SECURE AND EFFICIENT DYNAMIC SPECTRUM ACCESS SOLUTIONS FOR FUTURE WIRELESS NETWORKS

by
Qingqing Cheng

Dissertation submitted in fulfilment of the requirements
for the degree of

DOCTOR OF PHILOSOPHY

under the supervision of

Prof. Eryk Dutkiewicz
Dr. Diep N. Nguyen

School of Electrical and Data Engineering
University of Technology Sydney
Sydney, Australia

September 2019

ABSTRACT

The future wireless communication network (5G and beyond) is expected to provide many advantages, such as an extremely high peak rate, ultralow latency and less energy consumption. However, since an extremely large number of connecting devices will be deployed, the demand for the spectrum will also be growing exponentially, causing a problem of spectrum shortage. To effectively address the spectrum crunch, dynamic spectrum access (DSA), including both sensing-based and database-driven DSA, has been proposed.

In this thesis, we investigate critical challenges in DSA, including the efficiency in sensing-based techniques and privacy in database-driven techniques. First, to improve the sensing performance of the sensing-based DSA in half-duplex (HD) systems, we propose two sensing approaches leveraging the property of deep learning networks. Our solutions are significantly superior in terms of the robustness to noise uncertainty, timing delay, and carrier frequency offset (CFO), compared to conventional sensing methods. Moreover, our work does not require any prior information of signals, which however is essential for the traditional sensing methods. Second, to improve the sensing performance of sensing-based DSA in full-duplex (FD) systems, we develop two novel sensing methods using the features of orthogonal frequency division multiplexing (OFDM) signals. The developed sensing approaches are robust to not only residual SI but also timing delay or CFO. We also obtain the closed-form expressions of the probability of detection and false alarm for our approaches. Third, to protect the users' privacy in

the database-driven DSA, we develop two schemes to protect the operational privacy of Incumbent Users (IUs) and honest/dishonest Secondary Users (SUs). To implement our proposed work, we introduce an interference calculation scheme that allows users to calculate an interference budget without revealing operational information. It also reduces the computing overhead of our developed approaches. Additionally, we propose a "punishment and forgiveness mechanism to encourage dishonest SUs to provide truthful information. Theoretical analysis and extensive simulations show that our proposed schemes can better protect all users' operational privacy under various privacy attacks, yielding higher spectrum utilization with less online overhead, compared with state of the art approaches.

CERTIFICATE OF ORIGINAL AUTHORSHIP

I, QINGQING CHENG, declare that this thesis, is submitted in fulfilment of the requirements for the award of DOCTOR OF PHILOSOPHY, in the Faculty of Engineering and Information Technology at the University of Technology Sydney.

This thesis is wholly my own work unless otherwise reference or acknowledged. In addition, I certify that all information sources and literature used are indicated in the thesis.

This document has not been submitted for qualifications at any other academic institution.

This research is supported by the Australian Government Research Training Program.

Name of Student: Qingqing Cheng

Production Note:
Signature of Student: Signature removed prior to publication.

Date: 07/01/2020

ACKNOWLEDGMENTS

First and foremost, I would like to express my sincere gratitude to my supervisors Prof. Eryk Dutkiewicz and Dr. Diep N. Nguyen, for all the guidance, encouragement, and enduring patience. Prof. Dutkiewicz and Dr. Nguyen have taught me a lot on both the scientific and personal side of the research journey. Their guidance and support go far beyond this thesis, and I have been greatly fortunate to be supervised by them.

My deep appreciation goes to Associate Prof. Andrew Zhang and Dr. Markus Dominik (Intel Deutschland GmbH, Germany) for their insightful advice and continuous encouragement on my research and industry collaborations. I would like to thank Dr. Gengfa Fang, Dr. Forest Zhu and Dr. Yang Yang for their kind help during my PhD study. Furthermore, many thanks to all the staff from the School of Electrical and Data Engineering, University of Technology Sydney, for various forms of help they gave to me. I would like to thank all my colleagues and friends for their support and company.

Last but most importantly, my deepest gratitude, love and respect offer to my whole families. My loving husband, Zhenguo Shi, has been supporting me to go through all difficult times during this long journey. Without his infinite love, inspiration and patience, this work could never been accomplished. My beloved grandparents, parents and sisters have been supporting and encouraging me with every possible way as they always did. Their love, sacrifice and patience will be the constant source of motivation throughout my life.

Dedicated to My Beloved Husband, Parents and Grandparents

Contents

List of Figures

List of Tables

List of Publications

Journal publications

- **Qingqing Cheng**, Zhenguo Shi, Diep N. Nguyen, Eryk Dutkiewicz, "Sensing OFDM Signal: A Deep Learning Approach", *IEEE Transactions on Communications (TCOM)*, 2019, DOI: 10.1109/TCOMM.2019.2940013 (Corresponding to Chapter 3)

- **Qingqing Cheng**, Diep N. Nguyen, Eryk Dutkiewicz, Markus Mueck, "P-reserving Honest/Dishonest Users' Operational Privacy with Blind Interference Calculation in Spectrum Sharing System", *IEEE Transactions on Mobile Computing (TMC), 2019*, DOI: 10.1109/TMC.2019.2936377. (Corresponding to Chapter 5)

- **Qingqing Cheng**, Zhenguo Shi, Diep N. Nguyen, Eryk Dutkiewicz, "Sensing OFDM Signals in Full-duplex Systems with Residual Self-interference, Timing Delay and Carrier Frequency Offset", to be submitted to *IEEE Transactions on Communications (IEEE TCOM)* (Corresponding to Chapter 4)

Conference publications

- **Qingqing Cheng**, Eryk Dutkiewicz, Gengfa Fang, Zhenguo Shi, Diep N. Nguyen, Huiyang Wang, "A Novel Full-Duplex Spectrum Sensing Algorithm

for OFDM Signals in Cognitive Radio Networks", in *IEEE Global Communications Conference (GLOBECOM)*, Dec 2017, pp. $1-6$. (Corresponding to Chapter 4)

- **Qingqing Cheng**, Zhenguo Shi, Diep N. Nguyen, Eryk Dutkiewicz, "An OFDM Sensing Algorithm in Full-Duplex Systems with Self-Interference and Carrier Frequency Offset", accepted to *IEEE Global Communications Conference (GLOBECOM)*, 2019. (Corresponding to Chapter 4)

- **Qingqing Cheng**, Diep N. Nguyen, Eryk Dutkiewicz, Markus Mueck, "P-reserving operational information in spectrum access system with dishonest users", in *17th International Symposium on Communications and Information Technologies (ISCIT)*, Sep 2017, pp. $1-6$. (Corresponding to Chapter 5)

- **Qingqing Cheng**, Diep N. Nguyen, Eryk Dutkiewicz, Markus Mueck, "Protecting operational information of incumbent and secondary users in FCC spectrum access system", in *IEEE International Conference on Communications (ICC)*, May 2018, pp. $1-6$. (Corresponding to Chapter 5)

- **Qingqing Cheng**, Zhenguo Shi, Diep N. Nguyen, Eryk Dutkiewicz, "Non-cooperative OFDM Spectrum Sensing Using Deep Learning", accepted to appear at *International Conference on Computing, Networking and Communications (ICNC)*, 2020. (Corresponding to Chapter 3)

Other

- Zhenguo Shi, Andrew Zhang, Richard Xu, **Qingqing Cheng** "Deep learning networks for human activity recognition with CSI correlation feature extraction", in *IEEE International Conference on Communications (ICC)*, May 2019, pp. $1-6$.

- Asanka Kekirigoda, Kin-Ping Hui, **Qingqing Cheng**, Zhipeng Lin, Andrew Zhang, Diep N. Nguyen, Xiaojing Huang, "Massive MIMO for Tactical Ad-hoc Networks in RF Contested Environments", accepted to *IEEE Military Communications Conference (MILCOM)*, 2019.

- Huiyang Wang, Diep N. Nguyen, Dinh T. Hoang, Eryk Dutkiewicz, **Qingqing Cheng**, "Real- Time Crowdsourcing Incentive for Radio Environment Maps: A Dynamic Pricing Approach", in *IEEE Global Communications Conference (GLOBECOM)*, Dec, 2018, pp. $1 - 6$.

- Zhenguo Shi, Zhilu Wu, Zhendong Yin, Zhutian Yang, **Qingqing Cheng**, "Novel Markov channel predictors for interference alignment in cognitive radio network", in *Wireless Networks*, Vol. 24, Iss. 6, 2018.

Abbreviations

AWGN Additive white Gaussian noise

ANN Artificial Neural Network

BPSK Binary phase shift keying

BICS Blind interference calculation scheme

CFO Carrier frequency offset

CBSD Citizens Broadband Radio Service Device

CDMA Code Division Multiple Access

CRNs Cognitive radio networks

CNN Convolutional neural network

CSS Cooperative spectrum sensing

CM Covariance matrix

CP Cyclic Prefix

CRC Cyclic Redundancy Check

DL Deep learning

DoS Denial of service

DoD Department of Defense

DSA Dynamic spectrum access

ED Energy detection

ETSI European Telecommunications Standardization Institute

FFT Fast Fourier transform

FCC Federal Communications Commission

FSS Fixed Satellite System

FD-AC Frequency domain autocorrelation

FD Full-duplex

GMM Gaussian mixture model

GAA General Authorized Access

HD Half-duplex

HAAT Height above average terrain

IDN Identity number

IUs Incumbent users

KNN K-nearest-neighbor

LSA Licensed Shared Access

LRT Likelihood ratio test

LAT Listen and talk

LBT Listen before talk

ML Machine learning

MCMC Markov Chain Monte Carlo

Massive MIMO Massive Multiple-input and multiple-output

MIMO Multiple-input and multiple-output

NDE Negative decision error

NDER Negative decision error ratio

NOMA Non-orthogonal multiple access

OFDM Orthogonal frequency-division multiplexing

OFDMA Orthogonal frequency-division multiple access

PT Pilot Tone

PDE Positive decision error

PDER Positive decision error ratio

PUs Primary users

PA Priority Access

PAL Priority Access license

PSEO Privacy-preserving scheme with encryption and obfuscation methods

PF Punishment and forgiveness

RLSs Radio Location Services

ROC Receiver operating characteristic

RNN Recurrent neural network

RHs Reputation histories

RSs Reputation scores

SCM Sampled covariance matrix

SUs Secondary users

SINR Signal-to-interference-plus-noise ratio

SNR Signal-to-noise ratio

SAS Spectrum Access System

SAE Stacked autoencoder

SAE-SS Stacked autoencoder based spectrum sensing method

SAE-SS-AF SAE-SS with additional features

SAE-TF Stacked autoencoder based spectrum sensing method with time-frequency domain signals

SAE-TF-AF SAE-TF with additional features

SVM Support vector machine

TDMA Time Division Multiple Access

TDE Total decision error

TDER Total decision error ratio

TS-1 Training strategy 1

TS-2 Training strategy 2

Chapter 1

Introduction

This chapter provides an overview of this thesis. In Section 1.1, we introduce the background of the wireless communication system, including the advantages and drawbacks of conventional wireless networks, followed by the benefits and challenges of future wireless communications. In Section 1.2, we present the motivations and key contributions of this thesis. Section 1.3 shows the organization of the thesis.

1.1 Background

In recent decades, the wireless communication system has experienced a rapid development and has made a great impact around the world. Compared the wired networks, wireless systems are capable of offering many advantages. The principal benefit should be the mobility that enables the users to roam within its network range and access real-time information [1]. In other words, instead of getting disconnected from the network, users of wireless systems are allowed to stay connected to the network when they move within its network coverage. Second, the wireless network system can be installed in places that are not accessible for wires, thereby providing a wider network range. Another advantage of wireless networks is that it is much simpler and faster to configure a wireless system in a new place than building a wired network. Last but not least, the wireless systems can be easily changed or updated depending on the specific requirements of applications, which however is quite difficult for wired systems [1].

The first generation of wireless system (1G), a voice-only system, was initiated in the 1980s. Since then, wireless networks have been experiencing very rapid development, towards the second (2G), third (3G), and fourth generation wireless systems (4G) [2]. These generational systems have introduced a wide variety of techniques or standards to meet the increasing demands of wireless systems. For instance, the Code Division Multiple Access (CDMA) and Time Division Multiple Access (TDMA) were introduced in 2G to multiplex several users. Although these techniques were able to improve the spectral efficiency over 1G, the theoretical (downlink) speed was still very slow (e.g., 50kbps) [2]. To offer a higher transmission speed, various wireless techniques were released in 3G, e.g., wideband CDMA (with a downlink speed of 400kbps). In 4G, several key techniques (e.g., multiple-input multiple-output, MIMO and Orthogonal frequency-division multiple access, OFDMA) were proposed to provide much higher data rates that can be up to several hundred million bits per second (Mbps) [3].

Even after decades of rapid growth, traditional wireless technology still faces several challenging problems. First of all, an extremely large number of connecting devices (e.g., 50 billion by 2020 [4]) would result in a huge increase in mobile data volume. Second, the wireless users are expected to experience high data rates, e.g., at least 1Gb/s in 95 percent and 5Gb/s in 20 percent of workplaces, respectively [5]. Third, ultra-low latency and ultra-high reliability, e.g., with less than 5 ms end-to-end latency and with 99.999 percent reliability, are required to support a new range of applications, e.g., industry automation, intelligent transportation systems [5]. Last but not least, the energy consumption needs to be continuously reduced without degrading the communication performance. All the above challenges are beyond the capability of traditional wireless networks, which significantly restrict the rapid development of wireless communications. Therefore, the explosive growth of traffic volume, notable increase in connected devices, ultra-low latency, and super high reliability are the challenging issues that need to be addressed.

With the rapid growth of wireless communications in recent years, the future wireless systems (i.e., fifth generation wireless systems, 5G and beyond) are widely studied. A wide range of techniques or standards are proposed/released to meet

the increasing demands for wireless communications, e.g., Massive multiple-input and multiple-output (Massive MIMO), Beamforming, Edge computing, and non-orthogonal multiple access (NOMA) [6]. To name a few, Massive MIMO is one of the key techniques in future communication systems, which aims to increase the system capacity using a large number of antennas. Beamforming is to improve the signal quality and data transfer speeds. The basic idea is to combine elements in an antenna array so that the signals at desired angles would experience constructive interference while others would suffer from destructive interference [6, 7].

With these core techniques, the future wireless networks (i.e., 5G and beyond) are expected to address the challenging tasks of the conventional wireless technologies. More specifically, compared to the traditional wireless systems (e.g., $4G$), future wireless communication networks are envisioned to offer the following benefits [8]:

- 1000 times higher mobile data volume per area,
- 10 to 100 times higher transmission data rate,
- 10 to 100 times higher number of connecting devices,
- 5 times of reduced end-to-end latency,
- 10 times longer battery life for low-power massive machine communication.

Therefore, future wireless systems have the capability to provide wireless communications with much better performance. Besides, the future wireless systems can be employed in many applications and scenarios [5]. To name a few, for the dense urban information society, the data volume of future wireless networks can be up to 9Gbytes/h in busy periods. For the virtual reality office, with future wireless techniques, the maximum data rate can be from 1Gbps to 10Gbps. For smart grid networks, the reliability of future wireless communications can be achieved at 99.999%. Regarding the deployment of sensors and actuators, each access point will be able to support about 3×10^5 connecting devices [5]. These applications would significantly revolutionize almost every aspect of our life, e.g., education, home control systems, health care, military, and government.

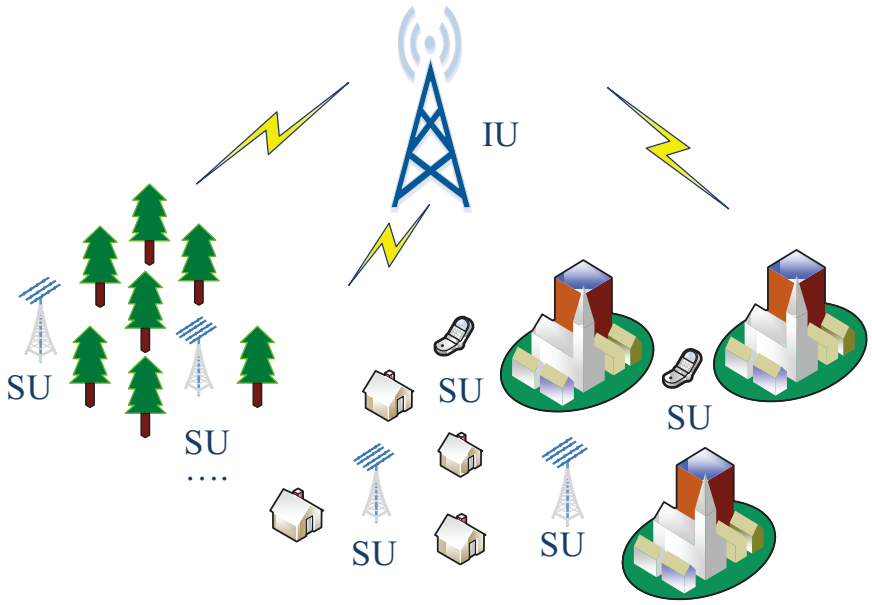


Figure 1.1: Spectrum allocation in dynamic spectrum access.

Although the future wireless network will be more capable of significantly improving communication performance than the prior systems, several technical challenging problems are yet to be resolved, e.g., spectrum shortage [7, 9]. With the increase in the number of connecting devices, the demand for the spectrum resource is also explosively growing. However, the available spectrum resource is limited and the spectrum utilization for the existing frequency bands is quite inefficient, causing a problem of spectrum shortage. For that, two possible options can be used to tackle the issue of spectrum shortage, exploiting new spectrum resources and improving the spectrum utilization for the existing frequency bands. Since the entire spectrum resource is finite, it is not realistic to continuously exploit extra new frequency bands. By contrast, utilizing the existing spectrum channels more efficiently becomes a wiser way to deal with the spectrum scarcity. For that purpose, dynamic spectrum access (DSA), one of the most important candidates for spectrum management, has been proposed and has attracted considerable attention.

To effectively facilitate DSA, standard bodies like the Federal Communications Commission (FCC) and the European Telecommunications Standardization Institute (ETSI) have been proposing spectrum management frameworks that adopt DSA or spectrum sharing as a core feature [10]. The basic idea of DSA is to

enable the opportunistic access of unoccupied or under-utilized licensed bands, so as to improve the spectrum usage of wireless communications. Specifically, in DSA, unlicensed users are allowed to opportunistically access temporarily idle or under-utilized spectrum bands of licensed users [11,12]. These unlicensed users are referred to as secondary users (SUs), and licensed users are known as primary users (PUs) or incumbent users (IUs), as shown in Fig. 1.1.

Although many DSA methods have been investigated in the existing literature, further study/work is still required for the following reasons. First, the performance of current DSA methods is susceptible to various communication conditions (e.g., noise uncertainty and timing delay) in wireless environments. These conditions would dramatically degrade the efficiency of spectrum utilization, leading to fewer spectrum bands for transmitting radio signals and more severe interference on data transmission. Besides, a large number of served users leads to an increase in energy cost. How to improve energy efficiency, i.e., more throughput with the same energy consumption, is also a challenging task for DSA in future wireless systems [7]. Second, the security issue in DSA is also one of the key problems for future wireless communications. Since radio signals that include communication information are transmitted through the wide space, potential adversaries may attack or eavesdrop on the communication links to damage or obtain the confidential data, such as the denial of service (DoS) attacks. Security attacks would lead to many harmful impacts on data communication, commercial interest or even national safety.

Among the above technical challenges, in this work, we will focus on the key challenges of DSA in future wireless networks, especially the efficiency and security solutions. In the context of DSA, SUs cannot cause harmful interference to IUs when utilizing the corresponding licensed spectrum channels; they are required to be capable of sensing or being informed by spectrum databases about IUs' activity states, which can be categorized as sensing-based DSA and data-based DSA. For sensing-based DSA, also known as spectrum sensing, SUs must determine the availability of IUs' licensed channels using sensing techniques, before using those channels for data transmission. The sensing task can be performed in half-duplex (HD) mode or full-duplex (FD) mode [13]. For HD-based spectrum sensing,

with the same frequency bands and time resource, SUs can perform either the sensing/reception or data transmission [14]. For FD-based spectrum sensing, over the same frequency channels, the sensing and transmission tasks can be conducted simultaneously [15]. For the data-based DSA, users are required to report their information to databases that allocate spectrum based on the received data from users. SUs are not allowed to use IUs' licensed bands for data transmission until successfully receiving the notification from the database [10].

Although both the sensing-based and data-based DSAs have the capability to effectively utilize the under-utilized licensed bands of IUs, they still face several challenging issues. For the sensing-based DSA methods, they are susceptible to various communication conditions, e.g., timing delay, carrier frequency offset (CFO), noise uncertainty [16]. For instance, the energy detection (ED) is very sensitive to noise uncertainty [17]. The sensing methods utilizing the orthogonal frequency-division multiplexing (OFDM) signals are sensitive to timing delay and CFO. A small error between the transmitted and received signals in the time or frequency domain will dramatically degrade the sensing results. Besides, it is quite difficult for sensing-based DSA to obtain reliable sensing results in low Signal-to-noise ratio (SNR) conditions [16, 18]. For data-based DSA methods, the security issue is a major concern. Specifically, to accomplish spectrum sharing, users' confidential information (e.g., location, frequency channels and transmitting power... [19, 20]) is required to share with the database. In such a case, potential adversaries can attack the communication links and obtain users' private data. Since users may be operated by governments or commercial institutions, the leakage of private information would result in having a harmful influence on the national security or the commercial interest [21].

1.2 Motivations and Contributions

To address the above challenging and significant problems, in this work, we propose different methods/schemes. Our work mainly focuses on efficiency and security solutions in DSA. For sensing-based DSA, we study the efficiency issue of spectrum

sensing. We develop two novel sensing methods to realize an efficient spectrum allocation in HD systems, by leveraging the properties of deep learning networks. In FD systems, we propose two novel feature-based sensing methods using Cyclic Prefix (CP) and Pilot Tone (PT) features of OFDM signals, so as to mitigate the severe effect of self-interference, timing delay and CFO. For the data-based DSA, we investigate the security problem of spectrum sharing. To deal with that concern, we propose a scheme to fully protect all users' (both IUs' and SUs') private information, meanwhile successfully realizing spectrum utilization. The main contributions of this thesis are summarized as follows.

- We develop two novel OFDM sensing frameworks utilizing the properties of deep learning networks. Specifically, we first propose a stacked autoencoder based spectrum sensing method (SAE-SS), in which a stacked autoencoder network is designed to extract the hidden features of OFDM signals for classifying the users' activities. Compared to the conventional OFDM sensing methods, SAE-SS is significantly superior in the robustness to noise uncertainty, timing delay, and CFO. Moreover, SAE-SS requires neither any prior information of signals (e.g., signal structure, CP or PT features) nor explicit feature extraction algorithms which, however, are essential for the conventional OFDM sensing methods. To further improve the sensing accuracy of SAE-SS, especially under low SNR conditions, we propose a stacked autoencoder based spectrum sensing method using time-frequency domain signals (SAE-TF). SAE-TF achieves higher sensing accuracy than SAE-SS using the features extracted from both time and frequency domains, at the cost of higher computational complexity. (Chapter 3).

- We investigate the issue of spectrum sensing with imperfect self-interference suppression in FD systems. By drawing support from a CP feature and PT feature of OFDM signals, respectively, we propose two novel spectrum sensing mechanisms. The CP method is robust to self-interference and timing delay. Comparing with other conventional CP sensing approaches in FD systems, the proposed CP method is independent of timing delay. That significantly

improves the sensing performance, even without requiring a complex process for timing delay estimation. Besides, the developed PT sensing approach holds the advantage in robustness not only to residual SI but also CFO, in comparison with the conventional sensing methods in FD systems. The proposed PT sensing method is able to accomplish sensing tasks in low SNR conditions with much lower computational complexity. (Chapter 4)

- We investigate the operational privacy issue of IUs and honest/dishonest SUs in SAS. For the case of IUs and honest SUs, we propose a privacy-preserving scheme for DSA by leveraging encryption and obfuscation methods (PSEO). To implement PSEO, we introduce an interference calculation scheme that allows users to calculate an interference budget without revealing operational information (e.g., antenna height, transmit power, location...), referred to as the blind interference calculation scheme (BICS). BICS also reduces the computing overhead of PSEO, compared with FCCs SAS by moving interference budgeting tasks to local users and calculating it in an offline manner. To further save the overhead in calculating the interference map, we introduce a quantization method and optimize the grid sizes of the terrestrial area of interest. Additionally, for the case of IUs and dishonest SUs, we propose a punishment and forgiveness (PF) mechanism, which draws support from SUs reputation scores (RSs) and reputation histories (RHs), to encourage SUs to provide truthful information. (Chapter 5)

1.3 Thesis Organization

The remainder of the thesis is organized as follows, as also illustrated in Fig. 1.2.

In Chapter 2, we provide a comprehensive literature review of efficient and secure solutions in DSA in recent years. We first introduce an overview of DSA, including the sensing-based and data-based systems in Section 2.1. Then, in Section 2.2, we present the efficiency issue and its corresponding solutions in HD-based DSA. Section 2.3 states the spectrum utilization of DSA in FD systems. Section 2.4 shows the security problem in data-based DSA.

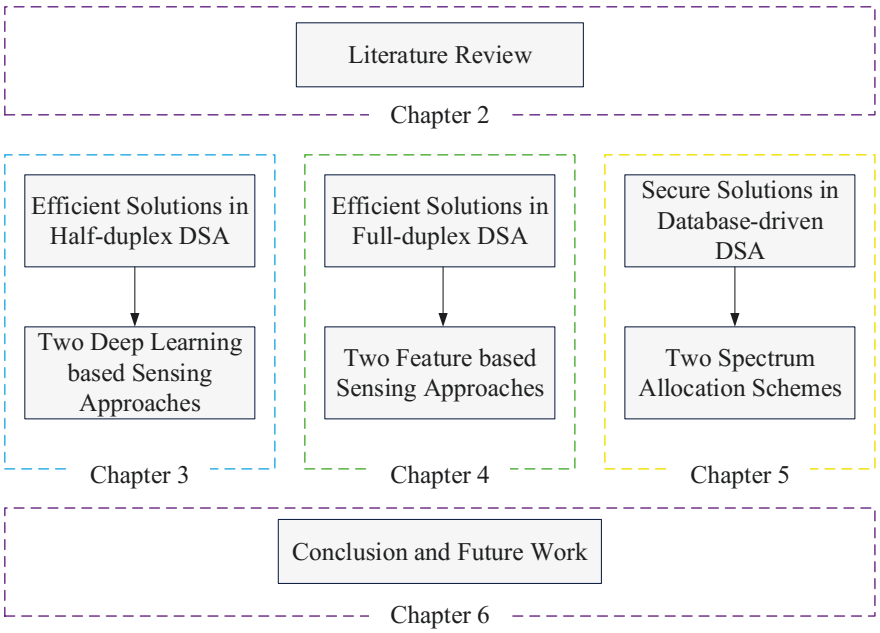


Figure 1.2: Thesis Organization.

In Chapter 3, we propose two novel spectrum sensing methods in HD systems, drawing support from the features of deep learning networks. We first provide an introduction to show state-of-the-art work in this area. The system model and problem formulation are provided in Section 3.2. Then, we develop the proposed sensing method using the signals from the time domain in Section 3.3. To further improve the sensing performance, especially under low SNR conditions, in Section 3.4, we present the sensing method adopting the signals from the time domain and frequency domain. The complexity analysis and other discussions about the proposed methods are stated in Section 3.5. In Section 3.6, we demonstrate numerical simulations results to verify the sensing performance of proposed methods. Finally, we summarize conclusion in Section 3.7.

In Chapter 4, we investigate the spectrum utilization in the FD system with residual self-interference and propose two novel sensing approaches to mitigate the residual self-interference and timing delay or CFO. In Section 4.1, we present the up-to-date relevant work about spectrum sensing methods in FD systems and analyze their disadvantages. In Section 4.2, we state the system model and problem formulation. The CP-based sensing method that is robust to timing delay and residual self-interference is presented in Section 4.3. In Section 4.4, we propose a PT-based

method that has the advantage of robustness to residual self-interference and CFO. We show extensive simulation results in Section 4.5, to evaluate the performance of proposed methods. The conclusion is summarized in Section 4.6.

In Chapter 5, we investigate the privacy preservation in SAS released by FCC and develop two schemes to successfully accomplish the spectrum allocation and fully protect all users' private information. In Section 5.1, the related work about privacy protection in SAS and the corresponding drawbacks are provided. Then, we present the system model of SAS and problem formulation in Section 5.2. In Section 5.3, we present a scheme to protect the operational privacy of IUs and honest SUs. To preserve the private information of IUs and dishonest SUs, we propose a scheme using punishment and forgiveness mechanism in Section 5.4. In Section 5.5, we express the quantization of attenuation map and the other discussions about the proposed schemes. The performance analysis of proposed schemes is demonstrated in Section 5.6. The simulation results and the conclusion are given in Section 5.7 and Section 5.8.

Finally, in Chapter 6, we conclude the main work in this thesis and describe the directions for future work.

Chapter 2

Literature Review

We investigate a large number of previous literature and ongoing work to illustrate the recent development of efficient and secure solutions in DSA. Specifically, Section 2.1 provides an overview of the current discussion for DSA. Section 2.2 describes newly proposed methods for the efficient issue in half-duplex spectrum sensing methods. Section 2.3 describes the same issue in full-duplex spectrum sensing approaches. Section 2.4 presents the security issue in spectrum sharing architectures, with a special focus on the market in the U.S.

2.1 Dynamic Spectrum Access

In recent years, an unprecedented development in wireless devices and applications has posed a critical demand for radio spectrum resource that is quite tight. However, the spectrum of licensed frequency bands is usually under-utilized, resulting in low average occupancy values. As such, improving the spectrum utilization of the existing frequency bands is the key to the success of wireless communications [6,22]. As an enabling technology for spectrum sharing, DSA has recently gained very considerable attention. To protect IUs from adverse interference, SUs must either be performing spectrum sensing techniques or being informed by spectrum databases about spectrum opportunities. In the following section, we will present detailed information about sensing-based DSA and data-based DSA.

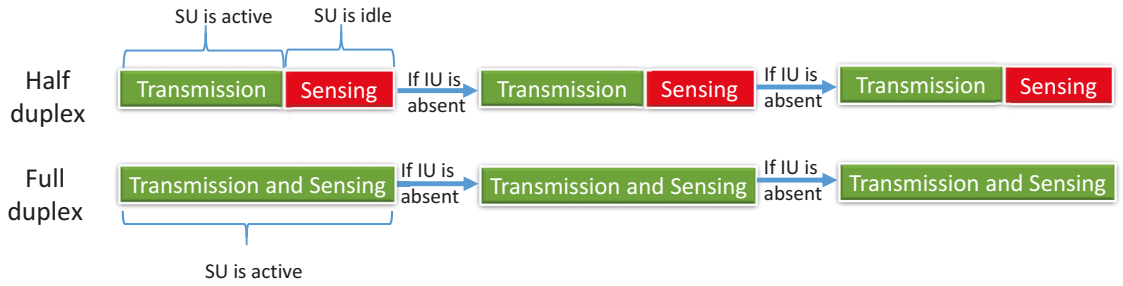


Figure 2.1: Spectrum sensing in half-duplex and full-duplex modes.

2.1.1 Sensing-based Dynamic Spectrum Access

Sensing-based DSA, also known as spectrum sensing, has attracted significant interest in its application to cognitive radio networks (CRNs). Under sensing-based DSAs, licensed but under-utilized spectrum bands of IUs are open for SUs with different access priority levels. To avoid harmful interference to IUs as well as to comply with the granted priority right, SUs are required to detect the activity of IUs (e.g., absence or presence). Reliable spectrum sensing allows SUs to occupy or vacate the spectrum bands, depending on the activity of IUs and other prioritized users [a] [23]. If IUs are detected as "absence", SUs start to utilize those channels for data transmission, or otherwise vacate those channels. In sensing-based DSA, SUs accomplish sensing tasks following either half-duplex (HD) or full-duplex (FD) communication paradigms, as shown in Fig. 2.1.

In HD systems, as illustrated in Fig. 2.1, users follow the traditional "listen before talk" (LBT) principle under which, at each time, users can conduct either the transmission or reception/sensing using the same frequency [24]. In other words, under LBT principle, with the same time resource, SUs users either sense the activity states of IUs in the corresponding bands or use those frequency bands for data transmission [25]. According to Fig. 2.1, the whole traffic of the SU is divided into two periods which do not happen simultaneously: sensing period and transmission period. To be specific, before using IU's licensed bands for data transmission, SU must determine that IU is absent from the channel. To do that, in the sensing

[a] Without loss of generality, in this work, we refer to all higher prioritized users (including IUs) as IUs and lower prioritized users as SUs.

period, SU analyzes the signals observed/captured by sensing detectors. This SU will start to utilize the IU's channel to send its packet during the transmission period when it detects the idle channel (i.e., IU is absent). If that IU restarts to use this licensed frequency band, SU will be informed and must interrupt its transmission and vacate that channel immediately. Under this situation, SU will switch to the sensing mode to seek other spectrum opportunities.

Although the LBT under HD paradigms is able to protect IUs from excessive interference caused by SUs, it actually dissipates the precious time resource and inevitably suffers from the following problems. First, SU has to sacrifice its transmission time for spectrum sensing. To be specific, in HD systems, the whole traffic of SU in HD systems has to be divided into several small slots for either sensing or data transmission. In such a case, SU's data transmission is split into several discontinuous slots, even if the spectrum hole (i.e., IU is absent on its channel) is continuous. Second, the spectrum sensing under HD paradigms may lead to collision or spectrum waste. For example, during the data transmission section, SUs cannot detect any action performed by IUs (e.g., arrivals or departures) at all until the next sensing section start. As a result, IUs may leave the spectrum band while SUs are unaware of it or IUs arrive at the spectrum band while the band is being used by SUs. Thus, the LBT may lead to a waste of spectrum resource (e.g., SUs do not sense the departures of IUs) or a high collision rate (e.g., SUs are not aware of the arrivals of IUs) [26]. In other words, the LBT principle in HD paradigms unavoidably increases the reaction time of SUs and reduces the throughput of both SUs and IUs [27]. For these reasons, extensive efforts have been recently made to improve SUs' spectrum awareness by enabling them to transmit and sense the medium at the same time, which boosts the development of FD radios.

In FD systems, as shown in Fig. 2.1, users are able to transmit and receive/sense signals on the same frequency channel simultaneously. In other words, FD radios allow users to sense the spectrum/medium during its whole traffic period, referred to as the "listen and talk" (LAT) protocol [14]. Using this principle, unlicensed SUs can sense the presence of licensed IUs while transmitting its data packets using the same time interval over the same frequency band (when IU is absent). From Fig. 2.1,

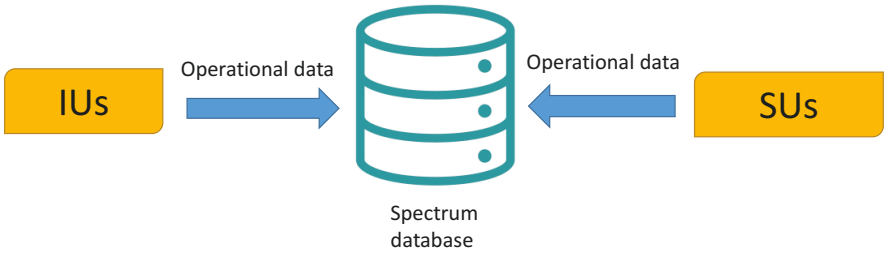


Figure 2.2: Architecture of data-based spectrum sharing.

SU's whole traffic also includes two periods (i.e., sensing period and transmission period) that can happen simultaneously. Specifically, after determining the lack of the IUs on the licensed channel, SU starts to use this channel for transmitting its packet; meanwhile, it keeps sensing the IU's states. If IU is detected as active on the licensed channel, SU will pause its transmission and vacate the channel instantly.

2.1.2 Data-based Dynamic Spectrum Access

In addition to spectrum sensing, data-based DSA has also been considered as a promising solution for addressing spectrum shortage. The basic principle of this technique is that SUs obtain the availability of IU's licensed bands by notifications from the database, instead of sensing techniques. Specifically, as illustrated in Fig. 2.2, for the purpose of spectrum allocation and interference protection, IUs provide their up-to-date operational information (e.g., locations and operating frequency bands) and the protection requirements to the database. SUs are also required to report their transmission parameters to a database for requesting IU's spectrum resource. Based on the received information from IUs and SUs, the database is able to allocate specific IU's channels that are temporarily idle or under-utilized to SUs without causing harmful interference to the corresponding IUs. It is important to note that SUs are not allowed to utilize IU's licensed frequency channels until successfully receiving the information from the database.

In recent years, a large number of data-based spectrum sharing architectures have been proposed, e.g., Licensed Shared Access (LSA) released by ETSI and Spectrum Access System (SAS) adopted by FCC. LSA was firstly released in 2011 to ensure the protection for the license holders and secondary licensees operating at

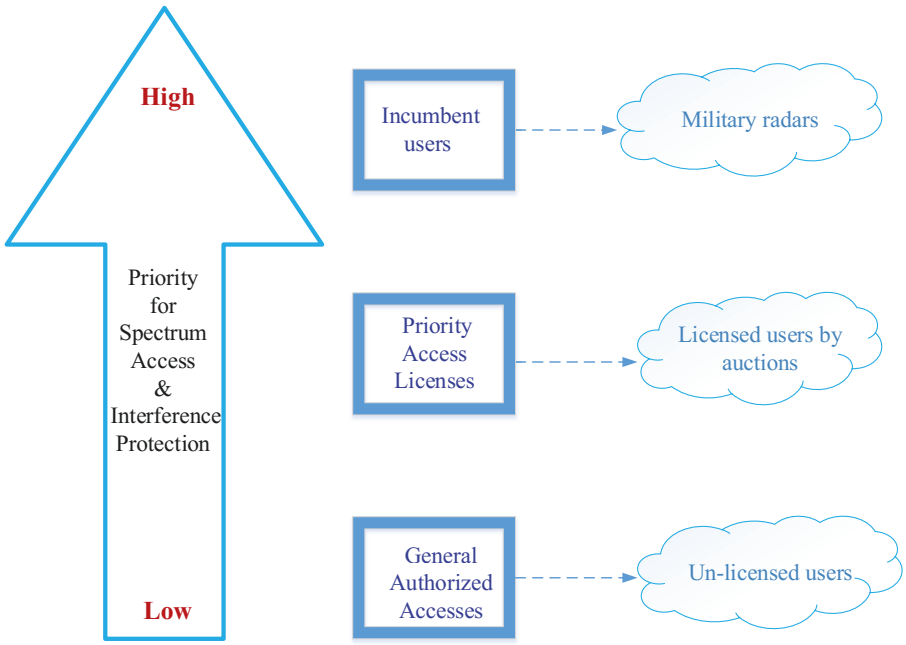


Figure 2.3: Priorities of spectrum access and interference protection in SAS.

2300 − 2400MHz in Europe. SAS was proposed to protect three tiers of users who operate on 3.5GHz band in the U.S. In the sequel, we present more details of the SAS architecture.

According to the FCC rules, the SAS architecture is a database-driven spectrum sharing system operating at the frequency band of 3.5−3.7GHz in the U.S. [28]. This architecture is released to manage the spectrum access across three tiers of users: Incumbent (tier−1), Priority Access (PA, tier−2) and General Authorized Access (GAA, tier−3). Incumbent users (IUs), a federal entity authorized for frequency bands, can use the spectrum without any limitations and get interference protection from lower tiers of users, as shown in Fig. 2.3. By the FCC rules, IUs in SAS architecture can be military facilities, Fixed Satellite System (FSS), Radio Location Services (RLS) or Terrestrial Wireless System. Priority Access license (PAL) users are users in the second tier, who can get interference protection from GAA users but not from IUs. Besides, a PAL user must pause its transmission and vacate the spectrum for IUs should they need to use it. GAA users, the last tier of users in SAS, do not get interference protection from PALs or IUs. The PAL users and GAAs users can be categorized as SUs, which are Citizens Broadband Radio Service Device (CBSD) in the U.S. The SAS administrator is an authorized entity to operate SAS,

Table 2.1: Summary of conventional OFDM sensing approaches.

Sensing Methods	Advantages	Disadvantages
ED [17]	simple and easy	sensitive to noise uncertainty
PT [32]	robust to noise uncertainty	vulnerable to CFO, higher complexity
CP [33]	robust to noise uncertainty	susceptible to timing delay, higher complexity
CM [33]	robust to noise uncertainty	sensitive to timing delay and CFO, higher complexity
ANN [34, 35]	higher sensing accuracy than feature-based methods	sensitive to noise uncertainty, timing delay and CFO, higher complexity
CNN [36]	higher sensing accuracy than feature-based methods	sensitive to noise uncertainty, timing delay and CFO, higher complexity

e.g., developing policies/procedures and allocating the spectrum resource across the three tiers of users [29].

