OPPORTUNISTIC ACCESS OF NONCONTIGUOUS SPECTRUM

By

RATNESH KUMBHKAR

A dissertation submitted to the

School of Graduate Studies

Rutgers, The State University of New Jersey

In partial fulfillment of the requirements

For the degree of

Doctor of Philosophy

Graduate Program in Electrical and Computer Engineering

Written under the direction of

Narayan B. Mandayam

And approved by

_____

_____

_____

_____

New Brunswick, New Jersey

JANUARY, 2018

ABSTRACT OF THE DISSERTATION

Opportunistic Access of Noncontiguous Spectrum

By RATNESH KUMBHKAR

Dissertation Director:

Narayan B. Mandayam

The world is getting more and more connected. Other than traditional telecommunication applications such as cellular communication and wireless broadband, many new technologies such as the Internet of things (IoT) and automotive vehicles are using wireless spectrum to establish the connection to the network. With these increasing number of devices, the data rate requirements are increasing enormously, which in turn, necessitate a more efficient utilization of available resources. In an effort to enable higher productive utilization of the available spectrum, the Federal Communications Commission (FCC) has recently opened up many spectrum bands such TV white space, 3.5 GHz Citizen Broadband Radio Service (CBRS) band and 5 GHz The Unlicensed National Information Infrastructure (U-NII) band among others for commercial, unlicensed and shared access. This has led to various innovations in cognitive radio technology, coexistence mechanism among heterogeneous technologies, spectrum sensing as well as novel proposals for dynamic spectrum access. Over a large part of the last decade, there has been a tremendous amount of research on spectrum policy as well as the theory and practice of cognitive radio networks including dynamic spectrum access (DSA) algorithms, networking protocols, and software radio platform development. Generally, the available spectrum to the users in a cognitive environment is not always contiguous and becomes fragmented due to either the presence of primary users or other secondary users. In this thesis, we specifically study the opportunity and challenges associated with the access of such fragmented spectrum.

This thesis first presents the problem of spectrum allocation for cases when the available spectrum is fragmented. As an example, the problem of allocating TV white-space to provide wireless backhaul communication is presented. In the second part of this thesis, the NC-OFDM based communication is introduced as a technique for agile and flexible access to a fragmented spectrum. The advantages of using NC-OFDM for spectrum allocation in a power constrained system are highlighted. In the latter part of the thesis, the challenges associated with the implementation of an NC-OFDM based communication system are discussed. Synchronization among different transmissions, and a separate control channel to enable frequency and time offset calculations are identified as two of the main challenges. The performance results are presented for an NC-OFDM-enabled asynchronous network, and solutions are provided to address this issue. A low-powered underlay channel is designed to help the NC-OFDM-enabled system in the transmission of control information, and frequency and time offset estimation. At last, a physical layer security analysis of NC-OFDM is presented for a low probability of exploitation (LPE) design.

Acknowledgements

I wish to thank Prof. Narayan B. Mandayam for all his guidance and support throughout my five years at WINLAB, Rutgers University. His encouragement during different stages of my Ph.D. gave me the opportunity to explore different fields in the wireless communication.

I am grateful for the support I have received at WINLAB, specifically from Ivan Šeškar, whose insight and passion into everything wireless has made me immensely appreciate this field. I also thank Dr. Gokul Sridharan for many helpful discussions without which a lot of my work would have remained unfinished. I am thankful to my labmates for making WINLAB feel like a second home. I thank Prof. Dipankar Raychaudhuri, Prof. Roy Yates and Dr. Sastry Kompella for being on my dissertation defense committee.

Lastly, I thank my parents Shivram Kumbhkar and Mamta Kumbhkar, and my sister Rashmi for all the love and support during the toughest of times.

This work is supported in part by a grant from the U.S. Office of Naval Research (ONR) under grant number N00014-15-1-2168. I am really thankful for the funding.

Dedication

To my parents.

Table of Contents

List of Tables

List of Figures

Chapter 1

Introduction

In the last few years, the number of devices that use the wireless medium to connect to a network has increased drastically. Applications such as Cellular communication, Mobile wireless broadband, Internet of things, Vehicular communication and Wireless backhaul among many others, have contributed to this growth. It is expected that this number will continue to increase with time, and therefore, the availability of the wireless spectrum to support this increase is a concern. One possible solution for this increasing spectrum requirement and higher throughput requirements is to utilize higher frequencies such as mmWave which is seen as one of the enabling technology for the future wireless broadband communication system. Another approach is the efficient utilization of the spectrum-bands which are already in use. The Federal Communications Commission (FCC) has recently reported that the current license spectrum is often underutilized [2]. One such example is the spectrum allocated for TV broadcasting which might be left unused in underpopulated areas. This unused TV spectrum is generally referred to as TV white space. In order to better use these underutilized bands the FCC is opening up previously licensed spectrum such as TV white spaces or Military radar bands for unlicensed use [3], and similarly, previously unlicensed spectrum are being opened to the licensed operator to provide additional throughput e.g. 5 GHz for LTE-unlicensed (LTE-U) [4] and LTE Licensed-Assisted-Access (LTE-LAA) [5]. The first scenario requires that the incoming technology accesses the spectrum as a secondary user (SU) while giving priority to the incumbent users e.g. radar, satellites or TV channels, which are referred as primary users (PU). The second scenario requires that the incoming technology (e.g. LTE-U or LTE-LAA) coexist with incumbent technology (e.g. WiFi) in a fair manner.

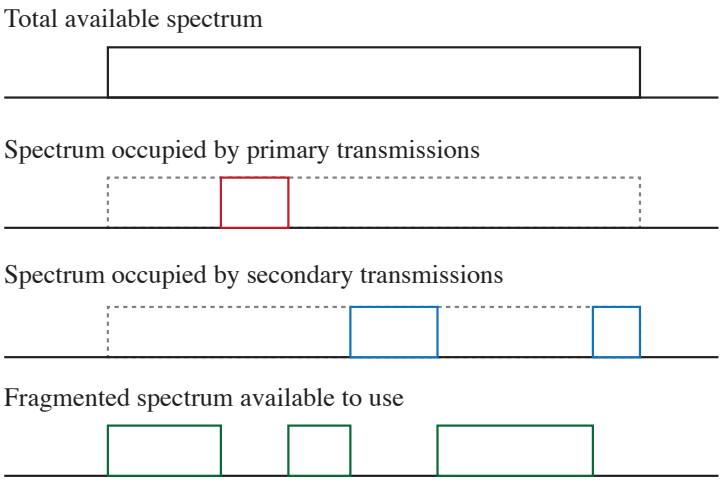


Figure 1.1: Fragmentation of spectrum.

1.1 Fragmentation of spectrum

The requirements emerging from the presented scenarios have led to many innovations in cognitive radio technology, spectrum sensing as well as novel designs for dynamic spectrum access. Over a good part of the last decade, there has been a tremendous amount of research on spectrum policy as well as the theory and practice of cognitive radio networks including dynamic spectrum access (DSA) algorithms, networking protocols and software radio platform development [6–15]. Note that the available spectrum in both of the presented scenarios becomes noncontiguous and has sporadic availability due to possibly time-varying access of spectrum by the PUs. This fragmented and intermittent availability of the spectrum demands an agile and flexible waveform for transmission. One basic requirement for such transmission is multicarrier design, which can potentially enable selective use of available spectrum. Next, we are going to discuss some multicarrier transmissions and challenges associated with them.

1.2 Challenges Associated Access of Noncontiguous Spectrum

Various multicarrier transmission methods such as Noncontiguous Orthogonal Frequency Division Multiplexing (NC-OFDM), Filter bank multicarrier (FBMC), Generalized Frequency Division Multiplexing (GFDM) and Universal Filtered Multi-Carrier (UFMC) are some multicarrier transmission methods which have been proposed to

efficiently utilize the fragmented spectrum [16–22]. NC-OFDM is one such method of transmission where some of the subcarriers in a regular OFDM transmission are nulled, and the remaining subcarriers are used for communication. Since NC-OFDM is an OFDM-based technology, it incorporates the advantages and disadvantages associated with an OFDM based transmission. It uses FFT based transceiver which can be very efficiently implemented. At the receiver, the channel equalization is trivial, since each channel appears to be flat even when the channel is frequency selective, therefore it can utilize one tap equalization to recover the symbol. FBMC is another such multi-carrier modulation scheme which uses filter bank approach, however, unlike NC-OFDM it does not require the orthogonality between all its subcarriers but only between neighboring subcarriers. This change in design is intended to reduce out-of-band transmission, however, to enable such design the transmitters/receivers need significant changes compared to an OFDM-based system and require higher digital signal processing complexity. UFMC and GFDM are also multi-carrier systems, which digitally implement the filter bank approach with some variations [20, 21]. However, they also impose increased transceiver complexity compared to NC-OFDM.

Noncontiguous orthogonal frequency division multiplexing allows agile access to the fragmented spectrum. An NC-OFDM transmission can be achieved by selectively disabling use of some of the subcarriers in a regular OFDM transmission. While NC-OFDM possesses some of the advantages associated with the OFDM such as efficient FFT-based design and one-tap equalization, it also introduces new challenges due to synchronization and control channel. Before we go into details of NC-OFDM we present a brief overview of OFDM.

1.3 Brief overview of OFDM

OFDM has been playing a very significant role in modern telecommunication, ranging from 802.11 WiFi systems to enabling current LTE systems. OFDM has evolved as a natural extension of multiplexing technique known as Frequency Division Multiplexing (FDM). FDM allows multiple signals to be transmitted simultaneously over multiple

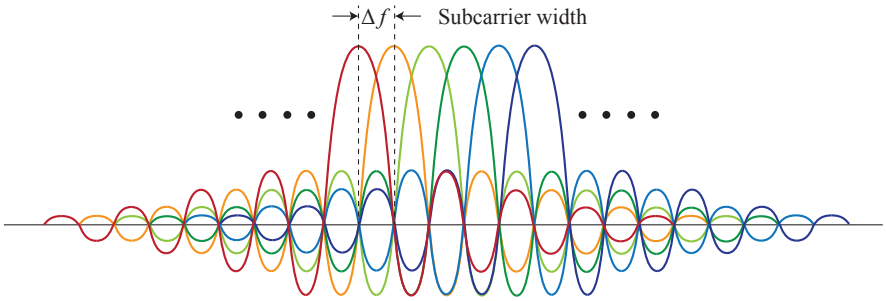


Figure 1.2: Representation of OFDM subcarriers.

subchannels. However, FDM suffered from the drawback that it required very complex receiver design to demodulate the signal from different subchannels and, it used the available spectrum very inefficiently due to the requirement of guardbands between subchannels. OFDM is a multi-carrier modulation technique where the signal is transmitted in closely spaced multiple orthogonal subcarriers and it addresses the problems encountered by the FDM. To alleviate the problem of using guardbands the OFDM allows the subcarriers to overlap as long as the orthogonality is maintained as shown in Fig. 1.2, which enables more efficient use of available spectrum. The orthogonality among OFDM subcarrier is achieved by keeping the subcarrier spacing to be the reciprocal of the symbol period. OFDM uses Inverse Discrete Fourier Transform (IDFT) to generate orthogonal waveforms and in practice, the IDFT is calculated using Fast Fourier Transform (FFT) algorithm. The OFDM transmission also makes the receiver design simple since the signal can be recovered by calculating the DFT and performing one-tap equalization. Most OFDM based systems such as LTE or WiFi use the cyclic prefix (CP) to counter intersymbol interference. A generic representation of OFDM transmitter-receiver is depicted in Fig. 1.3.

1.3.1 Representation of OFDM Signal

The baseband representation of the OFDM signal at a transmitter can be written as

$$s(t) = \sum_{l=0}^{\infty} \sum_{n \in \mathcal{N}} d_{ln}\, e^{j2\pi f_n (t - lT)} \mathrm{rect}\left(\tfrac{t-lT}{T}\right), \tag{1.1}$$

where d_{ln} is the data symbol to be transmitted, f_n is the center frequency for the nth subcarrier, and rect$(\cdot)$ represents the rectangular function that is 1 in the unit interval

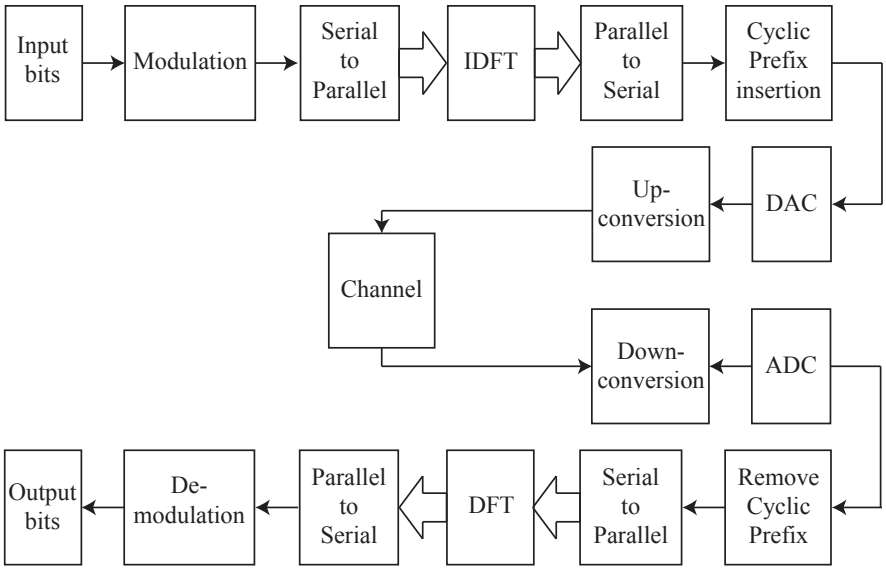


Figure 1.3: Generic block diagram of OFDM-based system.

and 0 elsewhere. $\mathcal{N}$ represents set of all subcarriers used and T denotes the overall duration of one OFDM symbol, including the cyclic prefix. We assume that a cyclic prefix of length N_{cp} is used. At the receiver, assuming a constant flat fading channel, after downconversion and accounting for frequency offset, the OFDM signal can be represented as $he^{j2\pi(\delta f)t}s(t)$, where h is the channel fading coefficient and δf is the frequency offset. When this signal is sampled at a rate of $1/T_s$, it can be written as

$$r[m] = he^{j2\pi(\delta f)(mT_s+\phi)}s(mT_s+\phi) \tag{1.2}$$

where $r[m]$ denotes the contribution of $s(t)$ to the mth sample of received signal $r(t)$, ϕ ($< T_s$) is the phase offset and (δf) is the frequency offset. We also assume that the sampling rate $T_s = T/(N + N_{cp}) = 1/B$, where B is the bandwidth of the signal.

1.3.2 Challenges associated with OFDM

Successful decoding of OFDM symbols relies on the orthogonality of the subcarriers. However, this synchronization can be lost either due to frequency offset or due to the timing offset between the transmitter and receiver. Therefore the symbol and carrier synchronization requirements for the OFDM are very strict. If timing offset becomes larger than the cyclic prefix length then orthogonality is lost between the subcarrier and Inter-carrier-interference (ICI) can be observed. Similarly, if the frequency offset

caused by the difference in oscillator frequencies of transmitter and receiver, is large enough, not only it reduces the signal strength it also introduces ICI.

Another major problem associated with OFDM is of peak to average power ratio (PAPR). PAPR results from the coherent addition of symbols in OFDM subcarriers. This peak power resulted from coherent summation can cause the power amplifiers to saturate and cause the disturbance in the system.

1.4 Noncontiguous OFDM

With the ever-increasing requirement for higher wireless data rates, efficient utilization of all available spectrum, licensed or otherwise, becomes paramount. In particular, with the wide availability of unlicensed spectrum in the TV-white-space band, the U-NII and ISM bands, and the requirement for dynamic frequency selection (DFS) to avoid interference with radar or other ISM devices, the ability to effectively use noncontiguous spectrum is vital to exploit the full potential of the available spectrum. Cognitive radios (CRs) enabled with noncontiguous-OFDM (NC-OFDM) [16, 23–25] are ideally suited to operate under such conditions as they permit dynamic spectrum access even when the available spectrum is fragmented. NC-OFDM is similar to OFDM, except that transmission on certain subcarriers is not permitted depending on the availability of the corresponding spectrum as highlighted in Fig.1.4. It should be noted that OFDM is used to provide multiple access to multiple users in LTE downlink and this method is referred as Orthogonal Frequency Division Multiple Access (OFDMA). However, this multiplexing is performed by the eNodeB and therefore does not suffer from any issues associated with the synchronization errors between different subcarriers.

Although NC-OFDM is similar to OFDM, there are significant challenges that emerge when using NC-OFDM in the presence of concurrent transmissions [17, 26–30], with timing (to identify the start of an NC-OFDM frame) and frequency offset recovery being one among them. When a p2p cognitive link uses NC-OFDM, the receiver of this link sees the aggregate of the desired NC-OFDM signal along with all the other concurrent transmissions. Due to the dynamic nature of this interference, it is not

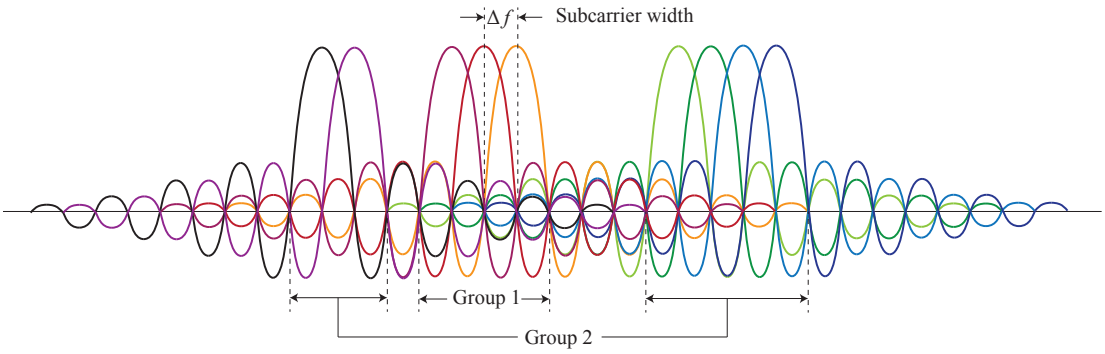


Figure 1.4: Representation of NC-OFDM subcarriers for two different transmissions.

always possible to filter these transmissions out. Under such circumstances, traditional techniques for OFDM timing recovery that rely on some form of symmetry in the time domain waveform [31–34] are no longer reliable. Although techniques involving custom preamble design for NC-OFDM are available [35], they are not well suited to be applied in dynamic environments.

1.4.1 NC-OFDM Signal Representation

The baseband representation of the NC-OFDM signal at the kth transmitter can be written as

$$s_k(t) = \sum_{l=0}^{\infty} \sum_{n \in \mathcal{N}_i} d_{kln}\ e^{j2\pi f_n (t-lT)} \mathrm{rect}\left(\frac{t-lT}{T}\right), \tag{1.3}$$

where d_{kln} is the data symbol to be transmitted, f_n is the center frequency for the nth subcarrier, and rect$(\cdot)$ represents the rectangular function that is 1 in the unit interval and 0 elsewhere. T denotes the overall duration of one NC-OFDM signal, including the cyclic prefix. We assume that a cyclic prefix of length N_{cp} is used at each link. At the receiver, assuming a constant flat fading channel, after downconversion and accounting for frequency offset, the kth NC-OFDM signal can be represented as $h_k e^{j2\pi(\delta f_k)t} s_k(t)$, where h_k is the channel fading coefficient and δf_k is the frequency offset. When this signal is sampled at a rate of $1/T_s$, it can be written as

$$r_{i(s_k)}[m] = h_k e^{j2\pi(\delta f_k)(mT_s+\phi_k)} s_k(mT_s + \phi_k) \tag{1.4}$$

where $r_{i(s_k)}[m]$ denotes the contribution of $s_k(t)$ to the mth sample of $r_i(t)$, ϕ_k ($< T_s$) is the phase offset and (δf_k) is the frequency offset. Note that the K NC-OFDM signals are not assumed to be synchronized. Similar to OFDM we assume that the sampling rate $T_s = T/(N + N_{cp}) = 1/B$. We use similar notations in coming chapters for all NC-OFDM related analyses.

