Primary User Obfuscation in an Incumbent Informed Spectrum Access System

Cameron Makin

Thesis submitted to the Faculty of the

Virginia Polytechnic Institute and State University

in partial fulfillment of the requirements for the degree of

Masters of Science

in

Electrical Engineering

Carl B. Dietrich, Chair

Harpreet S. Dhillon

Lingjia Liu

May 11, 2021

Blacksburg, Virginia

Keywords: Primary User Privacy, Spectrum Access System Privacy, Incumbent User Privacy

Copyright 2021, Cameron Makin

Primary User Obfuscation in an Incumbent Informed Spectrum Access System

Cameron Makin

(ABSTRACT)

With a growing demand for spectrum availability, spectrum sharing has become a high-profile solution to overcrowding. In order to enable spectrum sharing between incumbent/primary and secondary users, incumbents must have spectrum protection and privacy from malicious new entrants. In this Spectrum Access System (SAS) advancement, primary users are obfuscated with the efforts of the SAS and the cooperation of obedient new entrants. Further, the necessary changes to the SAS to support this privacy scheme are exposed to suggest improvements in Primary User (PU) privacy, Citizens Broadband Radio Service Device (CBSD)-SAS relations, and punishment for unauthorized transmission. Results show the feasibility for PU obfuscation with respect to malicious spectrum sensing users. Simulation results indicate that the obfuscation scheme can deliver location and frequency occupation privacy with 75% and 66% effectiveness respectively in a 100% efficient spectrum utilization oriented obfuscation scheme. A scheme without spectrum utilization constraint shows up to 91% location privacy effectiveness. Experiment trials indicate that the privacy tactic can be implemented on an open source SAS, however environmental factors may degrade the tactic's performance.

Primary User Obfuscation in an Incumbent Informed Spectrum Access System

Cameron Makin

(GENERAL AUDIENCE ABSTRACT)

With a growing demand for spectrum availability, wireless spectrum sharing has become a high-profile solution to spectrum overcrowding. In order to enable spectrum sharing between incumbent/primary (e.g.,federal communications, naval radar, users already grandfathered into the band) and secondary users (e.g., commercial communications companies), incumbents must have spectrum protection and privacy from malicious new entrants. In this SAS advancement, primary users are obfuscated with the efforts of the incumbent informed SAS and the cooperation of obedient new entrants. Further, the necessary changes to the SAS to support this privacy scheme are exposed to suggest improvements in PU privacy, CBSD-SAS relations, and punishment for unauthorized transmission. Results show the feasibility of PU obfuscation with respect to malicious spectrum sensing users. Simulation results indicate that the obfuscation tactic can deliver location and frequency occupation privacy with 75% and 66% effectiveness respectively in a 100% efficient spectrum utilization oriented obfuscation scheme. A scheme without spectrum utilization constraint shows up to 91% location privacy effectiveness. Experiment trials indicate that the privacy tactic can be implemented on an open source SAS, however environmental factors may degrade the tactic's performance.

Dedication

To my family who have supported me throughout my years of education and to all those who have acted as an educator or mentor as I have grown as a scholar

Acknowledgments

I would like to thank Dr. Carl Dietrich for supporting me and my research efforts over the past two years. Xavier Gomez was always willing to help with server and radio troubleshooting and FAQs, many thanks. Last, I would like to thank Joseph Tolley for his advice, endless support, and cooking abilities.

Contents

List of Figures **ix**

List of Tables **xii**

1 Introduction **1**

1.1 Purpose of Research 2

1.2 Thesis Outline 3

2 Background **4**

2.1 Spectrum Policy 4

2.1.1 CBRS Rules 5

2.2 Spectrum Access Systems 7

2.3 WInnForum 10

3 Literature Review **11**

3.1 PU Privacy 11

3.1.1 PU-Responsible Privacy 12

3.1.2 SAS-Responsible Privacy 14

3.1.3 Database Driven Privacy 15

3.1.4 Comparison of Privacy Approaches 20

3.1.5 Issues with Current PU Privacy Approaches 23

3.2 Incumbent Informing Capability 23

4 Proposed Solution **26**

4.1 Advanced SAS Requirements 26

4.2 PU Privacy Tactic 28

4.3 Proposed Obfuscation Schemes 35

5 Methodology **38**

5.0.1 Materials Used 38

5.0.2 Implementation and Development Process 43

5.0.3 Simulation 54

5.0.4 Analysis 54

5.0.5 Limitations 57

6 Results **62**

6.1 Simulation Results 62

6.2 Experiment Results 71

6.3 Discussion 74

6.3.1 Simulation Results 74

6.3.2 Experiment Results 76

6.3.3 Limitations / Edge Cases 77

7 Conclusion **80**

7.1 Future Work 80

7.1.1 Malicious User Transmission Interference 80

7.1.2 ASAS PU Obfuscation Routine - Time Obfuscation 82

7.1.3 Multi-Tactic Primary User Privacy 83

7.1.4 Spectrum Access System Development 83

7.2 List of Contributions 84

7.2.1 Virginia Tech Spectrum Access System 84

7.2.2 Primary User Obfuscation Schemes 84

7.2.3 Publications 85

Bibliography **86**

List of Figures

2.1 3.5 GHz CBRS Band Allocation 5

2.2 3.5 GHz CBRS Band PAL Channels 7

2.3 Generic SAS Architecture 8

2.4 WInnForum SAS-CBSD Protocols 9

3.1 Incumbent Informing Capability System Architecture 25

4.1 Example of Spectrum Utilization in PU Obfuscating Scheme 29

4.2 Relative Locations of PU, SUs, and MU in PU Location Privacy via SU Transmission Scheme 31

4.3 Received Power from the Perspective of the MU 32

4.4 Incumbent Informed SAS Flowgraph 33

4.5 Obfuscation Routine Flowgraph 34

5.1 CORNET Testbed Architecture 39

5.2 2 Stacked Ettus Research B210s 40

5.3 GNU Radio Flowgraph for a USRP Capable of TX 44

5.4 GNU Radio Flowgraph for a USRP Capable of RX 44

5.5 GNU Radio Flowgraph for a USRP Capable of Simultaneous TX and RX . . 45

5.6 SAS-CORNET Architecture 45

5.7 High Level Node Location Relationship 49

5.8 Experiment USRP Locations in Kelly Hall 50

5.9 MU Sensing PU without SU-Aided Obfuscation 51

5.10 MU Sensing PU with Partial SU-Aided Obfuscation 52

5.11 Node Layout for Two SUs 53

5.12 Typical USRP Installation Environment (ceiling tiles removed) 59

6.1 Obfuscation Scheme 1 in Simulation 63

6.2 Obfuscation Scheme 2 in Simulation 64

6.3 Obfuscation Scheme 3 in Simulation 65

6.4 Obfuscation Scheme 4 in Simulation 66

6.5 SU Utilization between All Four Schemes 67

6.6 Spectrum Sharing Efficiency between All Four Schemes 68

6.7 Frequency Obfuscation Efficiency between All Four Schemes 69

6.8 Location Obfuscation Efficiency between All Four Schemes 70

6.9 Obfuscation Scheme 1 in USRP Experiment with One SU 71

6.10 Obfuscation Scheme 1 in USRP Experiment with Two SUs 72

6.11 Obfuscation Scheme 2 in USRP Experiment with One SU 72

6.12 Obfuscation Scheme 2 in USRP Experiment with Two SUs 73

6.13 Broadband Service over SAS – End User Access would be managed by the service provider, not the SAS 79

7.1 SAS-induced MU Communications Jamming Basestation Map 81

7.2 MU Jamming Concept 82

List of Tables

1 Acronyms and Abbreviations xiii

1 Acronyms and Abbreviations xiv

1 Acronyms and Abbreviations xv

3.1 Summary of Reviewed Literature 17

3.1 Summary of Reviewed Literature 18

3.1 Summary of Reviewed Literature 19

3.1 Summary of Reviewed Literature 20

3.2 Comparison of Privacy Schemes 22

6.1 Comparison of Simulated Privacy Schemes 75

Table 1: Acronyms and Abbreviations

Acronyms	Name	Description
AOA	Angle of Arrival	The angle in which a signal is received
ASAS	Advance SAS	The name of the SAS proposed in this text with the additional features that are not currently required by FCC guidelines
BS	Basestation	A transmitting station, typically housing an antenna
CBRS	Citizens Broadband Radio Service	Spectrum band from 3550 - 3570 MHz in the United States reserved for spectrum sharing
CBSD	Citizens Broadband Radio Service Device	A node or network of nodes that operate with Priority or General Authorized Access in the CBRS
CORNET	Cognitive Radio Network Testbed	A testbed including a server, network-attached USRPs, and software that all enable wireless research
CR	Cognitive Radio	A radio that has the ability of spectrum sensing and RF parameter modification
CRN	Cognitive Radio Network	A network of linked cognitive radios
DoD	Department of Defense	The United States Department of Defense
DSS	Dynamic Spectrum Sharing	A method of spectrum sharing where users occupy available spectrum when the opportunity arises
EIRP	Effective Isotropic Radiated Power	A measurement of the transmit power of a radio
ESC	Environmental Sensing Capability	A system that can gather and delivery spectrum occupancy data
FCC	Federal Communications Commission	United States agency that creates and enforces spectrum policy
FFT	Fast Fourier Transform	An algorithm that allows time domain spectrum information to be converted to frequency domain
FPGA	Field Programmable Gate Array	A device that has re-programmable hardware for in-field modification

Table 1: Acronyms and Abbreviations

Acronyms	Name	Description
FSS	Fixed Satellite Service	Radio communication between a satellite and one or more fixed locations
GAA	General Authorized Access	The permission level associated with general users with SAS approved CBSDs
GRC	GNU Radio Companion	Open source software suited for visual programming of SDRs
IIC	Incumbent Informing Capability	A channel of communication where incumbent users may notify SASs of intended spectrum utilization
ISM	Industrial, Scientific, and Medical	A band utilized for over-the-air research
JS	JavaScript	Programming language used for web related software
MU	Malicious User	A SAS user or unregistered receiver that operates with the purpose of causing harm
MUSIC	MUltiple SIgnal Classification	An algorithm used for radio direction finding
NTIA	National Telecommunications and Information Administration	United States Department of Commerce agency that servers as the President's advisor for telecommunications related policy
PAL	Priority Access Licensee	A user that carries a Priority Access License
PIR	Private Information Retrieval	Accessing of sensitive data from the spectrum database
PU	Primary User	A spectrum occupant, typically governmental or incumbent, with the highest spectrum priority
PSD	Power Spectral Density	A measurement of signal power with respect to the frequency(ies) transmitted
QoS	Quality of Service	A phrase utilized to refer to how well a service is performing
SAS	Spectrum Access System	An automatic frequency allocator
SDR	Software Defined Radio	A device with configurable RF hardware

Table 1: Acronyms and Abbreviations

Acronyms	Name	Description
SINR	Signal to Interference plus Noise Ratio	Measurement describing the ratio of signal received and noise plus interference
SU	Secondary User	Any user of the SAS that does not have PU status
USRP	Universal Software Radio Peripheral	A device sold by Ettus Research that contains SDR technology with other supporting hardware
VTSAS	Virginia Tech SAS	Virginia Tech's Open Source SAS server
WInnForum	Wireless Innovation Forum	Organization that promotes wireless technology advancements

Chapter 1

Introduction

As a result of rapid technological innovation, wireless technology is becoming more feasible in all devices. Cisco reports indicate 29.3 billion Internet of Things (IoT) devices will have mobile connectivity by the year 2023 [3]. As wireless devices are created and mass-produced, spectrum availability decreases. Devices must compete for spectrum availability. In densely populated areas, many wireless devices may demonstrate poor quality of service (QoS) due to spectrum overcrowding and rising demand for spectrum.

While the Federal Communications Commission (FCC) has enabled Dynamic Spectrum Sharing (DSS) in bands with governmental, commercial, and general users, these bands are limited in frequency and may only provide marginal benefits as a result of spectrum sharing. In an ideal case, the entirety of typically vacant but federally allocated spectrum would utilize a sharing mechanism to greatly increase spectrum availability and utilization for all other users. To reach this ideal case, the incumbent users of various spectrum bands must be guaranteed privacy and protection from the new entrants that are provided this opportunity.

As a result, SAS architectures are being developed commercially and in research settings.

With SAS interface documentation provided by the Wireless Innovation Forum (WInnForum), along with an open-source SAS to develop with, SAS research and development becomes feasible. The technical specifications for data reported to the SAS by a CBSD are enough to create a functional automated frequency coordinator, but there are ways to help the SAS have extended functionality.

Increasing incumbent, or PU, privacy is a requirement before extending the bands in which spectrum sharing solutions are implemented. PU obfuscation, a subset of PU privacy techniques, may benefit from the aid of the new spectrum sharing system entrants, named Secondary Users (SUs). In this text, a Advanced SAS (ASAS) architecture is implemented where SUs will support PU obfuscation by transmitting over adjacent bands with idle SUs. Under the discretion of the controlling SAS, SUs will extend their permissions with the SAS to allow provide transmission control to deliver PU obfuscation.

1.1 Purpose of Research

The research efforts conducted for this text deliver two benefits to the academic community. The first delivered benefit stems from a lack of an open-source SASs. A SAS client has been built that follows WInnForum and FCC specifications to the fullest extent possible with the provided resources. This open-source client provides a foundation for other researchers to build similar clients for their Software Defined Radio (SDR) networks. Further, with an enabling client, the Virginia Tech Spectrum Access System (VTSAS) has been tested and is suitable for cloning on the GitHub repository. The second deliverable is a novel PU obfuscation scheme. The purpose of any PU obfuscation scheme is multi-dimensional. The imminent effect of PU obfuscation is increased PU privacy. Incumbent / PUss that offer shared spectrum have the expected privilege of maintaining transmission and location

privacy. PU obfuscation in this text proposes a novel method of keeping PU operation parameters private. A result of increased PU privacy may yield greater effects on DSS on different spectrum bands that are currently unavailable for shared use. Should 3.5 GHz CBRS sharing become a reliable and safe band for PU occupancy, this may unlock more spectrum for sharing, which may increase spectrum availability for SUs and result in more efficient spectrum usage for all.

1.2 Thesis Outline

In this Thesis, Chapter 2 introduces fundamental federal policies, systems, and organizations that are relative to the research conducted. Chapter 3 provides a survey of current PU privacy techniques along with a comparison table of the approaches as well as the approach proposed in this text. Chapter 4 describes the proposed ASAS features, a PU privacy tactic, multiple PU obfuscation schemes, and methodology of implementing the privacy tactic. Chapter 6 shows simulation and experiment results. Section 6.3 includes discussion about the simulation and experiment results along with exposed limitations of the tactic. The final chapter, Chapter 7, concludes the text and proposed future work to further the capabilities described in this text.

Chapter 2

Background

2.1 Spectrum Policy

The FCC enforces strict spectrum band occupancy rules and guidelines to enforce and manage spectrum users, however, the use of static boundaries and rules for spectrum allocation is showing its weakness as spectrum demand grows [13]. The FCC has addressed the need for increased spectrum availability. One of its latest initiatives includes the recent auctioning of 280 MHz of the C-band (3700-4200 MHz) for 5G cellular communications, moving the existing satellite communications to the upper section of the band [12]. Of greater importance, in 2015 the FCC adopted rules for spectrum sharing in the 3.5 GHz band (3550-3700 MHz) [11]. The 3.5 GHz band is tokened Citizens Broadband Radio Service (CBRS). The CBRS rules are detailed in the FCC's Title 47 Part 96 document [14]. The rules include information on permitted spectrum behavior, incumbent protection, priority access, general authorized access, SAS requirements, and Environmental Sensing Capability (ESC) requirements.

2.1.1 CBRS Rules

Incumbent User Protection

FCC Part 96 Subpart B contains the requirements for incumbent user spectrum protection [14]. Incumbent users are either federal entities, Fixed Satellite Service (FSS) operators, or grandfathered wireless broadband licensees. Grandfathered wireless broadband licensees are authorized to transmit over the frequencies 3650 - 3700 MHz whereas the rest of the PUs operate over the entire 3.5 GHz band. These are all given PU status to the system since they all carry the highest priority for spectrum access. The SAS is responsible for ensuring that there is no SU interference upon these users, thus protecting their spectrum access availability.

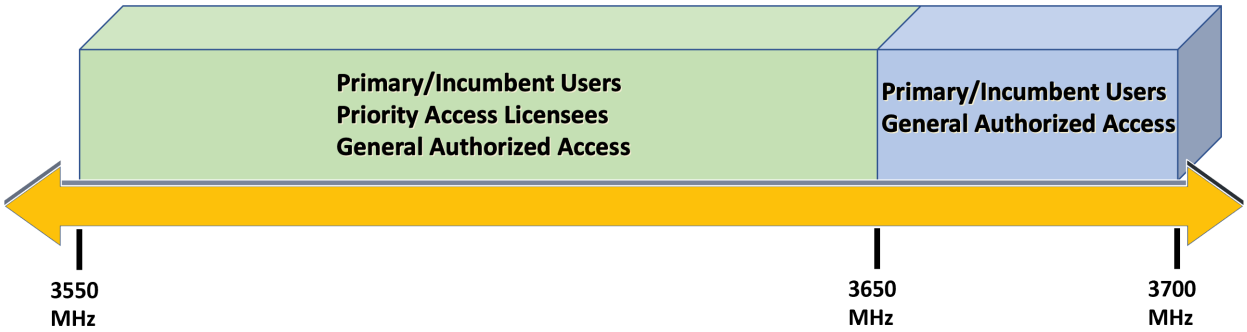

Figure 2.1: 3.5 GHz CBRS Band Allocation

PU protection includes channel vacancy timing and signal interference management. To protect the availability of a channel, all users except for PUs must have the ability to be notified to vacate a channel and do so in a timely manner. CBSDs are given 300 seconds from the moment PU presence is detected to turn off transmission or move to a different channel. This feature ensures that PUs are given spectrum on time, while also giving the SUs an appropriate amount of time to either suspend transmission or alter their frequency parameters. Interference management is a byproduct of revoking spectrum access to SUs. If

SUs are not transmitting, then they are not interfering with the PU.

Priority Access

The CBRS rules detail two types of spectrum channel privileges for SUs: Priority Access and General Access. The 3.5 GHz CBRS band is separated into two sections: 3550 - 3650 MHz and 3650 - 3700 MHz. The former 100 MHz region is available to both Priority Access Licensees (PALs) and General Authorized Access (GAA) users. The latter 50 MHz is only available to the GAA class of SUs. PALs are users who have completed a Priority Access License application with the FCC. To obtain a Priority Access License, a user must provide qualifications, testify the ability to serve the public by being a license holder, register CBSDs that are SAS compliant, along with other rigorous requirements.

Upon earning a Priority Access License, a PAL earns a higher priority than a GAA user in the 3550 - 3650 MHz band. While not as high on the priority scale as a PU, a PAL may have some priority over a general user. This advantage works for seven of the ten channels (10 MHz bands) within the 3550 - 3650 MHz band. There should not be more than seven PALs occupying channels in the 100 MHz band described. This limitation ensures that GAA users have an opportunity to utilize spectrum as well, while also providing some bandwidth for PALs. Additionally, no single PAL may aggregate more than four PAL channels at any given time. PALs may participate in competitive bidding to rank higher in their inner-tier. These funds are collected by the FCC.

In the remaining 50 MHz (3650 - 3700 MHz), PAL users are forbidden, however, GAA users are allowed to access this spectrum. GAA users are allowed to request spectrum and if no other user is occupying it, the channel is granted the GAA user. GAA users are not guaranteed interference protection from any other higher tiered user, and GAA users must

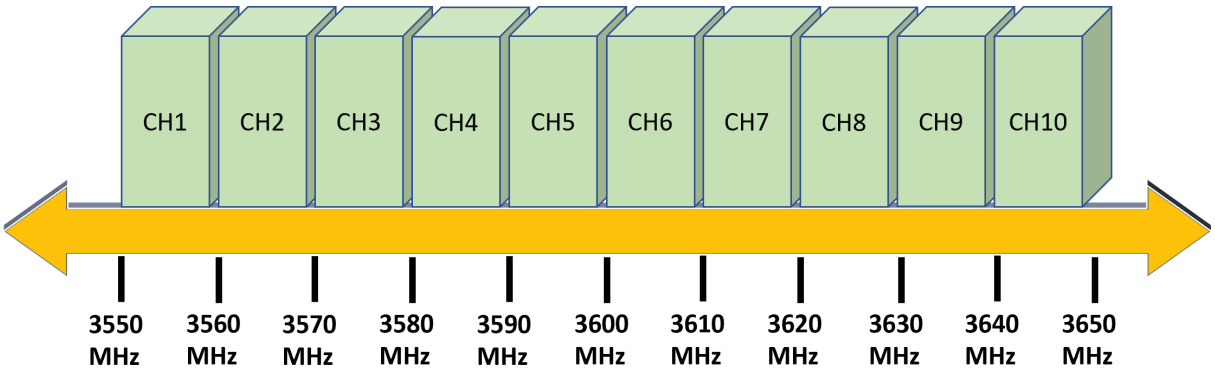

Figure 2.2: 3.5 GHz CBRS Band PAL Channels

make all efforts to not interfere with PALs or PUs.

2.2 Spectrum Access Systems

The ruleset governing the 3.5 GHz CBRS band extensively illustrates the use of an automatic frequency coordinator, also known as a spectrum access system (SAS) [11]. The SAS is a tiered system that allows for spectrum access and utilization should available spectrum exist. Traditionally, the 3.5 GHz band is allocated for fixed-satellite, federal radiolocation, federal aeronautical radionavigation, and fixed mobile use [13]. Currently, the FCC recognizes Google, Commscope, Amdocs, Sony, and Federated Wireless as SAS providers [26].

