pertaining to throughput represent the normalized throughput (ratio of payload size in bits to the time taken to transmit the payload) observed at the

MAC layer, assuming that the underlying PHY layer uses a rate of 1 Mbps. In case of NS-3 simulations, this is achieved by using the same fixed PHY rate for control and data frames, and scaling the resulting throughput by the fixed PHY rate. Each simulation run lasts for 90 seconds, and the results presented are averaged over 10 simulation runs with different seed values. In each plot, unless explicitly stated otherwise, markers represent results from NS-3 simulations whereas the lines without markers correspond to analytical results.

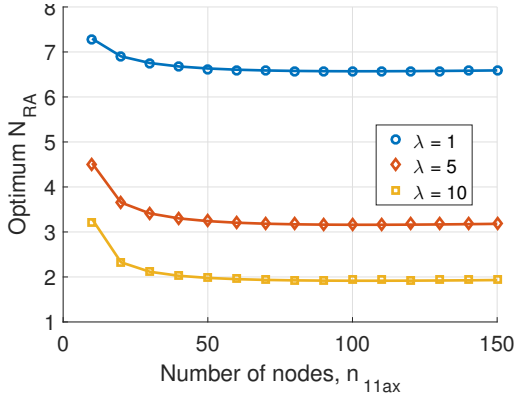
5.7.1 NS-3 Implementation of 802.11ax

For validating the analytical results derived throughout this chapter, we extend the capabilities of the NS-3 simulator to support MU OFDMA transmissions in the UL as well as DL. To achieve this, modules for PHY and MAC layer in the default NS-3 implementation were significantly modified. In legacy 802.11, all transmissions (in the UL as well as DL) occur over a single channel. In the MU OFDMA mode, however, these transmissions can occur in parallel, which necessitates the creation of separate transmit and receive chains for each RU. Furthermore, contending STAs in legacy 802.11 contend for a single channel. However, for the 802.11ax UL MU OFDMA to function, STAs contend for RA RUs. Therefore, state management functions such as the PHY state (e.g. IDLE/BUSY etc.) need to be implemented on a per-RU basis. We use the newly introduced *SpectrumWifiPhy* module to enable transmission and reception on specific OFDM sub-carriers. The use of this module also enables simulation of interference across transmissions from legacy (on an entire channel) and 802.11ax (on specific sub-channels) devices.

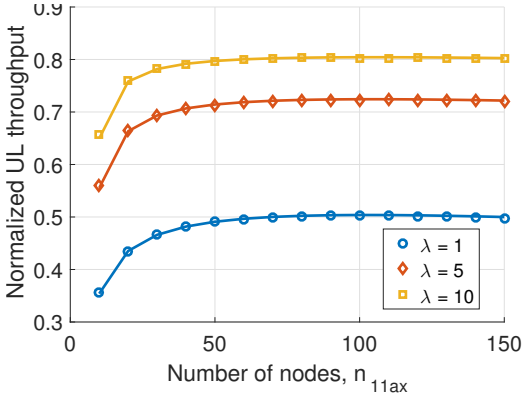
In order to facilitate other researchers in conducting 802.11ax based simulations, we have released the source-code of the modified NS-3 simulator [217]. In the near future, we also plan to make an official submission of our extended NS-3 modules to the NS-3 community.



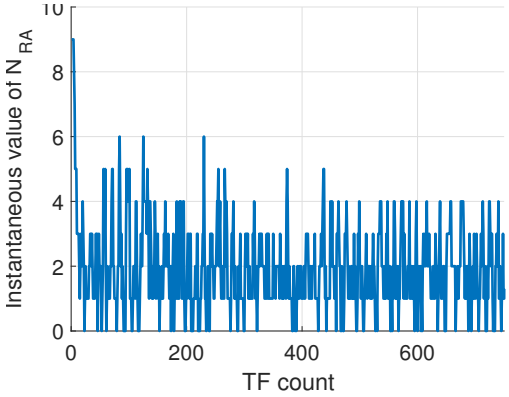
(a) Performance of Algorithm 1.



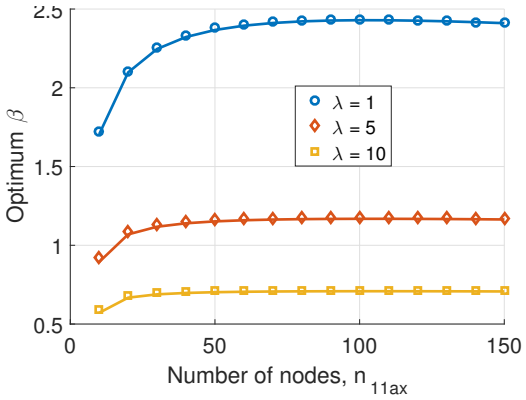
(b) Optimum N_{RA} versus n_{11ax}.



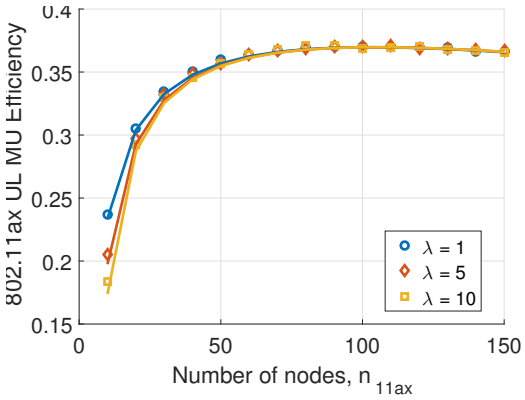
(c) UL throughput for different λ.



(d) Variation of N_{RA} across TF cycles.



(e) Optimum β versus n_{11ax}.



(f) MU Efficiency of 802.11ax.

Figure 5.2: UL performance of the 802.11ax MAC.

Table 5.1: Simulation parameters.

Parameter	**Value**	**Parameter**	**Value**
Prop. loss model	Okumura Hata	SIFS	16 μs
AP coverage	40 meters	T_δ	3 μs
$N_{\text{RA}}/N_{\text{SA}}$	From Alg. 1	N_{RU}	9
$\text{CW}_{\text{min}}/\text{OCW}_{\text{min}}$	32	m	5
$\text{CW}_{\text{max}}/\text{OCW}_{\text{max}}$	1024	TF-R	140 bytes
α	From Eq. (5.13)	P	1023 bytes
ACK	14 bytes	H	44 bytes

5.7.2 Performance of the 802.11ax MAC

Figure 5.2 shows the performance of UL MU OFDMA for a network that consists of only 802.11ax STAs. As described in the previous sections, λ represents the mean number of packets available in the transmit buffer of 802.11ax STAs. Figure 5.2(a) shows the MAC layer UL throughput of the network when $\lambda = 10$ and fixed N_{RA} values are used by the AP. The performance of these fixed allocation of RA RUs are compared with that of Algorithm 1. We first note that no fixed N_{RA} allocation offers throughput performance comparable to that of Algorithm 1. This is owing to the fact that the optimal N_{RA} value depends on λ as well as the network size, i.e., $n_{11\text{ax}}$. Thus, for each value of λ and $n_{11\text{ax}}$, the optimal N_{RA} is different. Furthermore, as discussed in Sec. 5.5, for the optimal allocation of RA RUs and SA RUs, the number of BSRs available at the AP must be N_{SA} on an average. To achieve this, Algorithm 1 dynamically changes the value of N_{RA} so as to maintain the steady state condition (Equation (5.11)). The variation of N_{RA} across TF cycles when an AP uses Algorithm 1 is shown in Figure 5.2(d). As seen in the figure, the instantaneous value of N_{RA} varies considerably, but its mean value converges to the optimal value obtained from Equation (5.11). This validates that Algorithm 1 indeed facilitates the optimal allocation of UL RUs in 802.11ax.

Figure 5.2(b) shows the optimal value (on an average) of N_{RA} for different values of λ, and the corresponding optimal throughputs are shown in Figure 5.2(c). For small values of λ, for example $\lambda = 1$ (which means, on an average, when an STA transmits a BSR, it informs

the AP that it has one packet available in its buffer), the optimal N_{RA} value is much higher than that for larger values of λ (for example $\lambda = 10$). This is intuitive because a small value of λ implies that the AP can schedule only a few packets on SA RUs in the UL based on the corresponding BSR. As a result, the AP needs to provision RA RUs frequently in order to collect enough BSRs and strike a balance between the demand on RA RUs and supply on the SA RUs. Further, a large value of N_{RA} implies that a larger fraction of RUs are used as RA RUs. This is corroborated by Figure 5.2(e), which shows the value of β, i.e. number of packets transmitted on RA RUs, for different values of λ. Now, since the efficiency of the random access mechanism in UL MU OFDMA can at best be around 38%, as seen in Figure 5.2(f), the throughput achieved is significantly lower than cases where N_{RA} is small.

Thus, in summary, a larger throughput can be achieved in UL MU OFDMA when λ is large. Large λ implies that the AP does not need to frequently collect BSRs from an STA, thereby allowing the former to allocate a large fraction of RUs as contention-free SA RUs. Additionally, Algorithm 1 facilitates the AP in optimally allocating RUs in the UL. The AP uses Algorithm 1 to dynamically adjust the value of N_{RA} on the fly and achieves optimal throughput for all values of $n_{11\mathrm{ax}}$ and λ. In all plots, the overlap between the markers (results from NS-3 simulations) and solid lines (results from analysis) validate the correctness of our analysis.

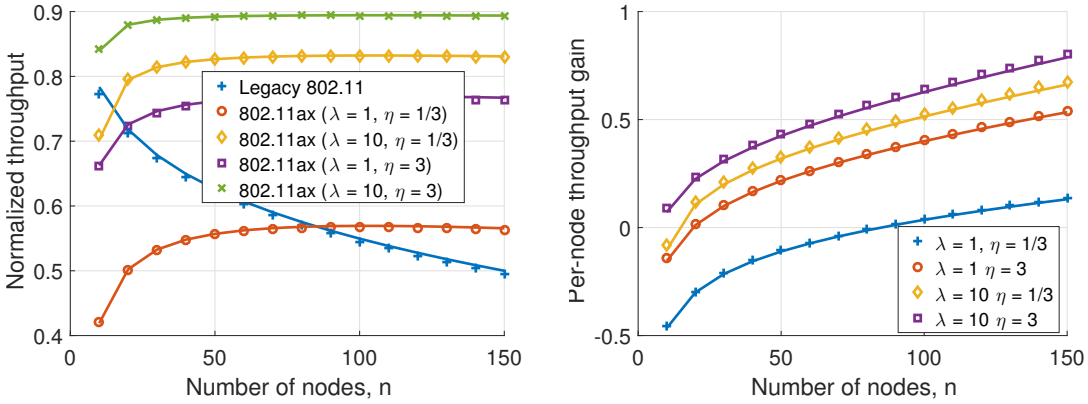
Next, we look at the aggregate (i.e., combined UL and DL) throughput performance of 802.11ax for different values of λ and η (i.e. DL to UL traffic ratio) and compare with legacy 802.11. Figure 5.3 summarizes our results. An important observation is that for legacy 802.11 networks, the aggregate throughput falls sharply as the network size increases, thus highlighting its lack of scalability to the network size. In contrast, an 802.11ax network scales well with the network size, which suggests that it can be deployed in use-case scenarios where an AP needs to support a large number of STAs (e.g., concerts, stadiums, etc.). However, it is also noteworthy that for certain values of λ and η, the performance of 802.11ax may not be as good as that of the legacy network. For instance, when UL dominates the DL traffic (i.e., small η) and λ (packet arrival rate at the MAC layer) is small, the AP must allocate

a large number of RA RUs for collecting BSRs which hurts the network throughput. *Thus, although in general, 802.11ax offers an improved performance over its legacy counterpart, our results indicate that a naive usage of 802.11ax without consideration of the network size and use-case scenario (η and λ) may lead to poor throughput performance in some cases.*

It must be noted that for legacy 802.11 systems, there is no explicit differentiation between UL and DL traffic. In most implementations of Wi-Fi, the legacy AP and STAs use the same set of contention parameters, resulting in same priority for UL and DL traffic. On the other hand, in 802.11ax systems, the DL traffic comprises of schedule-based transmissions, resulting in a deterministic and high DL throughput in comparison to UL traffic that comprises of both schedule-based and contention-based transmissions. Consequently, it follows that larger the value of η, higher is the aggregate network throughput. In most practical scenarios, the traffic in the DL indeed dominates traffic in the UL [218], which implies that in most scenarios, for an 802.11 network of a given network size (particularly, larger values of n_{11ax}), the aggregate network throughput in 802.11ax will be higher than that in a legacy network of same network size. Figure 5.3(b) shows the relative gain in per-STA throughput at the MAC layer for an 802.11ax network compared to a legacy 802.11 network. Thus, the per-node-throughput-gain, as specified in the functional requirements of 802.11ax, can be achieved in many scenarios. Admittedly, the gain reported in Figure 5.3(b) is further amplified if we consider the PHY-layer enhancements adopted by 802.11ax. A key observation is that *the gain in per-node-throughput is more pronounced for larger network sizes and for large η values.*

5.7.3 Joint Operation of Legacy Wi-Fi and 802.11ax

Now, we look at the joint operation of legacy 802.11 and 802.11ax when both categories of STAs are served by a single Wi-Fi AP. Figure 5.4(a) shows the aggregate throughput of such a network. For this study, we assume that the total number of STAs is fixed at 100 while we vary the proportion of 802.11ax and legacy STAs. In particular, we evaluate the aggregate



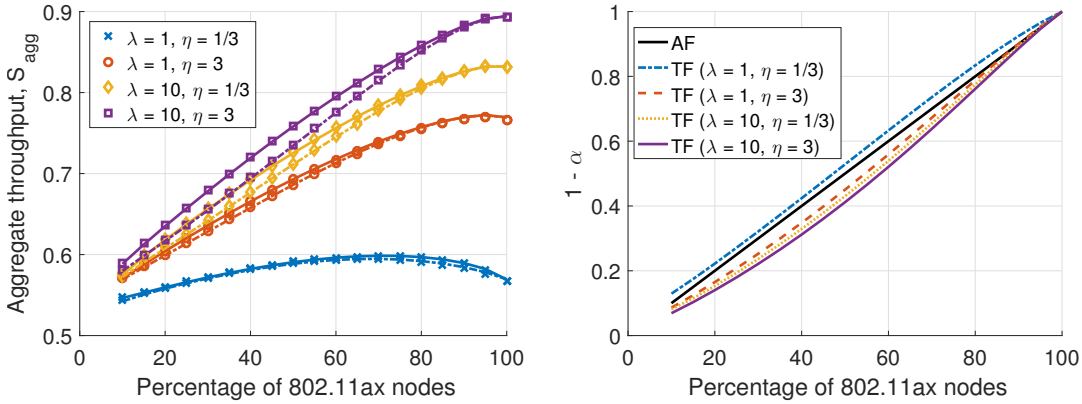
(a) Aggregate throughput.

(b) Gain in per-node throughput offered by 802.11ax.

Figure 5.3: Aggregate MAC-layer throughput of legacy Wi-Fi and 802.11ax.

throughput performance of such a heterogeneous Wi-Fi network by considering two fairness requirements: (i) the airtime is shared between legacy and 802.11ax STAs based on airtime fairness as described in Sec. 5.6, and (ii) the airtime is shared between the two types of STAs based on throughput fairness. In general, as expected, increasing the proportion of 802.11ax STAs in the network increases the aggregate network throughput. However, for small λ (e.g., $\lambda = 1$) and small η values, the aggregate throughput is not maximum when the fraction of 802.11ax nodes is 100%. Specially for small η, as seen in Figure 5.3(a), a legacy network with a small number of nodes (say 20 nodes) offers better throughput than an 802.11ax network with large number of nodes (say 80 nodes). In such cases, it is advantageous not to have too many nodes contending on 802.11ax. This observation indicates that based on the network dynamics, it may be beneficial at times to let some of the 802.11ax STAs contend in the legacy mode (since 802.11ax STAs can operate in single-user/legacy mode) so that the overall network throughput is maximized.

Finally, we show in Figure 5.4(b) the distribution of airtime between legacy Wi-Fi and 802.11ax when throughput fairness (TF) and airtime fairness (AF) are considered. Matching with our intuition, when AF is considered, the airtime is divided based on the proportion of legacy and 802.11ax STAs, resulting in a straight line. On the other hand, for achieving TF,



(a) Aggregate network throughput.

(b) Airtime allocated for 802.11ax transmissions.

Figure 5.4: Performance of a heterogeneous Wi-Fi network.

the airtime must be divided not only based on the proportion of STAs of a particular category, but also based on the throughput achieved by that class of STAs. For instance, 802.11ax achieves better throughput for large λ and η values. However, since the airtime dedicated to 802.11ax based on TF is small, this results in a reduced overall network throughput (see Figure 5.4(a)). Thus, our results show that in a heterogeneous Wi-Fi network, AF achieves the best aggregate network throughput in all use-case scenarios.

5.7.4 Practical Considerations

Latency of 802.11ax STAs

Although the SA RU-RA RU division algorithm presented in Sec. 5.5 achieves the optimal throughput for a given 802.11ax network, one limitation of the algorithm in its current form is that it favors those STAs whose BSR is already known at the AP. This can be unfair towards those STAs that are waiting to transmit their packets/BSRs on the RA RUs, particularly when λ is large. In practical scenarios, λ is large for applications that are bandwidth intensive (such as file transfer and downloads). However, such applications usually dominate the DL traffic. Moreover, these applications are less sensitive to delay; consequently making the

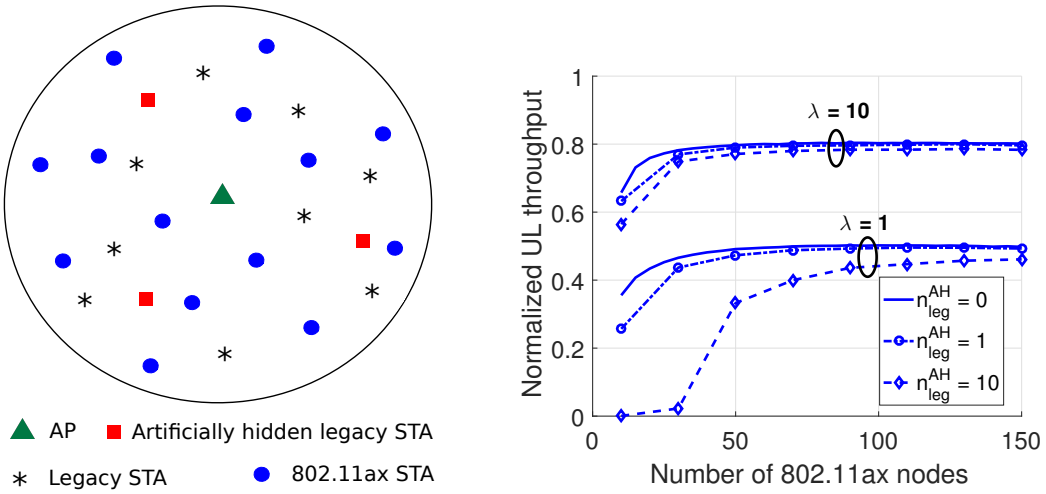
algorithm practical in most realistic scenarios. A class of application that can be bandwidth intensive as well as delay sensitive is media streaming. Algorithm 1 may likely offer poor performance in such scenarios, and alternate approaches to maximize throughput in such scenarios remains a part of our future work.