In coming chapters, we discuss some of the challenges associated with the implementation of NC-OFDM and provide solutions for corresponding issues.

1.5 Summary of Specific Contributions of the Dissertation

1.5.1 Included publications

This dissertation contains results from the following list of publications, which have addressed different aspects of noncontiguous spectrum access.

Paper 1: Spectrum Allocation for Backhaul using TV White Space [24]
The penetration of wireless broadband services in remote areas has primarily been limited due to the lack of economic incentives that service providers encounter in sparsely populated areas. Besides, wireless backhaul links like satellite and microwave are either expensive or require strict line of sight communication making them unattractive. TV white space channels with their desirable radio propagation characteristics can provide an excellent alternative for engineering backhaul networks in areas that lack abundant infrastructure. Specifically, TV white space channels can provide "free wireless backhaul pipes" to transport aggregated traffic from broadband sources to fiber access points. We investigate the feasibility of multi-hop wireless backhaul in the available white space channels by using noncontiguous Orthogonal Frequency Division Multiple Access (NC-OFDMA) transmissions between fixed backhaul towers. Specifically, we consider joint power control, scheduling and routing strategies to maximize the minimum rate across broadband towers in the network. Depending on the population density and traffic demands of the location under consideration, we discuss the suitable choice of cell size for the backhaul network. Using the example of available TV white space channels

in Wichita, Kansas (a small city located in the central USA), we provide illustrative numerical examples for designing such wireless backhaul network.

Paper 2: Opportunistic Spectrum Allocation for Max-Min Rate in NC-OFDMA [25]

We study the problem of fair spectrum allocation across multiple NC-OFDM-enabled, point-to-point cognitive radio links under certain practical considerations that arise from such noncontiguous access. When using NC-OFDM, the channels allocated to a cognitive radio link are spread across several disjoint frequency bands leading to a large *spectrum span* for that link. Increased spectrum span requires higher sampling rates, leading to increased power consumption in the ADC/DAC of the transmit/receive nodes. In this context, we propose a framework for spectrum allocation that maximizes the minimum rate achieved by the cognitive radio links, under a constraint on the maximum permissible spectrum span. For constant transmit powers and orthogonal spectrum allocation, such an optimization is an integer linear program and can be solved efficiently. There exists a clear trade-off between the max-min rate achieved and the maximum permissible spectrum span. The spectrum allocation obtained from the proposed optimization framework is shown to be close to the trade-off boundary, thus showing the effectiveness of the proposed technique. We find that it is possible to limit the spectrum span without incurring a significant penalty on the max-min rate under different interference environments. We also discuss an experimental evaluation of the techniques developed here using the ORBIT radio-network testbed that consists of multiple Universal Software Radio Peripherals (USRPs).

Paper 3: Impact of Asynchronous Transmissions in Noncontiguous OFDMA [36]

In this paper, we consider multiple point-to-point (p2p) communication links that share noncontiguously available spectrum via noncontiguous orthogonal frequency division multiple access (NC-OFDMA). NC-OFDMA divides the spectrum into orthogonal subcarriers and assigns nonoverlapping subsets of these subcarriers to each of the links.

Such a setup is motivated by the need for dynamic and opportunistic access to a large pool of spectrum that is fragmented due to the presence of incumbent transmissions. The transmissions of the p2p links are assumed to be asynchronous, i.e., the start and end of the NC-OFDM symbol are not time synchronized across the links. In such a setting, we study the inter-carrier-interference (ICI) arising from the loss of orthogonality between the subcarriers due to (a) the asynchronous nature of the communications and (b) the frequency offset between the links. An analytical characterization of this ICI reveals that in the absence of transmit power control, the impact of this ICI can be severe enough to disable the concurrent transmissions of the other p2p links. Experimental results using a Universal Software Radio Peripheral (USRP) platform validate our analysis and show that the negative effects of asynchronous transmission which are particularly significant at high SNR. To remedy this, a decentralized synchronization scheme is presented wherein beacons appended to the transmitted signal are used to enable timing coordination between two NC-OFDM links, thereby eliminating the ICI resulting from asynchronous transmission. The effectiveness of such a scheme is validated using experiments. In cases where such timing coordination cannot be enabled, our analysis is then used to provide guidelines on the choice of basic system parameters for the p2p links such as the number of contiguous subcarriers to be allocated to a link and length of guard band and range of operating SNRs to mitigate the effect of asynchronous NC-OFDM transmission.

Paper 4: Design and Implementation of an Underlay Control Channel for NC-OFDM-based Networks [37]

In this paper, we study the design of an underlay control channel for noncontiguous-OFDM-based cognitive networks. Noncontiguous OFDM (NC-OFDM) provides a fast and flexible manner of accessing disjoint parts of the spectrum and is ideally suited for dynamic spectrum access. While similar to OFDM, NC-OFDM explicitly restricts transmission to only certain subcarriers that are free of incumbent transmissions. In particular, we consider designing a control channel for a cognitive network consisting of

multiple point-to-point (p2p) links that operate over a wide bandwidth that might encompass some primary transmissions. In such a scenario, control channel becomes vital not only to share basic transmission parameters but also to aid timing and frequency recovery of NC-OFDM transmission; a nontrivial problem in itself. The proposed design is a low-power underlay transmission that spans the entire bandwidth regardless of any incumbent transmissions and uses direct sequence spread spectrum (DSSS). The control channel operates in one of two modes. The first mode aids timing and frequency recovery through a two-step process, while the second mode is used for control data transmission. To enable multiple access, the p2p links use orthogonal pseudo-noise (PN) sequences. The proposed control channel is implemented on USRPs in the ORBIT testbed using GNU Radio. Experimental results suggest robust timing and frequency offset recovery even in the presence of concurrent primary transmissions and support for about 10 to 20kbps over a 1 MHz bandwidth at an uncoded symbol-error-rate of about 10^{-2} under typical operating conditions.

Paper 5: Physical-layer Security of NC-OFDM-based Systems [38]

This paper examines the low-probability-of-exploitation (LPE) characteristics of a non-contiguous orthogonal frequency division multiplexing (NC-OFDM) system. NC-OFDM transmission is similar to OFDM transmission but only uses a subset of the frequencies either to avoid incumbent transmissions or due to tactical considerations. This paper considers an NC-OFDM transmission with a given set of active subcarriers and examines how an eavesdropper can infer transmission parameters such as total duration of an NC-OFDM symbol, the length of the cyclic prefix, etc., using tools like the cyclostationary analysis. Such an analysis reveals that difficulty in estimating the total nominal bandwidth of NC-OFDM transmissions (bandwidth that includes frequencies occupied by inactive subcarriers) poses a fundamental challenge in determining the correct sampling rate and the subsequent retrieval of the transmitted signal. The analysis also shows that the features of the cyclic autocorrelation function (CAF) of an NC-OFDM transmission depend closely on the set of active subcarriers. Procedures for inferring the transmission parameters from the CAF are discussed while noting that the choice

of an interleaved set of subcarriers introduces additional ambiguity in determining the transmission parameters. A PCA-based offline timing recovery scheme is proposed and used as a guidepost in determining the minimum rate at which an active set of subcarriers must be refreshed to avoid easy exploitation. Finally, key advantages of an NC-OFDM system over an OFDM system from an LPE-standpoint are discussed and suggestions are made for an LPE-centric design of NC-OFDM systems.

1.5.2 Other Contributions

Analysis and results from following list of publications have not been included in the dissertation, as they do not fit the scope of the topic.

- A. A. A. Abbass, R. Kumbhkar, N. B. Mandayam, and Z. Gajic, "WiFi/LTE-U Coexistence: An Evolutionary Game Approach", in submission for *IEEE ICC 2018*
- N. N. Krishnan, R. Kumbhkar, N. B. Mandayam, I. Seskar, and S. Kompella, "How Close Can I Be?-A Comprehensive Analysis of Cellular Interference on ATC Radar" *IEEE Global Communications Conference (GLOBECOM)*, Singapore, 2017.
- N. N. Krishnan, R. Kumbhkar, N. B. Mandayam, I. Seskar, and S. Kompella, "Coexistence of Radar and Communication Systems in CBRS Bands Through Downlink Power Control" *IEEE Military Communications Conference (MILCOM)*, Baltimore, USA, 2017.
- A. Garnaev, W. Trappe, R. Kumbhkar, and N. B. Mandayam, "Impact of Uncertainty About a User to be Active on OFDM Transmission Strategies" *EAI International Conference on Cognitive Radio Oriented Wireless Networks (CROWNCOM)*, Lisbon, Portugal, 2017.

Chapter 2

Noncontiguous Spectrum : Backhaul using TV white space

2.1 State of TV white space

The FCC's (Federal Communications Commission) opening up of TV white spaces for unlicensed use, has led to innovations in cognitive radio technology, spectrum sensing as well as novel proposals for dynamic spectrum access. Over a good part of the last decade, there has been a tremendous amount of research on spectrum policy as well as the theory and practice of cognitive radio networks including dynamic spectrum access (DSA) algorithms, networking protocols and software radio platform development (e.g. [6,8–10,15,39–55]). While recent and prospective policy reforms and the wealth of wireless technology innovations hold great promise for realizing the goals of achieving ubiquitous broadband and continued growth in the wireless sector and services, a significant barrier to broadband in rural areas is the lack of appropriate backhaul solutions. The absence of backhaul stems from a lack of fiber infrastructure necessary to reliably enable backbone connectivity to the global Internet.

While wide area cellular broadband networks have exploded in urban areas with high user densities, it has primarily been due to the ability to engineer smaller coverage areas (i.e., cell-splitting) supported by amply available backhaul infrastructure. The penetration of such broadband networks in rural areas has primarily been limited due to the lack of economic incentives that service providers encounter in sparsely populated areas. The "economies of scale" do not hold when sizable infrastructure investments need to be made to support a relatively small customer population in a rural area; a fact that is true even in countries like the U.S. which are thought to have an abundant infrastructure. While wired telephone services were historically rolled out in U.S. rural

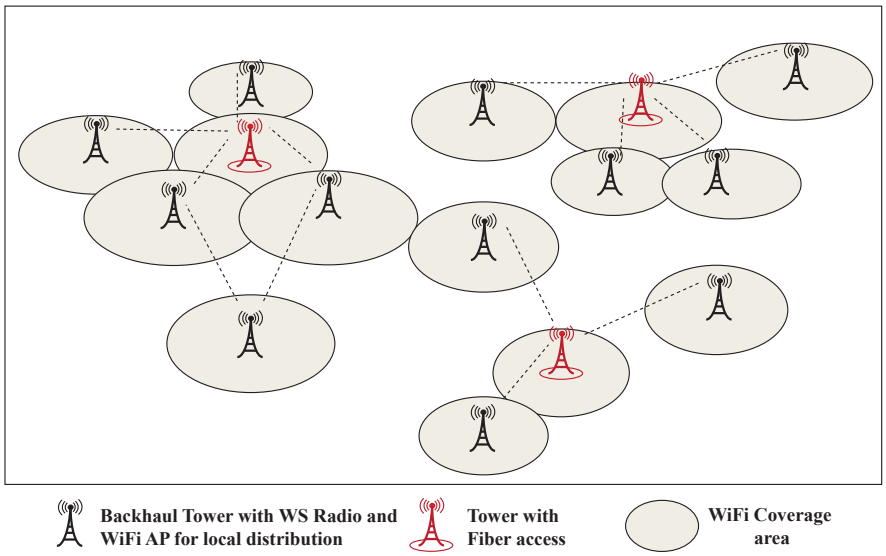


Figure 2.1: A TV White Space Mesh Network (WSMN) for Rural Backhaul

areas in the 20th century due to a federal mandate in exchange for AT&Ts monopoly on wired telephony, no such mandate exists for wireless broadband services. While optical transport networks and associated cloud/grid computing technologies are evolving rapidly, having the ubiquitous deployment of these in rural areas is far from being a reality. Wireless backhaul solutions such as based on satellites or using microwave links are expensive and require strict line of sight requirements making them unattractive and unreliable at times.

The scenario we envision is one where local access and distribution to end-users in a rural area will be through WiFi while backhaul enabling Internet connectivity will be through a wide area network of fixed point-to-point TV white space devices on towers [41] as shown in Figure 2.1. Due to the fact that WiFi local distribution will necessarily result in small coverage cells, there needs to be an abundance (spatially) of backhaul infrastructure that can support this system for ubiquitous rural broadband access. We propose to use TV white spaces for the backhaul traffic by designing a mesh network of white space (WS) radios that can transmit on the available white space channels that are possibly noncontiguous. Further, the uncertainty of available TV white space spectrum poses new challenges in system design in several directions such as planning tower deployments, radio resource management, network management and

caching of information.

Our earlier work has motivated the feasibility of rural backhaul using TV white spaces in New Jersey as a case study [41]. It is to be noted that when fiber/Ethernet backhaul is mentioned, the usual connotation implies very high bandwidth (e.g. the authors in [56] and [57] discuss 100 Gigabit Ethernet deployments). We rather envision a scenario where there are areas without other backhaul infrastructure and where a TV white space based network of fixed devices/towers as shown in Figure 1 can serve as a distribution and backhaul network to connect local traffic using various access modalities (e.g. WiFi, and even possibly limited wired or cellular connections) to the Internet (backbone network) at some distance away. The feasibility study in [41] relies upon several assumptions such as lack of other competing users and interferers in white space as well dynamic changes in traffic, and does not specify any specific modulation, MAC or routing strategies. In this chapter, we investigate the feasibility of multi-hop wireless backhaul in the available white space channels by using Noncontiguous Orthogonal Frequency Division Multiple Access (NC-OFDMA) or similar multi-carrier modulation based transmissions between fixed backhaul towers. Specifically, we consider joint power control, scheduling and routing strategies to maximize the minimum rate across broadband towers in the network. Depending on the population density and traffic demands of the location under consideration, we discuss the suitable choice of cell size for the backhaul network. Using the example of available TV white space channels in Wichita, Kansas (a small city located in the central USA), we provide illustrative numerical examples for designing such wireless backhaul networks.

There exists a large literature in planning towers for wide area wireless systems but these works have been primarily concerned with a specific cellular system and are based on network performance requirements and tower installation costs. For example, [58] focused primarily on supporting UMTS system performance based on signal-to-interference ratio measure, and [59] considers planning base stations and relay stations in 802.16j networks. NC-OFDMA, an access method with which a sender can transmit using noncontiguous spectrum chunks, has received attention in the literature [60–62] including our own recent work on routing and scheduling in multihop networks [1].

However, the issue of spectrum uncertainty due to reuse has not been addressed. Due to the nature of primary and secondary interference in TV white space bands, transmitters will have to use noncontiguous spectrum chunks (or channels) to achieve high data rates. Having multiple radio front-ends to access the noncontiguous chunks can be prohibitive due to cost and real estate available on the transceiver. NC-OFDMA allows nodes to access these noncontiguous spectrum chunks and put null sub-carriers in the remaining chunks [16]. However, nulling sub-carriers increases the sampling rate (spectrum span) which, in turn, increases the power consumption of radio front ends. Our preliminary work [1] has characterized this trade-off from a cross-layer perspective, specifically by showing how the slope of the ADC/DAC power-bandwidth response influences scheduling and routing decisions in a multi-hop network. In cognitive radio networks research, spectrum reuse (e.g. [11, 12]) and routing (e.g. [13, 14]) algorithms have been proposed to support spectrum coexistence; moreover, there exists a rich history of research in transmit power control for cellular networks, such as [63–65]. The key differentiators of the work in this chapter are the development of reuse and routing algorithms for spectrum coexistence by controlling white space radio channels to provide backhaul for the local traffic demands. Specifically, we design a rate optimal backhaul network using TV white space channels.

2.2 TV white space backhaul system model

2.2.1 Network model

We consider a network comprising of towers or base stations from a set $\mathcal{N}$ of size N. Each base station is equipped with white space radios which can communicate using TV white space channel. These base stations are placed in a grid structure with m_1 rows and m_2 columns, i.e. $m_1 \times m_2 = N$. Base stations are located at the center of each grid and the length of the sides of each grid is l km and each base station provides local WiFi access within each grid. Moreover, we do not consider the explicit design of the WiFi network within each grid. We assume that depending on the size of the grid, WiFi distribution itself can be based on using a mesh network of WiFi

Table 2.1: List of parameters for TV white space analysis

Notation	Description
$\mathcal{N}$	Set of base stations
$\mathcal{A}$	Set of points with fiber access
$\mathcal{E}$	Set of links
$\mathcal{M}$	Set of total available channel
M	Total number of available channels
r_i	Data rate at node i due to own traffic
r_{ij}^m	Data rate from node i to j on channel m
p_{ij}^m	Power consumed at node i, when transmitting to node j on channel m
g_{ij}^m	Link gain between node i and node j on channel m
x_{ij}^m	Scheduling variable for link ij using channel m
c_{ij}^m	capacity of link ij using channel m
s_{ij}^m	Signal-to-noise ratio for link ij using channel m
N_0	Power spectral density of noise
W	Bandwidth of each channel
N	Number of base stations
A	Number of base stations with fiber access
U	A large number $\geq P_{max}$
V	A large number $\geq$ maximum possible rate
P_I	Interference threshold in protocol model
P_{max}	Maximum power consumption allowed at each node

nodes. Among these N base stations, a set $\mathcal{A} \subseteq \mathcal{N}$ of size A consists of only those base stations which have access to high-speed fiber backhaul links, while remaining base stations in set $\{\mathcal{N} \setminus \mathcal{A}\}$ use only white space channels for backhaul communication. Base stations can use any of the M available white space channels from set $\mathcal{M}$ for the backhaul traffic as long as links satisfy interference constraints. These available white space channels can be noncontiguous and we assume that base stations are capable of accessing these channels using NC-OFDMA. Links are represented as ordered pairs, i.e. link ij represents communication from node i to node j, while link ji represents communication from node j to node i. We assume a scheduling indicator variable x_{ij}^m such that

$$x_{ij}^m = \begin{cases} 1, & \text{Link } ij \text{ is scheduled on channel } m \in \mathcal{M} \\ 0, & \text{Otherwise} \end{cases}$$

All communications are assumed to be half duplex and for any channel $m \in \mathcal{M}$, transmission to multiple base stations or reception from multiple base stations is not possible.