The SAS is the system that CBSDs must directly communicate to in order to be granted spectrum access. In order for a SU to be allowed to transmit over the CBRS band, it must first send the SAS a registration request. Once they are registered, the SU may send a spectrum inquiry request. This is a query that pulls from the spectrum database and relays the query results back to the SU. The spectrum inquiry request allow SUs to see what available channels there are for use. If the ESC determines there is a PU in the inquired

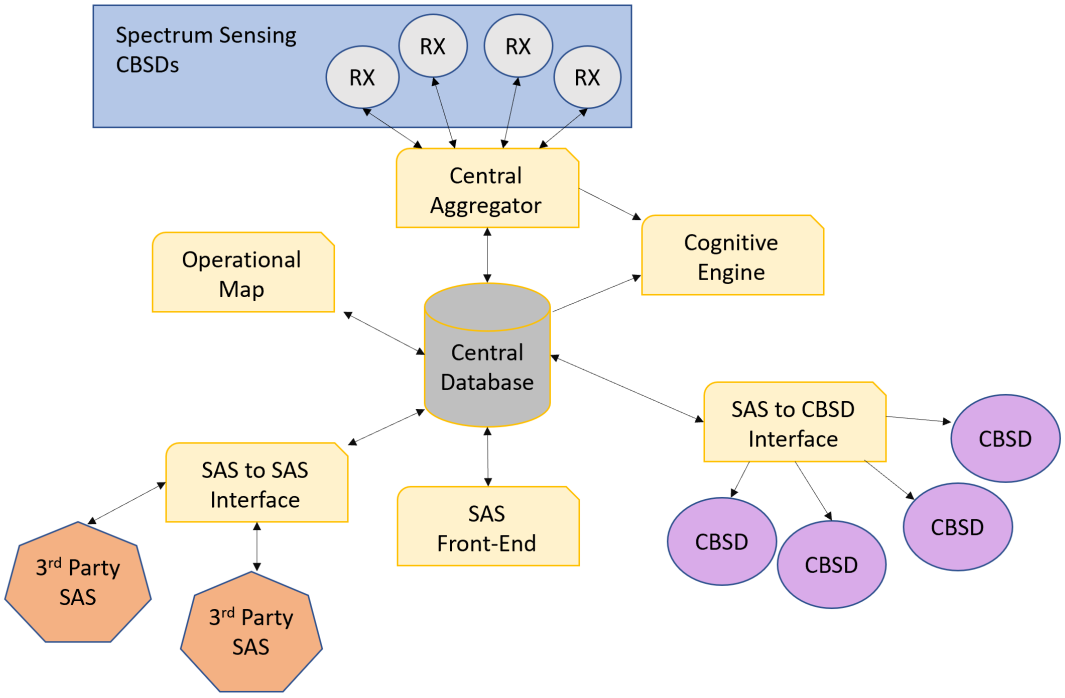

Figure 2.3: Generic SAS Architecture

spectrum, or if another user is currently granted in the channel, then the inquiry will notify the CBSD of the occupied channel.

Next is a grant request. A grant request is a formal message sent to the SAS to receive transmission permission. If the SAS provides a successful grant response, then the SU may continue to accessing the spectrum. While a CBSD may be granted, that does not mean it is allowed to transmit. Before the CBSD may access the spectrum, they must send a Heartbeat request and receive a successful heartbeat response. Then after initiating the first heartbeat, the SU may transmit. As long as the grant is active and the SU desires the spectrum, the heartbeat protocol is repeated.

The CBRS band, enabled by an automatic frequency coordinator, is a promising area of interest for those who want to begin the development of systems that defy the rules of static spectrum allocation and push the boundaries of spectrum availability.

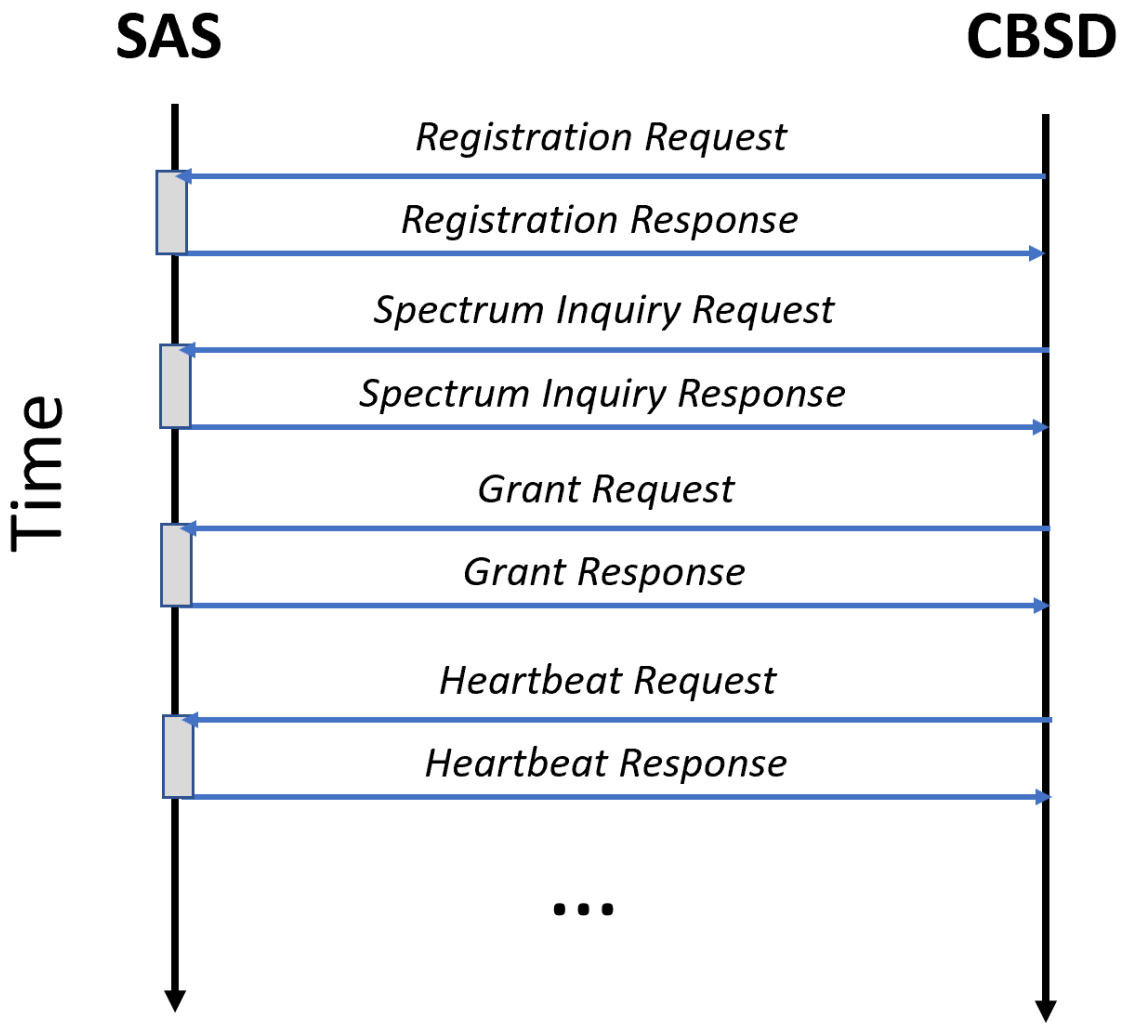

Figure 2.4: WInnForum SAS-CBSD Protocols

2.3 WInnForum

Due to the high interest in commercial, academic, and governmental organizations for the CBRS band, a commonplace for wireless innovation must exist. Introduce the WInnForum [22]. The WInnForum is an organization dedicated to communicating CBRS standards and advancements in spectrum sharing policy. High profile wireless providers (e.g.,, Verizon, AT&T), universities (e.g., Virginia Tech, University of Colorado Boulder), research and development companies (e.g., Qualcomm, Ericsson), and several more are all members of the WInnForum as the organization fosters a commonplace to put competition aside and place innovation first [24]. The WInnForum provides streamlined documentation for SAS specifications and SAS clients, called a CBSD [23]. The documentation provided by the WInnForum aligns with FCC requirements, which makes the WInnForum a reliable source for streamlined spectrum sharing literature.

Chapter 3

Literature Review

3.1 PU Privacy

Primary/Incumbent User Privacy is an essential requirement for any spectrum sharing system. Due to the nature of Department of Defense (DoD) and other federal agencies that would earn PU status, their information must remain secretive. Privacy may be manifested in multiple ways. Privacy includes basestation (BS) geographic location, spectrum frequency occupation, and spectrum access behavior. All of these, if detected by a malicious user (MU), would render all DSS opportunities useless and the FCC would be required to revoke all spectrum sharing privileges.

There are many published texts surveying and/or proposing techniques. Some techniques delegate actionable items to increase PU privacy onto the PU, while others place PU privacy responsibility onto the SAS. These methods may be mutually exclusive, allowing an overlap in techniques with a possible increase in privacy effectiveness.

3.1.1 PU-Responsible Privacy

In these privacy methods, the PU is responsible to take certain actions that the SAS may not be able to do.

Frequency Hopping

Frequency hopping is a very elementary technique that the PU can utilize. Traditionally, With spectrum sensing capability, frequency hopping may prove effective in avoiding overcrowded channels [17]. In the case of a PU, the goal is not only to reduce interference but also to strengthen privacy. Should a PU decide to utilize frequency hopping, privacy can be strengthened by hopping to random channels. A study has shown that PU behavior may be detected, especially when a PU is frequency hopping in a simplistic manner (i.e. hopping into the closest available channel in sequential order). If a PU decides to frequency hop, it is suggested to utilize a randomization method to mask its behavior from entities attempting to study PU frequency occupation [7].

The issue with this privacy technique is that frequency hopping requires a robust transmitter to receiver communications channel describing the hopping behavior. The receiver will need to be aware of the channel the transmitter plans on moving to and at what time. This overhead introduces a tradeoff between privacy and system simplicity. If the PU decides to change operating frequency, then the receiver must keep up with the movements of the transmitter which may prove demanding on radio hardware. Assuming the RF hardware is software defined or easily flexible, there is also overhead in data packets. More bits will need to be sent to the receiver describing the transmitters intentions, and these bits will also demand a redundancy protocol to ensure they are not lost in transmission, which increases the communications link complexity. Additionally, if the receiver and transmitter are able to

communicate transmitter movements, the latency from the intention transmission, reception, and processing, may not be quick enough to react to the change. Modern communications still show signs of struggling to stay in sync when multiple unrelated clock sources are utilized for precision timing.

PU Data Obfuscating

Clark and Psounis [6] features a privacy method that utilizes a codebook to report PU status to SUs, without providing sensitive PU information. The codebook is meant to be a layer of obfuscation that provides the SU enough information on the PU to take appropriate action but does not reveal the exact details regarding the whereabouts of the PU. The implementation of the codebook occurs at the PU, prior to database entry. The codebook input is the PUs true operating parameters, and the result of the codebook is a set of obfuscated data parameters. The result is then provided to the SAS for database entry.

Li et al. [18] address PU privacy with regard to database contents and SAS memory storage as well.

PU-Receiver Location Broadcasting

Another studied privacy method includes PU receiver and SU communication [20]. In an effort to minimize interference experienced by PUs, Radio-frequency identification (RFID) tags are mounted onto PU receivers. The RFID tags are then to alert nearby SUs of the PU receiver presence. The RFIDs can control SU power output to ensure the transmission power of the SU does not interfere with the PU receiver.

In an effort to minimize the reach of PU signal, Rajpoot and Tripathi have proposed that PU receivers communicate data reception analytics to the PU transmitters. By informing

the PU transmitter about the reception quality at the receiver, the transmitter is then proposed to alter its transmission parameters to limit the reach of the transmitted signal. Beamforming and reducing transmitted power are two methods of restraining a signal from reaching beyond its endpoint. By doing so, this limits the range in which a MU may attempt to receive PU data.

PU-Responsible Limitations

The issue with the proposed PU responsible solutions is the heavy burden that may be placed upon the PU. There are several assumptions made about the PU's capabilities, and considering the wide variety of incumbent users on the 3.5 GHz band, it is not feasible to demand these from them when SAS-centric PU privacy schemes exist.

3.1.2 SAS-Responsible Privacy

Ideally, PU privacy would be respected by the SAS. Since PUs are the highest priority users due to being grandfathers spectrum users or high priority government users, a SAS that is allowing spectrum sharing to less prioritized SUs, the SAS should make efforts for PU privacy along with protection. There are several unique proposed PU privacy techniques a SAS may adopt. With enough motivation, many of these may techniques may be used in the same system, which may result in greater PU privacy than by utilizing only one of the techniques.

Random SU Allocation

One SAS controlled PU privacy technique obscures PU spectrum usage by randomizing SU allocation [5]. SUs are not given information on occupied channels in this scheme.

Restricting such spectral information, and by randomly assigning channels to SUs, there would be difficulty for a MU to gain knowledge on where a PU may be operating. The cost of such system however is non-trivial. By not allowing SUs to select their channel, this may restrict SU ability for operation should they desire a specific channel for any reason. Further, if a PU enters a SAS region and the SAS must kick off the SU for the PU, then there can be implicit knowledge of PU activity, and this can be modeled over time to characterize PU behavior.

Entry Encryption

Dou et al. [10] utilize encryption when delivering sensitive information regarding PU operation from the SAS to SUs. Their spectrum allocation process targets PU privacy concerns by ensuring that communicated data from the SAS is encoded as to not publicly announce PU data over transmission. The encryption is known by all registered users so upon reception the intended receiver can decrypt the message. This tactic aids PU privacy by ensuring that no sensitive PU data is transmitted openly for any non-registered user to intercept and attempt to decipher.

3.1.3 Database Driven Privacy

SUs have two ways of receiving spectrum information: 1) they may send a spectrum inquiry request to the SAS or 2) they may use their receivers to observe the spectrum in their region. The database driven method may prove useful since it is full of crowdsourced data which the SU receiver may not be able to sense. However, the database also includes the registration information of SUs and potentially local PUs. Allowing SUs to query this database may be dangerous since location information is sensitive. Query attacks have proved effective in

stealing sensitive data so to maintain a standard of user privacy database architecture and query format must be robust to fight malicious attacks.

False PU Entries

To combat malicious study of PU activity and behavior, there have been studies that use false PU entries in the SAS centralized database [1, 4, 9, 21]. These are entries that are generated by the SAS which makes it appear as if PU is operating over a channel when in reality no PU is utilizing the spectrum. By doing this, it helps obscure PUs that may be operating in the SAS region in different channels. Inserting false PUs may throw off MUs who are studying PU behavior. The randomization of time and channel for the false PU data may thwart the conclusions made by the MUs studying PU behavior. The downfall to this method is that it makes extra spectrum unavailable to users, and spectrum sensing SUs may be able to detect the unoccupied spectrum and raise questions about the SAS's integrity when responding to the spectrum requests.

Multiple Database Servers

Considering the database that drives SAS functionality, Grissa et al. seek to ensure PU privacy is strengthened from malicious database users as well as malicious databases. This database-centric approach abandons the use of a single database for PU and SU record keeping. Multiple database technologies are implemented in this proposal. Authors acknowledge the weakness of single-server private information retrieval (PIR) and harness mulit-server PIR techniques to keep the location data of both PUs and SUs private [16]. As a result of testing the proposed database system on a cloud service, it is shown that Cognitive Radio Networks (CRNs) achieve faster end-to-end delay than in a traditional single-server PIR

architecture.

Limited Database Queries

To limit the amount of spectrum information a SU may obtain from a SAS over a given amount of time, Ben Mosbah et al. [2] provide a study that delivers an analytic model for limiting spectrum inquiries from a SU. The limitation of inquires is to aid in inference attacks, simply by limiting the amount of database access a SU may get. This approach of limiting SU interaction with the spectrum database provides a good basis for privacy approaches.

Privacy verses Utility Tradeoff Protocol

Zhang et al. [27] have produced a privacy-preserving protocol to ensure PUs, as well as SUs, have location privacy from the database. Their protocol named Utility Maximization protocol (UMax) preserves privacy by allowing PUs and SUs to control their levels of desired privacy and also optimize their transmit levels consequently. The PU and SU geographic locations are obscured by reporting a larger region in which the user may be present.

Table 3.1: Summary of Reviewed Literature

Privacy Technique	Description	Advantages	Disadvantages
PU-Responsible			
Frequency Hopping	PUs change transmission frequency sporadically and intentionally	If a MU is attempting to trace the source of a signal at a specific frequency, by changing frequency, the MU loses track of the signal it is attempting to trace	Requires overhead in coordinating the frequency jumps between the PU transmitter and receivers. Also requires the PU to have the infrastructure to enable frequency hopping.

Table 3.1: Summary of Reviewed Literature

Privacy Technique	Description	Advantages	Disadvantages
PU Data Obfuscating	PU operating parameters are altered by the PU. The details of true operation parameters / private data is never entered into the database, but information that would otherwise ensure SUs are not interfering with the PU is included	PU operating parameters can be manipulated however the PU pleases to provide any desired level of obfuscation	By entering obfuscated data into the database, SUs are given less knowledge on the PUs actual spectrum demands, and can limit available spectrum for shared usage.
PU-RX Location Broadcasting	PU receivers have attached RFID tags that allow SUs to know not to disturb (transmit) the receiver if operating in a nearby region	This provides a low complexity method of informing SUs to nearby PU receivers. Does not require database inquiries.	Not all PUs are emitting for an intended receiver (e.g., radar simply emits and receives the bounced back signal). SUs that are malicious are given PU receiver location information once they find the RFID tags.
SAS-Responsible			

Table 3.1: Summary of Reviewed Literature

Privacy Technique	Description	Advantages	Disadvantages
Random SU Allocation	When SUs request spectrum, the SAS grants the SU a random channel. This scheme does not provide SUs with channel occupancy information.	Without providing the SU the spectrum occupancy information and by randomly allocating spectrum to them, it is made more difficult for an MU to infer any PU behavior.	By randomly allocating spectrum, the SU may not get the preferred channel they requested. Also, if a PU enters the SAS region and demands an occupied band, then the SU can make an inference that they have had their grant suspended due to an entering PU requesting their band.
Data Encryption	Private data is encrypted before sending to inquiring SU	When transmitting Pu information to the SU, the encryption ensures that the PU data is not easily intercepted	This assumes that registered SUs cannot be malicious
Database-Driven			
False PU Entries	SAS enters false PU reports into the database	This obfuscates truthful PU usages since MUs cannot make inferences about the channels if the SAS is injecting false entries	The dishonest nature of the SAS may have SUs raise questions as to why a channel is unavailable, when utilizing its (SU) own receiving equipment, it does not detect activity in the channel.
Private Information Retrieval (PIR) with Multi-DB	Instead of a single database architecture, Mulit-DB architecture is proposed	Mulit-DB architectures have been proven to be faster than single-DB systems. Private Information Retrieval is known to be more robust in Mulit-DB systems compared to Single-DB	Requires consideration of DB architecture which may slow momentum in spectrum sharing initiatives.

Table 3.1: Summary of Reviewed Literature

Privacy Technique	Description	Advantages	Disadvantages
Limited DB Queries	SUs are only allowed to query the spectrum DB so often	By limiting the amount of information the SUs have access to, it makes it more difficult for MUs to create inferences on spectrum occupancy and PU behavior.	Mobile SUs must query the DB more often, especially if they are travelling at high speeds. Limiting queries may make it difficult for mobile SAS users to benefit from the shared system
Buffered Location Data in DB	Locations logged have a buffer around them	Low-complexity way of distorting location data for both PU and SUs	Reduces utility since a larger buffer means less reusable spectrum for that area

3.1.4 Comparison of Privacy Approaches

Table 2 outlines the capabilities and limitations of the different proposed privacy schemes. The following traits that compare the schemes original from important design constraints when considering SAS modifications:

Places Complexity Burden on PU - This trait either places the burden of privacy upon the PU or the SAS. Ideally, the burden and complexity of PU privacy would belong to the SAS. This is due to unknown PU capabilities. While some PUs may be able to abide by the required changes for the privacy technique, it cannot be assumed that every PU has the capability. If the burden of privacy was placed on the PU, then there would be significantly less incentive for incumbents to allow spectrum sharing.

Limits SU Privileges - This trait limits the amount of functionality the SU may utilize as compared to the original SAS. For example, in current SAS architecture, SUs have the ability

to inquire about spectrum as well and request to operate over a specific band. Some of the previously proposed schemes from the literature review limit these features. It would be more suitable if SAS advancements did not revoke current SU privileges.

Makes SAS Appear Truthful / Faulty - In the False PU DB Entry scheme proposed by several authors, while the concept provides a valid obfuscation method, there is a cascading effect that these entries may have upon SUs/MUs. In the case where a SU inquires the DB regarding access to a certain band, they are under the pretense that if the spectrum is available, then their grant would be provided. However, in the event that an SU inquires about a channel, and that channel happens to be one where a false PU is logged, the SU is rejected the grant. In this scenario, the SU may simply begin spectrum sensing the inquired channel, and suddenly realize the channel is vacant. This would foster confusion for the SU. Either: the SU receiver hardware is malfunctioning, or the SAS may have provided an invalid inquiry response. In the latter case, the SU may lose faith in the operation of the SAS and report to the SAS administrators regarding the conflicting SAS vs SU spectrum occupancy observation. Another scenario may unfold as follows: an MU inquires about spectrum and is returned with a false PU occupied channel response. The MU may also sense spectrum and realize that the SAS has mistakenly, or intentionally, provided an invalid response. The latter case of an intentionally invalid response may have the MU suspect that the SAS has flagged it as an MU. This may prompt the MU to deregister and reregister with the SAS under a different set of falsified credentials. This latter case costs the SAS its knowledge of a known MU, and it may take the SAS an extended period of time to re-detect the MU as malicious.

Obfuscates PU from Spectrum-Sensing MU - This trait entails that PU obfuscation is resistant to a network of colluding, spectrum sensing MUs. Radiolocation with PU signals is made more difficult in these schemes that inherit this trait.

May Degrade Spectrum Availability - This trait states that the approach may create an environment where SUs may not have access to non-PU occupied spectrum. This may be either because the spectrum database is limiting the amount of available spectrum, or the obfuscation may utilize available spectrum. Additionally, methods such as frequency hopping may limit spectrum availability since frequency hopping creates an unknown behavior in spectrum occupancy. This may render all otherwise available spectrum unavailable since it is unknown how frequent the PU will disturb the granted SUs.

Table 3.2: Comparison of Privacy Schemes

Privacy Technique	Places Complexity Burden on PU	Limits SU Privileges	Makes SAS Appear Untruthful / Faulty	Obfuscates PU from Spectrum-Sensing MU	May Degrade Spectrum Availability
ASAS	**NO**	**NO**	**NO**	**YES**	YES
Frequency Hopping	YES	**NO**	**NO**	**YES**	YES
PU Data Obfuscating	YES	YES	YES	NO	YES
RX RFID	YES	**NO**	**NO**	NO	YES
Random SU Allocation	**NO**	YES	**NO**	NO	**NO**
Data Encryption	**NO**	**NO**	**NO**	NO	**NO**
False PU DB Entries	**NO**	YES	YES	NO	YES
Mulit-DB PIR	**NO**	**NO**	**NO**	NO	**NO**
Limited DB Queries	**NO**	YES	**NO**	NO	**NO**
Buffered Location Data in DB	**NO**	YES	YES	NO	YES

3.1.5 Issues with Current PU Privacy Approaches

Of all reviewed SAS-responsible PU privacy approaches, none have created a real-world approach to thwarting MUs from determining the spectrum in which the PU is operating or utilizing radiolocation to determine PU location. The database-driven privacy models are promising for delivering location privacy, but these authors have not addressed PU spectrum occupancy privacy – recall that the database may include the PU's frequency selection along with its geographic location. It is imperative that the PU spectrum occupation be kept private. MUs with information on the PU's spectrum occupancy have an advantage to better study PU behavior or intercept PU signals. Behavioral studies by a MU may lead to an attack on the PU's operation via signal jamming since the MU has knowledge of the PU's typical operation. Additionally, with knowledge of the PU's channel of operation, a MU may be inclined to intercept the signal and attempt to decode the secret messages being transmitted by the incumbents, most importantly the DoD.