2.2 Efficient Solutions for Sensing-based Dynamic Spectrum Access in Half-duplex Systems

How to realize an efficient spectrum sharing is a challenging problem for DSA. To address this issue, a wide variety of methods are proposed. In this section, we will provide a review of sensing-based DSA in HD systems, especially for efficient solutions for spectrum utilization. Among them, as a widely accepted multi-carrier transmission paradigm, sensing of orthogonal frequency division multiplexing (OFDM) signals has received paramount interest [30, 31].

For the existing OFDM sensing approaches, as summarized in Table 2.1, the energy detection (ED) is one of the simplest and most popular sensing methods in

HD systems, which detects the IU's activity based on the energy of the received signals [17]. However, sensing performance of this method is very susceptible to noise uncertainty. To leverage the special features of OFDM signals, e.g., pilot tones (PT) [32], cyclic prefix (CP) [37, 38] and covariance matrix (CM) features [33], one can use the feature-based detection approaches. For instance, [37] presents methods to detect the IU's signals by exploiting the autocorrelation of CP. For the same purpose, the authors in [32] developed a sensing algorithm drawing support from the PT feature of OFDM signals. In [33], authors propose a CM-based method to determine the IU's activity states by leveraging the features of the covariance matrix of the discrete Fourier transform of the received signals. However, the sensing accuracy of these methods heavily depends on the noise uncertainty, CFO or synchronization errors/timing delay [16, 18]. To mitigate the severe impact of those bad communication conditions, highly complex processes and resources are required, causing huge complexity. Moreover, those methods require full or partial prior knowledge of IU's signals (e.g., the CP or PT structure of IU signals) and/or noise power that are not always available in practical applications (e.g., when IUs are military applications) [39]. Instead of requiring features as a priori knowledge, in this work, we employ the latest advances in machine learning (ML) to learn them. More importantly, our methods can also learn/capture the hidden features of OFDM signals to improve the sensing accuracy.

ML has recently found its applications in various areas such as object detection [40], speech recognition [41, 42], channel estimation [43], and pattern recognition [44, 45]. We observe that spectrum/signal sensing resembles a pattern recognition problem, as illustrated in Fig. 2.4. Specifically, pattern recognition involves the steps of the feature extraction and the classification [45]. Analogously, typical OFDM sensing methods consist of two steps: first, calculate the test statistic of the received signals; second, compare the test statistic with the corresponding thresholds to detect IU's activity. We then can map these first and second stages in OFDM sensing to the feature extraction and the classification in pattern recognition, respectively.

Most ML-based spectrum sensing works have been focusing on cooperative spectrum sensing (CSS) [46] that utilizes ML to fuse individual sensing results from

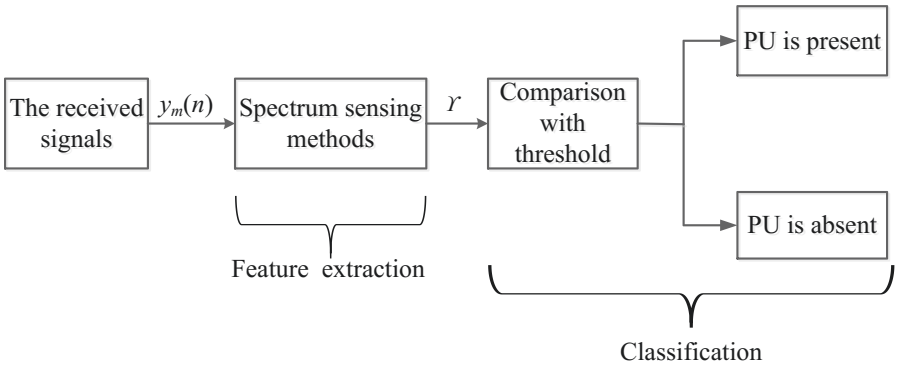


Figure 2.4: Relationship between spectrum sensing and pattern recognition.

multiple SUs for the decision process. The authors of [47] develop a linear fusion rule for CSS, which utilizes the Fisher linear discriminant analysis to obtain linear coefficients. The authors in [48] propose several cooperative sensing algorithms drawing support from support vector machine (SVM), weighted K-nearest-neighbor (KNN), K-means clustering, and Gaussian mixture model (GMM). They use the energy of received signals as feature vectors. The approach in [49], utilizing the fuzzy SVM and nonparallel hyperplane SVM, is also claimed to be robust to the noise uncertainty. Although those cooperative sensing methods can improve the sensing performance, their complexities are significantly high. To solve that problem, in [50], a convolutional neural network (CNN) based cooperative sensing method is proposed, which improves the sensing performance with low complexity. In [51], the K-means clustering and SVM techniques are used but take a low-dimensional probability vector as the feature vector, resulting in a smaller training duration and a shorter classification time. Besides, a ML-based mobile CSS framework for large-scale heterogeneous cognitive radio networks is proposed in [52], drawing support from the recent advances in Bayesian machine learning.

Unlike the above cooperative spectrum sensing methods, our work provides non-cooperative spectrum sensing solutions using deep learning in which very little has been investigated so far. The only and most relevant to ours is [34], as shown in Table 2.1, which proposes a sensing method based on Artificial Neural Network (ANN), utilizing the energy and Likelihood Ratio Test statistic as input features. In [35], the authors also apply ANN for the sensing purpose with the energy and cyclostationary

features as the input features. Using the same features as [35], the authors in [36] rely on the CNN architecture instead. Although these methods help improve the sensing performance in non-cooperative scenarios, their detection results are directly influenced by the accuracy of (one or more) input features that are explicitly extracted from the received signals. However, these extracted features (e.g., energy) are usually sensitive to noise uncertainty, timing delay or CFO. Besides, extracting specific or known features from the original received signal can only obtain partial information, which inevitably loses the information of implicitly hidden but helpful features.

In this work, we leverage deep learning networks to address all the above limitations. Instead of manually describing the event of interest with explicit features, deep learning (DL) [53] relies on multiple layers of nonlinear processing units (a so-called deep architecture) to extract both known as well as possibly hidden features of the input signals.

There are various deep learning network architectures, e.g., recurrent neural network (RNN), CNN, stacked autoencoder [54]. Among these, we adopt the stacked autoencoder (SAE) [55] for spectrum sensing for the following reasons. First, the SAE architecture has a unique training process that makes our work more suitable for practical scenarios with a limited amount of labeled data. Specifically, the SAE architecture can be trained through an unsupervised pre-training followed by a supervised fine-tuning process [56]. In the unsupervised pre-training phase, each layer is trained to extract features from the input data. Note that, in this phase the unlabeled training data can be used. In the supervised fine-tuning phase, the data with labels are used to improve the classification performance utilizing the back-propagation method. It is noteworthy that only a small number of the labeled data is required in the fine-tuning phase [57, 58]. By contrast, other deep learning architectures (e.g., CNN or RNN) often require a large amount of labeled data. When the labeled data is insufficient, the sensing accuracy of CNN or RNN would dramatically degrade. The deep Bayesian network can obtain a good result with small data regimes. However, the deep Bayesian network requires to obtain the posterior distribution for a model's parameters given the data, which is usu-

ally computationally intractable, especially with large network size [59, 60]. Some methods, e.g., Markov Chain Monte Carlo (MCMC), can be employed to obtain the approximate distributions. However, it is very much time-consuming for these methods (e.g., MCMC) to obtain distributions [61]. Besides, the approximation accuracy of the posterior distribution is also another challenging problem [59, 61]. Second, SAE is a fully connected network that can effectively extract the compact representation from input signals while retaining the most important information of the data [62]. This representation is critical in completely reconstructing the original input, thereby having great potential in feature extraction and generalization [63]. In other words, this property can effectively strengthen the feature propagation, and hence, to retain essential features (preventing them from vanishing by the time they reach the end of the network). By contrast, for typical CNN, it is inevitable to lose features/information in the process of feature extraction due to its partial connection model. Although introducing dense connections into CNN can effectively overcome the problem of information loss in the feature extraction, it comes at the cost of excessive complexity. Note that, when the amount of labeled data is small, SAE can achieve better sensing results than CNNs with dense connections. Third, the SAE architecture is conceptually simple and easy to be trained [64]. However, it is difficult to train RNN due to the well known "vanishing gradient" problem [65]. For the above reasons, in this work, we adopt SAE to process the received signals, so as to detect the IU's presence/absence.

2.3 Efficient Solutions for Sensing-based Dynamic Spectrum Access in Full-duplex System

As previously demonstrated, for sensing-based DSA under HD communications paradigm, SUs must determine the absence of IUs using sensing techniques before utilizing corresponding IUs' channels for transmission. In other words, in HD systems, the traffic of SUs is interrupted by the sensing activity that can not be conducted simultaneously with the data transmission [15]. This leads to an increase in SU's reaction time and a degradation in SU's spectrum utilization. To tackle this

issue, the FD radio has been proposed and has received considerable interest.

Unlike HD systems that follow the traditional LBT principle, FD radios are able to conduct simultaneous transmission and reception on the same frequency and even using the same antenna array. In such a case, SUs are able to reduce their reaction time to a shorter period, which thereby significantly enhances the sensing efficiency as well as increases the system throughput [66, 67]. Although the FD technique or LAT is promising for CRNs, it suffers from a crucial, yet inherent problem: self-interference [68]. Sensing the IU activity states (i.e., absence or presence) with the presence of self-interference in FD systems is challenging. This is because self-interference can lead to a low signal-to-interference-plus-noise ratio (SINR) and severely affect the test statistics of sensing methods.

To address self-interference in FD systems, a number of self-interference suppression techniques have been presented in the literature such as advanced time-domain interference cancellation [69, 70], signal inversion and adaptive cancellation [71] and antennas cancellation [72, 73]. For instance, the authors in [70] developed an interference mitigation method in multiple-input multiple-output (MIMO) systems. This method can replicate and remove the interference signal from the received signal relying on the condition of the known transmission channel and transmitted signal. In [73], the authors presented a method to mitigate self-interference using antenna placement, noise cancellation and digital interference cancellation. Although these self-interference suppression methods have made great progress in mitigating self-interference, none of these works can guarantee perfect self-interference suppression performance [74, 75]. Imperfect self-interference suppression causes residual/leaked self-interference that adversely impacts the sensing accuracy [13].

One of the most basic spectrum sensing methods in FD systems under residual self-interference is ED [76]. However, it is very much susceptible to noise uncertainty [77]. A small error in noise power estimation would lead to a very large degradation in sensing performance, restricting the application of ED in practice. Spectrum sensing using waveform-based detector in [78] could achieve better performance than the ED based approach; however, such a method is sensitive to timing delay. To mitigate the effect of timing delay, highly complex processes and resources are

required. Besides, some sensing methods that utilize special features of OFDM signals (e.g., PT) are also able to achieve better sensing performance, while they are greatly vulnerable to the CFO [33, 79]. A small synchronization error in the frequency domain can result in significant performance degradation. To estimate and mitigate the effect of CFO, a number of highly complex resources and processes are needed, posing significantly high complexity. Another main barrier for these sensing methods is that it is extremely difficult to achieve good sensing performance for conventional feature-based methods under low SNR conditions.

It is important noteworthy that, although the learning networks (e.g., ML or DL architectures) employed in HD systems are able to achieve reliable sensing results, they are not suitable for FD paradigms. The reason is that, different from HD systems where the sensing stage is allocated to a certain duration, the FD-based spectrum sensing occurs throughout the whole SU's traffic. For collision avoidance and spectrum utilization, the SU in FD systems is required to obtain the sensing results rapidly. If IU is detected as absent on the channel, SU can continue to access the frequency bands; otherwise, SU must abort its transmission immediately. However, the learning-based sensing methods usually require a relative long time for the training process, significantly increasing SU's sensing duration. Under this situation, SU cannot make a timely reaction in response to IU's action, leading to collision (e.g., IU's arrivals) or spectrum waste (e.g., IU's departures). Given all the aforementioned problems, in this work, we propose two novel sensing methods leveraging the CP feature and PT feature of OFDM signals, respectively.

2.4 Secure Solutions for Data-based Dynamic Spectrum Access

In this section, we present the recent work on the security issue in data-based DSA. In data-based DSA, primary owners of the spectrum (i.e., IUs) are protected from adverse interference effect from SUs [80,81]. To protect IUs, the interference induced by SUs is carefully calculated/budgeted. For that purpose, SUs are required to share their up-to-date operational information (such as users' location and transmitting

power [19, 20],...) with a third party [82]. In the SAS, proposed by FCC, a SAS administrator [83, 84] serves as the third party. However, the current mechanism to protect IUs/IUs in SAS can be too conservative, leading to poor utilization of spectrum sharing. Sharing IUs' operational data with the SAS administrator, hence, can create new opportunities to improve spectrum utilization and mitigate the problem of spectrum shortage, whereas it also causes the exposure of users' private information, such as users' location and transmitting power [85].

Since the user's private data is closely related to its business, the leakage of private information would compromise the user's interest and development [86, 87]. For instance, in the SAS architecture, the IUs are federal military facilities, and SUs (a.k.a., PALs and GAAs users) are commercial institutions. In such a case, the exposure of IUs' and SUs' information would result in serious threats to national security and commercial interests, respectively [21]. For these reasons, protecting user's operational data/information during the process of spectrum sharing is the key to success of any DSA systems, including SAS or the Licensed Spectrum Access (LSA), proposed by European Telecommunications Standards Institute (ETSI) [84].

The efforts in the literature can be categorized into three main types: obfuscation methods [88–90], anonymity methods [91, 92] and cryptosystems [93, 94], as summarized in Table 2.2. Specifically, authors in [88] propose an architecture drawing support from obfuscation methods to protect incumbent radar's (i.e., IU's) location security. In [90], SU's location is concealed by adding a blind factor to the actual location. Authors in [92] preserve user's operational information by leveraging anonymity, clustering and perturbation algorithms. Although schemes in [88], [90] and [92] have achieved great progress regarding protecting user's precise location or operational information, they inherit weaknesses from anonymity and perturbation algorithms (e.g., revealing user's rough direction or group information to potential adversaries). To address this problem, authors in [94] recruit the homomorphic encryption to protect IUs information. However, the proposed approach in [94] requires an additional entity to the SAS architecture, called the key distributor. The introduction of the key distributor does not honor the original SAS's architecture of FCC. Additionally, a large number of operations in the encrypted domain in [94]

Table 2.2: Summary for conventional privacy preservation schemes.

Schemes	Advantages	Disadvantages
Obfuscation [88–90]	simple and easy for implementation	only protect users' location, cannot fully protect location information from exposure, ignore the case of dishonest users
Anonymity [91, 92]	simple and easy for implementation	only protect users' location, cannot fully protect location information from exposure, ignore the case of dishonest users
Cryptosystems [93, 94]	fully protect private information from exposure	much higher complexity, ignore the case of dishonest users

with high complexity would prohibit [94] from practical implementation.

Additionally, all the above works assumed that users are always honest, i.e., users report their information truthfully and comply with what they report. However, such an assumption is not really realistic [95]. For example, in order to increase the probabilities of getting approval requests from the SAS administrator, some SUs may report lower values than their actual transmitting powers in their requests [96]. These dishonest/greedy behaviors would make the SAS administrator grant requests that can cause adverse interference to corresponding IUs or other SUs sharing the same spectrum source [96]. Therefore, investigating the privacy issue considering dishonest SUs is practically essential to promote effective and accurate spectrum allocations in SAS systems. However, this issue has not been sufficiently addressed. For that, in this work, we propose a novel scheme drawing support from encryption and obfuscation techniques to prevent users' operational data from being revealed.

2.5 Summary

In this chapter, we provided a general overview of the research work in DSA. First, we presented an overview of DSA including sensing-based and data-based modules. For the sensing-based DSA, we introduced HD and FD paradigms, and discussed their unique features for communications. For the data-based DSA, we reviewed its communication. Second, we presented the efficiency issue in sensing-based DSA, followed by the security issue in data-based DSA. Third, we analyzed the advantages and disadvantages of the existing efficient and secure solutions in DSA.

Chapter 3

Dynamic Spectrum Access in Half-duplex Systems

Sensing-based DSA or spectrum sensing has been widely considered as a promising solution to the radio spectrum shortage. To improve the spectrum efficiency, two sensing approaches leveraging the features of deep learning networks under HD paradigm are proposed and analyzed in this chapter.

3.1 Introduction

To facilitate the spectrum sensing technique and improve spectrum utilization, a large number of sensing methods in HD systems are proposed, which can be categorized into two main branches: conventional sensing methods (e.g., [33, 37]) and learning-based sensing methods (e.g., [34, 36]). For the former, SUs sense IU's presence/absence by using one or more kinds of specific features (e.g., the energy of received signals, PT or CP features). For the latter, machine learning architectures are adopted to detect IU's activity states by processing the features explicitly extracted from received signals. The current sensing methods (both conventional and learning-based) have made great progress in improving the sensing accuracy, while several challenging problems are yet to be resolved. Taking the conventional sensing methods as a study case, reliable sensing results are heavily dependent on the prior knowledge (e.g., IU's signal structure) which however is not always available,

especially for IUs that are military facilities [39]. Besides, these conventional sensing approaches are usually susceptible to various communication conditions, e.g., noise uncertainty, timing delay or CFO [16, 18]. To mitigate the severe effect caused by these conditions, many complex processes are required, leading to significant high complexity. For the learning-based sensing methods, their sensing performance closely relies on input features that are explicitly extracted from received signals, such as the energy of received signals. However, the explicit features are also sensitive to those communication conditions. Besides, these learning-based methods only extract specific features from the original received signal (e.g., the energy of received signal), while they lose other important features of input signal. In other words, these methods only obtain partial information but inevitably lose the information of implicitly hidden but helpful features. Given the challenges as mentioned above, in this chapter, we propose two novel OFDM sensing approaches drawing support from the properties of deep learning networks. The major contributions of this chapter are as follows:

- We propose a stacked autoencoder based spectrum sensing method (SAE-SS) to detect the IU's presence/absence. SAE-SS notably outperforms the existing (both conventional and learning-based) sensing methods regarding the robustness to timing delay, noise uncertainty and CFO. SAE-SS does not require any prior knowledge of the IU's signal structure nor any external feature extraction algorithms, which is however required by most existing ML-based methods.

- To further improve the sensing accuracy of SAE-SS, especially under low SNR conditions, we propose a new sensing method, called SAE-TF, by incorporating the frequency domain information into the SAE-SS. SAE-TF is able to achieve much better sensing results than SAE-SS, at the cost of higher computational complexity.

- We provide comprehensive analyses of SAE-SS and SAE-TF, e.g., the computational complexity, training time, and the feasibility. We also evaluate the performance of the proposed methods considering various conditions (e.g., CP

length, hidden units, OFDM blocks, and additional features).

The remainder of this chapter is structured as follows. In Section 3.2, the system model and problem formation are provided. In Section 3.3 and Section 3.4, we present the proposed SAE-SS and SAE-TF methods, respectively. The complexity analysis and other discussion are expressed in Section 3.5. In Section 3.6, we show the simulation results. Conclusions are finally summarized in Section 3.7.

3.2 System Model and Problem Formulation

In this chapter, we let $y_m(n)$ denote the received OFDM signals at the SU receiver, where $m \in [0, \ldots, M]$ is the total number of received OFDM blocks and $n \in [0, \ldots, N_c + N_d - 1]$. N_c denotes the length of the cyclic prefix and N_d denotes the data block size. $y_m(n)$ can be written as:

$$\begin{aligned} H_0 &: y_m(n) = w_m(n), \\ H_1 &: y_m(n) = e^{-j\frac{2\pi f_q n}{N_d}} \sum_{l=0}^{L_p-1} h_l s_m(n-\delta-l) + w_m(n), \end{aligned} \tag{3.1}$$

where H_0 and H_1 denote the hypotheses of absence and presence of IU, respectively. $w_m(n)$ is the complex additive white Gaussian noise (AWGN) with zero-mean and variance σ_w^2 (i.e., $w_m(n) \sim CN(0, \sigma_w^2)$). $s_m(n)$ denotes the transmitted OFDM signals by the IU transmitter. f_q is the normalized carrier frequency offset. δ denotes the timing delay. h_l represents the channel gain of the lth channel and we assume its value does not change during the sensing process. L_p represents the total number of multi-path components between the IU and the SU. Without loss of generality, $w_m(n)$, $s_m(n)$ and h_l are assumed to be mutually independent. According to the central limit theorem, when the length of the received signals is sufficiently large, $s_m(n)$ approximately obeys the complex Gaussian distribution, and its mean and variance are zero and σ_s^2, respectively. In that case, SNR of $y_m(n)$ under H_1 can be represented as $\text{SNR} = \sigma_s^2 \sum_{l=0}^{L_p-1} |h_l|^2 / \sigma_w^2$.

For typical OFDM sensing methods, e.g., the basic ED, its test statistic Υ_{ED} is:

$$\Upsilon_{\text{ED}} = \frac{1}{M(N_c + N_d)} \sum_{m=0}^{M-1} \sum_{n=0}^{N_c+N_d-1} |y_m(n)|^2. \tag{3.2}$$

The probability of false alarm (PFA) and probability of missed detection (PM) are

$$\mathrm{PFA_{ED}} = \Pr(\Upsilon_{\mathrm{ED}} > \lambda | H_0), \quad \mathrm{PM_{ED}} = 1 - \Pr(\Upsilon_{\mathrm{ED}} > \lambda | H_1), \tag{3.3}$$

where $\Pr(.)$ denotes the probability distribution function. λ is the sensing threshold based on the estimated noise variance ($\widetilde{\sigma}_w^2$). According to the above equations, ED only utilizes the received signals to detect the presence of IU without requiring any prior knowledge of IU signals. However, it is vulnerable to noise uncertainty. Moreover, even a small estimated error in the noise power would significantly deteriorate its sensing accuracy, especially in the low SNR regime [79].

For feature-based detections, e.g., CP-based [37] and CM-based [33], their test statistics are

$$\begin{aligned} \Upsilon_{\mathrm{CP}} &= \max_{\delta} \log\Big(\frac{\Pr(\mathbf{R}|H_1, \sigma_w^2, \sigma_s^2)}{\Pr(\mathbf{R}|H_0, \sigma_w^2)}\Big), \\ \Upsilon_{\mathrm{CM}} &= \frac{||\hat{\mathbf{R}} \odot (\mathbf{1}_{N_d} - \mathbf{I}_{N_d})||_{L_1}}{\sqrt{N_d^2 - N_d}}, \end{aligned} \tag{3.4}$$

where $\mathbf{R}$ is the correlation vector of the received signals. $\hat{\mathbf{R}}$ is the covariance matrix of received signals after discarding the CP in the frequency domain.

Although CP-based and CM-based detections are robust to noise uncertainty, they require some prior knowledge of the IU's signals, such as the IU's transmitting power or the CP structure. However, this information is usually not available. Moreover, as aforementioned, the feature-based detections are sensitive to timing delay and CFO, and even a small mismatch between the received and transmitted signals in the time domain or frequency domain would lead to significant degradation of sensing accuracy.

3.3 Stacked Autoencoder Based Spectrum Sensing

In this section, we propose SAE-SS that is robust to timing delay, noise uncertainty and CFO. In other words, these communication conditions cause less performance

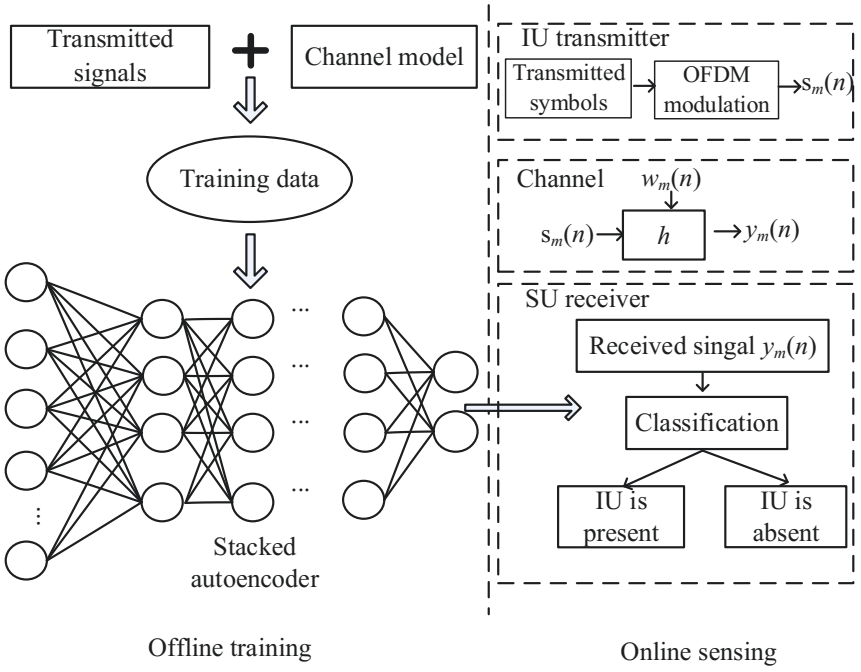


Figure 3.1: Architecture of the OFDM system with SAE-SS.

degradation on the proposed SAE-SS, compared to state-of-the-art methods. The architecture of the OFDM system with SAE-SS is shown in Fig. 3.1. The hidden features of received OFDM signals are extracted from the SAE network during the offline training stage. Those extracted features are then used to sense IU's activity during the online sensing stage. The key steps of SAE-SS can be summarized as: pretraining, fine-tuning of SAE, and classification (e.g., online spectrum sensing stage).

The spectrum sensing technique (both conventional and learning-based) can be described as a process of the feature extraction followed by the feature classification. The feature extraction aims to extract the essential features for sensing, which can be expressed as

$$\boldsymbol{\Upsilon} = F(\mathbf{y}), \tag{3.5}$$

where $\boldsymbol{\Upsilon}$ denotes the extracted feature vector, $\boldsymbol{\Upsilon} \in \mathbb{R}^{d_\Upsilon}$, d_Υ is the dimension of the feature vector. $\mathbf{y}$ stands for the received signal vector, $\mathbf{y} := \{y_0(0), y_0(1), \ldots, y_m(n), \ldots, y_M(N_c + N_d - 1)\}$, $\mathbf{y} \in \mathbb{R}^{d_y}$, $d_y = M(N_c + N_d)$. $F(.)$ is the function of feature extraction. Next, the extracted features will be classified into different classes for sensing the IU's presence. Note that for different sensing methods, the meanings of

$\boldsymbol{\Upsilon}$ and $F(.)$ are different.

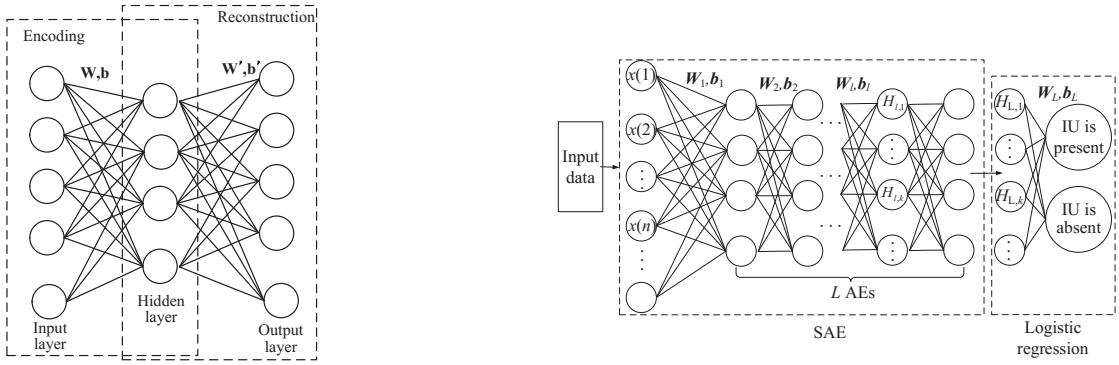
For the conventional sensing methods, $\boldsymbol{\Upsilon}$ in equation (3.5) denotes the test statistic of specific sensing methods, which is usually a one-dimensional feature, denoted as Υ. $F(.)$ stands for the function that calculates the test statistic, which is determined by the specific sensing methods with the certain models. Upon achieving Υ calculated by $F(.)$, the SU can detect the IU's presence by just comparing Υ with a threshold. Take the energy detection as an instance, Υ_{ED} is the test statistic that is a one-dimensional feature, and $F(.)$ is a function to calculate Υ_{ED}, $\Upsilon_{ED} = F(\mathbf{y}) = \frac{1}{d_y}\mathbf{y}\mathbf{y}^T$. If Υ_{ED} is smaller than the threshold, IU is absent, otherwise, IU is present.

For the learning-based sensing methods, $\boldsymbol{\Upsilon}$ in equation (3.5) is the feature vector extracted by the network, and $F(.)$ is the network structure. Take the proposed SAE-SS as an example, $\boldsymbol{\Upsilon}_{SAE}$ is the feature vector extracted by SAE. $F_{SAE}(.)$ is the SAE network structure which is parameterized by $\{\mathbf{W}, \mathbf{b}\}$, $\mathbf{W}$ stands for the weight matrix and $\mathbf{b}$ is the bias matrix. Generally, $\boldsymbol{\Upsilon}_{SAE}$ contains multiple features that involve IU's activity states (absence and presence). Thus a classifier is used to classify these features into separated classes for detecting the IU's presence. The basic idea is to utilize the SAE as a feature extractor to automatically extract the essential hidden features from the original input signal, without any external feature extraction algorithms. To that end, we need to train the SAE network for feature extraction.

The key idea of SAE-SS is to train the SAE network for extracting the hidden features from the original received signal. This training process is conducted during the offline stage (i.e., before the spectrum sensing phase), which includes the pre-training and fine-tuning. The trained SAE is then directly used to detect IU's activity states during the online sensing phase.

3.3.1 Pretraining of Stacked Autoencoder

The pretraining SAE aims to learn the hidden features of received signals through two stages. In the first stage, the SAE network is divided into independent Autoencoders (AEs) and these AEs are individually trained, one by one. Each AE is a



(a) Structure of AE

(b) Structure of SAE with logistic regression classifier

Figure 3.2: Structure of spectrum sensing based on traditional neural networks.

three-layer network including input layer, hidden layer and reconstruction layer, as illustrated in Fig. 3.2(a). In the second stage, the input and hidden layers of the trained AEs are stacked together, layer by layer, as shown in Fig. 3.2(b).

The training of each AE can be described as an encoding-decoding process. The input data is first mapped into a hidden presentation via an encoding process. In addition to known features (e.g., energy and test statistics features), this presentation also contains other useful yet unnamed/unknown information/features for the sensing purpose [97]. These features are referred to as the hidden/unknown features. The resulting latent presentation is then mapped back to a "reconstructed" vector through a decoding process. The encoding-decoding process aims to minimize the average reconstruction error.

Note that AE is only suitable for non-complex numbers, thus we partition the input signals into real and imaginary parts, respectively. The received signal in equation (3.1) is rewritten as:

$$\begin{aligned}\mathbf{y}_i : \quad &= \{\Re(y_i(0)), \Im(y_i(0)), \Re(y_i(1)), \Im(y_i(1)), \ldots, \\ &\Re(y_i(N_c + N_d - 1)), \Im(y_i(N_c + N_d - 1))\},\end{aligned} \tag{3.6}$$

where $\Re(.)$ and $\Im(.)$ mean the real part and the imaginary part, respectively. Thus the input vector of SAE-SS network $\mathbf{x}$ can be expressed as

$$\mathbf{x} := \{\mathbf{y}_0, \mathbf{y}_1, \ldots, \mathbf{y}_{M-1}\}^T, \tag{3.7}$$

where the length of $\mathbf{x}$ is $N_{input} = 2M(N_c + N_d)$. Next, $\mathbf{x}$ is used to train AEs. Take the lth AE as an example, let $H_{l,p}^{in}$, $H_{l,k}$ and $H_{l,q}^{out}$ denote the pth input unit, the kth hidden unit and the qth output unit, respectively. Then $H_{l,k}$ can be obtained with $H_{l,p}^{in}$ [98], which is shown as below:

$$H_{l,k} = f(\sum_{p=1}^{P_l} W_{l,p,k} H_{l,p}^{in} + b_{l,k}), \tag{3.8}$$

where P_l is the number of input units in the lth AE. $f(.)$ is the activation function. $W_{l,p,k}$ denotes the weight between the pth input unit and the kth hidden unit of the lth AE. $b_{l,k}$ is the bias of the kth input unit of the lth AE. Then $H_{l,q}^{out}$ can be achieved with $H_{l,p}^{in}$ and $H_{l,k}$, by

$$\begin{aligned} H_{l,q}^{out} &= f(\sum_{k=1}^{K_l} W_{l,k,q}^{'} H_{l,k} + b_{l,q}^{'}) \\ &= f\left(\sum_{k=1}^{K_l} W_{l,k,q}^{'} f\left(\sum_{p=1}^{P_l} W_{l,p,k} H_{l,p}^{in} + b_{l,k}\right) + b_{l,q}^{'}\right), \end{aligned} \tag{3.9}$$

where K_l is the number of units in the hidden layer of the lth AE. $W_{l,k,p}^{'}$ denotes the weight between the kth hidden unit and the qth output unit of the lth AE. $W_{l,p,k} = W_{l,k,q}^{'}$. $b_{l,q}^{'}$ is the bias of the qth output unit of the lth AE. When $l = 1$, the input vector $\mathbf{H}_1^{in}$ is the same as $\mathbf{x}$, which is

$$\mathbf{H}_1^{in} := \{H_{11}^{in}, H_{12}^{in}, \ldots, H_{1P_1}^{in}\}^T, \tag{3.10}$$

where P_1 is the number of input units in the first AE, $P_1 = N_{input} = 2M(N_c + N_d)$. In this work, the sigmoid function [64] is adopted as the activation function, which is

$$f(H_{l,p}^{in}) = \frac{1}{1 + e^{-H_{l,p}^{in}}}. \tag{3.11}$$

The aim of training the lth AE is to minimize the error between $H_{l,p}^{in}$ and $H_{l,p}^{out}$ by continuously updating the values of $W_{l,p,k}, b_{l,k}$ and $b_{l,q}^{'}$. The most typical error function to measure the difference between $H_{l,p}^{in}$ and $H_{l,p}^{out}$ is the mean square error:

$$\chi = \frac{1}{P_l} \sum_{p=1}^{P_l} ||H_{l,p}^{in} - H_{l,p}^{out}||^2. \tag{3.12}$$

However, this method is time-consuming for training, thus we select the cross-entropy method [99] to speed up the training process, which is

$$\chi = \sum_{p=1}^{P_l} [H_{l,p}^{in} \log(H_{l,p}^{out}) + (1 - H_{l,p}^{in}) \log(1 - H_{l,p}^{out})]. \tag{3.13}$$

Let $\Omega = \{W_{l,p,k}, b_{l,k}, b_{l,q}^{'}\}$, the objective function is

$$\Omega = \arg\min_{\Omega} \chi. \tag{3.14}$$

Moreover, we adopt the gradient descent method [100] to achieve the optimal Ω, by

$$\begin{aligned} W_{l,p,k}(n+1) &\leftarrow W_{l,p,k}(n) - \kappa \frac{\partial \chi(H_l^{in}, H_l^{out})}{\partial W_{l,p,k}}, \\ b_{l,k}(n+1) &\leftarrow b_{l,k}(n) - \kappa \frac{\partial \chi(H_l^{in}, H_l^{out})}{\partial b_{l,k}}, \\ b_{l,q}^{'}(n+1) &\leftarrow b_{l,q}^{'}(n) - \kappa \frac{\partial \chi(H_l^{in}, H_l^{out})}{\partial b_{l,q}^{'}}, \end{aligned} \tag{3.15}$$

where $W_{l,p,k}(n)$, $b_{l,k}(n)$ and $b_{l,q}^{'}(n)$ denote weight and bias of nth training. κ is the leaning rate.

Upon training all the AEs based on the above rules, the trained SAE is created by stacking the input and hidden layers of trained AEs together, layer by layer. The output of SAE's pre-training, which is also the hidden units of Lth AE, can be written as

$$\mathbf{H}_L := \{H_{L1}, H_{L2}, \ldots, H_{LK_L}\}^T, \tag{3.16}$$

where K_L is the number of units in the hidden layer of the Lth AE. $\mathbf{H}_L$ in equation (3.16) contains the hidden features of the received signals and will be used to sense the IU's activity states.

3.3.2 Fine-Tuning and Classification

The pretraining process of SAE can be interpreted as extracting IU's unsupervised features. Thus, the trained SAE needs to be fine-tuned to leverage the SAE's property for the spectrum sensing, as shown in Fig. 3.2(b). We select the logistic

regression classifier [101] to fine-tune the SAE network for the following reasons. First, the logistic regression classifier, a specialization of softmax classifiers for the case of binary classification, can produce not only the classification results but also the corresponding probabilities [102]. This helps us better evaluate the classification results, which is beneficial for spectrum sensing. Second, the training process of the logistic regression classifier can be easily completed with low complexity. By contrast, for neural networks (e.g., support-vector machines, SVM), they only compute the score for each class instead of the corresponding probabilities [103], which is hard to be interpreted for all classes. Additionally, the training time is usually long when the dataset is large [103].

The input of the logistic regression classifier is $\mathbf{H}_L$, which is the output of the pretraining SAE. U, the output of the logistic regression classifier, can be seen as a set of conditional probabilities of $\mathbf{H}_L$, $\mathbf{W}_R$ and $\mathbf{b}_R$. $\mathbf{W}_R$ and $\mathbf{b}_R$ are weights and biases of the logistic regression layer. Let $\tau = 1$ and $\tau = 0$ denote the presence and the absence of IU activity states, respectively. According to the logistic regression classifier [101], the conditional probability of U is:

$$\Pr(U=\tau|\mathbf{H}_L, \mathbf{W}_R, \mathbf{b}_R) = \frac{e^{\mathbf{W}_{R,\tau}\mathbf{H}_L+\mathbf{b}_{R,\tau}}}{\sum_{i=0}^{1} e^{\mathbf{W}_{R,i}\mathbf{H}_L+\mathbf{b}_{R,i}}}. \tag{3.17}$$

We apply the back-propagation method [104] to train the logistic regression classifiers. The whole SAE network is also fine-tuned at the same time. Upon pretraining and fine-tuning the SAE network in the offline phase, SAE-SS can detect the IU's activity states using only the received signals. In comparison with the feature-based OFDM spectrum sensing methods, the inputs of SAE-SS are the originally received signals. SAE-SS does not require any arithmetical operations such as calculating the energy or the correlation values, before feeding the original received signals into the SAE architecture. Consequently, the overhead of SAE-SS during the online sensing stage is reduced significantly. Moreover, the proposed SAE-SS can complete the sensing task without any prior knowledge of the IU's information, which is more suitable for the practical environment. This is particularly relevant to military applications, opening up the military radar bands for secondary use. Note that the impact of co-channel activities of other SUs on sensing accuracy can

Algorithm 1: Stacked Autoencoder Based Spectrum Sensing Method (SAE-SS)

begin
Initialize: the length of input N_{input}, number of SAE layer L, the number of hidden units in lth layer K_l, pretraining iterations N_{pr}, pre-training learning rate κ_p, fine-tuning iterations N_f, fine-tuning rate κ_f, number of classes C;
Achieve $\mathbf{x}$ based on $\mathbf{y}$
For $1 \leq l \leq L$
  Build an AE with N_v units of input layer and N_h units of hidden layer;
  If $l = 1$
    $N_v = N_{input}$; $N_h = K_1$; $\mathbf{x}$ is set as the input of AE;
  else
    $N_v = P_l$; $N_h = K_l$;
    the hidden units of previous layer $\mathbf{H}_{l-1}$ is set as the input of current layer $\mathbf{H}_l^{in}$;
  end
  Initialize AE, generate $\mathbf{W}_l$, $\mathbf{b}_l = \mathbf{b}_l^{'} = 0$
  For $1 \leq t \leq N_{pr}$
    Based on (3.9) calculate the output of reconstruction: $H_{l,q}^{out} = f(\sum_{k=1}^{K_l} W_{l,k,q}^{'} H_{l,k} + b_{l,q}^{'})$
    Based on (3.13) calculate the error: $\chi = \sum_{p=1}^{P_l} [H_{l,p}^{in} \log(H_{l,p}^{out}) + (1 - H_{l,p}^{in}) \log(1 - H_{l,p}^{out})]$
    Based on (3.15) update $\mathbf{W}_l$, $\mathbf{b}_l$ and $\mathbf{b}_l^{'}$ with κ_p
  end
  remove the reconstruction layer of AE
end
Initialize logistic regression layer: K_L unit of input layer, C unit of output layer
  For $1 \leq t \leq N_f$
    Based on (3.17) calculate probability of each class
    Based on back propagation, update parameters of every layer with κ_f
  end
end

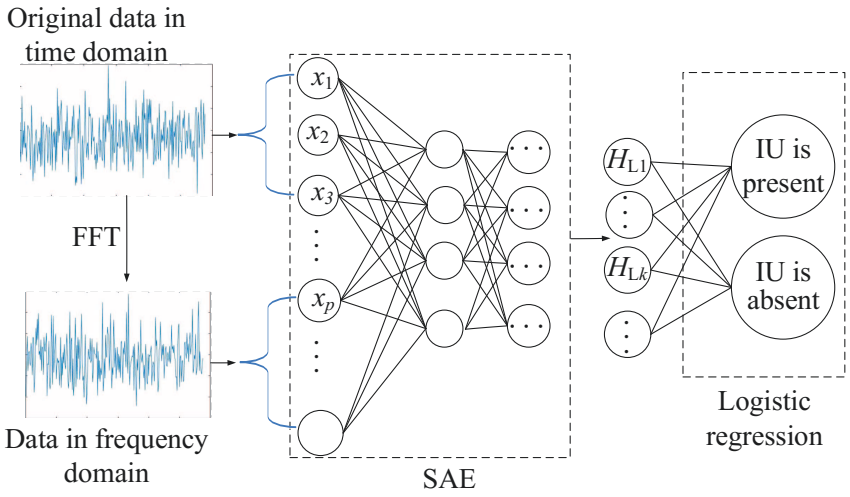


Figure 3.3: Structure of proposed SAE-TF with logistic regression classifier.

be addressed using either traditional multiple access control methods (at the MAC layer) or collaboration among SUs. For example, the presence of multiple SUs can be leveraged to improve the IU sensing accuracy by collaborating among SUs or with fusion centers [105]. For that, in the literature, the sensing task to detect IU's signals is often referred to as a 2−class classification issue: IU presence or absence. The procedure of SAE-SS is summarized in the pseudo-code in Algorithm 1.