These constraints can be written as follows

$$\sum_{j\in\mathcal{N},j\neq i} x_{ij}^m + \sum_{k\in\mathcal{N},k\neq i} x_{ki}^m \leq 1 \quad \forall\, i \in \mathcal{N},\ \forall\, m \in \mathcal{M}. \tag{2.1}$$

The power used for transmission on link ij using channel m is represented by p_{ij}^m. The total power used at any base station for transmission on a white space channel is limited by P_{max}, therefore

$$\sum_{j\in\mathcal{N}} \sum_{m\in\mathcal{M}} p_{ij}^m \leq P_{max} \ \ \forall\, i \in \mathcal{N}, \tag{2.2}$$

Based on the power allocated for any link ij on channel m, this link can support a rate r_{ij}^m which is limited by the capacity constraint as

$$\begin{aligned} r_{ij}^m &\leq c_{ij}^m = W \log(1 + s_{ij}^m) \quad \forall\, i, j \in \mathcal{N},\ i \neq j, \\ s_{ij}^m &= \frac{p_{ij}^m g_{ij}^m}{N_0 W} \quad \forall i, j \in \mathcal{N},\ i \neq j, \end{aligned} \tag{2.3}$$

where g_{ij}^m is the link gain, N_0 is the noise spectral density, and W is the bandwidth of a single channel. The data rate requirement of the traffic generated within coverage area of a base station i is denoted by r_i, therefore according to conservation of flow

$$\sum_{j\in\mathcal{N}} \sum_{m\in\mathcal{M}} r_{ij}^m = r_i + \sum_{k\in\mathcal{N}} \sum_{m\in\mathcal{M}} r_{ki}^m \ \ \forall\, i \in \{\mathcal{N} \setminus \mathcal{A}\} \tag{2.4}$$

$$\sum_{i\in\{\mathcal{N}\setminus\mathcal{A}\}} r_i = \sum_{i\in\mathcal{N}} \sum_{j\in\mathcal{A}} \sum_{m\in\mathcal{M}} r_{ij}^m \tag{2.5}$$

It can be observed from previous equations that all elements of $\mathcal{A}$ act as sinks in a network, i.e. all traffic generated by towers in $\mathcal{N} \setminus \mathcal{A}$ is equal to traffic entering towers in $\mathcal{A}$. Towers in set $\mathcal{A}$ do not transmit to other nodes using white space channels, therefore the power allocated to these base stations is zero. It can also be noticed that x_{ij}^m is 1 and r_{ij}^m has non-zero value only when allocated power p_{ij}^m is non-zero. If U and V are sufficiently large numbers then

$$p_{ij}^m \leq U x_{ij}^m, \quad r_{ij}^m \leq V x_{ij}^m, \tag{2.6}$$

To model the interference between different base stations we use a slightly modified protocol interference model. Under this model, transmission on link ij using channel m

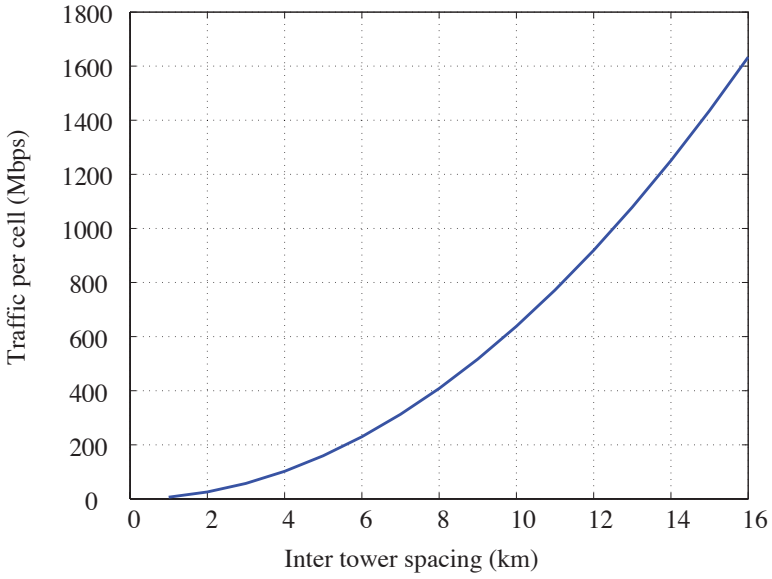


Figure 2.2: Estimate of data traffic per cell in year 2017

is successful if and only if on the same channel the interference at base station j from any other transmitting node k is less than some threshold P_I. This can be written as

$$p_{kl}^m + \left(P_{max} - \frac{P_I}{g_{kj}^m} \right) x_{ij}^m \leq P_{max} \quad \forall\, k \in \mathcal{N},\, l \in \mathcal{N} \tag{2.7}$$

While calculating the capacity we had ignored the interference caused by other nodes, but this is taken care of by choosing a small enough threshold P_I for interference in our protocol interference model.

The data rate supported by each base station in its cell should be more than the traffic requirement of that cell's population. To model the traffic demand in a cell, we use the results from a Cisco study that projects the traffic requirement for 2017. Specifically, the traffic demand is estimated using the Cisco Visual Networking Index (VNI) [66] as follows. Using the default values of application usage (e.g. file sharing, VOIP, gaming, video, and data) we obtain an estimate of 130 GB per month per connection (4.33GB per day). We calculate the traffic demand per cell for different cell sizes assuming penetration of Internet connection to 78% of total population (using ITU ICT statistics for the developed countries [67]). We assume that at any time only 25% of the population is active on the Internet and each household (therefore each subscription) consists of 3 members. Under the above assumptions, the estimate for

per-cell mobile data traffic in the year 2017 for different cell sizes is shown in Figure 2.2. We use this estimate for modeling the traffic demand and find the feasibility of a network using TV white space.

2.2.2 Link gain model

We use the ITU terrain propagation model to calculate the link gain between the base stations for different channels [68]. This is a good model to represent rural areas which might include buildings as well as open fields. Under this model, the median path loss for regular obstructions for LOS communication is given by

$$PL = FSL + A_d \quad dB, \tag{2.8}$$

where the free space path loss is given by

$$FSL = 20\log_{10} d + 20\log_{10} 1000f + 32.44 \quad dB \tag{2.9}$$

The distance d between base stations is in km, the frequency f is in GHz. The excess path loss A_d due to diffraction is given as

$$A_d = \frac{-20h}{F1} + 10 \quad dB, \tag{2.10}$$

where h is the height difference between the most significant path blockage and the LOS path between the base stations; and F_1 is the radius of the first Fresnel zone given by

$$F_1 = 17.3\sqrt{\frac{d_1 d_2}{fd}} \quad m, \tag{2.11}$$

where d_1 and d_2 are distances of obstruction from base stations in km. The complete link gain between two base stations and resulting SNR are given by

$$G_{link} = -PL - N_f + G_{TX} + G_{RX} \quad dB \tag{2.12}$$

$$SNR = P_T + G_{link} - 10 \times \log_{10} N_0 W \quad dB \tag{2.13}$$

where G_{TX} and G_{RX} are the antenna gains at transmitting and receiving base stations respectively, and P_T is the transmit power.

2.3 Max-min rate optimization

In this section, we solve the following optimization problem which maximizes the minimum of supported rate r_i at each base station i while performing joint power allocation, scheduling, and routing, subject to the various power and flow constraints discussed in the previous section.

maximize $\min r_i$

subject to :

$$\sum_{j\in\mathcal{N}}\sum_{m\in\mathcal{M}} p_{ij}^m \le P_{max} \;\; \forall\, i \in \mathcal{N} \tag{2.14}$$

$$p_{ij}^m = 0 \quad \forall\, i \in \mathcal{A},\, j \in \mathcal{N},\, m \in \mathcal{M} \tag{2.15}$$

$$r_{ij}^m \le W \log_2(1 + s_{ij}^m) \quad \forall\, i, j \in \mathcal{N},\; i \neq j,\; s_{ij}^m = \frac{p_{ij}^m g_{ij}^m}{N_0 W} \tag{2.16}$$

$$\sum_{j\in\mathcal{N}}\sum_{m\in\mathcal{M}} r_{ij}^m = r_i + \sum_{k\in\mathcal{N}}\sum_{m\in\mathcal{M}} r_{ki}^m \;\; \forall\, i \in \{\mathcal{N} \setminus \mathcal{A}\} \tag{2.17}$$

$$\sum_{j\in\mathcal{N}, j\neq i} x_{ij}^m + \sum_{k\in\mathcal{N}, k\neq i} x_{ki}^m \le 1 \quad \forall\, i \in \mathcal{N},\; \forall\, m \in \mathcal{M} \tag{2.18}$$

$$\sum_{i\in\{\mathcal{N}\setminus\mathcal{A}\}} r_i = \sum_{i\in\mathcal{N}}\sum_{j\in\mathcal{A}}\sum_{m\in\mathcal{M}} r_{ij}^m \tag{2.19}$$

$$p_{kl}^m + \left(P_{max} - \frac{P_I}{g_{kj}^m}\right) x_{ij}^m \le P_{max} \quad \forall\, k, l \in \mathcal{N},\, m \in \mathcal{M} \tag{2.20}$$

$$p_{ij}^m \le U x_{ij}^m \quad \forall\, i \in \mathcal{N},\, j \in \mathcal{N},\, m \in \mathcal{M} \tag{2.21}$$

$$r_{ij}^m \le V x_{ij}^m \quad \forall\, i \in \mathcal{N},\, j \in \mathcal{N},\, m \in \mathcal{M} \tag{2.22}$$

$$x_{ij}^m \in \{0, 1\},\; p_{ij}^m \ge 0,\; r_{ij}^m \ge 0,\; \forall\, i, j \in \mathcal{N},\, m \in \mathcal{M} \tag{2.23}$$

$$r_i \ge 0 \quad \forall i \in \mathcal{N} \tag{2.24}$$

This is a mixed integer nonlinear program, since x_{ij}^m variables are binary and capacity constraints are nonlinear. We modify the nonlinear capacity constraint to multiple linear constraints as a piecewise linear approximation. To get this approximation, we use values of SNR based on P_{max} as an upper bound. Starting with 0 dB SNR, each $\sim$ 10 dB increment is approximated by a line, which is tangential to the capacity curve.

We solve this modified mixed-integer linear program using MOSEK with CVX [69,

70]. MOSEK solves the mixed-integer program using the branch-and-bound method, which has exponential complexity. MOSEK might result in an infeasible solution due to the linearization of the capacity constraint. If an infeasible solution occurs, then corresponding SNR is calculated using power variables p_{ij}^m and then the new rate is calculated with this SNR as

$$r_{ij,\text{new}}^m = W \log_2 \left(1 + \frac{p_{ij}^m g_{ij}^m}{N_0 W}\right) \tag{2.25}$$

The supported data rate r_i at the base station i is decreased by $r_{ij}^m - r_{ij,\text{new}}^m$ to maintain the flow conservation, and after checking the feasibility of all rate variables a new minimum supported rate is calculated.

2.4 Simulation and results

We consider a small network of 9 base stations located in a 3×3 grid as shown in Figure 2.3, covering a total area of $9l^2$ sq. km in our simulation. Figure 2.3 shows base stations 1, 5 and 9 with fiber access as an example, while the other base stations use only white space channels to backhaul their traffic to one of the fiber access destinations. Table 2.2 shows the values of different parameters used in our simulation. There are seven white space channels available for fixed devices in Wichita, KS, USA, which we use in our simulation

$$\mathcal{M} = \{57, 79, 85, 491, 527, 533, 671\} \text{ MHz}$$

We vary the grid size and number of towers with fiber access points to check the feasibility of white space based backhaul. Different values of l are chosen from a set $\mathcal{L}$, where

$$\mathcal{L} = \{2, 3, 4, 5\} \ km$$

thus covering areas of 36, 81, 144 and 225 sq. km respectively, while values of $\mathcal{A}$ are chosen to be any of the following sets

$$\mathcal{A}_1 = \{1, 5, 9\},$$

$$\mathcal{A}_2 = \{1, 3, 7, 9\},$$

$$\mathcal{A}_3 = \{1, 3, 5, 7, 9\}$$

P_{max}	4 watts
Noise figure N_f	10 dB
d_1	d/2
d_2	d/2
G_{TX}	6 dB
G_{RX}	6 dB
Height of link	30m
Height of obstruction	15m
Channel bandwidth W	6 MHz

Table 2.2: Parameters used in simulation

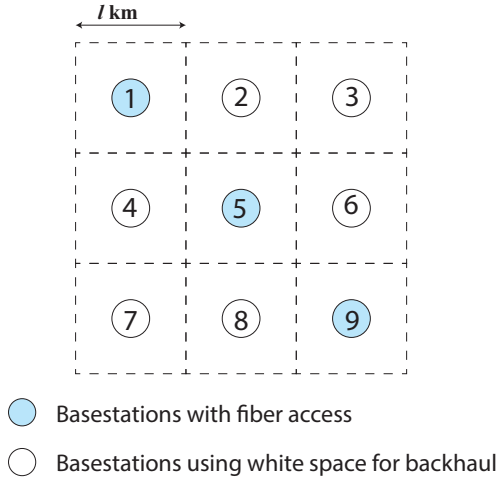


Figure 2.3: Simulation setup with $\mathcal{A} = \{1, 5, 9\}$

Due to the complexity of the mixed-integer linear program, we use an approximate version of this problem, which gives the highest feasible value of r_i with a granularity of 1Mbps. We use the traffic demand model described earlier to generate traffic for the entire 3x3 grid and check the feasibility of using white space based backhaul with different grid sizes and different values of $\mathcal{A}$.

Figure 2.4 shows a frequency scheduling and routing scheme that results from solving the optimization problem which achieves a minimum supporting data rate of 75 Mbps at each base station, where the grid size is $3km \times 3km$ and $\mathcal{A} = \{1, 3, 7, 9\}$.

Figure 2.5 shows the complete result obtained by solving the optimization problem for different values of the grid size and different values of set $\mathcal{A}$. The data traffic demand per cell increases as the cell size increases due to increase in the number of users per cell. It can be seen that for $l = 2km$, use of $\mathcal{A}_1$, $\mathcal{A}_2$ or $\mathcal{A}_3$ as fiber access points meets the

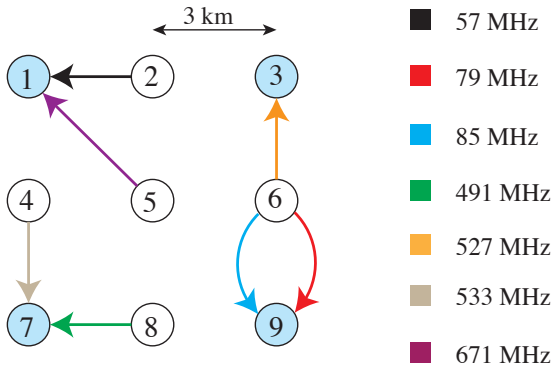


Figure 2.4: Routing and scheduling obtained for $\mathcal{A} = \{1, 3, 7, 9\}$ with $l = 3$km

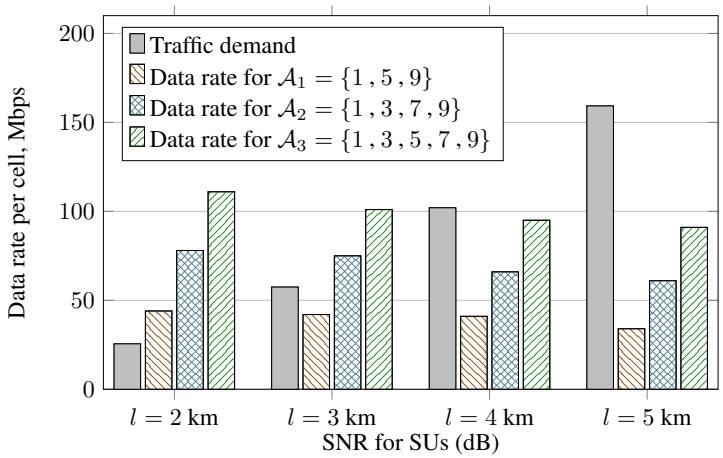


Figure 2.5: Data rate supported at each cell for different grid size

traffic demand. However, as the cell size increases, the traffic requirement is met only when the number of fiber access points is large. For $l = 5km$ and $l = 4km$, the traffic demand is not met by any of the fiber access configurations used in the simulations, but $l = 3km$ presents an interesting result. For $l = 3$km, the traffic demand is met by using $\mathcal{A} = \mathcal{A}_2$ or $\mathcal{A} = \mathcal{A}_3$. Note that the case of $\mathcal{A} = \mathcal{A}_2$ represents a scenario where only 4 base stations with fiber access (out of a total of 9) can provide backhaul for a coverage area of 81 sq. km.

2.5 Chapter Summary

The penetration of wireless broadband services in remote areas has primarily been limited due to the lack of economic incentives that service providers encounter in sparsely

populated areas. Besides, wireless backhaul links like satellite and microwave are either expensive or require strict line of sight communication making them unattractive. TV white space channels with their desirable radio propagation characteristics can provide an excellent alternative for engineering backhaul networks in areas that lack abundant infrastructure. Specifically, TV white space channels can provide "free wireless backhaul pipes" to transport aggregated traffic from broadband sources to fiber access points. We investigated the feasibility of multi-hop wireless backhaul using the available TV white space channels in Wichita, Kansas (a small city in the central USA) as an example. We performed joint power control, scheduling and routing to maximize the minimum rate across broadband towers in the network. Simulation results showed that a service provider could bring fiber to a subset of deployed towers but still could meet the backhaul requirement of each tower using white space channels.

Our work can be extended to minimize the fiber layout cost while supporting backhaul requirement of each tower in a rural area using TV white space channels. Since noncontiguous spectrum access increases the power consumed in the ADC and DAC transceiver circuitry due to increased spectrum span, it is also of interest to study the power consumption in such backhaul networks using noncontiguous spectrum access.

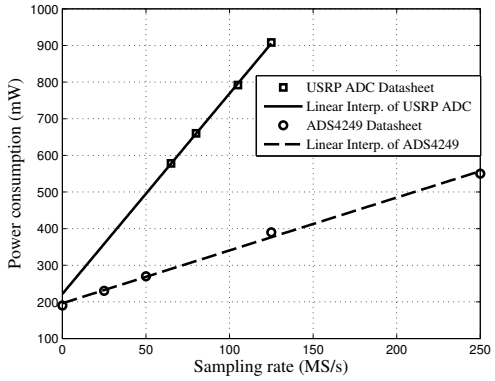
Chapter 3

Effect of Spectrum Span on Noncontiguous Spectrum Allocation

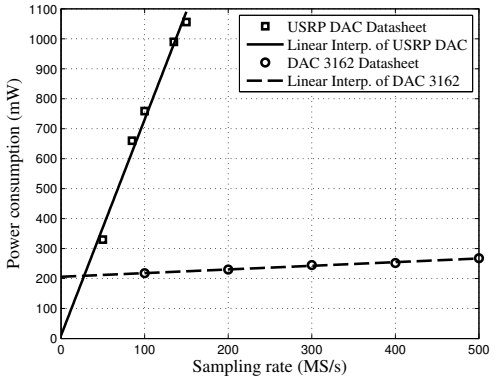
3.1 Spectrum span and system power consumption

One principal drawback of NC-OFDM is that it suffers from high out-of-band radiation due to the high sidelobes of its modulated subcarriers, which can potentially affect the performance of licensed users or other CRs in the unlicensed band [26]. Several techniques to address this issue have been proposed and we briefly touch upon these issues in the latter part of this chapter. Another significant concern when using NC-OFDMA is that the CR links are allocated disjoint frequency bands that lead to an increase in the *spectrum span* of a CR link. The spectrum span is defined as the difference between the frequencies of the extreme channels allocated to a CR link. The increase in the spectrum span leads to higher sampling rates that in turn lead to an increase in the power consumption at the transmit/receive nodes. Traditionally, the transmit power requirements of a transceiver system have dominated the total power consumption. However, the ADC/DAC power consumption can become comparable or even significantly larger than the transmit power consumption when the sampling rates become very large [1]. It is therefore important to impose a reasonable limit on the spectrum span.

In this chapter, we consider the problem of spectrum allocation across multiple point-to-point CR links between NC-OFDM-enabled transceivers in the presence of interference from out-of-network users. The main goal is to achieve a fair spectrum allocation that maximizes the minimum data rate across these CR links while limiting the spectrum span. Towards this goal, we propose an optimization framework to maximize the minimum rate, subject to the constraint that the spectrum span does



(a) ADS62P4x [72] (ADC of USRP radio) and ADS4249 [73]



(b) AD 9777 [74] (DAC of USRP radio) and DAC 3162 [75]

Figure 3.1: Linear increase in power consumption with increasing sampling rate in the ADC and the DAC of a USRP. Reproduced from [1].

not exceed a certain limit. For constant transmit powers and orthogonal spectrum allocation, such an optimization is a linear integer program and can be solved efficiently using readily available solvers. Simulation results show a trade-off between the max-min rate and spectrum span. In our simulations, we also show improvement in data rate based on spectrum allocation obtained by solving the optimization problem in the presence of interference. We also implement the NC-OFDM system using USRP [54] radios with GNU Radio software platform on the ORBIT testbed [51]. GNU Radio is a free and open-source software development toolkit that provides signal processing blocks to implement software radios [71].