Introduction of artificial hidden nodes

The 802.11ax standard, for the first time in Wi-Fi networks, introduces OFDMA based transmissions. In a heterogenous network comprising of both, legacy and 802.11ax STAs, the legacy devices cannot decode preambles for RU-level transmissions from 802.11ax devices. To circumvent this issue, an 802.11ax AP can set the NAV field in TF to the time corresponding to an entire TF cycle. However, there may arise situations where legacy STAs miss the TF transmission from the AP. This can particularly be a problem when legacy STAs wake from a sleep state after the TF was transmitted by the AP. Under these circumstances, such STAs have to rely solely on energy detection-based sensing for detecting MU OFDMA transmissions. Although less likely, the occurrence of such scenarios in plausible in realistic deployment scenarios.

Owing to the use of RA based transmissions in UL MU OFDMA, there can be deployment scenarios where the average number of RUs on which transmissions occur in a given TF cycle is small (for example when $N_{\mathrm{SA}} + \beta = 2$). When this occurs, legacy STAs using an energy detection-based sensing can infer that the channel is idle and initiate a transmission, thereby resulting in a collision at the AP. This is similar to the concept of the classical hidden node problem occuring Wi-Fi networks, and is referred to as *artificial hidden nodes* [219]. It is noteworthy that the root cause of the artificial hidden node problem is the presence of RU level transmissions in 802.11ax, making this problem unique to networks where legacy 802.11 devices operate in close proximity to 802.11ax devices.

We leverage our NS-3 simulator to study the impact of artificially hidden legacy STAs on the throughput performance of 802.11ax devices. The topology considered for these set of



(a) Network topology. (b) 802.11ax UL throughput.

Figure 5.5: Effect of artificial hidden nodes on 802.11ax UL throughput.

simulations is shown in Fig. 5.5(a). Since the number of artificially hidden legacy STAs is expected to be small in practical deployment scenarios, we consider only a small number of legacy STAs. The impact of the collisions caused by different number of artificially hidden legacy STAs on the throughput of 802.11ax network is shown in Fig. 5.5(b).

We first note that the *presence of artificial hidden legacy STAs causes a non-negligible degradation of throughput for the 802.11ax network, particularly for small values of λ, even when the number of such legacy STAs is small.* Recall from Fig. 5.2(b) that for small values of λ, using an optimal N_{RA} leads to a large fraction of the total RUs being used as RA RUs. Consequently, owing to the low spectral efficiency of the UORA procedure (as can be seen in Fig. 5.2(f)), for small values of λ, the average number of RUs used for transmissions are small, thereby aggravating the artifical hidden node problem. Furthermore, as the number of legacy STAs in the network increases, the performance degration caused to the 802.11ax network increases. This can be attributed to the fact that as the number of legacy STAs increases, even if one STA is artificially hidden to the 802.11ax nodes, it can potentially lead to collisions at the AP.

5.8 Chapter Summary

In this chapter, we presented a detailed analysis of the performance of MU OFDMA-based MAC of IEEE 802.11ax for a wide range of deployment scenarios. We considered the performance of 802.11ax network when the network comprises of only 802.11ax as well as a combination of 802.11ax and legacy stations. The later is a practical scenario, especially during the initial phases of 802.11ax deployments. Simulation results, obtained from our NS-3 based simulator, provide encouraging signs for 802.11ax performance in many real-world scenarios. That being said, there are some scenarios where naive usage of MU OFDMA by an 802.11ax-capable Wi-Fi AP can be detrimental to the overall system performance. Our results indicate that careful consideration of network dynamics is critical in exploiting the best performance, especially in a heterogeneous Wi-Fi network. Lastly, we report a key observation that in some cases, certain legacy stations can be "artificially hidden" to transmitting 802.11ax devices, thereby degrading the 802.11ax performance.

Chapter 6

Operational Security of Incumbent Users

6.1 Introduction

The use of *geolocation databases* (GDBs) for enabling spectrum sharing has been mandated by the Federal Communications Commission (FCC) in the U.S. TV band [191] and the 3.5 GHz band [12, 6], and it is very likely to be adopted for other spectrum sharing applications as well. A GDB houses an up-to-date repository of *primary users* (PUs) and their operational attributes (e.g., location, transmit power, receiver sensitivity, etc.) and uses this information to determine spectrum availability at the locations of *secondary users* (SUs). Specifically, when an entrant SU requests access to the spectrum, the GDB first computes how the addition of that SU impacts the aggregate interference experienced by the PU, and then allows the SU to access the spectrum only if the estimated aggregate interference at the PU is below a predefined threshold. The practical advantage of GDB-driven spectrum sharing over spectrum sensing-driven spectrum sharing is that the former can more reliably identify fallow spectrum and minimize the probability of interference events. This makes GDB-driven spectrum sharing a critical and FCC-mandated component of real-world sharing systems,

such as the *Spectrum Access System* (SAS)[1] used in the 3.5 GHz *Citizens Broadband Radio Service (CBRS)* band [12].

Although using GDBs for spectrum sharing has many pragmatic advantages, it raises a potentially serious *operational security* (OPSEC) problem. For instance, SUs, through seemingly innocuous queries to the database, may be able to collect multiple database-responses to infer PUs' operational parameters, such as their geolocation, times of operation, protected contour, transmit power, antenna attributes, receiver sensitivity, etc. [14]. When PUs are commercial systems, such as the case in TV bands, OPSEC is not a major concern. However, in federal-commercial spectrum sharing, where some of the PUs are federal government systems including military and public safety communication systems, the information revealed by the databases may result in a serious breach of PUs' OPSEC. For example, PUs of 3.5 GHz band in the U.S. and $2.3 - 2.4$ GHz band in Europe include military radars, tactical systems, satellite Earth stations, air traffic control and telemetry devices, whose location privacy is extremely important for national security. Therefore, devising techniques and policies for protecting the location privacy of these PUs, while, at the same time, enabling commercial SUs to effectively utilize fallow spectrum is a key challenge in realizing spectrum sharing in these bands.

Recently, the FCC has mandated the consideration and implementation of techniques and mechanisms to ensure OPSEC, including PU location privacy, in sharing systems for the CBRS band [12], [6]. It has been strongly emphasized that PUs' operating parameters must be sufficiently obfuscated such that inference attacks through repeated queries to the SAS can be thwarted. Motivated by this, in this chapter, we investigate one of the key aspects of OPSEC—i.e., PUs' *location privacy*—in GDB-driven federal-commercial spectrum sharing. Our goal is to understand the potential location-privacy threats that may arise due to the information released by the SAS to the SUs. We show that an adversary, by

[1]The Spectrum Access System is a term used in recent Federal Communications Commission (FCC) notices and publications to denote a network of databases and supporting infrastructure deployed to enable dynamic spectrum sharing.

masquerading as a legitimate SU, can make multiple queries to the database, collect responses and use them to effectively infer the PUs' locations. We refer to this as a *location inference attack*. Unfortunately, this problem cannot be fully or adequately addressed by tightly controlling access to the database (unless adversarial SUs are identified in advance with high certainty) because other honest SUs need access to the database for getting access to the fallow spectrum.

To counter location inference attacks, we propose an *optimal obfuscation strategy* than can be implemented by a GDB to preserve the location privacy of PUs. The GDB implements this strategy and responds to queries made by SUs with obfuscated responses by optimally perturbing the actual responses. One of our main objectives in this chapter is to understand and optimally balance the inevitable trade-off between PUs' location privacy and loss in SUs' spectrum access opportunities due to obfuscated responses. Our proposed obfuscation strategy is optimal in the sense that it maximizes the PUs' location privacy while ensuring that the expected degradation in SUs' performance due to obfuscated responses does not exceed a threshold. Privacy analysis of this kind may help in wider adoption of dynamic spectrum sharing by allowing privacy-aware PUs to quantify the risk posed to their privacy and by providing specific techniques to mitigate that risk.

The core contributions of this chapter are summarized below.

- We provide motivation for investigating the problem by describing a location inference attack, based on Bayesian learning, that can be used by adversarial SUs to infer the locations of PUs in GDB-driven spectrum sharing. The problem discussed in this chapter is based on the real-world security issues and performance constraints of the SAS ecosystem being built for the CBRS band in the U.S.
- We describe how an adversary can make an inference attack strategy by choosing the query locations optimally. For an adversary, querying from an optimally chosen location ensures that the utility of the location information contained in the database response is maximized.

- We propose an optimal obfuscation strategy that can be implemented by the GDB to counter the location inference attack. In doing so, we identify a fundamental trade-off between the PU's privacy and the SU's spectrum utilization efficiency. The proposed strategy maximizes the location privacy of PUs while ensuring that the degradation in SUs' utility due to obfuscated responses (provided by the database) does not exceed a predetermined threshold. We formulate the obfuscation problem as a formal optimization problem.
- Using simulation results, we demonstrate the efficacy of our proposed obfuscation strategy in countering location inference attacks, including the location-inference strategy described in this chapter.

The rest of the chapter is organized as follows. We provide some technical background in Section 6.2 followed by related work in Section 6.3. Section 6.4 introduces the location inference attack and adversary's strategy for optimally choosing the query locations. We present our proposed optimal obfuscation strategy in Section 6.5. Simulation results that illustrate the performance of the proposed obfuscation scheme are presented in Section 6.6. Finally, Section 6.7 concludes the chapter.

6.2 Preliminaries

6.2.1 Database-Driven Spectrum Sharing

Realizing that the effectiveness of dynamic spectrum sharing depends on proper spectrum management and coordination among users that share the spectrum, the FCC adopted GDB-driven spectrum sharing model in the U.S. TV bands [191]. The GDB provides centralized spectrum management among other functionalities. The GDB has also been adopted for enabling a three-tiered spectrum sharing model in the 3.5 GHz band [12]. Specifically, a network of GDBs and supporting infrastructure—often referred to as the SAS—has been

mandated for enabling federal-commercial spectrum sharing in the 3.5 GHz band. The SAS is a dynamic database system that computes aggregate interference on the fly and provides real-time spectrum management. It dictates how and when SUs access the spectrum. For example, when a SU sends a spectrum access query, the SAS uses a power allocation function (generally defined by the regulatory agency) to compute the maximum allowable transmit power at the query location and responds to the query accordingly.

6.2.2 The Need for Location Privacy in GDB-Driven Sharing

In its Report and Order [6], the FCC finalized rules for governing the innovative 3.5 GHz CBRS band. The Report and Order prescribes federal-commercial spectrum sharing through a network of GDBs (a.k.a. SAS) supported by a real-time spectrum sensing system called Environmental Sensing Capability (ESC). In particular, the SAS is fed with real-time spectrum occupancy measurements from the ESC, which is used to determine channel availability and to control spectrum access. The SAS would need PUs' operational parameters, such as their locations, times of operation, receiver sensitivity, etc., which are considered sensitive and must be protected from exposure to a potential adversary. This is critical because some of the PUs that currently operate in the 3.5 GHz band include Department of Defense (DoD) radar systems, satellite Earth stations, air traffic control and telemetry services, whose operational privacy is extremely important for national security.

To address this issue, a common industry and government standards body—namely, the Spectrum Sharing Committee (SSC)—was created in 2015 within the Wireless Innovation Forum (WinnForum). The SSC works with the FCC to support the development and advancement of spectrum sharing technologies based on the three-tier architecture proposed for the 3.5 GHz CBRS band [15]. The main objective of this committee is to ensure that the 3.5 GHz band can be successfully commercialized through the creation of standards that will encourage rapid development of the CBRS ecosystem, protect incumbent operations and benefit all potential stakeholders in the band. As a step forward, the Security Require-

ments Working Group (SRWG) was formed under the SSC, and was charged with defining the OPSEC requirements, including location privacy, as well as the communication security requirements for spectrum sharing ecosystems.

The WinnForum has drawn up security and privacy requirements in the 3.5 GHz band and acknowledged the importance of implementing mechanisms to protect the location privacy of PUs (among other operational parameters) against inference attacks carried out by legitimate SUs. The SRWG recently released a draft of the standard that mandates the use of three different obfuscation procedures to help preserve the location privacy, among other operational parameters, of PUs [220]. These procedures are: i) ESC position estimate uncertainty, i.e., requiring ESCs to ensure that the location of PU activity cannot be accurately estimated or tracked; ii) obfuscating the protected regions, a.k.a. exclusion zones[2], of PUs before they are incorporated into the SAS, and iii) requiring the SAS to limit the information disclosure from query responses. In this chapter, we focus our study on the third procedure and provide an optimal solution to thwart location inference attacks that are based on repeated queries to the SAS [220].

In practice, an adversary may have capabilities to infer PUs' locations through other sources, e.g., by employing a network of spectrum sensing nodes. However, such attacks are not instances of a pure database-inference attack—i.e., an inference attack that is purely based on information released by the database—and cannot be prevented by controlling/restricting access to the database. Thus, the main concern of the FCC and the DoD regarding PUs' OPSEC in GDB-driven sharing is the possible "lowering" of the threshold for adversaries to gather sensitive information/intelligence which is made possible by GDB-driven sharing. In other words, they are concerned about adversaries gaining sensitive OPSEC-related information/intelligence with minimal effort and with minimal probability of detection. Deploying a network of sensors to collect OPSEC information is certainly possible, but would require much more effort and resources, and more importantly, would be more readily detected by

[2]An exclusion zone is a spatial separation region defined around a PU where co-channel and/or adjacent-channel transmissions are not allowed.

enforcement entities. GDB-driven sharing makes intelligence gathering inherently easier and more difficult to detect—this is the main concern shared by the spectrum regulatory agencies and the PUs, viz., DoD.

6.2.3 Metrics for Quantifying Location Privacy

In [221], the authors discussed three metrics for evaluating location inference attacks: i) *uncertainty*, ii) *inaccuracy*, and iii) *incorrectness*. Suppose o denotes the information observed by the adversary (e.g., database's reply to a query). Also, suppose that the information that the adversary extracts from the observation is in the form of $p(x|o)$, which is the probability distribution for possible values of the PU's location given the observation. *Uncertainty* is the ambiguity of this posterior distribution with respect to finding a unique answer (note that a unique answer need not be the correct one). The uncertainty is maximized if the result of a location inference attack is a uniform distribution of the locations.

Because the attacker does not have infinite resources, the result of a location inference attack is only an estimate, $\hat{p}(x|o)$, of the posterior distribution, $p(x|o)$. *Inaccuracy* is the discrepancy between the distributions $p(x|o)$ and $\hat{p}(x|o)$. It has been shown that uncertainty and inaccuracy are only indirect measures of location privacy [221], [14]. Alternatively, the database can calculate the expected distance between the location inferred by the attacker and the PU's true location. This distance is called the *incorrectness* of the attacker's inference. Mathematically, incorrectness, IC, is defined as:

$$\text{IC} = \sum_i p_i d_i, \tag{6.1}$$

where p_i denotes an attacker's belief about the presence of a PU at a location that is d_i distance away from the PU's actual location.

Reference [221] formally justifies that the incorrectness of the adversary's inference attack (i.e., his expected estimation error) determines the location privacy of users. Based on the

discussions provided in their seminal work, incorrectness is the most appropriate metric for quantifying location privacy because it reflects the physical measurement of distance and relates to real-world user privacy requirements. The authors also show that other metrics for location privacy, such as entropy and k-anonymity, are indirect measures, and often times, such metrics mis-estimate the true location privacy of users. Subsequently, several recent papers have used incorrectness as a metric to quantify users' location privacy [222, 223, 224, 225]. Therefore, throughout this chapter, whenever an explicit measure of PUs' location privacy is required, we will also use incorrectness as the metric even-though our subsequent discussions apply for any location privacy metric in general. Henceforth, we shall use the terms "location privacy" and "incorrectness" interchangeably.

6.3 Related Work

The proliferation of database-offered services (e.g., location based services (LBS), where mobile users share their location to obtain services such as getting directions, finding nearby restaurants, etc.) has triggered considerable research efforts that investigate methods to protect the privacy of users in such settings. In this context, researchers have proposed several methods to reduce the granularity of data representation in order to keep the user data private. Most of the existing work—e.g., sending space- or time-obfuscated versions of users' attributes [226], [227], hiding some of the users' attributes by using mix zones [228], sending indistinguishable fake/dummy queries [229], *k-anonymity* [230], *l-diversity* [231], *t-closeness* [232], etc.—focus on preserving the privacy of users who seek LBS by providing their locations to the database.

In contrast, the focus of this chapter is to study the privacy of database contents; i.e., PUs' location information which is stored in the database. While the objectives seem similar, the location privacy issues of LBS and spectrum database are clearly different. In LBS, the database is the "honest but curious" adversary, whereas in GDB-driven spectrum sharing,

the querier is the "honest but curious" adversary. Also, obfuscation (adding intentional inaccuracies in location information) degrades the quality of the services provided by the database in both cases, but its impact is far greater in the latter due to the negative impact on the PU in the form of harmful interference. For example, in LBS, the use of obfuscated location of the querying user does not make services offered from any geographical region unusable. On the other hand, in spectrum sharing, obfuscating PUs' locations precludes an additional geographical area from being allowed for spectrum sharing [233]. Furthermore, user anonymization schemes, such as k-anonomity and k-clustering [14], are not applicable in spectrum sharing, especially in cases where PUs may be very sparse, and/or are operated by a single organization (such as military radars operated by the DoD in 3.5 GHz band), in which anonymization is not meaningful. Therefore, the location privacy issue in LBS and GDB-driven spectrum sharing are different problems and solutions for the former cannot be used for the latter without non-trivial modifications.

Differential privacy [234] is another privacy-preserving technique that has gained considerable attention in recent years. It provides a *semantic* privacy model with strong protection guarantees; it captures the amount of disclosure that occurs due to the publication of sensitive data in addition to mandating how the published data should look. The core idea of differential privacy is that an aggregate result over a database should be the same, whether or not a single entry is present in the database. A generalization of differential privacy, called "geo-indistinguishability", has been studied in [224] and [225] for protecting the location privacy of users in LBSs. Unfortunately, the requirements of the SAS limit the applicability of these techniques in safeguarding the privacy of PUs. In particular, as discussed in reference [222], the overall objective of spectrum sharing, i.e., offering improved spectrum access opportunities to SUs while protecting PUs from harmful interference, prevents the SAS from being differentially private.

There is only a few existing work that addresses privacy concerns in GDB-driven spectrum sharing. In [187], a taxonomy of threats in spectrum sharing, along with several privacy issues and respective countermeasures, are summarized. The privacy of SUs in spectrum sharing

is studied in [235, 236], where the authors propose privacy-preserving mechanisms based on the principle of *private information retrieval*. Similarly, several other works have studied the issue of SU location privacy in collaborative sensing [237, 238, 239, 240]. However, PUs and SUs play different roles in spectrum sharing, which precludes the direct application of aforementioned works in addressing the privacy concerns of PUs.

There are some recent works that propose solutions to address the privacy concerns of both PUs and SUs in GDB-driven spectrum sharing [241, 242]. The proposed solution of [241] achieves bilateral utility maximization for both PUs and SUs, but the SAS-SU protocol used in the chapter is not consistent with that specified in the standards. Furthermore, the communication overhead inherent in the proposed scheme might be a bottleneck in many spectrum sharing scenarios. Reference [242] uses homomorphic encryption technique and offers promising results in terms of both PU and SU privacy. However, it has limitations in terms of query response time and communication overhead, making it not a viable solution for practical dynamic spectrum sharing scenarios.

Some practical approaches for addressing the PU privacy problem are studied in [14, 243, 222, 223, 233]. In [14], the authors propose several privacy-preserving techniques, based on generalization techniques, such as k-anonymity and k-clustering, for preserving the privacy of PUs. Unfortunately, the performance of these techniques depends on spatial orientations (i.e., relative locations) of PUs, and hence, they do not perform effectively in all scenarios. Reference [222] studies a privacy bound for PUs as the number of time slots until which a desired level of PU privacy can be achieved. Reference [223] provides simulation results to demonstrate the trade-off between PU location privacy and SU spectrum utilization. However, none of these papers provides a rigorous analysis of the trade-off between PU location privacy and SU spectrum utilization.