3.4 Stacked Autoencoder Based Sensing with Time-Frequency Domain Signals

As aforementioned, the proposed SAE-SS achieves high sensing accuracy by extracting all hidden features of the received OFDM signals without requiring any external feature extraction algorithms. However, its sensing accuracy would degrade under low SNR conditions. To address that problem, we present a Stacked Autoencoder Based Spectrum Sensing Method with time-frequency domain signals (SAE-TF). The input data of SAE-TF involves both time domain and frequency domain signals, which are beneficial for SAE to extract more hidden features for the spectrum sensing purpose. The framework of SAE-TF is shown in Fig. 3.3.

The first step of SAE-TF is to transfer the original received signals from the time

domain to the frequency domain by Fast Fourier transform (FFT):

$$\mathbf{Y} = \mathbf{FFT}(\mathbf{y}), \tag{3.18}$$

where $\mathbf{FFT}(.)$ denotes the FFT operation. Then $\mathbf{Y}$ is divided into real and imaginary parts, respectively. Under this situation, the frequency domain signals are expressed as:

$$\mathbf{Y}_i := \{\Re(Y_i(0)), \Im(Y_i(0)), \ldots, \Re(Y_i(N_c + N_d - 1)), \Im(Y_i(N_c + N_d - 1))\}. \tag{3.19}$$

Thus the frequency domain input vector of SAE-TF $\mathbf{X}$ can be expressed as:

$$\mathbf{X} := \{\mathbf{Y}_0, \mathbf{Y}_1, \ldots, \mathbf{Y}_{M-1}\}^T, \tag{3.20}$$

where the length of $\mathbf{X}$ is equal to $2M(N_c + N_d)$.

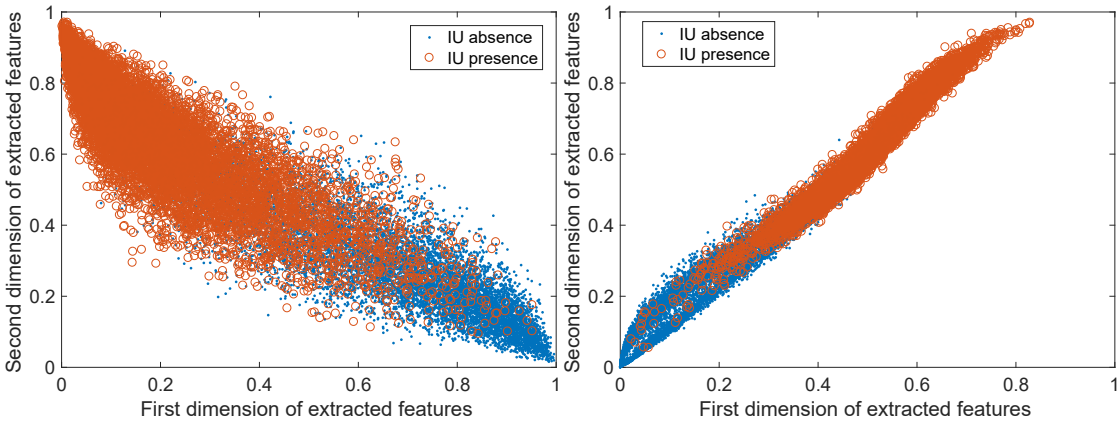
Then the input signals (the linear arrangement of $\mathbf{x}$ and $\mathbf{X}$), are fed into the SAE network for training, as shown in Fig. 3.3. After pre-training, fine-tuning of SAE, which are the same as in Chapter 3.3, SAE-TF is used to sense IU's presence/absence during the spectrum sensing stage.

Notably, unlike SAE-SS, the input of SAE-TF involves two parts: the original received signal $\mathbf{x}$ and the FFT of received signal $\mathbf{X}$. $\mathbf{x}$ (the only input to SAE-SS) provides the essential information/features in the time domain while $\mathbf{X}$ provides the useful features in the frequency domain. In such a case, SAE-TF can jointly extract more useful features from both time and frequency domains. This makes the two events of interest (IU presence and IU absence) more distinguishable/separate for the classification purpose. SAE-TF is hence able to improve the sensing performance of SAE-SS that only utilizes the time domain features.

We provide Fig. 3.4 to show the extracted two-dimensional features captured by SAE-SS and SAE-TF. It is clear that for SAE-SS, the distribution of two events (i.e., representing IU's presence and absence) has a larger overlap than that of SAE-TF. In other words, the features of SAE-TF can be more easily distinguished into separated classes than those of SAE-SS. Therefore, SAE-TF is able to achieve a better sensing performance than SAE-SS owing to the features extracted from both time and frequency domains. However, the number of input units of SAE-TF doubles that of SAE-SS, so the training complexity is higher. The pseudo-code of SAE-TF is in Algorithm 2.

Algorithm 2: Proposed Stacked Autoencoder Based Spectrum Sensing Method with Time-Frequency Domain Signals (SAE-TF)

begin
Transfer the received signals $\mathbf{y}$ using FFT and obtain $\mathbf{Y}$
Achieve $\mathbf{x}$ and $\mathbf{X}$ based on $\mathbf{y}$ and $\mathbf{Y}$
For $1 \leq l \leq L$
  Build an AE with N_v units of input layer and N_h units of hidden layer;
  If $l = 1$
    $N_v = 2 * N_{input}$; $N_h = K_1$;
    The input signals of the first AE are the linear arrangement of $\mathbf{x}$ and $\mathbf{X}$;
  else
    $N_v = P_l$; $N_h = K_l$;
    the hidden units of previous layer $\mathbf{H}_{l-1}$ is set as the input of current layer $\mathbf{H}_l^{in}$;
  end
Train SAE-TF with the input signals.
Training procedures are the same to Algorithm 1.
end



(a) Output signals of second hidden layer for SAE-SS in two dimensions

(b) Output signals of second hidden layer for SAE-TF in two dimensions

Figure 3.4: Performance of extracting hidden features for SAE-SS and SAE-TF in two dimensions.

3.5 Complexity Analysis and Other Discussions

3.5.1 Complexity Analysis

Table 5.1 shows the computational complexity of different sensing methods during the online sensing phase. We take the number of complex multiplications and the real multiplications as metrics because they are the most computationally expensive. Moreover, since one complex multiplication can be treated as four times of a real multiplication, we use the total number of real multiplications to show the computational complexity. In Table 5.1, K_l and K_L are the numbers of units in the hidden layer of the lth and Lth layer, respectively. P_l is the number of input units in the lth layer. S_δ (denoted as S_τ in [37]) is the set of consecutive indices for which $x(n) = x(n + N_d)$, given the synchronization mismatch δ. N_w denotes that the received signal is divided into N_w segments in [36]. The size of the convolution kernel is $N_x \times N_y \times N_{ch}$.

From this table, the online computational complexity of SAE-SS is intermediate, and that of SAE-TF is the highest, among these sensing methods. Note that there is no complex multiplication for SAE-SS because we partition the complex signals into the real and imaginary parts (refer to equation (3.6)). For SAE-TF, the complex

Table 3.1: Online computational complexity of different sensing methods.

Method	Complex Multiplications	Real Multiplications
CP	$(N_c+N_d)(M+N_{S_\tau}+1)+M(N_c+N_d)^2$	$2(N_c+N_d)(N_c+N_d-N_{S_\tau})$
CM	$MN_d\log_2\frac{N_d}{2}+MN_d^2$	$2(N_d^2-N_d)$
ANN	$2M(N_c+N_d)$	$4K_1+\sum_{l=2}^{L}K_lP_l+K_L$
CNN	$4M(N_c+N_d)(1+\log_2(N_d+N_c))$	$2N_wN_xN_yN_{ch}+K_L$
SAE-SS	None	$2MK_1(N_c+N_d)+\sum_{l=2}^{L}K_lP_l+K_L$
SAE-TF	$M(N_d+N_c)\log_2(N_d+N_c)$	$4MK_1(N_c+N_d)+\sum_{l=2}^{L}K_lP_l+K_L$

multiplications come from the operation of FFT (refer to equation (3.18)). When $N_c = 8$, $N_d = 64$, $M = 2$, $L = 2$, $N_{S_\tau} = 7$, $K_1 = 100$, $K_2 = 50$, $N_w = 10$, $N_x = N_y = 4$, and $N_{ch} = 5$, the total numbers of real multiplications of the proposed SAE-SS and SAE-TF are 33850 and 66202, respectively. By contrast, the numbers of ANN-based, CNN-based, CM-based and CP-based methods are 7754, 18170, 43392, and 53568, respectively. Besides, the online sensing time of SAE-TF is only about $0.647ms$ in our experiment environment, which is feasible in practice. Moreover, that time can be significantly reduced by using more powerful computing resources in practice. Note that although SAE-TF has the highest number of real multiplications, it achieves much better sensing performance than the other methods.

3.5.2 SAE-SS and SAE-TF with Additional Input Features

We further study the impact of additional information/features (e.g., the energy of received signal, CP feature and CM feature) on the sensing performance. As an example, for the CP and CM features, we adopt their test statistics from [37] and [33], respectively. We take the SAE-SS as a study case (similar results can be easily obtained for SAE-TF). Its new input signal is

$$\hat{\mathbf{x}} := \{\mathbf{x}, \mathbf{x}_{af}\}, \tag{3.21}$$

where $\mathbf{x}$ is the initial input signal, and $\mathbf{x}_{af}$ is the additional feature, which can be written as

$$\mathbf{x}_{af} := \{\Upsilon_{\mathrm{ED}}, \Upsilon_{\mathrm{CP}}, \Upsilon_{\mathrm{CM}}\}^T, \tag{3.22}$$

where Υ_{ED}, Υ_{CP} and Υ_{CM} are test statistics of ED, CP- and CM-based detections, respectively.

As observed in Fig. 3.14 in Section 3.6, additional features to the input can help SAE-SS and SAE-TF reduce PM. This implies that considering the additional features can improve the sensing performance of our proposed methods. However, that is achieved at the expense of higher complexity (in both the offline training and online spectrum sensing stages).

3.5.3 Training and Other Practical Aspects

Like other neural network-based methods (e.g., ANN-based [34] and CNN-based [36]), SAE-SS and SAE-TF require labeled data for the training purpose. However, we would like to emphasize that for the practical scenario, our proposed methods can still obtain the data with correct labels. Specifically, when the labeled data is not available, SU first uses conventional sensing methods (e.g., ED) for collecting and labeling data, which may be subject to false alarms and miss detections. According to the FCC document, SUs are required to sense at least 30 seconds to determine the IU's activity states [106]. In our experimental setup, the signal bandwidth is 5 MHz and the duration for each OFDM sample is 12.8 μs, so SU can obtain around 2×10^6 labeled samples within a period of 30s. The samples labeled by conventional sensing methods have to be calibrated/corrected before being used to train the SAE network.

According to the FCC proposals, the government agencies (e.g., FCC [107] or National Telecommunications and Information Administration, NTIA [108]) released a public notice that includes a list of IU's channels to improve the spectrum utilization. SUs can operate on these channels after determining the absence of IU by using sensing techniques. If SU's conventional sensing results are subject to miss detections (i.e., failing to detect IU's signals), agencies will notify SU immediately when it operates on IU's channels [109]. By this means, SU can correct/calibrate those samples suffering from miss detections. If SU's conventional sensing reports IU activities (but there is actually no IU activity, a.k.a. false alarms), according to the FCC proposals [109], in this case, the SU cannot utilize IU's channels and must

provide a notice of the detection to agencies. Besides, all SUs in the local network are required to respond whether they had detected IU's signal or not. In this way, the FCC can verify the correctness of the notice from SU by taking all responses from all SUs into consideration [109]. If the notice is correct (i.e., IU is present), agencies will remove the corresponding channel from the list of IU's channels, otherwise, notify SU about its wrong notice [109]. Under such a situation, SU can correct those samples subject to false alarms. Consequently, SU can calibrate the sensing results (i.e., labeled data), obtaining data with accurate labels.

Therefore, the sensing accuracies of our proposed methods are not dependent on those of the conventional sensing methods. Besides, since our proposed methods employ SAE architectures to learn and extract more essential features from the received signal for sensing, they are capable of achieving better sensing results than the conventional sensing methods. Note that these labeled data are only required at the beginning (i.e., the calibration) and after that our proposed framework can run autonomously (using learned features during the calibration). Besides, we agree that our approach using SAE involves a relatively large number of parameters. However, given its higher sensing accuracy and thanks to the latest advances in specialized hardware for ML-based computation (e.g., GPU circuits), radio devices can effectively manage the computation in our proposed SAE-based approaches.

3.6 Simulation Results

In this section, we first conduct simulations to analyze the performance of the proposed two methods (i.e., SAE-SS and SAE-TF) and compare them with conventional OFDM signal sensing methods (e.g., basic ED method, CP-based sensing method [37], CM-based sensing method [33]) and neural network-based methods (ANN-based [34], and CNN-based methods [36]). Besides, we provide the performance analysis of SAE-SS and SAE-TF with different parameters. The propagation channel between IU transmitter and SU receiver is a frequency selective Rayleigh fading channel. For both the training phase and sensing phase, we generate an OFDM system with the binary phase shift keying (BPSK) modulation [110]. The OFDM

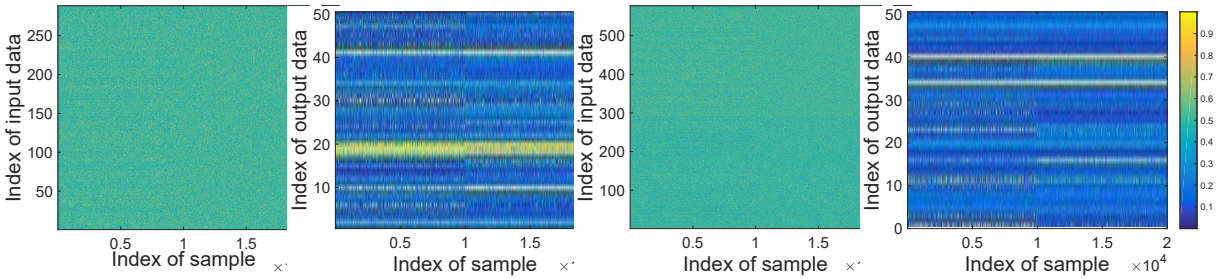
block size of IU signals is $N_d = 64$ and CP length is $N_c = N_d/8$. The signal bandwidth is 5 MHz, and the radio frequency is 2.4 GHz. Each subcarrier spacing is 78.125 kHz, and the duration for each OFDM sample is 12.8 μs. In both the training phase and the online sensing phase, SNR varies from -20dB to -8dB. The timing delay is $\delta \in [0, N_c + N_d - 1]$. The normalized CFO is $f_d \in [0, 1]$. The SNR, timing delay and CFO in the training phase are the same as in the sensing phase.

We set the number of hidden layers for both SAE-SS and SAE-TF as $L = 2$. The first and second hidden layers contain 100 and 50 units, respectively. The number of received OFDM blocks is $M = 2$. The number of input units for SAE-SS and SAE-TF are $2M(N_c+N_d)$ and $2*2M(N_c+N_d)$, respectively. The probability of false alarm is PFA= 0.05. Both the training data set and the testing data set contain $2 * 10^4$ samples. The learning rate is 0.01, the batch size is 100, and the number of epochs is 500. The Adam is selected as the optimizer, and the loss function is cross-entropy. The experiments are conducted on a 6-Core 3.6GHz PC with Nvidia P5000 graphic card (16GB memory).

Fig. 3.5 shows the performance of extracted hidden/unknown features for SAE-SS and SAE-TF under SNR= -15dB, compared with the input signals of the first layer. Specifically, the first 10^4 samples denote "IU is absent" and the second 10^4 samples mean "IU is present". The numbers of input data of the first layer for SAE-SS and SAE-TF are 288 and 576, respectively. For each method, the number of output signals of the second hidden layer is 50. From Fig. 3.5(a) and Fig. 3.5(c), it is very difficult to differentiate between "IU is absent" and "IU is present" based on the input signals only. However, they can be readily separated by the output signals of the second hidden layer as (much more clearly) visually observed in Fig. 3.5(b) and Fig. 3.5(d). We interpret that is because SAE-SS and SAE-TF extract more hidden features from the received signals.

3.6.1 Training Strategies for SAE-SS and SAE-TF

For our proposed schemes, we can use one of the two training strategies to train the SAE network. For the training strategy 1 (TS-1), we divide the training data into different groups with respect to the SNR conditions to train the different SAE



(a) (b) (c) (d)

Figure 3.5: Performance of extracting hidden features for SAE-SS and SAE-TF under SNR=-15dB. (a) Input signals of the first layer for SAE-SS; (b) Output signals of the second hidden layer for SAE-SS; (c) Input signals of the first layer for SAE-TF; (d) Output signals of the second hidden layer for SAE-TF.

architectures [35, 36]. The architecture parameters are held unchanged after the training process. During the spectrum sensing stage, depending on the level of the SNR, different SAE architectures can be selected. This adaptation can significantly improve the sensing performance.

For the training strategy 2 (TS-2), we use all the training data to train a single SAE network for all different SNR conditions. It means the trained SAE is later used without requiring SNR values. However, the sensing performance of TS-2 is worse than that of TS-1, under the same training conditions, as shown in Fig. 3.6.

Fig. 3.6 compares the sensing performance of TS-1 and TS-2 under the "perfect conditions". In the perfect conditions, there is no noise uncertainty, timing delay or carrier frequency offset. Additionally, the SU has sufficient prior knowledge of IU signals (e.g., signal structure, CP of IU's signals, transmitting power, and noise power). In this figure, it is clear that our proposed SAE-SS and SAE-TF can achieve a smaller PM using the strategy TS-1. Therefore, in the sequel, we use the strategy TS-1 to train SAE networks. Note that though TS-1 can achieve better sensing performance than TS-2, the accurate noise power is required for selecting the trained SAE architectures. Thus the noise uncertainty affects the performance of TS-1 (refer to Fig. 3.8). By contrast, TS-2 is immune to the noise uncertainty, as it does not need the noise power for the sensing purpose.

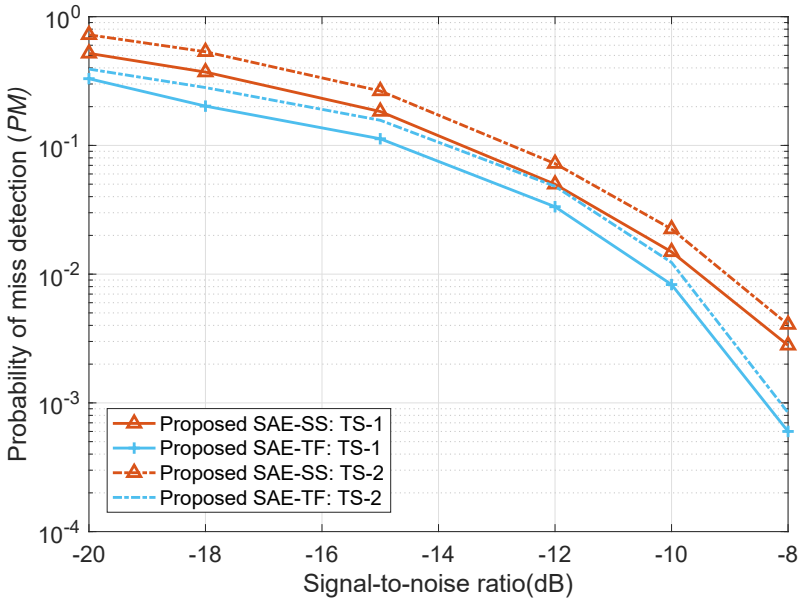


Figure 3.6: Probability of missed detection for SAE-SS and SAE-TF using two training strategies under perfect conditions.

3.6.2 Comparison with Existing OFDM Sensing Methods

In this subsection, we compare sensing performance and training time under different conditions for seven sensing methods.

Sensing performance

Under "perfect conditions", as can be seen in Fig. 3.7, the values of PM of SAE-SS and SAE-TF are much smaller than all other sensing methods. For instance, when SNR=−20dB, PM of SAE-SS and SAE-TF are only 0.5189 and 0.3298, respectively. By contrast, the figures for ED, CM-based, CP-based, ANN-based, and CNN-based sensing methods are 0.8279, 0.9192, 0.8145, 0.7413, and 0.652, respectively. Moreover, with the increase of SNR, PM of SAE-SS and SAE-TF reduce much faster than the other sensing methods.

Fig. 3.8 shows the impact of noise uncertainty η on seven sensing methods. According to this figure, it is clear that the proposed SAE-SS and SAE-TF are much more robust to noise uncertainty than the other five sensing methods. For instance, when η increases from 0.5dB to 1dB under SNR= −10dB, PM of the proposed SAE-SS and SAE-TF only increase from 0.0155 to 0.0190 and from 0.0098 to 0.0114, respectively. On the contrary, PM of CNN-based, ANN-based, CP-based,

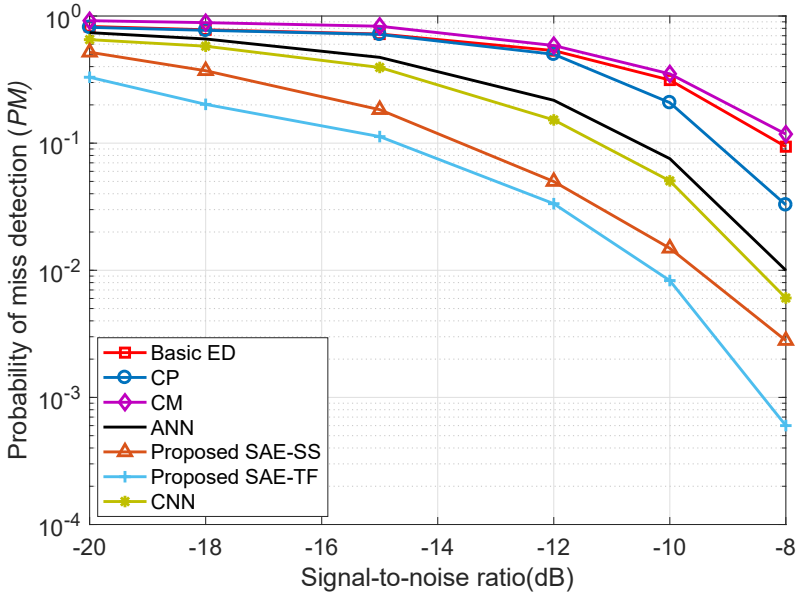


Figure 3.7: Probability of missed detection among different spectrum sensing methods under perfect conditions.

CM-based, and ED methods increase from 0.0615 to 0.0761, from 0.0845 to 0.1045, from 0.2549 to 0.3415, from 0.4213 to 0.5142, and from 0.4522 to 0.6450, respectively.

Fig. 3.9 compares the effect of random timing delay on the sensing performance of different methods. Since ED is not affected by timing delay, we only present the sensing performance of the other six sensing methods. In this figure, the timing delay is uniformly distributed in the range $[0, N_c + N_d - 1]$, where $N_d = 64$, $N_c = 8$. As can be seen, compared with the existing methods, our proposed SAE-SS and SAE-TF are more robust to timing delay. Moreover, our proposed methods are able to achieve a much smaller PM than the other methods.

Fig. 3.10 shows the impact of CFO. The normalized CFO in this figure is set to 0.5 and 1, respectively. The sensing results of ED are not presented in this figure, because they are not affected by CFO. It is obvious that the proposed SAE-SS and SAE-TF outperform the CP-based, CM-based, ANN-based, and CNN-based sensing methods regarding the robustness to CFO. SAE-SS and SAE-TF are capable of achieving much smaller PM than the other sensing methods. Moreover, PM of SAE-SS and SAE-TF increase slightly when the normalized CFO grows. However, PM of ANN-based, CM-based and CP-based methods increase significantly.

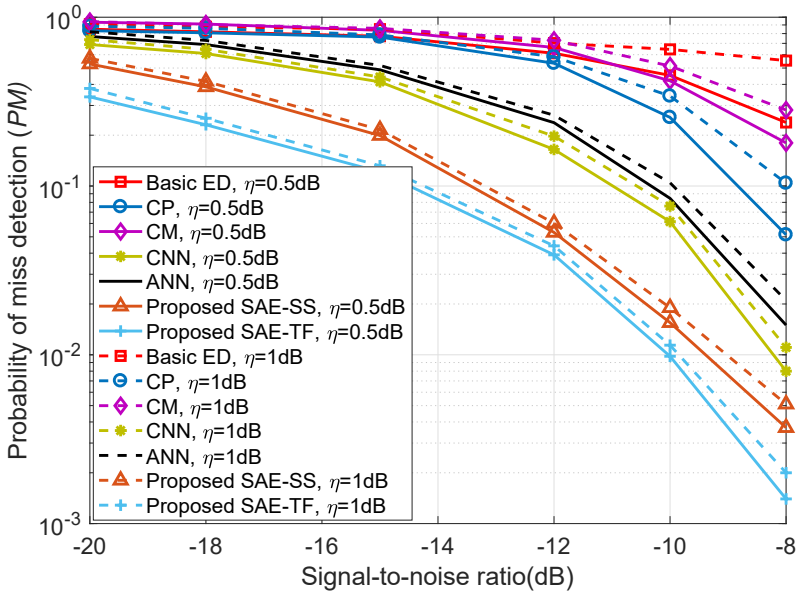


Figure 3.8: Probability of missed detection among different spectrum sensing methods with noise uncertainty.

Fig. 3.11 depicts the effect of incorrect labels on the probability of miss detection (PM). The SNR is this figure is -12dB. As can be seen, it is clear that PM of each method grows with the increased number of incorrect labels. However, compared to other ML-based methods, our proposed SAE-based methods have much lower PM, meaning that our work can achieve much higher sensing accuracy.

As can be seen from Fig. 3.7 $\sim$ Fig. 3.11, our SAE-based methods outperform ANN-based [34] and CNN-based [36] sensing methods. The reason is that the ANN-based method only uses the energy and Zhang test statistic [111] from the Likelihood Ratio Test statistic as features to train the ANN network. For CNN-based method, it only uses the energy and cyclostationary features to train the CNN for detecting IUs' presence. As such, both ANN- and CNN-based methods inevitably lose other important (but hidden) features of IU's activity (in addition to what were used). By contrast, in our proposed methods, SAE architectures are trained to learn all the important information from the originally received signals instead of explicitly extracted features. In this way, more essential information/features that are important to spectrum sensing can be obtained, enabling our proposed SAE-SS and SAE-TF to be more resistant to noise uncertainty, timing delay, CFO or incorrect labels.

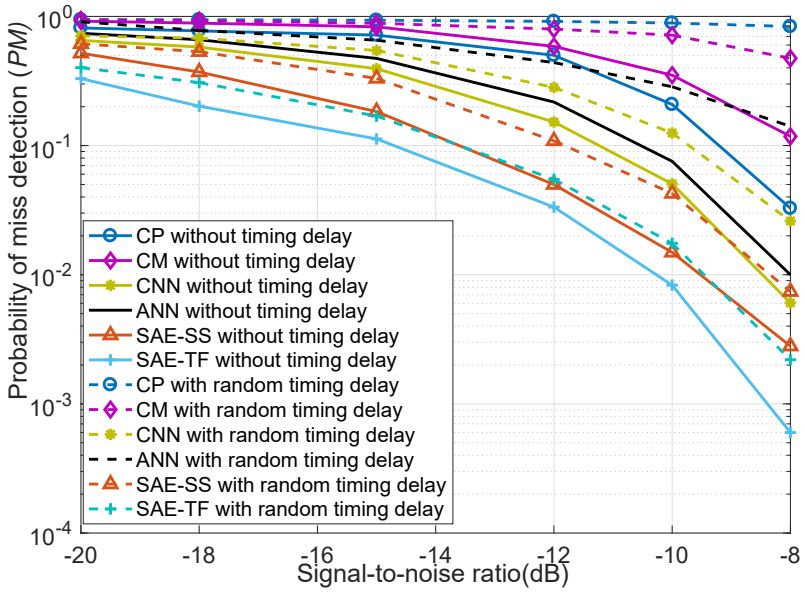


Figure 3.9: Probability of missed detection for SAE-SS and SAE-TF with random timing delay.

Table 3.2: Performance and training time of different learning-based methods.

Method	Offline Training Time			PM (SNR=−12dB)		
	$L_{TS}=10^3$	$L_{TS}=10^4$	$L_{TS}=10^5$	$L_{TS}=10^3$	$L_{TS}=10^4$	$L_{TS}=10^5$
SAE-SS	0.32mins	2.87mins	24.61mins	0.081	0.0499	0.0445
SAE-TF	0.59mins	5.81mins	43.68mins	0.072	0.0334	0.0264
ANN	0.12mins	0.97mins	8.21mins	0.524	0.2713	0.2132
CNN	0.21mins	1.72mins	15.74mins	0.388	0.1473	0.1121

Training time

Table 3.2 shows the relationship between the sensing performance and the training time with different number of training samples. In this table, L_{TS} stands for the number of OFDM samples in the training phase. As can be seen from this table, the more training samples, the lower PM (i.e., the higher sensing accuracy). Although our proposed sensing methods require a relatively large amount of data for training, the training phase is conducted offline. Hence the training phase does not occupy the time or resources of the spectrum sensing stage. Moreover, the offline training is only required once. After that, SUs can use the trained network for sensing IU's activity in the future as long as user's operational information does not change. As an example, in this study, the signal bandwidth is 5MHz, and the radio frequency

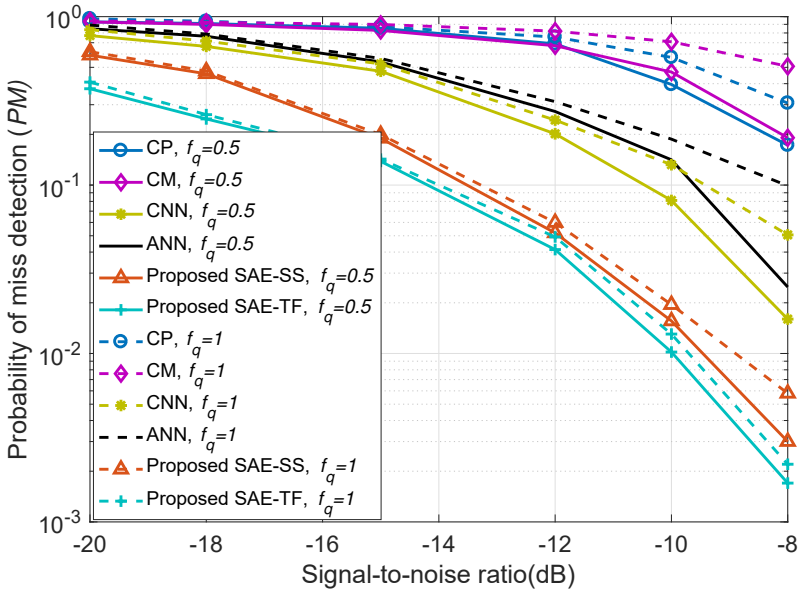


Figure 3.10: Probability of miss detection among different spectrum sensing methods with CFO.

is 2.4GHz. Each subcarrier spacing is 78.125 kHz, and the duration for each OFDM sample is 12.8μs. Thus it is feasible to obtain the required number of samples for our proposed approaches. Besides, the user can select a different amount of samples based on its specific requirements. Notably, that training time can be significantly reduced with the specialized hardware implementation/design in practice (e.g., using specialized GPU cards from NVIDIA).

3.6.3 Sensing Performance under Different Settings

In this subsection, we further analyze the sensing performance of the proposed SAE-SS and SAE-TF under different settings.

Fig. 3.12 shows the effect of a different number of hidden units on the sensing performance. In this figure, SNR= -18dB, $M = 2$ and $L = 2$, the numbers of input units for SAE-SS and SAE-TF are 288 and 576, respectively. When the number of hidden units is equal to or larger than the number of input units, PM is slightly reduced, meaning that the sensing accuracy is better. However, accordingly, the SAE network also becomes much more complicated, significantly increasing the complexity of the offline training and online sensing stages.

Fig. 3.13 shows the sensing performance of SAE-SS and SAE-TF with different

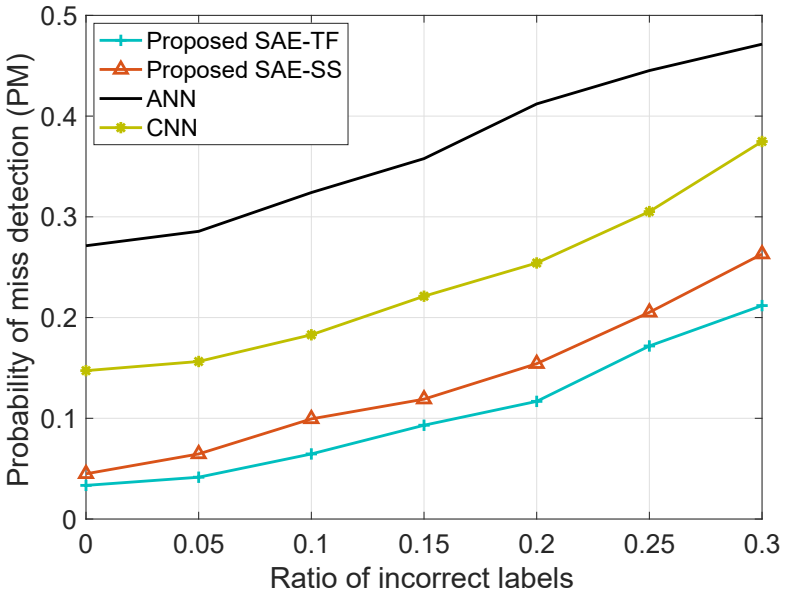


Figure 3.11: Effect of error labels on sensing accuracy for different deep learning architectures.

Table 3.3: Offline Training time for SAE-SS and SAE-TF with different M.

Methods \ M	$M = 1$	$M = 2$	$M = 3$
SAE-SS	104.68mins	159.32mins	254.15mins
SAE-TF	122.47mins	321.92mins	451.24mins

numbers of the received OFDM blocks M. According to this figure, it is obvious that the sensing performance of these two sensing methods is affected by the factor M. When M changes from 1 to 3, SNR=$-$10dB, PM of SAE-SS declines by 0.0402, and PM of SAE-TF decreases by 0.0221. Notably, the complexity also increases with the growth of M, captured by the training time recorded in Table 3.3.

Table 3.3 shows the offline training time of SAE-SS and SAE-TF with a different number of OFDM blocks M. The number of hidden layers is $L = 2$, and there are 100 and 50 units in the first and second hidden layer, respectively. The training data set contains 10^6 samples. Based on this table, the offline training time of SAE-TF is bigger than that of SAE-SS. Moreover, with the increase of M, the offline training time of SAE-TF is increasingly longer than SAE-SS. Since SAE-TF can achieve higher sensing performance than SAE-SS, it provides a better tradeoff

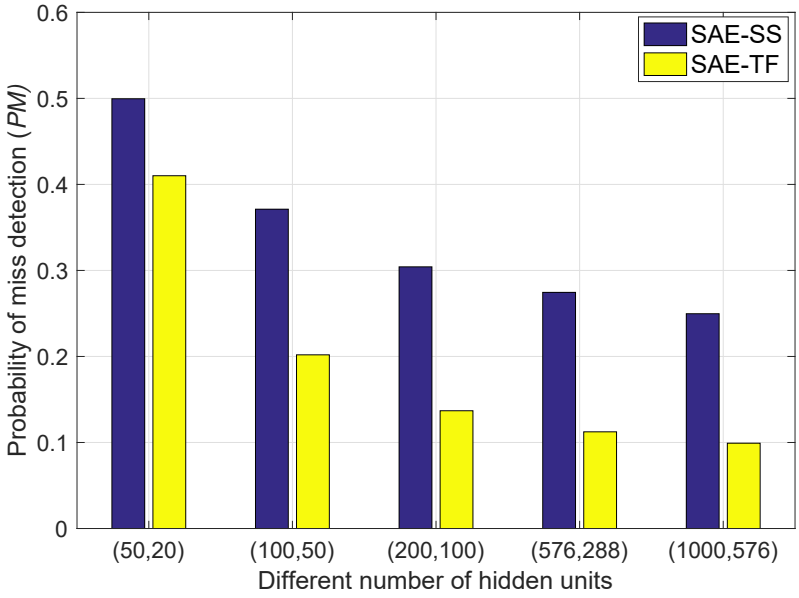


Figure 3.12: Probability of miss detection for SAE-SS and SAE-TF with different number of hidden units.

Table 3.4: Impact of different CP lengths (N_c) on the sensing performance.

Method \ CP length	$N_c = 0$	$N_c = 8$	$N_c = 16$
SAE-SS	0.066	0.0499	0.0301
SAE-TF	0.0498	0.0334	0.0211

between accuracy and complexity.

Table 3.4 shows the effect of different CP lengths (N_c) on the sensing performance, with SNR= -12dB. From this table, it is clear that for both SAE-SS and SAE-TF, the longer CP allows us to achieve better sensing accuracy (i.e., a smaller PM value). This implies that our proposed methods do extract more essential information from CP content. For instance, when N_c increases from 0 to 16, PM of SAE-SS and SAE-TF decrease from 0.066 to 0.0301 and from 0.0498 to 0.0211, respectively. However, it is important to note that the longer CP would lead to a smaller size of data block, reducing the efficiency of data transmission.

Fig. 3.14 depicts the values of PM of our proposed methods with additional features (i.e., the energy of received signal, CP feature and CM feature). As can be seen from this figure, the values of PM of SAE-SS with additional features

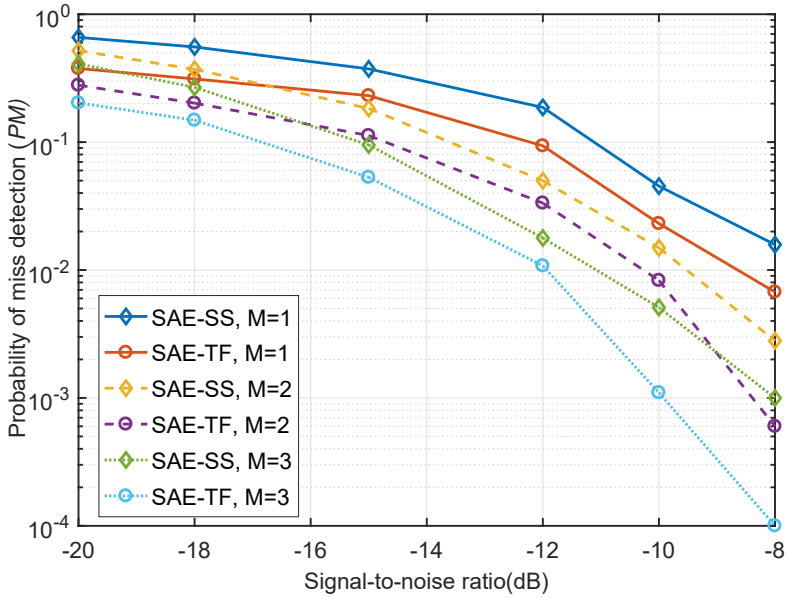


Figure 3.13: Probability of missed detection of SAE-SS and SAE-TF with different numbers of the received OFDM blocks.