Optimizing communication links for total transmit power is a well-studied area. However, in recent years, optimizing a communication link for total power consumption is attracting significant attention. The authors of [76] consider the effect of system power for energy efficient wireless communications. Modulation schemes optimized for system power consumption are studied in [77], while the authors in [78] present a communication-theoretic view of system power consumption. System power constraints specifically related to NC-OFDM are studied in [79, 80], where it is shown that the maximum spectrum span is limited by the power consumption at the ADCs/DACs [79] and that the requirement of a guard band affects the overall system throughput. The authors in [1] characterize the trade-off between the system power and spectrum span

from a cross-layer perspective in a multi-hop network. The authors in [81] provide a graph coloring method for spectrum allocation with the goal of providing equal rates to each user. To the best of our knowledge, fair spectrum allocation with system power considerations for an NC-OFDM-enabled system has not been studied so far. Our work focuses on opportunistic spectrum allocation to maximize the minimum rate while limiting the spectrum span of the NC-OFDM-enabled cognitive radio links.

3.2 Ad-hoc network using NC-OFDM

We consider a network of N point-to-point links that use NC-OFDM for communication. The set of N links in this model is represented by $\mathcal{N}$. These links have access to M channels, represented by the set $\mathcal{M} = \{1, 2, \ldots, M\}$, with each channel having a bandwidth of W Hz. We assume that each channel consists of t OFDM subcarriers. Transceivers in these links can be dynamically programmed to use different sets of channels. The distance between the transmitter and the receiver in link l is denoted as d_l. We assume that each channel experiences flat fading and the channel gain for link l on the m^{th} channel is represented as g_l^m. The link gain encompasses antenna gain, path loss, shadowing and fading. The transmit power used by each link l on each of the M channels is kept constant and is denoted as p. Hence, the received power at the receiver of link l on channel m is given by pg_l^m. The M available channels are distributed among the N links in an orthogonal manner while ensuring some measure of fairness. The $N \times M$ channel allocation matrix resulting from such a process is denoted by $\mathbf{A}$. Elements of matrix $\mathbf{A}$ can either be 1 or 0. The i^{th} row of $\mathbf{A}$ represents the channel allocation vector for the i^{th} link. Elements of $\mathbf{A}$ are defined as follows

$$a_{lm} = \begin{cases} 1, & \text{link } l \text{ is scheduled on channel } m \in \mathcal{M} \\ 0, & \text{otherwise.} \end{cases}$$

Since we assume that all N links in our model can potentially interfere with each other, we restrict ourselves to a disjoint or orthogonal allocation of the available channels.

Thus,

$$\sum_{l=1}^{N} a_{lm} \leq 1, \quad \forall\, m \in \mathcal{M}. \tag{3.1}$$

We also assume that the number of channels M is more than the number of links N and therefore, any fair allocation would not leave any link without any channel.

As discussed in the previous section, the total spectrum span of a CR link affects the sampling rate and hence the system power. Fig. 3.1 reproduced from [1], shows the power consumption in the ADCs and DACs that are typically used in USRP radios as a function of sampling rate. Higher bandwidth usage results in higher sampling rate, and this increases system power consumption in the ADC and DAC. Therefore, it becomes important to keep the overall spread of frequencies over which the channels are allocated to a link to a reasonably small value. We define the spectrum span B_l for a link l as the magnitude of the difference in the frequencies of the channels with the smallest and largest index that have been assigned to link l. For link l, spectrum span can be written as

$$B_l = \Big(\max_{m \in \mathcal{M}} (m.a_{lm}) - \min_{m \in \mathcal{M}} (m.a_{lm} + M(1 - a_{lm})) + 1 \Big) \times W. \tag{3.2}$$

We limit the spectrum span by defining a threshold b, so that

$$B_l \leq b \cdot W \quad \forall\, l \in \mathcal{N}. \tag{3.3}$$

We also assume that each of the N links experiences interference from any subset of out-of-network nodes and that we have no control over these interfering nodes. The $N \times M$ matrix $\mathbf{U}$ represents the cumulative interference power observed by the links from these out-of-network interferers on each of the M channels. Each element u_{lm} of this matrix represents the total out-of-network interference power observed by the receiver of link l on channel m. In such a scenario, the signal-to-interference-plus-noise ratio (SINR) on channel m for the receiver of link l is given by

$$s_l^m = \frac{p g_l^m}{N_0 W + u_{lm}} \quad \forall\, l \in \mathcal{N},\ m \in \mathcal{M}, \tag{3.4}$$

where N_0 is the power spectral density of the additive white Gaussian noise that corrupts the received signal. Since we assume orthogonal channel allocation, we do not

Table 3.1: List of notations for spectrum span analysis

Notation	Description
$\mathcal{N}$	Set of links
N	Number of links
$\mathcal{M}$	Set of total available channels
M	Number of total available channels
$\mathbf{A}$	Resource allocation matrix of size $N \times M$
a_{lm}	Allocation indicator variable for link l and channel m
$\mathbf{U}$	Interference matrix of size $N \times M$
u_{lm}	Interference for link l on channel m
g_l^m	Channel gain for link l using channel m
s_l^m	Signal-to-interference-plus-noise ratio for link l using channel m
c_l^m	Channel capacity for link l using channel m
r_l^m	Data rate for link l using channel m
r_l	Total data rate for link l
d_l	Distance between transmitter and receiver for link l
W	Bandwidth of each channel
N_0	Noise spectrum density

consider interference from the other $M-1$ links while calculating the SINR. When channel m is allocated to link l, the data rate for link l on channel m is given by

$$c_l^m = W \log_2(1 + s_l^m) \quad \forall\, l \in \mathcal{N},\ m \in \mathcal{M}. \tag{3.5}$$

Depending on whether this channel is allocated to this link or not, the rate r_l^m achieved by link l on this channel satisfies

$$r_l^m = c_l^m a_{lm}. \tag{3.6}$$

Thus, the total data rate achieved by link l is given by

$$r_l = \sum_{m=1}^{M} r_l^m \quad \forall\, l \in \mathcal{N}. \tag{3.7}$$

3.2.1 Problem formulation

The objective is to obtain a fair spectrum allocation across all the CR links in the system such that (a) it maximizes the minimum data rate among all the links under the condition that the spectrum be allocated in an orthogonal manner and (b) the resulting span is within a specified threshold, so as to limit the overall system power consumption.

To achieve this objective, we formulate an optimization problem to maximize the minimum data rate while restricting the spectrum span to be below a threshold b. Such an optimization problem can be written as follows

$$\text{maximize} \quad \min_{l \in \mathcal{N}} r_l$$

$$\text{subject to :}$$

$$B_l \leq bW \qquad \forall\, l \in \mathcal{N}, \tag{3.8}$$

$$r_l = \sum_{m=1}^{M} c_l^m . a_{lm} \qquad \forall\, l \in \mathcal{N},\ \forall\, m \in \mathcal{M}, \tag{3.9}$$

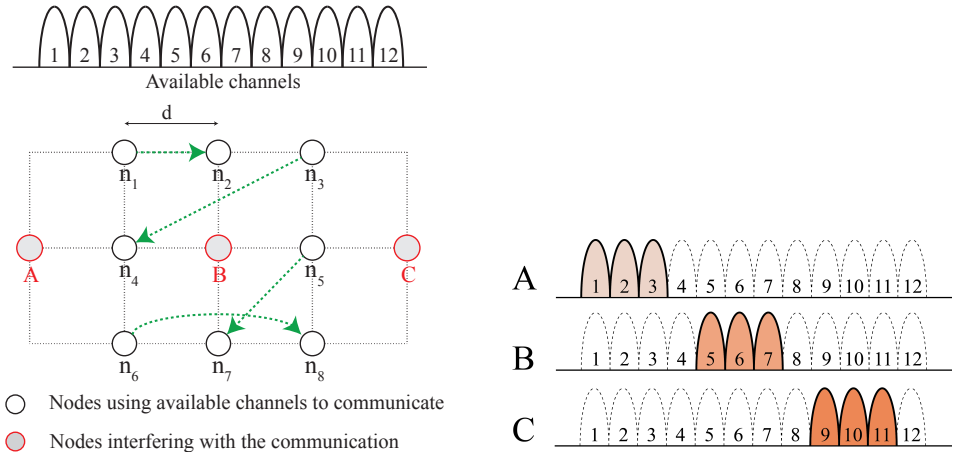
$$\sum_{l=1}^{N} a_{lm} \leq 1, \qquad \forall\, m \in \mathcal{M}, \tag{3.10}$$

$$a_{lm} \in \{0, 1\} \qquad \forall\, l \in \mathcal{N},\ \forall\, m \in \mathcal{M}. \tag{3.11}$$

Note that the only variables in above formulation are the integer variables a_{lm} since all the other variables can be eliminated in a straightforward manner. Such a formulation is seen to be a linear integer program. Maximizing the minimum rate and restricting the spectrum span are two competing objectives. Allowing a higher value for b provides the opportunity to allocate channels over a wide range of frequencies to a link which might result in a higher data rate, but this increase comes at the cost of higher system power consumption. On the other hand keeping the spectrum span threshold too small eliminates these allocation opportunities. We analyze this trade-off in the next section.

The above formulation does not consider the effect of interference from the N links on the out-of-network nodes. However, if the out-of-network nodes are treated as primary users and need to be protected, certain a_{lm} variables can be set to 0 depending on the value of u_{lm}. This change, however, does not impact the nature of the above formulation. In the rest of the chapter, the out-of-network nodes are merely treated as interferers and not as primary users.

This linear integer program can be solved using the MOSEK solver via CVX in MATLAB [69, 70, 82]. MOSEK solves the integer program using the branch-and-bound method, which is known to have an exponential complexity. Since integer programming



(a) Available channels and the network topology used in the simulation.

(b) Channels used by interfering nodes A, B and C.

Figure 3.2: Simulation setup used for spectrum allocation

is an NP-hard problem, MOSEK uses continuous relaxation with a goal of computing near-optimal solution instead of finding an optimal solution. The output of such an optimization generates a list of channel allocations for each link along with the rates achieved in each of the links.

3.3 Simulation setup

To analyze the effectiveness of the proposed approach, we test it on the topology shown in Fig. 3.2a. As shown in Fig. 3.2a, the nodes named n_1 to n_8 use the available channels in an opportunistic manner in the presence of interfering transmitters A, B and C. Nodes n_1, n_3, n_5 and n_6 are assumed to be transmitters, transmitting to nodes n_2, n_4, n_7 and n_8 respectively as shown in Table 3.2. In our simulation, we assume that grid spacing is $d = 1$ m and that there are 12 channels available for communication, with each channel having a bandwidth of 100 kHz. The transmission power is 0.1 mW. The noise power is calculated from the thermal noise power spectral density, assuming that the system operates at a temperature of $T = 300$ K. For such a system, the parameters corresponding to the system model are given as follows:

$$\mathcal{N} = \{L_1, L_2, L_3, L_4\},$$

Table 3.2: Links in the network used for the simulation.

Link	Nodes	Length
L_1	$n_1 \to n_2$	d
L_2	$n_3 \to n_4$	$\sqrt{5}d$
L_3	$n_5 \to n_7$	$\sqrt{2}d$
L_4	$n_6 \to n_8$	$2d$

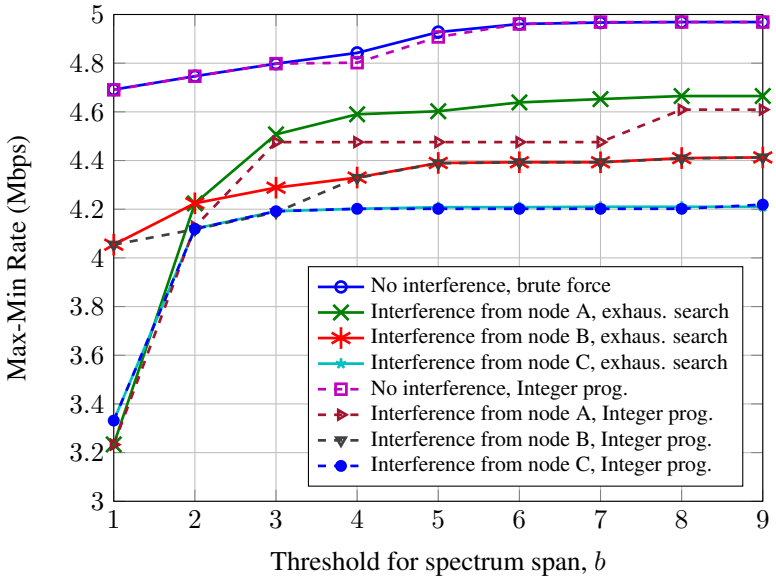


Figure 3.3: Trade-off between the max-min rate and the threshold on the spectrum span in the presence of interference from nodes A, B, or C.

$$\mathcal{M} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\},$$

$$W = 100 \text{ kHz},$$

$$N_0 = kT,$$

where k is the Boltzmann constant.

The channel gain in each of the channels is generated using a Rician flat fading model with K-factor of 30 dB. As shown in Fig. 3.2b, interfering nodes A, B and C operate in channels $(1, 2, 3)$, $(5, 6, 7)$ and $(9, 10, 11)$ respectively. The transmit SNR at the interfering nodes is assumed to be 33 dB in each of the channels. We assume that these interfering nodes can be turned on or off independent of each other.

As mentioned in the previous section, there exists a trade-off between the max-min rate and the restriction on the spectrum span. Clearly, the highest value of the max-min rate can be achieved when $b = M$. Obtaining this trade-off curve requires us

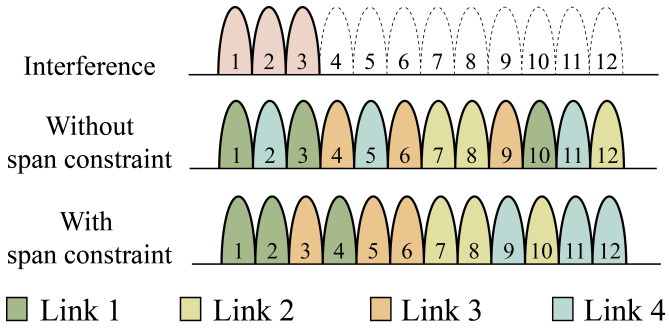


Figure 3.4: Effect of span constraint on the allocation of channels in the presence of interference from node A. Spectrum span threshold was set to be 4.

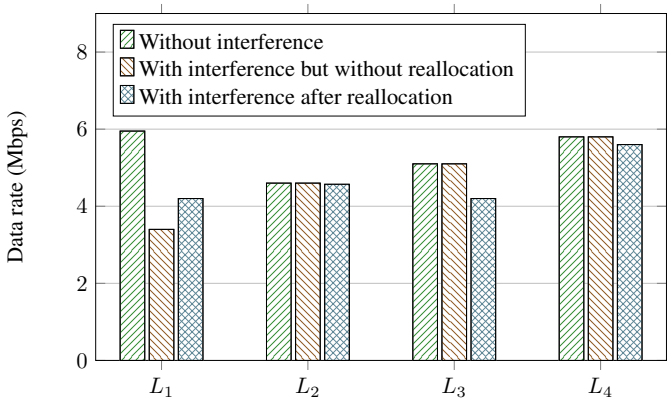


Figure 3.5: Data rates obtained by solving the optimization problem in the presence/absence of interference from node 'A' while restricting the spectrum span to $b = 4$.

to compute the globally optimal max-min rate for every value of b. Since the integer programming is an NP-Hard problem, computing the globally optimal solution is not possible using solvers such as MOSEK and must instead be computed in a brute-force manner by considering all possible channel allocations. A trade-off curve obtained through a brute-force search is shown in Fig. 3.3. Specifically, Fig. 3.3 plots the trade-off curve between the max-min rate and the spectrum span for four scenarios where the four in-network links see interference from either (i) node A only, (ii) node B only, (iii) node C only or (iv) see no interference at all. Fig. 3.3 also plots the max-min rate obtained by solving the integer program presented in Section III-A. Although solving the integer program is not guaranteed to find the globally optimal solution, it is seen that the overall average performance is relatively close to that obtained from a brute-force search. This highlights the effectiveness of the proposed framework.

Fig. 3.3 also shows that the max-min rate saturates well before the restriction on the spectrum span is increased to M. This indicates that the threshold b that limits the spectrum span can be set to a value significantly lesser than M while paying only a small penalty in the max-min rate.

Fig. 3.4 illustrates the effect of the span constraint on the channel allocation for a particular instance of the channel gains and when only node A causes interference. It is seen that channel allocation without any restriction on span can result in a link being allocated channels across a wide spectrum. However, with a span constraint of $b = 4$, spectrum gets reallocated so as to satisfy the span constraint while not incurring a significant penalty on the max-min rate.

Fig. 3.5 shows the change in throughput for each of the four links before and after the introduction of interference from node A. The spectrum span is restricted to be less than or equal to 4. The figure plots the throughput obtained when (a) spectrum is optimally allocated when there is no interference, (b) interference from node A is introduced, but spectrum allocation remains the same as in case (a), and (c) spectrum is reallocated while accounting for the interference from node A. As expected throughput drops from case (a) to case (b) but increases after reallocation in case (c). While the frequency of spectrum reallocation is certainly a function of the changes in the interference landscape, how often such a reallocation is permissible or necessary is also dependent on other application specific constraints and hardware limitations.

3.4 Experiments on orbit testbed

We test the proposed formulation on a scaled-down version of the network (see Fig. 3.2a) used for simulations in Section 3.3. For the experimental setup, we consider a network consisting of two links along with one out-of-network interferer, as shown in Fig. 3.6. The two point-to-point links are denoted as $L_1 = (n_1, n_2)$ and $L_2 = (n_3, n_4)$, and the interfering node is labeled as node A. Each node is a USRP2 node with a GNU Radio software platform. These nodes are part of the larger ORBIT testbed that consists of 400 radio nodes placed in a 20×20 grid with 1 m spacing between the

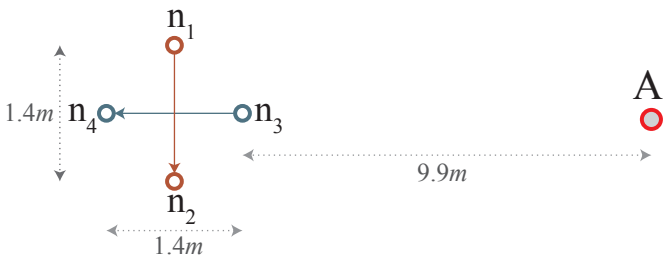


Figure 3.6: Topology used in the ORBIT testbed.

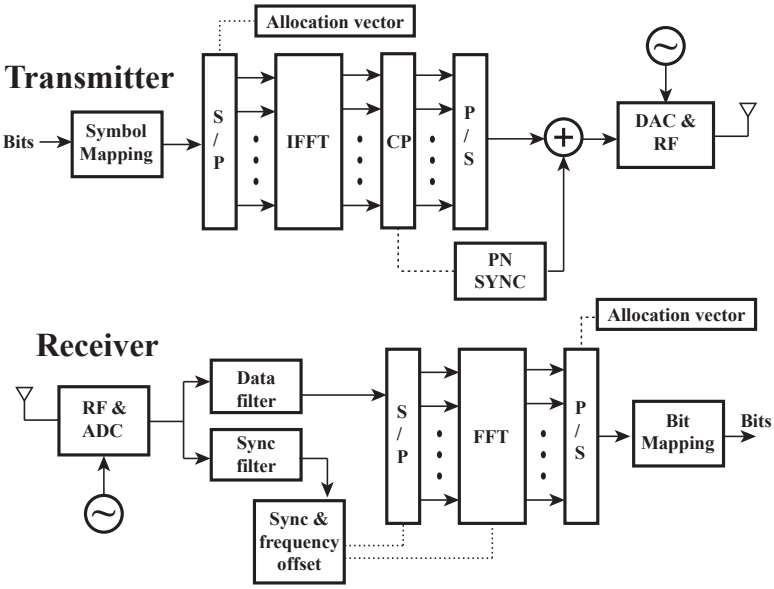


Figure 3.7: Block diagram for implementing NC-OFDM using the GNU Radio platform.

adjacent nodes. The testbed nodes are equipped with a variety of radio platforms including 802.11 a/b/g, Bluetooth, Zigbee, and various versions of software defined radios (SDRs) such as USRP platforms, WARP platforms, and the CRKit cognitive radios that were developed at WINLAB [54, 83, 84]. The nodes in our experiments are USRP N210 modules with the SBX transceiver daughter-card that can operate anywhere from 400 MHz to 4.4 GHz and transmit up to 100 mW of power. GNU Radio is a free and open-source SDR framework that provides the application programming interface (API) for several hardware platforms, including many USRP devices. The NC-OFDM communication paths are implemented in C++ and Python in GNU Radio. Fig. 3.7 represents the block diagram of the transmitter and receiver in our experimental setup.