In this chapter, we address the aforementioned limitations, and propose an optimal obfuscation strategy that can be implemented by a GDB to maximize PUs' location privacy, while at the same time, ensure that the degradation in SUs' utility caused due to obfuscation is

below a threshold. Our methodology provides a formal framework for studying the fundamental trade-off between PU location privacy and SU spectrum utilization in spectrum sharing. While there has been considerable amount of research on location privacy in the context of LBS, to our best knowledge, this is one of the few works that rigorously analyzes PU location privacy in the context of GDB-driven spectrum sharing.

6.4 Location Inference Attack

In this section, we first describe the system model wherein we provide the details of the database, the database access protocol and a model for an adversary that makes inference based on information obtained from the database. Then, we describe an algorithm that an adversary can use for launching a location inference attack against PUs. Finally, we introduce two types of adversaries and compare their performances in inferring the locations of PUs.

6.4.1 System Model

Database Governance Region

Let us assume that the region served by a GDB is divided into $X \times Y$ identical square grids, each of which is denoted by $g(x, y)$, where $1 \leq x \leq X$ and $1 \leq y \leq Y$ denote the x coordinate and the y coordinate of the grid, respectively. Suppose there are $\mathcal{P}$ PUs and $\mathcal{S}$ SUs in the system. There are C equal-bandwidth channels (say $\mathcal{W}$ MHz each) in the system, and all users (both PUs and SUs) share these channels. PUs have primary access to the channels whereas SUs can use them only if the GDB determines that they do not cause harmful interference to the PUs. Let us also assume that PUs are stationary—i.e., the movement of each PU is confined to the grid in which it is located. This assumption is valid for stationary PUs (e.g., satellite earth stations, stationary or slow-moving radars, etc), which is the main

focus of this chapter. In cases where PUs are mobile (e.g., vehicle-mounted military radar systems, tactical military communications systems, etc.), the problem of location inference becomes a particle tracking problem [244], and we discuss it in Section 6.6.

Transmit Power Allocation

The GDB implements a transmit-power allocation (TPA) function for computing the maximum allowable transmit power, P_{ts}, that a SU can transmit at its location without causing harmful interference to a co-channel PU. In practice, the TPA function is dictated by a regulatory agency, such as the FCC or the NTIA, which uses information such as propagation path-loss between the querying SU and the nearest co-channel PU, P_L, transmission spectral mask of SU, terrain information, antenna attributes, PU's interference protection criteria, etc., to compute P_{ts}. Nevertheless, in simple terms, P_{ts} depends on the interference tolerance threshold of the PU and P_L. Therefore, although the attack model described here is applicable to any TPA function in general, in this chapter, we assume that for a given interference tolerance threshold of the PU, the TPA function is a function of P_L and denote it as $h(P_L)$ for simplicity.

Database Access Protocol

The WinnForum's Spectrum Sharing Committee—which has been charged for defining the OPSEC requirements for spectrum sharing in the 3.5 GHz band—has recently finalized the rules/protocol for spectrum access in the CBRS band (the 3.5 GHz band) [245]. According to the WinnForum's protocol, a CBSD first authenticates itself to the SAS, and then submits a spectrum inquiry by specifying a list of supported frequency bands/channels. The SAS responds to the inquiry with spectrum availability information on each of the channels specified in the spectrum inquiry.

Adhering to the standards, we consider a GDB query protocol in which a SU sends a spectrum

query, $Q = (\text{ID}, \text{loc}, A, \mathbf{ch})$, to the database, where:

- ID is the querying SU's unique identifier,
- $\text{loc} \in g(x, y)$ denotes its location coordinates,
- A denotes its antenna attribute information, and
- **ch** denotes the list of channels ch_i, $i \in \{1 \dots K\}$ where $K \leq C$ denotes the total number of channels specified in the query. The SU seeks spectrum availability information in all **ch** channels at its location.

The GDB uses ID to authenticate each user before granting spectrum access. If the SU meets all regulatory requirements, the GDB checks, for each channel ch_i, whether ch_i can be used by the querying SU at loc while protecting the PUs from SU-generated interference. Then, the GDB sends a query response, $\boldsymbol{R}$ where each element of $\boldsymbol{R}$ is $R_i = (\text{ch}_i, P_{ts}^{\text{ch}_i}, T_i)$ and $i \in \{1 \dots K\}$. Here, $P_{ts}^{\text{ch}_i}$ and T_i denote the maximum allowed SU transmission power in ch_i, and time duration for which the SU can transmit on ch_i, respectively.

Our prime interest in this chapter is to study the relation between the number of query responses and the information revealed by such responses. To make the subsequent discussion/analysis easy to follow and without the loss of generality, henceforth, we assume that each query inquiry and response contains information pertaining to a single channel. Therefore, the notations **ch**, $\boldsymbol{R}$, $P_{ts}^{\text{ch}_i}$ and T_i can be simplified as ch, R, P_{ts}^{ch} and T respectively. Note that our subsequent analysis is applicable as it is even in cases where a query inquiry/response consists of information pertaining to multiple channels. In particular, the same inference principle can be applied to infer the locations of PUs in each channel and the same obfuscation strategy is applicable to obfuscate PUs' locations in each channel.

In practice, TPA functions are complex as they need to consider the combined effect of aggregate interference, receiver sensitivity, effective isotropic radiated power, etc. in protecting PUs from SU-induced interference as well as in maximizing spectrum utilization opportuni-

ties for SU. In this chapter, we assume that the GDB uses the following TPA function (see Equation (6.2)) to allocate transmit power to the querying SU in channel ch. This threshold-based TPA function considers path loss (between the PU and the SU) and PU's interference tolerance threshold as primary constraints for calculating the maximum allowable transmit power at the SU location. In the absence of a standardized TPA function for the 3.5 GHz band, our motivation for using the threshold-based TPA is based on the FCC rules defined for the TV band [246]. Finally, it is noteworthy that despite this choice of TPA function in our analysis, the discussions and results are equally applicable to systems that use any TPA function in general.

$$P_{ts}^{\text{ch}} = h(P_L) = \begin{cases} 0, & P_L \leq P_{th1} \\ P_1, & P_{th1} < P_L \leq P_{th2} \\ P_2, & P_L > P_{th2}, \end{cases} \tag{6.2}$$

where, P_{th1} and P_{th2} denote minimum required path loss between the querying SU and the nearest co-channel PU for allocating transmit powers P_1 and P_2, respectively. Clearly, $P_{th1} < P_{th2}$ and $P_1 < P_2$.

6.4.2 Adversary Model

We consider an adversary model in which the attacker has deterministic knowledge of $h(P_L)$ as well as the propagation model used by the GDB to compute P_L. The attacker may either be i) a single mobile SU that can move throughout the region serviced by the GDB, send queries and collect responses from the database, or ii) a group of colluding SUs in the region. In our attack model, these two cases are equivalent. Throughout this chapter, we shall use the term "adversary" to refer to both cases.

The adversary may have some prior incomplete information regarding PUs' locations (e.g., by hacking some of the ESC nodes or by obtaining information from previous spectrum

occupancy data), and it tries to update this prior belief by observing query responses. Here, the attacker is *honest-but-curious*, i.e., the attacker comprises of legitimate SUs that make honest queries to the GDB (does not send false loc and ID) and collects responses (does not violate the transmission rules specified in the response), but uses them to infer PUs' locations. In such a setting, the leakage of PUs' location information is inherent because the database uses such information to provide responses to queries.

6.4.3 Inference Algorithm

Here, we present the location inference attack as Algorithm 3. The algorithm uses a series of database query responses—which by themselves do not directly reveal PUs' locations—to infer the PUs' locations. Note that, as specified in references [226] and [222], the problem of inferring PUs' locations given a set of observations (query responses) is a pure instance of *Bayesian inference*. The adversary has incomplete information about PU's true location, and it continuously updates its hypothesis about this location based on observations in the form of query responses. In other words, the adversary observes the spectrum query response provided by the database, it knows the TPA function and the database's obfuscation strategy, and it has a prior incomplete information about PUs' locations. Using this information, the adversary implements Bayesian inference strategy for computing its posterior belief, and hence, infer PUs' locations.

Let us define a Bernoulli random variable, $\mathcal{B}_{xy}^{(\text{ch})}$, that is equal to 1 if a PU is active on channel ch in grid $g(x, y)$, and is 0 otherwise. Let $P(\mathcal{B}_{xy}^{(\text{ch})} = 1) = p_{xy}^{(\text{ch})}$ and $P(\mathcal{B}_{ij}^{(\text{ch})} = 0) = 1 - p_{xy}^{(\text{ch})}$, where $P(.)$ denotes the probability of an event. The adversary begins the inference attack by initializing the values of $p_{xy}^{(\text{ch})}$ for all x, y, and ch based on its side information. For instance, if we assume the attacker believes that there is at least one PU operating on each channel in the GDB service area—i.e,. in each channel, there is at least one PU in one of the $X \times Y$ equal-area grids, it initializes $p_{xy}^{(\text{ch})} = \frac{1}{XY}$ for all values of x, y, and ch. Then, after receiving each query response, the attacker updates $p_{xy}^{(\text{ch})}$ which reflects its inference about

the locations of PUs in each channel. Based on the TPA function considered in this study (see Equation (6.2)), there are three possible update scenarios.

- Case 1: $R = (\text{ch}, P_{ts}^{\text{ch}} = P_2, T)$. $P_{ts}^{\text{ch}} = P_2$ indicates that there is no PU operating on channel ch in any grids that have path loss values less-than-or-equal-to P_{th2} from the query location. However, this reply does not reveal any information about the presence/absence of PUs in other grids. The attacker sets $p_{xy}^{(\text{ch})} = 0$ for all grids that have path loss values smaller-than-or-equal-to P_{th2} from loc, but it does not alter $p_{xy}^{(\text{ch})}$ values for other grids and for other channels.

- Case 2: $R = (\text{ch}, P_{ts}^{\text{ch}} = P_1, T)$. $P_{ts}^{\text{ch}} = P_1$ indicates that there is no PU operating on channel ch in any grid that has a path loss value smaller-than-or-equal-to P_{th1} from loc. It also implies that there is at least one PU operating on channel ch in grids that have path loss values between P_{th1} and P_{th2} from loc. In this case, the database sets $p_{xy}^{(\text{ch})} = 0$ for all grids that have path loss values less-than-or-equal-to P_{th1} from loc. The update mechanism for $p_{xy}^{(\text{ch})}$, for grids that have path loss values between P_{th1} and P_{th2} from loc, is described below.

  Let us define *p-grids* as the grids where a PU is likely to be present (as inferred from the database response). In this case, p-grids for channel ch are the grids that have path loss values between P_{th1} and P_{th2} from loc and have $p_{xy}^{(\text{ch})} \neq 0$. The attacker updates $p_{xy}^{(\text{ch})}$ for each p-grid using the Bayes' rule. Suppose G denotes the number of p-grids, event H represents the hypothesis of the existence of a PU in a p-grid, and event O denotes the attacker's observation (extracted from the database's response) that there is a PU in grid $g(x, y)$ or one of the other $G-1$ p-grids. If event H^c denotes the absence of a PU in $g(x, y)$, then the probability of observing the same p-grids, $P(O|H^c)$, is $\frac{G-1}{G}$ (existence of a PU in one of the other $G-1$ p-grids). The Bayes rule indicates that:

$$\begin{aligned} P(H|O) &= \frac{P(O|H)P(H)}{P(O|H)P(H) + P(O|H^c)P(H^c)} \\ &= \frac{1 \times p_{xy}^{(\text{ch})}}{1 \times p_{xy}^{(\text{ch})} + \frac{G-1}{G} \times (1 - p_{xy}^{(\text{ch})})} \\ &= \frac{p_{xy}^{(\text{ch})}}{1 - \frac{1}{G}(1 - p_{xy}^{(\text{ch})})}. \end{aligned} \tag{6.3}$$

Therefore, for all the p-grids for channel ch, the attacker uses Equation (6.3) to compute $P(H|O)$ and updates $p_{xy}^{(\text{ch})}$ to $P(H|O)$.

Note that when G is a large value, $p_{xy}^{(\text{ch})}$ does not change significantly, but for small values of G, $p_{xy}^{(\text{ch})}$ escalates quickly. In the extreme case when $G = 1$, $p_{xy}^{(\text{ch})} = 1$.

- Case 3: $R = (\text{ch}, P_{ts}^{\text{ch}} = 0, T)$. $P_{ts}^{\text{ch}} = 0$ implies that there is at least one PU operating on channel ch in grids that have path loss values smaller-than-or-equal-to P_{th1} from loc. Therefore, the attacker uses Equation (6.3) to update inference probabilities for all grids that have path loss values smaller-than-or-equal-to P_{th1} from loc on channel ch. Note that, in this case, p-grids denote the grids that have path loss values less-than-or-equal-to P_{th1} from loc on channel ch.

The adversary (recall that this also denotes a group of colluding adversaries) makes multiple queries, say N queries, to the database from different grids and updates $p_{xy}^{(\text{ch})}$ after receiving each query response. The updated $p_{xy}^{(\text{ch})}$ values represent the result of the location inference attack.

In Figure 6.1, we demonstrate the performance of Algorithm 3 in inferring PUs' locations when the adversary is *random*. We define *random adversary* as the one that sends multiple queries to the database from randomly chosen locations—i.e., for each query, it randomly chooses one among all the grids. As expected, the incorrectness of the attacker's inference decreases monotonically with the increase in number of database responses. Each query response reveals some information about co-channel PUs' location, and hence the result.

Algorithm 3 Location Inference Attack

Require: Sequence of queries $\boldsymbol{\mathcal{Q}} = \{Q_1, Q_2, \cdots, Q_N\}$ and their corresponding responses $\boldsymbol{\mathcal{R}} = \{R_1, R_2, \cdots, R_N\}$.

Ensure: Updated inference probabilities, $p_{xy}^{(\text{ch})}$, for all x, y and ch.

1: Initialize $p_{xy}^{(\text{ch})}$ for all x, y and ch.
2: **for** $i = 1, \ldots, N$, **do**
3: Send query Q_i to the database.
4: Receive database response, R_i.
5: **if** $R_i = (\text{ch}, P_{ts}^{\text{ch}} = P_2, T)$ **then**
6: Set $p_{xy}^{(\text{ch})} = 0$ for all $g(x, y)$ that have path loss values less-than-or-equal-to P_{th2} from loc.
7: **else if** $R_i = (\text{ch}, P_{ts}^{\text{ch}} = P_1, T)$ **then**
8: Set $p_{xy}^{(\text{ch})} = 0$ for all $g(x, y)$ that have path loss values less-than-or-equal-to P_{th1} from loc.
9: Update $p_{xy}^{(\text{ch})}$ for all p-grids for channel ch using Equation (6.3).
10: **else if** $R_i = (\text{ch}, P_{ts}^{\text{ch}} = 0, T)$ **then**
11: Update $p_{xy}^{(\text{ch})}$ for all $g(x, y)$ for channel ch that have path loss values less than or equal to P_{th1} from loc using Equation (6.3)
12: **end if**
13: **end for**

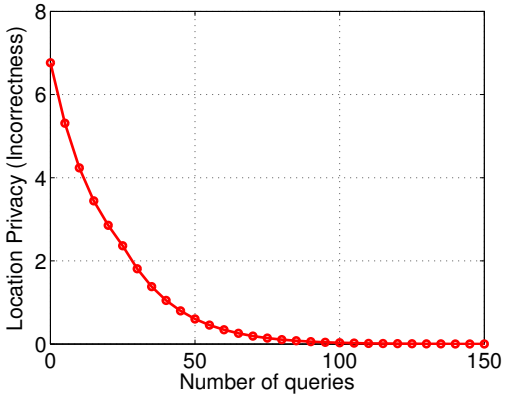


Figure 6.1: Performance of the location inference attack when the attacker makes queries from randomly chosen grids.

6.4.4 Strategic Adversary

In practice, an adversary will likely try to maximize the efficacy of a location inference attack by choosing the query locations strategically. We refer to such an adversary as a *strategic adversary*. In particular, a strategic adversary chooses the query locations optimally, and hence, ensures that the useful information contained in the database response is maximized. This minimizes the PUs' location privacy (incorrectness in our case). In this subsection, we describe how a strategic adversary chooses the next query location to achieve the aforementioned objective. If a strategic adversary pursues to threaten the location privacy of PUs in a particular channel, it sends multiple spectrum inquiries for that channel from optimally chosen query locations and collects corresponding responses to facilitate the inference.

In Section 6.5, we will provide details regarding the GDB's optimal location-privacy preserving strategy. We will learn that the GDB preserves the PUs' location privacy by replying to an SU's query with an obfuscated response, R', instead of the actual response, R. This implies that the actual response will be hidden from the querying SU. In such scenario, given a query location, loc, the adversary can calculate the conditional expected incorrectness for an arbitrary obfuscated response, R', and an arbitrary PU's location, $\mathrm{PU}_{\mathrm{loc}}$, as follows:

$$\mathbf{E}[\mathrm{IC}|\mathrm{loc}, R', \mathrm{PU}_{\mathrm{loc}}] = \mathrm{IC}\left(\boldsymbol{\mathcal{I}}, \mathrm{PU}_{\mathrm{loc}}\right),$$

where $\mathbf{E}[.]$ denotes an expectation operator; $\boldsymbol{\mathcal{I}} = u(\boldsymbol{\mathcal{I}}^{(-1)}, R')$ is an inference matrix that represents the updated inference probabilities, $p_{xy}^{(\mathrm{ch})}$, after observing R'; and $u(\boldsymbol{\mathcal{I}}^{(-1)}, R')$ is a function that updates the previous inference matrix, $\boldsymbol{\mathcal{I}}^{(-1)}$, to $\boldsymbol{\mathcal{I}}$ after observing R' using the location inference algorithm described in Algorithm 3.

For a query made from loc, let $P(R'|\mathrm{loc})$ denote the probability that the querying SU observes R' as the GDB's response. Also, let $P\left(\mathrm{PU}_{\mathrm{loc}}\right)$ denote the attacker's belief about the location of PU at grid $\mathrm{PU}_{\mathrm{loc}}$. For an adversary, $P\left(\mathrm{PU}_{\mathrm{loc}}\right)$ corresponds to the updated inference probabilities after observing the most recent query response.

Similar to the design of any state-of-the-art privacy-preserving mechanisms, we assume that an adversary has knowledge of the GDB's location-privacy preserving strategy, but not the input parameters. The GDB's strategy will be discussed in detail in Section 6.5. Using the GDB's optimal strategy, the adversary can compute $\mathcal{F}^* = \{f^*(R'|R)|\boldsymbol{\mathcal{I}}^{(-1)}, \forall R' \in \mathcal{R}\}$ for each possible loc. Here, the notation $\mathcal{R}$ represents the set of all possible obfuscated responses for a given R, and $\mathcal{F}^*$ denotes the optimal obfuscation strategy, which represents a set of obfuscation probabilities. Each element of $\mathcal{F}^*$—i.e., $f^*(R'|R)$—denotes the probability that the actual response R is replaced with an obfuscated response R'. Provided this, the expected incorrectness for a given loc and an arbitrary R can be written as,

$$\mathbf{E}[\text{IC}|\text{loc}, R] = \sum_{R'} \left(f^*(R'|R) \sum_{\text{PU}_{\text{loc}}} P\left(\text{PU}_{\text{loc}}\right) \text{IC}\left(\boldsymbol{\mathcal{I}}, \text{PU}_{\text{loc}}\right) \right).$$

Recall that the database hides the actual response R from the adversary. This forces the adversary to compute the expectation of incorrectness over all possible R. Also, as we shall learn later in Section 6.5, the term $f^*(R'|R)$ (and hence $\mathbf{E}[\text{IC}|\text{loc}, R]$) is conditional on $\mathcal{C}_{\max}$, a parameter used by the database to control the obfuscation level. This tunable parameter is independent of the query location loc and is hidden from the adversary, which forces the latter to compute the expectation of incorrectness over all possible $\mathcal{C}_{\max}$ values. Therefore, the adversary computes the expected incorrectness for a given loc as follows,

$$\mathbf{E}[\text{IC}|\text{loc}] = \sum_{R} \left\{ P(R|\text{loc}) \sum_{\mathcal{C}_{\max}} P(\mathcal{C}_{\max}) \mathbf{E}[\text{IC}|\text{loc}, R] \right\}. \tag{6.4}$$

where, $P(\mathcal{C}_{\max})$ denotes the probability with which the attacker believes that the database uses $\mathcal{C}_{\max}$ as the obfuscation parameter. Since the adversary in general does not know the value of $\mathcal{C}_{\max}$ used by the database, it may assume a uniform distribution over all possible $\mathcal{C}_{\max}$ values and set $P(\mathcal{C}_{\max})$ accordingly.