(SAE-SS-AF) and SAE-TF with additional features (SAE-TF-AF) are smaller than those of SAE-SS and SAE-TF. This implies that considering the additional features can improve the sensing performance of our proposed methods. However, adding additional features would lead to much higher computational complexity for the online sensing phase due to the feature extraction process (refer to Table 5.1 for more details). Therefore, users can select different input signal taking their requirements of sensing performance and computational complexity into account.

Table 3.5 shows the values of PM of our proposed methods with different numbers of training samples. From this table, it is clear that the overfitting occurs when the number of training samples reduces, significantly increasing PM. This is because when the size of training samples is small, the SAE adopted in this work extracts too much detailed information from the (small) training dataset, thereby negatively impacting on its generalization performance and severely influencing the sensing results. On the contrary, when the number of training samples keeps increasing, PM is slightly reduced, meaning that the sensing accuracy is better. However, accordingly, the SAE network also processes much more samples, which significantly increases the complexity of the training stage. Therefore, users can select different numbers of training samples based on their specific requirement of sensing accuracy

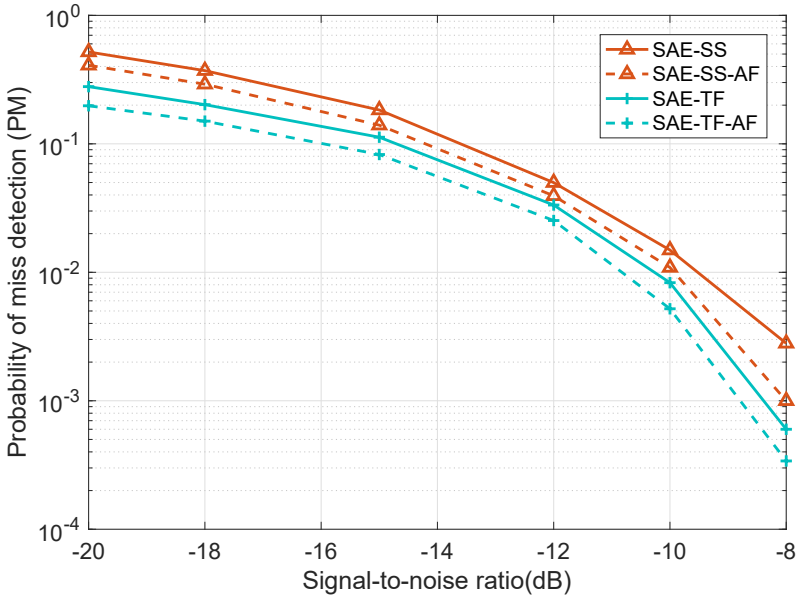


Figure 3.14: Probability of miss detection for SAE-SS and SAE-TF with additional features under perfect conditions.

Table 3.5: Performance of proposed methods with a different number of training samples.

Method	PM (SNR=−12dB)				
	$L_{TS} = 10^2$	$L_{TS} = 10^3$	$L_{TS} = 10^6$	$L_{TS} = 10^7$	$L_{TS} = 10^8$
SAE-SS	0.3954	0.081	0.0422	0.04145	0.04139
SAE-TF	0.2874	0.072	0.0226	0.02138	0.02131

and complexity.

Fig. 3.15 illustrates the effect of hidden layers (L). As can be seen, when L is small, the values of PM for these two sensing methods become smaller by increasing L. However, the overfitting occurs if the number of hidden layers keeps increasing, thereby increasing PM. This is because continuously increasing the number of hidden layers introduces too many parameters, over-complicating the network and degrading the sensing performance.

We also examine the effect of different DL architectures on the sensing accuracy, as shown in Fig. 3.16. The input data for each DL architecture are the original received signals. The SNR in this figure is −12dB. The CNN with dense connections is adopted from [112], which has two dense blocks with the same number of layers. The size of each convolutional kernel is 3×3 with stride 2. We use 1×1 convolution

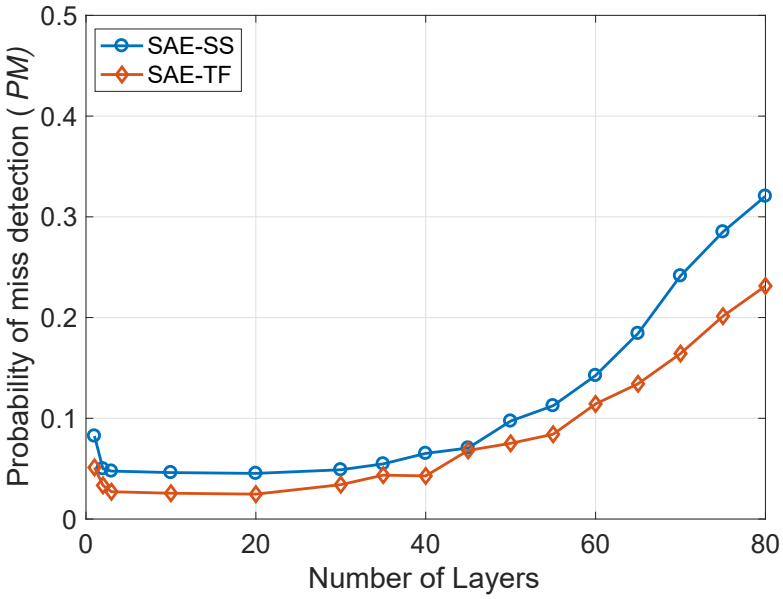


Figure 3.15: Probability of miss detection for proposed methods with different number of hidden layers.

followed by 2×2 average pooling as transition layers between two contiguous dense blocks. For the typical CNN without dense connections, it has two convolutional layers, and the size of the convolution kernel is 3×3 with stride 2. From this figure, it is clear that when the number of labeled samples is small (e.g., 10^3), the values of PM for our proposed SAE-SS and SAE-TF are notably smaller than those under the CNN with and without dense connections. In other words, our proposed SAE-based methods are able to achieve better sensing accuracy than CNN-based methods, with a limited amount of labeled data. We also observe that by increasing the labeled samples, CNN with dense connections can achieve a smaller PM than other methods. This improved performance comes at the cost of high complexity.

3.7 Conclusion

In this chapter, we proposed a Stacked Autoencoder Based Spectrum Sensing Method (SAE-SS) and a Stacked Autoencoder Based Spectrum Sensing Method with time-frequency domain signals (SAE-TF) to detect the activity states of IUs using OFDM signal. SAE-SS and SAE-TF are more robust to timing delay, CFO, and noise uncertainty, compared with the conventional OFDM sensing methods. Moreover, they are able to detect IU's activities solely based on the received signals and without

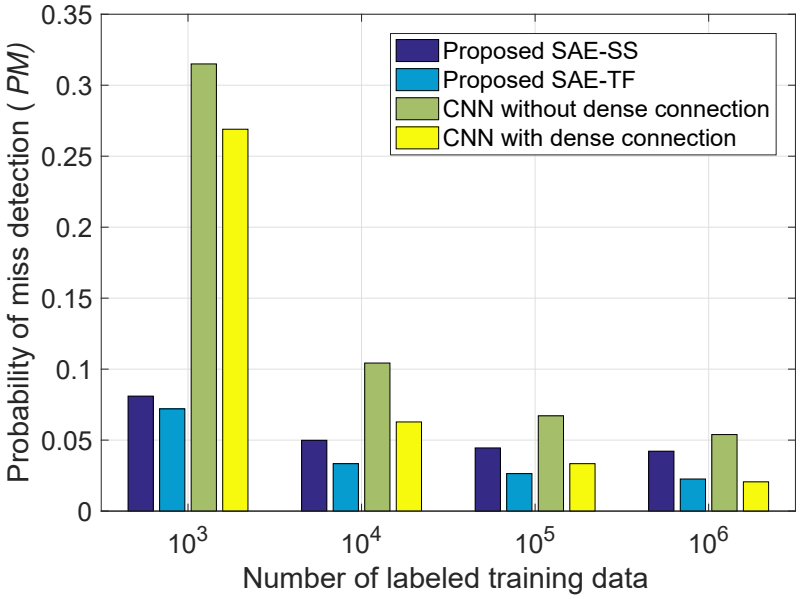


Figure 3.16: Probability of miss detection with different deep learning architectures.

any requirement of prior knowledge of IU's signals. SAE-SS and SAE-TF also do not require any external feature extraction algorithms. SAE-TF achieves a better sensing accuracy than SAE-SS, especially under low SNR conditions, while it has the higher complexity. Extensive simulation results demonstrate that SAE-SS and SAE-TF are capable of achieving much higher sensing performance than traditional OFDM sensing methods even under low SNR and severe timing delay, CFO, and noise uncertainty conditions. This is thanks to the capability of the underlying deep neural networks of SAE-SS and SAE-TF that extract both known and unknown hidden features of OFDM signals.

Chapter 4

Dynamic Spectrum Access in Full-duplex Systems

In the previous chapter, we studied the spectrum sensing methods in HD systems, which however are deficient in addressing the problem of spectrum scarcity. In this chapter, for improving the spectrum utilization, we present two novel spectrum sensing approaches under the FD communication paradigm by leveraging the CP feature and PT feature of OFDM signals, respectively. The proposed CP and PT approaches aim to reduce the severe impact of the residual self-interference, and are able to mitigate the timing delay and CFO, respectively.

4.1 Introduction

In FD systems, detecting the IU's activity states (i.e., presence or absence) is challenging due to the residual self-interference that leads to low SINR and severely affects the test statistics of sensing methods [74, 75]. Although some methods that leverage the unique features of signals (e.g., CP or PT feature of OFDM signals) can alleviate the adverse effect of self-interference to some extent, they are heavily vulnerable to timing delay or CFO [33, 79]. A small mismatch between the received and transmitted signals in the time domain or frequency domain would significantly degrade the sensing accuracy. Besides, it is challenging for conventional feature-based methods to achieve good sensing performance under low SNR conditions. For

the above reasons, in this chapter, we will propose two sensing methods drawing support from the CP and PT structures of OFDM signals, respectively. The main contributions of this chapter are summarized below.

- We investigate spectrum sensing and its related issues in the OFDM cognitive FD system and propose a novel spectrum sensing method with the help of CP and PT features of OFDM signals, respectively. We consider two different self-interference signals (with or without the CP (PT) structure) to analyze the sensing performance of the presented approaches. We also derive the closed-form expressions of the probability of detection and false alarm for the proposed approaches.

- Comparing with other conventional spectrum sensing approaches (using CP features [37]), the presented CP method is robust to various levels of timing delay and residual self-interference, thereby achieving much higher sensing accuracy, even under low SNR conditions. In addition, the proposed CP spectrum sensing approach can completely avoid complex estimation processes for mitigating the impact of the timing delay, which is, however, necessary for conventional spectrum sensing approaches (using CP-based features [37]).

- In comparison with conventional PT-based spectrum sensing methods (e.g., [79]), the presented PT sensing approach is more robust to the residual SI and CFO. Unlike the conventional PT-based sensing methods which require complex estimation processes to estimate the impact of the CFO, the presented PT sensing approach is able to completely avoid such a requirement, significantly reducing the computational complexity. Additionally, our PT approach is also capable of achieving much higher sensing accuracies under the low SNR condition.

The rest of this chapter is organized as follows. In Section 4.2, we present the system model and problem formation. The proposed CP-based sensing approach and the PT-based sensing method are expressed in Section 4.3 and Section 4.4, respectively. The numerical simulations results are presented in Section 4.5. Finally, Section 4.6 concludes our findings.

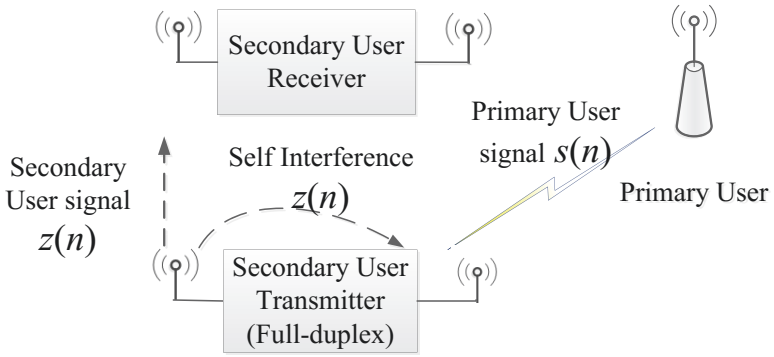


Figure 4.1: System model of FD: SU is in the "Listen and Talk" mode.

4.2 System Model and Problem Formulation

In this chapter, we consider a simplified cognitive FD system, depicted in Fig. 4.1. The IU has the highest priority to utilize the licensed spectrum and transmits OFDM signals. The SU works in the full-duplex mode, e.g, simultaneously sensing the licensed spectrum and using that licensed channel (when IU is absent) for its data transmission. The SU transmits two types of signals: OFDM signals or other modulation signals, as will be discussed in Section 4.3.1. The received signal at the SU transmitter, which is used to detect the presence of the IU, can be expressed as

$$\begin{aligned} H_0 &: y_m(n) = r_m(n) + w_m(n), \\ H_1 &: y_m(n) = \sum_{l=0}^{L_p-1} h_l s_m(n-l) + r_m(n) + w_m(n), \end{aligned} \tag{4.1}$$

where H_0 refers to the null hypothesis standing for the absence of IU. H_1 is the alternate hypothesis denoting the presence of IU. $y_m(n)$ is the received signal with $m = 0, \ldots, M$ and M is the total number of received OFDM blocks. $n = 0, \ldots, N_c + N_d - 1$, $N_c + N_d$ stands for the length of OFDM signal. N_c is the length of the cyclic prefix and N_d denotes the data block size. $w_m(n) \sim CN(0, \sigma_w^2)$ is the complex additive white Gaussian noise (AWGN). $r_m(n)$ is the residual self-interference. L_p denotes the number of multi-path components between the IU and the SU. h_l stands for the channel gain of the lth channel component ($h_l \sim CN(0, \sigma_h^2)$).

The test statistics of the received signal by two classical detectors (energy detec-

tor and wave-form-based detector), namely T_{EN} and T_W, can be obtained by

$$T_{EN} = \frac{1}{(N_c + N_d - 1)M} \sum_{m=0}^{M-1} \sum_{n=0}^{N_c+N_d-1} |y_m(n)|^2, \tag{4.2}$$

$$T_W = \frac{1}{(N_c + N_d - 1)M} \sum_{m=0}^{M-1} \sum_{n=0}^{N_c+N_d-1} y_m(n) s_m(n)^H, \tag{4.3}$$

where $(.)^H$ denotes the conjugate transpose.

As discussed previously, the received signals are collected for detecting the activity states of IU (i.e., presence or absence). However, it is clear that the residual self-interference signals are involved in the received signals under both H_0 and H_1, thereby notably degrading the sensing performance in FD systems, especially for the energy detector [77]. Although the sensing performance of the waveform-based detector is better than that of the energy detector [78], the timing delay significantly affects the results of the waveform-based detector. Thus complex estimation methods have to be applied to reduce the effect of timing delay, highly increasing sensing overhead. The sensing methods leveraging CP features or PT features [33] can achieve better sensing methods with the residual self-interference; however, they are sensitive to timing delay or CFO that causes dramatic performance degradation. To address the above problems, in the next sections, we develop two novel sensing methods by leveraging the CP and PT features of OFDM signals, respectively.

4.3 Cyclic Prefix based Spectrum Sensing Approach

In this section, we first present our spectrum sensing method based on the CP feature of OFDM signals to address the residual self-interference and timing delay. Then the theoretical expressions of the probability of detection (P_d) and false alarm (P_f) of our method are derived.

The received signal in equation (4.1) can be rewritten as

$$\begin{aligned} H_0 &: y_m(n) = r_m(n) + w_m(n), \\ H_1 &: y_m(n) = \sum_{l=0}^{L_p-1} h_l s_m(n - \delta - l) + r_m(n) + w_m(n), \end{aligned} \tag{4.4}$$

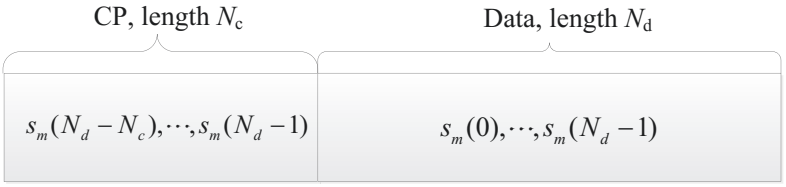


Figure 4.2: Simplified structure of the mth OFDM block.

where δ is the integer timing delay. $r_m(n) \sim CN(0, \sigma_r^2)$ stands for the RSI, and it can be expressed as $r_m(n) = \alpha z_m(n)$, where $z_m(n)$ is the self-interference signal (transmitted signal of SU), and α is the self-interference suppression factor [26] which is defined as $\alpha = \sqrt{\frac{P_s}{P_{s_T}}}$, where P_s is the power of self-interference and P_{s_T} is the power of SU's transmitted signal.

Consider the FD system shown in Fig. 4.1, the transmitted signal from the IU is OFDM modulated, where CP (the length of N_c) is placed before the data part (the length of N_d) in each OFDM symbol block (refer to Fig. 4.2). CP is a replication of some data symbols, which provides a unique feature when computing the correlation of the received signal. Based on this special character, we propose a new cross-correlation:

$$T_i = \sum_{m=0}^{M-1} \sum_{j=0}^{N_c-1} y_m^H(i+j) y_m(i+j+N_d), \tag{4.5}$$

where $i = 0, \ldots, N_c + N_d - 1$. According to equation (4.5), the new cross-correlation T_i correlates the received signal with the window of length N_c over all the received OFDM symbol blocks. $\mathbf{T} = [T_0, T_1, \ldots, T_{N_c+N_d-1}]^T$ is the new test statistic and will be applied to sense the spectrum. Taking the vector $\mathbf{T}$ rather than a single T_i to sense the interested spectrum has a merit that the impact of timing delay δ on the sensing performance can be eliminated, thus the complex processes for estimating δ can be avoided. However, an estimation process with high complexity is necessary if just a single T_i is taken into account (the details will be given in the following section).

Based on the generalized likelihood ratio test (LRT), the test statistic of the proposed detection is given as

$$\mathcal{R} = \frac{P_r(\mathbf{T}|H_1)}{P_r(\mathbf{T}|H_0)} \underset{H_1}{\overset{H_0}{\lessgtr}} \gamma, \tag{4.6}$$

where $P_r(\cdot)$ stands for the probability density function (*pdf*) and γ is the threshold. According to equation (4.5), T_i can be assumed to obey a complex Gaussian distribution based on the central limit theorem when N is large under H_0 and H_1. Thus, $P_r(\mathbf{T})$ are equal to

$$P_r(\mathbf{T}|H_0) = \frac{1}{(2\pi)^{\frac{(N_c+N_d)}{2}}|\mathbf{G}_{0,\delta}|^{\frac{1}{2}}}\exp(-\frac{1}{2}\mathbf{T}^H\mathbf{G}_{0,\delta}^{-1}\mathbf{T}), \tag{4.7}$$

$$\begin{aligned} P_r(\mathbf{T}|H_1) &= \frac{1}{(2\pi)^{\frac{(N_c+N_d)}{2}}|\mathbf{G}_{1,\delta}|^{\frac{1}{2}}}\exp(-\frac{1}{2}(\mathbf{T}-\mu_{\mathbf{T}})^H \\ &\quad \times\mathbf{G}_{1,\delta}^{-1}(\mathbf{T}-\mu_{\mathbf{T}})), \end{aligned} \tag{4.8}$$

where $\mu_{\mathbf{T}}$ denotes the mean vector of $\mathbf{T}$ under H_1. $\mathbf{G}_{0,\delta}$ and $\mathbf{G}_{1,\delta}$ are the covariance matrices of $\mathbf{T}$ under H_0 and H_1 with timing delay δ, respectively. Thus, equation (4.6) can be rewritten as

$$\mathcal{R} = \frac{|\mathbf{G}_{0,\delta}|^{\frac{1}{2}}}{|\mathbf{G}_{1,\delta}|^{\frac{1}{2}}}\frac{\exp(-\frac{1}{2}(\mathbf{T}-\mu_{\mathbf{T}})^H\mathbf{G}_{1,\delta}^{-1}(\mathbf{T}-\mu_{\mathbf{T}}))}{\exp(-\frac{1}{2}\mathbf{T}^H\mathbf{G}_{0,\delta}^{-1}\mathbf{T})} \underset{H_1}{\overset{H_0}{\lessgtr}} \gamma. \tag{4.9}$$

Since the closed-form distribution expression of $\mathcal{R}$ is hard to be obtained, the threshold γ has to be computed empirically. However, this computational process costs a lot of extra time and system resources. To solve this problem, we assume that all T_i are independent. Thus the derivation of the joint distribution of $\mathbf{T}$ is simplified. Consequently, $\mathcal{R}$ can be approximated as

$$\begin{aligned} \mathcal{R} &= \frac{\prod_{i=0}^{N_c+N_d-1}\frac{1}{\sqrt{2\pi}\sigma_{i,1}}\exp(-\frac{|T_i-\mu_{i,1}|^2}{2\sigma_{i,1}^2})}{\prod_{i=0}^{N_c+N_d-1}\frac{1}{\sqrt{2\pi}\sigma_{i,0}}\exp(-\frac{|T_i|^2}{2\sigma_{i,0}^2})} \\ &= \prod_{i=0}^{N_c+N_d-1}\frac{\sigma_{i,0}}{\sigma_{i,1}}\exp(-\frac{|T_i-\mu_{i,1}|^2}{2\sigma_{i,1}^2}+\frac{|T_i|^2}{2\sigma_{i,0}^2}), \end{aligned} \tag{4.10}$$

where $\mu_{i,1}$ is the mean of T_i under H_1, and $\sigma_{i,0}^2$, $\sigma_{i,1}^2$ stand for the variance of T_i under H_0 and H_1, respectively. Let $a_i \triangleq \sigma_{i,0}^2\sigma_{i,1}^2/(\sigma_{i,1}^2-\sigma_{i,0}^2)$, $b_i \triangleq a_i\mu_{i,0}/\sigma_{i,1}^2$, and applying a few manipulations, equation (4.10) can be rewritten with the new test statistic $\mathcal{R}_1$ and threshold γ_1 as follows

$$\begin{aligned} \mathcal{R}_1 &= \frac{|T_0+b_0|^2}{a_0}+\frac{|T_1+b_1|^2}{a_1}+\cdots+\frac{|T_{N_c+N_d-1}+b_{N_c+N_d-1}|^2}{a_{N_c+N_d-1}} \\ &= \sum_{i=0}^{N_c+N_d-1}\frac{|T_i+b_i|^2}{a_i} \underset{H_1}{\overset{H_0}{\lessgtr}} \gamma_1, \end{aligned} \tag{4.11}$$

where

$$\gamma_1 \triangleq \sum_{i=0}^{N_c+N_d-1} (\frac{b_i^2}{a_i} + \frac{\mu_{i,1}^2}{\sigma_{i,1}^2}) + 2\ln(\gamma \prod_{i=0}^{N_c+N_d-1} \frac{\sigma_{i,1}}{\sigma_{i,0}}).$$

4.3.1 Probability of False Alarm and Detection

In the previous section, the test statistic of the proposed detector has been provided. In this part, we derive the expressions for P_d and P_f of the proposed algorithm.

To get the distribution of $\mathcal{R}_1$, the means and variances of T_i under both H_0 and H_1 are required (see equation (4.11)). Since T_i is the value of correlation based on the CP structure, whether the received signals have the CP structure will greatly affect statistical characteristics of T_i. Since the noise signal has no CP structure, its effect on the test statistic is quite small. For the self-interference signal, it is possible to hold the CP structure, so discussing the structure of the self-interference signal (whether it holds the CP structure or not) is significant to achieve a satisfactory performance. In this part, two special cases are taken into consideration: self-interference signals which do not have the CP structure and self-interference signals which have the CP structure as the IU.

1) Case A: Self-interference signals do not have CP structure

In this case, in order to get the *pdf* of $\mathcal{R}_1$, the means and variances of T_i in hypotheses H_0 and H_1 have to be calculated first. Under H_0, since the received signal contains the self-interference signal and noise, T_i is

$$\begin{aligned} T_i|H_0 &= \sum_{m=0}^{M-1}\sum_{j=0}^{N_c-1} \big(\alpha z_m(i+j) + w_m(i+j)\big)^H \\ &\quad \times \big(\alpha z_m(i+j+N_d) + w_m(i+j+N_d)\big). \end{aligned} \tag{4.12}$$

Since the self-interference signal does not have the CP structure, $z_m(i+j)$ and $z_m(i+j+N_d)$ are independent of each other. Moreover, the self-interference signal is independent of noise. Thus, the mean and variance of T_i are

$$\begin{aligned} \mu_{i,0} &= \mathrm{E}[\sum_{m=0}^{M-1}\sum_{j=0}^{N_c-1} (\alpha z_m(i+j)+w_m(i+j))^H(\alpha z_m(i+j+N_d)+w_m(i+j+N_d))] \\ &= 0, \end{aligned} \tag{4.13}$$

$$\sigma_{i,0}^2 = \mathrm{E}[|T_i|^2|H_0] - \mathrm{E}[T_i|H_0]^2 = MN_c(\sigma_w^2 + \alpha^2 E_z)^2, \tag{4.14}$$

where E_z is the power of the self-interference signal. Under H_1, according to equation (4.4), T_i is equal to

$$T_i|H_1 = \sum_{m=0}^{M-1}\sum_{j=0}^{N_c-1}[(y_m^H(i+j)|H_1)(y_m(i+j+N_d)|H_1), \tag{4.15}$$

and the mean of T_i is

$$\mu_{i,1} = \mathrm{E}[T_i|H_1] = M\sum_{j=0}^{N_c-1}\sum_{l=0}^{L_p-1}\sigma_h^2\mathrm{E}[s_m^H(i+j-\delta-l)s_m(i+j-\delta-l+N_d)]. \tag{4.16}$$

Due to the CP structure of the IU signal, if $i+j-\delta-l \in \epsilon$, where $\epsilon = [0,1,2,\ldots,N_c-1]$, then

$$\mathrm{E}[s_m^H(i+j-\delta-l)s_m(i+j-\delta-l+N_d)] = E_s, \tag{4.17}$$

where E_s is the power of the IU signal. Let's define an indicator function

$$\mathbf{1}_\epsilon(\tau) := \begin{cases} 1, & \text{if } \tau \in \epsilon, \\ 0, & \text{if } \tau \notin \epsilon. \end{cases} \tag{4.18}$$

Consequently, equation (4.16) can be expressed as

$$\mu_{i,1} = \sigma_h^2 M E_s \sum_{j=0}^{N_c-1}\sum_{l=0}^{L_p-1}\mathbf{1}_\epsilon(i+j-\delta-l). \tag{4.19}$$

Let $\Lambda(i,\delta,L_p) \triangleq \sum_{j=0}^{N_c-1}\sum_{l=0}^{L-1}\mathbf{1}_\epsilon(i+j-\delta-l), i=0,\ldots,N_c+N_d-1$, then the final expression of $\mu_{i,1}$ is

$$\mu_{i,1} = \sigma_h^2 M E_s \Lambda(i,\delta,L). \tag{4.20}$$

The variance $\sigma_{i,1}^2$ can be calculated as

$$\begin{aligned}\sigma_{i,1}^2 &= \mathrm{E}[|T_i|^2|H_1] - \mathrm{E}[T_i|H_1]^2 \\ &= M\sigma_h^4 E_s^2 \Lambda(i,\delta,L)^2 + MN_c(L\sigma_h^2 E_s + \alpha^2 E_z + \sigma_w^2)^2.\end{aligned} \tag{4.21}$$

2) Case B: Self-interference signals have the CP structure

In this scenario, as self-interference signals have the CP structure with a length of N_s, thus $z_m(i+j)$ and $z_m(i+j+N_d)$ are equal when $i+j \in \omega$, and $\omega =$

$[0, 1, 2, \ldots, N_s - 1]$. As a result, according to equation (4.12), the mean and variance of T_i under H_0 are

$$\begin{aligned}\mu_{i,0} &= \mathrm{E}[T_i|H_0] = M\sum_{j=0}^{N_c-1}\alpha^2\mathrm{E}[z_m^H(i+j)z_m(i+j+N_d)] \\ &= M\alpha^2 E_z\Theta(i), \end{aligned} \tag{4.22}$$

$$\begin{aligned}\sigma_{i,0}^2 &= \mathrm{E}[|T_i|^2|H_0] - \mathrm{E}[T_i|H_0]^2 \\ &= M\alpha^4 E_z^2\Theta(i)^2 + MN_c(\alpha^2 E_z + \sigma_w^2)^2, \end{aligned} \tag{4.23}$$

where $\Theta(i) \triangleq \sum_{j=0}^{N_s-1}\mathbf{1}_\omega(i+j), i = 0, \ldots, N_c + N_d - 1$. Following similar derivation methods discussed in the previous section, the mean and variance of T_i under H_1 can be obtained as

$$\mu_{i,1} = \sigma_h^2 M E_s\Lambda(i, \delta, L) + M\alpha^2 E_z\Theta(i). \tag{4.24}$$

$$\begin{aligned}\sigma_{i,1}^2 &= \mathrm{E}[|T_i|^2|H_1] - \mathrm{E}[T_i|H_1]^2 \\ &= M\big(\sigma_h^4 E_s^2\Lambda(i, \delta, L)^2 + \alpha^4 E_z^2\Theta(i)^2\big) + MN_c\big(L\sigma_h^2 E_s + \alpha^2 E_z + \sigma_w^2\big)^2. \end{aligned} \tag{4.25}$$

As discussed above, the means and variances of T_i can be obtained in the two special cases. Getting the distribution of $\mathcal{R}_1$ in equation (4.11), the expression has to be further simplified. Consider the low signal-to-noise ratio (SNR) situation; according to equations (4.14), (4.21), (4.23) and (4.25) we can assume $\sigma_{i,0}^2 \approx \sigma_{i,1}^2$. So $\mathcal{R}_1$ in equation (4.11) can be further rewritten with $\mathcal{R}_2$ and γ_2 as follows:

$$\mathcal{R}_2 = \sum_{i=0}^{N_c+N_d-1}\frac{\mu_{i,1}}{\sigma_{i,0}^2}\mathrm{Re}(T_i) \underset{H_1}{\overset{H_0}{\lessgtr}} \gamma_2, \tag{4.26}$$

where $\gamma_2 \triangleq \ln(\gamma_1) + \sum_{i=0}^{N_c+N_d-1}\mu_{i,1}^2/2\sigma_{i,0}^2$. Re(.) means taking the real part. According to the central limit theorem, T_i can be assumed to obey a complex Gaussian random distribution when the received data is large, and thus $\mathrm{Re}(T_i)$ is a Gaussian random variable. Obviously, $\mathcal{R}_2$ in equation (4.26) has a Gaussian distribution that

$$\mathcal{R}_2 \sim \begin{cases} \mathcal{N}(0, \sum_{i=0}^{N_c+N_d-1}\frac{\mu_{i,1}^2}{2\sigma_{i,0}^2}) & , \mathcal{H}_0 \\ \mathcal{N}(\sum_{i=0}^{N_c+N_d-1}\frac{\mu_{i,1}^2}{\sigma_{i,0}^2}, \sum_{i=0}^{N_c+N_d-1}\frac{\mu_{i,1}^2\sigma_{i,1}^2}{2\sigma_{i,0}^4}) & , \mathcal{H}_1. \end{cases} \tag{4.27}$$

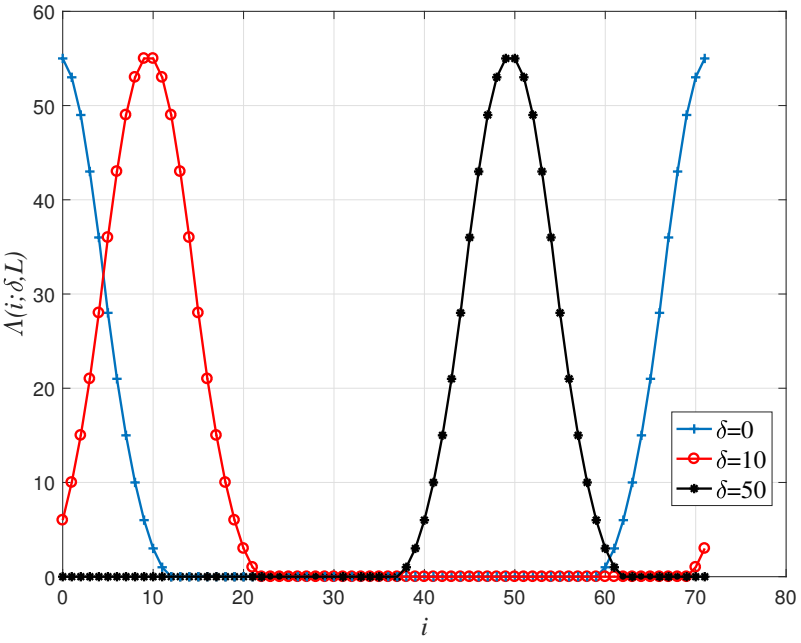


Figure 4.3: Value of $\Lambda(i,\delta,L)$, $L=10$, $N_d=64$, $N_c=8$.

Therefore, the probability of P_f and P_d can be expressed as

$$P_f = Q\left(\frac{\gamma_2}{\sqrt{\sum_{i=0}^{N_c+N_d-1}\frac{\mu_{i,1}^2}{2\sigma_{i,0}^2}}}\right), P_d = Q\left(\frac{\gamma_2 - \sum_{i=0}^{N_c+N_d-1}\frac{\mu_{i,1}^2}{\sigma_{i,0}^2}}{\sqrt{\sum_{i=0}^{N_c+N_d-1}\frac{\mu_{i,1}^2\sigma_{1,i}^2}{2\sigma_{i,0}^4}}}\right). \tag{4.28}$$

The performance of the proposed spectrum sensing method can be evaluated based on the NP criterion [113] which fixes the P_f or P_d to get the threshold γ_2.

4.3.2 Analysis of Timing Delay Impact on Sensing Performance

According to P_f, P_d, as well as the means and variances expressions of T_i, since only $\sum_{i=0}^{N_c+N_d-1}\frac{\mu_{i,1}^2}{2\sigma_{i,0}^2}$ and $\sum_{i=0}^{N_c+N_d-1}\frac{\mu_{i,1}^2\sigma_{1,i}^2}{2\sigma_{i,0}^4}$ contain the timing delay δ, we just discuss the influence of δ on these two parts. Take the mean and variance of T_i in the case A as an example, these two terms are equal to

$$\begin{aligned}\sum_{i=0}^{N_c+N_d-1}\frac{\mu_{i,1}^2}{2\sigma_{i,0}^2} &= \sum_{i=0}^{N_c+N_d-1}\frac{(\sigma_h^2 M E_s \Lambda(i,\delta,L))^2}{M N_c \sigma_w^4} \\ &= \frac{\sigma_h^4 M E_s^2}{N_c\sigma_w^4}\sum_{i=0}^{N_c+N_d-1}\Lambda(i,\delta,L)^2,\end{aligned} \tag{4.29}$$

$$\sum_{i=0}^{N_c+N_d-1} \frac{\mu_{i,1}^2 \sigma_{i,1}^2}{\sigma_{i,0}^4}$$
$$= \sum_{i=0}^{N_c+N_d-1} \frac{[\sigma_h^2 M E_s \Lambda(i,\delta,L)]^2}{M^2 N_c^2 \sigma_w^8} [M\sigma_h^4 E_s^2 \Lambda(i,\delta,L)^2 + MN_c(L\sigma_h^2 E_s + \sigma_w^2)^2]$$
$$= \frac{\sigma_h^4 M E_s^2}{N_c \sigma_w^8} [\frac{\sigma_h^4 E_s^2}{N_c} \sum_{i=0}^{N_c+N_d-1} \Lambda(i,\delta,L)^4 + (L\sigma_h^2 E_s + \sigma_w^2) \sum_{i=0}^{N_c+N_d-1} \Lambda(i,\delta,L))^2]. \quad (4.30)$$

Thus, δ only affects $\sum_{i=0}^{N_c+N_d-1} \Lambda(i,\delta,L)^2$ and $\sum_{i=0}^{N_c+N_d-1} \Lambda(i,\delta,L)^4$. Fig. 4.3 shows the value of $\Lambda(i,\delta,L)$ for $L = 10$. Clearly, the value of δ only determines the position of $(\Lambda(i,\delta,L))_{max}$, but does not affect the actual value of $\Lambda(i,\delta,L)$. Thus, $\sum_{i=0}^{N_c+N_d-1} \Lambda(i,\delta,L)^2$ and $\sum_{i=0}^{N_c+N_d-1} \Lambda(i,\delta,L)^4$ are constant for a fixed L. Therefore, P_f and P_d of the proposed method are independent of timing delay.

4.4 Pilot Tone based Spectrum Sensing Approach

In the previous section, we proposed a CP based sensing method to address the residual self-interference and timing delay. In this section, we will develop a sensing approach by leveraging the PT features of OFDM signals to overcome the residual self-interference and CFO in FD systems. Specifically, the details of our proposed spectrum sensing algorithm based on the PT feature of OFDM signals are firstly provided. We then derive theoretical expressions of the probability of miss detection (P_m) and false alarm (P_f) of our developed sensing approach.

The received signal in equation (4.1) can be expressed as

$$\begin{aligned} H_0 &: y_m(n) = r_m(n) + w_m(n), \\ H_1 &: y_m(n) = e^{\frac{j2\pi f_q n}{N_d}} \sum_{l=0}^{L_p-1} h_l s_m(n-l) + r_m(n) + w_m(n), \end{aligned} \quad (4.31)$$

where f_q represents the CFO normalized to the subcarrier spacing. $s_m(n)$ is the transmitted OFDM signal and can be given by

$$s_m(n) = \sqrt{\frac{E_s}{N_d}} \sum_{k=0}^{N_d-1} I_m(k) e^{j2\pi nk/N_d}, n \in [-N_c, N_d - 1], \quad (4.32)$$

where E_s stands for the transmitted power of each symbol. N_d is the data block size. $I_m(k)$ represents the symbol modulating the kth subcarrier with unit variance.

Given an OFDM system, PTs are always designed/added to meet the channel estimation requirement. In this chapter, we adopt a circular configuration type of PT [114], meaning that the pilot signals are different in one block but they are reused in every several blocks. Besides, all PTs signals have the same amplitude. As a result, the correlation features between PTs can provide unique features that can be utilized to sense the presence of IU. Furthermore, in order to utilize the PT feature for the sensing purpose, the received time domain signal should be converted into frequency domain. Specifically, the discrete Fourier transform of the received signal (the CP structure is already discarded) can be written as

$$\widetilde{Y}_m(k) = U_m(k) + R_m(k) + W_m(k), \tag{4.33}$$

where

$$\begin{aligned} U_m(k) &= \sum_{n=0}^{N_d-1} \sqrt{E_s}\Delta_{f_q}(n-k)H(n)I_m(n), \\ \Delta_{f_q}(i) &= \frac{sin(\pi f_q)}{sin(\frac{\pi}{N_d}(f_q+i))}\exp(j\frac{\pi}{N_d}((N_d-1)f_q-i)), \end{aligned} \tag{4.34}$$

where $H(n) = \sum_{l=0}^{L-1} h_l e^{-j2\pi ln/N_d}$ represents the frequency response of the nth subcarrier. $R_m(k) \sim CN(0, \sigma_r^2)$ and $W_m(k) \sim CN(0, \sigma_w^2)$ denotes the residual self-interference and noise in the frequency domain, respectively. Since the signal of IU has the circular configuration PT structure, $\widetilde{Y}_m$ and $\widetilde{Y}_s$ have the same PT arrangement if $m - s = dv, d = 1, 2, 3 \ldots$, where v is the circular period. On the basis of this feature, the proposed new cross-correlation matrix is given by

$$\mathbf{C} = \frac{1}{N_v} \sum_{N_v} \widetilde{\mathbf{Y}}_m^{PT} (\widetilde{\mathbf{Y}}_s^{PT})^H, \tag{4.35}$$

where $\mathbf{C}$ stands for the cross-correlation matrix of size $N_p \times N_p$. N_p is the length of PT. $\widetilde{\mathbf{Y}}_m^{PT}$ denotes the PT vector in the mth OFDM block. N_v is defined as $N_v = \lceil \frac{M-1}{2v} \rceil (2M - v - v\lceil \frac{M-1}{v} \rceil)$ representing the total number of OFDM block pairs (m, s) with the same PT arrangement. $(.)^H$ means the conjugate transpose.