The largest issue facing all previously proposed privacy schemes is the trait acknowledging MU spectrum sensing. Regardless of the practices used by all the schemes (except frequency hopping), there is nothing stopping a colluding network of MUs from spectrum sensing and utilizing radiolocation to identify PU basestation location.

3.2 Incumbent Informing Capability

To date, there are FCC regulations that require a SAS to be able to detect PU activity in the operating region. The rules that enforce this are instated as a measure to ensure PU spectrum protection. Since the PUs have no obligation to announce their occupancy intentions, the SAS must reactively ensure the channel the PU occupies is clear of SU activity.

This model of utilizing a reactive system verse a proactive system has cascading consequences that are limiting the potential of a more robust automated frequency allocator. In the traditional reactive system, a PU would simply begin transmission and then the SAS would be responsible for any interfering SUs that may be granted on the same spectrum as the PU. There is a 300 second grace period between when the SAS detects a PU and when all interfering SUs must vacate the spectrum. This 300 second buffer is a result of a reactive approach to PU protection.

Enabling the transition from a reactive to a proactive system, one fundamental change in architecture is required; PUs must have a secure and independent channel of communication to the SAS. A fundamental change to spectrum sharing begs for PU/Incumbent user communication to the SAS prior to operation. There have not been any research papers that have proposed this architecture or have provided any additional system modifications with the assumption of such a system. Recently, however, there has been evidence that a PU informed spectrum access system is under review by federal authorities.

The National Telecommunications and Information Administration (NTIA) has released a document proposing incumbent informing capability (IIC) [8]. Describing the system as more reliable than traditional ESCs, a SAS with IIC would remove layers of complexity in SAS PU detection and protection. This spectrum sharing model with IIC would create a secure interface for PUs to the SAS. PUs may report their anticipated time, frequency, and location of operation to the interface which relays the information to the SAS.

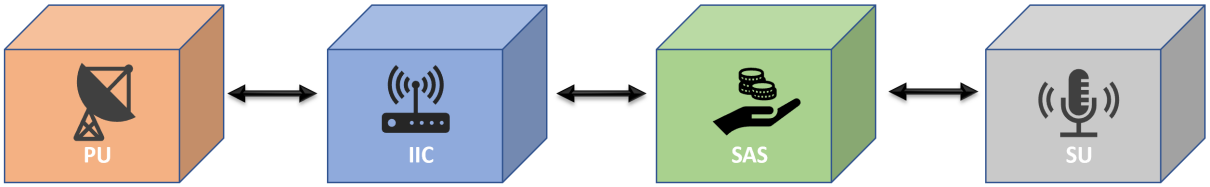

Figure 3.1: Incumbent Informing Capability System Architecture

Chapter 4

Proposed Solution

Considering a traditional SAS, there are several features that if implemented, may result in greater system capabilities. In this proposed implementation of an ASAS, features may support:

- Strengthened PU privacy
- Strengthened PU protection
- Punishment of MU transmission
- Increased methods for CBSDs to increase SAS relations

4.1 Advanced SAS Requirements

In order to support these features, there are two alterations to the base SAS architecture that must occur:

1. The ASAS requires incumbent informing capability

2. The ASAS requires the ability to control the transmitters of all willing CBSD participants

The first change that must occur is that, rather than relying on ESC or crowdsourced spectrum data, the SAS must have dedicated and secure correspondence with any PUs that may enter the operating region of the SAS. Assumptions for such coordination may presume that the SAS is operated by the same agency that controls the PU, or contracts are set ahead of time indicating to the SAS of PU intent. The exact method of communication between the PU and SAS is not of relevance to this study. While there is a system requirement for direct PU to SAS correspondence in this situation, FCC regulations must be respected and an ESC will still be required for any SAS. There exists solutions for providing IIC to spectrum sharing systems which may be of interest in further research [8]. Incumbent informed SAS solutions provide benefits for spectrum sharing, therefore continuing this study with the assumption that an incumbent informed SAS is feasible proves reasonable.

Another requirement for the features previously mentioned is for the SAS to have the ability to control CBSD TX capabilities. In the base SAS, CBSDs set their RX parameters as permitted by the SAS. In a similar message structure, the CBSD may have easily have its transmission parameters controlled. This requires TX-capability information to be included into the Registration Request the CBSD makes to the SAS.

The incentive for proving this control to the SAS may come in the form of higher trust or possibly higher temporary priority. SASs are encouraged to include some form of incentive for CBSDs that are confirmed to provide accurate crowdsourced information, typically in the form of a trust score. In the event a CBSD does not have receiving capability, the CBSD may still provide value to the SAS by offering its transmission capabilities when requested by the SAS and while not actively granted/transmitting. There is no apparent harm in allowing the SAS control the transmitter of a CBSD from the perspective of the CBSD, and the SAS

has plenty to gain from SU transmitter utilization. In return, the SAS may opt to reward the willing SU. This has the potential to ease any financial requirements that a SU would otherwise have to be burdened with, so long that the SAS values the transmission control from the CBSD.

4.2 PU Privacy Tactic

A capability of the ASAS includes a PU privacy tactic that is inspired by the multiple references implementing PU falsification by including false PU entries in the spectrum database. This database manipulation method of obfuscation can be easily breached if the MU simply begins spectrum sensing, in which case they may verify that there is in fact no PU operating over the supposedly occupied channel. Considering how large a SAS operating region is in terms of land, a singular MU may not be able to detect a PU operating on the other side of the county, therefore the MU has no justification to make assumptions about the SAS's either truthful or falsified PU detection. However, if the MU is part of a larger colluding network that has the capability to spectrum sense over the entire SAS operating region, then in this event, the MU would have the justification to assume the SAS is falsifying database entries.

This can lead SUs to lose trust in the integrity of the SAS, or MUs may assume they have already been identified as malicious. In the former event, the SU could report the SAS as dysfunctional, or it could lead the SU to question its hardware functionality which would be rather shameful for the SAS to do. In the latter scenario, this may prompt the MU to deregister from the system, and re-register under different false credentials, resetting the trust score of the MU and requiring the SAS to identify the MU. MU identification is non-trivial, and to lose all progress in accurately detecting a MU would hurt the system.

With prior knowledge of PU spectrum occupancy and PU antenna location, the SAS will have a 100% certainty of PU operation over a specific channel – this is important as to ensure that the CBSDs being utilized for obfuscation are not being wasted on a trespassing MU. If the traditional SAS's ESC is of extremely high quality, then this obfuscation scheme may still be implemented. However, it would be best if the SAS knew with 100% certainty that there is a PU that deserves obfuscation before requesting transmission access from CBSDs. With PU intent information along with the location and TX control of idle CBSDs, the SAS can obscure PU operation by transmitting over co-channel or adjacent channels relative to the known PU band. Parameters that are obfuscated may include spectrum frequency occupation, geographic basestation location, and spectrum occupancy time. Figure 4.1 includes a description of how spectrum may be occupied under such conditions.

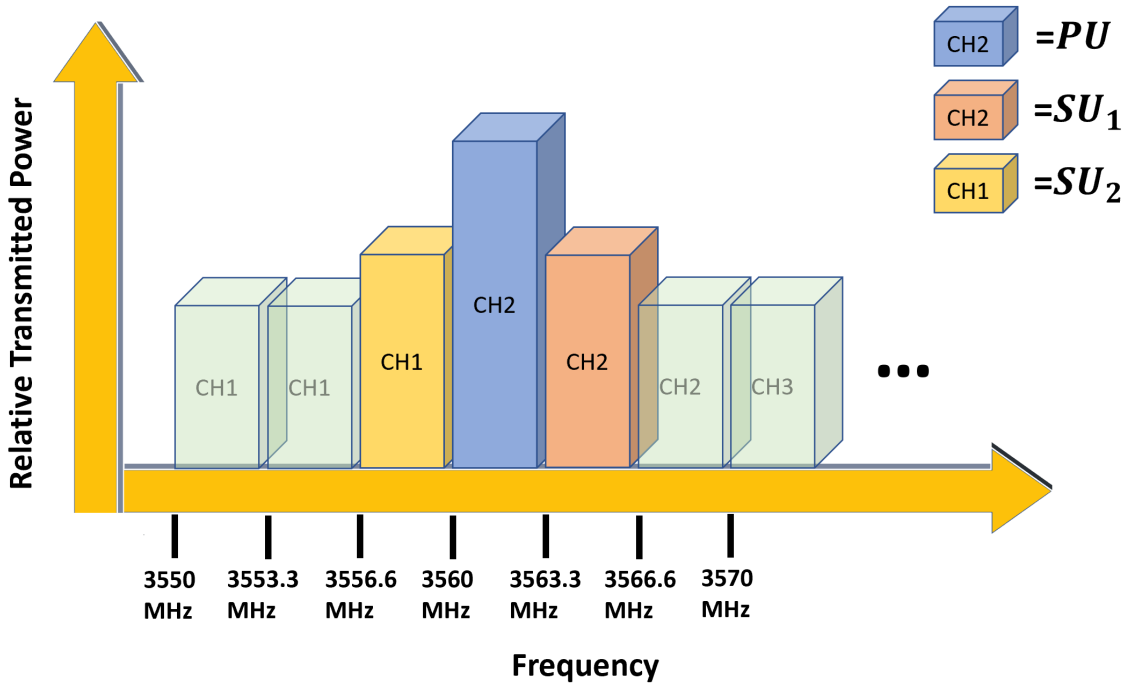

Figure 4.1: Example of Spectrum Utilization in PU Obfuscating Scheme

Ideally, for the best PU privacy, the PU would only transmit as much energy as possible

while still meeting all other operational requirements. By having a transmit energy closely matched to that of a CBSD's max effective isotropic radiated power (EIRP)/power spectral density (PSD) as stated in [14], the PU's privacy may increase. Since there are restrictions on the maximum EIRP for CBSDs, if a PU operates within the SU constraints, it would help the PU not stand out amongst the other users. Estimating the transmit power required of the PU to be comparable to the power levels of the SUs aiding in the obfuscation is a privilege of the SAS, considering it has all knowledge of SU power and PU power, along with location. While path loss and other means of signal degradation disallow the SAS to precisely compute the exact reception power at any given geographical region, the SAS may make best estimates and adjust the SUs or inform the PUs about more optimal power outputs for enhanced obfuscation.

With CBSD location and PU location available as well, the SAS may select CBSDs that best protect the PU by selecting surrounding CBSDs to the PU. This creates a region where a MU attempting to determine PU location may have greater uncertainty on PU location as demonstrated in Figure 4.2. Although MU location will not always be known, regardless of where the SUs are located, a level of uncertainty is introduced in the MU radiolocation attempt, proving the SAS's and SU's efforts worthwhile even if it is not in the best case scenario as in figure 4.3.

Because the SAS strategically assigns the output power of the SUs with location considered, the PU is obfuscated. The angle of arrivals (AOAs) from the perspective of the MU indicate three separate signals with different AOAs. This is preferable to the non-obfuscated scenario where the PU is the only signal occupying the channel and the MU only has one AOA to trace.

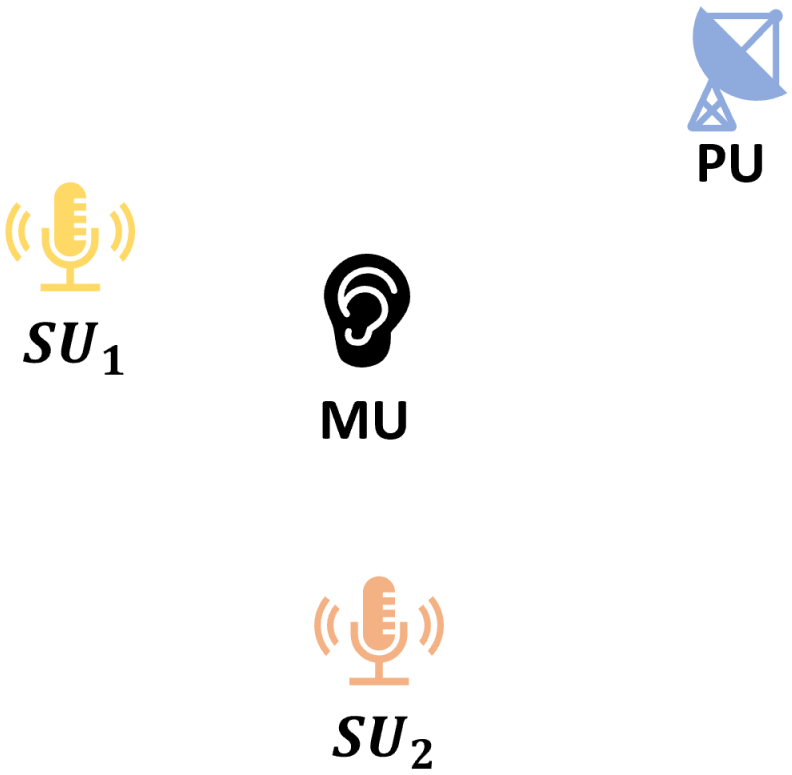

Figure 4.2: Relative Locations of PU, SUs, and MU in PU Location Privacy via SU Transmission Scheme

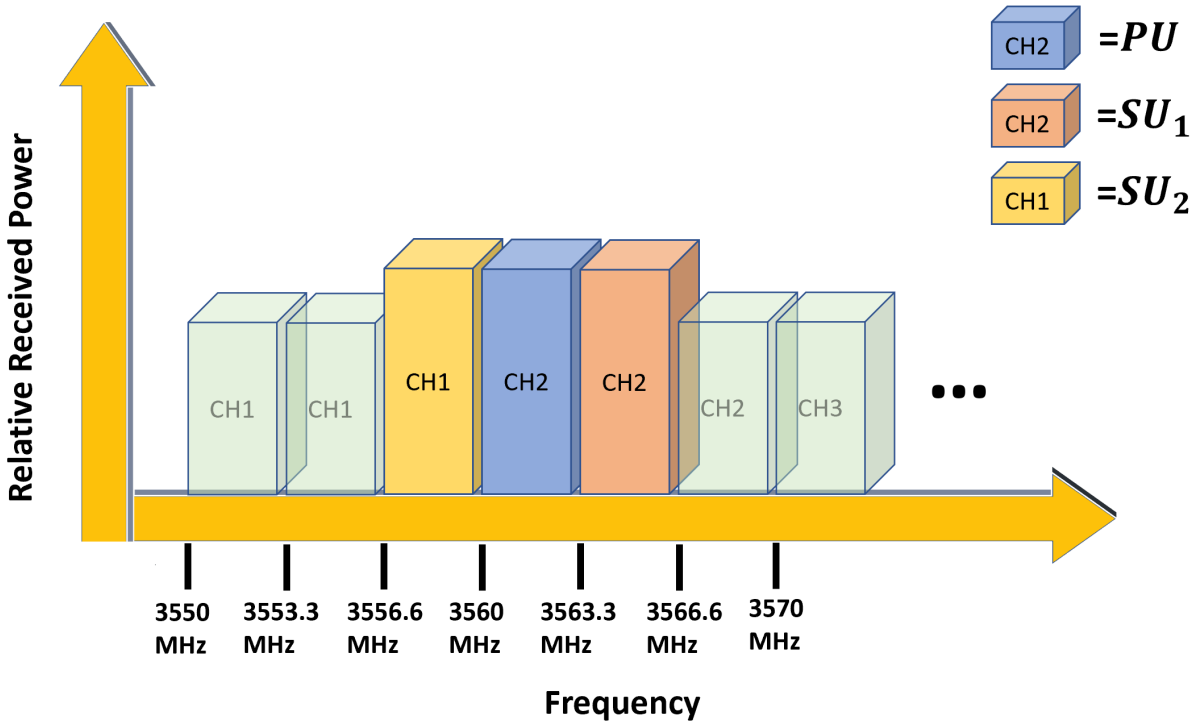

Figure 4.3: Received Power from the Perspective of the MU

Figure 4.4 shows the high level addition to the SAS's PU IIC protocol. In this implementation, the SAS has a unique socket handler for PU/Incumbent information. This event handler is only called by a PU that is willing to give, at minimum, the frequencies it plans on transmitting over. Since there is no FCC or WInnForum defined protocol or message format, only essential operating parameters are delivered to the SAS though this event handler. Additional parameters include start time, end time, antenna installation longitude and latitude, power, and desire for obfuscation.

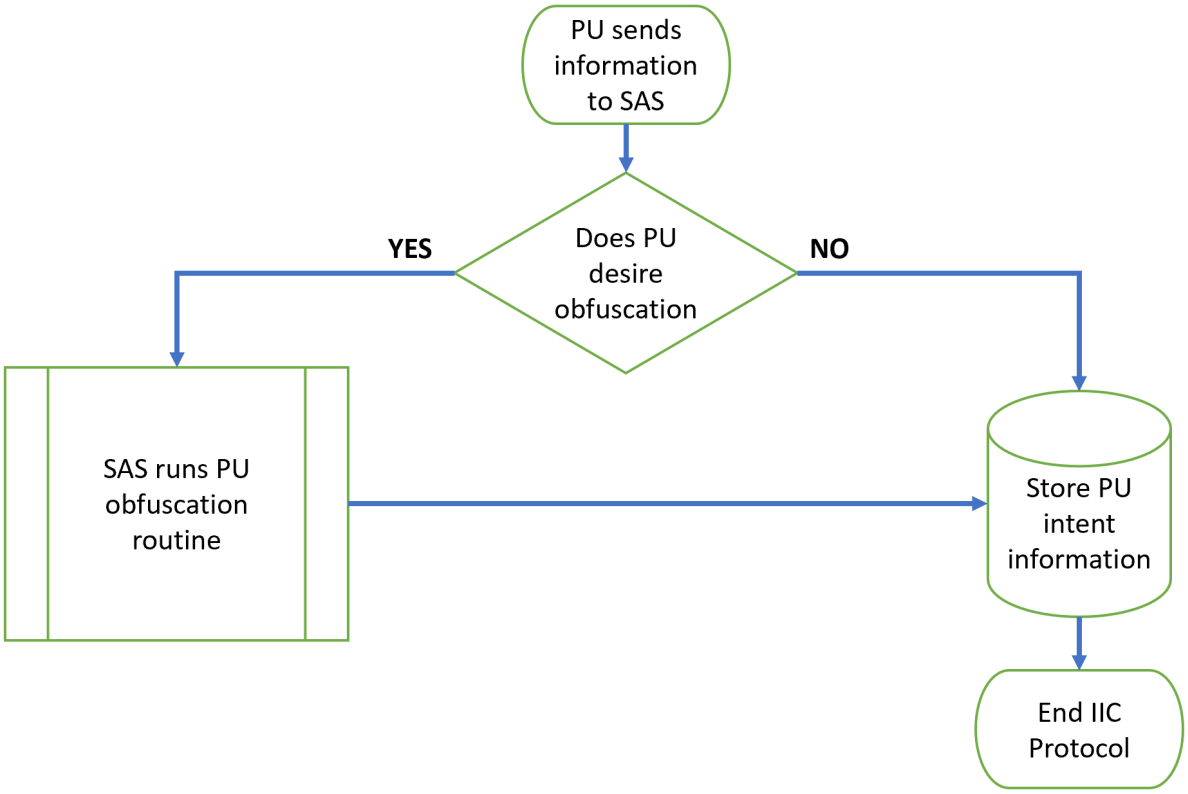

Figure 4.4: Incumbent Informed SAS Flowgraph

Regardless of the PU requests obfuscation, the SAS may store and utilize the provided information to increase spectrum scheduling efficiency. Scheduling algorithms are highly researched in the context of computer instruction scheduling. With the availability of prior PU intent, the SAS can better schedule SUs to avoid interference with upcoming incumbents

and maintain high QoS for the SUs. Without PU intent information, an SU may be granted spectrum for an unreasonably short amount of time before their grant is suspended, which would result in poor QoS for the SU. Further, is an SU somehow where to indicate that the short amount of time is acceptable for them, then the SAS may decide to override the current scheduling/priority algorithm to better utilize the spectrum and schedule out the shorter grant.

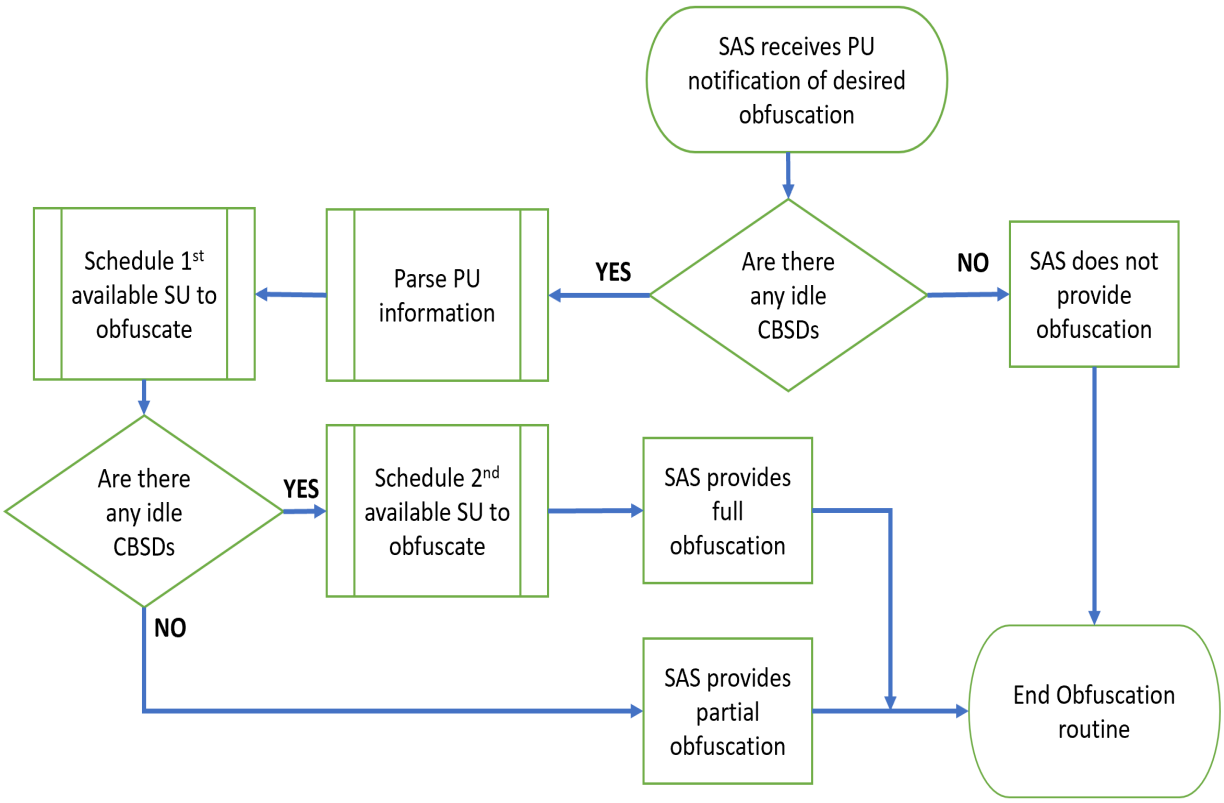

Figure 4.5: Obfuscation Routine Flowgraph

Figure 4.5 outlines the routine utilized by the SAS when a PU requests obfuscation. First, the SAS must check to see if there are any eligible SU nodes for obfuscation use. SU eligibility is only implemented as having an "IDLE" grant status, however further algorithms may be developed to consider SU transmit capability, antenna installation, and expected scheduled grant requests from the SU. The next step in the routine is to extract all of the information that the PU provided. Since all of the information is optional, the script must be sure to check for each parameter in the message. Once all of the parameters are extracted, the SAS can utilize the low and high frequency parameters to determine the adjacent frequencies and/or channel that would best obfuscate the PU.