For a strategic adversary, the query location that minimizes the location privacy of PUs is the one that minimizes $\mathbf{E}[\text{IC}|\text{loc}]$. Therefore, the adversary solves Equation (6.5) to find the

$$
\begin{aligned}
\mathrm{loc}^* &= \underset{\mathrm{loc}}{\operatorname{argmin}}\, \mathbf{E}[\mathrm{IC}|\mathrm{loc}] \\
&= \underset{\mathrm{loc}}{\operatorname{argmin}} \sum_{R} \left(P(R|\mathrm{loc}) \sum_{\mathcal{C}_{\max}} P(\mathcal{C}_{\max}) \mathbf{E}[\mathrm{IC}|\mathrm{loc}, R] \right) \\
&= \underset{\mathrm{loc}}{\operatorname{argmin}} \sum_{R} \left[P(R|\mathrm{loc}) \sum_{\mathcal{C}_{\max}} \left\{ P(\mathcal{C}_{\max}) \sum_{R'} \left(f^*(R'|R) \sum_{\mathrm{PU}_{\mathrm{loc}}} P\left(\mathrm{PU}_{\mathrm{loc}}\right) \mathrm{IC}\left(\boldsymbol{\mathcal{I}}, \mathrm{PU}_{\mathrm{loc}}\right) \right) \right\} \right] \\
&\quad . \qquad (6.5)
\end{aligned}
$$

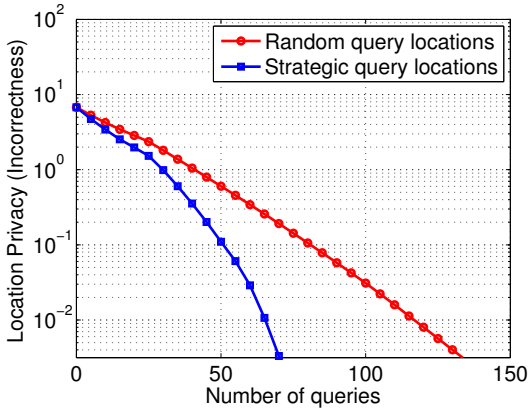


Figure 6.2: Location-inference results of a random adversary versus a strategic adversary.

optimal query location, loc^*, in each iteration of Algorithm 3. Note that, for a collusion attack, i.e., an attacker representing a group of malicious SUs, the solution of Equation (6.5) can be used to select the SU whose query response (database response to the query made from this SU's location) yields maximum information about PUs' locations.

In Figure 6.2, we compare the performance of the strategic adversary against the random adversary. Clearly, the former outperforms the latter. The strategic adversary is able to reduce the incorrectness of its inference in very few queries as compared to the random adversary, making the location-inference-attack more efficient.

6.5 Optimal Location-Privacy Preserving Strategy

6.5.1 Perturbation based Obfuscation

The perturbation based obfuscation method (a.k.a. random obfuscation method) is a technique for privacy-preserving databases that uses data distortion in order to mask the attribute values of records. In this method, sufficiently large noise is added to the database contents for preventing the recovery of these values by an adversary. Alternatively, noise can also be added to the database responses. One key advantage of perturbation is that it is relatively simple, and it does not require knowledge of the distribution of other records in the data. Perhaps, the most basic perturbation methods used in privacy-preserving databases is the *additive noise*, which is why we use it as a basis for designing our proposed location-privacy preserving scheme. Moreover, perturbation-with-noise can be considered as a generalization of several other obfuscation techniques, such as enlarging the protected contours [223, 14], adding dummy PUs [222, 233], etc., that have been extensively studied in the literature. In this method, the database replaces the original response, R, with a response $R' = R + \eta$ where η is the additive noise. Since the querier (adversary) observes R' instead of R and makes inference based on it, this scheme improves the privacy of the database contents (in our case, PUs' locations). Note that obfuscating database responses is equivalent to obfuscating PUs' locations.

6.5.2 Trade-off between Privacy and Spectrum Utilization

The perturbation-based obfuscation scheme can be implemented in privacy-preserving spectrum databases as follows. The original response, $R = (\text{ch}, P_{ts}^{\text{ch}}, T)$, is modified to $R' = (\text{ch}, P_{ts}^{\text{ch}'}, T)$, where $P_{ts}^{\text{ch}'} = P_{ts}^{\text{ch}} + \epsilon$ and ϵ is a non-positive random noise. Here, P_{ts}^{ch} is the actual available transmit power in channel ch at the query location (computed using Equation (6.2)), and it is replaced by the perturbed transmit power, $P_{ts}^{\text{ch}'}$, for generating the obfus-

cated response. Since $\epsilon \leq 0$, $P_{ts}^{\text{ch}'} \leq P_{ts}^{\text{ch}}$. This is desired because, otherwise, $P_{ts}^{\text{ch}'} > P_{ts}^{\text{ch}}$ (i.e., allowing a SU to transmit with a power higher than the actual allowed maximum transmit power) will likely result in harmful interference to the PUs. Intuitively, adding a non-positive ϵ to P_{ts}^{ch} is equivalent to enlarging the protection contour of the PU.

Suppose that a SU in each grid is a network (e.g., a Long Term Evolution (LTE) network) consisting of a single transmitter/eNodeB/access point and multiple (say N_{UE}) receivers/user equipments (UEs). Also assume that the SU network uses the available shared channel as a supplemental downlink channel. When the SU transmitter uses a transmit power of P_{ts}^{ch} Watts, the SU network's downlink capacity, $C_{\text{su}}^{\text{ch}}$, in bits per second (bps)—which is a metric we use to quantify the SU network's spectrum utilization efficiency—is given by the Shannon's channel capacity theorem:

$$\begin{aligned} C_{\text{su}}^{\text{ch}} &= \mathcal{W} \sum_{i=1}^{N_{\text{UE}}} \zeta_i \log_2(1 + \text{SINR}_i) \\ &= \mathcal{W} \sum_{i=1}^{N_{\text{UE}}} \zeta_i \log_2 \left(1 + \frac{\lambda_i P_{ts}^{\text{ch}}}{I_{\text{ch}_i}}\right), \end{aligned} \tag{6.6}$$

where ζ_i denotes the fraction of time spent for transmissions to the i^{th} SU receiver, $\text{SINR}_i = \frac{\lambda_i P_{ts}^{\text{ch}}}{I_{\text{ch}_i}}$ denotes the signal to noise and interference ratio in the link between the SU transmitter and the i^{th} SU receiver, λ_i denotes the attenuation-factor due to signal propagation from the SU transmitter to the i^{th} SU receiver, and I_{ch_i} represents the aggregate interference and noise in the link.

Similarly, for an obfuscated response (P_{ts}^{ch} replaced by $P_{ts}^{\text{ch}'}$), the SU network's downlink capacity, $C_{\text{su}}^{\text{ch}'}$, is given by

$$C_{\text{su}}^{\text{ch}'} = \mathcal{W} \sum_{i=1}^{N_{\text{UE}}} \zeta_i \log_2 \left(1 + \frac{\lambda_i P_{ts}^{\text{ch}'}}{I_{\text{ch}_i}}\right). \tag{6.7}$$

In our model, we assume that the database response dictates the maximum transmit power

of the SU transmitter, but not of the SU UEs (because our assumption is that the shared channel is used for downlink transmissions only and that there exists a dedicated channel for uplink transmissions). Hence, for a given set of λ_i and I_{ch_i}, the total loss in SU network capacity due to the obfuscated response from the database is,

$$\begin{aligned}\Delta C_{\mathrm{su}}^{\mathrm{ch}} &= C_{\mathrm{su}}^{\mathrm{ch}} - C_{\mathrm{su}}^{\mathrm{ch}'} \\ &= \mathcal{W}\sum_{i=1}^{N_{\mathrm{UE}}} \zeta_i \left\{ \log_2\left(1+\frac{\lambda_i P_{ts}^{\mathrm{ch}}}{I_{\mathrm{ch}_i}}\right) - \log_2\left(1+\frac{\lambda_i P_{ts}^{\mathrm{ch}'}}{I_{\mathrm{ch}_i}}\right)\right\} \\ &= \mathcal{W}\sum_{i=1}^{N_{\mathrm{UE}}} \zeta_i \log_2\left(\frac{I_{\mathrm{ch}_i}+\lambda_i P_{ts}^{\mathrm{ch}}}{I_{\mathrm{ch}_i}+\lambda_i P_{ts}^{\mathrm{ch}'}}\right).\end{aligned} \tag{6.8}$$

Since $P_{ts}^{\mathrm{ch}'} \leq P_{ts}^{\mathrm{ch}}$ and $\Delta C_{\mathrm{su}}^{\mathrm{ch}} \geq 0$, a SU network experiences a non-negative loss in downlink capacity due to obfuscation. A greater amount of obfuscation (i.e., adding more noise to responses) results in improved location privacy, but at the same time, the difference between P_{ts}^{ch} and $P_{ts}^{\mathrm{ch}'}$ becomes larger. This results in larger $\Delta C_{\mathrm{su}}^{\mathrm{ch}}$, which implies lower spectrum utilization efficiency (measured in bps). On the other hand, less obfuscation results in reduced location privacy but offers improved spectrum utilization efficiency. Clearly, *there is an inherent trade-off between the PUs' location privacy and the SUs' spectrum utilization efficiency.*

6.5.3 Optimal Obfuscation Strategy

An ideal obfuscation strategy is the one that applies maximum obfuscation if the query is originated from an adversary and applies no obfuscation otherwise. However, in an insider-attack model, such as the case-in-hand, it is often difficult, if not impossible, to deterministically identify the adversary just by observing a single query. Therefore, in order to protect the location privacy of PUs, the database should either obfuscate every query response, or it should learn the nature of queries and only obfuscate those responses that are more likely to reveal more information about PUs' locations. Here, we define an optimal obfuscation

strategy as a strategy that maximizes PUs' location privacy while ensuring that the loss in spectrum utilization, caused due to obfuscated responses, is less than a threshold.

Similar to the design of any other privacy-preserving system, we assume that the privacy-preserving entity (i.e., the database) does not know the attacker's exact inference strategy but knows its best possible strategy (Bayesian inference in the case of database inference attacks). However, regardless of the strategy used by the adversary, the database is able to keep track of the information revealed through its query responses. For example, if the database responded to a previous query with transmit power P_2 in channel ch, it knows that the querying entity has knowledge of the absence of PUs in grids that have path loss less-than-or-equal-to P_{th1} from the query location. Consequently, the database leverages this information, along with the current query location, to compute the best obfuscation strategy for generating the current response. Note that while the database is able to thwart any inference that is inferred directly from the query responses, it cannot prevent the inference resulting from other sources. For example, an adversary may have sensing capabilities, in which case it can perform sensing operations to infer the locations of PUs. However, in general, the database is unaware of the attacker's resources/capabilities and side information, and it is often difficult to counter the adversary's inference in such cases. Moreover, when the adversary infers PUs' locations using other sources, such inference attack is not an instance of a purely database-inference attack, and hence, such attacks are out of the scope of this chapter.

On the other hand, we assume that an adversary has knowledge of the database's optimal obfuscation strategy. In such scenario, it is possible for the adversary to reverse engineer and nullify the effect of obfuscation if the database uses a deterministic obfuscation. Therefore, a probabilistic obfuscation scheme that adds uncertainty to the adversary's inference even when the adversary knows the database's obfuscation strategy is desired. Henceforth, we seek to compute a probability distribution function that can be used to optimally obfuscate the database response such that doing so maximizes the PUs' location privacy on average, under the SUs' constraints regarding spectrum utilization efficiency.

Let $\mathcal{F} = \{f(R'|R)|\boldsymbol{\mathcal{I}}^{(-1)}, \forall R' \in \mathcal{R}\}$ denote an arbitrary obfuscation strategy, where $\mathcal{R}$ denotes the set of all possible obfuscated responses, R', when the actual response is R. Given the information revealed until the beginning of current query, $\mathcal{F}$ represents a set of probabilities where each entry, $f(R'|R)$, denotes the probability of obfuscating R with R'. Recall that R' is generated by replacing P_{ts}^{ch} with $P_{ts}^{\text{ch}'}$ such that $P_{ts}^{\text{ch}'} \leq P_{ts}^{\text{ch}}$. Assuming finite discrete values of $P_{ts}^{\text{ch}'}$, specifically, $P_{ts}^{\text{ch}'} \in \{0,\ P_1,\ P_2\}$, $\mathcal{F}$ represents an obfuscation strategy that satisfies the following equation:

$$\sum_{R'} f(R'|R) = 1, \quad \forall R. \tag{6.9}$$

The expected location privacy, a.k.a. incorrectness, achieved by $\mathcal{F}$ is

$$\mathbf{E}[\text{IC}|\,\mathcal{F}] = \sum_{R'} f(R'|R)\text{IC}\left(\boldsymbol{\mathcal{I}}, \text{PU}_{\text{loc}}\right),$$

where $\boldsymbol{\mathcal{I}} = u(\boldsymbol{\mathcal{I}}^{(-1)}, R')$ is an updated inference matrix that represents the information regarding PUs' locations that is revealed by the database through query responses, including the current response R'. The notation $u(\boldsymbol{\mathcal{I}}^{(-1)}, R')$ denotes a function that updates the inference matrix, $\boldsymbol{\mathcal{I}}^{(-1)}$, to $\boldsymbol{\mathcal{I}}$ after observing R' using the Bayesian inference algorithm discussed in Section 6.4.

While the main goal of the optimal obfuscation strategy is to maximize $\mathbf{E}[\text{IC}|\mathcal{F}]$, its secondary goal is to minimize the adverse effect of obfuscation on spectrum utilization. Therefore, in the optimization problem formulation of the optimal obfuscation strategy, the objective function, $\mathcal{O}$, is to maximize:

$$\begin{aligned}\mathcal{O} &= \mathbf{E}\big[(\alpha\text{IC} - \beta\Delta C_{su}^{\text{ch}})|\mathcal{F}\big] \\ &= \sum_{R'} \{\alpha f(R'|R)\text{IC}\left(\boldsymbol{\mathcal{I}}, \text{PU}_{\text{loc}}\right)\} - \beta\mathcal{W}\sum_{R'}\left\{f(R'|R)\sum_{i=1}^{N_{\text{UE}}}\zeta_i\log_2\left(\frac{I_{\text{ch}_i} + \lambda_i P_{ts}^{\text{ch}}}{I_{\text{ch}_i} + \lambda_i P_{ts}^{\text{ch}'}}\right)\right\},\end{aligned} \tag{6.10}$$

where, the weights α and β correspond to the relative importance of location privacy and spectrum utilization respectively. For example, if a regulator wants to prioritize location privacy over spectrum utilization, then it would choose $\alpha > \beta$.

As discussed before in Section 6.5.2, the performance of perturbation-based obfuscation strategy is directly proportional to the amount of noise added in the query response. Unfortunately, more noise corresponds to less spectrum utilization. Let us assume that the maximum tolerable expected loss in a SU's link capacity per query is $\mathcal{C}_{\max}$. This forces the database to constrain the amount of noise that can be added in each query response. Mathematically, this constraint can be expressed as,

$$\mathbf{E}\big[\Delta C_{su}^{\mathrm{ch}} | \mathcal{F}\big] \leq \mathcal{C}_{\max}$$

$$\text{i.e.,} \mathcal{W} \sum_{R'} \left\{ f(R'|R) \sum_{i=1}^{N_{\mathrm{UE}}} \zeta_i \log_2 \left(\frac{I_{\mathrm{ch}_i} + \lambda_i P_{ts}^{\mathrm{ch}}}{I_{\mathrm{ch}_i} + \lambda_i P_{ts}^{\mathrm{ch}'}} \right) \right\} \leq \mathcal{C}_{\max} \tag{6.11}$$

Combining Equations (6.9), (6.10), and (6.11), the database formulates the optimization problem specified by Equation (6.12) for finding the optimal obfuscation strategy. This strategy primarily depends on two factors: (i) information revealed by the database until the immediately preceding query response, and (ii) the current query location submitted by the attacker. This strategy works because the actual response R and the obfuscation parameter $\mathcal{C}_{\max}$ are hidden from the adversary. The database injects false positive responses (by replacing R with R') and dilutes the information revealed by the query responses, which, in turn, makes it difficult for the adversary to infer the PUs' locations.