Note that in (4.35), the proposed cross-correlation matrix only computes the the pilot tones but ignores other transmitted symbols, so it is able to remove the correlation noise and reduce the effect of residual self-interference. Thus the test

statistic of the proposed method can be written as

$$T = \frac{1}{N_p^2} \sum_{p=0}^{N_p-1} \sum_{q=0}^{N_p-1} |C(p,q)|^2. \tag{4.36}$$

4.4.1 Probability of False Alarm and Detection

In this section, the expressions for P_f and P_m of the proposed algorithm are derived based on the test statistic provided previously. According to equation (4.36), T is the the sum of N_p^2 variables ($|C(p,q)|^2$). Thus in order to get the distribution of T, the statistical features of $C(p,q)$ should be discussed first. Since $C(p,q)$ is the value of cross-correlation of PT structures, statistical characteristics of $C(p,q)$ are dependent on whether the received signals have PT structures or not. For the noise signal, it does not have a PT structure, so its effect on test statistics is quite small. Regarding the residual self-interference signal (i.e., SU's transmitted signal), it is possible to have the PT structure, so it is desirable to discuss the structure of residual self-interference for achieving satisfactory sensing performance. In the following parts, we consider two different cases: residual self-interference signals which have no PT structure and residual self-interference signals which have the PT structure.

1) Case A: Residual self-interference signals without PT structure

In this scenario, for deriving the *pdf* of T, we first calculate the means and variances of $C(p,q)$ in hypotheses H_0 and H_1. Under H_0, since the received signal only contains the residual self-interference signal and noise, $C(p,q)$ can be expressed as:

$$C(p,q)|H_0 = \frac{1}{N_v} \sum_{N_v} \big(R_m(p) + W_m(p)\big)\big(R_s(q) + W_s(q)\big)^H. \tag{4.37}$$

As the residual self-interference signal has no PT structures, $R_m(p)$ is independent of $R_s(q)$. Besides, as mentioned previously, the residual self-interference signal and noise are independent of each other, hence, the mean and variance of $C(p,q)$ can be obtained by

$$\mu_0(p,q) = \mathrm{E}[\frac{1}{N_v} \sum_{N_v} \big(R_m(p) + W_m(p)\big)\big(R_s(q) + W_s(q)\big)^H] = 0, \tag{4.38}$$

$$\sigma_0^2(p,q)=\mathrm{E}[|C(p,q)|^2|H_0]-\mu_0^2(p,q)=\frac{(\sigma_w^2+\sigma_r^2)^2}{N_v}. \tag{4.39}$$

Under H_1, according to equation (4.33), $C(p,q)$ can be written as

$$C(p,q)|H_1 \;=\; \frac{1}{N_v}\sum_{N_v}\big(U_m(p)+R_m(p)+W_m(p)\big)\big(U_s(q)+R_s(q)+W_s(q)\big)^H. \tag{4.40}$$

As discussed above, for the PT structure of the IU signal, if block index difference $m-s=dv, d=1,2,3\ldots$, then two OFDM blocks have the same PT arrangement. Thus the mean of $C(p,q)$ is

$$\begin{aligned}\mu_1(p,q) &= \mathrm{E}[C_s(p,q)|H_1]\\ &= E_s\sum_{n=0}^{N_d-1}|H(n)|^2\Delta_{f_q}(n-p)\Delta_{f_q}(n-q)^H.\end{aligned} \tag{4.41}$$

The variance of $C(p,q)$ can be given by

$$\sigma_1^2(p,q)=\mathrm{E}[|C(p,q)|^2|H_1]-\mu_1^2(p,q). \tag{4.42}$$

Since the SU intends to sense the licensed spectrum under low SNR conditions, when M is lager, $\sigma_1^2(p,q)$ can be approximated by

$$\begin{aligned}\sigma_1^2(p,q) \;=\; & \frac{3E_s^2}{N_v}\sum_{n=0}^{N_d-1}|H(n)|^4|\Delta_{f_q}(n-p)|^2|\Delta_{f_q}(n-q)|^2\\ & +\frac{E_s(\sigma_w^2+\sigma_r^2)}{N_v}\Big(\sum_{n=0}^{N_d-1}|H(n)|^2|\Delta_{f_q}(n-p)|^2\\ & +|\Delta_{f_q}(n-q)|^2\Big)+\frac{(\sigma_r^2+\sigma_w^2)^2}{N_v}.\end{aligned} \tag{4.43}$$

2) Case B: Residual self-interference signals hold the same PT structure as IU

In this case, we assume the residual self-interference signals have the same PT arrangement as the IU signals. Thus when $n-s=dv$ $(d=1,2,3\ldots)$, $R_m(p)$ is equal to $R_s(p)$, $p=[0,1,\ldots,N_p-1]$, implying that the residual self-interference signal causes a great impact on the value of $C(p,q)$. In such a case, the mean and variance of $C(p,q)$ under H_0 can be obtained according to equation (4.37):

$$\mu_0(p,q)=\mathrm{E}[C(p,q)|H_0]=\sigma_r^2, \tag{4.44}$$

$$\begin{aligned}\sigma_0^2(p,q) &= \mathrm{E}[|C(p,q)|^2|H_0]-\mathrm{E}[C(p,q)|H_0]^2\\ &= \frac{1}{N_v}(\sigma_w^4+2\sigma_w^2\sigma_r^2).\end{aligned} \tag{4.45}$$

The mean and variance of $C(p,q)$ under H_1 can be obtained by following similar derivation processes provided in the previous section, which are

$$\mu_1(p,q) = E_s \sum_{n=0}^{N_d-1} |H(n)|^2 \Delta_{f_q}(n-p)\Delta_{f_q}(n-q)^H + \sigma_r^2, \tag{4.46}$$

$$\begin{aligned}\sigma_1^2(p,q) &= \frac{3E_s^2}{N_v}\sum_{n=0}^{N_d-1}|H(n)|^4|\Delta_{f_q}(n-p)|^2|\Delta_{f_q}(n-q)|^2 \\ &+\frac{E_s(\sigma_w^2+3\sigma_r^2)}{N_v}(\sum_{n=0}^{N_d-1}|H(n)|^2|\Delta_{f_q}(n-p)|^2 \\ &+|\Delta_{f_q}(n-q)|^2) + \frac{2\sigma_r^2\sigma_w^2+\sigma_w^4}{N_v}.\end{aligned} \tag{4.47}$$

Based on all the derivations above, the means and variances of $C(p,q)$ in two special cases can be calculated. According to the central limit theorem, $C(p,q)$ can be approximated as complex Gaussian variable ($C(p,q) \sim CN(\mu(p,q),\sigma^2(p,q))$) when M is large under both H_0 and H_1. As a result, $2|C(p,q)|^2/\sigma^2(p,q)$ obeys a non-central Chi-square distribution with $2|\mu(p,q)|^2/\sigma^2(p,q)$ non-centrality parameter and two degrees of freedom [115]. So the test statistic in equation (4.36) can be rewritten as

$$T' = \frac{1}{N_p^2}\sum_{p=0}^{N_p-1}\sum_{q=0}^{N_p-1}\frac{2|C(p,q)|^2}{\sigma^2(p,q)} \underset{H_1}{\overset{H_0}{\lessgtr}} \gamma, \tag{4.48}$$

where γ is the threshold. According to equation (4.48), $T^{'}$ is the sum of N_p^2 independent and identically distributed non-central Chi-square variables. Thus $T^{'}$ obeys the non-central Chi-square distribution with $2N_p^2$ degree of freedom. The non-central parameters and the probability distribution function of $T^{'}$ under H_0 and H_1 are equal to

$$\begin{aligned}\lambda_{T',0} &= \sum_{p=0}^{N_p-1}\sum_{q=0}^{N_p-1}\frac{2|\mu_0(p,q)|^2}{\sigma_0^2(p,q)}, \\ \lambda_{T',1} &= \sum_{p=0}^{N_p-1}\sum_{q=0}^{N_p-1}\frac{2|\mu_1(p,q)|^2}{\sigma_1^2(p,q)},\end{aligned} \tag{4.49}$$

$$f(T';\eta,\lambda_{T',i}) = \frac{1}{2}e^{\frac{-(T^{'}+\lambda_{T',i})}{2}}(\frac{T^{'}}{\lambda_{T',i}})^{\frac{\eta-2}{4}}B_{\frac{\eta-2}{2}}(\sqrt{\lambda_{T',i}T^{'}}), \tag{4.50}$$

where $i = 0, 1$. η denotes the degree of freedom. $B_\alpha(\theta)$ stands for the modified Bessel function of the first kind defined as $B_\alpha(\theta) = (\frac{\theta}{2})^\alpha \sum_{j=0}^{\infty}[(\frac{\theta^2}{4})^j / j!\Gamma(\alpha + j + 1)]$ and Γ denotes the Gamma function. The cumulative distribution function of $T^{'}$ can be calculated as

$$F(T^{'};\eta,\lambda_{T',i}) = \sum_{j=0}^{\infty} e^{\frac{-\lambda_{T',i}}{2}} \frac{\Lambda(\eta/2 + j, T^{'}/2)}{\Gamma(\eta/2 + j)} \frac{(\lambda_{T',i}/2)^2}{j!}, \tag{4.51}$$

where Λ denotes the lower incomplete Gamma function.

Based on the derivations and definitions above, the expressions of P_f and P_d can be obtained by

$$\begin{aligned} P_f &= 1 - F(\gamma; 2N_p^2, \lambda_{T',0}), \\ P_d &= 1 - F(\gamma; 2N_p^2, \lambda_{T',1}). \end{aligned} \tag{4.52}$$

According to the Neyman-Pearson criterion [113], the performance of the proposed sensing method can be evaluated by fixing P_f to obtain the threshold γ which is

$$\gamma = F^{-1}(1 - P_f; 2N_p^2, \lambda_{T',0}). \tag{4.53}$$

4.4.2 Computational Complexity

In this section, we compare the computational complexity of the proposed sensing approach with other relevant sensing methods, e.g., sampled covariance matrix (SCM) [33] and frequency domain autocorrelation (FD-AC) [79], as shown in Table 4.1.

We select the number of complex multiplications as a metric to validate the computational complexity because it is the most computationally expensive. In Table 4.1, N_{FFT} and N_{comp} stand for the FFT size and the number of used subcarriers (denoted as K and K_{comp} in [79]), respectively. As can be seen from this table, our proposed method costs a much less number of complex multiplications, compared to the other two sensing methods. For instance, when $N_d = 64$, $N = 20$, $N_p = 16$, $v = 3$, $N_{FFT} = 1024$ and $N_{comp} = 242$, the total number of complex multiplications of SCM [33] and FD-AC [79] are 87243 and 151640, respectively. By contrast, the number of the proposed sensing method is only 19915, much lower than the other two sensing methods.

Table 4.1: Computational complexity of different sensing methods.

Method	Number of complex multiplications
SCM [33]	$MN_d \log(N_d) + MN_d^2$
FD-AC [79]	$MN_{FFT} \log(N_{FFT}) + 2MN_{comp}$
Proposed method	$MN_d \log(N_d) + N_v N_p^2$

4.5 Simulation Results

In this section, numerical results of the proposed spectrum sensing approaches are given via Monte Carlo simulations in the FD system. Unless otherwise stated, the simulation configurations are set as follows. The binary phase shift keying (BPSK) modulation is applied to generate an OFDM system. The data block size of the received OFDM signals is $N_d = 64$, and the CP of SU is set as $N_c = N_d/8$ if SU has the CP structure. The length of the PT structure is set as $N_p = 16$ with circular period $v = 3$. The operating radio frequency is 2.4 GHz, and the signal bandwidth is set to be 5 MHz. The spacing for each subcarrier is 78.125 kHz. SNR varies in the range of $-20 \backsim -8$dB, and the normalized CFO is evenly distributed in $[-0.5, 0.5)$. The residual self-interference power at SU's transmitter η is set to be -87dBm adopting the self-interference suppression method proposed in [116]. The number of the received OFDM blocks is $M = 20$, P_f is set to 0.05, and the number of multi-paths L is 10.

4.5.1 Simulation Results of Cyclic Prefix based Approach

Fig. 4.4 compares the probability of miss detection (P_m, $P_m = 1 - P_d$) of the proposed method and energy detection in [76] with different SIS factors. It is obvious that the SIS factor affects these two spectrum sensing methods, but to different extents. Specifically, when α is small, the energy detector in [76] is better than other approaches. However, when α is large, the performance of the energy detector dramatically degrades. For the proposed CP method, although α affects P_m both in cases A and B, the impact is quite small compared with the energy detector in [76]. Therefore, the proposed CP method is superior as it achieves

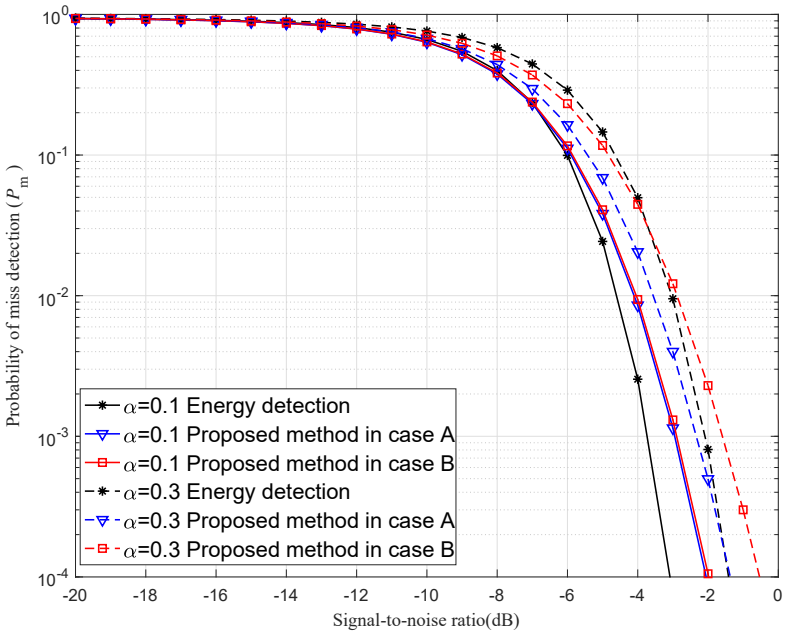


Figure 4.4: Probability of miss detection (P_m) of sensing methods with different self suppression factors.

better performance with big SIS factors. Besides, the proposed CP method can achieve a better performance in case A than in case B. The reason is that in case A, self-interference signals do not have the CP structure, thus the impact of self-interference signals on the T_i is less than that in case B. Thus, under this situation, the proposed CP approach is capable of obtaining better performance.

The impact of timing delay on the sensing methods is illustrated in Fig. 4.5. The timing delay is set to 0-symbol, 5-symbol, and $\alpha = 0.1$. It is apparent that although the wave-based detector in [78] can get better performance than our proposed method with $\delta = 0$ (i.e., without timing delay), it is sensitive to timing delay. By contrast, the timing delay has no influence on the proposed CP algorithm both in cases A and B. For example, when SNR is -5dB, P_m of waveform-based detector increases from 0.031 to 0.13 with δ changing from 0-symbol to 5-symbol. By contrast, P_m of proposed CP method keeps stable at 0.048.

The receiver operating characteristic (ROC) curves for different approaches at SNR = -10dB are shown in Fig. 4.6, where $\alpha = 0.3$ and $\delta = 3$. It can be seen that the proposed CP detector can achieve better performance compared with the other detectors when the communication condition is poor (e.g., the self-interference

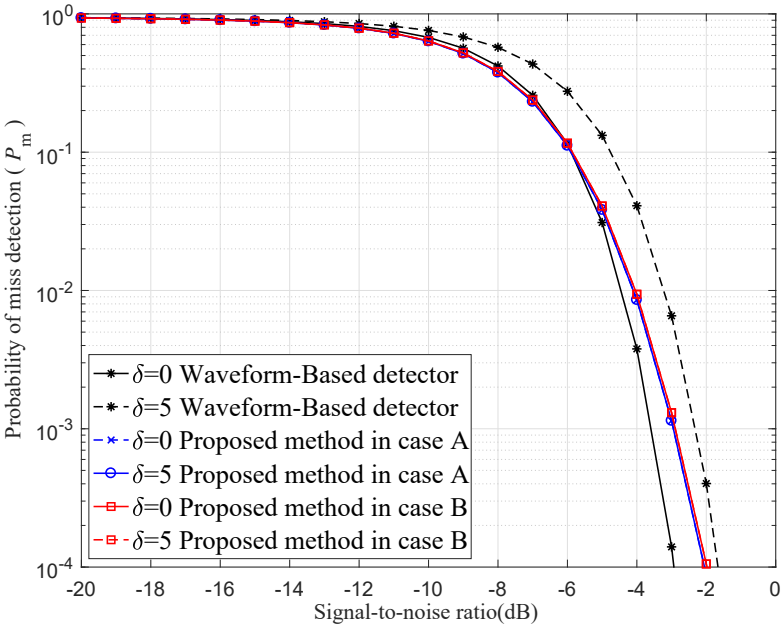


Figure 4.5: Impact of timing delay on different sensing methods, $\alpha = 0.1$.

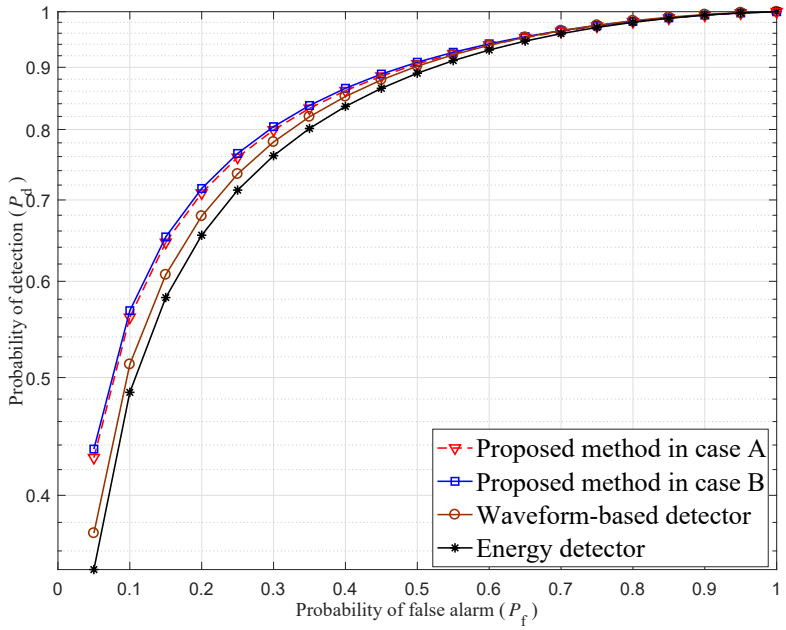


Figure 4.6: ROC curves for different detectors at SNR = -10 dB.

is serious and the timing delay is large), thus the proposed CP approach is more suitable for practical applications.

The impact of different CP ratios (N_c/N_d) of the IU on sensing performance is shown in Fig.4.7, where $M = 15$, $\alpha = 0.3$, $N_s = 8$. Obviously, the performance of the proposed CP method is greatly affected by the CP ratio. Take the case B

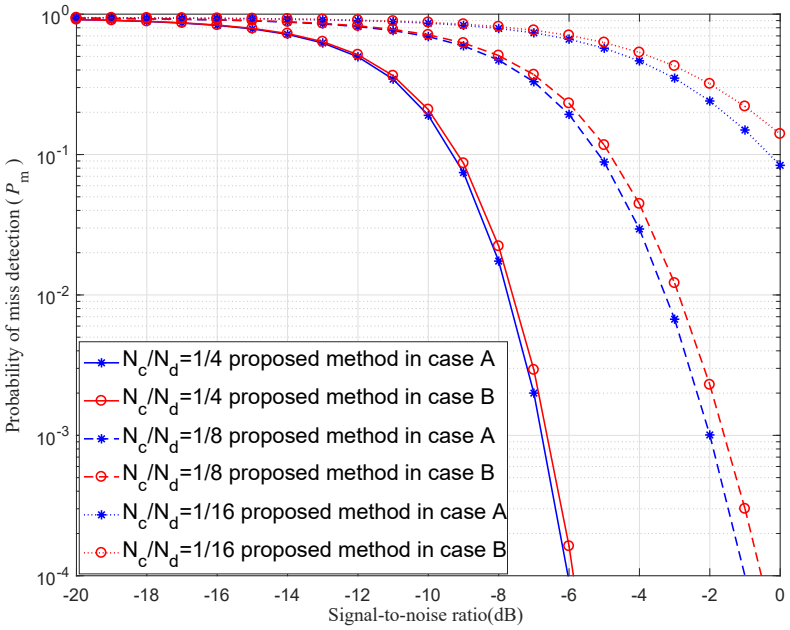


Figure 4.7: Probability of miss detection (P_m) of the proposed method with different CP ratios.

at SNR= -6dB as an example; P_m decreases from 0.81 to 0.03 when the CP ratio increases from 1/16 to 1/4. Thus, the proposed CP sensing method can achieve better performance when IU has a larger CP ratio.

4.5.2 Simulation Results of Pilot Tone based Approach

In Fig. 4.8, we compare the probability of miss detection (P_m) of our proposed PT approach with the other two sensing methods, e.g., SCM [33] and FD-AC [79]. As can be seen, our presented PT approach for both Cases A and B significantly outperforms the other two methods regardless of whether CFO is present or not. Although all the sensing methods are affected by CFO, the impact on our developed PT approach is much less compared with the other two methods. The figure also shows that our proposed PT approach for Case A can achieve better sensing performance, i.e., lower P_m, than Case B. This is because the residual self-interference signal in the Case A has no PT structure, hence, its impact on $\mathbf{C}$ is less than that in the Case B (refer to equation (4.35)), leading to higher sensing accuracy.

To further evaluate the sensing performance, we show the receiver operating characteristic (ROC) curves for various algorithms at SNR $= -15$dB in Fig. 4.9.

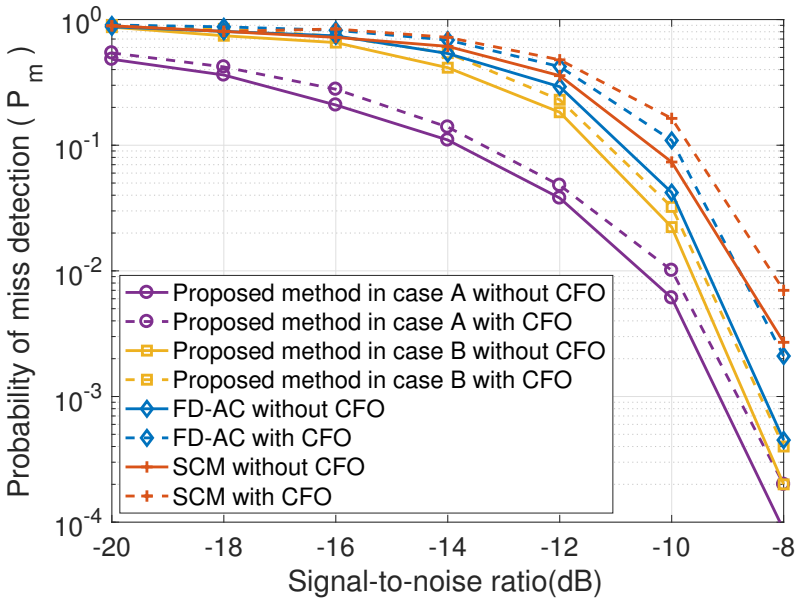


Figure 4.8: Impact of CFO on probability of miss detection (P_m) of various sensing methods.

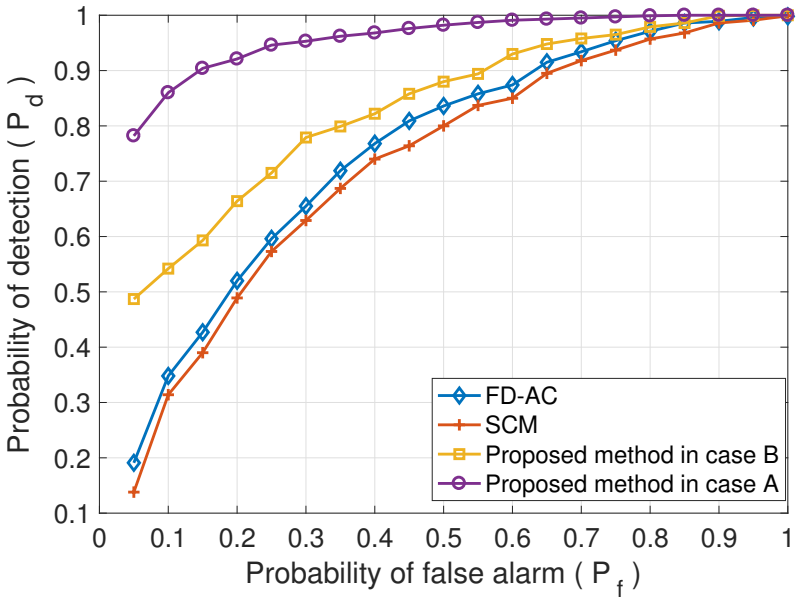


Figure 4.9: ROC curves for different detectors at SNR = -15 dB.

As can be seen, this figure illustrates the relationship between P_d ($P_d = 1 - P_m$) and P_f. We can observe that our proposed PT sensing approach clearly outperforms the other two methods. In particular, with a fixed P_f, the two cases of our proposed PT approach are capable of achieving much better sensing accuracy (i.e., higher P_d) compared with the other two sensing methods. When $P_f = 0.05$, P_d of our proposed PT algorithm in Case A and Case B are 0.782 and 0.487, respectively. However, P_d

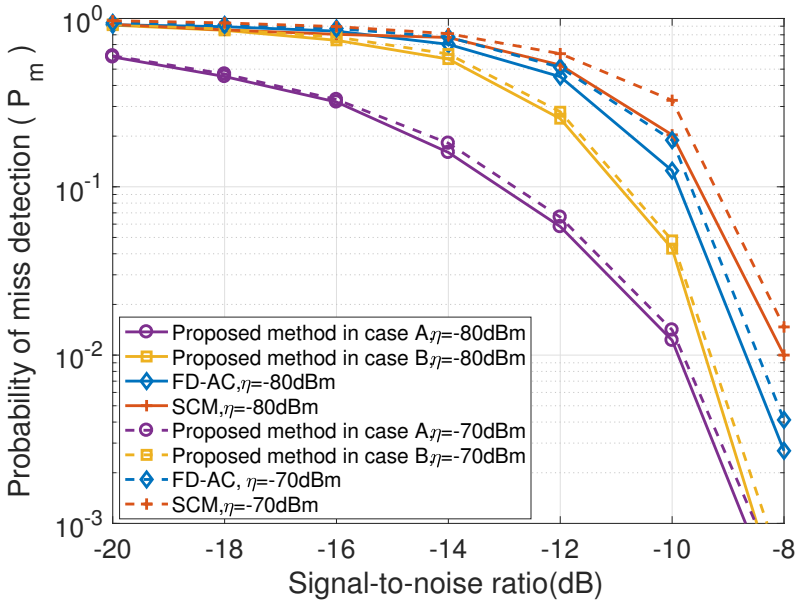


Figure 4.10: Impact of residual self-interference on probability of miss detection (P_m) of different sensing methods.

of FD-AC [79] and SCM [33] methods are only 0.191 and 0.138, respectively.

From Fig. 4.8 and Fig. 4.9, we can obtain an observation that either P_m or ROC is able to show the sensing performance of various sensing methods. Due to the space limitation, in the sequel, we will only discuss P_m.

Fig. 4.10 demonstrates the P_m performance of various methods in the presence of residual self-interference. From this figure, it is apparent that our presented PT algorithm is superior to others regarding the robustness to residual self-interference. Besides, the sensing performance of our method in Case A is better than in Case B because of different types of residual self-interference signals. When SNR is -10dB, as the residual self-interference power η rises from -80dBm to -70dBm, P_m of our designed PT approach in Case A and Case B increase from 0.0122 to 0.0141, and from 0.0429 to 0.0480, respectively. However, P_m of SCM [33] and FD-AC [79] increase from 0.2035 to 0.3263, and from 0.1247 to 0.1892, respectively.

Fig. 4.11 illustrates the impact of the number of received OFDM blocks M on the sensing accuracy of various sensing methods. Obviously, our proposed PT sensing approach in both two cases can achieve much more significant improvements in sensing accuracy (i.e., smaller P_m) with increasing M, compared with the other methods. Moreover, for each sensing method, increasing M can lead to a better sens-

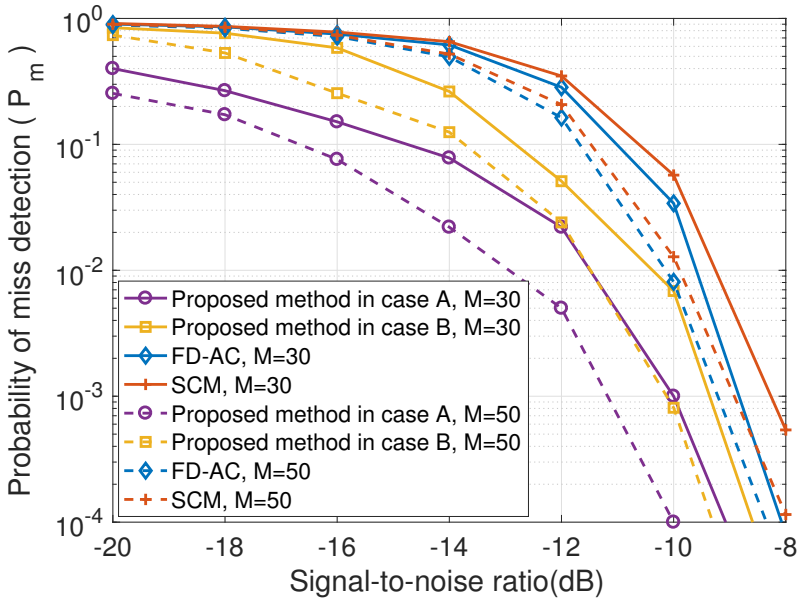


Figure 4.11: Probability of miss detection (P_m) of the proposed method with a different number of blocks, M.

ing performance, while this comes at the cost of higher computational complexity.

In Fig. 4.12, we present the impact of different PT lengths (N_p) on sensing accuracy. We see from this figure that the length of PT can greatly affect the sensing performance of our proposed PT method in both two cases. For instance, as N_p increases, a smaller P_m, i.e., better sensing performance, can be achieved. Take Case A as an instance, P_m decreases from 0.156 to 0.004 with increasing N_p from 8 to 32. However, it is worth noting that a larger N_p leads to higher computational complexity.

4.6 Conclusion

In this chapter, we investigated the spectrum sensing under the imperfect self-interference in the cognitive full-duplex systems. To study the spectrum sensing technique in full-duplex systems with timing delay and self-interference, we proposed a novel spectrum sensing approach with the help of the CP feature of OFDM signals. To investigate the OFDM spectrum sensing in full-duplex systems in the presence of self-interference and CFO, we proposed a novel OFDM sensing method by lever-

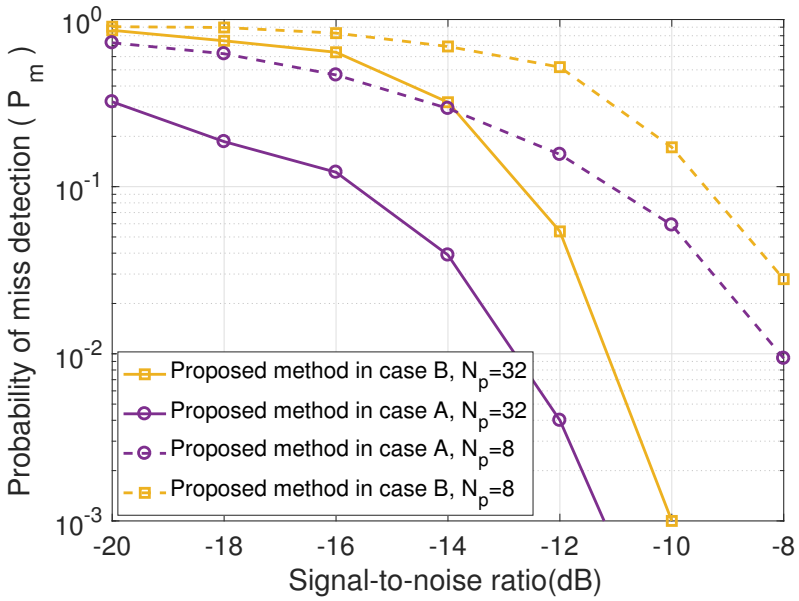


Figure 4.12: Probability of miss detection (P_m) of the proposed method with different PT lengths (N_p).

aging the PT feature of OFDM signals. Two different types of self-interference signals (with or without a PT structure) are taken into account when analyzing the sensing performance of the proposed methods. We obtained the closed-form expressions of the probability of miss detection and false alarm of the presented approaches. Extensive simulation results demonstrated our proposed CP approach obtains better performance than conventional CP based spectrum sensing methods in the FD system even with self-interference and timing delay. Besides, our proposed PT sensing method is more robust to the residual self-interference and CFO than the conventional ones. Additionally, the proposed PT method can achieve better sensing performance under the low SNR condition with much lower computational complexity.

Chapter 5

Privacy Preservation for Spectrum Access System

In addition to the sensing-based DSA, the data-based DSA has also been gaining its popular adoption as a potential solution to improve spectrum utilization in future wireless systems. To effectively realize the data-based DSA, users are required to share their operational data, which risks exposing their privacy and business plans to unintended agents. In this chapter, we propose a novel scheme to protect the private information of IUs and honest/dishonest SUs from being revealed. The proposed scheme aims to fully preserve users' operational data and successfully guarantee efficient spectrum utilization.

5.1 Introduction

Protecting users' operating information is the core to successfully facilitate the data-based DSAs. For that purpose, a large number of methods have been proposed, e.g., obfuscation methods [88–90], anonymity methods [91, 92] and encryption methods [93, 94]. Although the existing work is able to protect users' operational privacy to a certain degree, they still face several challenging problems, e.g., protecting users' precise information but exposing the rough locations/directions [88–90, 92] and greatly high complexity [93, 94]. Another serious problem is that most of the existing methods only investigate the privacy issue of honest users but fail to consider

the case of dishonest users, which is however not really realistic [95].

Given the above, this chapter aims to provide practical methods to protect the operational information of IUs and honest/dishonest SUs in data-based DSA, with the special focus on the U.S. (i.e., Spectrum Access System, SAS). It is important to note that, in this chapter, we don't study the resource allocation but focus on realizing the results of any resource allocation/auctioning frameworks (e.g., [117–119]) while protecting users' operational data (e.g., location, antenna heights) under SAS architectures. Main contributions of this chapter are summarized below:

- For IUs and honest SUs, we first propose a privacy-preserving scheme by leveraging encryption and obfuscation methods (PSEO) to protect all users' privacy. In PSEO, all operations are conducted with users' encrypted or obfuscated data. As a result, the user's actual operating information is only accessible to itself, whereas other users or adversaries are not able to obtain or infer any relevant information. Moreover, PSEO is capable of successfully guaranteeing efficient spectrum utilization while preserving users' privacy.

- Besides protecting users' information, we propose a blind interference calculation scheme (BICS), the core of PSEO, to calculate the interference budget without revealing their operational information. In comparison with the FCC's SAS, BICS moves interference budgeting tasks to local users and calculates it in an offline manner (i.e., before the spectrum requesting stage). That calculated result is later reused in all future spectrum requests, which dramatically reduces the online computing overhead of PSEO.

- For dishonest SUs, we augment a "punishment and forgiveness" mechanism into PSEO (namely PF-PSEO) to prevent dishonest SUs from using other users' information. Moreover, we account for SUs' reputation scores (RSs) and reputation history (RHs) [120] to evaluate SUs' behaviors, which encourage SUs to engage in honest activities.

- Unlike the traditional obfuscation methods, the obfuscations in our proposed PSEO and PF-PSEO do not degrade the spectrum utilization. Besides, we

consider four kinds of threat scenarios and tackle them using our proposed schemes. We provide the theoretical analysis to analyze the performance of PESO and PF-PSEO from various aspects.

The rest of this chapter is organized as follows. Section 5.2 introduces the system model and problem formulation. In Section 5.3, we propose PSEO to protect the privacy of IUs and honest SUs. In Section 5.4, PF-PSEO is presented to preserve the private data of IUs and dishonest SUs. Section 5.5 provides the quantization of attenuation map and other discussions. The performance analysis of PSEO and PF-PSEO are expressed in Section 5.6. We demonstrate the simulation results in Section 5.7, followed by the conclusion in Section 5.8

5.2 System Model and Problem Formulation

In this section, we first describe the system model of spectrum sharing in the SAS architecture. The four different privacy threats are then introduced, followed by the overview of the Paillier Cryptosystem.

5.2.1 Spectrum Sharing in SAS Architecture

We study the spectrum sharing in the protection zone of SAS, in which the spectrum management consists of four entities: the SAS administrator and three kinds of users (IUs, PALs, and GAAs) [121], as shown in Fig. 5.1. The SAS administrator is the database/server which is used to collect all relevant information and provide reliable spectrum access for SUs. IUs, which are the agencies of defense (e.g., military radars), hold the highest priorities regarding spectrum access and interference protection, while GAAs have the lowest rights. PALs and GAAs, which are categorized as SUs, are usually from industry. According to FCC proposals (refer to Subpart A-96.3 in [121]), SUs are fixed stations or networks of such stations that transmit and receive radio communication signals at a fixed location. They may be moved from time to time but they must turn off and re-send a report to the SAS administrator prior to transmitting from a new location [121]. As such, we assume SUs are semi-stationary, i.e., they are stationary during the spectrum request and

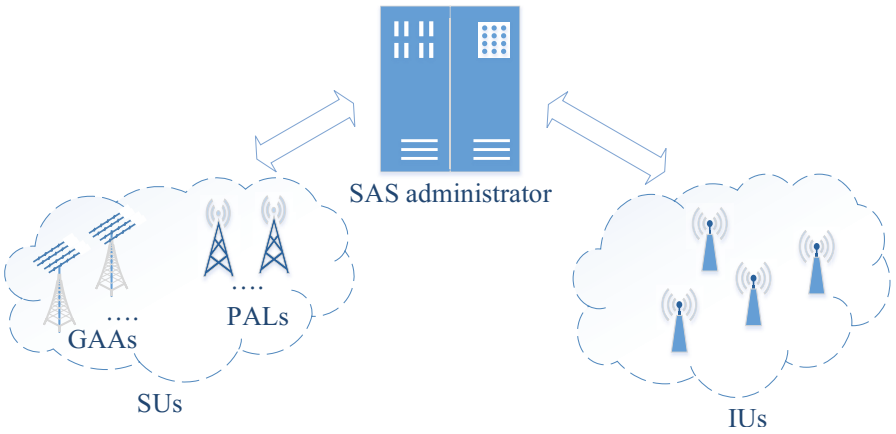


Figure 5.1: Spectrum sharing in a SAS architecture.

spectrum leasing terms. The SAS administrator allocates a spectrum chunk to a user based on the operational information provided by users. For that, the SAS administrator processes multiple SUs' requests (with grant or reject decisions) in a sequential manner.

The process of spectrum sharing between IU i and SU g in a SAS Architecture is summarized as follows [89].

1) In order to get the access of IU i's spectrum band, SU g is required to send its operational information to the SAS administrator, which includes its location (x_g, y_g), operating frequency f_g, antenna height h_g, etc.

2) IU i, for its interference protection, sends its operational data (including its location (x_i', y_i'), operating frequency f_i', antenna height h_i', and interference threshold X_i) to the SAS administrator to update its spectrum usage.

3) The SAS administrator first calculates the attenuation map of SAS architecture $\mathbf{A}'$ using terrestrial propagation models [122]. $\mathbf{A}'$ specifies the attenuation between any two points in the area. The attenuation map is a function of location, antenna height, and operating frequency, etc.

$$\mathbf{A}' := \{A'\ (x_1, x_2, y_1, y_2, h_1, h_2, f_1, f_2)\}, \tag{5.1}$$

where (x_1, y_1), h_1, and f_1 denote the first point's location, antenna height and operating frequency, respectively. (x_2, y_2), h_2, and f_2 are the second point's location, antenna height and operating frequency, respectively.