This process is shown to repeat for one additional iteration to provide low and high frequency obfuscation. However, decision making for engaging SU transmission may require more than 2 iterations for different algorithm implementations. This preliminary obfuscation routine creates the foundation for future work in real-world obfuscation.

4.3 Proposed Obfuscation Schemes

Leveraging the ASAS's framework to implement obfuscation schemes, four obfuscation schemes have been devised.

1. *Double Pad with Equal Bandwidth (Scheme 1)* – Up to two obfuscating SUs transmit with the same exact bandwidth as the PU. SUs are allowed to occupy adjacent channels to fulfil their assignments. SUs are randomly assigned to obfuscate either above or below the PU in the event that only one SU is available, otherwise if there are two available SUs assignment order does not matter. If there is not enough bandwidth to obfuscate above or below a PU, then no obfuscation is delivered in that spectrum. I.e. if a PU is transmitting at the bottom of the CBRS band, then no obfuscation is

delivered below the PU since it would break FCC rules.

2. *Only Fill PU Channel(s) (Scheme 2)* – Obfuscating SUs must adjust bandwidth to only fill the channel(s) the PU is already occupying. SUs are not allowed to occupy adjacent channels since it it not part of the scheme. If there is only one available SU, only the top or the bottom of the channel is filled. If there are more than two SUs, then more than one SU can contribute to filling the band. E.g., if there are 3 available SUs and the PU transmits over 5 of the 10 MHz in a channel, the 3 SUs will divide the remaining 3 MHz in order to decrease the amount of bandwidth each SU is responsible for.

3. *Fill PU Channel and Random Adjacent Channel(s) (Scheme 3)* – Similar to Scheme 2, this scheme assigns SUs to occupy any remaining spectrum that PUs are also occupying. However, this scheme also allows SUs to occupy adjacent spectrum from the PU channel(s). In this scheme, the SUs occupy a random portion of adjacent channels to obfuscate the channel the PU may be utilizing. If there is only 1 SU, then only one side of the PU will be obfuscate.

4. *Fill PU Channel and Fill Adjacent Channel(s) (Scheme 4)* – Similar to Scheme 3, this scheme assigns SUs to occupy any remaining channels that PUs are occupying along with adjacent spectrum. Different from Scheme 3, this method entirely fills adjacent channels. I.e. if a PU is partially occupying channel 2, then SUs will transmit over channel 1, channel 3, and any available spectrum in channel 2, as to obfuscate the channel the PU may be occupying.

The motivation for the first scheme stems from an assumption made about MU intelligence. Since the current CBRS band has not taken preventative action towards obfuscating PU transmissions, MUs may already have behavioral intelligence on PUs. More specifically,

MUs may already know what signal to be looking for with respect to bandwidth. If PUs typically have a certain bandwidth that the MUS can utilize for detection, then utilizing equal-bandwidth SU(s) for obfuscation may provide greater PU obfuscation.

The second ruleset is trialed with the concern of preserving maximum available spectrum to users. SUs in this obfuscation scheme only obfuscate the PU within the channel(s) the PU occupies. This ensures that the obfuscation does not degrade the spectrum availability.

Chapter 5

Methodology

This chapter describes all of the processes, systems, and tools utilized to create the ASAS as well as the simulation and experiments dedicated to the proposed obfucscation schemes.

5.0.1 Materials Used

CORNET

Cognitive Radio Network Testbed (CORNET) is a testbed for enabling SDR usage over the internet. Featuring a server, Universal Software Radio Peripheral (USRP) hardware, and software solutions all in one, the testbed is a critical tool for wireless research. Figure 5.1 outlines the utilized tools provided by the testbed.

Server: The CORNET server utilizes open source software and Linux operating system distributions. Together, they create a very open, developer-friendly atmosphere for tailoring the server to the needs of the user. The server offers features remote access capabilities for development off campus. Additionally, with proper security protocols in place, the remote

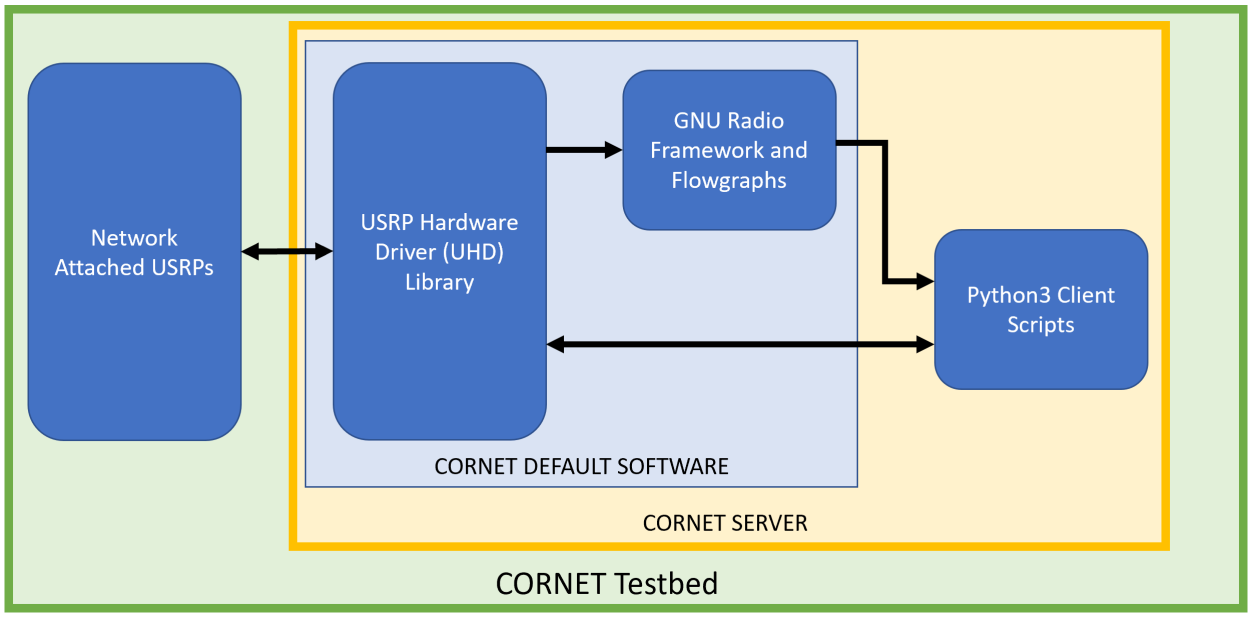

Figure 5.1: CORNET Testbed Architecture

access ability allows for the use of the SDRs by any user with remote access permissions. The ability to utilize SDRs remotely enables a web-based interface for radio transmit and receive parameters and characteristics.

Radios: CORNET hosts approximately 20 Ettus Research USRPs (see figure 5.2). A majority of them are B210 models that house unique daughterboards with different RF abilities. The B210 boasts an Analog Devices transceiver, Xilinx Spartan 6 Field Programmable Gate Array (FPGA), and daughterboard support. RF transmission capabilities extensively cover mid-band spectrum, and daughterboard specifications dictate the receiving abilities of the radios. An ample number of CORNET nodes have 3.5 GHz CBRS band receiving capability.

Software: CORNET includes an installation of GNU Radio Companion (GRC) that is maintained by CORNET administrators. GRC is a visual programming language tool that

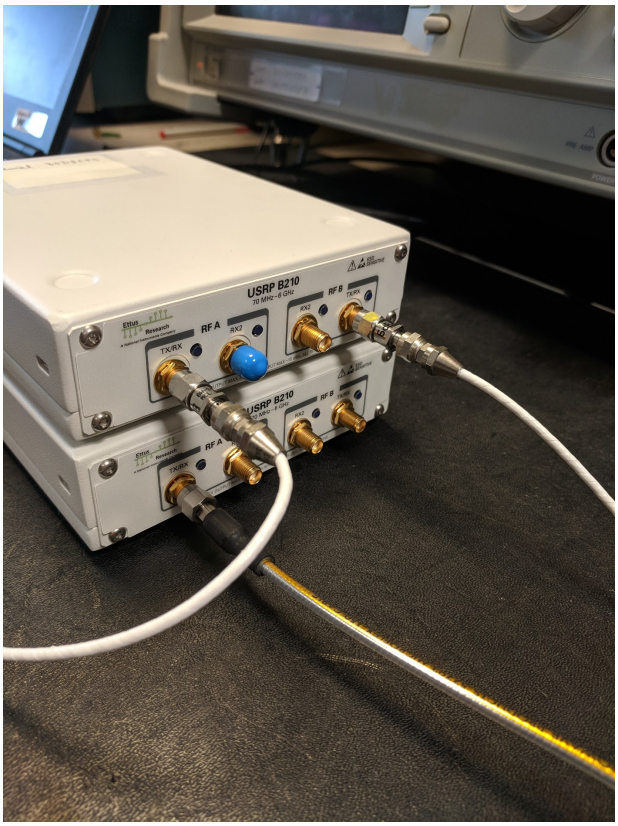

Figure 5.2: 2 Stacked Ettus Research B210s

is tailored to signal processing and interfacing with SDRs [15]. GRC flowgraph design is taught at Virginia Tech in the Software Defined Radios course, and GRC is installed on the laboratory servers for availability for research students. Key blocks provided by GNU Radio are the USRP Source and USRP Sink blocks which control receive and transmit capabilities respectively. These allow for easy configuration of the transmitter and receiver properties of the SDR. The receiver flowgraph also features a Fast Fourier Transform (FFT) block and a probe block which allow for power values to be arranged into an array for programming use.

A critical library used for USRP development is the USRP Hardware Driver (UHD) library for Python. Provided by Ettus Research, the UHD library provides all the necessary drivers in C++ for the USRPs to operate. The library includes modules for Python that acts as a simple API to the C++-based features.

Laptop

An essential tool for software development is some form of computing device with an operating system that supports programming. A personal HP laptop was utilized for the development of the experiment and all the supporting code. Windows 10 is the operating system on the laptop. Visual Studio Code and Sublime Text Editor were use for programming, and MobaXterm was used as an SSH client for connecting to CORNET.

Software

Python: Python, specifically Python3, is used for the entirety of the development of the SAS Client and experiment scripts. The largest driving factor for selecting Python was the fact that GRC generates flowgraphs into either C++ or Python. Of the two options, Python provides more rapid development speed over C++. While there is a tradeoff between development time and software robustness, development time was heavily favored over software robustness. C++ provides great memory management and the ability to decrease compiled software complexity and execution time, however the amount of time that would have to be spent to build the software would not be justifiable to any researcher or project sponsor. During the development of the client, JavaScript (JS) was used to provide a simple server for the client to connect to for debugging and development purposes. Sublime Text editor and Visual Studio Code were used to write the code.

Virginia Tech Open Source Spectrum Access System: To enable dynamic spectrum access research, an open-source spectrum access system was built, and is being maintained, at Virginia Tech. The VTSAS began development in conjunction with the CORNET client to ensure proper WInnForum standards were being met on both systems. The VTSAS is

the only open source SAS available – all other SASs are owned by corporations that may charge for SAS usage. Additionally, the corporate SASs are not suitable for research purposes since their system is not open source. Since the VTSAS is open source, it allows for easy modification to extend upon the WInnForum standards that have been met by the project.

The VTSAS server and algorithms are all implemented in Python, and a web client interface has been created using TypeScript and PHP. The server is written with modular functions that allow for modifications in server response to new entrants and general behavior. This allows for easy modifications to routines such as the trust system, SU scheduling, and PU spectrum protection. It also allows for new routines to be including while utilizing the abstracted functions for PU detection and SU management.

The VTSAS server code can be executed using the CORNET server. Although the CORNET server will host the SAS server as well as the network-attached USRPs, socket protocols will still be mandated as if the server were hosted elsewhere.

5.0.2 Implementation and Development Process

CORNET Client Development

To be able to run experiments regarding SAS upgrades or updates, a radio-connected client for the SAS needed to be built. The VTSAS provides a system in which CORNET's hardware may be used to further research SAS architectures and client interfaces. To leverage CORNET and the VTSAS, a client wrapper that conforms to WInnForum standards must be built.

USRP Code To begin development, GRC flowgraphs were created to instantiate three USRP types: TX, RX, and TX/RX. The TX radio only has transmitting ability, the RX radio only has receiving ability, and the TX/RX radio can receive and transmit concurrently. The TX/RX radio is enabled by a USRP with multiple RF hardware installed in one device; i.e. the TX/RX USRP has separate antennas and hardware for each function, simply housed in one device. The benefit of this device over the other two is that the transmitted signal from one set of hardware can be received by the other set of hardware without the worry of pathloss. Multipath interference may still occur, but since the antennas are only a matter of centimeters apart, this allows the receiver to have the opportunity to receive a stronger signal than all the other installed USRPs. Figures 5.4, 5.3, and 5.5 show the block diagrams for the USRPs.

By default, all transmitted signals are wideband Gaussian noise sources. GNU Radio provides the flexibility to input files for transmission. However, to create a client, signal detection scheme, and obfuscation routine, the particle signal was not of interest during development.

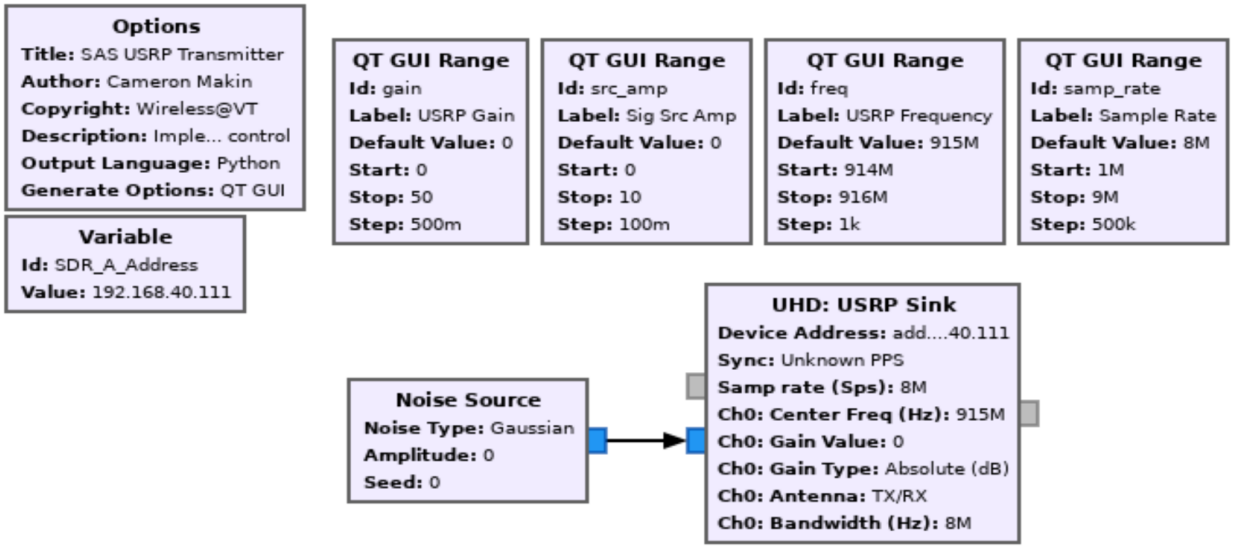

Figure 5.3: GNU Radio Flowgraph for a USRP Capable of TX

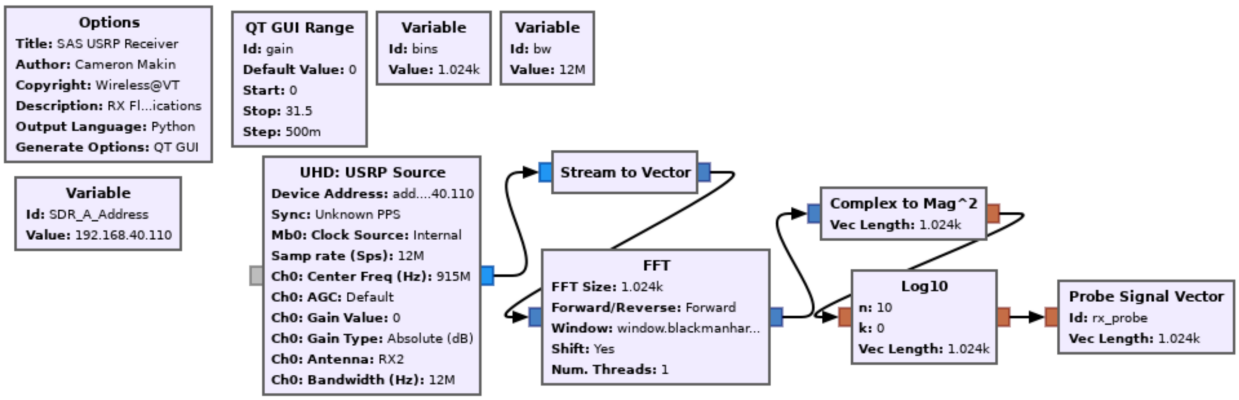

Figure 5.4: GNU Radio Flowgraph for a USRP Capable of RX

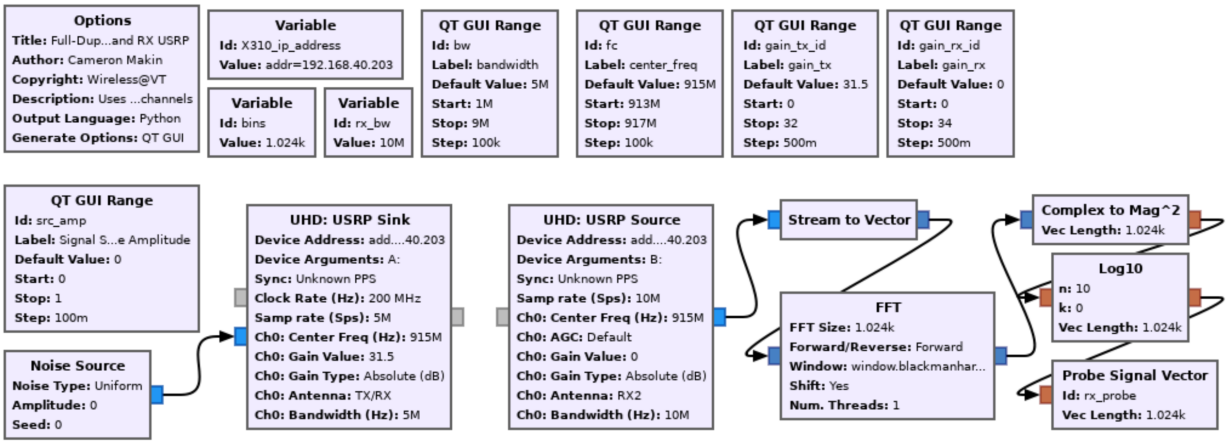

Figure 5.5: GNU Radio Flowgraph for a USRP Capable of Simultaneous TX and RX

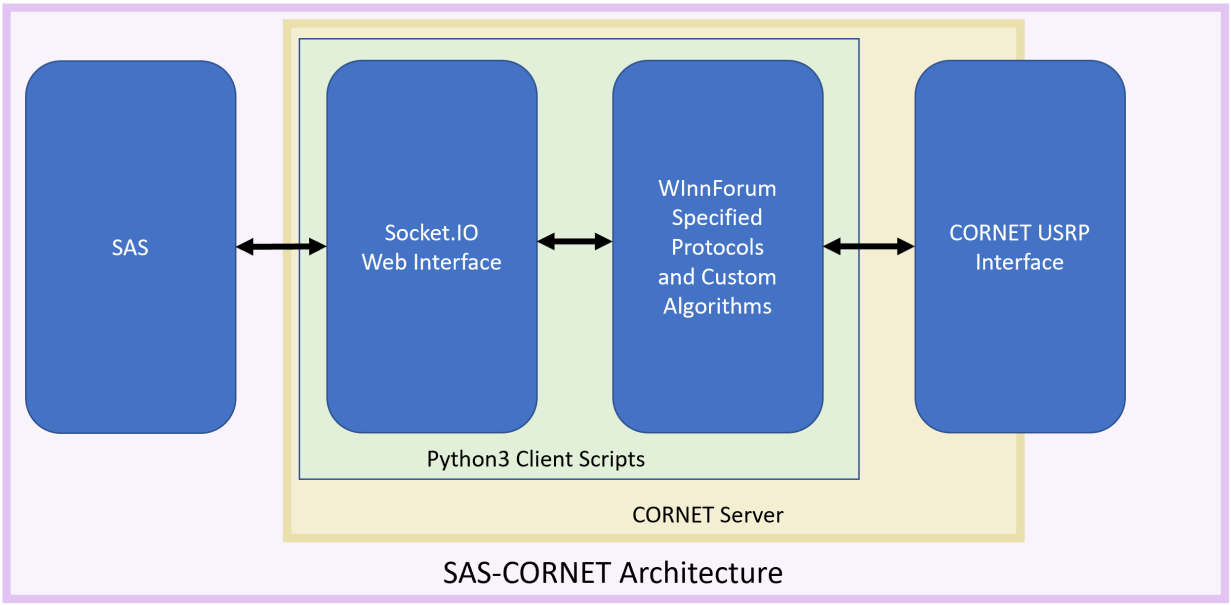

Figure 5.6: SAS-CORNET Architecture

SocketIO Code Once the flowgraphs have been completed and tested for capability resembling that of the desired end product, attention is given to the Python scripts that these flowgraphs generate. The Python scripts are a rather short, object-oriented implementation of the same logic as built in the flowgraph. The generated Python scripts from the flowgraphs allow the flexibility of adding extra functionality that Python can deliver. Most notably, the socketio module is a key feature in creating the SAS client. Socket.IO is a library that enables real-time web communications with cross-platform capability. Socket.IO makes accessing the TCP/IP stack for web communications very simple. Python includes a module that provides socketio support. This module allows the GRC flowgraphs to now connect to the SAS, how there are a significant number of socket protocols that must be written to provide any functionality to the flowgraphs.