The experiment is designed to allow for simultaneous operation of the two links.

Both links have access to a total bandwidth of 1 MHz and transmit using a carrier frequency of 1.5 GHz. The 1 MHz bandwidth is divided into 128 subcarriers.Among the available 128 subcarriers, only 112 subcarriers are used for data transmission. The remaining 16 subcarriers are used for control and synchronization purposes. Our experiments on this setup revealed that OFDM implementations using the USRP2 platform are not robust when using less than 4 subcarriers on a single link. Hence, we group the 112 data subcarriers into groups of 4 subcarriers each to form 28 channels, each having a bandwidth of 31.25 kHz.

Algorithm 1: Guard band creation after channel allocation

Input: $\mathbf{A}$, r_l^m, r_l
Output: $\mathbf{A}$
l_b = link using channel 1
$m_b = 1$
for $m = 2$ *to* M **do**
  l_n = link using channel m
  if *(*$(l_n \neq l_b)$ *and* $(l_n \neq NULL)$*)* **then**
    if *(*$(r_{l_n} - r_{l_n}^m) \leq (r_{l_b} - r_{l_b}^{m_b})$*)* **then**
      $a_{l_n m} = 0$,
      $r_{l_n}^m = 0$,
    else
      $a_{l_b m_b} = 0$,
      $r_{l_b}^{m_b} = 0$,
    end
  end
  $m_b = m$
  $l_b = l_n$
end

A significant challenge that affected synchronization as well as data transmission while running our experiment was interference from the sidelobes of adjacent channels that were being used by either the interferer or the other link in the network. Different methods of handling the issue of sidelobe power have been proposed including the usage of a guard band or techniques for sidelobe suppression [26, 27, 85]. While this problem can also be addressed by designing filters with sharp cut-offs, such a solution is not practical in a dynamic system where spectrum allocation changes constantly. To resolve issues with synchronization due to sidelobe interference, we set aside 8 subcarriers at

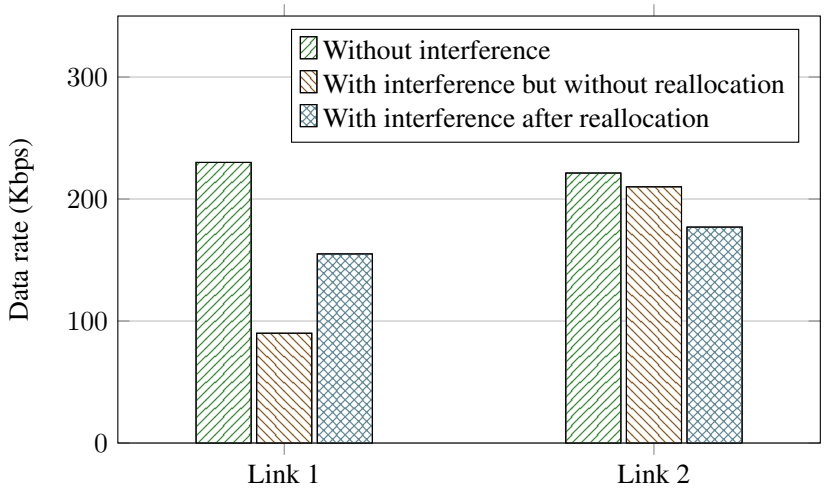


Figure 3.8: Data rates obtained using the ORBIT testbed.

either end of the 1 MHz spectrum exclusively for synchronization in each of the two links. For each link, robust synchronization was achieved by transmitting PN-sequence preambles [86] through the 8 dedicated subcarriers assigned to that link. To address sidelobe interference among the data subcarriers, subsequent to channel allocation by the integer program, a guard band is introduced whenever adjacent subcarriers are assigned to different links. The guard band is created by nulling one of the two adjacent channels, resulting in a small loss in throughput while increasing the overall signal quality. The pseudocode for deciding which of the two adjacent channels to null is presented in Algorithm 1, and operates on the principle of nulling the channel that leads to the smallest drop in throughput. Fig. 3.7 presents a block diagram of our implementation of NC-OFDM using GNU Radio; note the separation between the data and synchronization paths at the receiver.

Due to the short distance between the USRP nodes in the experimental setup, the channel gains between the nodes are approximated using a line-of-sight path loss model. Channel allocation was carried out at a centralized location using the framework proposed in Section III-A. The allocated channels were then conveyed to each of the two links, which was followed by the insertion of guard bands as described earlier.

Fig. 3.8 plots the throughput achieved in each of the two links through such an

experimental setup. The results in Fig. 3.8 follow the same general trend that was observed in Fig. 3.5 despite the insertion of guard bands and the lack of perfect channel knowledge.

3.5 Chapter Summary

This chapter considered the problem of fair spectrum allocation in NC-OFDM-enabled point-to-point links in the presence of interfering nodes while imposing a spectrum span constraint. Assuming a fixed transmit power across all subcarriers and orthogonal spectrum allocation, we formulated a linear integer program to maximize the minimum rate in the network under certain spectrum span constraints. Such an optimization problem can be efficiently solved using readily available solvers. It was seen that there exists a clear trade-off between the spectrum span and the max-min rate. Simulation results indicated that the spectrum span can be restricted to a relatively small number without adversely affecting the overall throughput of the system. An experimental evaluation of the techniques developed in this work using USRPs on the ORBIT radio network testbed was also presented. Experimental results further strengthen the general trend observed in simulations.

Chapter 4

Synchronization Challenges in NC-OFDMA

4.1 Impairments due to lack of synchronization

We consider a secondary network of L point-to-point (p2p) links that operate over a wide bandwidth of potentially disjoint bands of frequencies, as shown in Fig. 4.1. The links in this network are assumed to use NC-OFDM and are assigned a subset of subcarriers for transmission. All links are assumed to use N-subcarrier OFDM, with the same subcarrier spacing. Subcarriers occupied by incumbent transmissions are not assigned to any of the links. More importantly, the p2p links are assumed to transmit asynchronously, i.e., the start of the OFDM symbol is not governed by a global clock. Further, we assume that the cross channels gains in the secondary network can be as strong as the direct channel gains.

Since the secondary network may be deployed in scenarios with no centralized control and coordination, it may not always be possible to synchronize the L links. Under such a setting, the asynchronous nature of these transmissions results in interference between these p2p links, despite them being assigned non-overlapping subcarriers. This inter-carrier interference (ICI) is caused due to loss of orthogonality between the subcarrier waveforms arising from the lack of synchronization between the OFDM symbols transmitted by two different links. In addition to this, ICI is also caused by frequency offset between any two links. We characterize the ICI resulting from the lack of timing and frequency synchronization across the multiple p2p links. Focusing on ICI between a pair of subcarriers assigned to two different links, it is seen that the ICI is a function of the transmit power of the interfering subcarrier, the exact timing and frequency offset, and the spacing between the subcarriers (difference in indices). More importantly, it is noticed that the cumulative ICI from all the interfering subcarriers can be severe even

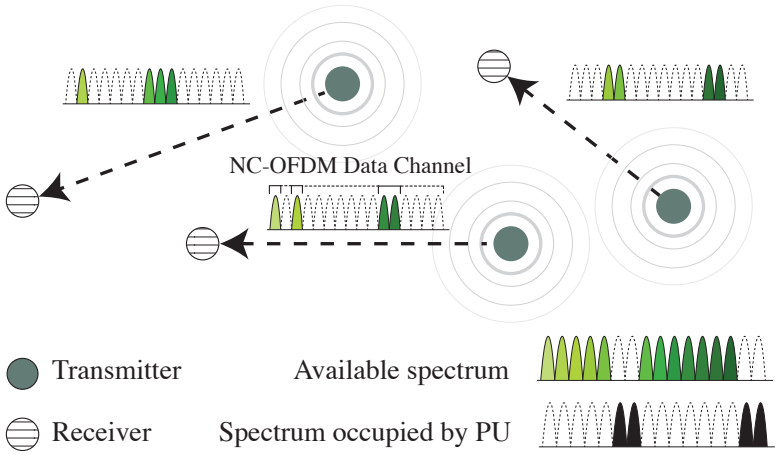


Figure 4.1: Asynchronous p2p communication using NC-OFDMA.

when the links aim to achieve moderate signal-to-noise ratios (SNR).

The severity of this ICI prompts a careful examination of how such NC-OFDM systems are to be designed. Noting that these issues can be alleviated by enabling timing coordination across multiple transmissions, this chapter presents one such scheme wherein NC-OFDM links use beacon signals to synchronize the start of their NC-OFDM symbols. In the proposed scheme low-power underlay PN-sequences are periodically transmitted to indicate the start of an NC-OFDM symbol. These PN-sequences acts as beacons for subsequent NC-OFDM links to synchronize their own transmissions. We present experimental results using a USRP platform which show that enabling such timing coordination is effective in mitigating ICI. These results reveal that the benefits of this scheme are particularly significant at higher operating SNRs. However, in the absence of such a mechanism to enable timing coordination guard band allocation and power control play a crucial role in mitigating this ICI.

Using the results on ICI characterization we propose a guard band design to limit interference to be below a certain threshold for a given secondary SNR. Such a design reveals that guard band requirements can significantly impact the number of subcarriers available for transmission when the secondary links operate at high SNRs. This highlights the importance of addressing subcarrier assignment, guard band allocation and transmit power control in a holistic manner when designing asynchronous NC-OFDM systems. Since such an optimization requires significant coordination across

the L links in addition to knowledge of all cross-channel gains (requirements that are hard to satisfy in a secondary network that is opportunistically using the spectrum), we instead make as few assumptions on channel knowledge as necessary and focuses on establishing broad guidelines on the choice of transmission parameters such as the number of contiguous subcarriers allocated to a link, the range of operating SNRs, and the length of guard bands to ensure viability of such networks.

While the design of asynchronous NC-OFDM systems has been of interest only recently, issues arising from the asynchronous arrival of the transmitted symbols is well studied in the context of uplink transmissions in cellular networks that use OFDMA. The resulting ICI in such a context is characterized in [87, 88]. Multiple access interference due to asynchronous transmissions is also studied in the context of ad-hoc networks [89–91]. While [88–91] focus exclusively on timing offset, ICI due to frequency offset is also considered in [87]. Although certain aspects of the ICI analysis in this chapter overlap with the existing literature, its impact on the design of asynchronous NC-OFDM systems has not been studied before—this forms the primary focus of this thesis.

Typically, to mitigate the effects of this ICI, mechanisms to estimate time and frequency offsets in OFDMA transmissions [92–94] or interference cancellation techniques are proposed [93,95]. While the use of interference cancellation techniques is possible in uplink communications where all received signals are of interest, it is not immediately applicable in the context of designing asynchronous NC-OFDM systems. Another mechanism to avoid interference is to perfectly filter all undesired subcarriers, however, this method is not very practical in a dynamic environment where channel allocation might change frequently; further, it also introduces a new interference term as the OFDM subcarrier shape (sinc) is altered due to filtering [96]. Unlike the above approaches that try to actively counter the resulting ICI at the cost of increased complexity and the need for global channel knowledge, this chapter focuses on avoiding this ICI by the use of guard bands. Guard band design based on such an analysis has not been proposed to the best of our knowledge. Unlike previous works that assume guard band to be a fixed constant [97, 98], our analysis reveals that guard band design is intrinsically We take

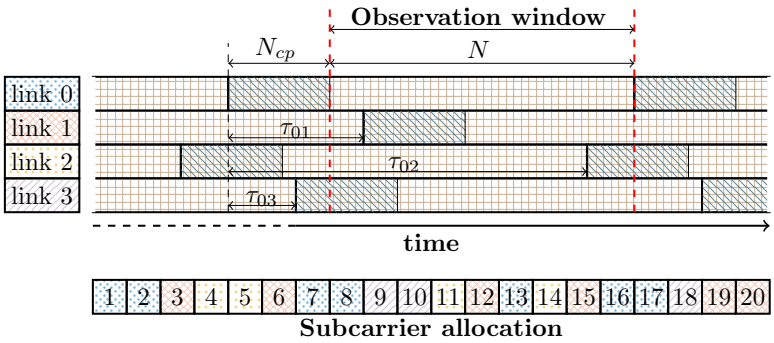


Figure 4.2: Time offset in asynchronous NC-OFDM system with $L = 4$ links and $N = 20$ subcarriers.

this analysis even further to establish a set of guidelines on the choice of transmission parameters that are best suited for asynchronous NC-OFDM systems.

4.2 System Model

Consider a network of L p2p wireless links communicating using NC-OFDM over a bandwidth of B Hz. Some portions of this bandwidth may be occupied by an incumbent or primary user (PU) and only the remaining bandwidth, that is potentially non-contiguous, is available for the L links to use. The ability to quickly adapt to changes in the incumbent transmissions motivates the use of NC-OFDM. NC-OFDM divides the available bandwidth into N subcarriers, each with a bandwidth of $f_s = \frac{B}{N}$ Hz. The lth link is assigned a set of subcarriers $\mathcal{A}_l$ such that

$$\mathcal{A}_l \subseteq \{1, 2, 3, 4, \ldots, N\} \quad \forall l \in \mathcal{L}, \tag{4.1}$$

$$\mathcal{A}_l \cap \mathcal{A}_{l'} = \emptyset \quad \forall\, l \neq l', \tag{4.2}$$

where $\mathcal{L} = \{1, 2, \ldots, L\}$. Subcarriers occupied by the PU are not allocated to any of the L links. The effect of the PU is further minimized by creating a guard band of subcarriers around the PU. With the PU sufficiently isolated, and in an ideal scenario with no time and frequency offset between the links, such an allocation will result in non-interfering transmissions between the L secondary links. However, in this work, we assume that the L links operate in an asynchronous manner, i.e., the start and end of their OFDM frames are not centrally managed. Fig. 4.2 represents such a

network with 4 links. The asynchronous nature of these transmissions in addition to potential frequency offsets leads to loss of orthogonality between the subcarriers and results in inter-carrier interference (ICI). We focus on understanding the impact of this ICI and its implications on designing networks based on NC-OFDM. Henceforth, we focus exclusively on the asynchronous secondary transmissions and assume the entire bandwidth to be available.

Let the symbols transmitted by Link l on the mth subcarrier of the kth OFDM symbol be denoted by $c_{km}^{(l)}$. We assume that the symbols are independently drawn and have variance $\alpha_m^{(l')}$. At the transmitter, the time domain samples are obtained from the transmit symbols after an N-point IDFT and are given by

$$C_{kn}^{(l)} = \begin{cases} \frac{1}{\sqrt{N}} \sum_{m \in \mathcal{A}_l} c_{km}^{(l)} e^{\frac{j2\pi m(n-N_{cp})}{N}}, & N_{cp} \leq n \leq N_{cp}+N-1 \\ C_{k(n+N)}^{(l)}, & 0 \leq n \leq N_{cp}-1, \end{cases} \tag{4.3}$$

where N_{cp} is the length of the cyclic prefix. The transmitted signal is then given by

$$x^{(l)}[p] = \sum_k \sum_n C_{k,n}^{(l)} \delta\left(p - n - (N+N_{cp})k\right), \tag{4.4}$$

where $\delta()$ is the Kronecker delta function. Note that the total duration of an OFDM symbol is $N_t T_s$, where $T_s = 1/B$ is the sample duration and $N_t = N + N_{cp}$. At the receiver, the received signal after sampling at a rate of $1/T_s$ is given by

$$r^{(l)}[p] = \sum_{l' \in \mathcal{L}} h_{ll'} e^{j2\pi(\delta f_{ll'})pT_s} x^{(l')}[p - \tau_{ll'}] + z^{(l)}[p], \tag{4.5}$$

where $z^{(l)}[p]$ denotes additive noise, $\tau_{ll'}$ represents the time offset between the start of the OFDM symbols of links l and l', $\delta f_{ll'}$ represents the frequency offset between the receiver of Link l and transmitter of l', and $h_{ll'}$ denotes the fading coefficient, including distance dependent path loss. We assume the frequency offset $\delta f_{ll'}$ to be in the range of $(-\delta f_0, \delta f_0)$ Hz. The time offset $\tau_{ll'}$ is assumed to be an integer multiple of sample duration (T_s). While actual time offset need not be an integer multiple T_s, considering the long duration of the OFDM symbol, a more careful analysis does not

significantly impact the results presented here. Also note that although we assume a flat fading channel, it is easy to incorporate multipath (frequency selective) fading in our analysis by extending the summation in (4.5) to also include all significant signal paths while accounting for their respective delays. Since the overall goal of this chapter is to derive guidelines for designing asynchronous NC-OFDM systems, we restrict focus to a flat fading channel and present a worst-case analysis of the ICI while making as few assumptions on the exact channel conditions as possible.

Assuming the start of an OFDM symbol to be known exactly (i.e. $\tau_{ll} = 0$), receiver l first splits $r[n]$ into sequences of length N_t and drops the cyclic prefix. Fig. 4.2 illustrates this by identifying the observation window for Link 0. The remaining length-N sequence is passed through an N-point DFT to recover the transmitted symbols. Setting $\tau_{ll} = 0$, the signal corresponding to the mth subcarrier of the kth OFDM symbol is given by

$$\hat{c}_{km} = \frac{1}{\sqrt{N}} \sum_{n=N_{cp}}^{N_t-1} r[N_t k + n] e^{\frac{-j2\pi m(n-N_{cp})}{N}} \tag{4.6}$$

$$\begin{aligned} =& \tfrac{1}{\sqrt{N}} \sum_{n=N_{cp}}^{N_t-1} h_{ll} x^{(l)}[N_t k + n] e^{\frac{-j2\pi m(n-N_{cp})}{N}} \\ &+ \tfrac{1}{\sqrt{N}} \sum_{n=N_{cp}}^{N_t-1} \sum_{l' \neq l} \Big\{ h_{ll'} x^{(l')}[N_t k + n - \tau_{ll'}] e^{2\pi j \delta f_{ll'} N_t k T_s} e^{2\pi j \delta f_{ll'} n T_s} e^{\frac{-j2\pi m(n-N_{cp})}{N}} \Big\} \\ &+ \tilde{z}^{(l)}[N_t k + n] \end{aligned} \tag{4.7}$$

$$\begin{aligned} =& h_{ll} c_{km}^{(l)} + \tfrac{1}{\sqrt{N}} \sum_{n=N_{cp}}^{N_t-1} \sum_{l' \neq l} \Big\{ h_{ll'} x^{(l')}[N_t k + n - \tau_{ll'}] e^{2\pi j (\delta f_{ll'})(N_t k + n) T_s} e^{\frac{-j2\pi m(n-N_{cp})}{N}} \Big\} \\ &+ \tilde{z}^{(l)}[N_t k + n]. \end{aligned} \tag{4.8}$$

In the absence of any time and frequency offsets, it is easy to see that the second term representing ICI evaluates to zero.