Based on the received operational information from IU i and SU g, the SAS

administrator calculates the interference from SU g to IU i:

$$G_g := P_g - \mathbf{A}' \ (x_g, x_i', y_g, y_i', h_g, h_i', f_g, f_i'), \tag{5.2}$$

where P_g is the transmitting power of SU g. Next, the SAS administrator compares G_g with IU's interference threshold X_i and decides whether to approve SU g's request or not.

4) The SAS administrator sends a reply to SU g, which includes a response to SU g's request. If SU g gets an approval response, it can use IU i's spectrum band for data communication. Otherwise, SU g is not allowed to access IU i's spectrum.

As the SAS administrator receives and stores operational information from both the IU and SU, serious threats to user's privacy and interest are of concern. Notably, some IUs (e.g., military radars) in FCC's SAS are even forbidden to share any operational information with the SAS administrator [121]. For that case, the SAS administrator receives IUs' operational information or activity from the Environmental Sensing Capability (ESC). However, ESC is not protected at the level of IUs, hence it is still vulnerable to attacks, which would leak the IU's operational information. Therefore, the privacy threat always exists whether IUs communicate directly with the SAS administrator or not.

5.2.2 Privacy Threats

We consider four types of threat that would compromise the user's operational privacy.

1) Privacy threats occurring at IU i's side

IU i's information is eavesdropped through the communication link between the SAS administrator and IU i, which is the 2nd step shown in Fig. 5.2.

2) Privacy threats occurring at SU g's side

SU g's private information is compromised by eavesdroppers from communication links between the SAS administrator and SU g (e.g., the 1st and the 4th steps in Fig.5.2).

3) Privacy threats occurring at SAS administrator's side

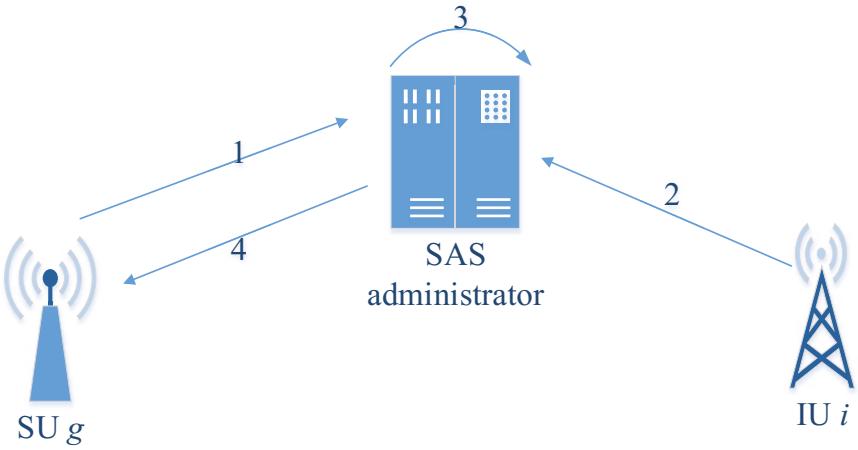


Figure 5.2: Process of spectrum sharing between IU i and SU g in SAS architecture.

The SAS administrator can be attacked by adversaries and hence expose IU's and/or SU's operational information (e.g., the 3rd step in Fig.5.2), which brings risks on the operational privacy of IU i and/or SU g. It is also possible for the SAS administrator to steal/reveal IU i's and/or SU g's operational data. For example, the SAS administrator could be operated by commercial parties (e.g., Google) [123]. For this kind of SAS administrator, it can faithfully execute the proposed spectrum allocation; however, it may attempt to access users' operational data for its own interest.

4) Collusion attack between SAS administrator and rogue SUs

As the SAS administrator can be owned and operated by a third party, there is a chance for them to be compromised (as high-value targets for attackers). In such a case, the SAS administrator can collude with a rogue SU to reveal the IU's actual operational data. Another possibility is that an adversary attacks/eavesdrops both the SAS administrator and the SU to obtain information from both sides to infer the actual operational data of IUs. These two threats are referred to as a Collusion attack in this chapter.

In the sequel, we present our proposed privacy-preserving schemes for DSA, which leverage properties of public key cryptosystem and obfuscation methods. According to the public key cryptosystem, any one that holds additive homomorphic properties (details in Section 5.2.3) can be applicable to our proposed schemes. In this chapter, we adopt the Paillier cryptosystem [124].

5.2.3 Overview of Paillier Cryptosystem

The Paillier encryption cryptosystem consists of three main parts: key generation, encryption, and decryption [124].

Key Generation

p and q are two large prime numbers which are randomly selected, as long as they follow the condition that

$$\gcd\big(pq\ (p-1)(q-1)\big) = 1. \tag{5.3}$$

Compute n and λ by

$$n = pq, \tag{5.4}$$

$$\lambda = \mathrm{lcm}(p-1, q-1). \tag{5.5}$$

Then compute u using n and λ,

$$u = \big(L(z^{\lambda} \bmod n^2)\big)^{-1} \bmod n, \tag{5.6}$$

where z is a integer number that is randomly selected, $z \in \mathbf{Z}^*_{n^2}$, $L(u)=(u-1)/u$.

The public key (for encryption) K_P is (n, z).

The secret key (for decryption) K_S is (λ, u).

Encryption

Let m be the plaintext that needs to be encrypted, and $E_P(m)$ denote the ciphertext (encrypted from m) with the public key K_P. $E_P(m)$, is calculated by

$$E_P(m) = z^m \cdot r^n \bmod n^2, \tag{5.7}$$

where r is a one-time random number. With the help of r, the same m with the same public key K_P would result in different ciphertexts for each encryption process.

Decryption

The plaintext m can be obtained from $E_P(m)$ by

$$m = L\big[\big([E_P(m)]^{\lambda} \bmod n^2\big) \cdot u\big] \bmod n. \tag{5.8}$$

From the above steps, obviously, it is impossible to decrypt the ciphertext $E_P(m)$ without the corresponding secret key K_S. Moreover, r can make a difference in the process of Encryption, whereas it does not affect the Decryption process (refer to equation (5.7) and (5.8)). In other words, for each encryption process, one plaintext can be encrypted to different ciphertexts using the same public key as a result of r. However, one ciphertext can only be decrypted to one plaintext with the same secret key.

Additive Homomorphic Properties

The additive homomorphic properties of the Paillier cryptosystem allow one to execute additive operations (e.g., addition, subtraction and scalar multiplication operations) on the ciphertexts, i.e., without decrypting them. In our design, this homomorphic feature enables the interference budgeting calculation on the ciphertext. The additive homomorphic properties are as follows.

Let $E_P(m_1)$ and $E_P(m_2)$ are ciphertexts of m_1 and m_2, respectively. The ciphertext of $(m_1 + m_2)$ then can be calculated as:

$$E_P(m_1 + m_2) = E_P(m_1) \cdot E_P(m_2). \tag{5.9}$$

For a constant c_1, the ciphertext of $c_1 \cdot m_1$ is:

$$E_P(c_1 \cdot m_1) = \big[E_P(m_1)\big]^{c_1}. \tag{5.10}$$

The ciphertext of $m_1 - m_2$ can be also directly computed from $E_P(m_1)$ and $E_P(m_2)$

$$E_P(m_1 - m_2) = E_P(m_1) \cdot [E_P(m_2)]^{-1}. \tag{5.11}$$

Note that the Paillier cryptosystem is only suitable for the non-negative integer numbers. As such, we map all non-integer numbers by rounding them up to three

digits after the decimal and multiplying all data with 10^3 before the encryption. Note that, rounding up to more digits (e.g., 8 digits) can result in slightly smaller decision error ratio than 3 digits, while it causes more computational complexity. Additionally, under our setting and interference calculation below, $m_1 - m_2$ is the only possible operation which may result in a negative number. To deal with this, we adopt the additive property of Paillier cryptosystem, which is

$$\begin{aligned} E_P(m_3) &= E_P(c_2 + m_1 - m_2) \\ &= E_P(c_2) \cdot E_P(m_1) \cdot [E_P(m_2)]^{-1}, \end{aligned} \tag{5.12}$$

where c_2 is a positive integer and $0 \leq m_2 < c_2$. $E_P(c_2)$ is the cipertext of c_2 with the public key K_P. When m_3 is obtained from the decryption operation, $m_1 - m_2$ can be easily obtained by $m_3 - c_2$.

5.3 Privacy-preserving Scheme using Encryption and Obfuscation Methods

In this section, we first present the overview of PSEO. Then we discuss the details of BICS that is the core of PSEO.

5.3.1 Overview of PSEO

PSEO is made up of 10 steps, as shown in Fig. 5.3, in which (K_{IP}, K_{IS}) and (K_{SP}, K_{SS}) are key pairs of IU i and SU g, respectively. K_{IP} and K_{SP} are public keys, which are used to encrypt original data into the encrypted domain. Moreover, these public keys are distributed to each part of the system. K_{IS}, the secret key of IU i, can decrypt the data encrypted with the public key K_{IP}. K_{SS}, the secret key of SU g, is used to decrypt the data encrypted with the public key K_{SP}. These secret keys K_{IS} and K_{SS} are confidential information and only held by IU i and SU g, respectively.

Notably, in PSEO, IU i and SU g keep their own secret keys by themselves and do not require a third party to manage the key distribution. That makes PSEO

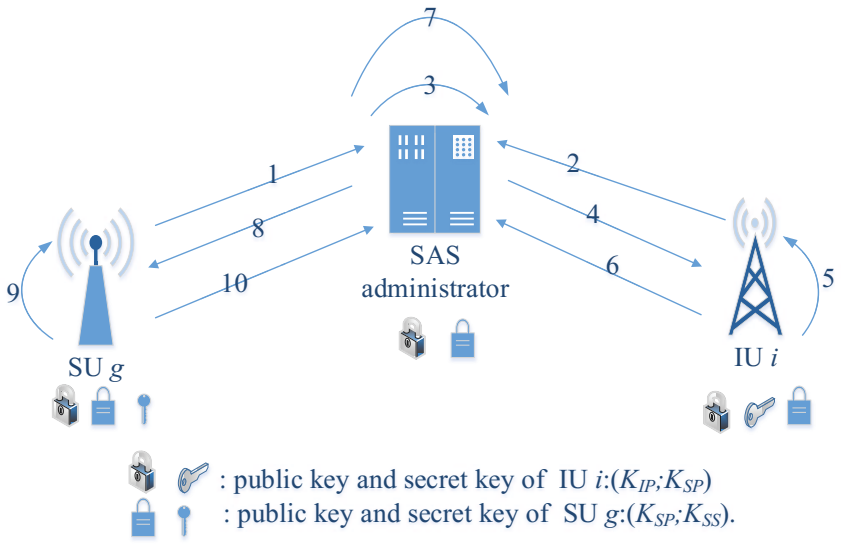


Figure 5.3: Key steps of proposed PSEO.

much more practical than the privacy-preserving schemes using public cryptosystems which require the third party for key management (such as P^2-SAS scheme in [94]). Moreover, drawing support from obfuscation methods [92], our scheme is able to prevent IUs' information from being inferred, even if there is a collusion between the SAS administrator and SUs (refer to 6th step in section 5.3.3). In addition, the obfuscation methods can also protect SU g's privacy from being revealed, even if IU i can decrypt the SU g's ciphertext that is encrypted with IU i's public key (refer to 3rd and 4th steps in section 5.3.3).

BICS is the core of PSEO that allows the interference budgeting to be calculated locally at SUs while no specific information of IUs is required. Additionally, it reduces the online overhead and facilitates the homomorphic operations at the SAS administrator without requiring IUs or SUs to share/send their operational information (i.e., referred to as the blind interference calculation method).

5.3.2 Blind Interference Calculation Scheme

In the SAS framework, the interference from SU g to IU i is calculated by the SAS administrator with operational information from both IUs and SUs. That increases the online overhead (referring to the computational complexity during the spectrum requesting stage) and risks leaking users' actual operational information.

By contrast, in BICS, the interference from SU g to IU i is calculated at SU g's side instead of SAS administrator's side, bringing two major associated advantages. First, the online overhead of proposed PSEO is significantly reduced, as the interference calculation is now conducted offline before the spectrum requesting stage, which does not occupy the resource or time in the spectrum requesting stage. Second, SU g calculates the interference with its operational data only, without any information from IU i. That prevents IU i and SU g from leaking their operational information (through sharing it with each other or with the third party).

In BICS, the SAS administrator sends the attenuation map of SAS $\mathbf{A}'$ to all users before the process of spectrum request. To reduce the complexity, we introduce a quantization method to quantize $\mathbf{A}'$. We consider a service area $X \times Y$. H is the maximum value of antenna height. F_{max} and F_{min} are the maximum and minimum value of operating spectrum, respectively. $F = F_{max} - F_{min}$ is the spectrum bandwidth in SAS. Then we quantize X, Y, F, and H into equal-size X_q, Y_q, F_q, and H_q grids, respectively, obtaining a quantized attenuation map $\mathbf{A}$ (refer to Section 5.5.1 for more details).

The quantized attenuation map $\mathbf{A}$ which is an eight-dimensional matrix can be represented by

$$\begin{aligned}\mathbf{A} &\coloneqq \{\mathbf{A}'\}_{X_q^2 \times Y_q^2 \times H_q^2 \times F_q^2} \\ &= \big\{A(x_1, x_2, y_1, y_2, h_1, h_2, f_1, f_2)\big\}_{X_q^2 \times Y_q^2 \times H_q^2 \times F_q^2}. \end{aligned} \tag{5.13}$$

Upon receiving $\mathbf{A}$ from the SAS administrator, SU g determines its location in $\mathbf{A}$ and obtains its eight-dimensional attenuation map $\mathbf{A}_g$, which is

$$\begin{aligned}\mathbf{A}_g &\coloneqq \mathbf{A}(x_g, :, y_g, :, h_g, :, f_g, :) \\ &= \big\{A(x_g, x_2, y_g, y_2, h_g, h_2, f_g, f_2)\big\}_{X_q^2 \times Y_q^2 \times H_q^2 \times F_q^2}, \end{aligned} \tag{5.14}$$

where x_g, y_g, h_g, and f_g are operational parameters of SU g. (x_2, y_2, h_2, f_2) is the operational data of a *potential* IU that happens to be at location (x_2, y_2) with antenna height h_2 and operating frequency f_2. Note that the potential IU does not necessary mean the existence of a real/physical IU. For that, the operational information of the IU is protected (not being shared).

SU g then calculates the interference caused by itself to the potential IU i. Since SU g is prohibited from accessing any IU's operational information, it assumes IU i would be located in any grid in $\mathbf{A}_g$. The interference map of SU g is calculated by

$$\begin{aligned}\mathbf{G}_g :&= \left\{G\ (x_g, :, y_g, :, h_g, :, f_g, :)\right\}_{X_q^2 \times Y_q^2 \times H_q^2 \times F_q^2} \\ &= P_g - \mathbf{A}_g \\ &= P_g - \mathbf{A}(x_g, :, y_g, :, h_g, :, f_g, :),\end{aligned} \tag{5.15}$$

where P_g is the transmitting power of SU g.

BICS is capable of preserving the operational privacy of all users. This is because under BICS, each SU does not need to know the operational information of any IU (e.g., IU's physical locations). Instead, the SU assumes that an IU can be located in any grid. Then the interference from the SU to the IU (any grid) is completed at the SU's side before the spectrum requesting stage, only using the SU's operational information. In other words, only the SU is involved in the process of the interference calculation using its own operational information, without any participation from other parties, e.g., IUs or the SAS administrator. Therefore, neither the IU nor SU have to share their operational information. The BICS can thus protect users' operational privacy.

5.3.3 Details of PSEO

The main steps of PSEO are presented as follows.

1) In order to apply IU i's spectrum bands, SU g first encrypts its interference map $\mathbf{G}_g$ (which is calculated through the above BICS) with the IU i's public key K_{IP} and obtains the ciphertext $E_{K_{IP}}\left[\mathbf{G}_g\right]$, which is

$$\mathbf{G}_g \xrightarrow[encryption]{K_{IP}} E_{K_{IP}}\left[\mathbf{G}_g\right], \tag{5.16}$$

where *encryption* denotes the encryption process discussed in Section 5.2.3. SU g then sends $E_{K_{IP}}\left[\mathbf{G}_g\right]$ to the SAS administrator.

2) IU i determines the interference threshold map based on its operational information. If the operational information of IU i is (x_i', y_i', h_i', f_i'), the corresponding

quantized interference threshold map is

$$\begin{aligned}\mathbf{X}_i &\coloneqq \left\{X\ (:, x_i', :, y_i', :, h_i', :, f_i')\right\}_{X_q^2 \times Y_q^2 \times H_q^2 \times F_q^2} \\ &= \left\{X\ (x_1, x_i', y_1, y_i', h_1, h_i', f_1, f_i')\right\}_{X_q^2 \times Y_q^2 \times H_q^2 \times F_q^2},\end{aligned} \tag{5.17}$$

where (x_1, y_1, h_1, f_1) is the operational data of a *potential* SU. Notably, if there are more than one IU's threshold values in one grid, the smallest value should be selected as the new threshold for that gird. IU i encrypts $\mathbf{X}_i$ using its public key K_{IP} and obtains $E_{K_{IP}}\left[\mathbf{X}_i\right]$ by

$$\mathbf{X}_i \xrightarrow[encryption]{K_{IP}} E_{K_{IP}}\left[\mathbf{X}_i\right]. \tag{5.18}$$

Upon obtaining $E_{K_{IP}}\left[\mathbf{X}_i\right]$, IU i sends $E_{K_{IP}}\left[\mathbf{X}_i\right]$ to the SAS administrator to update its spectrum usage.

3) The SAS administrator compares $E_{K_{IP}}\left[\mathbf{X}_i\right]$ and $E_{K_{IP}}\left[\mathbf{G}_g\right]$ without decrypting them, by

$$\begin{aligned}E_{K_{IP}}\left[\mathbf{B}_g\right] &= E_{K_{IP}}\left[\mathbf{C} + \mathbf{X}_i - \mathbf{G}_g\right] \\ &= E_{K_{IP}}[\mathbf{C}] \cdot E_{K_{IP}}\left[\mathbf{X}_i\right] \cdot \left[E_{K_{IP}}\left[\mathbf{G}_g\right]\right]^{-1},\end{aligned} \tag{5.19}$$

where $E_{K_{IP}}\left[\mathbf{B}_g\right]$ is the interference budget in the ciphertext domain. $E_{K_{IP}}\left[\mathbf{C}\right]$ is the ciphertext of $\mathbf{C}$ with the public key K_{IP}. $\mathbf{C}$ is a positive integer matrix, which has the same dimensions with $\mathbf{X}_i$. As mentioned above, $\mathbf{C}$ is used to ensure that $\mathbf{B}_g$ is a positive integer matrix, which guarantees $E_{K_{IP}}\left[\mathbf{B}_g\right]$ is valid. Notably, $\mathbf{C}$ is randomly generated and kept by the SAS administrator only.

4) Since IU i is the only part that holds the secret key K_{IS}, the SAS administrator sends $E_{K_{IP}}\left[\mathbf{B}_g\right]$ to IU i to obtain the decrypted value of $E_{K_{IP}}\left[\mathbf{B}_g\right]$. However, this process would risk the operational information of SU g being exposed to IU i, which is contrary to the goal of PSEO. In order to solve this problem, we recruit the following obfuscation methods before sending $E_{K_{IP}}\left[\mathbf{B}_g\right]$ to IU i:

$$\begin{aligned}E_{K_{IP}}\left[\mathbf{B}_g'\right] &= E_{K_{IP}}\left[c_3 \cdot \mathbf{B}_g\right] \\ &= \left[E_{K_{IP}}\left[\mathbf{B}_g\right]\right]^{c_3},\end{aligned} \tag{5.20}$$

and

$$E_{K_{IP}}\left[\mathbf{C}^{'}\right] = E_{K_{IP}}\left[c_3 \cdot \mathbf{C}\right] = \left[E_{K_{IP}}\left[\mathbf{C}\right]\right]^{c_3}, \tag{5.21}$$

where c_3 is a positive integer generated by the SAS administrator randomly. Notably, c_3 does not degrade the spectrum utilization, which will be discussed in Section 5.5.3. After obtaining $E_{K_{IP}}\left[\mathbf{C}^{'}\right]$ and $E_{K_{IP}}\left[\mathbf{B}_g^{'}\right]$, the SAS administrator sends them to IU i to be decrypted.

5) IU i decrypts $E_{K_{IP}}\left[\mathbf{B}_g^{'}\right]$ and $E_{K_{IP}}\left[\mathbf{C}^{'}\right]$ with the secret key K_{IS}, by

$$E_{K_{IP}}\left[\mathbf{B}_g^{'}\right] \xrightarrow[decryption]{K_{IS}} \mathbf{B}_g^{'}, \tag{5.22}$$

$$E_{K_{IP}}\left[\mathbf{C}^{'}\right] \xrightarrow[decryption]{K_{IS}} \mathbf{C}^{'}, \tag{5.23}$$

where *decryption* denotes the decryption process discussed in Section 5.2.3. Then IU i obtains the interference calculation result $\mathbf{R}_g'$ by $\mathbf{R}_g' = \mathbf{B}_g^{'} - \mathbf{C}^{'}$, which is an eight-dimensional matrix. IU i compares the value of each grid in $\mathbf{R}_g'$ with 0. If all numbers in $\mathbf{R}_g'$ are positive, which means the interference caused by SU g is lower than IU i's interference threshold, IU i generates a decision 'YES'. Otherwise, IU i generates a decision 'NO'.

6) In order to preserve its operational privacy, IU i obfuscates $\mathbf{R}_g'$ by

$$\mathbf{R}_g = c_4 \cdot \mathbf{R}_g^{'}, \tag{5.24}$$

where c_4 is a positive integer which is randomly generated by IU i. Note that, like c_3, thanks to our design, c_4 doesn't impact the spectrum utilization (refer to Section 5.5.3). Then IU i encrypts $\mathbf{R}_g$ with SU g's public key K_{SP} by

$$\mathbf{R}_g \xrightarrow[encryption]{K_{SP}} E_{K_{SP}}\left[\mathbf{R}_g\right]. \tag{5.25}$$

IU i sends $E_{K_{SP}}\left[\mathbf{R}_g\right]$ and decision 'YES/NO' to the SAS administrator.

7) The SAS administrator updates interference threshold budget $E_{K_{IP}}\left[\mathbf{X}_i\right]$ based on 'YES/NO'. If the SAS administrator receives 'NO', it will reject SU g's request

and not update $E_{K_{IP}}[\mathbf{X}_i]$. Otherwise, it will approve SU g's request and update $E_{K_{IP}}[\mathbf{X}_i]$ by

$$E_{K_{IP}}[\mathbf{X}_i] \longleftarrow E_{K_{IP}}[\mathbf{B}_g]. \tag{5.26}$$

8) The SAS administrator generates a signature D_g that includes the request decision and encrypts it with the public key of SU g, which is denoted as $E_{K_{SP}}[D_g]$. The SAS administrator sends $E_{K_{SP}}[\mathbf{R}_g]$ and $E_{K_{SP}}[D_g]$ to SU g.

9) SU g decrypts $E_{K_{SP}}[\mathbf{R}_g]$ and $E_{K_{SP}}[D_g]$ using its K_{SS} by

$$E_{K_{SP}}[D_g] \xrightarrow[decryption]{K_{SS}} D_g, \tag{5.27}$$

$$E_{K_{SP}}[\mathbf{R}_g] \xrightarrow[decryption]{K_{SS}} \mathbf{R}_g. \tag{5.28}$$

D_g is used to inform the request decision to SU g. Moreover, since it is generated using some digital signature techniques, it can identify SU g's identity and prevent the spoofing attack. $\mathbf{R}_g$ is used to guarantee the validity of the decision D_g (to SU g's request). This can be seen as a second layer of protection (e.g., Cyclic Redundancy Check, CRC, and checksum) for the message D_g from any kind of attack that may corrupt/flip the "YES" or "NO" decision in D_g. Specifically, D_g is regarded as a valid decision if all the numbers in $\mathbf{R}_g$ are positive and D_g is 'YES' or at least one number in $\mathbf{R}_g$ is non-positive and D_g is 'NO'. For all the other cases, the request decision is marked as invalid, and SU g will report it to the SAS administrator. Moreover, $\mathbf{R}_g$ (achieved from equation (5.24)) is the obfuscated interference calculation result that does not reveal the user's actual operational data, so SU g cannot infer the IU i's actual operational information with $\mathbf{R}_g$.

10) SU g sends a confirmation message to the SAS administrator to confirm its received response. If the value of each grid in $\mathbf{R}_g$ is positive and the request is approved by the SAS administrator, SU g will generate a positive confirmation message V_{gp}. Otherwise, SU g will generate a negative confirmation message V_{gn}. Then SU g sends back V_{gp} or V_{gn} to the SAS administrator to verify its received decision. If the SAS administrator receives V_{gp}, it will complete the request stage of SU g and turn to another SU's request. Otherwise, the SAS administrator will re-process the request from this SU.

Summary 1: Key Steps of PSEO

1 SU g:	sends $E_{K_{IP}}[\mathbf{G}_g]$ to SAS admin.
	$\mathbf{G}_g \xrightarrow[encry]{K_{IP}} E_{K_{IP}}[\mathbf{G}_g]$
2 IU i:	sends $E_{K_{IP}}[\mathbf{X}_i]$ to SAS admin.
	$\mathbf{X}_i \xrightarrow[encry]{K_{IP}} E_{K_{IP}}[\mathbf{X}_i]$
3 SAS admin:	calculates $E_{K_{IP}}[\mathbf{B}_g]$.
	$E_{K_{IP}}[\mathbf{B}_g] = E_{K_{IP}}[\mathbf{C} + \mathbf{X}_i - \mathbf{G}_g]$
4 SAS admin:	sends $E_{K_{IP}}[\mathbf{B}_g^{'}]$ and $E_{K_{IP}}[\mathbf{C}^{'}]$ to IU i
	$E_{K_{IP}}[\mathbf{B}_g^{'}] = \left[E_{K_{IP}}[\mathbf{B}_g]\right]^{c_3}$, $E_{K_{IP}}[\mathbf{C}^{'}] = \left[E_{K_{IP}}[\mathbf{C}]\right]^{c_3}$
5 IU i:	calculates $\mathbf{R}_g^{\prime}$.
	$E_{K_{IP}}[\mathbf{B}_g^{'}] \xrightarrow[decry]{K_{IS}} \mathbf{B}_g^{'}$, $E_{K_{IP}}[\mathbf{C}_g^{'}] \xrightarrow[decry]{K_{IS}} \mathbf{C}_g^{'}$
	$\mathbf{R}_g^{\prime} = \mathbf{B}_g^{'} - \mathbf{C}_g^{'}$
	determines the property of all numbers in $\mathbf{R}_g^{\prime}$
	if all numbers are positive
	generates "YES"
	else
	generates "NO"
	end
6 IU i:	sends "YES/NO" and $E_{K_{SP}}[\mathbf{R}_g]$ to SAS admin
	$\mathbf{R}_g = c_4 \cdot \mathbf{R}_g^{'}$, $\mathbf{R}_g \xrightarrow[encry]{K_{SP}} E_{K_{SP}}[\mathbf{R}_g]$
7 SAS admin:	updates $E_{K_{IP}}[\mathbf{X}_i]$
	if receives "YES"
	approve SU g's request and
	update $E_{K_{IP}}[\mathbf{X}_i]$ by $E_{K_{IP}}[\mathbf{B}_g]$
	else
	reject SU g's request and
	do not update $E_{K_{IP}}[\mathbf{X}_i]$
	end
8 SAS admin:	sends $E_{K_{SP}}[\mathbf{R}_g]$ and $E_{K_{SP}}[D_g]$ to SU g
	$D_g \xrightarrow[encry]{K_{SP}} E_{K_{SP}}[D_g]$
9 SU g:	verifies $\mathbf{R}_g$ and D_g
	$E_{K_{SP}}[\mathbf{R}_g] \xrightarrow[decry]{K_{SS}} \mathbf{R}_g$, $E_{K_{SP}}[D_g] \xrightarrow[decry]{K_{SS}} D_g$
10 SU g:	sends a confirmation message to SAS admin.

Based on all the steps described above, users' actual information is only kept by themselves through the whole process of PSEO, hence, their operational privacy can be protected. The summary of key steps for PSEO is listed in **Summary 1**, in which "SAS admin" denotes the SAS administrator.

5.4 Dealing with Dishonest SUs: Punishment and Forgiveness Mechanism

In this section, we investigate the operational privacy issue of IUs and dishonest SUs. Since IUs are usually the agents of defense (e.g., military radars), it is quite reasonable to assume that they are trustworthy. By contrast, SUs, which are commercial organizations may behave dishonestly/greedily for their own benefit. As noted in Section 5.1, existing privacy-preserving schemes are proposed mainly relying on the assumption of honest SUs, hence, their performance would be dramatically degraded, suffering from dishonest SUs.

To deal with greedy/dishonest SUs, we propose the "punishment and forgiveness" cooperating with PSEO, namely PF-PSEO, which is able to effectively deal with two types of dishonest SUs: the SUs who provide an invalid identity number (IDN) and the SUs who provide a valid IDN but proceed to report lower transmit power values than they actually plan to use, referred to as greedy SUs. For the first type of SUs, PF-PSEO can detect their dishonest behaviors utilizing our proposed "Authentication of SU" and ask them to send valid IDNs. For the second type of SUs, i.e., the greedy SUs, PF-PSEO can punish them (when they are found to be dishonest) using our "Punishment and Forgiveness (PF)" scheme and hence consequently encourage them to comply with what they report.

The objective of PF in PF-PSEO is to punish the greedy SUs by rejecting their requests, which reduces their spectrum access opportunities. However, PF also forgives greedy SUs who received the punishment (i.e., they were rejected previously) by giving them spectrum access opportunities during the future requests. It is worth noting that after a finite times of being dishonest (i.e., a threshold), the greedy SUs' requests will never be granted even if they behave honestly. In other

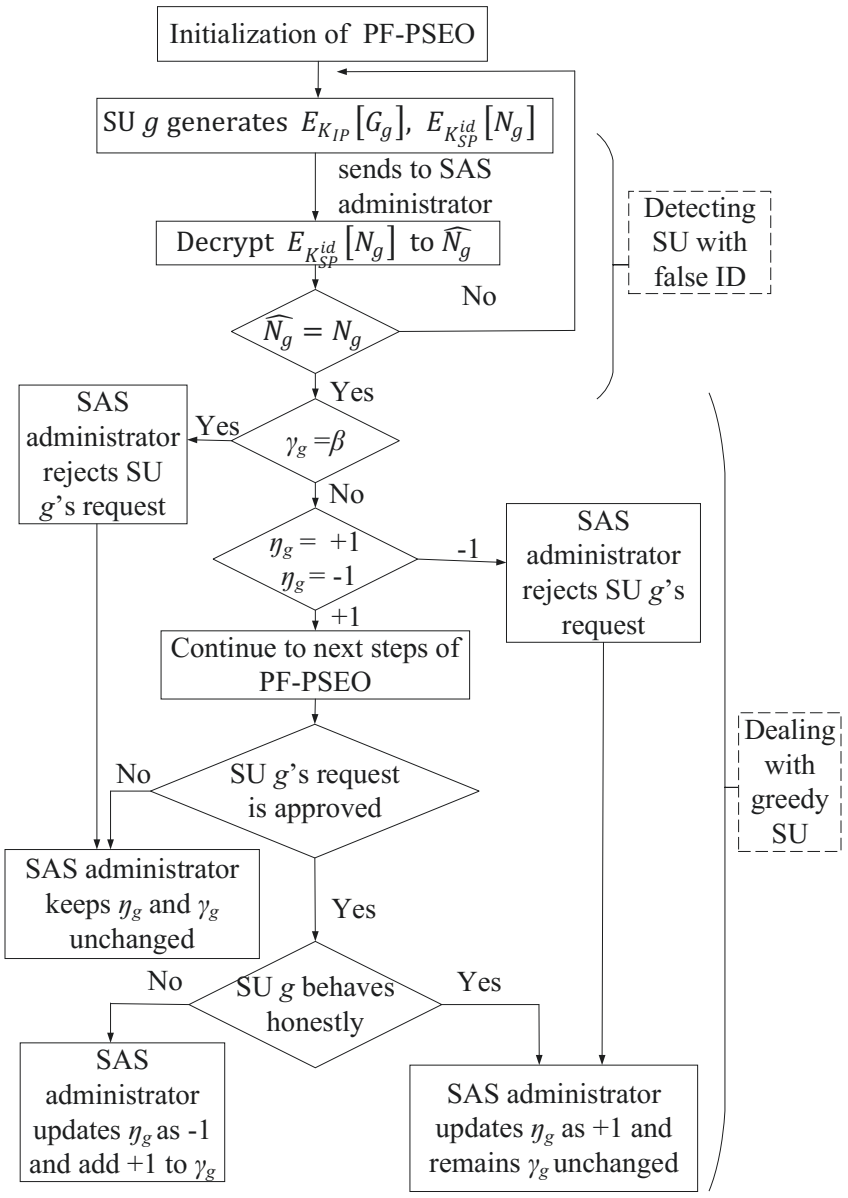


Figure 5.4: Dealing with greedy/dishonest SUs in PF-PSEO.

words, our proposed framework only tolerates a given number of dishonest times. All greedy SUs that exceed this threshold will be banned forever from accessing the spectrum from SAS. That helps eliminate greedy/dishonest SUs/behaviors and "softly" enforce SUs to report the true information and behave in accordance with their reported/request information (to be able to access shared spectrum). In the following section, we will specifically illustrate how PF-PSEO can effectively deal with the two types of dishonest SUs, as shown in Fig. 5.4. .

5.4.1 Initialization of PF-PSEO

In order to implement PF-PSEO, the SAS administrator first generates each SU's identity number (IDN) and the IDN key pair (i.e., the IDN public key and the IDN secret key). The IDN key pair is used to verify the SU's IDN to prevent the SU from using other users' IDNs. The SAS administrator distributes the IDN and the IDN public key to the corresponding SU, and keeps the IDN secret key to itself. Note that the IDN is a positive integer for the purpose of encryption. For each SU, it can only access its own IDN and IDN public key. Let N_g denote the SU g's IDN, and $(K_{SP}^{id}, K_{SS}^{id})$ denote its IDN key pair, where K_{SP}^{id} is the IDN public key of SU g, K_{SS}^{id} is the corresponding IDN secret key (kept by the SAS administrator only).

5.4.2 Authentication of SU: Detecting SUs with False ID

In this subsection, we develop an authentication scheme to prevent SUs from sending other users' IDNs during spectrum requesting periods. The SU g's spectrum request sent to the SAS administrator consists of three parts: its own IDN N_g, $E_{K_{SP}^{id}}[N_g]$ and $E_{K_{IP}}\big[\mathbf{G}_g\big]$. N_g and $E_{K_{SP}^{id}}[N_g]$ are used to verify SU g's authenticity. $E_{K_{SP}^{id}}[N_g]$ is the ciphertext of N_g using the IDN public key K_{SP}^{id}, which is

$$N_g \xrightarrow[encryption]{K_{SP}^{id}} E_{K_{SP}^{id}}\big[N_g\big]. \tag{5.29}$$

Upon receiving N_g and $E_{K_{SP}^{id}}[N_g]$, the SAS administrator verifies SU g's authenticity. Specifically, the SAS administrator searches for the IDN secret key stored in its memory with the IDN N_g, and uses that IDN secret key to decrypt $E_{K_{SP}^{id}}[N_g]$ by

$$E_{K_{SP}^{id}}\big[N_g\big] \xrightarrow[decryption]{K_{SS}^{id}} \hat{N}_g. \tag{5.30}$$

The SAS administrator then verifies SU g's authenticity by comparing $\hat{N}_g$ and N_g, which has two results:

$\hat{N}_g \neq N_g$: this means SU g did not send its actual IDN to the SAS administrator, then the SAS administrator will ask SU g to re-send its IDN.

$\hat{N}_g = N_g$: this means SU g sent its own IDN, then the SAS administrator will continue to process SU g's request. Note that the SU g cannot be approved to

proceed to the next steps of PF-PSEO (e.g., the steps in PF scheme) until providing its true IDN.

5.4.3 Punishing, Forgiving, and Banning Greedy SUs

In our PF scheme, we use γ_g to denote the number of times that SU g has been dishonest, referred to as the reputation history (RH). η_g, referred to as the reputation score (RS), reflects the honesty of SU g's behavior during the last data transmission: $\eta_g = +1$ ($\eta_g = -1$) if SU g behaved honestly (dishonestly). Both γ_g and η_g are first generated (then kept track of) by the SAS administrator with initial values of 0 and $+1$, respectively. If a SU g is found to be honest, the SAS administrator will not change the values of γ_g and η_g. If not, the SAS administrator will update η_g as -1, which means SU g's next request will be rejected. The value of γ_g is then added by $+1$. If γ_g reaches the honesty threshold, β, SU g will be classified as a *regularly dishonest user*.

Upon receiving a request from the SU g, the SAS administrator first checks the value of γ_g to verify whether SU g is a regularly dishonest user, which has two potential cases.

Case A

$\gamma_g = \beta$, meaning that SU g is regarded as a regularly dishonest user. In that case, SU g's request will be rejected. Moreover, as a regularly dishonest user, SU g's future requests will never be granted even if it behaves honestly in the future (i.e., no forgiveness). The values of γ_g and η_g will not be updated, and the user is forever banned from obtaining the shared spectrum.

Case B

$\gamma_g < \beta$, which means SU g is not a regularly dishonest user. Then the SAS administrator checks the value of η_g to verify the honesty of SU g's behavior during the last data transmission.

$\eta_g = -1$: i.e., SU g's behavior did not abide by its report during the last

transmission experience (e.g., reporting a lower transmitting power than its actual one), the SAS administrator will jump to the punishment stage that denies SU g's request directly. After that, the SAS administrator will update η_g from -1 to $+1$, which is called forgiveness. Moreover, the SAS administrator does not update γ_g.

$\eta_g = +1$: i.e., SU g's behavior complied with its report during the last data transmission, then the SAS administrator will continue to process SU g's request, which are the $3-10$ steps of PSEO in Section 5.3.3. The values of γ_g and η_g will be updated depending on the outcome of SU g's request and its behavior. Specifically, if SU g's request is denied by the SAS administrator, the SAS administrator will keep the values of γ_g and η_g unchanged. If SU g's request is approved, γ_g and η_g will be updated as aforementioned (depending on if its transmission complies with its reported information or not).

Note that although the SAS administrator does not receive the unencrypted data from SUs, it can still find out if a granted SU complies with its requested values or not. Specifically, the government agency (e.g., FCC or NTIA [125]) monitors SUs behavior during the data transmission period (to find out greedy behaviors) using the spectrum monitoring and signal analysis techniques [126]. Interested readers are also referred to [127] and [128] for similar spectrum monitoring approaches. Then the agency generates an interference map of this SU using the observed data and attenuation map (public knowledge). Next, the agency encrypts this map using the IU's public key before sending it to the SAS administrator. Upon receiving the ciphertext from the agency, the SAS administrator calculates a subtraction in the ciphertext domain, by subtracting it from the ciphertext data reported by the SU in the spectrum requesting period. After that, the SAS administrator sends the calculated result to the IU to verify the honesty of the SU. The IU decrypts the received result and checks its value: If all values are non-negative which means the actual operating value is no more than the SU's requested value, the IU will report to the SAS administrator that the SU is honest during its data transmission. Otherwise, the IU will report to the SAS administrator that the SU is dishonest.

5.5 Quantization of Attenuation Map and Discussion

In this section, we first focus on the quantization of the attenuation map. We then discuss the effect of the quantization selection on the attenuation map, followed by the effect of obfuscating factors on the spectrum utilization.