The WInnForum specifies message formats in order for a client to respectfully address a certified SAS [25]. These messages have been formatted in Python using an object-oriented paradigm that follows the exact WInnForum specifications. To further ease implementation, each object has a method that converts all class attributes into a single JavaScript Object Notation (JSON) formatted dictionary. The incentive for creating a class-to-dictionary method is to allow for the WInnForum defined objects to be serialized via JSON so that the socketio module can send the data to the SAS server. Below is an example of the implementation of the *Relinquishment Request*:

```
1 class RelinquishmentRequest:
2   """
3   RelinquishmentRequest - Array of RelinquishmentRequest objects.
4     Each RelinquishmentRequest object Represents a relinquishment
        request of a CBSD.
5
6   Attributes
```

```
7   ----------
8   cbsdId : string (required)
9     The CBSD shall set this parameter to the value of its CBSD identity
        .
10
11  grantId : string (required)
12    The CBSD shall set this parameter to the value of the Grant
        identity of this Grant.
13
14  """
15  def __init__(self, cbsdId, grantId):
16    self.cbsdId = cbsdId #R
17    self.grantId = grantId #R
18
19  def asdict(self):
20    return_dict = {}
21    if(self.cbsdId):
22      return_dict["cbsdId"] = self.cbsdId
23    if(self.grantId):
24      return_dict["grantId"] = self.grantId
25    return return_dict
```

Additionally, creating classes for each WInnForum object proves extremely useful in catching poorly formatted messages. Due to Python's dynamically typed nature and runtime execution, it is very easy to script invalid statements that would appear to be valid but in execution cause fatal errors. A large issue discovered during development is Python's treatment of the decimal value of 0 (zero). In most other languages, zero is a unique value from

NULL. However, in Python, it has been discovered that if any objects have an attribute that happens to be zero, for instance, antenna gain, then Python will claim that there is no value found for that parameter and a fatal error will be thrown. This issue resulted in extra layers of data formatting. First, regardless of the datatype, all values that to be passed through the socket are type-casted to type sting in this implementation. Typecasting to string ensures that zeros are transported across the socket. However, this means that once the SAS attempts to utilizes the Python class file with all the class definitions in it, it must be mindful that there are string datatypes in place of what is typically a float or integer (frequency, bandwidth, etc.). This creates the need to recast the values into their respective datatype before they are utilized for any arithmetic or operations.

Conversion of Messages to Commands Once the client has properly formatted messages that can be sent to and from the SAS server over sockets, the last major piece in development is translating the messages into commands to send to the USRPs. For example, when a CBSD moves states from "GRANTED" to "AUTHORIZED", the USRP is allowed to initiate transmission over the granted spectrum. This segment of development took the longest in order to ensure the system has the behavior as desired by the WInnForum and spectrum users.

After all relevant sub-components of the system have been programmed and all of the behavior has been implemented, the CORNET client can transmit over available spectrum as per FCC and WInnForum standards.

Advanced SAS PU Obfuscation Routine

While several limitations in research environment do not allow for a proper study of angle of arrival, PU obfuscation tactics are still delivered and may hold value in a free space testing

atmosphere. The implemented PU IIC provides a routine for the ASAS to automatically provide adjacent frequency obfuscation. The routine can be easily modified to implement different obfuscation schemes.

To test the capability of the SAS-aided obfuscation routine, an experiment has been set up to show adjacent channel obfuscation in action. Figure 5.7 shows the node setup for the experiment. In this trial, a receiving USRP will be placed approximately equidistant from two transmitting USRPs. Figure 5.8 shows the physical layout of the utilized CORNET nodes. Layered on top of a map of Kelly Hall, the same symbols for the three devices are found.

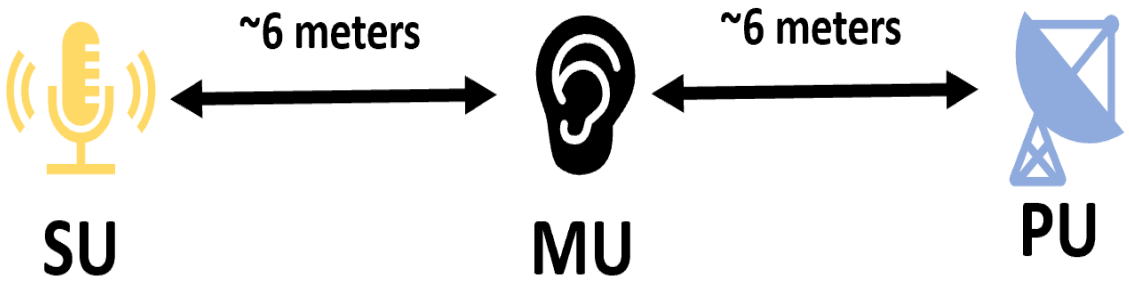

Figure 5.7: High Level Node Location Relationship

Figure 5.9 shows the received spectrum activity from the perspective of the MU located between the devices. At the instance of this measurement, only the PU actor is transmitting. This serves as a baseline for PU detection. Additionally this allows for a relative reading for the device's noise floor which is later used for the spectrum occupancy detection function. The PU signal is received by the MU, and if this were in a free space environment, radiolo-

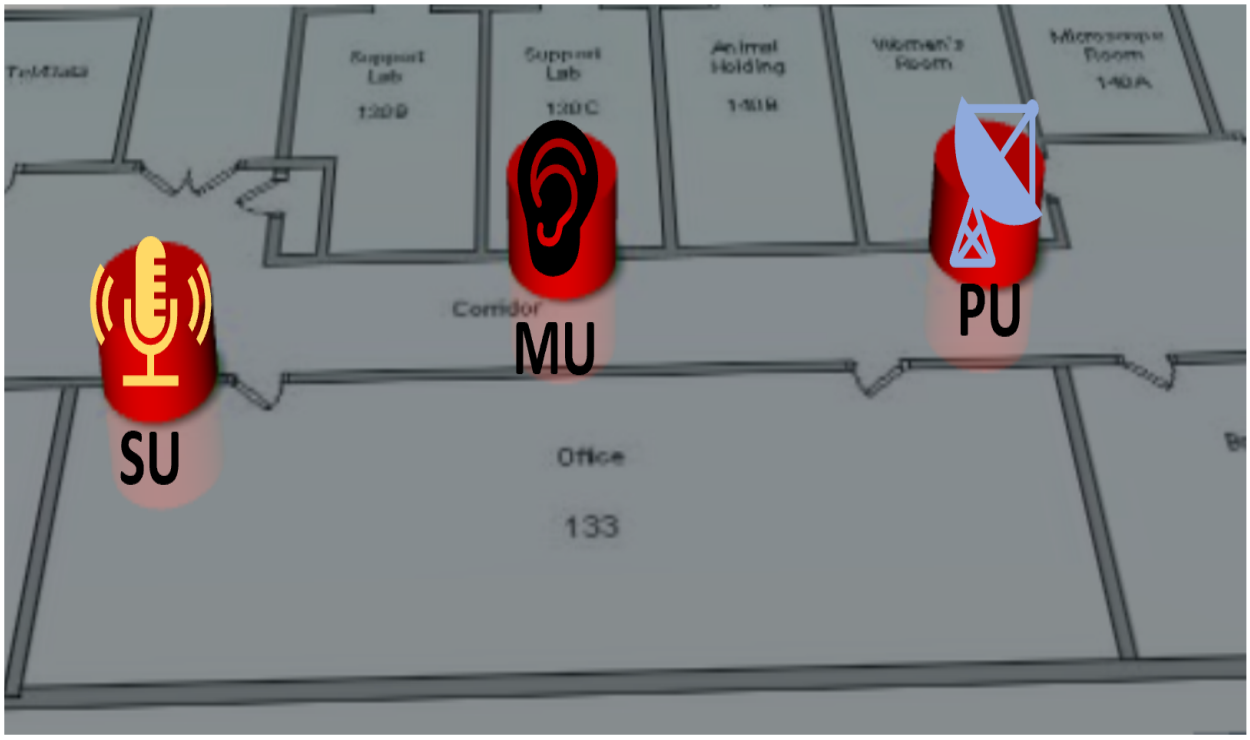

Figure 5.8: Experiment USRP Locations in Kelly Hall

cation techniques may locate the PU with great certainty, especially AOA based detection.

Figure 5.10 shows the perceived spectrum occupancy with the PU obfuscation routine enabled. In this trial, only 1 SU was registered and idle. Once the idle SU was registered in the SAS, a PU sent the SAS only its operating frequency range. The time of transmission was assumed to be instant, so no scheduling was required for this experiment.

Once the SAS received the operating parameters of the PU, the obfuscation routine began. The routine found the frequency range from the bottom of the channel, in this case the second PAL channel, up to the bottom of the expected PU.

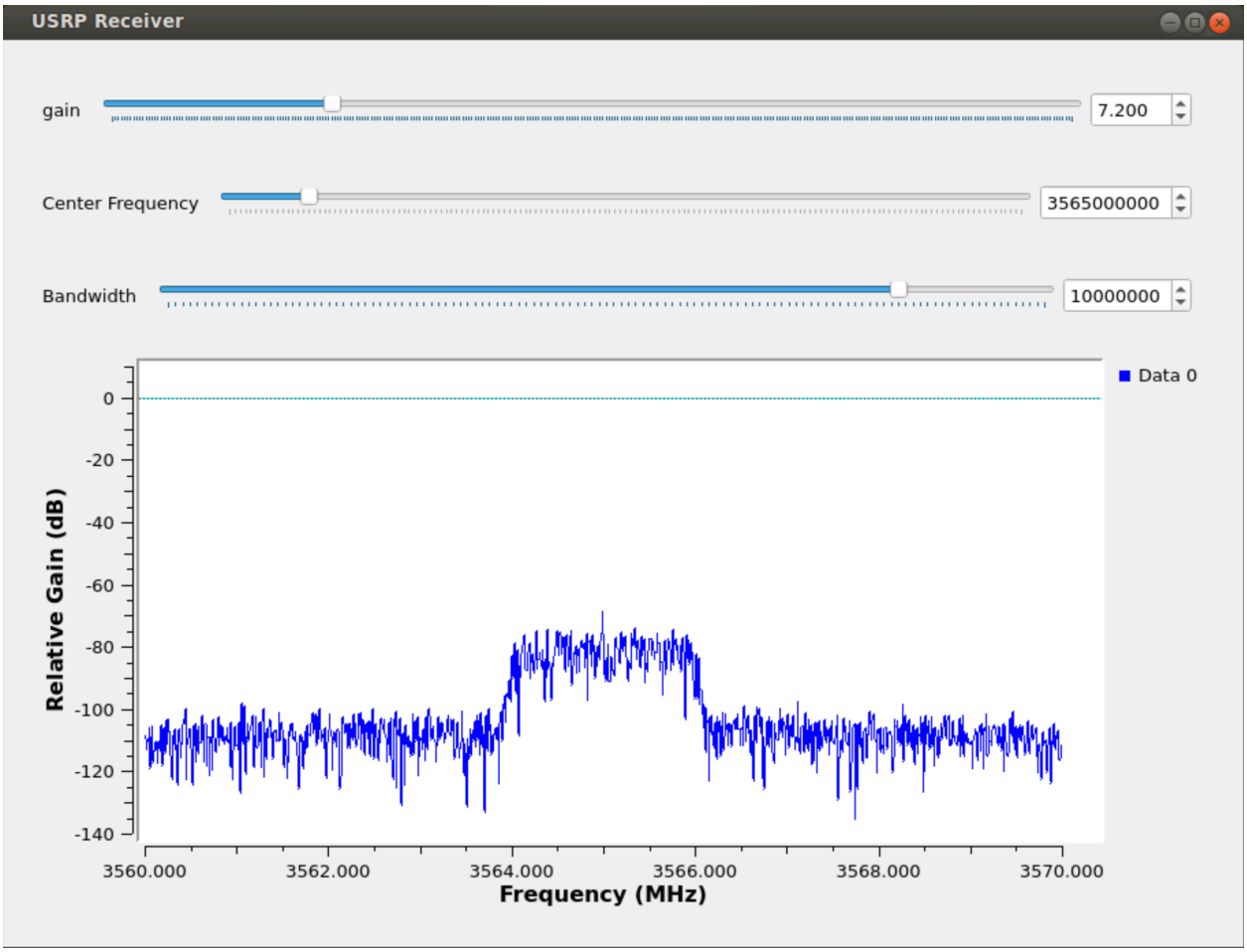

Figure 5.9: MU Sensing PU without SU-Aided Obfuscation

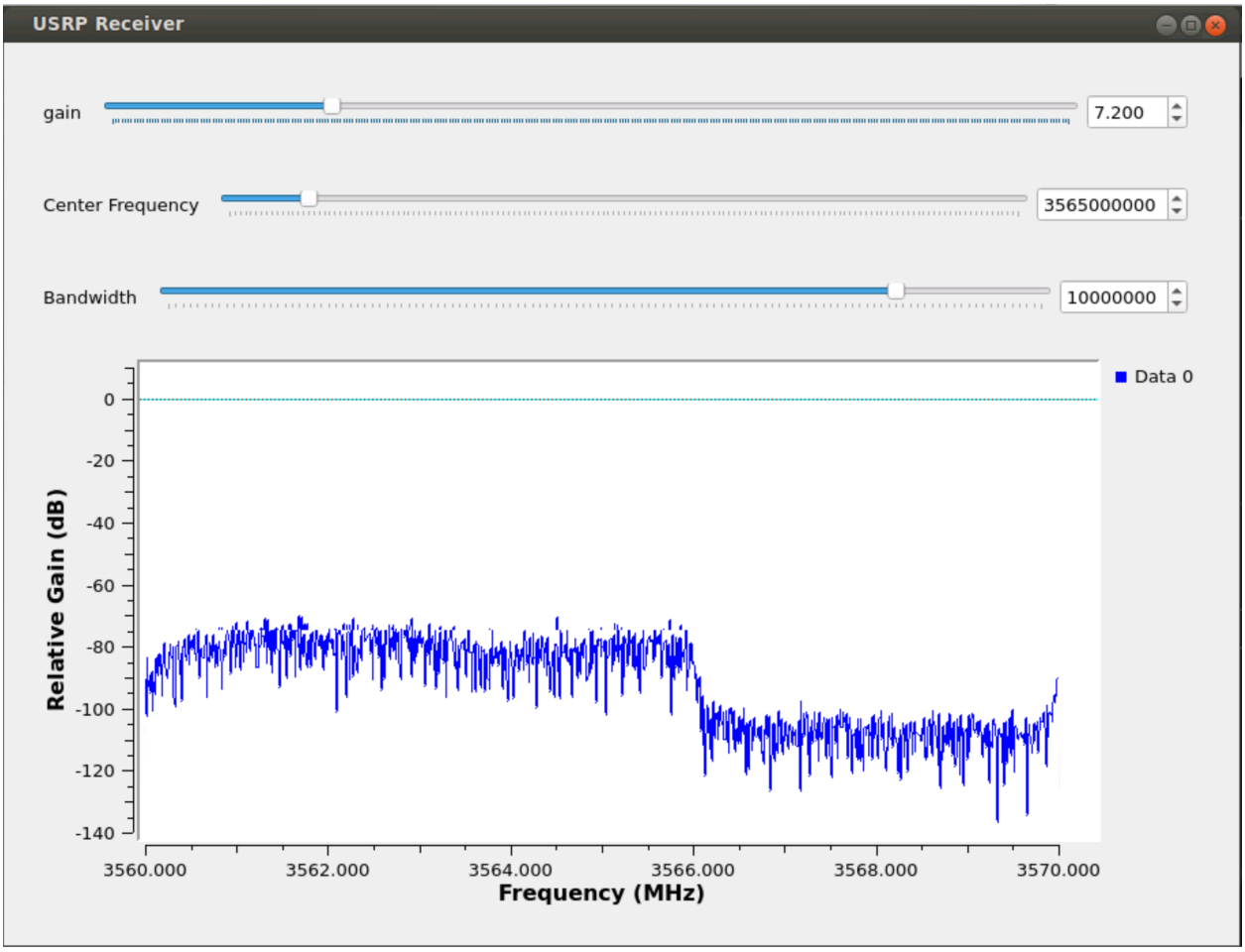

Figure 5.10: MU Sensing PU with Partial SU-Aided Obfuscation

For experiments with two SUs, figure 5.11 shows the placement of the devices. Note that *SU 2* is physically further from the spectrum sensing MU than *SU 1*.

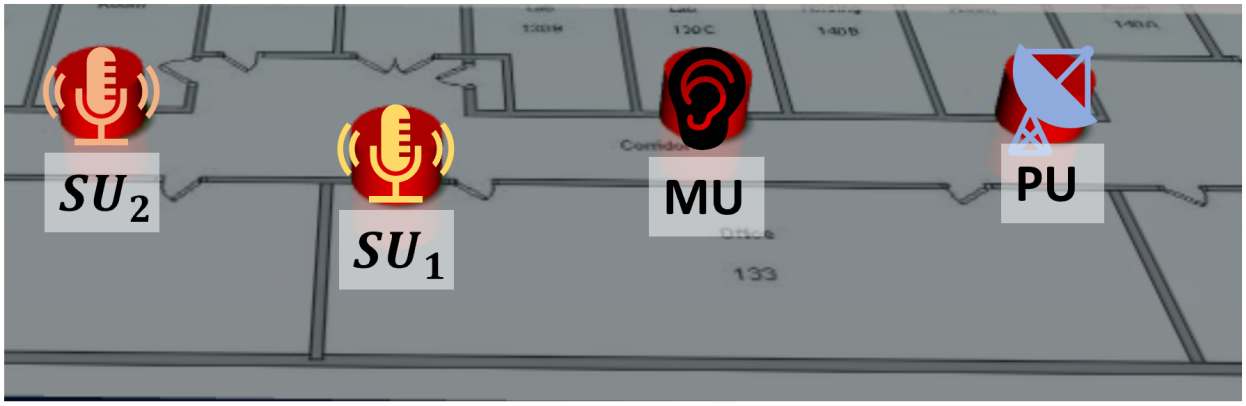

Figure 5.11: Node Layout for Two SUs

5.0.3 Simulation

A simulation of PU, SU, and MU behavior has been developed in Python to compliment the proven implementation of the ASAS PU obfuscation tactic proposed. This simulation allows for metrics to be gathered without demanding more hardware resources than that is available. The simulation trials are under the following restrictions / assumptions:

- The simulation spectrum represents 10 channels (100 MHz)
- All transmitting devices transmit in discrete increments of 1 MHz
- There is only 1 PU
- Each instance of a PU and SU have unique basestation locations
- The PU has a randomly assigned bandwidth [1, 10] MHz for each trial of the simulation
- The PU does not have to self contain itself to one channel (i.e. the PU can have 10 MHz of bandwidth and transmit across two channels rather than filling one channel)
- All four obfuscation schemes are simulated
  - Simulations are executed for SU counts ranging [1, 10]
  - 100 trials are executed for each SU count (i.e. 100 trials with 1 SU, 100 trials with 2 SUs, etc.)

5.0.4 Analysis

Simulation Analysis

In the simulation, PUs and SUs are placed into a Python list that represents the spectrum being simulated. After the PU and SUs are allocated as according to the obfuscation scheme,

a function is called to search through the list for sections of continuous utilized spectrum. The function then reports back the low and high frequencies detected. This function is to act as the MU searching for occupied spectrum. Other collected data includes how many PUs, SUs, and MUs are provided to the Simulation object constructor.

In the trials of the different obfuscation schemes, three metrics are collected:

- Spectrum Sharing Efficiency
- Frequency Obfuscation Efficiency
- Location Obfuscation Efficiency

Spectrum Sharing Efficiency

$$Spectrum\ Sharing\ Efficiency = \frac{Available\ Channels}{Total\ Non-PU\ Channels}$$

where

Available Channels is the count of the channels that are empty

and

Total Non-PU Channels is the count of the channels that do not contain the PU.
E.g., let a PU utilize 1 of the 10 PAL channels, and the obfuscating SU utilize an extra 1 channel, then *Available Channels* = 8 (10 PAL channels - 1 PU occupied channel - 1 SU occupied channel) and *Total Non-PU Channels* = 9 (10 PAL channels - 1 PU occupied channel). In this example, since the SU is utilizing what could otherwise be available spectrum, the *Spectrum Sharing Efficiency* = $8/9 \approx 89\%$.

Frequency Obfuscation Efficiency

$$Frequency\ Obfuscation\ Efficiency = 1 - \frac{PU\ Occupied\ Spectrum}{Total\ Contiguous\ Occupied\ Spectrum}$$

where

PU Occupied Spectrum is the amount of spectrum (in MHz) occupied by the PU

and

Total Contiguous Occupied Spectrum is the total amount of spectrum (in MHz) occupied by both the PU and the obfuscation SU(s).

Location Obfuscation Efficiency

$$Location\ Obfuscation\ Efficiency = 1 - \frac{PU\ Location}{Total\ \#\ of\ Transmitting\ Devices}$$

where

PU Location is a constant value of 1 since there is assumed to be 1 PU location

and

Total # of Transmitting Devices is the total number of basestation locations in the occupied spectrum.

It is assumed that each PU and SU contribute to 1 unique location each. E.g., if there is one PU and 2 obfuscating SUs, *PU Location* $= 1$ and *Total # of Transmitting Devices* $= 3$, therefore the location obfuscation efficiency $\approx 67\%$.

SU Utilization In addition to the three primary metrics, a fourth metric has been included to add perspective to the behavior of each scheme. The fourth metric is SU utilization.

$$SU\ Utilization = \frac{SUs\ Utilized}{Total\ Available\ SUs}$$

This provides insight on how many SUs are deployed for obfuscation in each set of trials for the simulations.