The optimization problem specified in (6.12) is a *linear programming* (LP) problem, and it can be solved by using any of the readily available LP solvers. Note that although we define optimal obfuscation with respect to the incorrectness metric, our problem formulation is equally applicable even when the location privacy is defined in terms of a different metric.

$$\mathcal{F}^* = \underset{\mathcal{F}}{\text{argmax}} \sum_{R'} \left[f(R'|R) \left\{ \alpha \text{IC}\left(\boldsymbol{\mathcal{I}}, \text{PU}_{\text{loc}}\right) - \beta \mathcal{W} \sum_{i=1}^{N_{\text{UE}}} \zeta_i \log_2 \left(\frac{I_{\text{ch}_i} + \lambda_i P_{ts}^{\text{ch}}}{I_{\text{ch}_i} + \lambda_i P_{ts}^{\text{ch}'}} \right) \right\} \right]$$

$$\text{subject to: } \mathcal{W} \sum_{R'} \left\{ f(R'|R) \sum_{i=1}^{N_{\text{UE}}} \zeta_i \log_2 \left(\frac{I_{\text{ch}_i} + \lambda_i P_{ts}^{\text{ch}}}{I_{\text{ch}_i} + \lambda_i P_{ts}^{\text{ch}'}} \right) \right\} \leq \mathcal{C}_{\max}$$

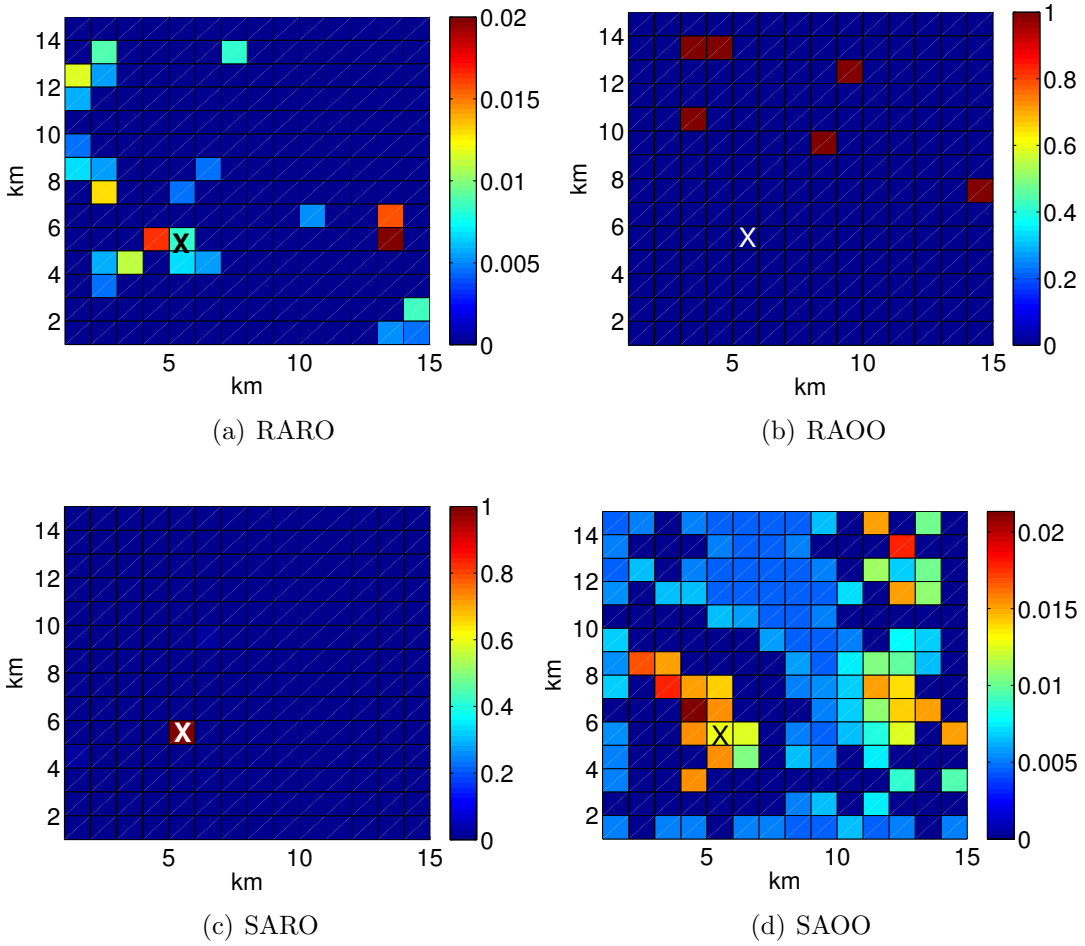
$$\sum_{R'} f(R'|R) = 1 \tag{6.12}$$

6.6 Simulation Results

In this section, we demonstrate the performance of the proposed obfuscation strategy in countering an adversary's location inference attack. The trade-off between PUs' location privacy and loss in SU link capacity due to obfuscation is also analyzed in detail.

Let us define a database governance area as a 15 km by 15 km square area, which is divided into 15 by 15 square grids, each with a side length of 1 km. For simplicity, let us assume that the average radio propagation path loss is only a function of distance between the two wireless nodes. Suppose P_{th1} and P_{th2} correspond to path loss values at a distance of 1 km and 2 km respectively. The channel bandwidth, $\mathcal{W}$, is assumed to be 10 MHz. Also, for simplicity and for abstracting away the details of radio wave propagation and aggregate interference, let us assume, without loss of generality, $N_{\text{UE}} = 1$, $\zeta_1 = 1$, $\frac{\lambda_1}{I_{\text{ch}_1}} = \tau$ (a constant), and set $P_1 = \frac{1}{\tau}$ Watt and $P_2 = \frac{2}{\tau}$ Watt.

An attacker (or a group of colluding attackers) launches a location inference attack by making multiple queries to the database from multiple grids at different time slots. Similar to any insider-attack model, the attacker truthfully reports its location (i.e., the center of the grid in which it is located) and strictly follows the instructions provided in the database response, but it keeps track of all database responses, and uses them to infer the PUs' locations. We study two types of adversaries as discussed in Section 6.4: (i) random attacker (RA), which randomly chooses the query locations, and (ii) strategic attacker (SA), which uses Equation



(a) RARO (b) RAOO

(c) SARO (d) SAOO

Figure 6.3: Inferring the locations of stationary PUs. The actual locations are denoted by 'X'.

(6.5) to find the best query location that minimizes the location privacy of PUs on average.

The database implements obfuscation strategy and responds to each query with either a true response or an obfuscated response. Specifically, we compare two obfuscation strategies: (i) random obfuscation (RO) in which all possible obfuscated responses (this also includes the true response) are chosen with equal probabilities, and (ii) optimal obfuscation (OO) strategy which refers to our proposed scheme, the solution of Equation (6.12). Henceforth, whenever we compare these two strategies, we ensure that the average loss in SUs' spectrum utilization per query response is same in both cases, which justifies a fair comparison between the two.

Based on these attacker and database strategies, we define the following 4 scenarios, and perform a comparative performance analysis.

- Random Attacker, Random Obfuscation (RARO)
- Random Attacker, Optimal Obfuscation (RAOO)
- Strategic Attacker, Random Obfuscation (SARO)
- Strategic Attacker, Optimal Obfuscation (SAOO)

We assume that the strategic attacker has complete knowledge of the database's optimal obfuscation strategy and the range of $\mathcal{C}_{\max}$ values, but it does not know the actual value of $\mathcal{C}_{\max}$ used in the optimal obfuscation. Therefore, the strategic attacker minimizes the expectation of location privacy (i.e., incorrectness) over all possible $\mathcal{C}_{\max}$ values as expressed in Equation (6.5).

In our simulations, the performance of each scenario is computed as the average over 100 simulation runs. Also, we assume that location privacy and spectrum utilization are equally important considerations in spectrum sharing, and hence we set $\alpha = \beta = 1$ in Equation (6.12).

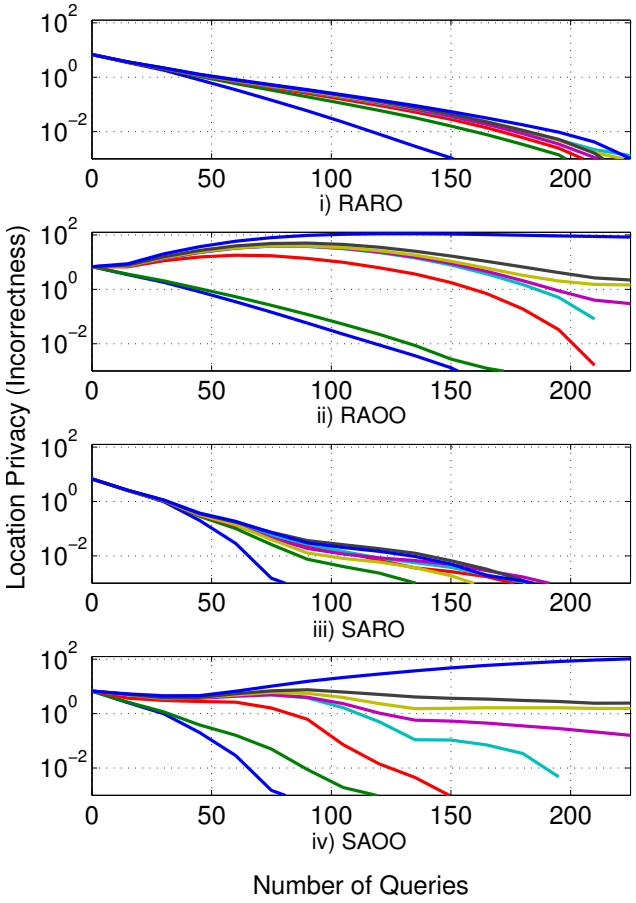


Figure 6.4: Effect of number of queries on location privacy for different attacker-database strategies. Each curve in each subfigure represents different $\mathcal{C}_{\max}$ values, where the bottom-most curve corresponds to the smallest $\mathcal{C}_{\max}$ value and the uppermost curve corresponds to the largest $\mathcal{C}_{\max}$ value.

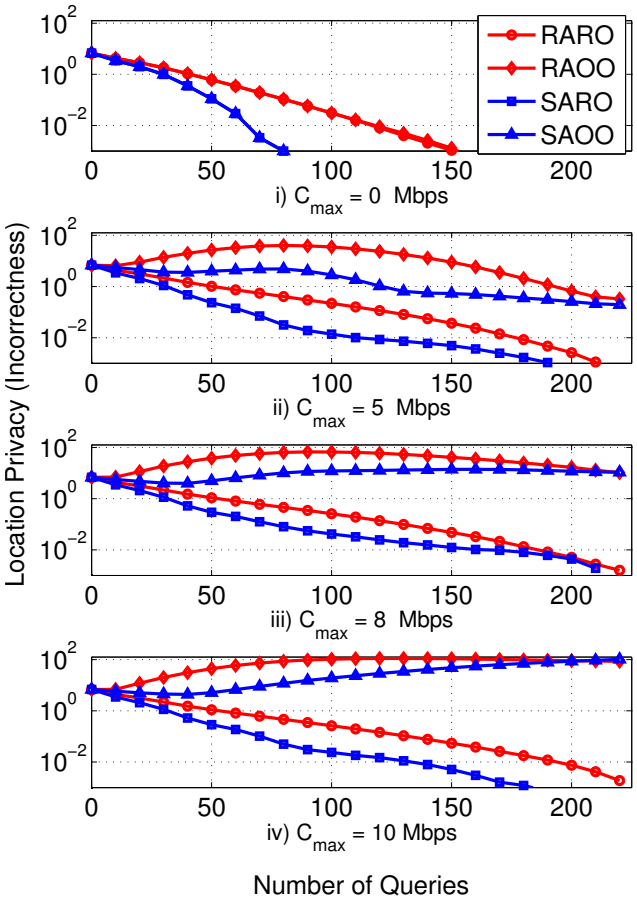


Figure 6.5: Comparative privacy performance with different $\mathcal{C}_{\max}$ values. The legend of the first subfigure applies to all subfigures.

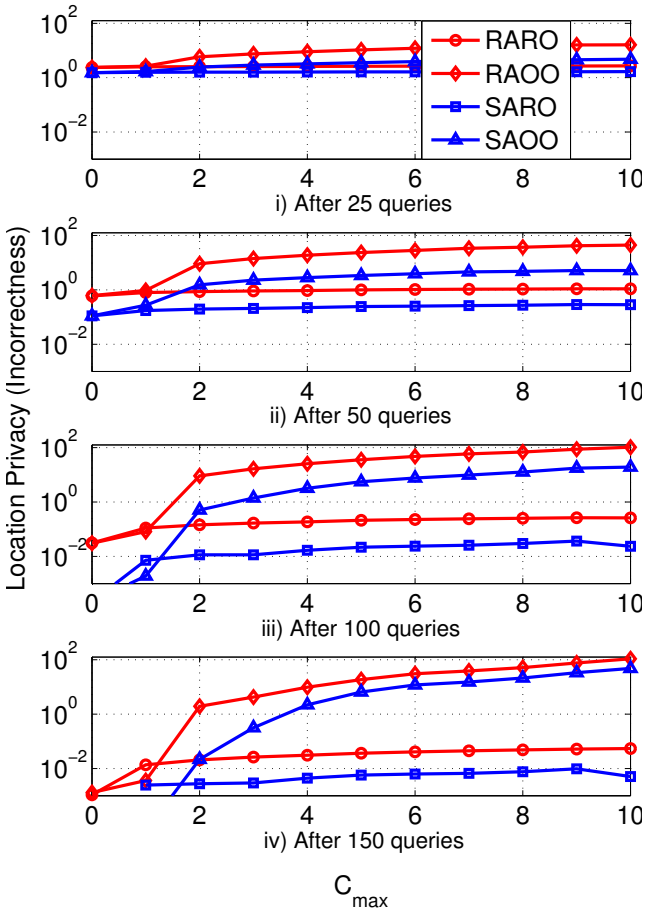


Figure 6.6: Trade-off between location privacy and spectrum utilization. The legend of the first subfigure applies to all subfigures.

6.6.1 Inferring the Locations of Stationary PUs

Here, we demonstrate the performance of an adversary in inferring the locations of stationary PUs. Let us assume that a single stationary PU is located in grid $(5, 5)$. Note that our assumption of a single PU has a purpose: we want to highlight the effectiveness of optimal obfuscation strategy in hiding the true location of the PU. Nevertheless, our simulation results are equally relevant for the case with multiple PUs. In such a case, our results can be interpreted as the average performance for multiple PUs.

In Figure 6.3, we provide visualizations of an adversary's inference after it collects 75 query responses from the database. Here, the color map denotes the adversary's belief about the presence of a PU in a grid. Since we assume that the adversary does not precisely know the total number of PUs present in the map, these plots represent the relative belief (unnormalized probability) but not the probability in a formal sense.

When the adversary uses strategic inference and the database uses the random obfuscation strategy (SARO scenario), the adversary can accurately infer the actual location of the PU (see Figure 6.3(c)). This is because when the noise is generated from the same distribution (recall that the random obfuscation strategy samples responses from a uniform distribution over all possible obfuscated responses), then an adversary can issue multiple queries and calculate the average of the responses to infer the PU's true location. However, when the adversary and the database both use random strategies (RARO scenario), the adversary's inference has large uncertainty regarding the location of the PU. By comparing SARO against RARO, we can observe the effectiveness of the strategic adversary in reducing the uncertainty of the inference.

Interestingly, when the random adversary launches an inference attack against a database that implements optimal obfuscation (RAOO scenario), the database can effectively force the adversary to wrongly infer the locations of PUs with high certainty. Figure 6.3(b) shows the results. Here, the adversary, with high certainty, believes that there are multiple PUs located at several grids, while in fact, there is only a single PU located at grid $(5, 5)$. However, it is

noteworthy that the inferred grids are located far from the grid in which the PU is located. This results in very high location privacy (incorrectness) for the PU. Lastly, Figure 6.3(d) demonstrates the performance of the strategic adversary against the optimal obfuscation strategy (SAOO scenario). Here also, we can see the uncertainty in adversary's inference due to obfuscated responses generated by the database using the optimal obfuscation strategy.

6.6.2 Effect of Number of Queries

Figure 6.4 shows the effect of the number of query responses collected by the attacker on PUs' location privacy. Without obfuscation (the bottom-most curves of all plots in Figure 6.4), location privacy declines sharply as the attacker gets access to increasing number of query responses. This effect is more pronounced when the attacker chooses the query locations optimally using Equation (6.5). The database response for a query performed from an optimally chosen grid provides maximum expected information about the locations of PUs, and hence the result.

Figure 6.4 can also be interpreted in another way. For instance, if our interest is in studying the change in location privacy with respect to time, we can easily do so by dividing the number of queries (the current x-axis) by the average query frequency (i.e., the average number of queries per unit time) such that the new x-axis denotes the time duration. Such study helps in analyzing the time duration for which a desired privacy level can be reliably achieved. We do not provide such plots in this chapter due to space limitations.

Referring to Figure 6.4, as $\mathcal{C}_{\max}$ increases, the false positives in the database responses also increase which results in better location privacy. However, for the random obfuscation strategy (see Figures 6.4 i) and 6.4 iii)), irrespective of the attacker's strategy, increasing $\mathcal{C}_{\max}$ leads to only a slight improvement in location privacy. Since only few randomly chosen responses are obfuscated, the effect of false positive responses is often nullified by unobfuscated responses. Specifically, for SARO (see Figure 6.4 iii)), increasing $\mathcal{C}_{\max}$ does not seem to have much improvement on location privacy because this scenario models a strong attack

(strong/strategic attack but weak/random obfuscation). The gain in location privacy obtained by the obfuscated responses is negligible because the database obfuscates only a few randomly chosen responses whereas the adversary chooses the query locations optimally.

Initially, location privacy is high, say LP_0, when the database does not reveal any information to the attacker (when the attacker does not have access to query responses), and it decreases as the attacker collects more number of responses. Surprisingly, when the database implements optimal obfuscation strategy (see Figures 6.4 ii) and 6.4 iv)) with large $\mathcal{C}_{\max}$, location privacy after a large number of query responses is even higher than LP_0. At first, this result seems counter-intuitive. However, recall that according to incorrectness metric (Equation (6.1)), location privacy is maximum when the adversary confidently, i.e., with high probability, believes that a PU is located in a grid that is far away from PU's true location. In other words, if $\boldsymbol{d}$ represents a vector of d_i, then according to Equation (6.1), IC is maximum when $p_i = 1$ for $d_i = \max(\boldsymbol{d})$ and $p_i = 0$ otherwise. The optimal obfuscation strategy exploits this fact and injects false positives in the database responses optimally. These false positives mislead the attacker into believing that a PU is located very far from its actual location. As a result, the optimal obfuscation strategy provides high location privacy to the PU even after the attacker collects a large number of query responses.

6.6.3 Effect of $\mathcal{C}_{\max}$

In Figure 6.5, we compare the performance of the attacker and database strategies with respect to location privacy for different numbers of query responses and $\mathcal{C}_{\max}$ values. Clearly, the strategic adversary always outperforms the random adversary for all $\mathcal{C}_{\max}$ values, for any database strategy and for any number of query responses. Similarly, the optimal obfuscation strategy outperforms the random obfuscation strategy at all $\mathcal{C}_{\max}$ values. The gap between their performance curves widens as $\mathcal{C}_{\max}$ increases which demonstrates the effectiveness of the optimal obfuscation scheme in injecting false positives in database responses.

6.6.4 Trade-off between PU Privacy and SU Utility

Figure 6.6 illustrates the inherent trade-off between the PUs' location privacy and spectrum utilization efficiency. Specifically, each sub-figure in Figure 6.6 shows the trade-off curves after an attacker collects a specific number of query responses. As expected, the SARO scenario offers the worst trade-off situation as the strategic adversary is still able to make correct inference when the database adopts random obfuscation. On the other hand, the RAOO scenario provides the best trade-off—i.e., even with a small loss in the SUs' link capacity, the gain in location privacy is significantly high because the optimal obfuscation strategy is successful in hiding PUs' true location to the random adversary. Unlike the case with random obfuscation strategy, when the database implements optimal obfuscation strategy, the location privacy increases monotonically with increasing $C_{\max}$ irrespective of adversary's strategy, which demonstrates the effectiveness of the optimal obfuscation scheme in balancing the trade-off between location privacy and spectrum utilization.

6.6.5 Inferring the Trajectory/Path of Mobile PUs

In this subsection, we extend our analysis and illustrate how an adversary can infer the trajectory/path of a mobile PU. Examples of mobile PUs include vehicle-mounted military radar systems, tactical military communications systems, etc. that operate in the shared spectrum. Note that the knowledge of the path of movement of the PU may allow an adversary to infer the origins, intermediate transits and intended destinations of PUs. Therefore, mission-critical PUs require that their trajectories be obfuscated.

Suppose that the region of interest is an area represented by 15×15 grids of square cells, where the side length of each cell is 1 km. Let us assume that a PU is moving within this region. For characterizing the movement of the PU, we assume a random walk mobility model. Using this model, the PU, in each step/time-slot, decides with equal probability to move either to the east, west, north or south. Similarly, the adversary, in each step/time-slot,

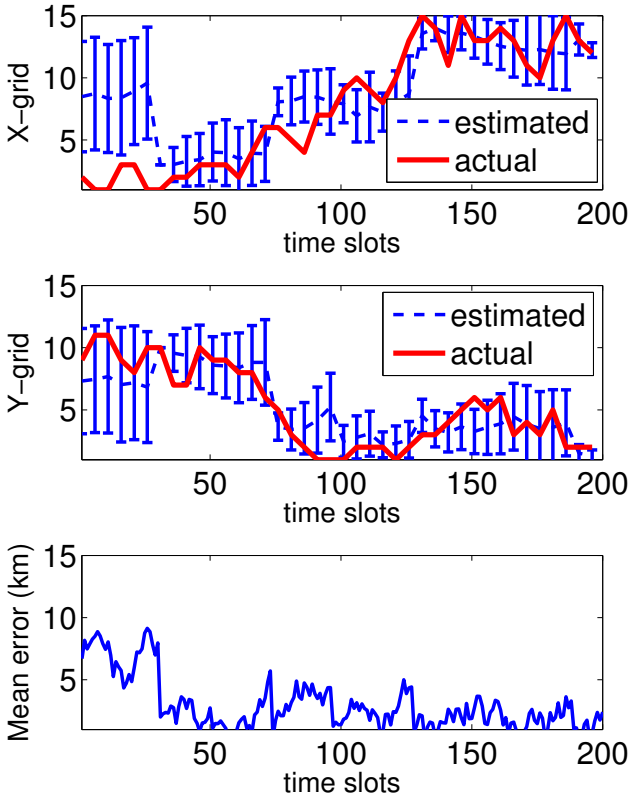


Figure 6.7: Inferring the trajectory/path of a mobile PU. (without obfuscation).