5.5.1 Quantization of Attenuation Map

The quantization process aims to partition the attenuation map into N grids to reduce the online complexity. For PSEO and PF-PSEO, the size of each grid in the quantized attenuation map $\mathbf{A}$ dramatically affects the precision of the attenuation value in each grid and the computational complexity. The smaller grid size, the higher precision of the attenuation map, hence the fewer decision errors made by the SAS administrator. However, that comes at the extra cost of the overhead computation. Similar to the scheme in [94], to optimize the balance between the precision of attenuation value and the computational complexity, we formulate the following optimization problem that aims to find the optimal quantization tuple:

$$\begin{aligned} \underset{X_q,Y_q,H_q,F_q}{\text{minimize}} \quad & E_r\big(X_q, Y_q, H_q, F_q\big) \\ \text{subject to} \quad & cost(X_q, Y_q, H_q, F_q) \leq C_n \\ & X_q \in \{2, 3, ..., X_N\}, \\ & Y_q \in \{2, 3, ..., Y_N\}, \\ & H_q \in \{2, 3, ..., H_N\}, \\ & F_q \in \{2, 3, ..., F_N\}, \end{aligned} \tag{5.31}$$

where $E_r(\cdot)$ indicates the decision error made by the SAS administrator. We adopt three types of metrics to measure $E_r(\cdot)$: the positive decision error (PDE), the negative decision error (NDE), and the total decision error (TDE). PDE occurs when the SU's request should have been denied by the SAS administrator, but gets an approval response. NDE denotes the case that the SAS administrator makes a denial decision to the SU's request that should have been approved. TDE is the total

number of PDE and NDE, which is the number of all incorrect requests decisions. $cost(\cdot)$ is the cost function which denotes the computational complexity of each request period. That refers to the total number of online operations (as in Table 5.1) or online processing time for each SU's request, which is proportional to the total number of grids. X_N, Y_N, F_N, and H_N are maximum quantization numbers for X, Y, F, and H, respectively. C_n is the computational complexity (cost) limit that depends on specific requirements in different scenarios.

The maximum quantization levels X_N, Y_N, F_N, and H_N are selected based on specific requirements of performance in different scenarios, e.g., the balance between the accuracy of spectrum allocation and the computational complexity. For instance, the quantization tuple (50, 50, 20, and 20) may provide a very high level of accuracy at the expense of high computational complexity (refer to Table 5.4). Thus, that tuple can be selected as the maximum boundary of the optimization variables for scenarios that can tolerate a higher error ratio. For the above integer programming, we apply the branch and bound method [129] to solve it. Since this optimization procedure is completed offline by the SAS administrator, it does not increase the online overhead of PSEO during all the later spectrum requests.

Note that each grid generated from equation (5.31) involves original attenuation values, referring to the attenuation values calculated by the SAS administrator using the terrain data. These data are sent to all users in the system before the stage of the spectrum requesting period. We provide three different methods to estimate the attenuation value for each grid, which are Maximum value, Minimum value, and Average value estimation methods.

The Maximum value estimation method can be expressed as

$$A = \max\big(A^1, A^2, ...A^L\big), \tag{5.32}$$

where $A^1, A^2, ...A^L$ are original attenuation values in one grid area. L means the total number of the original attenuation values in the grid. Obviously, this estimation method selects the maximum value from L values as the value of the grid.

For the Minimum value estimation method, the attenuation value for each grid

is the minimum value in that gird, which is

$$A = \min\big(A^1, A^2, ...A^L\big). \tag{5.33}$$

In terms of the Average value estimation method, the attenuation value of each grid is the average of all the original values in that grid, which is

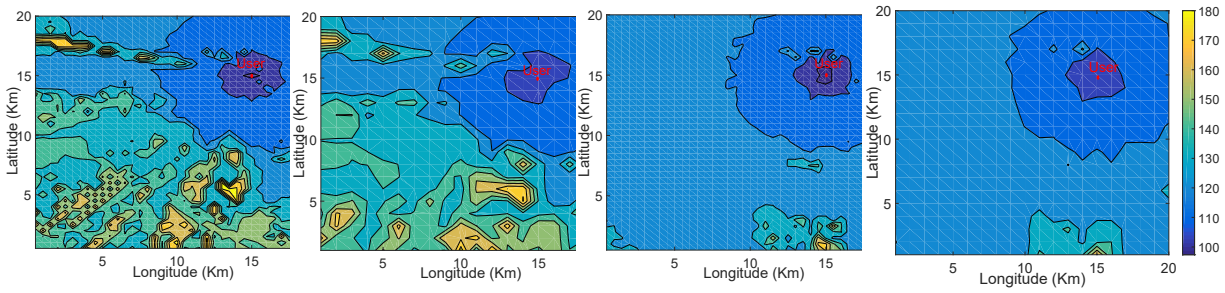
$$A = \frac{1}{L}\sum_{l=1}^{L} A^l. \tag{5.34}$$

These three estimation methods would result in different impacts on actual attenuation values. For example, "Maximum value" estimation method would cause over-estimation of attenuation values, and "Minimum value" would lead to under-estimation of actual attenuation values. Different estimation methods can be selected according to various specific requirements in different scenarios.

5.5.2 Effect of Quantization Selection on Attenuation Map

To illustrate the effect of the quantization selection on the attenuation map under different scenarios (e.g., different antenna heights), we provide Fig. 5.5. Different colours in each subfigure indicate the various attenuation values from the user to the corresponding locations, which vary in a range of $100 - 180$dB, as shown in the color bar. The subfigures in Fig. 5.5 show the attenuation map of the same user with different quantization tuples and antenna heights. Specifically, the user's antenna heights in both Fig. 5.5(a) and Fig. 5.5(b) are 6 m, but quantization tuples are $(40, 40, 10, 10)$ and $(20, 20, 6, 6)$, respectively. For Fig. 5.5(c) and Fig. 5.5(d), the antenna heights are 60 m, while the quantization tuples are $(40, 40, 10, 10)$ and $(20, 20, 6, 6)$, respectively.

It is clear that the effect of quantization on the attenuation maps varies with different antenna heights. As can be seen in Fig. 5.5(a) and Fig. 5.5(b), when the antenna height is 6m, decreasing the number of quantization grids (e.g., increasing the grid size) would lose a lot of details in the attenuation map. In this case, there will be a big error between the actual attenuation value and the estimated one, which degrades the accuracy of the proposed schemes. However, when the antenna height is 60m, as shown in Fig. 5.5(c) and Fig. 5.5(d), less details in the attenuation map are



(a) (b) (c) (d)

Figure 5.5: Effect of quantization selection (or grid size) on the attenuation map varies with different antenna heights. (a) User's antenna height is 6m, quantization tuple (40, 40, 10, 10); (b) User's antenna height is 6m with quantization tuple (20, 20, 6, 6); (c) User's antenna height is 60m with quantization tuple (40, 40, 10, 10); (d) User's antenna height is 60m with quantization tuple (20, 20, 6, 6).

lost when decreasing the number of quantization grids, resulting in less degradation of the performance of proposed schemes. Therefore, in different scenarios, the effect of the quantization method on the attenuation maps varies, leading to different effects on the performance of the proposed schemes.

5.5.3 Effect of c_3 and c_4 on Spectrum Utilization

As discussed in Section 5.3.3, the obfuscating factors, i.e., c_3 and c_4, are used to obfuscate users' actual private information, which can protect the operational privacy. Notably, unlike the conventional obfuscation methods (e.g., [92]), in our method, using obfuscation factors does not degrade the spectrum utilization.

For the conventional obfuscation methods (e.g., [92]), the obfuscating parameters are added to the user's actual data to preserve the user's actual operational information. The spectrum decisions are hence made based on the obfuscated values, leading to degradation of the spectrum utilization.

By contrast, for our proposed schemes, the spectrum decision 'YES/NO' (as described above) is made by counting the number of positive and negative terms, instead of the specific value of each term. Moreover, the obfuscating parameters c_3 and c_4 that are positive integers, used to multiply the numbers, do not change the positiveness/negativeness property of numbers. Therefore, the obfuscation does not

degrade the spectrum utilization in our proposed schemes.

5.6 Performance Analysis of PSEO and PF-PSEO

5.6.1 Privacy Analysis of PSEO and PF-PSEO

In this subsection, we analyze the privacy performance of proposed PSEO and PF-PSEO. Notably, PSEO and PF-PSEO achieve the same performance according to privacy-preserving. That is because these two schemes leverage the same BICS with similar obfuscation methods and additive homomorphic properties of the Paillier cryptosystem to preserve users' privacy. Therefore, we only analyze the privacy performance of PSEO.

Theorem 1 PESO is capable of protecting IUs' and SUs' operational privacy from the first three privacy threats described in Section 5.2.2.

Proof: We take the *Privacy threat 3)* in Section 5.2.2 as a study case to prove this theorem. For the other two privacy threats, similar conclusions can be easily obtained. If an adversary is able to eavesdrop the ciphertext of IU or SU, it will attempt to decrypt the ciphertext to access user's actual operational information. According to the semantically secure Paillier cryptosystem, it is impossible to decrypt the ciphertext correctly unless with the corresponding secret key [124]. However, as the secret keys are only kept by their owners (i.e., IUs or SUs), the adversary is not able to access neither the IU's nor the SU's secret key. The probability of generating the correct secret key is $1/2^K$, where K is the bit length of the secret key which is usually a large number. For instance, in this paper $K = 2048$, then the probability for the SAS administrator to get the correct key is only $1/2^{2048}$. As a result, the adversary cannot infer any actual operational information from the user's ciphertext. Similarly, even if the SAS administrator obtains the ciphertexts of IU or SU, it cannot infer any relevant information about the IU or SU. ■

As mentioned in the fourth type of attack, rogue SUs and a compromised SAS administrator may attempt to collude to reveal/obtain IUs' operational information. We have the following theorem.

Theorem 2 PSEO is able to protect IU's operational information under a

collusion attack.

Proof: Throughout all the steps in PSEO above, if there is a collusion between the SU and the SAS administrator, the SAS administrator or the SU may obtain $\mathbf{R}_g$ by decrypting $E_{K_{SP}}[\mathbf{R}_g]$ (refer to equation (5.28)). Note that $\mathbf{R}_g$ is the obfuscated value of the interference budget $\mathbf{R}'_g$ that is calculated with IU's and the SU's operational information. Thus, the IU's precise operational information can be revealed as long as $\mathbf{R}'_g$ is known. However, neither the SAS administrator nor the SU is able to access the actual value of $\mathbf{R}'_g$, because the obfuscating factor c_4 is only accessible to the IU. As a result, the IU's precise operational privacy is preserved even if the SAS administrator colludes with the SU. Similarly, if an adversary successfully eavesdrops information from the SAS administrator and the SU, it is unable to infer any precise operational information about the IU without the obfuscating factor c_4 (known only by the IU).

Additionally, neither the SAS administrator nor SU g can infer IU i's operational information (e.g., location) based on the positiveness/negativeness of numbers/grids in $\mathbf{R}_g$, even in an extreme case with only one negative grid. In other words, if the value of a grid is negative in $\mathbf{R}_g$, it does not necessarily imply that the IU is located in this grid or nearby grids. This is because in addition to the distance, various complex parameters (e.g., terrain, antenna height) are taken into account when calculating the radio attenuation map. Consequently, the interference map $\mathbf{G}_g$ and the interference threshold map $\mathbf{X}_i$ are not monotonically increasing with distance/location from the SU g and IU i, respectively (refer to Fig. 5.5). We can completely remove the correlation between the positiveness/negativeness of numbers/grids in $\mathbf{R}_g$ and the IU's location by randomly rearranging all the elements in $E_{K_{SP}}[\mathbf{R}_g]$ (refer to the 6th step in PSEO) (other users' precise operating information is protected via the obfuscation procedure). ■

Notably, the P^2-SAS scheme proposed in [94] is vulnerable to the collusion attack. When the SAS administrator and the key distributor (e.g., introduced in [94]) collude, the IUs' information can be decrypted. Even if the two entities do not collude, attackers can attempt each of the two separately then obtain the necessary information that allows them to interpret the operational data of IUs.

Theorem 3 Under PSEO, SUs' operating information is protected from the IU (as long as the IU does not collude with the SAS administrator).

Proof: Throughout all PSEO's steps, step 4 is the only potential one during which the IU can infer the SU's operational information. According to equation (5.19), IU i can infer SU g's actual information $\mathbf{B}_g$ if it gets access to $\mathbf{G}_g$. To deal with it, a positive number c_3 (in equation (5.20) and (5.21)), which is randomly generated by the SAS administrator, is used to obfuscate the actual information of $\mathbf{B}_g$. Since there is no collusion between the SAS administrator and IU i, IU i is not able to get c_3. As a result, after the decryption process, IU i would only obtain the obfuscated data $\mathbf{B}'_g$ instead of $\mathbf{B}_g$. Note that, similar to **Theorem** 2, IU i cannot infer SU g's operational information (e.g., location) using the positiveness/negativeness property of numbers in $\mathbf{B}'_g$. Another easy option to protect the SU's location is that the SAS administrator randomly rearranges all the elements in $E_{K_{IP}}\left[\mathbf{C}'\right]$ and $E_{K_{IP}}\left[\mathbf{B}'_g\right]$ (following the same arrangement rule) before sending $E_{K_{IP}}\left[\mathbf{B}'_g\right]$ and $E_{K_{IP}}\left[\mathbf{C}'\right]$ to IU (refer to the 4th step in PSEO). ■

From the above, we note that if the IU and the SAS administrator collude, the SU's operational privacy would be compromised (e.g., refer to the 4th step of PSEO). That is the weakness of PSEO, which is also our future work. However, in practice, IUs are often the agencies of defense (e.g., military radars) that are highly-trusted and most-protected components. The chance for IUs to be compromised or to collude with the SAS server is negligibly small.

5.6.2 Complexity Analysis of PSEO and PF-PSEO

In this subsection, we analyze the complexity of the proposed schemes that involve the online overhead and the offline complexity. As aforementioned, the online overhead refers to the computational complexity during the spectrum requesting stage. The offline complexity refers to the computational complexity before the spectrum requesting stage.

We emphasize that under SAS and all existing work (e.g.,P^2-SAS scheme in [94]), the interference map has to be computed for *every* SU's request (even when the SU does not move or the topology does not change). This is because the interference

Table 5.1: Total complexity per SU's request.

Operation		Proposed PSEO	Proposed PF-PSEO	P^2-SAS scheme
Offline	Subtractions	N/N_F	N/N_F	None
Online	Encryptions	$(4N+1)$	$(4N+2)$	$(8N+1)$
	Decryptions	$(3N+1)$	$(3N+2)$	$(2N+1)$
	Hom Add	N	N	$4N$
	Hom Sub	N	N	$4N$
	Hom S-Mul	$2N$	$2N$	$4N$

map is part of the interference budgeting at each IU, and this budget may change (e.g., a request from other SUs is granted) even if the SU or the topology does not change (related to the interference map). This is a shortcoming of P^2-SAS scheme in [94] as well as all other SAS-based frameworks. We observe this problem and propose our approach in which we separate the interference map calculation (above referred to as the offline overhead/complexity) from the interference budget update/calculation (the online overhead) so that the interference map does not have to be updated as frequently as the IU interference budgeting. Note that the offline complexity under PSEO and PF-SEO is only required once for every single SU and the map will be reused for all the future spectrum requests from that SU (i.e., well amortized by all future spectrum requests). Thus, the total complexity under our model is significantly reduced.

Table 5.1 shows the total complexity for each SU's request. In this table, N is the total number of grids. "Hom Add", "Hom Sub" and "Hom S-Mul" denote the homomorphic additions, homomorphic subtractions and homomorphic scalar multiplications, respectively. Regarding the offline overhead, since only N subtraction operations (one for each grid) in the plaintext domain are conducted (refer to the equation (5.15)), as shown in Table 5.1, for proposed PSEO and PF-PSEO, the average number of subtractions (i.e., the offline overhead) per SU's request is N/N_F (N_F is the number of all future requests of this SU). That is negligible (especially when N_F is a very large number).

For the online overhead, since the homomorphic operations (such as encryption, decryption, homomorphic additions, homomorphic subtractions, and homomorphic

scalar multiplications) are very much computationally demanding, we use the number of these operations as metrics. Unlike PSEO and PF-PSEO, P^2-SAS scheme in [94] conducts all interference calculations in the ciphertext domain during the spectrum requesting stage which more than doubles the online overhead, as seen in the Table 5.1. For the case of multiple IUs that use different public keys, the requesting SU encrypts its interference map using all IUs' public keys (so that any IU can decrypt it). However, in practice, multiple or even all IUs (e.g., military radars from the Department of Defense, DoD) may share the same public key, e.g., P^2-SAS scheme in [94]. Thus, the complexity scaling with the number of IUs in this case is practically marginal. We take PSEO as an example to demonstrate how these homomorphic operations above are counted:

- At the 1st and the 2nd steps in PSEO, the SU and the IU encrypt their own operational information, requiring $2N$ times of encryption.
- At the 3rd step, the SAS administrator calculates the interference budget in the ciphertext domain, incurring N times of encryption, addition and subtraction.
- At the 4th step, the SAS administrator obfuscates the interference budget, resulting in $2N$ times of scalar multiplication.
- At the 5th step, the IU decrypts the received information with $2N$ times of decryption.
- At the 6th step, the IU encrypts the obfuscated calculation with N times of encryption.
- At the 9 step, the SAS administrator encrypts the request decision, requiring 1 time of encryption.
- At the 10th step, the SU decrypts the received information, requiring $(N+1)$ times of decryption.

Therefore, the numbers of encryption, decryption, addition, subtraction, and scalar multiplication of PSEO for processing each SU's request are $(4N+1)$, $(3N+1)$, N, N, and $(2N)$, respectively.

It is similarly straightforward to compute the online overhead of PF-PSEO or P^2-SAS scheme in [94]. Notably, for PF-PSEO, in addition to the operations above, its online overhead also includes one encryption and one decryption operation, which occur at the stage of "Authentication of SU". It is clear that the number of homomorphic operations of PSEO or PF-PSEO is much smaller than those in P^2-SAS scheme, making the computation time of PSEO or PF-PSEO more than 50% faster than that in P^2-SAS scheme. For instance, if $N = 40 \times 40 \times 12 \times 8$, the total numbers of encryptions, online homomorphic additions, homomorphic subtractions, and homomorphic scalar multiplications for P^2-SAS scheme in [94] are 1.2288×10^6, 6.144×10^5, 6.144×10^5, and 6.144×10^5, respectively. By contrast, those numbers for our proposed schemes are only about 6.144×10^5, 1.536×10^5, 1.536×10^5 and 3.072×10^5, respectively. Note that, IUs and SUs under SAS are usually military radar systems and base stations, respectively [121], thus they have relatively strong computing capability and power to effectively facilitate those encryption and decryption operations. The experiment results are shown in Section 5.7.3.

5.6.3 PSEO and PF-PSEO with Coexistence of Multiple SASs

In practice, there may be multiple SASs which work in parallel to provide a nation-wide spectrum sharing service. For the case that SU a in SAS A wants to request the spectrum band of IU b in SAS B, the proposed PSEO and PF-PSEO are also capable of protecting users' operational privacy. Specifically, for the systems with multiple SASs, the operating frequency range of each SAS is broadcast, i.e., public knowledge, available for all SAS administrators and users [130]. Thus, SU a knows that its requesting frequency falls in the frequency range of SAS B, but it does not know which IU owns the spectrum nor IU's bandwidth. As such, SU a encrypts its interference map using all IUs' public keys in SAS B before sending the encrypted data (together with the unencrypted information guiding SAS A to forward the request to SAS B) to SAS administrator A. Then SAS administrator A forwards

the encrypted data to SAS administrator B for processing SU a's request. Note that SU a would not be able to send the request directly to SAS B as SUs can only talk to its administering SAS [130]. After that, SAS administrator B will process SU a's encrypted request, following the steps $2-7$ of our proposed PSEO. After the decision of SU a's request is made, SAS administrator B sends it to SU a via SAS administrator A. Then SU a verifies the request decision and sends a confirmation to SAS administrator B via SAS administrator A.

It is worth noting that for multiple SAS coexistence, SAS administrators do not need to exchange interference thresholds of IUs with each other. This is because each IU is administered by only one SAS who solely manages the IU's interference budget/threshold. Each SAS administrator updates the interference thresholds of IUs under its management based on the decision for each SU's request, and keeps the threshold to itself. All SUs' requests to this IU are processed solely by the IU's SAS, not any other one.

5.7 Simulation Results

We deploy a protection zone of SAS in a 20 km by 20 km rectangular area. We experiment the computation task using parallelization implementation on four distributed desktops with Intel $XeonE5-2690$ and 64GB RAM. The Paillier cryptosystem is constructed based on the GMP library [131]. The radio propagation model in this chapter is the Longley-Rice (L-R) model [132] that takes multiple parameters into account when calculating the attenuation value, such as locations, operating frequencies, polarization, terrain data, etc, and we generate it using $SPLAT!$ [133]. The attenuation value is calculated using the real terrain data in Washington D.C. from $SRTM3$ [134]. The simulation results are averaged over 2000 independent runs. In each run, the user's operational information (e.g., users' locations, antenna heights, transmitting powers, etc) is uniformly distributed within the corresponding ranges. Take the user's antenna height as an instance, each user's antenna height is uniformly distributed between $1 \sim 60\,m$. The relevant height of the user's antenna to the average terrain, e.g., the height above average terrain (HAAT), is also different,

Table 5.2: Simulation Parameters.

Number of IUs	20
Number of SUs	1500
Value of X	20 km
Value of Y	20 km
Value of H	60 m
Bandwidth of each SU	10MHz
Frequency band F	3.55 $\sim$ 3.65 GHz
Transmitting power of each SU	$-40 \sim -20$dBm
Sensitive interference threshold	-80 $\sim$ -120 dBm

depending on the user's specific locations. Other important simulation parameters are in Table. 5.2 [106]. Besides, we select the number of grids by applying equation (5.31). Specifically, we use three different types of metrics to measure the objective function, $Er(.)$: PDE, NDE and TDE, for achieving optimal grids. Moreover, we apply three estimation methods to obtain the estimated values of grids (refer to equations (5.32)-(5.34)). Consequently, we can obtain 9 groups of optimal grids considering the different combinations of $Er(.)$ and estimation methods. We select three groups of grids in this section to evaluate the performance of proposed schemes.

To evaluate the level of greediness of each greedy SU, we introduce a parameter α, which is

$$\alpha = \frac{G_r}{G_a}, \tag{5.35}$$

where G_r is the reported interference in the SU's request, G_a is the actual interference caused by that SU. $0 < \alpha \leq 1$. If $\alpha = 1$, the SU's behavior conforms to its report, i.e., the SU is honest, otherwise, the SU is dishonest.

We evaluate the performance of the proposed schemes and other work using three metrics: privacy performance, spectrum utilization and online overhead.

5.7.1 Privacy Performance of PSEO and PF-PSEO

To evaluate how PSEO/PF-PSEO protect IUs'/SUs' information, we use the location privacy as the representative. The same conclusions for other operating informa-

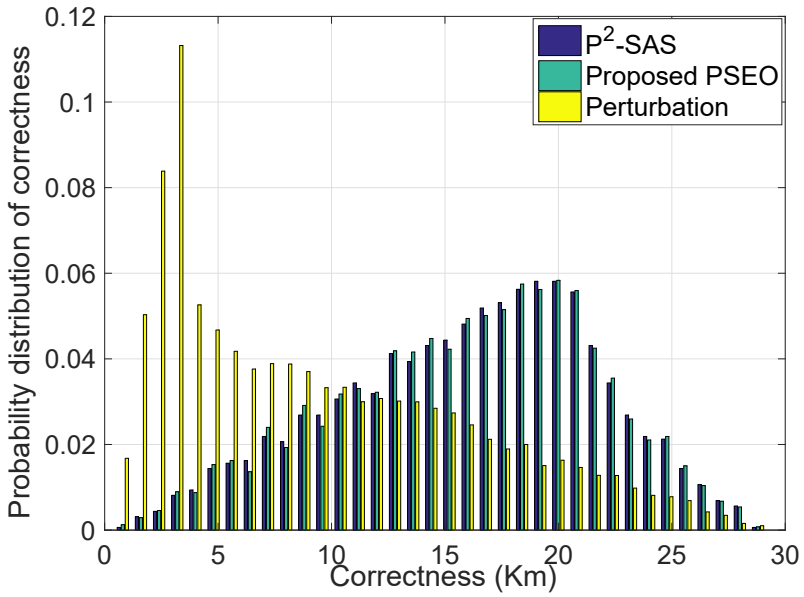


Figure 5.6: Privacy performance of IU for three methods.

tion (e.g., operating frequency bands) then follow. We adopt the correctness [135], which is the distance between the estimated location and the actual location, as the metric to evaluate the privacy preservation capability. The larger the correctness, the better/higher privacy performance. Due to the space limitation, we only present the performance of PSEO while PF-PSEO achieves similar performance regarding IUs'/SUs' privacy protection.

Fig. 5.6 and Fig. 5.7 compare the privacy performance of PSEO with two latest methods (e.g., the Perturbation with additive noise method in [92] and P^2-SAS scheme in [94]). The sum of all the probabilities for each method is 1. X_q, Y_q, H_q, and F_q in these two figures are 40, 40, 12, and 10 grids, respectively. The estimated attenuation value for the quantized gird is calculated using the "average value estimation method" (refer to equation (5.34)).

Fig. 5.6 compares the probability distribution of correctness of the three methods (i.e., PSEO and those in [92] and [94]). Since the secret keys are only held by users themselves, adversaries can only generate the secret keys via random guessing. Thus the probabilities of correctness under PSEO and P^2-SAS scheme in [94] are distributed as the random guessing in Fig. 5.6, indicating that adversaries cannot infer additional information about the IU, without the correct secret keys. However, for [92], adversaries can roughly infer the user's location information, i.e., extracting

user information from the data preserved by perturbation (e.g., with the additive noise method) [92]. For example, in Fig. 5.6, under the scheme in [92], when the correctness is less than or equal to 5km, the corresponding probability is around 0.364. In contrast, the probabilities for PSEO and the scheme in [94] are both lower than 0.042. In other words, for [92], there is still a high probability of revealing IU's rough location. By contrast, the corresponding probabilities for P^2-SAS scheme in [94] and our proposed PSEO are much lower.

For both IU and SU location protection (in Fig. 5.6 and Fig. 5.7, respectively), PSEO and P^2-SAS scheme in [94] achieve nearly the same correctness. That is because both leverage the properties of homomorphic cryptosystems to protect users' privacy. However, as mentioned before, P^2-SAS scheme in [94] is vulnerable to the collusion attack. By contrast, our proposed PSEO is able to protect IUs operational information under that attack. Moreover, PSEO requires much less online overhead (thanks to the proposed BICS) than P^2-SAS scheme in [94], which will be shown in Section 5.7.3.

5.7.2 Spectrum Utilization for PSEO and PF-PSEO

The accuracy of accepting or rejecting a spectrum request is the decisive factor to the proper operation of SAS. As discussed above, we first use the positive decision error ratio (PDER), the negative decision error ratio (NDER), and the total decision error ratio (TDER) to evaluate the spectrum utilization of the proposed schemes.

Table. 5.3 illustrates TDER, PDER and NDER. The grid tuple of (X_q, Y_q, H_q, F_q) is $(40, 40, 12, 11)$, i.e., X_q, Y_q, H_q, F_q in the equation (5.31) are 40, 40, 12, and 11 grids, respectively. We use three estimation methods, e.g., equation (5.32), (5.33) and (5.34), to calculate the estimated attenuation value for each gird. From this table, it is clear that PSEO is able to guarantee a very small error rate, which is similar to that of P^2-SAS scheme in [94], but with much lower complexity. Besides, the error rates of PSEO and the scheme in [94] are much smaller than those of [92]. This is because the Perturbation scheme in [92] preserves users' private data by adding noise signals into users' operational information, causing extra errors to users' data. By contrast, thanks to the properties of the cryptosystem, our proposed PSEO

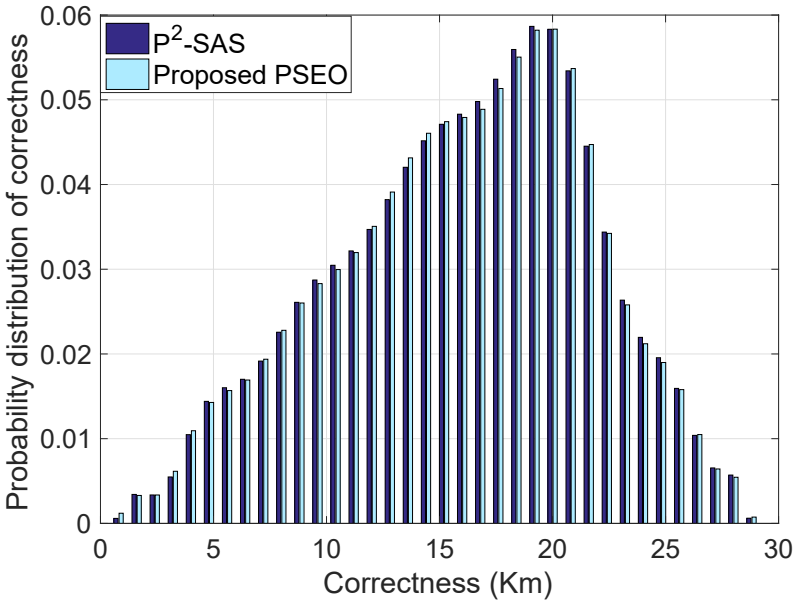


Figure 5.7: Privacy performance of SU for two methods.

enables secure interference budgeting/calculation without inducing extra errors to user's operational information. This table also shows the decision error ratios for different estimation methods (e.g., equation(5.32), (5.33) and (5.34)) used in the attenuation map quantization.

Table 5.3: Decision Error Ratios.

Result / Methods	TDER	PDER	NDER
PSEO equ (5.32)	0.031	0.000	0.031
PSEO equ (5.33)	0.029	0.029	0.000
PSEO equ (5.34)	0.035	0.019	0.016
Perturbation in [92]	0.061	0.037	0.024
P^2-SAS scheme in [94]	0.027	0.027	0.000

To further evaluate the spectrum utilization of different schemes, we provide Fig. 5.8 adopting the SU's averaged capacity [136] as a metric. From this figure, it is clear that the SU's averaged capacity of our proposed PSEO is more than 30% (on average) higher than that of Perturbation scheme in [92]. This is because our proposed PSEO can achieve smaller decision errors than [92], thereby SU can obtain a higher probability to utilize IU's spectrum. It is noteworthy that the proposed PSEO achieves similar spectrum utilization to that of P^2-SAS scheme but with much

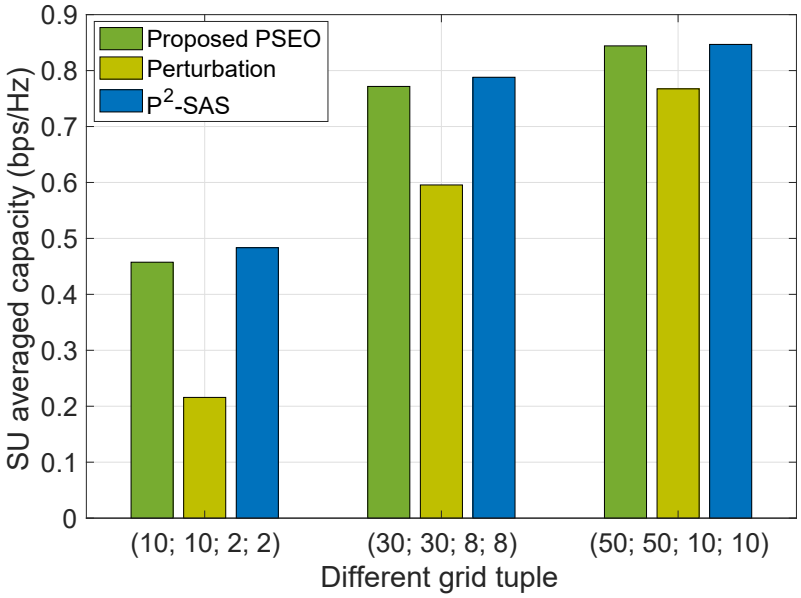


Figure 5.8: SU's averaged capacity of different schemes.

lower complexity. Besides, for each scheme, increasing the number of grids (e.g., the grid's size is smaller) can increase the SU's averaged capacity.

From Table. 5.3 and Fig. 5.8, either the decision accuracy and SU's averaged capacity can demonstrate the spectrum utilization of different schemes. Due to the space limitation, in the sequel, we only discuss the decision accuracy.

Fig. 5.9 shows TDER of different schemes considering the user mobility. In this case, the SUs move but do not report their new locations, i.e., not comply with the FCC's requirement (explained in Section 5.2.1) and are treated as dishonest users. In this figure, the grid tuple is (50, 50, 10, 10). The total number of SUs is 200, and the number of mobile SUs is 100. The processing time for SU's request is 16.5s (refer to Table 5.4). The speed of mobile SU (such as Vehicle-mounted base stations) is $100-120km/h$, so SU can move up to 600m during this period. If SU moves straight, it can move up to two grids (with the side length of 400 m) horizontally. As such, we select the number of grids moved by SU is $N_m = 0, 1, 2$. As can be seen from Fig. 5.9, TDER for each scheme dramatically increases with more grids moved by SU. This is because the SU's mobility results in a difference between its reported data and the actual information, thereby severely impacting on the decision accuracy of SU's requests. As aforementioned, this kind of dishonest SUs is recognized and later banned under PSEO.

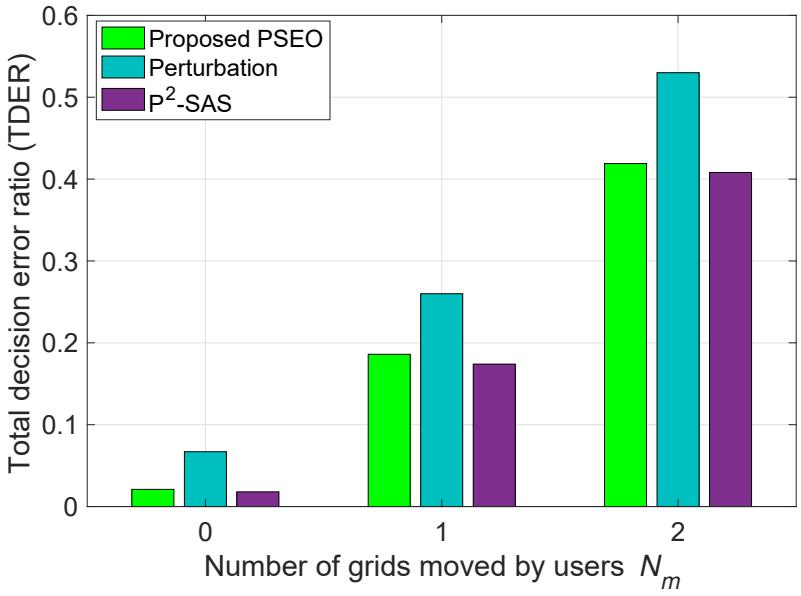


Figure 5.9: Impact of SU's mobility on total decision error ratio.

Table 5.4: Tradeoff between the complexity and the decision error ratio.

Result / Tuple	TDER	Online processing time
$(10, 10, 2, 2)$	0.4700	0.108s
$(20, 20, 4, 4)$	0.2150	0.952s
$(30, 30, 8, 8)$	0.1060	3.81s
$(40, 40, 10, 10)$	0.0360	9.72s
$(50, 50, 10, 10)$	0.0220	16.50s

Table. 5.4 shows the tradeoff between the complexity and the accuracy performance. It is clear that the quantization tuples with less number of grids (e.g., the grid's size is larger) require less processing time, while its performance degrades (e.g., the decision errors increase). Take the quantization tuple $(10, 10, 2, 2)$ as an example; its processing time for each SU's request is 0.108s, while its TDER is 0.4700. Moreover, the TDER for the tuple $(50, 50, 10, 10)$ is 0.0220, requiring processing time of 16.50s for each SU request. Therefore, the performance of spectrum utilization can be improved at the expense of the online complexity. In practical deployment, difference sizes of grids can be selected depending on the online complexity and the accuracy requirements.

Fig. 5.10 illustrates the effect of different rules in selecting IU's thresholds

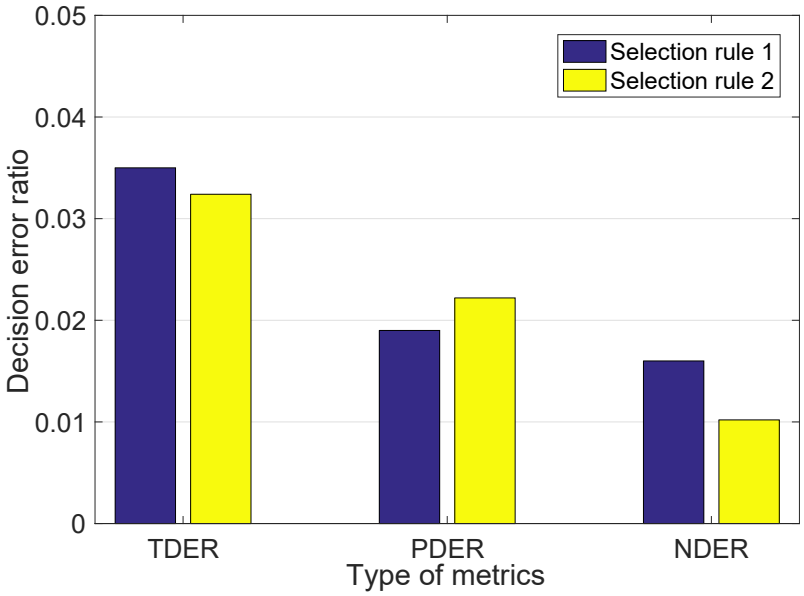


Figure 5.10: Impact of selecting IU's threshold on spectrum utilization.

(refer to the 2nd step in PSEO) on decision accuracies. The selection rule 1 means selecting the smallest value in the grid as the interference threshold, which is also the method used in the 2nd step in PSEO. The selection rule 2 denotes calculating the interference threshold from IU's location to the centers of other grids. As can be seen, the NDER under rule 1 is slightly higher than that under rule 2. This is because although this operation can protect IU from the interference caused by SU, it minimizes the interference threshold in each grid, increasing the NDER. By contrast, the PDER under rule 1 is slightly smaller than that under rule 2. Therefore, the user can select different selection rules based on their requirements.

Fig. 5.11 shows the impact of converting a non-integer to an integer (refer to the paragraph below the equation (5.11)) on the spectrum utilization. Note that this conversion process, which slightly degrades the spectrum utilization, is required because the Paillier cryptosystem is only suited for non-negative integer numbers. From this figure, it is clear that the decision error ratio for converting a non-integer to an integer by rounding up to 8 digits is slightly smaller than by rounding up to 3 digits, with more computational complexity.

Fig. 5.12 and Fig. 5.13 show the decision accuracy of PF-PSEO with dishonest SUs. We use TDER to evaluate PF-PSEO's performance. In these two figures, all SUs can apply for the spectrum access initially, but those who are dishonest will be

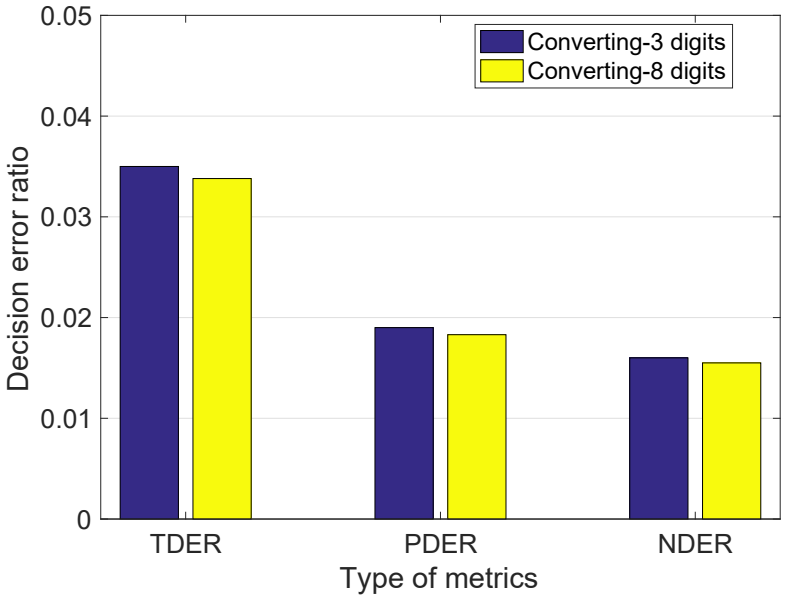


Figure 5.11: Impact of conversion on spectrum utilization.

punished and potentially banned under PF-PSEO. TDER is calculated by averaging all values within a period of time, depending on different cases (i.e., Case A and Case B under PF-PSEO). Take Case A as an instance, the period is from when the first dishonest user behaves dishonestly to when the last dishonest user gets banned. We assume the dishonest SUs prefer to behave dishonestly when they can apply for spectrum access. This leads to more decision errors on spectrum allocation, which can better evaluate the performance of the proposed PF-PSEO in eliminating the severe impact caused by those dishonest SUs. The quantization tuple (X_q, Y_q, H_q, F_q) is $(40, 41, 12, 8)$. We use equation (5.34) to achieve the attenuation value for each grid. The total number of SUs in these three figures is 200.