Experiment Analysis

Obfuscation schemes one and two will be the only schemes implemented in experiment. Due to the wider bandwidths required for the second two schemes, the available equipment does not appear on the spectrum sensing plots. In the experimental trials of the obfuscation, frequency obfuscation is the only studied metric. Frequency obfuscation is calculated the same as in 5.0.4. *Total Contiguous Occupied Spectrum* is measured differently in the experiment. Derived from the VTSAS's PU detection function, a new function is created that similarly detects spectrum occupancy, however a significantly lower threshold is assigned. The sensing function averages the power of the received power and then is the average is above a certain dB threshold the function indicates there is a signal present. This function assigns the MU to spectrum sense for users in 1 MHz sections. Then, similar to the simulation, the MU reports the amount of spectrum that was found to be continuously occupied. The amount of continually sensed spectrum serves as the denominator to the frequency obfuscation equation. For these experiments, the threshold for spectrum occupancy will be set to and arbitrary 15 dB above the noise floor ($\approx$ -110 db on Relative Gain Axis).

5.0.5 Limitations

As with many research studies, there are limitations to what may be achieved given several constraints.

Cost

Sponsored by several grants, the development of the VT SAS has been awarded the support of multiple entities with unique expectations for a deliverable. Software development and research costs were provided. However the budget only allows for so many radios and the

radios can only be so powerful. Further, the server on which the software is executed may not compare to the performance of a modern supercomputer. Execution times may be insignificantly slower (¿ 1 us) than if the experiments were conducted using faster computing resources. While a larger budget would allow for these upgrades, it does not create adverse effects on the quality of the research.

Hardware

A large limitation to the research potential stems from the hardware utilized.

CORNET Server CORNET, a testbed with SDRs connected to the internet, has unstable server uptime. While the system is useful for delivering SDRs, its complex nature including several packages, dependencies, and networking permissions, all may attribute to the unstable nature of the system.

Radios The majority of the USRPs are Ettus Research B210 devices. Many of them house unique daughterboards with different supported Radio Frequency (RF) bands. Additionally, each of the B210 devices is outfitted with different unbranded antennas. The concern regarding the antennas is that different antennas are better suited for operating at different bands. Considering the typical 915 MHz Industrial, Scientific, and Medical (ISM) band usage of CORNET, utilizing the same antennas for the 3.5 GHz CBRS band may not be strongly supported. Lack of support is visible through low received power.

The largest inhibitor of experimentation is the installation of the USRPs. All 20 network attached nodes are installed in the ceilings of Kelly Hall. While the nodes are only a matter of approximately 6 meters apart, they must endure significant resistance that introduces path loss. Considering the great path loss, it is impossible for the entire network of nodes

to be able to sense each other. While it may portray a real-life SAS that covers an entire county, for research purposes, this limits the number of radios that may participate in a trial.

Another limitation of the USRPs is that wide bandwidths ($>$ 4 MHz) are not strongly sensed by the spectrum sensing node in the experiments. Since power must be preserved, as the transmit bandwidth increases, the maximum received power decreases. This limits the detection capacities that are implemented for the schemes that are to be experimented with the USRP. If a trial is to be ran with a 14 MHz signal, the current equipment cannot produce the signal with enough power for the spectrum sensing equipment to detect at this time.

Figure 5.12: Typical USRP Installation Environment (ceiling tiles removed)

As illustrated in figure 5.12, the ceilings in which these nodes are installed contain significant signal interferes. There is no direct line of sight for these nodes to communicate, so all

signals that are received are the result of a signal which has been sensed through path loss and signal bouncing. Multipath loss is another phenomenon that causes signal degradation. Considering the indirect installation of these nodes, any AOA studies would simply be a result of signal which have bounced before being received, which does not properly resemble the communications which occur over radio towers with less path loss.

Network

With regards to the network architecture including the SAS and CORNET, since CORNET is a larger server that has university permissions and is proven to allow IP traffic, it will host the SAS server in addition to the USRPs. This limitation does not restrict server or client capabilities on other hosting computers. The network limitation is simply that rather than utilizing a computing device as a server that has not undergone proper server setup that abides by university policy, CORNET has plenty of resources to allow SAS server execution. Although CORNET will host both the network-attached USRPs and the SAS server, the interactions between the two subsystems will remain the same as if the SAS were hosted by some public domain. For research purposes, there is no need to register a domain and host the SAS server on a rented server or personal laptop, although in a production-grade SAS this would be the ideal network architecture.

Incumbent Information

One hindrance to the obfuscation routine stems from the possibility that the IIC may provided buffered data to the SAS in an attempt to provide another layer of obfuscation. Clark and Psounis proposed a technique of obfuscating PU data before entering the PU data into the spectrum database [6]. For database purposes, this may be an acceptable technique,

however concerning the IIC-SAS relationship, the IIC and PU must provide truthful PU operation parameters. If the PU were to prematurely obfuscate the real operating parameters, the obfuscation routine implemented in the ASAS would incorrectly determine the frequencies to transmit for proper obfuscating which may not increase PU privacy.

Chapter 6

Results

6.1 Simulation Results

Figures 6.1, 6.2, 6.3, and 6.4 show the previously mentioned metrics for each of the four obfuscation schemes in their simulations. All four obfuscation schemes were simulated.