4.3 Effect of timing and frequency offset

In the following analysis, we focus on a particular subcarrier m and study the impact of an interfering subcarrier μ on this subcarrier. Assuming the impact from all the interfering subcarriers to be independent of each other, the aggregate impact on subcarrier m is obtained by simply summing the ICI for all values of μ. While subcarriers

belonging to the same link have the same time and frequency offset, assuming them to be independent allows the analysis to be agnostic to the exact subcarrier allocation. For notational convenience, we define the relative frequency offset $\epsilon_{ll'}$ as

$$\epsilon_{ll'} = \frac{\delta f_{ll'}}{f_s} = \frac{N\delta f_{ll'}}{B}. \tag{4.9}$$

Focusing on subcarrier m and setting $\mathcal{A}_{l'} = \{\mu\}$, the ICI resulting from subcarrier μ is given by

$$I_{\mu\to m} = \tfrac{1}{\sqrt{N}} \sum_{n=N_{cp}}^{N_t-1} \Big\{ h_{ll'} x^{(l')}[N_t k + n - \tau_{ll'})] e^{\frac{2\pi j(\epsilon_{ll'})(N_t k+n)}{N}} e^{\frac{-j2\pi m(n-N_{cp})}{N}} \Big\}. \tag{4.10}$$

Since we focus on subcarrier-to-subcarrier impact, we redefine the time and frequency offsets using subcarrier indices and set $\tau_\mu = \tau_{ll'}$ and $\epsilon_\mu = \epsilon_{ll'}$ in the rest of the analysis. Due to the periodicity of the OFDM transmissions, it suffices to consider τ_μ such that $0 \le \tau_\mu \le N + N_{cp} - 1$. The impact of an interfering subcarrier can be categorized into two cases as illustrated in Fig. 4.2 where Link 0 is the link of interest and Links 1, 2 and 3 are interfering links with different time offsets. When $0 \le \tau_\mu \le N_{cp}$, as in the case of Link 3, the interfering signal component from subcarrier μ belongs to a single OFDM symbol. However, when $N_{cp} < \tau_\mu \le N + N_{cp} - 1$, the interfering signal component from subcarrier μ belongs to two contiguous and independent OFDM symbols. This is the case with Links 1 and 2 in Fig. 4.2. The resulting interference in both these cases can be characterized as follows:

Case 1 : $0 \le \tau_\mu \le N_{cp}$: In this case, only a single OFDM symbol contributes to interference and hence,

$$\begin{aligned}
I_{\mu\to m} &= \tfrac{h_{ll'}}{\sqrt{N}} \sum_{n=N_{cp}}^{N_t-1} \Big\{ \frac{1}{\sqrt{N}} c_{k\mu}^{(l')} e^{\frac{j2\pi\mu(n-\tau_\mu-N_{cp})}{N}} e^{\frac{2\pi j\epsilon_\mu(N_t k+n)}{N}} e^{\frac{-j2\pi m(n-N_{cp})}{N}} \Big\} \\
&= \tfrac{1}{\sqrt{N}} \sum_{\tilde{n}=0}^{N-1} \Big\{ h_{ll'} \frac{1}{\sqrt{N}} c_{k\mu}^{(l')} e^{\frac{j2\pi\mu(\tilde{n}-\tau_\mu)}{N}} e^{\frac{2\pi j(\epsilon_{ll'})(N_t k+\tilde{n}+N_{cp})}{N}} e^{\frac{-j2\pi m(\tilde{n})}{N}} \Big\} \\
&= \tfrac{1}{\sqrt{N}} \sum_{\tilde{n}=0}^{N-1} \Big\{ h_{ll'} \frac{1}{\sqrt{N}} c_{k\mu}^{(l')} e^{\frac{j2\pi\mu(\tilde{n}-\tau_\mu)}{N}} e^{\frac{2\pi j(\epsilon_{ll'})(N_t k+N_{cp})}{N}} e^{\frac{-j2\pi m(\tilde{n}-\epsilon_{ll'})}{N}} \Big\}
\end{aligned}$$

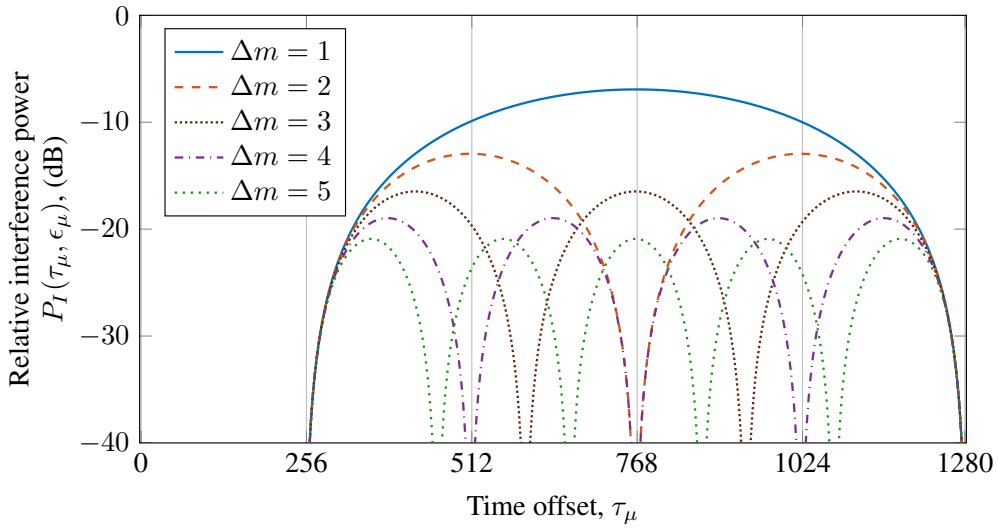


Figure 4.3: Relative interference power for different values of Δm and zero frequency offset with $N = 1024$ and $N_{cp} = 256$. The plot can be interpreted to show the INR at subcarrier m when the interfering signal at subcarrier μ is received at 0 dB INR.

$$= \frac{h_{ll'} e^{j2\pi\theta}}{N} \sum_{\tilde{n}=0}^{N-1} \left\{ c_{k\mu}^{(l')} e^{j2\pi \frac{\mu(\tilde{n}-\tau_\mu)-\tilde{n}(m-\epsilon_\mu)}{N}} \right\}, \tag{4.11}$$

where $\theta = \epsilon_\mu(N_t k + N_{cp})/N$. This can be further simplified to show that the resulting interference power is given by

$$\mathbf{E}\left[|I_{\mu\to m}|^2\right] = \frac{\alpha_m^{(l')} |h_{ll'}|^2 \sin^2(\pi\hat{m})}{N^2 \sin^2(\pi\hat{m}/N)} = \alpha_m^{(l')} |h_{ll'}|^2 P_{I,\mu}^{(m)}(\tau_\mu, \epsilon_\mu), \tag{4.12}$$

where

$$P_{I,\mu}^{(m)}(\tau_\mu, \epsilon_\mu) = \frac{\sin^2(\pi\hat{m})}{N^2 \sin^2(\pi\hat{m}/N)}, \tag{4.13}$$

and

$$\hat{m} = \mu - m + \epsilon_\mu = \Delta m + \epsilon_\mu. \tag{4.14}$$

Note that when $\epsilon_\mu = 0$ and $m \neq \mu$ this interference is always zero, suggesting that the cyclic prefix provides some robustness against time offset, as long as the time offset is smaller than N_{cp}. More generally, for $\epsilon_\mu \neq 0$ it can be seen that the interference is not a function of τ_μ. However, since $P_{I,\mu}^{(m)}(\tau_\mu, \epsilon_\mu)$ decays rapidly as $\hat{m}$ increases,this interference is only significant when the subcarriers μ and m are close to one another.

Case 2 : $N_{cp} < \tau_\mu \leq N + N_{cp} - 1$: In this case, two NC-OFDM symbols contribute to interference, and hence,

$$\begin{aligned}
I_{\mu\to m} &= \frac{h_{ll'}}{\sqrt{N}} \sum_{n=N_{cp}}^{\tau_\mu-1} \left\{ \frac{1}{\sqrt{N}} c_{(k-1)\mu}^{(l')} e^{\frac{j2\pi\mu(n-\tau_\mu+N)}{N}} e^{\frac{2\pi j\epsilon_\mu(N_t k+n)}{N}} e^{\frac{-j2\pi m(n-N_{cp})}{N}} \right\} \\
&\quad + \frac{h_{ll'}}{\sqrt{N}} \sum_{n=\tau_\mu}^{N_t-1} \left\{ \frac{1}{\sqrt{N}} c_{k\mu}^{(l')} e^{\frac{j2\pi\mu(n-\tau_\mu-N_{cp})}{N}} e^{\frac{2\pi j\epsilon_\mu(N_t k+n)}{N}} e^{\frac{-j2\pi m(n-N_{cp})}{N}} \right\} \\
&= \frac{h_{ll'}e^{2\pi j\theta}}{N} \left[\sum_{\tilde{n}=0}^{\tau_\mu-N_{cp}-1} \left\{ c_{(k-1)\mu}^{(l')} e^{j2\pi\frac{\mu(\tilde{n}+N_t-\tau_\mu)-\tilde{n}(m-\epsilon_\mu)}{N}} \right\} \right. \\
&\quad \left. + \sum_{\tilde{n}=\tau_\mu-N_{cp}}^{N-1} \left\{ c_{k\mu}^{(l')} e^{j2\pi\frac{\mu(\tilde{n}-\tau_\mu)-\tilde{n}(m-\epsilon_\mu)}{N}} \right\} \right] \\
&= \frac{h_{ll'}}{N} \left(e^{j\phi_1} \sum_{\tilde{n}=0}^{\tau_\mu-N_{cp}-1} c_{(k-1)\mu}^{(l')} e^{j2\pi\frac{\hat{m}\tilde{n}}{N}} + e^{j\phi_2} \sum_{\tilde{n}=\tau_\mu-N_{cp}}^{N-1} c_{k\mu}^{(l')} e^{j2\pi\frac{\hat{m}\tilde{n}}{N}} \right),
\end{aligned} \tag{4.15}$$

where $\hat{m}$ is as defined in (4.14) and ϕ_1 and ϕ_2 are some constants independent of n. The interference power in this case is given by

$$\mathbf{E}\left[|I_{\mu\to m}|^2\right] = \alpha_m^{(l')} |h_{ll'}|^2 P_{I,\mu}^{(m)}(\tau_\mu,\epsilon_\mu), \tag{4.16}$$

where

$$P_{I,\mu}^{(m)}(\tau_\mu,\epsilon_\mu) = \tfrac{1}{N^2} \left| \sum_{n=0}^{\tau_\mu-N_{cp}-1} e^{\frac{j2\pi\hat{m}n}{N}} \right|^2 + \tfrac{1}{N^2} \left| \sum_{n=\tau_\mu-N_{cp}}^{N-1} e^{\frac{j2\pi\hat{m}n}{N}} \right|^2. \tag{4.17}$$

Using (4.12) and (4.16), we now examine the resulting ICI as a function of time and frequency offset. Note that the strength of this ICI is proportional to the channel strength and the power of the signal received on subcarrier μ. To present the results in a manner that is independent of the actual channel gain values, we focus on the relative interference power, i.e. $\mathbf{E}[|I_{\mu\to m}|^2]/(\alpha_m^{(l')}|h_{ll'}|^2) = P_{I,\mu}^{(m)}(\tau_\mu,\epsilon_\mu)$. Under the assumption that $|h_{ll'}| \leq |h_{l'l'}|$ subtracting the relative interference power (in dB) from the operating SNR of Link l' gives the maximum interference-to-noise ratio (INR) at Link l due to subcarrier μ. Fig. 4.3 plots the relative interference power as a function of the time offset τ_μ and the difference in subcarrier index Δm assuming no frequency offset. It can be seen that the resulting ICI can be significant on the neighboring subcarriers. For example, suppose subcarrier $(m+1)$ is assigned to Link l' and the signal from this

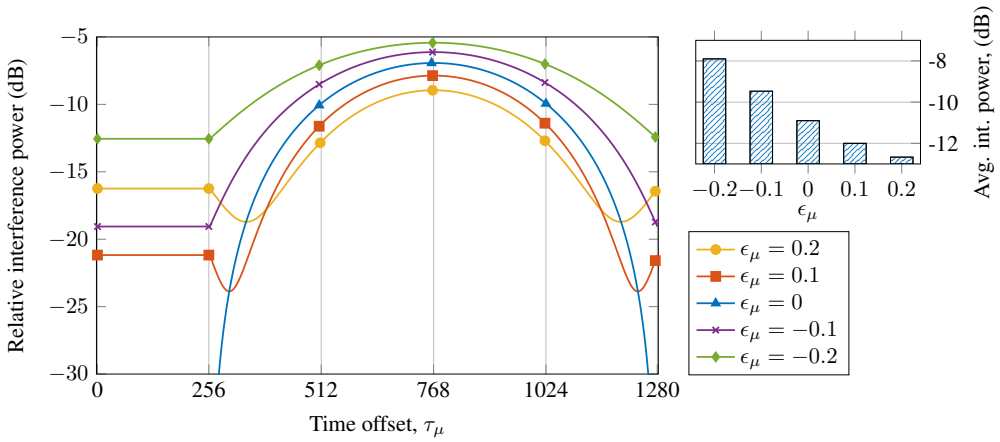


Figure 4.4: Effect of frequency offset on relative interference power for $\Delta m = 1$, $N = 1024$ and $N_{cp} = 256$.

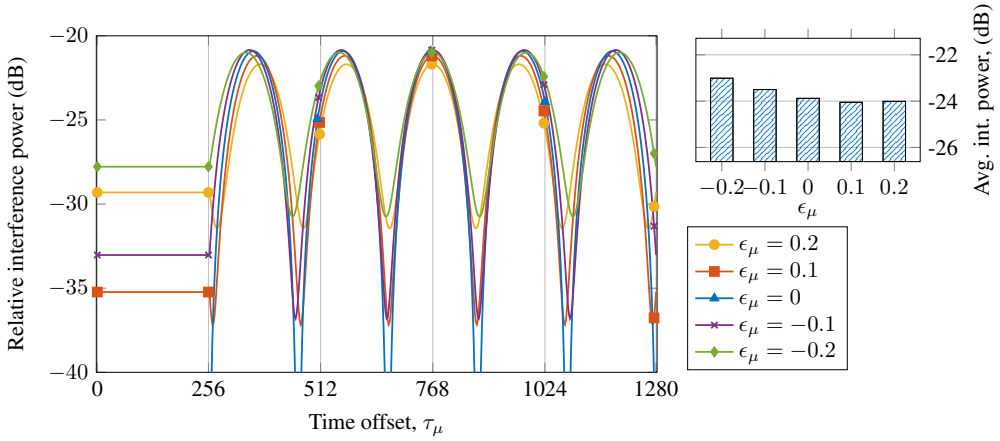


Figure 4.5: Effect of frequency offset on relative interference power for $\Delta m = 5$, $N = 1024$ and $N_{cp} = 256$.

transmission is received at the $(m+1)$ th subcarrier of Link l at 20 dB, then the worst case INR at subcarrier m of Link l can be as high as 12 dB, and remains above 10 dB for most values of τ_μ. In general, ICI decreases as Δm increases. As expected, we do not observe any interference when time offset is smaller than the cyclic prefix.

Figs. 4.4 and 4.5 set Δm to be 1 and 5 respectively, and consider the effect of frequency offset on the relative interference power. The frequency offset ϵ_μ is held fixed at $\pm 10\%$ or $\pm 20\%$ of the subcarrier spacing. Unlike Fig. 4.3, ICI is now observed even when τ_μ is less than the cyclic prefix. The effect of frequency offset is seen to diminish as Δm increases. Figs. 4.4 and 4.5 also plot the relative interference power averaged over all values of τ_μ, assuming τ_μ is governed by a uniform distribution. It

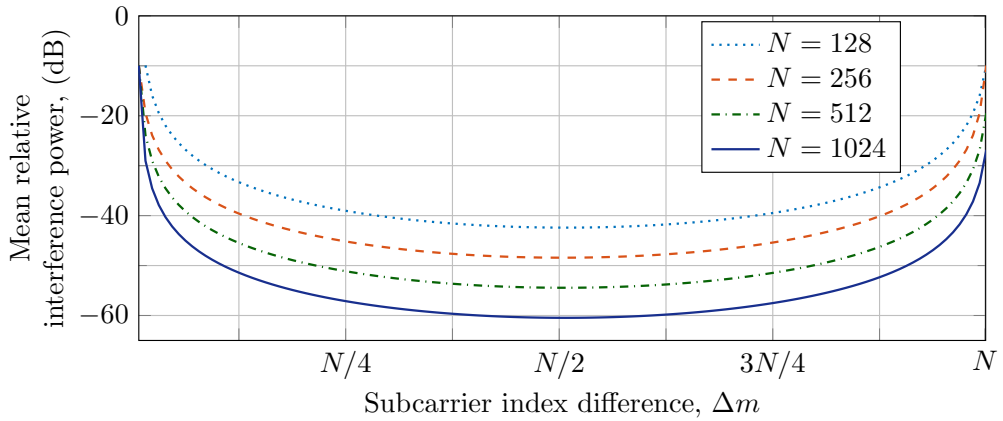


Figure 4.6: The mean relative interference power for $N = 1024$ and frequency offset $\epsilon = 0$.

can be observed that the effect of frequency offset is not symmetric across values of ϵ_μ, and this asymmetry is clearly seen for the case when $\Delta m = 1$. Positive offsets increase subcarrier separation thus leading to smaller ICI. When $\Delta m = 5$, for a wide range of frequency offsets, the average INR is around -24 dB when the received INR on subcarrier μ is 0 dB, with higher and more variability in INRs observed when $\Delta m = 1$.

Another important observation on relative interference power $P_{I,\mu}^{(m)}(\tau_\mu, \epsilon_\mu)$ is that this ICI is not a function of the subcarrier spacing, and instead only depends on the difference between the subcarrier indices, i.e., Δm. Consequences of this behavior are further explored in the next section.

Treating τ_μ as a uniformly distributed random variable, the mean relative interference power from subcarrier μ to subcarrier m is defined as

$$\hat{P}_{I,\mu}^{(m)}(\epsilon_\mu) = \mathbf{E}_{\tau_\mu}\left[P_I^{(m)}(\tau_\mu, \epsilon_\mu)\right]. \tag{4.18}$$

A vector representing mean relative interference caused by subcarrier μ on all other subcarriers is given by

$$\hat{\mathbf{P}}_{I,\mu}(\epsilon_\mu) = \left[\hat{P}_{I,\mu}^{(1)}(\epsilon_\mu),\ \hat{P}_{I,\mu}^{(2)}(\epsilon_\mu), \ldots,\ \hat{P}_{I,\mu}^{(N)}(\epsilon_\mu)\right]^T. \tag{4.19}$$

Fig. 4.6 plots the vector $\hat{\mathbf{P}}_{I,\mu}(\epsilon_\mu)$ with $\mu = 0$, $\epsilon_\mu = 0$ for varying N. The plots show that the ICI plateaus as Δm approaches $N/2$. This plateau decreases with increasing N. This plot indicates that a single high power subcarrier from an interfering link can potentially raise the effective noise floor for a large majority of subcarriers at the link of

interest. This indicates that the combined interference from only a few such interfering subcarriers can severely impact link performance. The curves are symmetric around $N/2$ due to the discrete signal model that factors in the effects of sampling the received signal at the Nyquist rate.

Before proceeding further, we define an $N \times N$ interference matrix Λ that succinctly captures the effect of time-and-frequency-offset-induced ICI. The (μ, m)th element of Λ, denoted as $\lambda_{\mu,m}$ represents the relative interference power from subcarrier μ to subcarrier m, when μ and m are assigned to two different links. In particular,

$$\lambda_{\mu,m} = \mathbf{E}_{\epsilon_\mu}[\hat{P}_{I,\mu}^{(m)}(\epsilon_\mu)], \tag{4.20}$$

where the expectation is computed assuming frequency offset to be a uniform random variable over a given range.

The analysis presented in this section shows that time offset between two different p2p NC-OFDM transmissions can significantly degrade the SINR for some of the subcarriers. To mitigate the impact of this effect, the p2p links can either try to coordinate transmissions in a decentralized manner or employ guard band and power control to sufficiently isolate their transmissions. The next two sections explore these two options.

4.4 Timing coordination to mitigate ICI

This section presents a scheme for timing coordination between two NC-OFDM links using beacons appended to the transmission and experimentally validates the effectiveness of such a scheme.