Fig. 5.12 shows the TDER of PF-PSEO and PSEO v.s. the number of dishonest SUs. β and α are 3 and 0.7, respectively. The γ's initial value is 0. We show the TDER of PF-SPEO with two cases, e.g., $CaseA$ and $CaseB$ in Section 5.4.3. According to this figure, PF-PSEO is able to achieve a much smaller TDER than PSEO. For example, when the dishonest SUs' number is 100, the TDER for PSEO is 0.313 that is much higher than PF-PSEO (e.g., 0.068 for $CaseA$ and 0.087 for $CaseB$). Additionally, for PF-PSEO, $CaseA$ achieves a smaller value of TDER than $CaseB$. That is because $CaseA$ is capable of rejecting regularly dishonest SUs' requests permanently drawing support from γ, which mitigates the negative

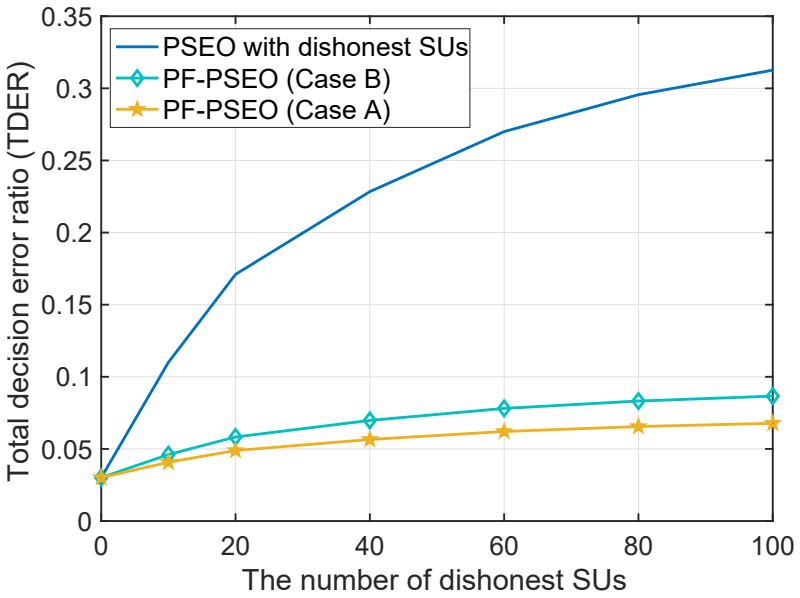


Figure 5.12: TDER of PF-PSEO and PSEO with number of dishonest SUs.

impact caused by dishonest SUs.

Fig. 5.13 describes the effect of α on TDER of PF-PSEO and PSEO. The number of dishonest SUs is 40. The decrease of α means that the reputation of SU's honesty is becoming poor. Obviously, the TDER of PSEO increases much more dramatically than that of PF-PSEO (including $CaseA$ and $CaseB$) with the decrease of α. For example, if α decreases from 0.9 to 0.1, reflecting the decreasing dishonesty of the SU, the TDER of PSEO rises from 0.119 to 0.327. By contrast, the corresponding TDER of PF-PSEO only grows slightly, e.g., from 0.048 to 0.089 for $CaseA$ and from 0.057 to 0.119 for $CaseB$. This implies that PF-PSEO is more robust to the impact of α or dishonest SUs than PSEO.

We can conclude from Fig. 5.12 and Fig. 5.13 that the performance of PSEO dramatically suffers from dishonest SUs. By contrast, PF-PSEO is capable of achieving much better performance with the help of the punishment and forgiveness scheme.

5.7.3 Online Overhead of PSEO and PF-PSEO

In this subsection, we evaluate the online overhead of PSEO and PF-PSEO.

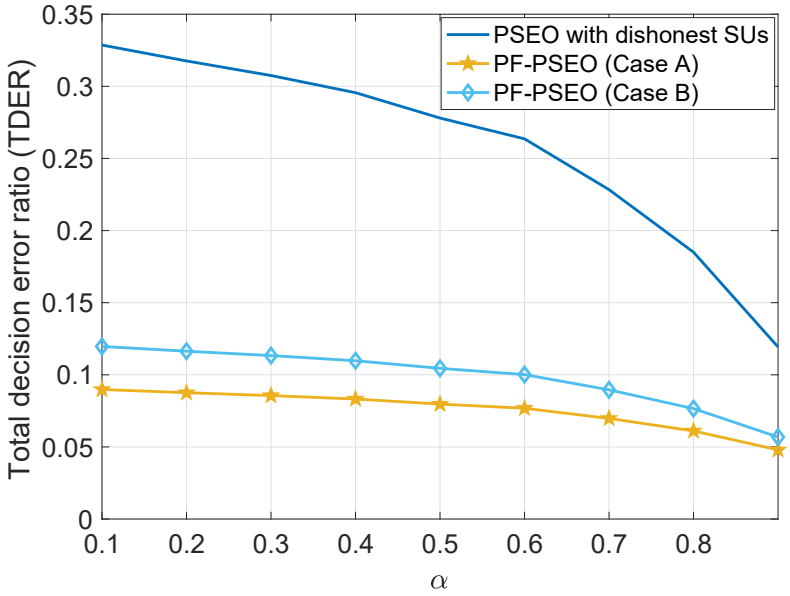


Figure 5.13: TDER of two schemes with different values of α.

As shown in Table 5.1, with the same N, the numbers of homomorphic additions and subtractions of PSEO and PF-SPEO are about one-fourth of those in P^2-SAS scheme. Moreover, PSEO and PF-PSEO require only half the number of encryptions and scalar multiplications of P^2-SAS scheme in [94]. Notably, the value of N is usually large in SAS, making the complexity reduction of PSEO and PF-PSEO very much significant, compared with that of P^2-SAS scheme in [94]. For instance, in our simulation (run on four distributed desktops with Intel XeonE5-2690 and 64GB RAM), when the total number of grids $N = 40 \times 40 \times 12 \times 8$, PSEO requires 9.61s to process an SU's request, and the total time to serve 1000 SUs is around 2.67h (the online processing time of PF-PSEO is the same as PSEO due to the very close number of operations). That can be significantly reduced with specialized hardware implementation/design in practice. For P^2-SAS scheme in [94], the online processing time for each SU's and 1000 SUs' requests are 18.94s and 5.26h, respectively (i.e., doubling the processing time of PSEO). Note that the SAS administrator is a powerful database/server [121] that can efficiently handle a great number of complex operations. The IUs are military radar systems and SUs can be base stations of cellular systems [121] that are also rich in computing resource.

5.8 Conclusion

In this chapter, we investigated the operational privacy issues of IUs and two types of SUs (e.g., honest SUs and dishonest SUs) in the SAS architecture. Specifically, for the case of IUs and honest SUs, we provided an operational information preserving scheme for IUs and SUs in SASs. The cores of our scheme are the blind interference calculation scheme (BICS) and a novel information exchange procedure using homomorphic encryption and obfuscation. BICS facilitates the interference budgeting without requiring IUs or SUs to reveal their operational information. That also reduces the online overhead of our scheme. For dishonest SUs, we proposed a punishment and forgiveness mechanism to encourage SUs to provide truthful information. Extensive simulation results showed that PSEO and PF-PSEO are able to preserve the operational privacy of IUs and honest/dishonest SUs with much less online overhead, compared with the state of the art schemes.

Chapter 6

Conclusion and Future Work

This thesis developed efficient and secure solutions for dynamic spectrum access (DSA) in future wireless communications. In this chapter, we summarize the contributions of this thesis and discuss future research directions.

In Chapter 3, we addressed the efficient issue of spectrum sensing in Half-duplex systems. First, we proposed a sensing approach by leveraging the property of deep learning networks. Unlike the traditional methods, our approach does not require any prior knowledge such as IU's signal structure, which can effectively protect IU's private operational information. Besides, the proposed work does not need any feature extraction algorithms to process the input signal of deep learning networks, which however is required by existing learning-based methods. This can reduce the sensing complexity and improve the sensing accuracy. Second, by exploiting signal properties in both time and frequency domains, we designed a sensing method to further improve sensing performance, especially in low SNR conditions. Simulations indicate that our developed approaches are notably superior to conventional sensing methods (both feature-based and learning-based) in terms of the robustness to noise uncertainty, timing delay and carrier frequency offset (CFO). To further evaluate the sensing performance, we conducted extensive simulations considering various conditions, and the numerous results also verify the superiority of our proposed methods. For future work, we will design a sensing approach that takes into account the background traffic caused by other SUs. We believe that other SUs activities strongly affect the sensing accuracy. To address this issue, the cooperative sensing

techniques can be investigated in future work.

In Chapter 4, we developed the efficient solutions of spectrum sensing in Full-duplex (FD) paradigms. Unlike the issues tackled in Chapter 3, the (residual) self-interference is a major challenge that impacts the sensing performance. To address this problem, we proposed two feature-based sensing algorithms drawing support from the properties of OFDM signals. Specifically, by exploiting the Cyclic Prefix of OFDM signals, we designed a sensing approach that is robust to residual self-interference. Our work also holds the advantage regarding the robustness to timing delay. Unlike the conventional OFDM sensing methods that require complex processes to estimate the impact of timing delay, our proposed work can completely avoid such a requirement, thereby effectively reducing the complexity. Additionally, by leveraging the Pilot Tone structures, we proposed a sensing method which is robust not only to residual self-interference but also to CFO. This developed work does not need any process to estimate CFO that however is necessary for existing methods. We also derived the closed-form expressions of the probability of detection and false alarm for the proposed approaches. Extensive simulations also confirm that our proposed methods are notably superior to the existing work under various communication conditions.

In Chapter 5, we investigated the privacy issue in Spectrum Access System (SAS). First, by leveraging cryptosystems and obfuscation methods, we designed a scheme to preserve the confidential information of IUs and honest SUs. To reduce the online overhead of the proposed scheme and further protect users' operational data, we proposed a novel interference calculation scheme. It is able to complete interference budgeting tasks at the SU's side in an offline manner (i.e., before the spectrum requesting stage), requiring SUs' operational data only. Second, to protect the privacy of dishonest SUs, we proposed a punishment and forgiveness mechanism to encourage SUs to engage in honest activities. Compared to existing methods, our proposed schemes are capable of fully protecting all users' operational information and successfully guaranteeing spectrum utilization. We also provided theoretical analysis to comprehensively analyze the performance of our developed schemes. In this thesis, we only investigated the privacy issues based on the condition that

the SAS administrator processes SUs' requests sequentially. The scenario that the SAS administrator processes multiple SUs' requests simultaneously has not been considered and hence left for future work. Future work may include leveraging the properties of blockchain to protect the user's operational privacy.

Bibliography

[1] J. Olenewa, *Guide to Wireless Communications*, 3rd ed. Delmar Learning, 2013.

[2] A. Goldsmith, *Wireless Communications*. New York, NY, USA: Cambridge University Press, 2005.

[3] E. Dahlman, S. Parkvall, and J. Skold, *4G: LTE/LTE-Advanced for Mobile Broadband*, 1st ed. Orlando, FL, USA: Academic Press, Inc., 2011.

[4] Ericsson, "More than 50 billion connected devices," *White Paper*, Feb 2011. [Online]. Available: http://www.ericsson.com/res/docs/whitepapers/wp-50-billions.pdf

[5] I.-. M. Project, "Scenarios, requirements and kpis for 5g mobile and wireless system," *Del.D1.1*, May 2013. [Online]. Available: https://www.metis2020.com/documents/deliverables/

[6] J. G. Andrews, S. Buzzi, W. Choi, S. V. Hanly, A. Lozano, A. C. Soong, and J. C. Zhang, "What will 5g be?" *IEEE Journal on selected areas in communications*, vol. 32, no. 6, pp. 1065–1082, 2014.

[7] M. Agiwal, A. Roy, and N. Saxena, "Next generation 5g wireless networks: A comprehensive survey," *IEEE Communications Surveys Tutorials*, vol. 18, no. 3, pp. 1617–1655, thirdquarter 2016.

[8] A. Osseiran, V. Braun, T. Hidekazu, P. Marsch, H. Schotten, H. Tullberg, M. A. Uusitalo, and M. Schellman, "The foundation of the mobile and wireless communications system for 2020 and beyond: Challenges, enablers and

technology solutions," in *2013 IEEE 77th Vehicular Technology Conference (VTC Spring)*, June 2013, pp. 1–5.

[9] A. Alexiou and M. Haardt, "Smart antenna technologies for future wireless systems: trends and challenges," *IEEE Communications Magazine*, vol. 42, no. 9, pp. 90–97, Sep. 2004.

[10] NTIA, "Assessment of the near-term viability of accommodating wireless broadband systems in the 1675-1710 MHz, 1755-1780 MHz, 3500-3650 MHz, 4200-4220 MHz, and 4380-4400 MHz bands," Oct 2010.

[11] W. y. Lee and I. F. Akyildiz, "Optimal spectrum sensing framework for cognitive radio networks," *IEEE Transactions on Wireless Communications*, vol. 7, no. 10, pp. 3845–3857, October 2008.

[12] T. Yucek and H. Arslan, "A survey of spectrum sensing algorithms for cognitive radio applications," *IEEE Communications Surveys & Tutorials*, vol. 11, pp. 116–130, 2009.

[13] E. Everett, A. Sahai, and A. Sabharwal, "Passive self-interference suppression for full-duplex infrastructure nodes," *IEEE Transactions on Wireless Communications*, vol. 13, no. 2, pp. 680–694, February 2014.

[14] S. K. Sharma, T. E. Bogale, L. B. Le, S. Chatzinotas, X. Wang, and B. Ottersten, "Dynamic spectrum sharing in 5g wireless networks with full-duplex technology: Recent advances and research challenges," *IEEE Communications Surveys Tutorials*, vol. 20, no. 1, pp. 674–707, Firstquarter 2018.

[15] Y. Liao, T. Wang, L. Song, and Z. Han, "Listen-and-talk: Protocol design and analysis for full-duplex cognitive radio networks," *IEEE Transactions on Vehicular Technology*, vol. 66, 2017.

[16] D. Cohen and Y. C. Eldar, "Sub-nyquist cyclostationary detection for cognitive radio," *IEEE Transactions on Signal Processing*, vol. 65, no. 11, pp. 3004–3019, June 2017.

[17] S. Dikmese, P. C. Sofotasios, T. Ihalainen, M. Renfors, and M. Valkama, "Efficient energy detection methods for spectrum sensing under non-flat spectral characteristics," *IEEE Journal on Selected Areas in Communications*, vol. 33, no. 5, pp. 755–770, May 2015.

[18] S. K. Sharma, T. E. Bogale, S. Chatzinotas, B. Ottersten, L. B. Le, and X. Wang, "Cognitive radio techniques under practical imperfections: A survey," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 1858–1884, Fourthquarter 2015.

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

[20] E. Bertino and R. Sandhu, "Database security - concepts, approaches, and challenges," *IEEE Transactions on Dependable and Secure Computing*, vol. 2, no. 1, pp. 2–19, Jan 2005.

[21] M. M. Sohul, M. Yao, T. Yang, and J. H. Reed, "Spectrum access system for the citizen broadband radio service," *IEEE Communications Magazine*, vol. 53, no. 7, pp. 18–25, 2015.

[22] L. Ericsson, "More than 50 billion connected devices," *White Paper*, 2011.

[23] G. I. Tsiropoulos, O. A. Dobre, M. H. Ahmed, and K. E. Baddour, "Radio resource allocation techniques for efficient spectrum access in cognitive radio networks," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 824–847, Firstquarter 2016.

[24] Y. Liao, T. Wang, L. Song, and Z. Han, "Listen-and-talk: Protocol design and analysis for full-duplex cognitive radio networks," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 1, pp. 656–667, Jan 2017.

[25] S. Chaudhari, V. Koivunen, and H. V. Poor, "Autocorrelation-based decentralized sequential detection of ofdm signals in cognitive radios," *IEEE Transactions on Signal Processing*, vol. 57, 2009.

[26] W. Afifi and M. Krunz, "Incorporating self-interference suppression for full-duplex operation in opportunistic spectrum access systems," *IEEE Transactions on Wireless Communications*, vol. 14, no. 4, pp. 2180–2191, April 2015.

[27] A. Sabharwal, P. Schniter, D. Guo, D. W. Bliss, S. Rangarajan, and R. Wichman, "In-band full-duplex wireless: Challenges and opportunities," *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 9, pp. 1637–1652, Sept 2014.

[28] FCC, "Amendment of the commission's rules with regard to commercial operations in the 3550-3650 mhz band," Federal Commun. Commission, Washington, DC, USA, 2016.

[29] ——, "Fcc nprm in the matter of amendment of the commissions rules with regard to commercial operations in the 3550-3650 mhz band," *Washington, D.C. 20554*, 2012.

[30] W. Xu, X. Zhou, C. Lee, Z. Feng, and J. Lin, "Energy-efficient joint sensing duration, detection threshold, and power allocation optimization in cognitive OFDM systems," *IEEE Transactions on Wireless Communications*, vol. 15, no. 12, pp. 8339–8352, Dec 2016.

[31] H. Tang, "Some physical layer issues of wide-band cognitive radio systems," in *First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005.*, Nov 2005, pp. 151–159.

[32] Z. Lu, Y. Ma, P. Cheraghi, and R. Tafazolli, "Novel pilot-assisted spectrum sensing for OFDM systems by exploiting statistical difference between subcarriers," *IEEE Transactions on Communications*, vol. 61, pp. 1264–1276, April 2013.

[33] W. Xu, W. Xiang, M. Elkashlan, and H. Mehrpouyan, "Spectrum sensing of ofdm signals in the presence of carrier frequency offset," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 8, pp. 6798–6803, Aug 2016.

[34] M. R. Vyas, D. K. Patel, and M. Lopez-Benitez, "Artificial neural network based hybrid spectrum sensing scheme for cognitive radio," in *2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, Oct 2017, pp. 1–7.

[35] Y. Tang, Q. Zhang, and W. Lin, "Artificial neural network based spectrum sensing method for cognitive radio," in *2010 6th International Conference on Wireless Communications Networking and Mobile Computing*, Sept 2010, pp. 1–4.

[36] D. Han, G. C. Sobabe, C. Zhang, X. Bai, Z. Wang, S. Liu, and B. Guo, "Spectrum sensing for cognitive radio based on convolution neural network," in *2017 10th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics (CISP-BMEI)*, Oct 2017, pp. 1–6.

[37] E. Axell and E. G. Larsson, "Optimal and sub-optimal spectrum sensing of ofdm signals in known and unknown noise variance," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 2, pp. 290–304, February 2011.

[38] A. Ali and W. Hamouda, "Advances on spectrum sensing for cognitive radio networks: Theory and applications," *IEEE Communications Surveys Tutorials*, vol. 19, no. 2, pp. 1277–1304, Secondquarter 2017.

[39] M. Jin, Q. Guo, J. Xi, Y. Li, and Y. Li, "On spectrum sensing of OFDM signals at low SNR: New detectors and asymptotic performance," *IEEE Transactions on Signal Processing*, vol. 65, no. 12, pp. 3218–3233, June 2017.

[40] S. Zhang, X. Yu, Y. Sui, S. Zhao, and L. Zhang, "Object tracking with multi-view support vector machines," *IEEE Transactions on Multimedia*, vol. 17, no. 3, pp. 265–278, March 2015.

[41] L. Deng and X. Li, "Machine learning paradigms for speech recognition: An overview," *IEEE Transactions on Audio, Speech, and Language Processing*, vol. 21, no. 5, pp. 1060–1089, May 2013.

[42] S. Zhang, S. Zhang, T. Huang, and W. Gao, "Speech emotion recognition using deep convolutional neural network and discriminant temporal pyramid matching," *IEEE Transactions on Multimedia*, vol. 20, no. 6, pp. 1576–1590, June 2018.

[43] H. Ye, G. Y. Li, and B. H. Juang, "Power of deep learning for channel estimation and signal detection in OFDM systems," *IEEE Wireless Communications Letters*, vol. 7, no. 1, pp. 114–117, Feb 2018.

[44] L. He, G. Wang, and Z. Hu, "Learning depth from single images with deep neural network embedding focal length," *IEEE Transactions on Image Processing*, vol. 27, no. 9, pp. 4676–4689, Sept 2018.

[45] H. C. Shin, M. R. Orton, D. J. Collins, S. J. Doran, and M. O. Leach, "Stacked autoencoders for unsupervised feature learning and multiple organ detection in a pilot study using 4D patient data," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 35, no. 8, pp. 1930–1943, Aug 2013.

[46] M. Bkassiny, Y. Li, and S. K. Jayaweera, "A survey on machine-learning techniques in cognitive radios," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 3, pp. 1136–1159, Third 2013.

[47] K. W. Choi, E. Hossain, and D. I. Kim, "Cooperative spectrum sensing under a random geometric primary user network model," *IEEE Transactions on Wireless Communications*, vol. 10, no. 6, pp. 1932–1944, June 2011.

[48] K. M. Thilina, K. W. Choi, N. Saquib, and E. Hossain, "Machine learning techniques for cooperative spectrum sensing in cognitive radio networks," *IEEE Journal on Selected Areas in Communications*, vol. 31, pp. 2209–2221, November 2013.

[49] Y. Huang, Y. Liang, and G. Yang, "A fuzzy support vector machine algorithm for cooperative spectrum sensing with noise uncertainty," in *2016 IEEE Global Communications Conference (GLOBECOM)*, Dec 2016, pp. 1–6.

[50] W. Lee, M. Kim, D. Cho, and R. Schober, "Deep sensing: Cooperative spectrum sensing based on convolutional neural networks," *CoRR*, vol. abs/1705.08164, 2017. [Online]. Available: http://arxiv.org/abs/1705.08164

[51] Y. Lu, P. Zhu, D. Wang, and M. Fattouche, "Machine learning techniques with probability vector for cooperative spectrum sensing in cognitive radio networks," in *2016 IEEE Wireless Communications and Networking Conference*, April 2016, pp. 1–6.

[52] Y. Xu, P. Cheng, Z. Chen, Y. Li, and B. Vucetic, "Mobile collaborative spectrum sensing for heterogeneous networks: A bayesian machine learning approach," *IEEE Transactions on Signal Processing*, vol. 66, no. 21, pp. 5634–5647, Nov 2018.

[53] J. Schmidhuber, "Deep learning in neural networks: An overview," *Neural Networks*, vol. 61, pp. 85 – 117, 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0893608014002135

[54] Q. Mao, F. Hu, and Q. Hao, "Deep learning for intelligent wireless networks: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, pp. 1–1, 2018.

[55] D. Singh and C. K. Mohan, "Deep spatio-temporal representation for detection of road accidents using stacked autoencoder," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–9, 2018.

[56] J. Masci, U. Meier, D. Cireşan, and J. Schmidhuber, "Stacked convolutional auto-encoders for hierarchical feature extraction," in *Artificial Neural Networks and Machine Learning – ICANN 2011*, T. Honkela, W. Duch, M. Girolami, and S. Kaski, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 52–59.

[57] Y. Bengio, "Learning deep architectures for ai," *Found. Trends Mach. Learn.*, vol. 2, no. 1, pp. 1–127, Jan. 2009. [Online]. Available: http://dx.doi.org/10.1561/2200000006

[58] D. Erhan, Y. Bengio, A. Courville, P.-A. Manzagol, P. Vincent, and S. Bengio, "Why does unsupervised pre-training help deep learning?" *J. Mach. Learn. Res.*, vol. 11, pp. 625–660, Mar. 2010. [Online]. Available: http://dl.acm.org/citation.cfm?id=1756006.1756025

[59] T. Ching, D. S. Himmelstein, B. K. Beaulieu-Jones, A. A. Kalinin, B. T. Do, G. P. Way, E. Ferrero, P.-M. Agapow, M. Zietz, M. M. Hoffman *et al.*, "Opportunities and obstacles for deep learning in biology and medicine," *Journal of The Royal Society Interface*, vol. 15, no. 141, p. 20170387, 2018.

[60] Y. Gal and Z. Ghahramani, "Dropout as a bayesian approximation: Representing model uncertainty in deep learning," in *international conference on machine learning*, 2016, pp. 1050–1059.

[61] Q. Liu and D. Wang, "Stein variational gradient descent: A general purpose bayesian inference algorithm," in *Advances in Neural Information Processing Systems 29*, D. D. Lee, M. Sugiyama, U. V. Luxburg, I. Guyon, and R. Garnett, Eds. Curran Associates, Inc., 2016, pp. 2378–2386. [Online]. Available: http://papers.nips.cc/paper/6338-stein-variational-gradient-descent-a-general-purpose-bayesian-inference-algorithm.pdf

[62] Y. Bengio, P. Lamblin, D. Popovici, and H. Larochelle, "Greedy layer-wise training of deep networks," in *Advances in Neural Information Processing Systems 19*, B. Schölkopf, J. C. Platt, and T. Hoffman, Eds. MIT Press, 2007, pp. 153–160. [Online]. Available: http://papers.nips.cc/paper/3048-greedy-layer-wise-training-of-deep-networks.pdf

[63] J. Yu, C. Hong, Y. Rui, and D. Tao, "Multitask autoencoder model for recovering human poses," *IEEE Transactions on Industrial Electronics*, vol. 65, pp. 5060–5068, June 2018.

[64] J. Xu, L. Xiang, Q. Liu, H. Gilmore, J. Wu, J. Tang, and A. Madabhushi, "Stacked sparse autoencoder (ssae) for nuclei detection on breast cancer histopathology images," *IEEE Transactions on Medical Imaging*, vol. 35, no. 1, pp. 119–130, Jan 2016.

[65] J. Martens and I. Sutskever, "Learning recurrent neural networks with hessian-free optimization," in *Proceedings of the 28th International Conference on International Conference on Machine Learning*, ser. ICML'11. USA: Omnipress, 2011, pp. 1033–1040. [Online]. Available: http://dl.acm.org/citation.cfm?id=3104482.3104612

[66] Y. Liao, L. Song, Z. Han, and Y. Li, "Full duplex cognitive radio: a new design paradigm for enhancing spectrum usage," *IEEE Communications Magazine*, vol. 53, no. 5, pp. 138–145, May 2015.

[67] D. Bharadia, E. McMilin, and S. Katti, "Full duplex radios," *ACM SIGCOMM Computer Communication Review*, vol. 43.

[68] Z. Zhang, X. Chai, K. Long, A. V. Vasilakos, and L. Hanzo, "Full duplex techniques for 5g networks: self-interference cancellation, protocol design, and relay selection," *IEEE Communications Magazine*, vol. 53, no. 5, pp. 128–137, May 2015.

[69] S. Hong, J. Brand, J. I. Choi, M. Jain, J. Mehlman, S. Katti, and P. Levis, "Applications of self-interference cancellation in 5g and beyond," *IEEE Communications Magazine*, vol. 52, no. 2, pp. 114–121, February 2014.

[70] T. Riihonen, S. Werner, and R. Wichman, "Mitigation of loopback self-interference in full-duplex mimo relays," *IEEE Transactions on Signal Processing*, vol. 59, no. 12, pp. 5983–5993, Dec 2011.

[71] M. Jain, J. I. Choi, T. Kim, D. Bharadia, S. Seth, K. Srinivasan, P. Levis, S. Katti, and P. Sinha, "Practical, real-time, full duplex wireless," in *Proceedings of the 17th annual international conference on Mobile computing and networking (MobiCom)*. ACM, 2011, pp. 301–312.

[72] A. Sabharwal, P. Schniter, D. Guo, D. W. Bliss, S. Rangarajan, and R. Wichman, "In-band full-duplex wireless: Challenges and opportunities," *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 9, pp. 1637–1652, Sep. 2014.

[73] J. I. Choi, M. Jain, K. Srinivasan, P. Levis, and S. Katti, "Achieving single channel, full duplex wireless communication," in *Proceedings of the sixteenth annual international conference on Mobile computing and networking (MobiCom)*. ACM, 2010, pp. 1–12.

[74] C. Politis, S. Maleki, C. G. Tsinos, K. P. Liolis, S. Chatzinotas, and B. Ottersten, "Simultaneous sensing and transmission for cognitive radios with imperfect signal cancellation," *IEEE Transactions on Wireless Communications*, vol. 16, no. 9, pp. 5599–5615, Sep. 2017.

[75] G. Zheng, I. Krikidis, and B. o. Ottersten, "Full-duplex cooperative cognitive radio with transmit imperfections," *IEEE Transactions on Wireless Communications*, vol. 12, no. 5, pp. 2498–2511, May 2013.

[76] T. Riihonen and R. Wichman, "Energy detection in full-duplex cognitive radios under residual self-interference," in *2014 9th International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CROWNCOM)*, June 2014, pp. 57–60.

[77] W. Afifi and M. Krunz, "Exploiting self-interference suppression for improved spectrum awareness/efficiency in cognitive radio systems," in *2013 Proceedings IEEE INFOCOM*, April 2013, pp. 1258–1266.

[78] ——, "Adaptive transmission-reception-sensing strategy for cognitive radios with full-duplex capabilities," in *2014 IEEE International Symposium on Dynamic Spectrum Access Networks (DYSPAN)*, April 2014, pp. 149–160.

[79] S. Dikmese, Z. Ilyas, P. C. Sofotasios, M. Renfors, and M. Valkama, "Sparse frequency domain spectrum sensing and sharing based on cyclic prefix

autocorrelation," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 1, pp. 159–172, Jan 2017.

[80] A. Osseiran, F. Boccardi, V. Braun, K. Kusume, P. Marsch, M. Maternia, O. Queseth, M. Schellmann, H. Schotten, H. Taoka *et al.*, "Scenarios for 5g mobile and wireless communications: the vision of the metis project," *IEEE Communications Magazine*, vol. 52, no. 5, pp. 26–35, 2014.

[81] Q. Zhao and B. M. Sadler, "A survey of dynamic spectrum access," *IEEE signal processing magazine*, vol. 24, no. 3, pp. 79–89, 2007.

[82] I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, and S. Mohanty, "Next generation/dynamic spectrum access/cognitive radio wireless networks: A survey," *Computer Networks*, vol. 50, no. 13, pp. 2127 – 2159, 2006.

[83] NTIA, "Assessment of the near-term viability of accommodating wireless broadband systems in the 1675-1710 mhz, 1755-1780 mhz, 3500-3650 mhz, 4200-4220 mhz, and 4380-4400 mhz bands," 2010.

[84] T. Institute, "Mobile broadband services in the 2300-2400 mhz frequency band under licensed shared access regime," *France: ETSI*, vol. V1.1.1, 2013.

[85] M. B. Weiss, W. H. Lehr, A. Acker, and M. M. Gomez, "Socio-technical considerations for spectrum access system (sas) design," in *Dynamic Spectrum Access Networks (DySPAN), 2015 IEEE International Symposium on.* IEEE, 2015, pp. 35–46.

[86] P. Zhou, W. Wei, K. Bian, D. O. Wu, Y. Hu, and Q. Wang, "Private and truthful aggregative game for large-scale spectrum sharing," *IEEE Journal on Selected Areas in Communications*, vol. PP, no. 99, pp. 1–1, 2017.

[87] Z. Qin, S. Yi, Q. Li, and D. Zamkov, "Preserving secondary users' privacy in cognitive radio networks," in *IEEE INFOCOM 2014 - IEEE Conference on Computer Communications*, April 2014, pp. 772–780.

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

[89] M. Clark and K. Psounis, "Can the privacy of primary networks in shared spectrum be protected?" in *IEEE INFOCOM 2016 - The 35th Annual IEEE International Conference on Computer Communications*, 2016.

[90] Z. Gao, H. Zhu, Y. Liu, M. Li, and Z. Cao, "Location privacy in database-driven cognitive radio networks: Attacks and countermeasures," in *2013 Proceedings IEEE INFOCOM*, April 2013, pp. 2751–2759.

[91] B. Gedik and L. Liu, "Protecting location privacy with personalized k-anonymity: Architecture and algorithms," *IEEE Transactions on Mobile Computing*, vol. 7, no. 1, pp. 1–18, Jan 2008.

[92] B. Bahrak, S. Bhattarai, A. Ullah, J. M. J. Park, J. Reed, and D. Gurney, "Protecting the primary users' operational privacy in spectrum sharing," in *2014 IEEE International Symposium on Dynamic Spectrum Access Networks (DYSPAN)*, April 2014, pp. 236–247.

[93] J. Liu, C. Zhang, H. Ding, H. Yue, and Y. Fang, "Policy-based privacy-preserving scheme for primary users in database-driven cognitive radio networks," in *2016 IEEE Global Communications Conference (GLOBECOM)*, Dec 2016, pp. 1–6.

[94] Y. Dou, K. Zeng, H. Li, Y. Yang, B. Gao, K. Ren, and S. Li, "p^2 -sas: Privacy-preserving centralized dynamic spectrum access system," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 1, pp. 173–187, Jan 2017.

[95] W. Wang, L. Chen, K. G. Shin, and L. Duan, "Secure cooperative spectrum sensing and access against intelligent malicious behaviors," in *INFOCOM, 2014 Proceedings IEEE*. IEEE, 2014, pp. 1267–1275.

[96] R. K. Sharma and D. B. Rawat, "Advances on security threats and countermeasures for cognitive radio networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 2, pp. 1023–1043, 2015.

[97] Y. Chen, Z. Lin, X. Zhao, G. Wang, and Y. Gu, "Deep learning-based classification of hyperspectral data," *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*, vol. 7, no. 6, pp. 2094–2107, June 2014.

[98] Y. Bengio, "Learning deep architectures for ai," *Foundations and Trends in Machine Learning*, vol. 2, pp. 1–127, 2009.

[99] P. Planini and D. Gleich, "Temporal change detection in SAR images using log cumulants and stacked autoencoder," *IEEE Geoscience and Remote Sensing Letters*, vol. 15, no. 2, pp. 297–301, Feb 2018.

[100] B. Matter, *Iterative Methods for Optimization*, pp. 161–180. [Online]. Available: http://epubs.siam.org/doi/abs/10.1137/1.9781611970920.bm

[101] M. Khodadadzadeh, J. Li, A. Plaza, H. Ghassemian, J. M. Bioucas-Dias, and X. Li, "Spectral-spatial classification of hyperspectral data using local and global probabilities for mixed pixel characterization," *IEEE Transactions on Geoscience and Remote Sensing*, vol. 52, no. 10, pp. 6298–6314, Oct 2014.

[102] C. Molnar, *Interpretable Machine Learning*, 2019, https://christophm.github.io/interpretable-ml-book/.

[103] H. Byun and S.-W. Lee, "Applications of support vector machines for pattern recognition: A survey," in *International Workshop on Support Vector Machines*. Springer, 2002, pp. 213–236.

[104] C. Hong, J. Yu, J. Wan, D. Tao, and M. Wang, "Multimodal deep autoencoder for human pose recovery," *IEEE Transactions on Image Processing*, vol. 24, no. 12, pp. 5659–5670, Dec 2015.

[105] E. Visotsky, S. Kuffner, and R. Peterson, "On collaborative detection of tv transmissions in support of dynamic spectrum sharing," in *First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005.*, Nov 2005, pp. 338–345.

[106] FCC, "Unlicensed operation in the tv broadcast bands, final rules," Jun. 2010. [Online]. Available: https://www.govinfo.gov/content/pkg/FR-2010-12-06/pdf/2010-30184.pdf

[107] ——, "Spectrum policy task force," Nov. 2002. [Online]. Available: https://www.fcc.gov/document/spectrum-policy-task-force

[108] NTIA, "Spectrum monitoring pilot program," *National Telecommunications and Information Administration*, Aug. 2013.

[109] FCC, "Before the federal communications commission, second memorandum opinion and order," 2010. [Online]. Available: https://docs.fcc.gov/public/attachments/FCC-10-174A1.pdf

[110] M. Baghani, A. Mohammadi, M. Majidi, and M. Valkama, "Analysis and rate optimization of OFDM-based cognitive radio networks under power amplifier nonlinearity," *IEEE Transactions on Communications*, vol. 62, no. 10, pp. 3410–3419, Oct 2014.

[111] J. Zhang and Y. Wu, "Likelihood-ratio tests for normality," *Computational Statistics and Data Analysis*, vol. 49, no. 3, pp. 709–721, 2005.

[112] G. Huang, Z. Liu, L. van der Maaten, and K. Q. Weinberger, "Densely connected convolutional networks," in *The IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, July 2017.

[113] S. Y. Tu, K. C. Chen, and R. Prasad, "Spectrum sensing of ofdma systems for cognitive radio networks," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 7, pp. 3410–3425, Sept 2009.

[114] H. Chen, W. Gao, and D. G. Daut, "Spectrum sensing for ofdm systems employing pilot tones," *IEEE Transactions on Wireless Communications*, vol. 8, no. 12, pp. 5862–5870, December 2009.

[115] Z. Lei and F. P. S. Chin, "Sensing ofdm systems under frequency-selective fading channels," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 4, pp. 1960–1968, May 2010.

[116] E. Ahmed and A. M. Eltawil, "All-digital self-interference cancellation technique for full-duplex systems," *IEEE Transactions on Wireless Communications*, vol. 14, no. 7, pp. 3519–3532, July 2015.

[117] X. Zhou and H. Zheng, "Trust: A general framework for truthful double spectrum auctions," in *IEEE INFOCOM 2009*, April 2009, pp. 999–1007.

[118] F. Wu and N. Vaidya, "A strategy-proof radio spectrum auction mechanism in noncooperative wireless networks," *IEEE Transactions on Mobile Computing*, vol. 12, no. 5, pp. 885–894, May 2013.

[119] X. Feng, Y. Chen, J. Zhang, Q. Zhang, and B. Li, "Tahes: A truthful double auction mechanism for heterogeneous spectrums," *IEEE Transactions on Wireless Communications*, vol. 11, no. 11, 2012.

[120] M. R. Hassan, G. Karmakar, and J. Kamruzzaman, "Reputation and user requirement based price modeling for dynamic spectrum access," *IEEE Transactions on Mobile Computing*, vol. 13, no. 9, pp. 2128–2140, 2014.

[121] FCC, "Report and order and second further notice of proposed rulemaking," *Federal Communication Commission*, April 2015.

[122] K. Chamberlin and R. Luebbers, "An evaluation of longley-rice and gtd propagation models," *IEEE Transactions on Antennas and Propagation*, vol. 30, no. 6, pp. 1093–1098, 1982.

[123] PCAST, "Report to the president realizing the full potential of government-held spectrum to spur economic growth," 2012.

[124] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 1999, pp. 223–238.

[125] M. Cotton and R. Dalke, "Spectrum occupancy measurements of the 3550 3650 mhz maritime radar band near san diego, ca," NTIA Report TR-14-500, 2014.

[126] A. Nika, Z. Li, Y. Zhu, Y. Zhu, B. Y. Zhao, X. Zhou, and H. Zheng, "Empirical validation of commodity spectrum monitoring," in *Proceedings of the 14th ACM Conference on Embedded Network Sensor Systems CD-ROM*, ser. SenSys '16, 2016, pp. 96–108.

[127] L. Yang, Z. Zhang, B. Y. Zhao, C. Kruegel, and H. Zheng, "Enforcing dynamic spectrum access with spectrum permits," in *Proceedings of the Thirteenth ACM International Symposium on Mobile Ad Hoc Networking and Computing*, ser. MobiHoc '12, 2012, pp. 195–204.

[128] J. Park, J. H. Reed, A. A. Beex, T. C. Clancy, V. Kumar, and B. Bahrak, "Security and enforcement in spectrum sharing," *Proceedings of the IEEE*, vol. 102, no. 3, pp. 270–281, March 2014.

[129] E. L. Lawler and D. E. Wood, "Branch-and-bound methods: A survey," *Operations research*, vol. 14, no. 4, pp. 699–719, 1966.

[130] FCC, "Amendment of the commission rules with regard to commercial operations in the 3550 - 3650 mhz band, federal communications commission," *Federal Communication Commission*, September 2015.

[131] T. Granlund *et al.*, *GNU MP 6.0 Multiple Precision Arithmetic Library*. Samurai Media Limited, 2015.

[132] *Longley-Rice Methodology for Evaluating TV Coverage and Interference*, document FCC 69, Office of Eng. and Technol. (OET) Bulletin, 2004.

[133] *http://www.qsl.net/kd2bd/splat.html*.

[134] $http://dds.cr.usgs.gov/srtm/version2_1/SRTM3/North_America/$.

[135] R. Shokri, G. Theodorakopoulos, J. L. Boudec, and J. Hubaux, "Quantifying location privacy," in *2011 IEEE Symposium on Security and Privacy*, 2011.

[136] J. Kim, Y. Shin, T. W. Ban, and R. Schober, "Effect of spectrum sensing reliability on the capacity of multiuser uplink cognitive radio systems," *IEEE Transactions on Vehicular Technology*, vol. 60, no. 9, 2011.