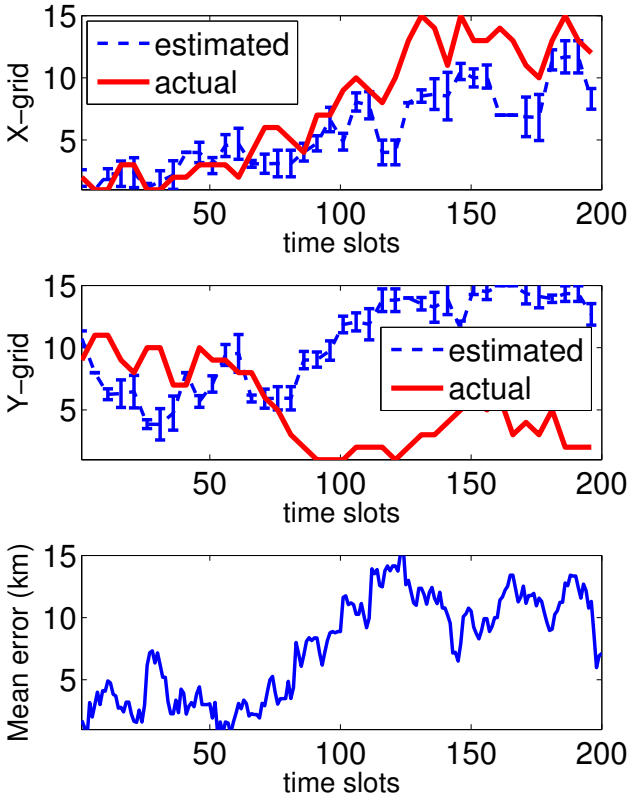


Figure 6.8: Inferring the trajectory/path of a mobile PU. (with obfuscation).

queries the database from a randomly selected grid, observes the database response and uses it to infer the current position of the PU.

For the adversary, we assume that it implements a particle filter for inferring the path of the mobile PU. We will not provide the details of particle filter, but rather, refer the interested readers to [244]. In general, the particle filter algorithm goes through three phases in each time step: i) prediction, ii) update, and iii) resample. In our implementation, the adversary uses database responses to update the particle weights.

Figure 6.7 illustrates the results of an inference of a mobile PU in terms of its X-grid and Y-grid position. Here, it is assumed that the database responds truthfully to each query generated by the SU. This represents the case where the database does not use any form of obfuscation. The PU's actual path of movement, the path inferred by an adversary and the average error in adversary's inference are plotted. Clearly, we can see that, after few time-slots, the adversary is able to accurately infer the trajectory/path of the PU. The mean error in adversary's inference is small, which demonstrates the effectiveness of using particle filter for movement tracking.

On the other hand, when the database implements obfuscation, the adversary's inference becomes polluted. Figure 6.8 shows the results. Here, the database uses perturbation-based obfuscation and replies to queries with false-positive responses by following the random obfuscation strategy. As seen in the plots, there is a large error in the attacker's inference, which demonstrates the effectiveness of obfuscation in protecting the path-of-movement privacy of PUs. Finally, note that the analysis of an optimal inference strategy and an optimal obfuscation strategy in case of mobile PUs is itself a different and challenging research topic, and we shall pursue it in our future work.

6.7 Chapter Summary

In this chapter, we showed that malicious SUs (i.e., queriers) can readily infer the locations of the PUs even if the database's responses to queries do not directly reveal such information. We also showed that an adversary can make the inference attack more effective by choosing the query locations optimally. Moreover, in order to counter the location inference attack, we proposed an optimal obfuscation strategy that makes a very favorable trade-off between location privacy and spectrum utilization efficiency. Our simulation results demonstrate the effectiveness of our proposed obfuscation strategy. The results show that a large gain in location privacy can be obtained while incurring a small loss in the SUs' link capacity when the database implements the proposed optimal obfuscation strategy.

Chapter 7

Conclusion

This dissertation focused on the idea of improving the utilization efficiency of the shared spectrum in dynamic spectrum access networks while protecting the incumbent users (IUs) from secondary user (SU)-induced interference and from operational security (OPSEC) threats. In particular, we first investigated efficient approaches for characterizing aggregate interference experienced by IUs due to transmissions from multiple SUs. Second, we leveraged this analytical methodology in redefining the legacy notion of inadequately flexible and conservative exclusion zones (EZs) that are defined for protecting IUs from harmful interference. Third, we investigated the need to protect the confidentiality and security of spectrum users in the light of management frameworks that require sharing significant information about the location and usage of spectrum resources. To this end, we proposed an optimal obfuscation strategy that can be employed by the spectrum management entity for maximizing the location privacy of IUs while ensuring that the degradation in spectrum utilization due to obfuscated responses does not exceed a threshold.

In short, we began the dissertation by asking four questions related to spectrum efficiency and security in dynamic spectrum sharing. In this chapter, we shall conclude the dissertation by summarizing our findings to those questions.

How can we estimate the aggregate interference in a computationally efficient manner?

To seek an answer to this question, we investigated an analytical approach for characterizing the aggregate interference in dynamic spectrum sharing networks. Our proposed solution addresses the two main limitations of existing methods that rely on computationally intensive terrain-based propagation models. First, our analytical framework provides a closed-form expression for aggregate interference which makes it computationally efficient. Second, it does not necessitate the precise geolocation information of IUs and SUs, making our approach extremely practical in large, location privacy-aware real-time spectrum sharing applications. This contribution helps in providing real-time incumbent protection from SU-induced interference while at the same time maximizes the utilization of shared spectrum because, unlike legacy approaches, it does not unnecessarily limit SUs' spectrum utilization opportunities.

How can we redefine the legacy notion of overly conservative mechanisms for protecting incumbents from harmful interference?

We addressed this question by proposing a novel framework for implementing ex-ante enforcement that addresses the limitations of legacy EZs. In particular, we introduced the concept of *Multi-tiered Incumbent Protection Zones* (MIPZ) and showed that it can be used to dynamically adjust the IU's protection boundary based on the radio network dynamics, spectrum demand, SU density and IU interference protection criteria. MIPZ redefines legacy notion of EZs by prescribing dynamically adjustable EZ boundaries. Our extensive simulation results show that MIPZ can be used to improve the overall utilization opportunities for the shared spectrum while ensuring adequate protection to the IUs. We believe that this contribution facilitates spectrum regulators in gaining insights of and determine the trade-off between interference protection and spectrum utilization efficiency.

How can new wireless protocols be standardized for improving the spectrum utilization efficiency?

We addressed this question by analyzing the performance of the next generation Wireless Fidelity (Wi-Fi) protocol—namely, IEEE 802.11ax. In particular, we proposed an optimal

resource allocation scheme for the IEEE 802.11ax MAC, analyzed its performance, and showed that it can offer spectral efficiency almost twice more than legacy Wi-Fi protocols in some use-case scenarios. Thus, in general, we demonstrated that emerging wireless protocols, if carefully standardized, have the potential to alleviate the problem of spectrum scarcity. While efficient utilization of the shared spectrum is still an open problem, our contributions helps in facilitating a deeper understanding of methods, apparatus and emerging standards that utilize the spectrum more dynamically and effectively.

How can we safeguard users' operational information when access to such information is a key to enabling efficient spectrum sharing?

We addressed this question by investigating location inference attacks in database-driven spectrum sharing regimes. Specifically, we proposed an optimal location obfuscation strategy that can be employed by the spectrum database to thwart location inference attacks from malicious users. The proposed scheme maximizes the location privacy of IUs while ensuring that the degradation in SUs' spectrum utilization due to obfuscated responses does not exceed a threshold. Using simulation results, we demonstrated the effectiveness of the proposed strategy in preserving the location privacy of IUs. Privacy analysis of this kind may help in wider adoption of dynamic spectrum sharing by allowing privacy-aware IUs to quantify the risk posed to their privacy and by providing specific techniques to mitigate that risk.

In summary, the broader impact of the research presented in this dissertation is that it provides a better understanding of the underlying challenges and lays out solution approaches for improving efficient utilization of the shared spectrum. Our contributions facilitate regulators with effective tools and apparatus for gaining insights and striking an appropriate balance between the three key objectives in dynamic spectrum sharing, viz. improving spectrum utilization efficiency, ensuring adequate interference protection, and minimizing OPSEC threats.

Bibliography

[1] PCAST, "Report to the President Realizing the Full Potential of Government-Held Spectrum to Spur Economic Growth," Jul. 2012.

[2] Cisco, "Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2014-2019," tech. rep., Feb. 2015.

[3] FCC, "Auction 97: Advanced Wireless Services (AWS-3)." Accessed: 2015-11-09.

[4] FCC, "Second Memorandum Opinion and Order (FCC 08-260)," Sep. 2010.

[5] FCC, "Report and Order and Second Further Notice of Proposed Rulemaking, GN Docket No. 12-354," Apr. 2015.

[6] FCC, "Order on Reconsideration and Second Report and Order, GN Docket No. 12-354," May 2016.

[7] FCC, "First Report and Order (ET Docket No. 13-49)," Apr. 2014.

[8] J. Lansford, J. Kenney, P. Ecclesine, T. Yucek, and P. Spaanderman, "Final Report of DSRC Coexistence Tiger Team," tech. rep., Mar. 2015.

[9] FCC, "Office of Engineering and Technology and Wireless Telecommmunications Bureau Seek Information on Current Trends in LTE-U and LAA Technology, Docket No. 15-105," May 2015.

[10] S. Yrjola, "Licensed Shared Access (LSA) Field Trial Using LTE Network and Self Organized Network LSA Controller," in *Communications Technologies and Software Defined Radio (WinnComm-Europe), 2015 Wireless Innovation Forum European Confernece on*, Oct. 2015.

[11] OfCom, "A Framework for Spectrum Sharing," Jul. 2015.

[12] FCC, "Report and Order and Second Further Notice of Proposed Rulemaking, GN Docket No. 12-354," Apr 2015.

[13] E. Drocella, J. Richards, R. Sole, F. Najmy, A. Lundy, P. McKenna, "3.5 GHz Exclusion Zone Analyses and Methodology," tech. rep., 2015.

[14] B. Bahrak, S. Bhattarai, U. Abid, J.-M. Park, J. Reed, and D. Gurney, "Protecting the primary users operational privacy in spectrum sharing," in *Dynamic Spectrum Access Networks (DYSPAN), 2014 IEEE International Symposium on*, IEEE, 2014.

[15] Wireless Innovation Forum, "Spectrum Sharing Committee." `http://www.wirelessinnovation.org/spectrum-sharing-committee`. Accessed: 2016-02-24.

[16] DARPA, "Shared Spectrum Access for Radar and Communications (SSPARC)." `http://www.darpa.mil/program/shared-spectrum-access-for-radar-and-communications`. Accessed: 2016-02-24.

[17] A. J. Paverd, A. Martin, and I. Brown, "Modelling and Automatically Analysing Privacy Properties for Honest-but-Curious Adversaries," tech. rep., 2014.

[18] R. Murty, R. Chandra, T. Moscibroda, and P. Bahl, "Senseless: A database-driven White Spaces Network," *IEEE Transactions on Mobile Computing*, vol. 11, no. 2, pp. 189–203, 2012.

[19] D. Gurney, G. Buchwald, L. Ecklund, S. Kuffner, and J. Grosspietsch, "Geo-Location Database Techniques for Incumbent Protection in the TV White Space," in *IEEE Symposium on Dynamic Spectrum Access Networks (DySPAN), 2008.*, pp. 1–9, Oct. 2008.

[20] B. Gao, J.-M. Park, and Y. Yang, "Supporting Mobile Users in Database-driven Opportunistic Spectrum Access," in *Proceedings of the 15th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, MobiHoc '14, pp. 215–224, ACM, 2014.

[21] B. Gao, S. Bhattarai, J.-M. Park, Y. Yang, M. Liu, K. Zheng, and Y. Dou, "Incentivizing Spectrum Sensing in Dynamic Spectrum Sharing," in *Proceedings of the 2016 IEEE International Conference on Computer Communications (INFOCOM)*, Apr. 2016.

[22] FCC, "Report of the Spectrum Efficiency Working Group, ET Docket 02-135," Nov. 2002.

[23] OfCom, "Spectrum Framework Review: a Consultation on Ofcom's views as to how radio spectrum should be managed," Nov. 2004.

[24] FCC, "Connecting America: The National Broadband Plan," Mar. 2010.

[25] The White House, "Unleashing the Wireless Broadband Revolution," Jun. 2010.

[26] The White House, "Expanding America's Leadership in Wireless Innovation," Jun. 2013.

[27] FCC, "Revision of Part 15 of the Commissions Rules to Permit Unlicensed National Information Infrastructure (U-NII) Devices in the 5 GHz Band (NPRM 13-22)," Feb. 2013.

[28] OfCom, "Geolocation for Cognitive Access: A Discussion on using Geolocation to enable License-exempt Access to the Interleaved Spectrum," Jul. 2009.

[29] OfCom, "Implementing Geolocation: Summary of Consultation Responses and Next Steps," Sep. 2011.

[30] OfCom, "Spectrum Management Strategy: Ofcoms Strategic Direction and Priorities for Managing Spectrum over the Next 10 Years," Apr. 2014.

[31] Industry Canada, "Consultation on a Policy and Technical Framework for the Use of Non-broadcasting Applications in the Television Broadcasting Bands below 698 MHz (SMSE-012-11)," Aug. 2011.

[32] Industry Canada, "Framework for the Use of Certain Non-broadcasting Applications in the Television Broadcasting Bands Below 698 MHz (SMSE-012-12)," Oct. 2012.

[33] Infocomm Development Authority of Singapore, "Trial of White Space Technology Accessing VHF and UHF Bands in Singapore," Jul. 2010.

[34] Infocomm Development Authority of Singapore, "Regulatory Framework for TV White Space Operations in he VHF/UHF Bands," Jun. 2014.

[35] T. Wang, G. Li, J. Ding, Q. Miao, J. Li, and Y. Wang, "5G Spectrum: is China Ready?," *IEEE Communications Magazine*, vol. 53, pp. 58–65, Jul. 2015.

[36] European Paliament and Council, "Decision No 243/2012/EU of the European Parliament and of the Council of 14 March 2012 Establishing a Multiannual Radio Spectrum Policy Programme," Mar. 2012.

[37] Radio Spectrum Policy Group, "RSPG Opinion on Licensed Shared Access (RSPG13-538)," Nov. 2013.

[38] European Commission, "2013/195/EU: Commission Implementing Decision of 23 April 2013 Defining the Practical Arrangements,Uniform Formats and a Methodology in Relation to the Radio Spectrum Inventory Established by Decision No 243/2012/EU of the European Parliament and of the Council Establishing a Multiannual Radio Spectrum Policy Programme," Apr. 2013.

[39] ECC, "Technical and Operational Requirements for the Possible Operation of Cognitive Radio Systems in the 'White Spaces' of the Frequency Band 470-790 MHz ," Jan.

[40] P. A. Tenhula, "Regulatory Framework(s) for Facilitating New Spectrum Sharing Schemes," Jul. 2012.

[41] International Telecommunications Union (ITU) , "Definitions of Software Defined Radio (SDR) and Cognitive Radio Systems (CRS)," Sep. 2009.

[42] B. Wang and K. Liu, "Advances in cognitive radio networks: A survey," *IEEE Journal on Selected Topics in Signal Processing*, vol. 5, pp. 5–23, Feb. 2011.

[43] E. Hossain, D. Niyato, and D. I. Kim, "Evolution and future trends of research in cognitive radio: a contemporary survey," *Wireless Communications and Mobile Computing*, vol. 15, pp. 1530–1564, Aug. 2015.

[44] OECD., "New Approaches to Spectrum Management," *OECD Digital Economy Papers*, May 2014.

[45] M. Matinmikko and M. Mustonen and D. Roberson and J. Paavola and M. Höyhtyä and S. Yrjölä and J. Röning, "Overview and comparison of recent spectrum sharing approaches in regulation and research: From opportunistic unlicensed access towards licensed shared access," in *Dynamic Spectrum Access Networks (DYSPAN), 2014 IEEE International Symposium on*, pp. 92–102, Apr. 2014.

[46] METIS, "Deliverable D5.1: Intermediate description of the spectrum needs and usage principles," Aug. 2014.

[47] J. M. Chapin and W. H. Lehr, "Cognitive Radios for Dynamic Spectrum Access - The Path to Market Success for Dynamic Spectrum Access Technology," *IEEE Communications Magazine*, vol. 45, pp. 96–103, May 2007.

[48] FCC and NTIA, "Coordination Procedures in the 1695-1710 MHz and 1755-1780 MHz bands (FCC 13-185)," Jul 2014.

[49] FCC, "Notice of Proposed Rulemaking (ET Docket No. 13-49)," Feb. 2013.

[50] Fierce WirelessTech, "Verizon, Qualcomm lobby for LTE-U, Wi-Fi coexistence scheme." `http://www.fiercewireless.com/tech/story/verizon-qualcomm-lobby-lte-u-wi-fi-coexistence-scheme/2015-07-20`. Accessed: 11-29-2015.

[51] FCC, "Report and Order, ET Docket No. 07-113," Aug. 2013.

[52] FCC, "Report and Order, WT Docket No. 02-146," Oct. 2003.

[53] FCC, "Memorandum Opinion and Order, WT Docket No. 02-146," Mar. 2005.

[54] FCC, "Notice of Proposed Rulemaking, GN Docket No. 14-177," Oct. 2015.

[55] NTIA, "Fifth Interim Progress Report on the Ten-Year Plan and Timetable ," Apr. 2015.

[56] ECC, "Request for Opinion on Licensed Shared Access (LSA)," Nov. 2012.

[57] ECC, "Licensed Shared Access (LSA)," Feb. 2014.

[58] OfCom, "Ofcom Consultation on the UK Preparations for the World Radio Communication Conference 2015 (WRC-15)," Jun. 2014.

[59] OfCom, "Implementing TV White Spaces," Feb. 2015.

[60] Industry Canada, "White Space Devices (WSDs) (RSS-222)," Feb. 2015.

[61] Radio Spectrum Management, "Television White Space Devices Certification and Licensing Rules," Nov. 2014.

[62] M. Palola, M. Matinmikko, J. Prokkola, M. Mustonen, M. Heikkila, T. Kippola, S. Yrjola, V. Hartikainen, L. Tudose, A. Kivinen, J. Paavola, and K. Heiska, "Live field trial of Licensed Shared Access (LSA) concept using LTE network in 2.3 GHz band," in *IEEE Symposium on Dynamic Spectrum Access Networks (DySPAN)*, 2014.

[63] J.-M. Park, J. Reed, A. Beex, T. Clancy, V. Kumar, and B. Bahrak, "Security and enforcement in spectrum sharing," *Proceedings of the IEEE*, vol. 102, pp. 270–281, Mar. 2014.