4.4.1 Proposed Methodology

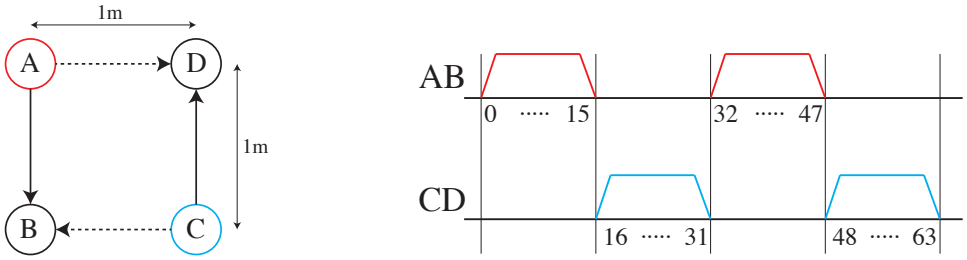
In the proposed scheme a low-power underlay PN-sequence is used as a beacon signal to indicate the start of an NC-OFDM symbol to other subsequent NC-OFDM links. Since it is important for this beacon signal to be independent of subcarrier assignment and easily detected by other neighboring NC-OFDM transmitters, this signal spans a bandwidth that is fixed beforehand and remains unchanged. Since this bandwidth may

subsequently be also occupied by primary or secondary transmissions, it is important that such a beacon be a low power signal, so as to minimize its impact on the incumbent transmissions. With these design considerations in mind, we periodically transmit a PN-sequence spanning the entire bandwidth to aid the other NC-OFDM links in the vicinity. Such an underlay transmission is also shown to be useful for timing and frequency recovery of NC-OFDM transmissions in [37]. As an alternative to transmitting an explicit beacon signal, other patterns and features that are implicitly present in most OFDM-based systems can also be used to aid timing coordination [99, 100].

Suppose that at a given instant an NC-OFDM transmitter is engaged in active transmission. This transmission, by design, consists of a low-power underlay PN-sequence followed by a fixed number of NC-OFDM symbols (constituting a frame) that are periodically transmitted as shown in Fig. 4.8. Now, when a second NC-OFDM transmitter is ready to start its own transmissions it first scans the medium for the presence of beacon signals that indicate ongoing signal transmissions. If no such beacons are found for a specified duration then the transmitter declares a time out and starts to transmit. If a beacon signal is detected then the timing of the beacon signal is used to determine the start of its own transmission as depicted in Fig. 4.8. If multiple beacon signals are detected then the start is determined by the strongest of these signals. Note that the start of transmission does not require frame-level synchronization. Even if the frames are offset, it suffices if the constituent NC-OFDM symbols are aligned in time. Further, it can be shown that if the cyclic prefix duration exceeds the channel delay spread (denoted as N_{ts}), then synchronization to within $(N_{cp} - N_{ts})/2$ samples of accuracy suffices to mitigate the interference due to timing offset.

4.4.2 Experimental Procedure

The method described above is used to establish timing coordination in a simple two-link NC-OFDM-based network. For experimental evaluation, we use the topology shown in Fig. 4.7a with two NC-OFDM links AB and CD where each link is using a disjoint set of subcarriers for communication. Solid arrows in Fig. 4.7a represent the intended transmission while the dashed arrows show the undesired interference to the other



(a) Topology (b) Subcarrier allocation

Figure 4.7: Experimental setup with two NC-OFDM links and corresponding subcarrier allocation.

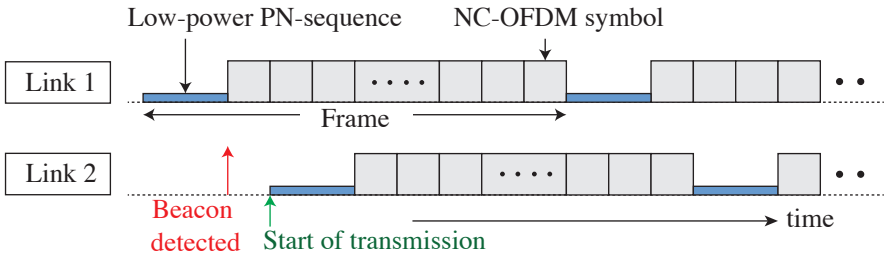


Figure 4.8: Beacon detection and NC-OFDM symbol alignment in experimental setup.

receiver. This topology allows us to observe the combined signal from two transmitters at either of the receivers with the ability to vary the time offset and signal power for both the links. In this experiment, we first start the transmissions of node A and then turn on node C, allowing the second transmitter to adjust its own transmissions based on the beacons detected from the first transmission. The signals from both transmitters are received at both the receivers and the intended transmission is recovered individually from this combined received signal.

4.4.3 Hardware and Parameter Settings

We use USRP N210 radios with SBX daughterboards having the capability to operate from 400 MHz to 4.4 GHz while transmitting up to a maximum bandwidth of 40 MHz [101]. The NC-OFDM links are set to operate over a 10MHz wide bandwidth, which is further divided into $N = 64$ subcarriers. The cyclic prefix is set to $N_{cp} = 16$, thus making each NC-OFDM symbol span a total of 80 samples lasting for $8\mu s$. For the purposes of this experiment, no primary transmissions are assumed. Subcarrier allocation between the two links is as shown in Fig. 4.7b, where subcarriers numbered 0

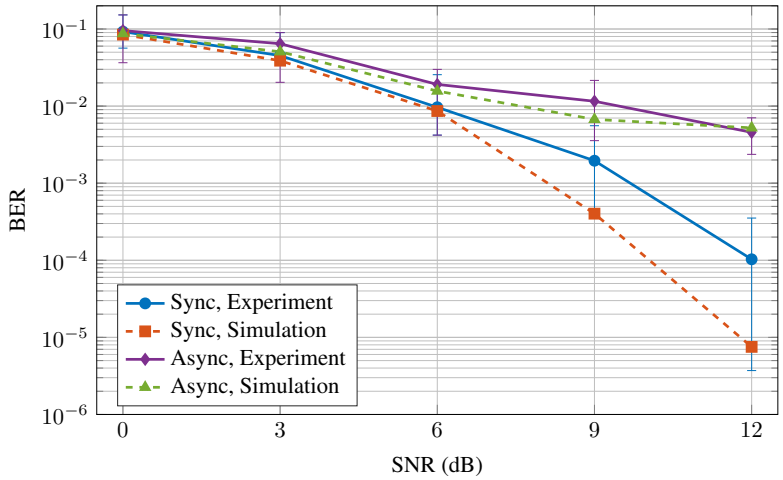


Figure 4.9: BER comparison between asynchronous and synchronous transmissions when SNRs for both links AB and CD are the same.

to 15 and 32 to 47 (total 32 subcarriers) are allocated for the link AB, while remaining 32 subcarriers are used by link CD. Since we are specifically focusing on analyzing the effect of asynchronous transmission, any effect of frequency offset between the two transmitters is removed by using a common external clock source. Note that the operation of searching for the beacons and adjusting the frame boundary is a one-time operation for this experimental setup since there is no frequency offset between the two transmitters. Note that in the presence of a frequency offset, a periodic beacon search is necessary to stay synchronized. The PN-sequence is chosen to 160 samples long (spans two NC-OFDM symbols). We use QPSK symbols for all our experiments.

4.4.4 Experimental Results and Observations

Fig. 4.9 presents the bit error rate (BER) from both synchronous and asynchronous transmissions when the target operating SNRs for both the links are set to be the same. The experimental results are also compared against simulation results from MATLAB. The simulation setup uses a simple additive-white-gaussian-noise (AWGN) channel and only considers the effect of timing offset between the two transmissions. Experimental and simulation results depicted in Fig. 4.9 show that asynchronous transmission has a clear detrimental effect on BER. In the case of asynchronous transmissions, it is seen that BER saturates between 10^{-2} and 10^{-3}, suggesting that unmitigated ICI can be a

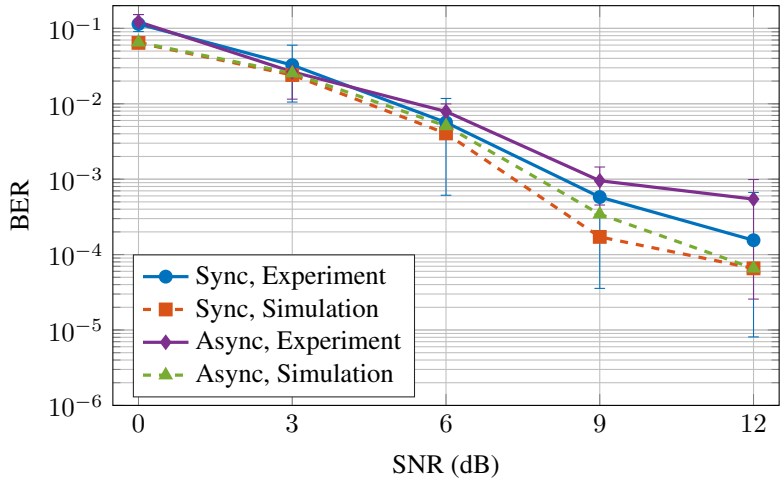
major impediment to operating at higher SNRs. It is precisely in the high SNR regime that the impact of timing coordination is significant, allowing the ability to achieve BERs of 10^{-4}.

Next, Fig. 4.10 considers a scenario where the two links operate at two different SNRs. In particular, the operating SNR of link AB is set to be 3 dB higher than the operating SNR of link CD (operating SNRs are set by turning on one link at a time). Fig. 4.10a shows the BER plot for link AB, where it can be observed that the impact of timing coordination is marginal, owing to lesser interference from the other link. However the impact of timing coordination on link CD, as shown in Fig. 4.10b is significant, with a considerable decrease in BER. These results suggest that when two NC-OFDM links with disjoint subcarrier allocations are transmitting simultaneously, it is in the interest of the link operating at lower SNR to use timing coordination to mitigate ICI from the other link.

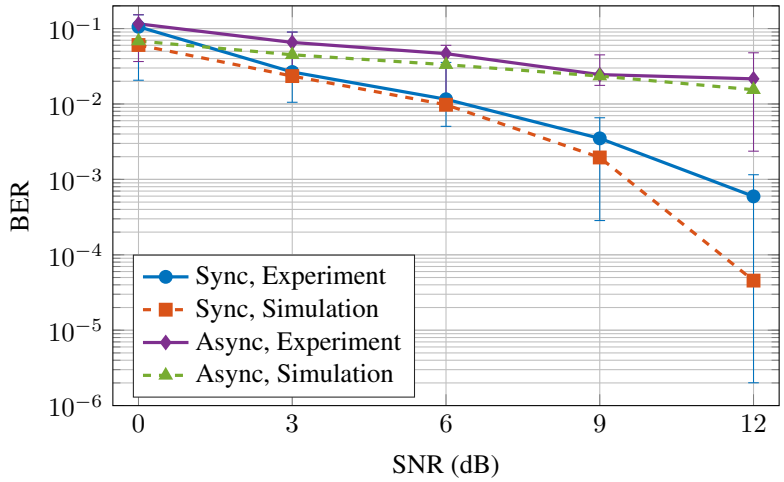
We observe that enabling decentralized timing coordination to align NC-OFDM symbols across different transmissions can improve the performance significantly. These improvements become more significant as the operating SNR increases. In a scenario where such timing coordination cannot be enabled, it becomes important to consider other alternatives to reduce ICI due to asynchronous transmissions. The next section looks into addressing this problem by studying guard band design between different transmissions and providing guidelines on selecting transmission parameters to strike the right balance between maximizing throughput while avoiding ICI.

4.5 Guard band requirement

This section utilizes the analysis presented in the section-4.3 to study guard band requirements in asynchronous NC-OFDM systems. The guard band is defined as the minimum separation required between subcarriers allocated to two different links to ensure that the ICI caused by time and frequency offsets are below a certain threshold. Subcarriers falling in the guard band are left unassigned. When direct and cross-channel gains are known at a centralized location, guard band design is intrinsically



(a) BER vs SNR for link AB



(b) BER vs SNR for link CD

Figure 4.10: BER performance comparison between asynchronous and synchronous transmissions when the SNR for link AB is 3 dB more than link CD.

coupled to subcarrier assignment and transmit power optimization. Since global channel knowledge is rarely known, we instead focus on a worst case guard band design that sidesteps the requirement of exact channel knowledge, with the aim of providing channel-agnostic guidelines on guard band design. We make a crucial assumption that the cross-channel gains are no stronger than the direct channel gains. Typical network formation protocols that pair a receiver to the strongest transmitter ensure that this criterion is satisfied. In such a setting, the received SNR of Link l' on subcarrier μ acts as an upper bound on the received INR on subcarrier μ at Link l. This upper bound on received INR is used to propose a worst-case guard band design.

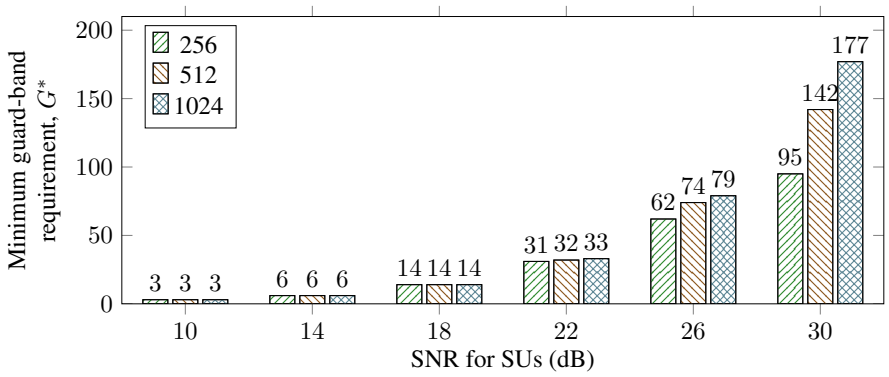


Figure 4.11: Minimum guard band requirement between SUs. Computed assuming cross channel links to be as strong as direct channel links.

To get an estimate of the minimum guard band required between two secondary links, we assume a scenario where M contiguous subcarriers are assigned to Link l (denoted as $\mathcal{A}_{l,M}$) with a guard band of G subcarriers on either side of this spectrum. The remaining subcarriers are assigned to Link l' (denoted as $\mathcal{A}_{l',M,G}$) which is operating at an SNR of ρ_{su}. Subcarrier indices are assumed to be circular so that a total of $2 \times G$ subcarriers are always set aside as guard band. The total interference power at subcarrier $m \in \mathcal{A}_{l,G}$ for such an allocation is approximated as

$$P_{I,M,G}^{(m)} = \sum_{k \in \mathcal{A}_{l',M,G}} \frac{|h_{ll'}|^2}{|h_{l'l'}|^2} \lambda_{k,m} \sigma^2 \rho_{su} \approx \sum_{k \in \mathcal{A}_{l',M,G}} \lambda_{k,m} \sigma^2 \rho_{su}, \tag{4.21}$$

where σ^2 is the per-subcarrier noise variance. In such a scenario, the guard band length G must be such that no subcarrier in $\mathcal{A}_{l,M}$ experiences ICI that exceeds a certain threshold I_{th}. Noting that the subcarriers at the extreme ends of $\mathcal{A}_{l,M}$ experience the most amount of ICI, it suffices to ensure that this criterion is satisfied at the two ends of the contiguous spectrum assigned to Link l. Further, with a worst-case guard band design in mind, it suffices to consider the case when $M = 1$ as the number of interfering subcarriers $|\mathcal{A}_{l',M,G}|$ is maximized for a given G. Thus the worst case guard band requirement when Link l' operates at an SNR of ρ_{su} can be expressed as

$$G^*(\rho_{su}) = \underset{G}{\operatorname{argmin}} : P_{I,1,G}^{(m)} \leq I_{th}$$

$$\forall\, \mathcal{A}_{l,1},\, \mathcal{A}_{l',1,G} \text{ with } m \in \mathcal{A}_{l,1}, \tag{4.22}$$

where $\mathcal{A}_{l,1}$ is a set containing a single subcarrier index. Choosing the length of guard band in this manner ensures that ICI is below the specified threshold for any contiguous allocation $\mathcal{A}_{l,M}$, irrespective of the choice of M.

Fig. 4.11 presents the required guard band computed using such an approach for various values of N and ρ_{su}. It can be seen from the figures that while the length of guard band remains at a reasonable value for secondary SNRs of up to 14 dB, the guard bands grow significantly longer when the operating SNRs exceed 22 dB. In fact this computation indicates that if a secondary link operates at 30 dB SNR, and if cross-channel gains are comparable to direct channel gains, then more than 20% of all available subcarriers are to be set aside as guard band, leading to a significant decrease in the throughput of such systems and a very inefficient use of available resource.

This observation also draws attention to the importance of the transmit power control in asynchronous NC-OFDM systems, despite the subcarriers being allocated in an orthogonal manner. Even with an orthogonal subcarrier allocation, ICI due to the asynchronous nature of transmissions couples the transmit power control (and consequently the operating SNRs) across the L links, making it difficult to infer a reasonable set of transmission parameters for such systems.

4.5.1 Guidelines for Transmission Parameters

Consider a channel-symmetric L-link NC-OFDM network where all direct channels are equal and cross channels are comparable to direct channels. In such a setting, all subcarriers are equivalent to each other and only the total number of subcarriers assigned to a link determines the throughput of the link, assuming sufficient guard bands are used to isolate the links. To ensure fairness across the L links, suppose that Q subcarriers are assigned to each link and that each link aims to operate at an SNR of ρ_{su}. To ensure ICI is less than the noise floor, subcarriers assigned to two different links are separated by $G^*(\rho_{su})$ subcarriers. Due to the equivalence between the N subcarriers and the need to use guard bands, it can be assumed without loss of generality that the

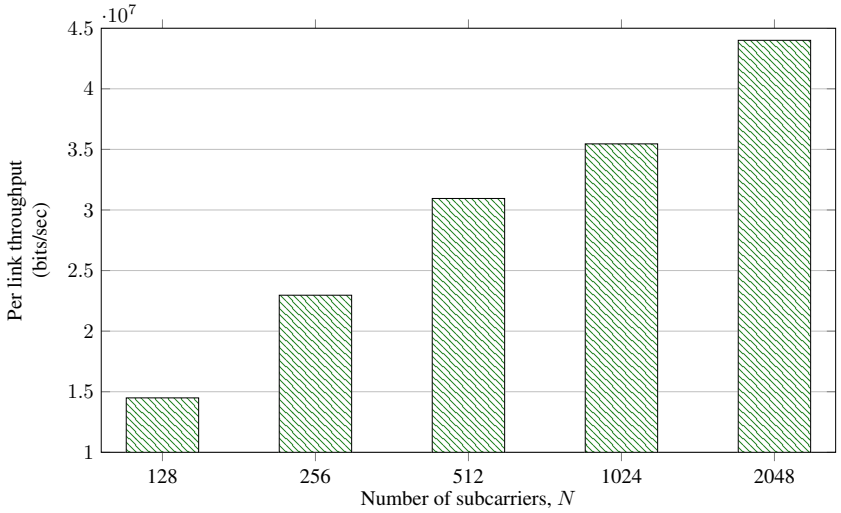


Figure 4.12: Per link throughput for varying values of N for B =100 MHz, $L = 10$ and $\delta f_0 = 10$ KHz. Bandwidth unavailable due to presence of PU = 10 MHz.

Table 4.1: Choice of parameters for different N resulting in highest per-link throughput

	Number of subcarriers, N				
	128	256	512	1024	2048
ρ_{su} (SNR in dB)	12	14	16	20	22
Q (Allocated subcarriers)	7	17	37	71	151
$G^*(\rho_{su})$ (Minimum guard band)	4	6	9	21	33

Q subcarriers assigned to a link will be contiguous. Thus, $\frac{Q}{Q+G^*(\rho_{su})}$ fraction of the available subcarriers are used for transmission with the rest serving as guard bands. Under these assumptions, the throughput r_l of a link is given by

$$\begin{aligned} r_l &= Q\frac{B}{N}\log_2(1+\rho_{su}) \\ &= \left(\left\lfloor \frac{N}{L} \right\rfloor - G^*(\rho_{su})\right)\frac{B}{N}\log_2(1+\rho_{su}). \end{aligned} \tag{4.23}$$

For a given L and N, the above expression is only a function of the secondary operating SNR ρ_{su}. Optimizing this throughput over the range of practical values for ρ_{su}, gives us the ideal operating SNR for such a network. Once the operating SNR is determined, it is straightforward to determine Q.