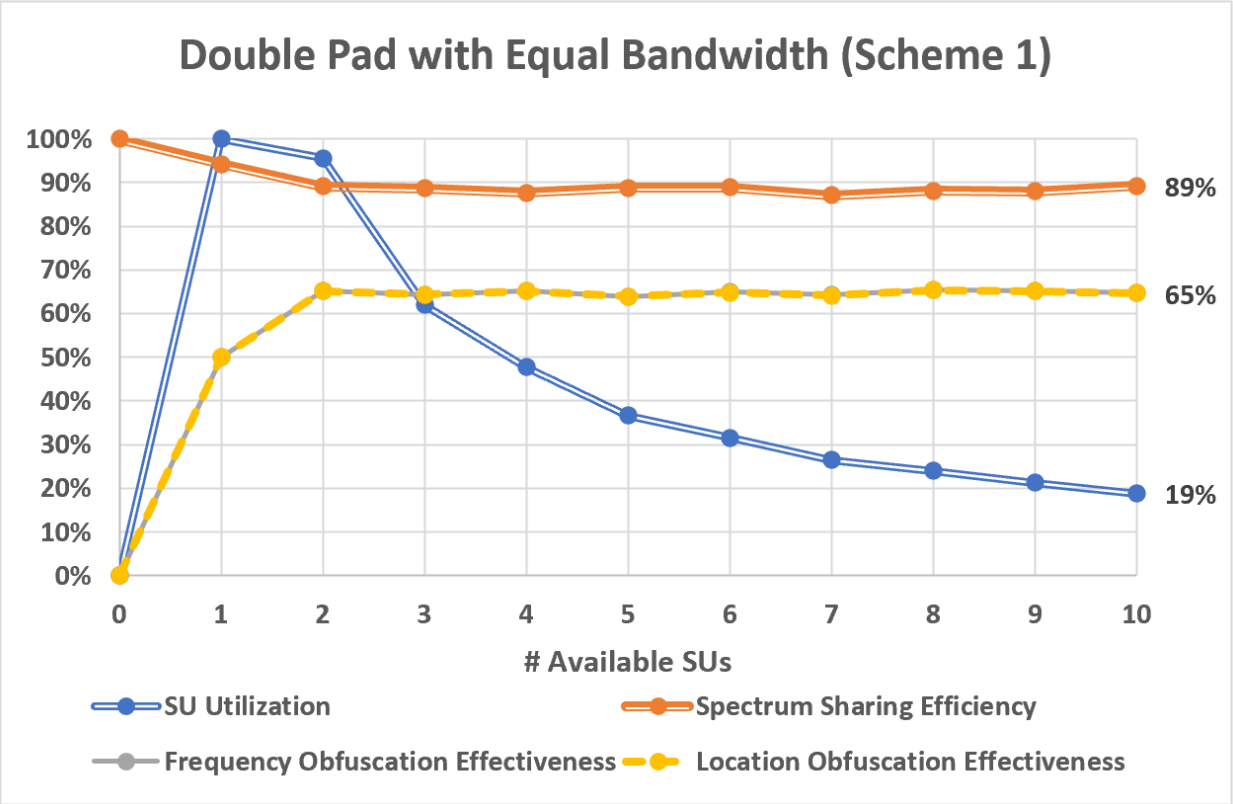

Figure 6.1: Obfuscation Scheme 1 in Simulation

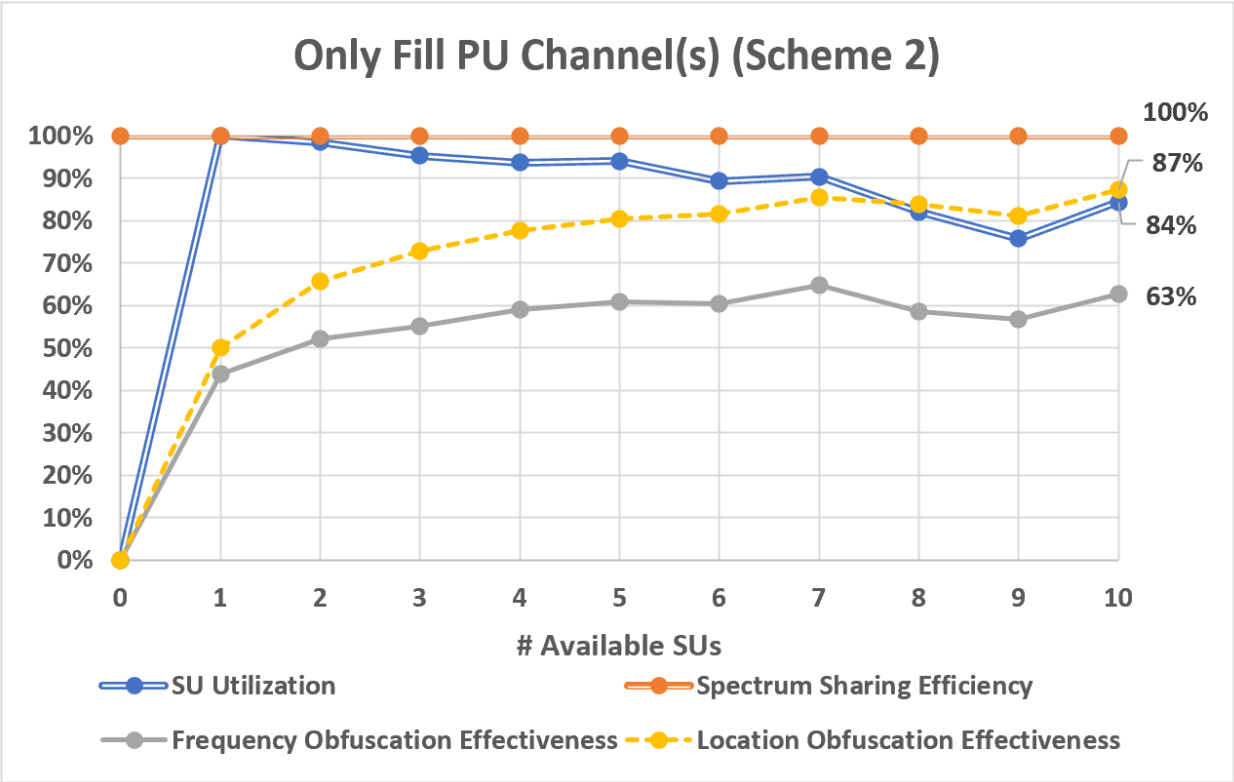

Figure 6.2: Obfuscation Scheme 2 in Simulation

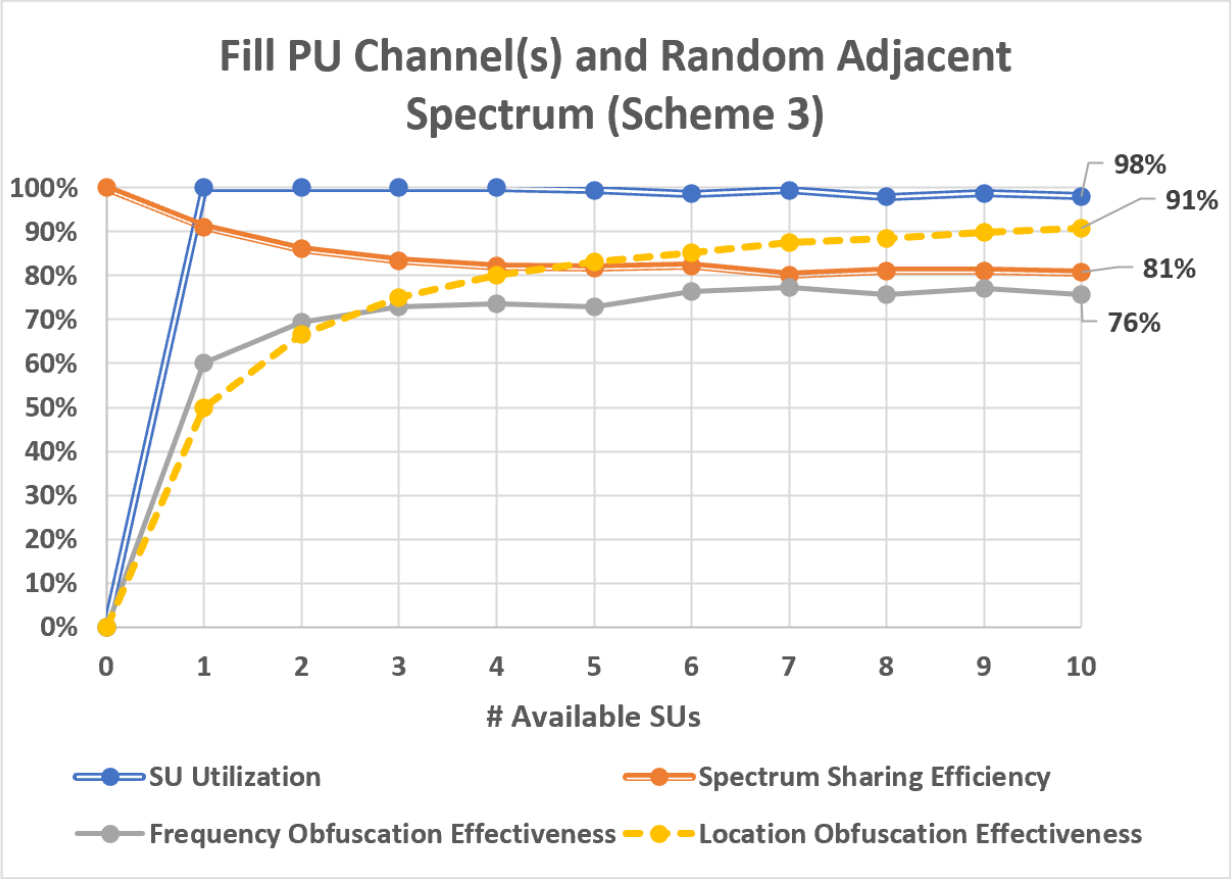

Figure 6.3: Obfuscation Scheme 3 in Simulation

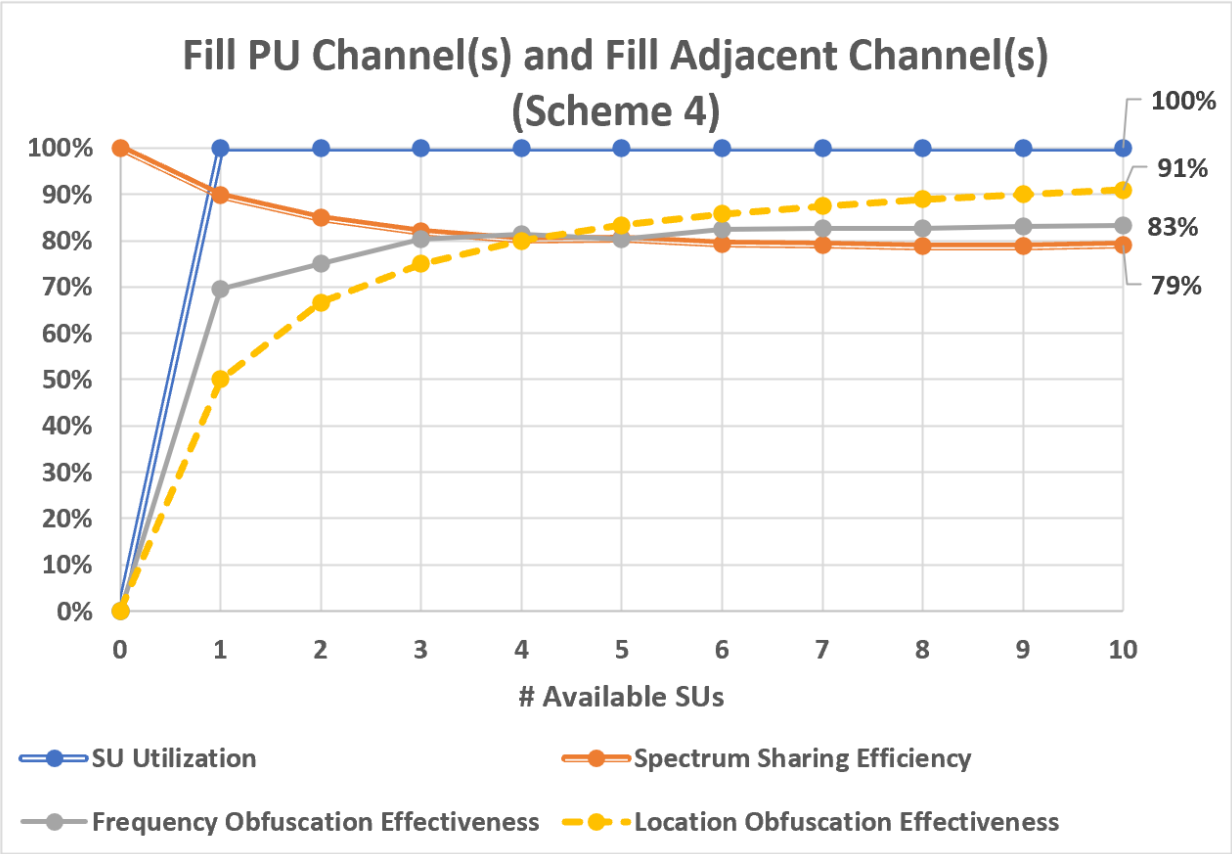

Figure 6.4: Obfuscation Scheme 4 in Simulation

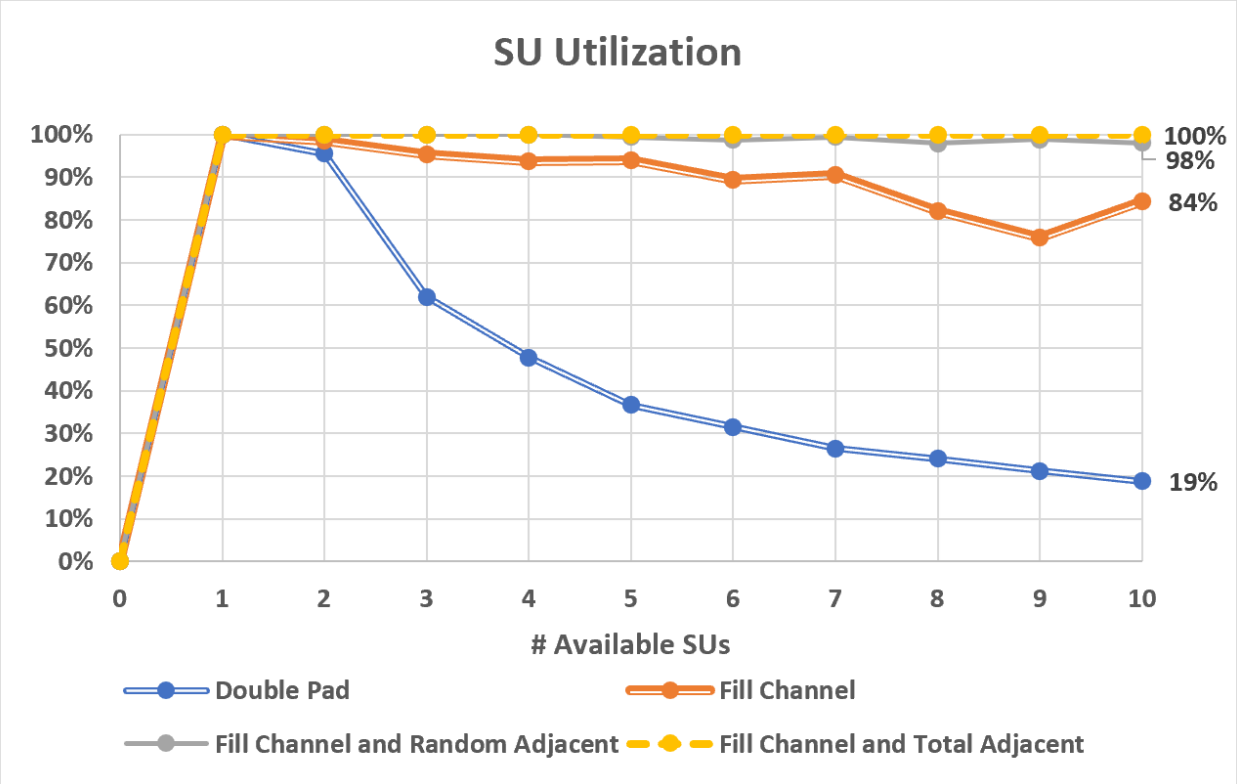

Figure 6.5: SU Utilization between All Four Schemes

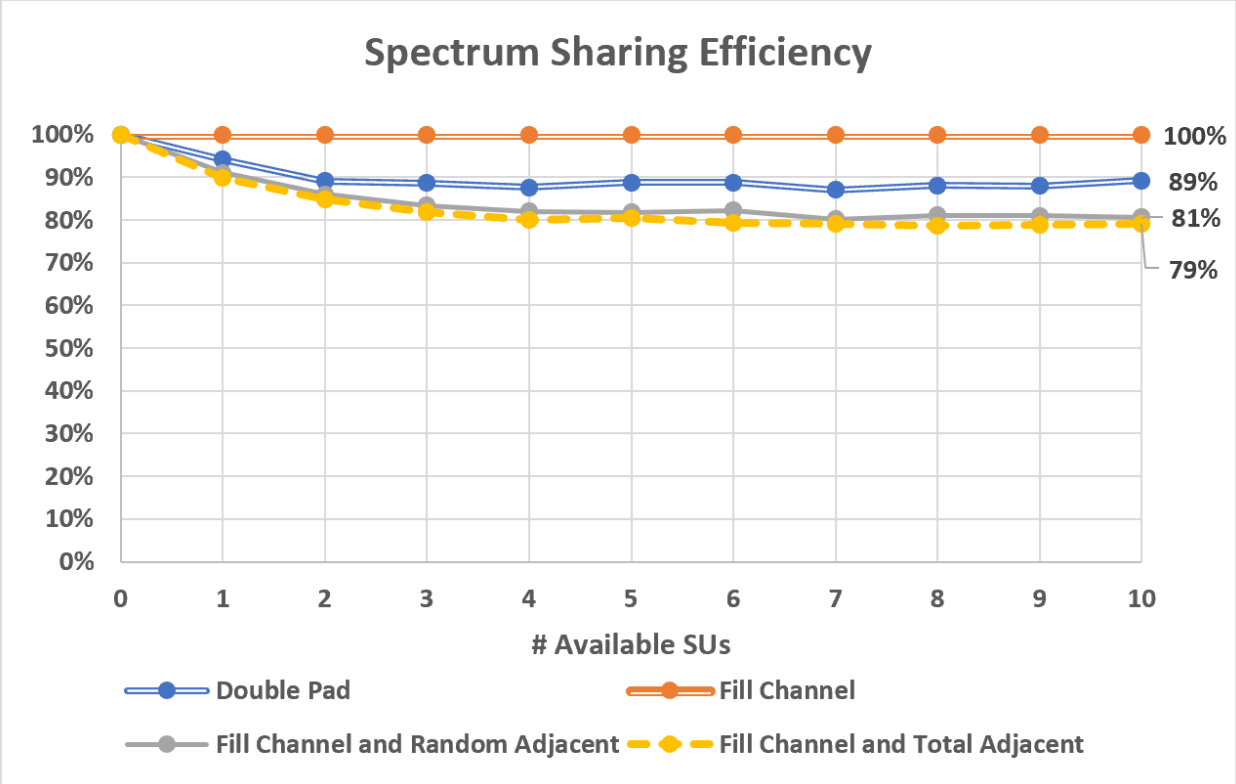

Figure 6.6: Spectrum Sharing Efficiency between All Four Schemes

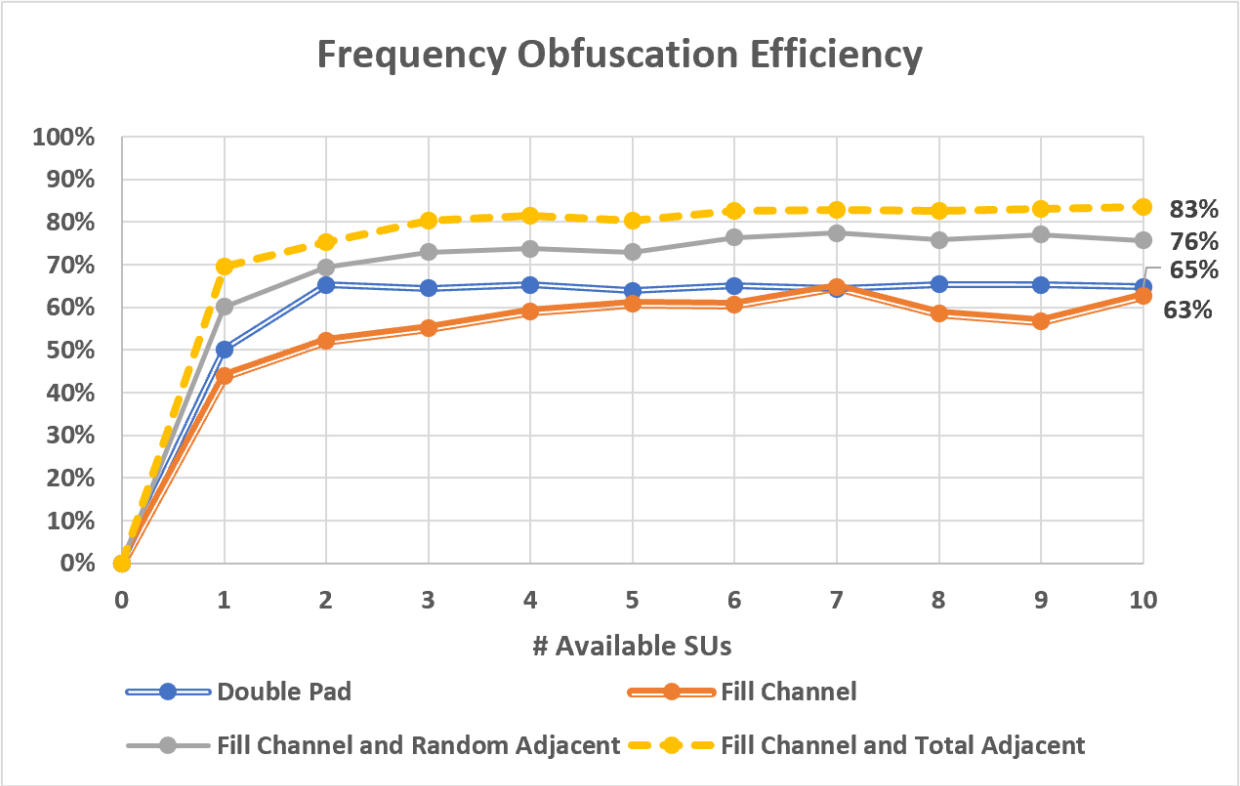

Figure 6.7: Frequency Obfuscation Efficiency between All Four Schemes

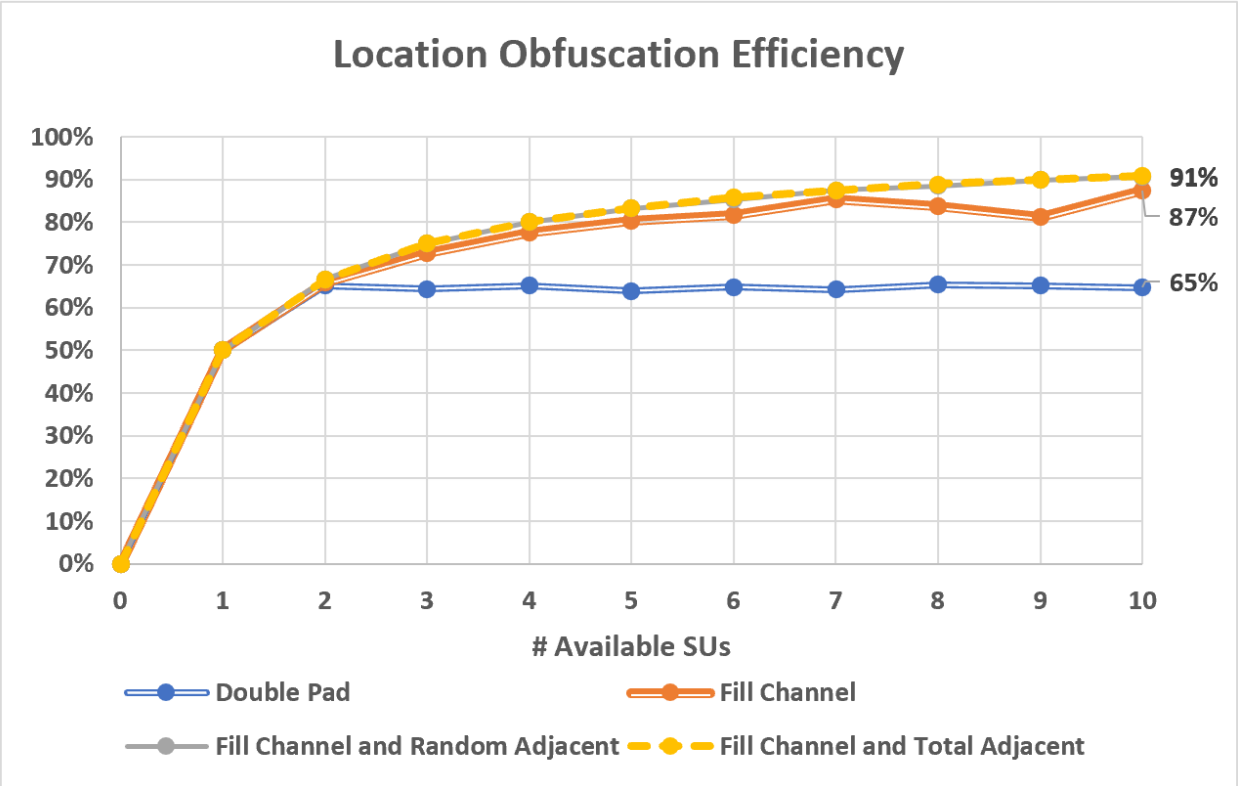

Figure 6.8: Location Obfuscation Efficiency between All Four Schemes

6.2 Experiment Results

The following four figures are the received spectrum from the perspective of the MU. The noise floor is approximated and drawn across the figures with a horizontal red bar. Obfuscation schemes *Double Pad* (scheme one) and *Fill Channel* (scheme 2) were implemented. Trials were conducted with one available SU then two available SUs.

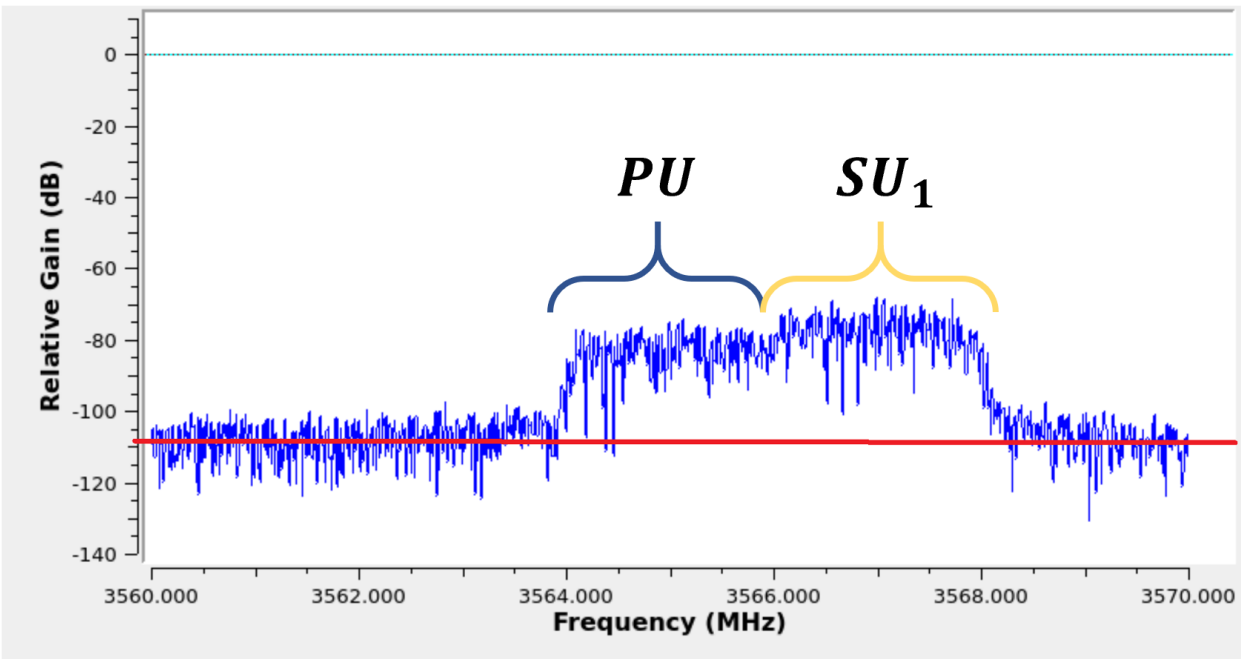

Figure 6.9: Obfuscation Scheme 1 in USRP Experiment with One SU

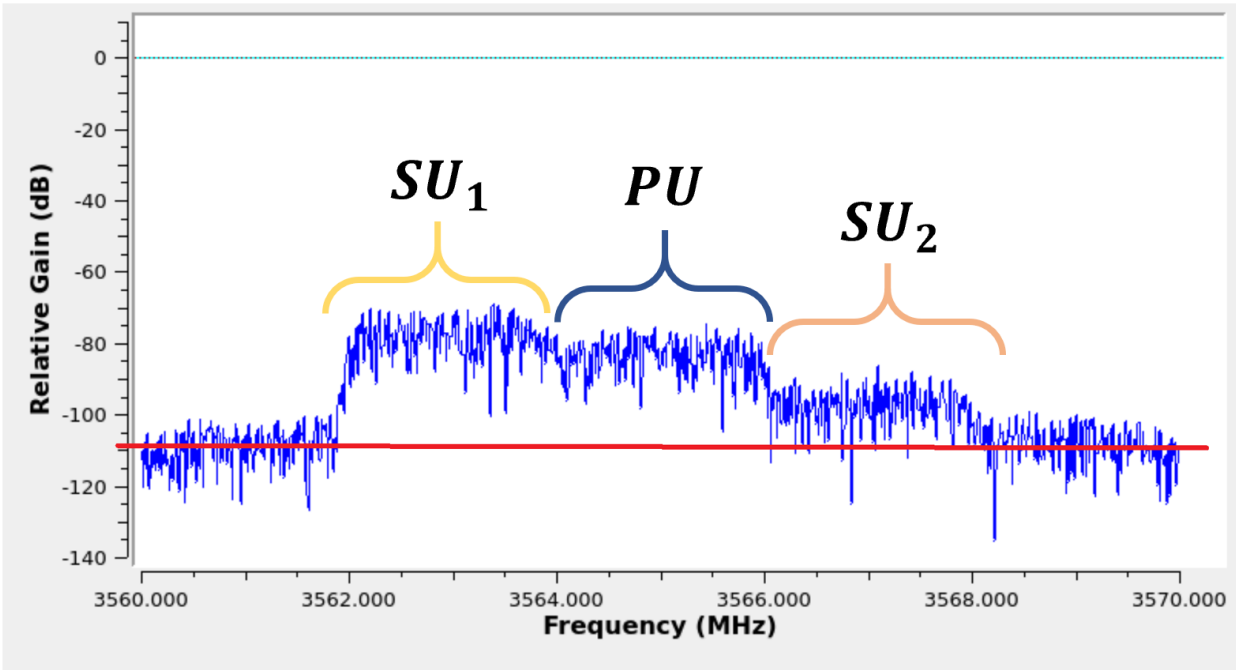

Figure 6.10: Obfuscation Scheme 1 in USRP Experiment with Two SUs

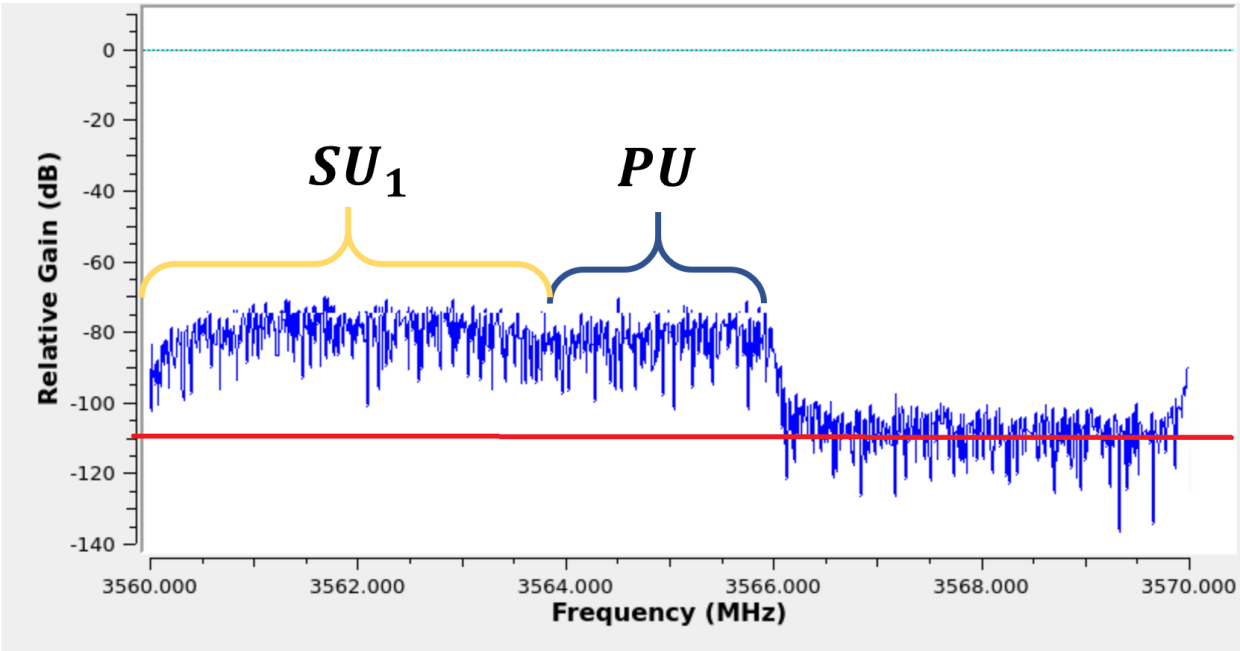

Figure 6.11: Obfuscation Scheme 2 in USRP Experiment with One SU

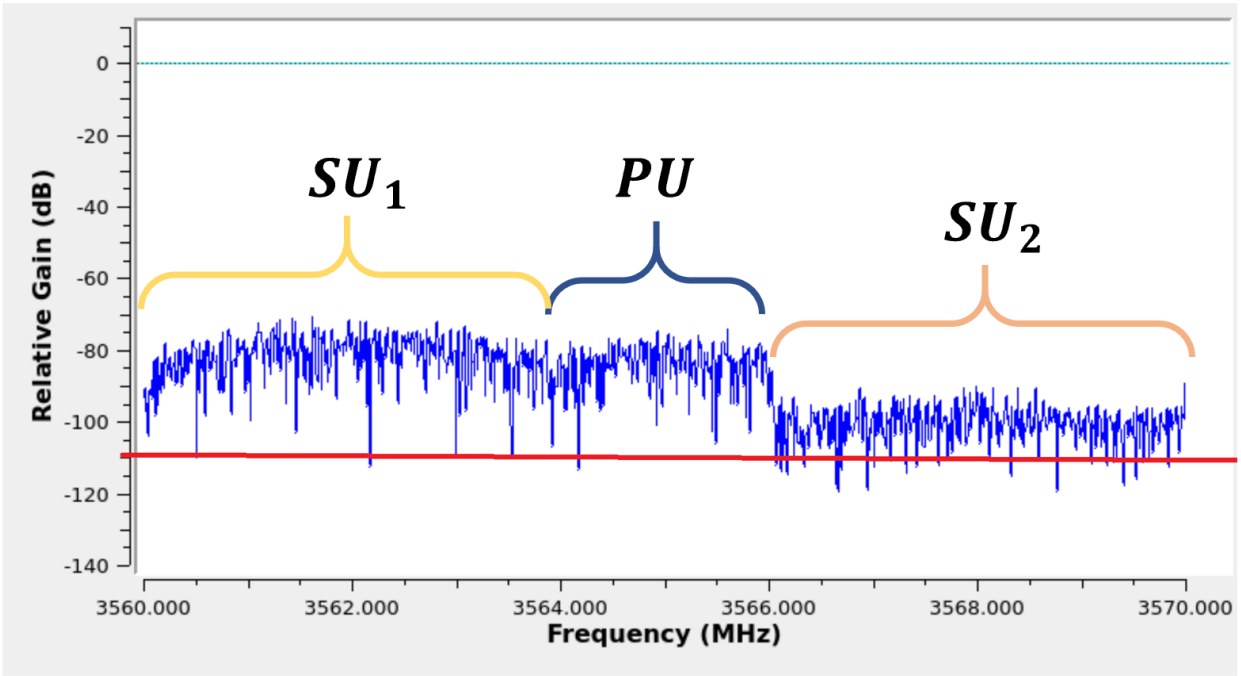

Figure 6.12: Obfuscation Scheme 2 in USRP Experiment with Two SUs

6.3 Discussion

6.3.1 Simulation Results

Double Pad (Scheme 1) The first obfuscation scheme shows equal frequency and location obfuscation. The average of the trials including only one SU shows an increase of obfuscation effectiveness of 50% from 0%. The obfuscation increase from one to two SUs however is only $\approx 15\%$. Since no more than two SUs are utilized in this scheme, the obfuscation effectiveness remains the same for all subsequent trials. Since no more than two SUs are utilized in this scheme, the SU utilization drops with each additional SU added to the list of available SUs. The spectrum sharing efficiency in this scheme stays relatively high, however it is not perfect. This means that this scheme requires the SAS to sacrifice spectrum availability from other SUs in order to provide the obfuscation.

Fill Channel (Scheme 2) This obfuscation scheme prioritizes spectrum availability. Unlike the other schemes, this scheme guarantees 100% spectrum sharing efficiency. As more SUs are added to this scheme, both obfuscation metrics increase while SU utilization drops to the 80% range for the recorded trials. The obfuscation metrics show a logarithmic increase in effectiveness as more SUs are added to the system.

Fill Channel and Random Adjacent Channel(s) (Scheme 3) This scheme extends the amount of spectrum that is used for obfuscation from scheme 2. While it is similar to scheme 2, there is a major tradeoff made – this scheme provides greater frequency obfuscation, but degrades spectrum sharing efficiency.

Fill Channel and Full Adjacent Channel(s) (Scheme 4) This scheme has marginally greater frequency obfuscation effectiveness than Scheme 3. Since adjacent channels are filled every trial, it is expected that the frequency obfuscation of this scheme would be greater than Scheme 3. SUs show 100% utilization rates. Location obfuscation increases monotonically and asymptotically.

Table 6.1: Comparison of Simulated Privacy Schemes

	SU Utilization	Spectrum Sharing Efficiency	Frequency Obfuscation Efficiency	Location Obfuscation Efficiency
Double Pad	Utilizes the least number of SUs	2nd best spectrum availability	3rd best	Worst location obfuscation
Fill Channel	High SU utilization	Perfect spectrum sharing efficiency	Worst frequency obfuscation	3rd best location obfuscation
Fill Channel and Random Adjacent	Near-maximum SU utilization	3rd best spectrum sharing efficiency	2nd best frequency obfuscation	Tied for best location obfuscation
Fill Channel and Total Adjacent	Maximum SU utilization	Worst spectrum sharing efficiency	Best frequency obfuscation	Tied for best location obfuscation

Table 6.1 displays a comparison of the different obfuscation approaches and their measured metrics. It can be seen that the scheme with the highest obfuscation efficiencies also has the worst spectrum sharing efficiency. This tradeoff is made apparent as other schemes with less obfuscation efficiency also have higher spectrum sharing efficiency.

6.3.2 Experiment Results

Double Pad with One SU (Scheme 1) Figure 6.9 shows the MU sensed spectrum during a trial of the double padding scheme with one SU. In this trial, the PU is occupying the spectrum from 3564 MHz - 3566 MHz, and the single equal bandwidth SU is occupying 3566 MHz - 3568 MHz, which can be received by the spectrum sensing MU. The MU detection function reports that there is 4 MHz of occupied spectrum. Therefore, in this trial, the frequency obfuscation effectiveness = 50%, similar to the simulated result.