[64] M. Altamimi and M. B. Weiss, "Enforcement and Network Capacity in Spectrum Sharing: Quantifying the Benefits of Different Enforcement Scenarios," in *Proceedings of The 41st Research Conference on Communication, Information and Internet Policy*, Mar. 2014.

[65] B. Bahrak, A. Deshpande, and J.-M. . Park, "Spectrum Access Policy Reasoning for Policy-based Cognitive Radios," *Computer Networks*, vol. 56, no. 11, pp. 2649–2663, 2012.

[66] C. Li, A. Raghunathan, and N. Jha, "An Architecture for Secure Software Defined Radio," in *Design, Automation Test in Europe Conference Exhibition, 2009. DATE '09.*, pp. 448–453, Apr. 2009.

[67] S. Xiao, J.-M. Park, and Y. Ye, "Tamper Resistance for Software Defined Radio Software," in *Computer Software and Applications Conference, 2009. COMPSAC '09. 33rd Annual IEEE International*, vol. 1, pp. 383–391, Jul. 2009.

[68] C. R. Aguayo González and J. H. Reed, "Power Fingerprinting in SDR Integrity Assessment for Security and Regulatory Compliance," *Analog Integr. Circuits Signal Process.*, vol. 69, pp. 307–327, Dec. 2011.

[69] X. Li, J. Chen, and F. Ng, "Secure Transmission Power of Cognitive Radios for Dynamic Spectrum Access Applications," in *Information Sciences and Systems, 2008. CISS 2008. 42nd Annual Conference on*, pp. 213–218, Mar. 2008.

[70] S. Bhattarai, A. Ullah, J.-M. Park, J. Reed, D. Gurney, and B. Gao, "Defining Incumbent Protection Zones on the Fly: Dynamic Boundaries for Spectrum Sharing," in *Proc. of IEEE Symposium on Dynamic Spectrum Access Networks (DySPAN)*, Sep-Oct 2015.

[71] A. Ullah, S. Bhattarai, J.-M. Park, J. Reed, D. Gurney, and B. Bahrak, "Multi-Tier Exclusion Zones for Dynamic Spectrum Sharing," in *Proc. of IEEE International Conference in Communications (ICC)*, Jun. 2015.

[72] R. O'Connor, "Understanding Television's Grade A and Grade B Service Contours," *Broadcasting, IEEE Transactions on*, vol. 47, pp. 309–314, Sep. 2001.

[73] FCC, "Propagation Data Required for the Evaluation of Coordination Distances in the Frequency Range 0.85-60 GHz (Rec. ITU-R P.620-3)," Jul. 2014.

[74] NTIA, "Portal Opens for AWS-3 Spectrum Sharing Coordination." `https://www.ntia.doc.gov/blog/2015/portal-opens-aws-3-spectrum-sharing-coordination`. Accessed: 11-30-2015.

[75] S. Shellhammer, S. Sai, T. Rahul, and T. James, "Performance of power detector sensors of DTV signals in IEEE 802.22 WRANs," in *Proc. of ACM Workshop on Technology & Policy for Accessing Spectrum*, 2006.

[76] R. Tandra, S. Mishra, and A. Sahai, "What is a Spectrum Hole and What Does it Take to Recognize One?," *Proceedings of the IEEE*, vol. 97, May. 2009.

[77] National Telecommunications and Information Administration, "An Assessment of the Near-Term Viability of Accommodating Wireless Broadband Systems in the 1675-1710 MHz, 1755-1780 MHz, 3500-3650 MHz, and 4200-4220 MHz, 4380-4400 MHz Bands," Oct. 2010.

[78] RYSAVY Research, "Spectrum Sharing: The Promise and the Reality," Jul. 2012.

[79] J. C. Ribeiro, J. Ribeiro, J. Rodriguez, R. Dionisio, H. Esteves, P. Duarte, and P. Marques, "Testbed for Combination of Local Sensing with Geolocation Database in Real Environments," *IEEE Wireless Communications*, vol. 19, Aug. 2012.

[80] T. Zhang and S. Banerjee, "Inaccurate Spectrum Databases? Public Transit to its Rescue!," in *Proc. ACM HotNets'13*, Nov. 2013.

[81] A. Chakraborty and S. R. Das, "Measurement-Augmented Spectrum Databases for White Space Spectrum," in *Proc. ACM CoNEXT'14*, Dec. 2014.

[82] D. Rojerio, J. Ribeiro, P. Marques, and J. Rodriguez, "Combination of a Geolocation Database Access with Infrastructure Sensing in TV Bands," *EURASIP Journal on Wireless Communications and Networking*, Dec. 2014.

[83] N. Wang, Y. Gao, and B. Evans, "Database-Augmented Spectrum Sensing Algorithm for Cognitive Radio," in *Communications (ICC), 2015 IEEE International Conference on*, pp. 7468–7473, Jun. 2015.

[84] Y. Zhao, B. Le, and J. H. Reed, "Network Support—The Radio Environment Map," in *Cognitive Radio Technology*, Elsevier, 2006.

[85] H. B. Yilmaz, T. Tugcu, F. Alagöz, and S. Bayhan, "Radio Environment Map as Enabler for Practical Cognitive Radio Networks," *IEEE Communications Magazine*, vol. 51, Dec. 2013.

[86] Y. Zhao, L. Morales, J. Gaeddert, K. Bae, J.-S. Um, and J. Reed, "Applying Radio Environment Maps to Cognitive Wireless Regional Area Networks," in *New Frontiers in Dynamic Spectrum Access Networks, 2007. DySPAN 2007. 2nd IEEE International Symposium on*, pp. 115–118, Apr. 2007.

[87] V. Pankonin and R. Price, "Radio Astronomy and Spectrum Management: The Impact of WARC-79," *Communications, IEEE Transactions on*, vol. 29, pp. 1228–1237, Aug 1981.

[88] T. Gergely, "Spectrum Access for the Passive Services: The Past and the Future," *Proceedings of the IEEE*, vol. 102, pp. 393–398, Mar. 2014.

[89] J. Ford and K. Buch, "RFI mitigation techniques in radio astronomy," in *Geoscience and Remote Sensing Symposium (IGARSS), 2014 IEEE International*, pp. 231–234, Jul. 2014.

[90] ITU-R, "Techniques for Mitigation of Radio Frequency Interference in Radio Astronomy (Rep. ITU-R RA.2126)," 2007.

[91] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless Device Identification with Radiometric Signatures," in *Proceedings of the 14th ACM International Conference on Mobile Computing and Networking*, MobiCom '08, pp. 116–127, 2008.

[92] B. Danev and S. Capkun, "Transient-based Identification of Wireless Sensor Nodes," in *Information Processing in Sensor Networks, 2009. IPSN 2009. International Conference on*, pp. 25–36, Apr. 2009.

[93] W. Hou, X. Wang, and J. Chouinard, "Physical Layer Authentication in OFDM Systems based on Hypothesis Testing of CFO Estimates," in *Communications (ICC), 2012 IEEE International Conference on*, pp. 3559–3563, Jun. 2012.

[94] O. Ureten and N. Serinken, "Wireless Security through RF Fingerprinting," *Electrical and Computer Engineering, Canadian Journal of*, vol. 32, no. 1, pp. 27–33, 2007.

[95] I. J. Cox, M. Miller, and A. McKellips, "Watermarking as Communications with Side Information," *Proceedings of the IEEE*, vol. 87, pp. 1127–1141, Jul. 1999.

[96] C. Fei, D. Kundur, and R. Kwong, "Analysis and Sesign of Secure Watermark-based Authentication Systems," *Information Forensics and Security, IEEE Transactions on*, vol. 1, pp. 43–55, Mar. 2006.

[97] N. Goergen, T. Clancy, and T. Newman, "Physical Layer Authentication Watermarks through Synthetic Channel Emulation," in *New Frontiers in Dynamic Spectrum, 2010 IEEE Symposium on*, pp. 1–7, Apr. 2010.

[98] J. E. Kleider, S. Gifford, S. Chuprun, and B. Fette, "Radio Frequency Watermarking for OFDM Wireless Networks," in *Acoustics, Speech, and Signal Processing, 2004. Proceedings. (ICASSP '04). IEEE International Conference on*, vol. 5, pp. V–397–400 vol.5, May 2004.

[99] V. Kumar, J.-M. Park, T. Clancy, and K. Bian, "PHY-layer Authentication by Introducing Controlled Inter Symbol Interference," in *IEEE CNS*, pp. 10–18, 2013.

[100] Y. Liu, P. Ning, and H. Dai, "Authenticating Primary Users' Signals in Cognitive Radio Networks via Integrated Cryptographic and Wireless Link Signatures," in *IEEE Symp. Security and Privacy*, pp. 286–301, May 2010.

[101] R. Miller and W. Trappe, "Short paper: ACE: Authenticating the Channel Estimation Process in Wireless Communication Systems," in *Proc. ACM WiSec*, pp. 91–96, 2011.

[102] X. Tan, K. Borle, W. Du, and B. Chen, "Cryptographic Link Signatures for Spectrum Usage Authentication in Cognitive Radio," in *Proc. ACM WiSec*, pp. 79–90, Jun. 2011.

[103] X. Wang, Y. Wu, and B. Caron, "Transmitter Identification using Embedded Pseudo Random Sequences," *IEEE Trans. Broadcast.*, vol. 50, pp. 244–252, Sep. 2004.

[104] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "Using the Physical Layer for Wireless Authentication in Time-Variant Channels," *IEEE Trans. Wireless Commun.*, vol. 7, pp. 2571–2579, Jul. 2008.

[105] P. Yu, J. Baras, and B. Sadler, "Physical-Layer Authentication," *IEEE Trans. Inf. Forensics Security*, vol. 3, pp. 38–51, Mar. 2008.

[106] B. Danev, H. Luecken, S. Čapkun, and K. Defrawy, "Attacks on Physical-Layer Identification," in *ACM WiSec*, pp. 89–98, 2010.

[107] V. Kumar, and J-M. Park and K. Bian, "Blind Transmitter Authentication for Spectrum Security and Enforcement," in *Computer and Communications Security (CCS), 21st ACM Conference on*, Oct. 2014.

[108] "IEEE Standard for Policy Language Requirements and System Architectures for Dynamic Spectrum Access Systems," *IEEE Std 1900.5-2011*, pp. 1–51, Jan. 2012.

[109] R. Chen, J.-M. Park, and J. Reed, "Defense against Primary User Emulation Attacks in Cognitive Radio Networks," *IEEE J. Sel. Areas Commun.*, vol. 26, pp. 25–37, Jan. 2008.

[110] S. Liu, Y. Chen, W. Trappe, and L. J. Greenstein, "Non-Interactive Localization of Cognitive Radios based on Dynamic Signal Strength Mapping," in *Proc. Sixth Int. Conf. on Wireless On-Demand Network Systems and Services*, pp. 77–84, 2009.

[111] T. He, C. Huang, B. M. Blum, J. A. Stankovic, and T. Abdelzaher, "Range-Free Localization Schemes for Large Scale Sensor Networks," in *Proc. ACM MobiCom*, pp. 81–95, 2003.

[112] A. Dutta and M. Chiang, "See Something, Say Something: Crowdsourced Enforcement of Spectrum Policies," *Wireless Communications, IEEE Transactions on*, vol. PP, no. 99, pp. 1–1, 2015.

[113] K. Woyach, A. Sahai, G. Atia, and V. Saligrama, "Crime and Punishment for Cognitive Radios," in *Communication, Control, and Computing, 2008 46th Annual Allerton Conference on*, pp. 236–243, Sep. 2008.

[114] M. B. H. Weiss, W. Lehr, M. Altamimi, and L. Cui, "Enforcement in Dynamic Spectrum Access Systems," in *2012 Confernece on TRPC*, Mar. 2012.

[115] FCC: Spectrum/Receiver Performance Working Group, "Introduction to Interference Resolution, Enforcement, and Radio Noise," tech. rep., Jun. 2014.

[116] Standard ECMA-392, "MAC and PHY for Operation in TV White Space," Dec 2009.

[117] T. Baykas, M. Kasslin, M. Cummings, H. Kang, J. Kwak, R. Paine, A. Reznik, R. Saeed, and S. Shellhammer, "Developing a Standard for TV White Space Coexistence: Technical Challenges and Solution Approaches," *Wireless Communications, IEEE*, vol. 19, pp. 10–22, Feb. 2012.

[118] "IEEE Standard for Information Technology– Local and Metropolitan Area Networks—Specific Requirements– Part 22: Cognitive Wireless RAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Policies and Procedures for Operation in the TV Bands," *IEEE Std 802.22-2011*, pp. 1–680, July 2011.

[119] IEEE 802.11 homepage. Accessed: 2015-12-01.

[120] "Project Authorization Request for IEEE Standard for Local and Metropolitan Area Networks Part 15.4: Low Rate Wireless Personal Area Networks (LR-WPANs) Amendment: TV White Space between 54 MHz and 862 MHz Physical Layer," *IEEE Std 802.15.4m*, Jul. 2011.

[121] "Project Authorization Request for P1900.7 Radio Interface for White Space Dynamic Spectrum Access Radio Systems Supporting Fixed and Mobile Operation," Jun. 2011.

[122] T. Baykas, M. Cummings, H. Kang, M. Kasslin, J. Kwak, R. Paine, A. Reznik, R. Saeed, and S. Shellhammer, "Developing a Standard for TV White Space Coexistence: Technical Challenges and Solution Approaches," *IEEE 802.19.1 Task Group White Paper*, 2011.

[123] "Workshop on TV White Space Coexistence: IEEE 802.19.1 Overview," Jul. 2010. Accessed: 2015-12-01.

[124] P. M. and F. S., "LTE Unlicensed and Wi-Fi: Moving beyond Coexistence," tech. rep., 2015.

[125] Qualcomm Research, "LTE in Unlicensed Spectrum: Harmonious Coexistence with Wi-Fi," tech. rep., Jun. 2014.

[126] Signals Research Group, "The Prospect of LTE and Wi-Fi Sharing Unlicensed Spectrum: Good Fences Make Good Neighbors," tech. rep., Feb. 2015.

[127] T. Nihtila, V. Tykhomyrov, O. Alanen, M. Uusitalo, A. Sorri, M. Moisio, S. Iraji, R. Ratasuk, and N. Mangalvedhe, "System Performance of LTE and IEEE 802.11 Coexisting on a Shared Frequency Band," in *Wireless Communications and Networking Conference (WCNC), 2013 IEEE*, pp. 1038–1043, Apr. 2013.

[128] R. Ratasuk, M. Uusitalo, N. Mangalvedhe, A. Sorri, S. Iraji, C. Wijting, and A. Ghosh, "License-exempt LTE Deployment in Heterogeneous Network," in *Wireless Communication Systems (ISWCS), 2012 International Symposium on*, pp. 246–250, Aug. 2012.

[129] M. Xing, Y. Peng, T. Xia, H. Long, and K. Zheng, "Adaptive Spectrum Sharing of LTE Co-Existing with WLAN in Unlicensed Frequency Bands," in *Vehicular Technology Conference (VTC Spring), 2015 IEEE 81st*, pp. 1–5, May 2015.

[130] J. Stine and C. Caicedo Bastidas, "Enabling Spectrum Sharing via Spectrum Consumption Models," *Selected Areas in Communications, IEEE Journal on*, vol. 33, pp. 725–735, April 2015.

[131] C. Caicedo and J. Stine, "Spectrum Markets and Sharing via Spectrum Consumption Models," in *41st Res. Conf. TPRC*, Mar. 2013.

[132] J. Stine and C. Bastidas, "Service Level Agreements with Spectrum Consumption Models," in *Dynamic Spectrum Access Networks (DYSPAN), 2014 IEEE International Symposium on*, pp. 206–214, Apr. 2014.

[133] R. Etkin, A. Parekh, and D. Tse, "Spectrum Sharing for Unlicensed Bands," *Selected Areas in Communications, IEEE Journal on*, vol. 25, pp. 517–528, Apr. 2007.

[134] J. Suris, L. DaSilva, Z. Han, and A. MacKenzie, "Cooperative Game Theory for Distributed Spectrum Sharing," in *Communications, 2007. ICC '07. IEEE International Conference on*, pp. 5282–5287, Jun. 2007.

[135] S. Yun and L. Qiu, "Supporting WiFi and LTE Co-existence," in *Computer Communications (INFOCOM), 2015 IEEE Conference on*, pp. 810–818, Apr. 2015.

[136] N. Gupta, A. Prakash, and R. Tripathi, "Medium access control protocols for safety applications in vehicular ad-hoc network: A classification and comprehensive survey," *Vehicular Communications*, vol. 2, no. 4, pp. 223–237, 2015.

[137] Y. Niu, Y. Li, D. Jin, L. Su, and A. V. Vasilakos, "A survey of millimeter wave communications (mmwave) for 5g: opportunities and challenges," *Wireless Networks*, vol. 21, no. 8, pp. 2657–2676, 2015.

[138] S. Rangan and T. S. Rappaport and E. Erkip, "Millimeter-Wave Cellular Wireless Networks: Potentials and Challenges," *Proceedings of the IEEE*, vol. 102, pp. 366–385, Mar. 2014.

[139] B. Bahrak, S. Bhattarai, A. Ullah, J.-M. Park, J. Reed, and D. Gurney, "Protecting the Primary Users' Operational Privacy in Spectrum Sharing," in *Dynamic Spectrum Access Networks (DYSPAN), 2014 IEEE International Symposium on*, pp. 236–247, April 2014.

[140] C. Dwork, "Differential privacy," in *International Conference on Automata, Languages and Programming*, pp. 1–12, 2006.

[141] M. E. Andrés, N. E. Bordenabe, K. Chatzikokolakis, and C. Palamidessi, "Geo-indistinguishability: Differential Privacy for Location-based Systems," in *Proceedings of the 2013 ACM SIGSAC Conference on Computer, Communications Security*, CCS '13, pp. 901–914, ACM, 2013.

[142] N. E. Bordenabe, K. Chatzikokolakis, and C. Palamidessi, "Optimal Geo-Indistinguishable Mechanisms for Location Privacy, booktitle = Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security," CCS '14, (New York, NY, USA), pp. 251–262, ACM, 2014.

[143] Z. Gao, H. Zhu, Y. Liu, M. Li, and Z. Cao, "Location Privacy in Database-driven Cognitive Radio Networks: Attacks and Countermeasures," in *IEEE Proc. of INFOCOM*, pp. 2751–2759, April 2013.

[144] Z. Chen, J. Wang, Z. Zhang, and S. Xinxia, "A Fully Homomorphic Encryption Scheme with Better Key Size," *Communications, China*, vol. 11, pp. 82–92, Sept 2014.

[145] R. Shokri, G. Theodorakopoulos, C. Troncoso, J.-P. Hubaux, and J.-Y. Le Boudec, "Protecting Location Privacy: Optimal Strategy Against Localization Attacks," in *Proc. of the 2012 ACM Conference on Computer and Communications Security*.

[146] M. Gruteser and D. Grunwald, "Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking," in *Proceedings of the 1st International Conference on Mobile Systems, Applications and Services*, MobiSys '03, pp. 31–42, ACM, 2003.

[147] J. Freudiger, R. Shokri, and J.-P. Hubaux, "On the Optimal Placement of Mix Zones," *Privacy Enhancing Technologies*, vol. 5672, pp. 216–234, 2009.

[148] R. Chow and P. Golle, "Faking Contextual Data for Fun, Profit, and Privacy," in *Proceedings of the 8th ACM Workshop on Privacy in the Electronic Society*, WPES '09, pp. 105–108, ACM, 2009.

[149] B. Gedik and L. Liu, "Protecting Location Privacy with Personalized k-Anonymity: Architecture and Algorithms," *Mobile Computing, IEEE Transactions on*, vol. 7, pp. 1–18, Jan. 2008.

[150] ICANN, "FactSheet: Root Server Attack on 6 February 2007," Feb. 2007.

[151] NSF, "Enhancing Access to the Radio Spectrum," Aug. 2010.

[152] R. Dionisio, J. Ribeiro, P. Marques, and J. Rodriguez, "Combination of a Geolocation Database Access with Infrastructure Sensing in TV Bands," *EURASIP Journal on Wireless Communications and Networking*, 2014.

[153] G. Baldini, T. Sturman, A. Biswas, R. Leschhorn, G. Godor, and M. Street, "Security Aspects in Software Defined Radio and Cognitive Radio Networks: A Survey and A Way Ahead," *Communications Surveys Tutorials, IEEE*, vol. 14, no. 2, pp. 355–379, 2012.

[154] D. Symeonidis and G. Baldini, "European Standardization and SDR Certification," in *Telecommunications (AICT), 2010 Sixth Advanced International Conference on*, pp. 136–141, May 2010.

[155] J. Giacomoni and D. Sicker, "Difficulties in Providing Certification and Assurance for Software Defined Radios," in *New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005. 2005 First IEEE International Symposium on*, pp. 526–538, Nov. 2005.

[156] A. Ullah, S. Bhattarai, J.-M. Park, J. H. Reed, D. Gurney, and B. Bahrak, "Multi-Tier Exclusion Zones for Dynamic Spectrum Sharing," in *Proc. IEEE ICC'15*, Jun. 2015.

[157] G. Hufford, "The ITS Irregular Terrain Model, version 1.2.2 The Algorithm," tech. rep.

[158] G.A. Hufford, A.G. Longley, W.A. Kissick, "A Guide to the Use of the ITS Irregular Terrain Model in the Area Prediction Mode," tech. rep., Apr. 1982.

[159] H.K. Wong, "Field Strength Prediction in the Irregular Terrain PTP Model," tech. rep., Nov. 2002.

[160] S. Bhattarai, A. Ullah, J.-M. Park, J. H. Reed, D. Gurney, and B. Gao, "Defining Exclusion Zones on the Fly: Dynamic Boundaries for Spectrum Sharing," in *Proc. IEEE DySPAN'15*, Sept. 2015.

[161] G. Pastor, I. Mora-Jimnez, A. J. Caamao, and R. Jntti, "Log-Cumulant Matching Approximation of Heavy-Tailed-Distributed Aggregate Interference," in *2015 IEEE International Conference on Communications (ICC)*, pp. 4811–4815, June 2015.

[162] A. Ghasemi and E. S. Sousa, "Interference Aggregation in Spectrum-Sensing Cognitive Wireless Networks," *IEEE Journal of Selected Topics in Signal Processing*, vol. 2, pp. 41–56, Feb 2008.

[163] J. Guo, S. Durrani, and X. Zhou, "Characterization of Aggregate Interference in Arbitrarily-Shaped Underlay Cognitive Networks," in *2014 IEEE Global Communications Conference*, pp. 961–966, 2014.

[164] M. S. Ali and N. B. Mehta, "Modeling Time-Varying Aggregate Interference from Cognitive Radios and Implications on Primary Exclusive Zone Design," in *2013 IEEE Global Communications Conference (GLOBECOM)*, pp. 3760–3765, Dec 2013.

[165] M. F. Hanif, M. Shafi, P. J. Smith, and P. Dmochowski, "Interference and Deployment Issues for Cognitive Radio Systems in Shadowing Environments," in *2009 IEEE International Conference on Communications*, pp. 1–6, June 2009.

[166] FCC, "Notice of Proposed Rulemaking and Order, GN Docket No. 12-354," Dec. 2012.

[167] NOAA, "The Global Land One-km Base Elevation Project." `http://www.ngdc.noaa.gov/mgg/topo/globe.html`. Accessed: 03-25-2016.

[168] R. Tandra, S. Mishra, and A. Sahai, "What is a Spectrum Hole and What Does it Take to Recognize One?," *Proceedings of the IEEE*, vol. 97, pp. 824–848, May 2009.

[169] R. O'Connor, "Understanding Television's Grade A and Grade B Service Contours," *Broadcasting, IEEE Transactions on*, vol. 47, pp. 309–314, Sep. 2001.

[170] S. Sinanovic, H. Burchardt, H. Haas, and G. Auer, "Sum Rate Increase via Variable Interference Protection," *IEEE Transactions on Mobile Computing*, vol. 11, pp. 2121–2132, Dec 2012.

[171] B. R. Cobb and R. Rumi, "Approximating the Distribution of a Sum of Log-normal Random Variables," in *Proceedings of Sixth European Workshop on Probabilistic Graphical Models*, 2012.

[172] L. Fenton, "The Sum of Log-Normal Probability Distributions in Scatter Transmission Systems," *IRE Transactions on Communication Systems*, vol. 8, no. 1, pp. 57–67, 1960.

[173] S. Schwartz and Y. S. Yeh, "On the Distribution Function and Moments of Power Sums with Log-normal Components," *Bell System Technical Journal*, vol. 61, pp. 1141–1462, September 1982.

[174] N. Mehta, J. Wu, A. Molisch, and J. Zhang, "Approximating a Sum of Random Variables with a Lognormal," *IEEE Transactions on Wireless Communications*, vol. 6, no. 7, pp. 2690–2699, 2007.

[175] N. Beaulieu and Q. Xie, "An Optimal Lognormal Approximation to Lognormal Sum Distributions," *IEEE Transactions on Vehicular Technology*, vol. 53, pp. 479–489, March 2004.

[176] T. Yokota and M. Gen, "Solving for Nonlinear Integer Programming Problem using Genetic Algorithm and its Application," in *Proceedings of IEEE International Conference on Humans, Information and Technology*, vol. 2, pp. 1602–1609, Oct 1994.

[177] M. Altamimi and M. B. Weiss, "Enforcement and Network Capacity in Spectrum Sharing: Quantifying the Benefits of Different Enforcement Scenarios," in *Proceedings of The 41st Research Conference on Communication, Information and Internet Policy*, March 2014.

[178] R. Murty, R. Chandra, T. Moscibroda, and P. Bahl, "Senseless: A database-driven White Spaces Network," *IEEE Transactions on Mobile Computing*, vol. 11, no. 2, pp. 189–203, 2012.

[179] R. O'Connor, "Understanding Television's Grade A and Grade B Service Contours," *Broadcasting, IEEE Transactions on*, vol. 47, pp. 309–314, Sep 2001.

[180] M. Vu, N. Devroye, and V. Tarokh, "On the Primary Exclusive Region of Cognitive Networks," *IEEE Transactions on Wireless Communications*, vol. 8, pp. 3380–3385, July 2009.

[181] S. Kusaladharma and C. Tellambura, "Aggregate Interference Analysis for Underlay Cognitive Radio Networks," *IEEE Wireless Communications Letters*, vol. 1, pp. 641–644, Dec 2012.

[182] S. Shellhammer, S. Sai, T. Rahul, and T. James, "Performance of power detector sensors of DTV signals in IEEE 802.22 WRANs," in *Proc. of ACM Workshop on Technology & Policy for Accessing Spectrum*, 2006.

[183] PCAST, "Report to the President Realizing the Full Potential of Government-Held Spectrum to Spur Economic Growth," Jul 2012.

[184] A. Ullah, S. Bhattarai, J.-M. Park, J. Reed, D. Gurney, and B. Bahrak, "Multi-Tier Exclusion Zones for Dynamic Spectrum Sharing," in *Proc. of IEEE International Conference in Communications (ICC)*, 2015.

[185] M. Altamimi, M. B. Weiss, and M. Mchenry, "Enforcement and Spectrum Sharing: Case Studies of Federal-Commercial Sharing," 2013.

[186] FCC and NTIA, "Coordination Procedures in the 1695-1710 MHz and 1755-1780 MHz bands (FCC 13-185)," July 2014.

[187] J.-M. Park, J. Reed, A. Beex, T. Clancy, V. Kumar, and B. Bahrak, "Security and enforcement in spectrum sharing," *Proceedings of the IEEE*, vol. 102, pp. 270–281, March 2014.

[188] FCC, "Propagation Data Required for the Evaluation of Coordination Distances in the Frequency Range 0.85-60 GHz (Rec. ITU-R P.620-3)," tech. rep., Jul 2014.

[189] W. Baan, "Spectrum Protection Criteria for teh Square Kilometer Array," Nov 2005.

[190] "In Support of AWS-3 Transition Planning for the 1755-1780 MHz Band," tech. rep., Cisco, Aug 2014.

[191] FCC, "Second Report and Order and Memorandum Opinion and Order (FCC 08-260)," Nov. 2008.

[192] Y. Zhao, M. Anjum, and M. Song, "A New Interference Model for the IEEE 802.22 Cognitive WRAN," in *Computer Communication and Networks (ICCCN), International Conference on*, pp. 1–8, Aug 2014.

[193] M. Haenggi and R. K. Santi, *Interference in Large Wireless Networks*. Now Publishers, 1st ed., Nov 2009.

[194] T. S. Rappaport, R. W. Heath Jr, R. C. Daniels, and J. N. Murdock, *Millimeter Wave Wireless Communications*. 2nd ed., Sep 2014.

[195] O. Ibe, *Fundamentals of Applied Probability and Random Processes*. June 2014.

[196] S. Asmussen, J. Jensen, and L. Rojas-Nandapaya, "A Literature Review on Lognormal Sums," tech. rep.

[197] F. Rayal, "The Hype and Reality of Small Cells Performance," tech. rep., Cisco, Feb 2012.

[198] R. Dionisio, J. Ribeiro, P. Marques, and J. Rodriguez, "Combination of a Geolocation Database Access with Infrastructure Sensing in TV Bands," *EURASIP Journal on Wireless Communications and Networking*, 2014.

[199] RYSAVY Research, "Complexities of Spectrum Sharing: How to Move Forward," Apr 2014.

[200] K. Chen, Z. Wo, and Z. Xia, "A New Cutting Plane Algorithm for Integer Linear Programming," in *Proceedings of International Conference on Computer Science and Service System*, 2012.

[201] J. Eckstein, "Control Strategies for Parallel Mixed Integer Branch and Bound," in *Supercomputing '94., Proceedings*, pp. 41–48, Nov 1994.

[202] M. Juskauskas, J. Krivochiza, J. Aleksandravicius, K. Svirskas, B. Dzindzeleta, R. Aleksiejunas, and M. Zilinskas, "Experimental investigation of radar interference into lte system at 1800 mhz frequency band," in *21st Telecommunications Forum*, pp. 28–30, Nov 2013.

[203] K. D. Gordon, J. R. Agre, D. K. Correa, B. Brykczynski, J. K. Burton, L. H. Jones Jr., M. C. Mineiro, and B. D. A. Mussington, "A Review of Approaches to Sharing or Relinquishing Agency-Assigned Spectrum," *IDA Science and Technology Policy Institute*, Jan. 2014.

[204] MarketsandMarkets, "Global Wi-Fi Market by Business (Model Indoor Wi-Fi, Outdoor Wi-Fi, Transportation Wi-Fi), Product (Access Points, WLAN Controllers, Wireless Hotspot Gateways, Others), Service, Vertical, Region- Global Forecast to 2020," July 2015.

[205] High Efficiency (HE) Wireless LAN Task Group, "IEEE P802.11 Task Group ax." Online: http://www.ieee802.org/11/Reports/tgax_update.htm.

[206] O. Aboul-Magd, "802.11 hew sg proposed par," *Doc. IEEE802*, pp. 11–14, 2014.

[207] R. Karmakar, S. Chattopadhyay, and S. Chakraborty, "Impact of IEEE 802.11n/ac PHY/MAC High Throughput Enhancements on Transport and Application Protocols-A Survey," *IEEE Communications Surveys Tutorials*, vol. 19, pp. 2050–2091, Fourthquarter 2017.

[208] C. Ghosh, R. Stacey, *et al.*, "Random Access with Trigger Frames using OFDMA," May 2015.

[209] G. Bianchi, "Performance Analysis of the IEEE 802.11 Distributed Coordination Function," *IEEE J.Sel. A. Commun.*, vol. 18, pp. 535–547, Sept. 2006.

[210] B. Bellalta and K. Kosek-Szott, "AP-initiated Multi-User Transmissions in IEEE 802.11ax WLANs," *CoRR*, vol. abs/1702.05397, 2017.

[211] L. Lanante, H. O. T. Uwai, Y. Nagao, M. Kurosaki, and C. Ghosh, "Performance analysis of the 802.11 ax UL OFDMA random access protocol in dense networks," in *Communications (ICC), 2017 IEEE International Conference on*, pp. 1–6, IEEE, 2017.

[212] O. Sharon and Y. Alpert, "Scheduling strategies and throughput optimization for the Downlink for IEEE 802.11 ax and IEEE 802.11 ac based networks," *arXiv preprint arXiv:1709.04818*, 2017.

[213] A. I. B and T. G. Venkatesh, "Adaptive Backoff Algorithm for IEEE 802.11 DCF under MPR Wireless Channels," March 2013.

[214] M. Laddomada, F. Mesiti, M. Mondin, and F. Daneshgaran, "On the throughput performance of multirate IEEE 802.11 networks with variable-loaded stations: analysis, modeling, and a novel proportional fairness criterion," *IEEE Transactions on Wireless Communications*, vol. 9, pp. 1594–1607, May 2010.

[215] L. B. Jiang and S. C. Liew, "Proportional fairness in wireless LANs and ad hoc networks," in *IEEE Wireless Communications and Networking Conference, 2005*, vol. 3, pp. 1551–1556 Vol. 3, March 2005.

[216] G. Tan and J. Guttag, "Time-based Fairness Improves Performance in Multi-rate WLANs," in *Proceedings of the Annual Conference on USENIX Annual Technical Conference*, ATEC '04, (Berkeley, CA, USA), pp. 23–23, USENIX Association, 2004.

[217] G. Naik, "IEEE 802.11ax MU OFDMA Simulator." https://github.com/ieee80211axsimulator/muofdma, 2017.

[218] Ericsson, "Ericsson Mobility Report—on the pulse of the networked society," November 2012.

[219] R. Hedayat *et al.*, "Uplink MU Transmission and Coexistence." Online: https://mentor.ieee.org/802.11/dcn/15/11-15-0086-02-00ax-uplink-mu-transmission-and-legacy-coexistence.pptx, 2015.

[220] "CBRS Operational Security, Document WINNF-TS-0071," tech. rep., WinnForum, Jul. 2017.

[221] R. Shokri, G. Theodorakopoulos, J. Boudec, and J. Hubaux, "Quantifying location privacy," in *IEEE Symposium on Security and Privacy*, 2011.

[222] M. Clark and K. 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*, pp. 1–9, April 2016.

[223] P. Vaka, S. Bhattarai, and J. Park, "Location Privacy of Non-Stationary Incumbent Systems in Spectrum Sharing," in *2016 Proceedings of IEEE GLOBECOM*, Dec. 2016.

[224] M. E. Andrés, N. E. Bordenabe, K. Chatzikokolakis, and C. Palamidessi, "Geo-indistinguishability: Differential privacy for location-based systems," in *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*, CCS '13, (New York, NY, USA), pp. 901–914, ACM, 2013.

[225] N. E. Bordenabe, K. Chatzikokolakis, and C. Palamidessi, "Optimal geo-indistinguishable mechanisms for location privacy," in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, CCS '14, (New York, NY, USA), pp. 251–262, ACM, 2014.

[226] R. Shokri, G. Theodorakopoulos, C. Troncoso, J.-P. Hubaux, and J.-Y. Le Boudec, "Protecting location privacy: Optimal strategy against localization attacks," in *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, CCS '12, (New York, NY, USA), pp. 617–627, ACM, 2012.

[227] M. Gruteser and D. Grunwald, "Anonymous usage of location-based services through spatial and temporal cloaking," in *MobiSys International conference on Mobile systems, applications and services*, 2003.

[228] J. Freudiger, R. Shokri, and J. Hubaux, "On the optimal placement of mix zones," in *International Symposium on Privacy Enhancing Technologies*, 2009.

[229] R. Chow and P. Golle, "Faking contextual data for fun, profit, and privacy," in *WPES '09: Proceedings of the 8th ACM workshop on Privacy in the electronic society*, 2009.

[230] L. Sweeney, "k-anonymity: A model for protecting privacy," *International Journal on Uncertainty, Fuzziness and Knowledge-based Systems*, vol. 10, no. 5, pp. 557–570, 2002.

[231] A. Machanavajjhala, D. Kifer, J. Gehrke, and M. Venkitasubramaniam, "l-diversity: Privacy beyond k-anonymity," *ACM Transactions on Knowledge Discovery from Data (TKDD)*, vol. 1, no. 1, 2007.

[232] N. Li, T. Li, and S. Venkatasubramanian, "t-closeness: Privacy beyond k-anonymity and l-diversity," in *International Conference on Data Engineering (ICDE)*, 2007.

[233] N. Rajkarnikar, J. M. Peha, and A. Aguiar, "Location privacy from dummy devices in database-coordinated spectrum sharing," in *2017 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*, pp. 1–10, March 2017.

[234] C. Dwork, "Differential privacy," in *International Conference on Automata, Languages and Programming*, pp. 1–12, 2006.

[235] Z. Qin, S. Yi, Q. Li, and D. Zamkov, "Preserving secondary users' privacy in cognitive radio networks," in *2014 Proceedings IEEE INFOCOM*, pp. 772–780, April 2014.

[236] Z. Gao, H. Zhu, Y. Liu, M. Li, and Z. Cao, "Location privacy in database-driven cognitive radio networks: Attacks and countermeasures," in *2013 Proceedings IEEE INFOCOM*, pp. 2751–2759, April 2013.

[237] Z. Gao, H. Zhu, S. Li, S. Du, and X. Li, "Security and privacy of collaborative spectrum sensing in cognitive radio networks," *IEEE Wireless Communications*, vol. 19, pp. 106–112, December 2012.

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

[239] B. Kasiri, I. Lambadaris, F. R. Yu, and H. Tang, "Privacy-preserving distributed cooperative spectrum sensing in multi-channel cognitive radio manets," in *2015 IEEE International Conference on Communications (ICC)*, pp. 7316–7321, June 2015.

[240] W. Wang and Q. Zhang, "Privacy-preserving collaborative spectrum sensing with multiple service providers," *IEEE Transactions on Wireless Communications*, vol. 14, pp. 1011–1019, Feb 2015.

[241] Z. Zhang, H. Zhang, S. He, and P. Cheng, "Achieving bilateral utility maximization and location privacy preservation in database-driven cognitive radio networks," in *2015 IEEE 12th International Conference on Mobile Ad Hoc and Sensor Systems*, pp. 181–189, Oct 2015.

[242] Y. Dou, K. C. Zeng, H. Li, Y. Yang, B. Gao, C. Guan, K. Ren, and S. Li, "P2-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*, MobiHoc '16, (New York, NY, USA), pp. 321–330, ACM, 2016.

[243] B. Bahrak, "Ex Ante Approaches for Security, Privacy and Enforcement in Spectrum Sharing (Doctoral Thesis)," *Virginia Tech.*, 2013.

[244] N. G. Branko Ristic, Sanjeev Arulampalam, *Beyond the Kalman Filter: Particle Filters for Tracking Applications*. Artech Print on Demand, 2004.

[245] WinnForum, "SAS to CBSD Protocol Technical Report-B, Document WINNF-15-P-0062," tech. rep., Mar. 2016.

[246] FCC, "Report and Order (FCC GN Docter No. 12-268)," Aug. 2015.