Double Pad with Two SUs (Scheme 1) Figure 6.10 shows the double pad scheme with two available SUs. Since the location of the second SU is further to the MU than the first SU, the received power is lower than that of the signal transmitted by the closer SU. This exposes a limitation of the proposed obfuscation scheme.

Fill Channel with one SU (Scheme 2) Figure 6.11 shows the fill channel scheme with one SU. The SU is marked to show the dynamic nature of the channel filling scheme. It can be seen that the SU has been commanded by the SAS to obfuscate the PU by transmitting from the bottom of the channel up to the PU. The MU has reported 6 MHz of contiguous spectrum which infers a 66% frequency obfuscation effectiveness.

Fill Channel with two SUs (Scheme 2) Figure 6.12 shows the fill channel scheme with two available SUs. SU1 is well received by the MU, however since this scheme requires a wider bandwidth than the previous scheme, the PSD must be preserved, and this results in lower received signal strength from the MU. in this trial, the frequency obfuscation effectiveness is 66% again. Although it should have been 80%, SU2 is not received at a level in which the MU is trained to categorized it as occupied spectrum. While this threshold has been set

arbitrarily in this study, it emphasizes the impact that received power has on the obfuscation effectiveness of the proposed tactic.

6.3.3 Limitations / Edge Cases

MU Location

The double pad scheme with two SUs reveals a limitation of the obfuscation tactic. Since the SAS may not have any idea where a MU is located, the SUs selected for obfuscation may not be sensed by the MU. In this case, the obfuscation would not provide any additional privacy to the PU. Depending on the scheme, this may degrade spectrum availability with no added benefit.

Not addressed in the simulation or experiment is the potential of a network of MUs. There may be a case where more than one MU is spectrum sensing in collusion with other MUs. While this would increase the region in which the malicious network would be able to spectrum sense for the PU, this also increases the region in which the obfuscating SUs may be received as well. Therefore if a MU is a network or single node, the obfuscation still remains effective.

Scalability

Considering the sample sizes of the simulation and experiment, scalability is not properly addressed. Scalability with respect to the number of active PUs and SUs is an important concept to consider when implementing the novel obfuscation tactic in a busy environment. Two major situations arise when adding more PUs and SUs to the spectrum sharing band. The first situation is the one where PUs may inhabit a large majority of the band. In

this case, there will be little available spectrum for SUs to obfuscate any of the PUs. The worst case scenario for this would be the event where a single PU occupies a majority of the spectrum, making it very difficult to obfuscate with its great frequency presence.

The second situation that may arise with an increase of spectrum occupants is a lower SU utilization. Assume a situation where two PUs are operating with some amount of spectrum separating the two signals. An obfuscating SU that occupies the spectrum between the two signals may provide obfuscation to two PUs rather than just one, an in the simulation and experiment. This would lower SU utilization since fewer SUs would be required to provide the same degree of frequency obfuscation.

Millisecond Dynamic Spectrum Access

While the SAS is an enabler for Dynamic Spectrum Allocation (DSA), there are applications where more granular spectrum access time is desired, such as in cellular applications. Spectrum access on the order of milliseconds is sought after for cellular proposes. With respect to the current FCC guidelines, it appears as though the SAS archetype for managing spectrum is not tailored to rapid access. Since PAL status is auctioned, this only provides broadband providers higher spectrum access priority. The features delivered by the SAS are best suited for operation on top of any protocols provided by the broadband carrier. The SAS allows the broadband service provider to operate over the PAL channels, but once a grant is given to the service provider, it is up to the service provider to further develop protocols for rapid end user device communication to the broadband service provider's basestations. For example, it would be suggested that a broadband service provider request for a grant for an extended period of time (> 1 day), so that the end users (mobile traffic) may be managed by the broadband service provider, while the SAS provides the spectrum for the users to communicate. This eliminates the current timing restrictions set by the spectrum database

and other SAS architecture elements.

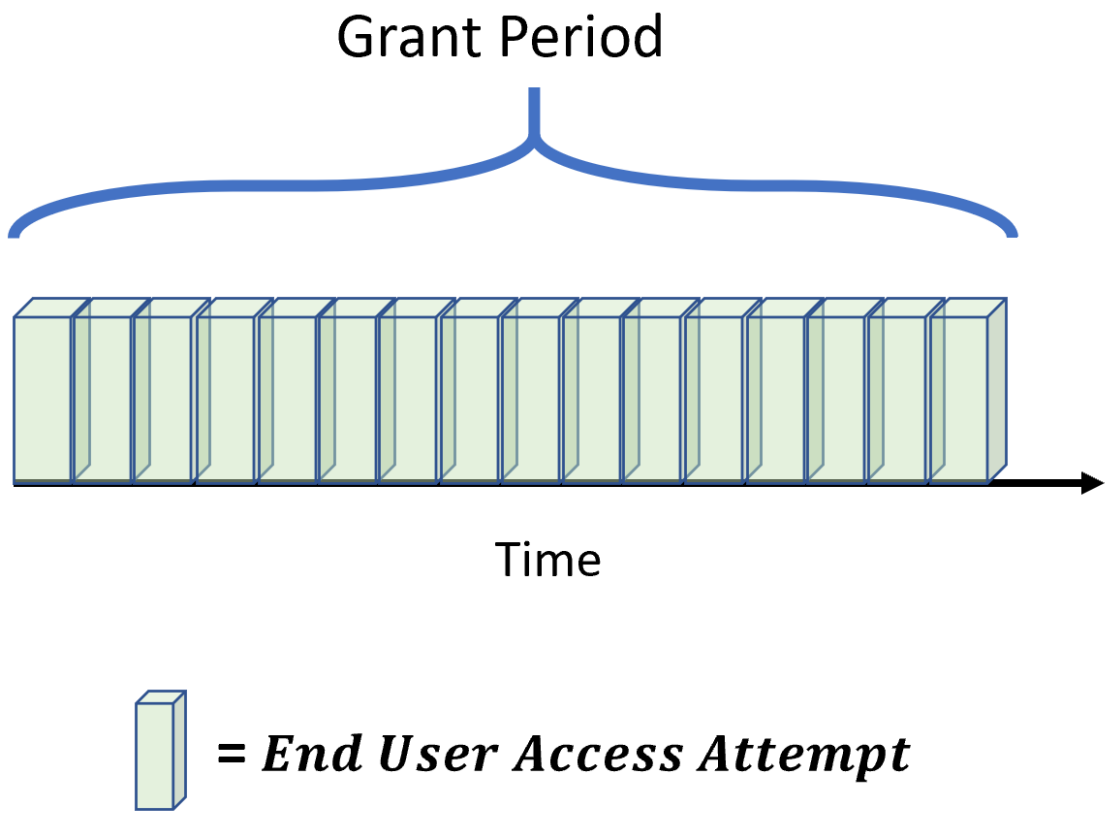

Figure 6.13: Broadband Service over SAS – End User Access would be managed by the service provider, not the SAS

Should the Heartbeat protocol be adjusted, and database querying be replaced with a faster operation, then SAS-like DSA could support the demands of cellular spectrum access, however at this time it is not an adequate solution.

Chapter 7

Conclusion

A functioning SAS has been leveraged to implement a novel PU obfuscation tactic. A framework for a client to the VTSAS was detailed and implemented. A novel PU privacy tactic has been proposed. Four novel obfuscation schemes have been simulated and two of which were experimented. Simulation shows PU obfuscation with 50% - 91% effectiveness with varying spectrum sharing efficiencies. PU obfuscation is shown to be achievable with no reduction in spectrum availability to other users. Experiments prove that the PU obfuscation tactic is feasible on a SAS with IIC and SU transmission permission and control.

7.1 Future Work

7.1.1 Malicious User Transmission Interference

Another feature that may be enabled by the ASAS is the ability to interfere with the operation of MUs. Motivation for this feature may vary. One given motivation for this feature is as a punishment for nodes that have falsely reported spectrum data. A key motivator for

spectrum occupancy falsification is as follows: A user may own multiple CBSDs. One CBSD reports that a SAS channel appears to be occupied. This then results in the SAS clearing any SUs on that channel. Now the MU may assume that there is an empty channel for one of their other nodes to operate over without SAS authorization, since the SAS may now assume a PU occupied that region and had to remove any SUs that were granted in that channel. With this structured attack on the SAS, if the SAS detects the malicious intent of the user that is now operating illegally, the advanced SAS would have the ability to transmit over the MU's signal, thus punishing them by destroying their communications. While that is one use for the SAS transmission capability, this introduces communications jamming capabilities which may be useful for other applications, especially in defense, should the SAS architecture be replicated in other operating regions. Communications jamming techniques escape the

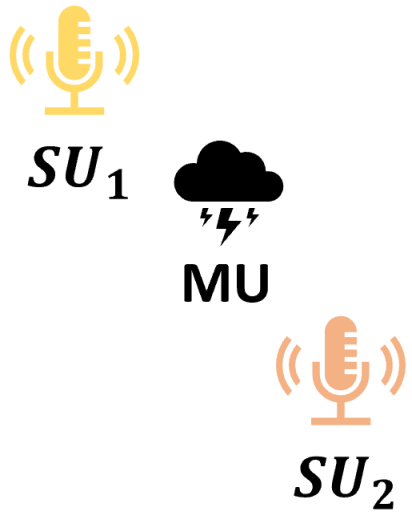

Figure 7.1: SAS-induced MU Communications Jamming Basestation Map

scope of this Thesis, however it is noted that full control of multiple transmitters with known locations, various communications jamming techniques may be suitable for such application. Co-channel and adjacent channel interference are prospects for MU jamming. Figure 7.2 shows the spectrum in the scenario where a MU is detected transmitting in a channel. The

two SUs that are geographically nearby the source of MU operation are assigned to transmit a more powerful signal in the same band and adjacent to the MU.

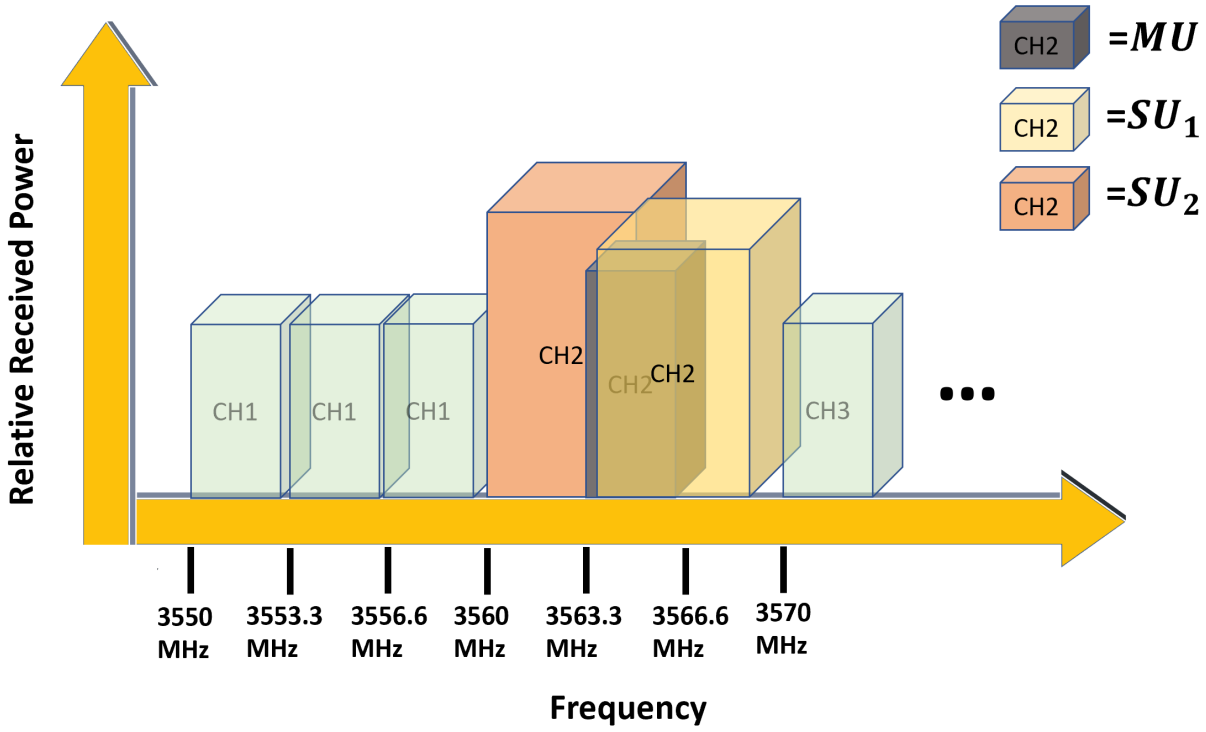

Figure 7.2: MU Jamming Concept

7.1.2 ASAS PU Obfuscation Routine - Time Obfuscation

Another dimension of PU obscurity besides frequency and location privacy includes occupancy time privacy. Not demonstrated in the simulation is the obfuscation of PU spectrum entry and departure time. Both of the previous techniques ideally would be implemented together along with a time masking element. In order to mask PU operation time, since the SAS has prior knowledge of when the PU will transmit, the SAS may occupy the respective spectrum channel earlier in time to create the illusion that the PU may have initiated trans-

mission. Once the SAS expects the PU to enter the region, it may open the specific band the PU will transmit over, while leaving the adjacent bands still occupied. In an ideal situation, the spectral power will remain constant during this transition. Likewise, once the PU ends transmission, the SAS may utilize another CBSD to replace the PUs transmission over the band so that the exit of the PU remains difficult to identify. Introducing this dimension of privacy provides greater PU operation privacy. This feature would further obfuscate the PU's activity and increase difficulty for MUs to identify the PU's behavior.

7.1.3 Multi-Tactic Primary User Privacy

Further, those interested in enhancing PU privacy should seek to implement multiple of the previously reviewed PU privacy strategies from table 3.1 along with the ASAS PU obfuscation routine. Many of the privacy techniques are mutually exclusive in design which allows them to be implemented in parallel.

7.1.4 Spectrum Access System Development

The newly developed open source SAS and client create a great potential for further development and research in many different areas of research. Machine learning may be leveraged to create better PU and MU detection systems. Those interested in system security have the option to implement any new security features that may resist SAS data breaches and misuse. Research institutes with networked SDRs may utilize the server and client code to conduct their own spectrum sensing experiments. One particular experiment of interest would include using the MUltiple SIgnal Classification (MUSIC) algorithm for AOA or other proposed Direction of Arrival (DOA) algorithms [19] in conjunction with crowdsourced SDR data.

7.2 List of Contributions

As a result of all of the efforts mentioned in this Thesis, major contributions to the research community have been provided. A majority of the work that has been leveraged for this Thesis resides in implementation efforts of an open source spectrum access system and framework for SAS clients.

7.2.1 Virginia Tech Spectrum Access System

The largest contribution made is the creating of an open source spectrum access system. This system is an accumulation of large and plentiful Python scripts. Divided into two sections, there is the SAS server available for use, and there is a client that was created for CORNET, but servers as a framework for any network of USRPs. The client has been utilized for the construction of this text as demonstrated by figures 5.9 and 5.10. Written with modularity in mind, the client provides a foundation for any other researcher to reuse the client code.

Available on GitHub at URL: https://github.com/vtwireless/SAS.

7.2.2 Primary User Obfuscation Schemes

As a result of a literature review regarding PU privacy, it was made clear that there is a lack in real world approaches to PU obfuscation. Key elements required to deliver real world were identified, justified, and implemented. A proof of concept ASAS is described in detail as being capable of delivering the obfuscation that is proposed. Simulations are included to demonstrate the effectiveness of the proposed obfuscation schemes.

7.2.3 Publications

Additional contributions to research take form in co-authored papers.

Spectrum Trust Comparisons in a Crowdsourced Sharing Environment is a survey on the current state of trustworthiness in crowdsourced radio spectrum occupancy information. This text details the great importance of accurately detecting a PU with crowdsourced data, and the issues faced due to MUs sending invalid data. A study on SAS decision making with crowdsourced data is provided.

Optimizations and Additional Features of Spectrum Access System Heartbeat Protocol is a paper which studies the capabilities of the Heartbeat routine required by the FCC for county SASs. Currently, there are no standards with respect to Heartbeat timing, so simulations show the capabilities of the underlying network technology that would deliver Heartbeat functionality between a SAS and CBSDs. Further, extensions to Heartbeat payload data is proposed in order to enhance SAS capabilities.

Survey of Radar and Communications Spectrum Sharing is a Systematization of Knowledge encompassing a large number of publications relative to dynamic spectrum sharing. Over 200 publications are summarized in this survey.

Bibliography

[1] Behnam Bahrak, Sudeep Bhattarai, Abid Ullah, Jung-Min Jerry Park, Jeffery Reed, and David Gurney. Protecting the Primary Users' Operational Privacy in Spectrum Sharing. In *2014 IEEE International Symposium on Dynamic Spectrum Access Networks (DYSPAN)*, pages 236–247. IEEE, 2014.

[2] A. Ben Mosbah, T. A. Hall, M. Souryal, and H. Afifi. An analytical model for inference attacks on the incumbent's frequency in spectrum sharing. In *2017 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*, pages 1–2, 2017. doi: 10.1109/DySPAN.2017.7920770.

[3] Cisco. Cisco annual internet report (2018–2023) white paper, 2020. URL https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html.

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

[5] Matthew Clark and Konstantinos Psounis. Achievable privacy-performance tradeoffs for spectrum sharing with a sensing infrastructure. In *2018 14th Annual Conference*

on Wireless On-demand Network Systems and Services (WONS), pages 103–110. IEEE, 2018.

[6] Matthew Clark and Konstantinos Psounis. Optimizing Primary User Privacy in Spectrum Sharing Systems. *IEEE/ACM Transactions on Networking*, 28(2):533–546, 2020.

[7] Matthew A Clark and Konstantinos Psounis. Trading utility for privacy in shared spectrum access systems. *IEEE/ACM transactions on networking*, 26(1):259–273, 2017.

[8] Michael DiFrancisco, Edward Drocella, Charles J Cooper, and Paul Ransom. Incumbent Informing Capability (IIC) for Time-Based Spectrum Sharing. *Available at SSRN 3748483*, 2020.

[9] X. Dong, T. Zhang, D. Lu, G. Li, Y. Shen, and J. Ma. Preserving Geo-Indistinguishability of the Primary User in Dynamic Spectrum Sharing. *IEEE Transactions on Vehicular Technology*, 68(9):8881–8892, 2019. doi: 10.1109/TVT.2019.2929592.

[10] Yanzhi Dou, Kexiong (Curtis) Zeng, Yaling Yang, and Kui Ren. Preserving Incumbent Users' Privacy in Exclusion-Zone-Based Spectrum Access Systems: Poster. In *Proceedings of the 22nd Annual International Conference on Mobile Computing and Networking*, MobiCom '16, page 473–474, New York, NY, USA, 2016. Association for Computing Machinery. ISBN 9781450342261. doi: 10.1145/2973750.2985283. URL https://doi-org.ezproxy.lib.vt.edu/10.1145/2973750.2985283.

[11] FCC. 3.5 ghz band overview, . URL https://www.fcc.gov/wireless/bureau-divisions/mobility-division/35-ghz-band/35-ghz-band-overview.

[12] FCC. FCC expands flexible use of the c-band for 5g, . URL https://www.fcc.gov/document/fcc-expands-flexible-use-c-band-5g-0.

[13] FCC. FCC spectrum allocation table, . URL https://transition.fcc.gov/oet/spectrum/table/fcctable.pdf.

[14] FCC. Part 96 citizens broadband radio service, 2021. URL https://www.ecfr.gov/cgi-bin/text-idx?node=pt47.5.96.

[15] GNU. Gnu radio. URL https://wiki.gnuradio.org/index.php/Main_Page.

[16] Mohamed Grissa, Attila Altay Yavuz, and Bechir Hamdaoui. Location privacy in cognitive radios with multi-server private information retrieval. *IEEE Transactions on Cognitive Communications and Networking*, 5(4):949–962, 2019.

[17] M. Hammouda, M. El-Khamy, and M. El-Sharkawy. Frequency Multiplexed Spectrum Sensing for Enhanced Primary User Protection. In *2012 8th International Conference on Wireless Communications, Networking and Mobile Computing*, pages 1–4, 2012. doi: 10.1109/WiCOM.2012.6478528.

[18] H. Li, Y. Dou, C. Lu, D. Zabransky, Y. Yang, and J. J. Park. Preserving the Incumbent Users' Location Privacy in the 3.5 GHz Band. In *2018 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*, pages 1–10, 2018. doi: 10.1109/DySPAN.2018.8610470.

[19] P. Neesen, M. Meuleners, and C. Degen. A novel doppler-based direction-of-arrival estimation scheme. In *2018 25th International Conference on Telecommunications (ICT)*, pages 148–153, 2018. doi: 10.1109/ICT.2018.8464889.

[20] V. Rajpoot and V. S. Tripathi. A Novel Algorithm for Protection of Primary Receiver in Cognitive Radio Network. In *2017 14th IEEE India Council International Conference (INDICON)*, pages 1–5, 2017. doi: 10.1109/INDICON.2017.8487822.

[21] A. Robertson, J. Molnar, and J. Boksiner. Spectrum Database Poisoning for Operational Security in Policy-Based Spectrum Operations. In *MILCOM 2013 - 2013 IEEE Military Communications Conference*, pages 382–387, 2013. doi: 10.1109/MILCOM.2013.72.

[22] WInnForum. About the WInnForum, . URL https://www.fcc.gov/wireless/bureau-divisions/mobility-division/35-ghz-band/35-ghz-band-overview.

[23] WInnForum. WInnForum CBRS knowledge base, . URL https://cbrs.wirelessinnovation.org/standards.

[24] WInnForum. WInnForum members, . URL https://cbrs.wirelessinnovation.org/membership.

[25] WInnForum. Signaling protocols and procedures for citizens broadband radio service (cbrs):spectrum access system (sas) -citizens broadband radio service device (cbsd) interface technical specification, NOVEMBER 2020. URL https://winnf.memberclicks.net/assets/CBRS/WINNF-TS-0016.pdf.

[26] WInnForum. Fcc spectrum access system (sas) administrators, NOVEMBER 2020. URL https://cbrs.wirelessinnovation.org/sas-administrators.

[27] Z. Zhang, H. Zhang, S. He, and P. Cheng. Bilateral Privacy-Preserving Utility Maximization Protocol in Database-Driven Cognitive Radio Networks. *IEEE Transactions on Dependable and Secure Computing*, 17(2):236–247, 2020. doi: 10.1109/TDSC.2017.2781248.