To illustrate the insight that can emerge from such a process, we consider setting

up a 10-link NC-OFDM network over a bandwidth of 100 MHz, of which 10 MHz is unavailable due to the presence of a PU. This 10 MHz is also assumed to include guard band around the PU transmission so as to sufficiently protect and isolate it. The remaining 90 MHz is to be distributed among the 10 secondary links. Using (4.23) as a measure of throughput and optimizing over the operating SNRs, Table 4.1 summarizes the set of transmission parameters that are best suited for operating this network for a range of values for N. The frequency offset is assumed to be in the range of -10 KHz to 10 KHz. This range is representative of general frequency offsets observed at carrier frequencies close to 1 GHz with up to 10 ppm error in oscillator frequency. It also ensures that relative frequency offset is within 20% of subcarrier spacing even for large N. The target SNR is varied from 0 dB to 30 dB in steps of 2 dB.

It can be observed from Table 4.1 that the ideal operating SNRs increase with N. This increasing trend is a direct consequence of ICI only depending on the difference in subcarrier indices and not on subcarrier spacing. Thus, for large values of N even if a higher number of subcarriers are used as the guard band, this does not amount to a large penalty in terms of absolute bandwidth. Guard band requirement in terms of absolute bandwidth is highest for $N = 128$ when each guard band occupies 3.06 MHz of bandwidth. Fig. 4.12 plots the optimized throughput as a function of N. As expected the throughput increases with N. Although this trend suggests setting N to large values, practical considerations such as coherence time of channel (large N leads to small subcarrier spacing, which in turn lengthens the duration of the OFDM symbol) place a natural limit on the value of N.

Finally, although these guidelines emerge from an analysis of the channel-symmetric NC-OFDM system, they nevertheless serve as useful starting points for further optimization in the general case and provide insight on overall system design along with expected throughput in such systems. Further, such an analysis establishes the viability of supporting asynchronous p2p links using NC-OFDM in spite of the ICI resulting from time and frequency offsets.

4.6 Chapter Summary

This chapter characterizes the ICI arising from time and frequency offset in asynchronous p2p links that use NC-OFDM. It is observed that the time offset across different links can cause substantial interference even with orthogonal subcarrier allocation across the links, while the effect of frequency offset is significant only when the subcarriers assigned to these links are close to each other. A decentralized synchronization scheme using beacons appended to NC-OFDM symbols is presented and experimentally verified to be effective in mitigating the ICI arising from asynchronous transmissions. Results from the experiment indicate that enabling timing coordination is particularly beneficial when operating at high SNRs. For cases when such timing coordination cannot be enabled, our analysis is used to compute guard band requirements for such systems so that the resulting ICI is negligible. This result also highlights the importance of the transmit power control in asynchronous NC-OFDM systems even when subcarriers are orthogonally assigned. Guidelines on the choice of basic transmission parameters such as length of contiguous subcarriers assigned to a link and operating SNRs for each link are also provided.

Chapter 5

Control Channel Design for NC-OFDMA

5.1 Requirement of a control channel

With the ever-increasing requirement for higher wireless data rates, efficient utilization of all available spectrum, licensed or otherwise, becomes paramount. In particular, with the wide availability of unlicensed spectrum in the TV-white-space band, the U-NII and ISM bands, and the requirement for dynamic frequency selection (DFS) to avoid interference with radar or other ISM devices, the ability to effectively use noncontiguous spectrum is vital to exploit the full potential of the available spectrum. This chapter considers the design of a cognitive network of multiple point-to-point (p2p) links that operate over a wide bandwidth of several disjoint bands of frequencies, as shown in Fig. 5.1. Two key components to any cognitive network are the data plane and the control plane. Rather than treating them as two independent components, we take a holistic approach and focus on the design of a control channel that is tailor-made for an NC-OFDM-based data plane. In particular, we discuss the design and implementation of a low-power CDMA-like underlay control channel (UCC) for each link that is designed specifically with the needs of NC-OFDM in mind.

Control channel design for cognitive networks is a well-studied subject [102–109] with designs that can be broadly classified as either being in-band or out-of-band. Out-of-band designs call for a dedicated narrowband channel that is used to transmit the control signals [102, 105], while in-band designs typically involve a UCC spanning the full bandwidth [103, 104, 109]. While a dedicated narrowband control channel is straightforward to implement and provides higher reliability, setting aside a dedicated narrowband chunk of the spectrum may not always be feasible, or sometimes even unnecessary. In-band designs typically propose to use spread spectrum techniques to

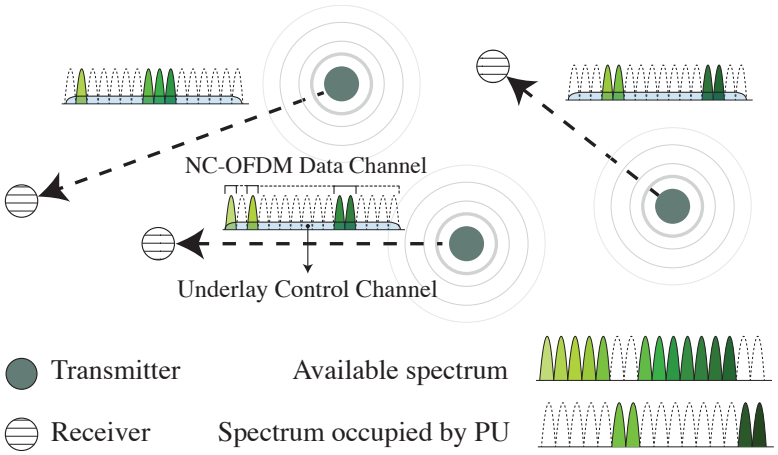


Figure 5.1: A cognitive network of multiple point-to-point links using NC-OFDM to access noncontiguous spectrum.

implement a low-power UCC spanning the entire bandwidth with or without considerations for the primary transmissions [103, 104]. Although such a design is exposed to the primary and secondary transmissions, it involves no spectrum overhead and is well-suited for a low-data-rate communication channel. We propose an in-band UCC spanning the entire bandwidth, as shown in Fig. 5.1.

When a p2p cognitive link uses NC-OFDM, the receiver of this link sees the aggregate of the desired NC-OFDM signal along with all the other concurrent transmissions. Due to the dynamic nature of this interference, it is not always possible to filter these transmissions out. Under such circumstances, traditional techniques for OFDM timing recovery that rely on some form of symmetry in the time domain waveform [31–34] are no longer reliable. Although techniques involving custom preamble design for NC-OFDM are available [35], they are not well suited to be applied in dynamic environments. In this chapter, we aim to solve this problem by designing a UCC to specifically aid timing and frequency offset recovery in addition to providing a low-rate communication link to share the control data. We propose an independent UCC for each p2p link in the cognitive network that does not require any time synchronization with the other links in the network. Each such channel operates using the principles of direct sequence spread spectrum (DSSS) and is assigned a unique pseudo-noise (PN) sequence that is orthogonal to the other links' PN sequence. To address the dual-intent of the

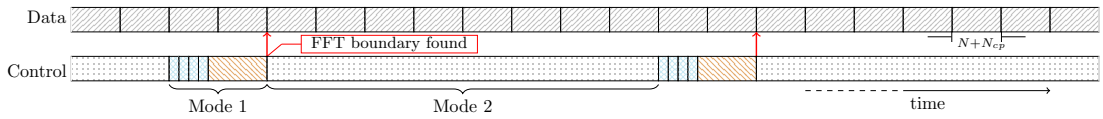


Figure 5.2: Sequence of transmissions over the NC-OFDM-based data channel and the underlay control channel. Underlay control channel is used for timing and frequency offset recovery.

proposed UCC, the channel operates in one of two modes. The first mode is designed to aid timing and frequency offset recovery for NC-OFDM and the second mode is used to transmit control data. In the first mode, a two-stage mechanism for timing and frequency offset recovery is proposed. The second mode uses straightforward spread spectrum techniques to transmit the control data. The underlay channel is always transmitted at noise floor so as to have minimal impact on the primary transmissions.

The proposed UCC is implemented on USRP N210 radios [54] with the GNU-Radio software platform [71] on the ORBIT testbed [83]. Experimental results are then used to explore the impact of the strength of the overlay transmissions and the choice of the various design parameters on the performance of the UCC. We study the performance of the proposed UCC in terms of the accuracy of timing and frequency offset estimation and the achievable data rate by varying the design parameters. In particular, experimental results indicate that the proposed design is capable of reliable timing and frequency offset recovery even in the presence of concurrent primary transmissions and supports about 10 to 20 kbps over a 1 MHz bandwidth at an uncoded symbol-error-rate of about 10^{-2} under typical operating conditions.

5.2 System Model

Consider a network of K p2p cognitive links operating over a total bandwidth of B, as shown in Fig. 5.1. Primary transmitters operate in certain parts of this bandwidth, thus fragmenting the available bandwidth into multiple noncontiguous segments. The primary transmissions are collectively denoted as $p(t)$. Each of the K p2p links is assumed to use NC-OFDM to access this fragmented spectrum and uses a total of N subcarriers. NC-OFDM restricts transmission to only a subset of these N subcarriers

by first sensing the spectrum for incumbent transmissions and barring transmission over frequencies that are in use. Computing an optimal assignment of the available spectrum among the K links is a challenging problem [25, 110] and falls outside the scope of this work. We assume that a set of subcarriers $\mathcal{N}_i$ for $i = 1, 2, \ldots, K$ is assigned to each of the K links. As the bandwidth occupied by the incumbent transmissions changes, the spectrum assignment is recomputed and shared among the K links. The NC-OFDM signal transmitted by the kth transmitter is denoted as $s_k(t)$.

In addition to using NC-OFDM for data transfer, each of the K links is also supported by a p2p UCC, denoted as $c_k(t)$. This UCC is used to transmit the communication parameters, subcarrier assignment, and other control data to the receiver. Since the control channel plays a key role in enabling the use of NC-OFDM, it is important that this channel be easy to establish, while being robust to changes in the primary/secondary transmissions. A low-power UCC that spans the entire bandwidth, that is agnostic to spectrum assignment and has a minimal impact on primary transmissions is ideally suited for this purpose.

In such a setting, the received signal at the ith receiver of the cognitive network, without considering receiver impairments, is given by

$$r_i(t) = \underbrace{\sum_{k=1}^{K} h_k(t) * s_k(t)}_{K \text{ NC-OFDM signals}} + \underbrace{\sum_{k=1}^{K} h_k(t) * c_k(t)}_{K \text{ control signals}} + \underbrace{h_p(t) * p(t)}_{\text{primary signal}} + \underbrace{n(t)}_{\text{additive noise}}, \tag{5.1}$$

where the various components of the received signal are labeled and $h_i(t)$ denotes the time domain channel impulse response. Note that the K NC-OFDM signals and the primary transmissions use orthogonal subcarriers and therefore do not interfere with each other.

5.2.1 NC-OFDM Signal Representation

The baseband representation of the NC-OFDM signal at the kth transmitter can be written as

$$s_k(t) = \sum_{l=0}^{\infty} \sum_{n \in \mathcal{N}_i} d_{kln}\ e^{j2\pi f_n (t - lT)} \text{rect}\Big(\tfrac{t - lT}{T}\Big), \tag{5.2}$$

where d_{kln} is the data symbol to be transmitted, f_n is the center frequency of the nth subcarrier, and rect$(\cdot)$ represents the rectangular function that is 1 in the unit interval and 0 elsewhere. T denotes the overall duration of one NC-OFDM signal, including the cyclic prefix. We assume that a cyclic prefix of length N_{cp} is used at each link. At the receiver, assuming a constant flat fading channel, after downconversion and accounting for frequency offset, the kth NC-OFDM signal can be represented as $h_k e^{j2\pi(\delta f_k)t} s_k(t)$, where h_k is the channel fading coefficient and δf_k is the frequency offset. When this signal is sampled at a rate of $1/T_s$, it can be written as

$$r_{i(s_k)}[m] = h_k e^{j2\pi(\delta f_k)(mT_s+\phi_k)} s_k(mT_s + \phi_k) \tag{5.3}$$

where $r_{i(s_k)}[m]$ denotes the contribution of $s_k(t)$ to the mth sample of $r_i(t)$, ϕ_k $(< T_s)$ is the phase offset and (δf_k) is the frequency offset. Note that the K NC-OFDM signals are not assumed to be synchronized. Similar to OFDM we assume that the sampling rate $T_s = T/(N + N_{cp}) = 1/B$.

The ith receiver decodes the NC-OFDM signal $s_i(t)$ from discrete time samples of the received signal $r_i(t)$. Two critical aspects of decoding an NC-OFDM signal are timing and frequency offset recovery. Timing recovery requires identifying the start of the NC-OFDM frames, which in the above representation occurs at every $(l(N + N_{cp}) + 1)$th sample. Frequency offset correction is also important to the reliable recovery of the NC-OFDM signals as it otherwise results in inter-carrier interference (ICI). Note that correcting the phase offset ϕ_i can be done at the detection stage using the aid of pilot symbols. While traditional OFDM-based systems use preambles that result in a time domain waveform with repeated patterns to aid timing and frequency recovery, the dynamic nature of spectrum allocation along with the presence of multiple concurrent transmissions make it difficult to directly apply these techniques to NC-OFDM-based systems. With these challenges in mind, we propose to use the UCC in a novel way to aid the timing and frequency offset recovery of the desired NC-OFDM signal. Details of the proposed mechanism are discussed in Section 5.3.

5.2.2 Control Signal Representation

The low-power UCC is operated in one of two modes, as shown in Fig. 5.2. In mode 1, the channel is used to aid timing and frequency offset recovery and in mode 2, it is used to transmit control data. In mode 2, the control channel for each of K links operates as a conventional DS-CDMA channel where the message bits are first spread using a pre-assigned PN sequence $p_{kd}[m]$, of length l_d, and then transmitted over the air. The PN sequences for the K links are chosen to be orthogonal to each other so as to minimize multiple-access interference. The control signal can be represented as

$$c_k(t) = \sum_{l} \sum_{m=1}^{l_d} g_{kl} p_{kd}[m] \text{rect}\Big(\tfrac{t - l l_d T_c - (m-1)T_c}{T_c}\Big) \tag{5.4}$$

where T_c is the chip rate and g_{kl} is the control data to be transmitted. Since we assume that the UCC occupies the full bandwidth, we set $T_c = 1/B$, i.e., the sampling rate for the NC-OFDM signal and the control channel are the same. The UCC is always transmitted at a power equal to the noise floor in order to have minimal impact on the NC-OFDM signal. The receiver uses a single correlator and a demodulator to recover the transmitted control signals.

5.3 Control Channel Design for Timing and Frequency Offset Recovery

This section is focused on mode 1 of the control channel design. We propose a two-stage mechanism for timing and frequency offset recovery, as depicted in Fig. 5.2. In the first stage the ith transmitter transmits a short PN sequence $p_{is}[m]$ of length l_s repeatedly for R times. This is then followed by the transmission of a long PN sequence $p_{il}[m]$ of length l_l. The primary purpose of the first stage is to allow the receiver to compute an estimate of the frequency offset, while the second stage is used to identify the timing instance. At the ith receiver, suppose $r_i[m]$ denotes the samples of the received signal, the control channel component of interest in this sample during the first stage of mode

1, is given by

$$r_{i(c_i)}[m] = h_i p_{is}[1 + \text{mod}(m-1, l_s)] e^{j2\pi(\delta f_i)(mT_s+\phi_i)} \tag{5.5}$$

where we have assumed a flat fading channel. The receiver uses a correlator matched to $p_{is}[m]$ to serially scan the received signal to identify the transmission of the short PN sequence. The output of such a correlator is given by

$$w_{is}[m] = \sum_{n=1}^{l_s} r_i[m+n-l_s] p_{is}[n] \tag{5.6}$$

A short PN sequence is said to have been detected if $|w_{is}[m]|$ exceeds a certain threshold τ_s. Suppose in an ideal scenario, R such correlation peaks are detected, these R peaks can be used to compute a coarse estimate of the frequency offset. Let the indices corresponding to these R peaks be given by m, $m + l_s$, ..., $m + (R-1)l_s$. In a noiseless, interference less scenario and without any overlay NC-OFDM signals, two consecutive peaks differ only in phase by a value of

$$\Delta\psi = 2\pi(\delta f_i)((m+l_s)T_s + \phi_i) - 2\pi(\delta f_i)(mT_s - \phi_i) \tag{5.7}$$

$$= 2\pi l_s(\delta f_i)T_s, \tag{5.8}$$

This observation leads us to estimate the frequency offset as

$$\hat{(\delta f_i)} = \frac{\sum_{n=1}^{R-1} \angle w_{is}[m+nl_l] - \angle w_{is}[m+(n-1)l_l]}{2\pi l_s T_s (R-1)} \tag{5.9}$$

However, it is pertinent to address two key issues that emerge with regard to correlation peak detection. First, it is important that the length of the PN sequence l_s be small enough that $(\delta f_i) l_s T_s << 1$. When this condition is violated, the duration of the transmission of the PN sequence is such that its phase can undergo a rotation of more than 2π radians because of the frequency offset. This proves detrimental to the detection of the correlation peaks and also affects the accuracy of the offset estimate. However, this brings up the second issue of being able to detect all R correlation peaks. Given the challenging environment under which this UCC is required to operate and the necessity to limit the length l_s, we consider detecting only a fraction α of the peaks. This entails detecting αR peaks within a window of $l_s R$ samples, which then triggers the receiver to estimate the frequency offset and move to the next stage of timing recovery.

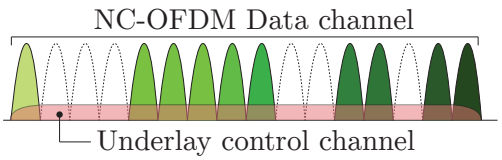


Figure 5.3: A low powered control channel spanning complete bandwidth.

In the second stage, the receiver first uses the frequency offset estimate to correct the offset in the received signal, then puts this signal through a correlator matched to the long PN sequence $p_{il}[m]$. The output of this correlator is given by

$$w_{il}[m] = \sum_{n=1}^{l_l} e^{-j2\pi(\delta\hat{f}_i)(m+n-l_l)T_s} r_i[m+n-l_l] p_{il}[n] \tag{5.10}$$

A threshold τ_l is used to declare a correlation peak. When a peak is detected, it indicates the start of an NC-OFDM symbol. The use of a long PN sequence in the second stage ensures that even under challenging operating conditions, timing instances are reliably recovered and false peaks are minimized. Note that using the frequency offset estimate is crucial to enable the reliable detection of long PN sequences in the second stage.

5.3.1 Choice of Thresholds τ_l and τ_s

Under time varying conditions, the thresholds τ_l and τ_s cannot be held at fixed values and must instead be adaptive. To dynamically alter the threshold τ_l, we propose a first-order auto-regressive update procedure of the form

$$\tau_{l,new} = \beta\tau_{l,\text{current}} + \gamma\nu, \tag{5.11}$$

that updates the value of τ_l once every P samples (PT_s seconds), with the value of ν being either the latest long correlation peak detected in the previous PT_s seconds, or a preset value τ_o, in case no peaks were detected. The design parameters $0 \leq \beta \leq 1$, $0 \leq \gamma \leq 1$, and the integer P determine the rate at which the threshold adapts to current network conditions. In all our experiments we set $\beta = 0.7$ and $\gamma = 0.2$. A similar procedure can also be adopted for τ_s.

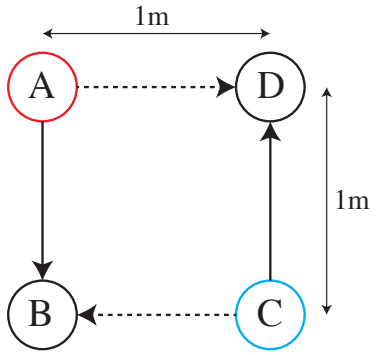


Figure 5.4: Topologies used in experiments.

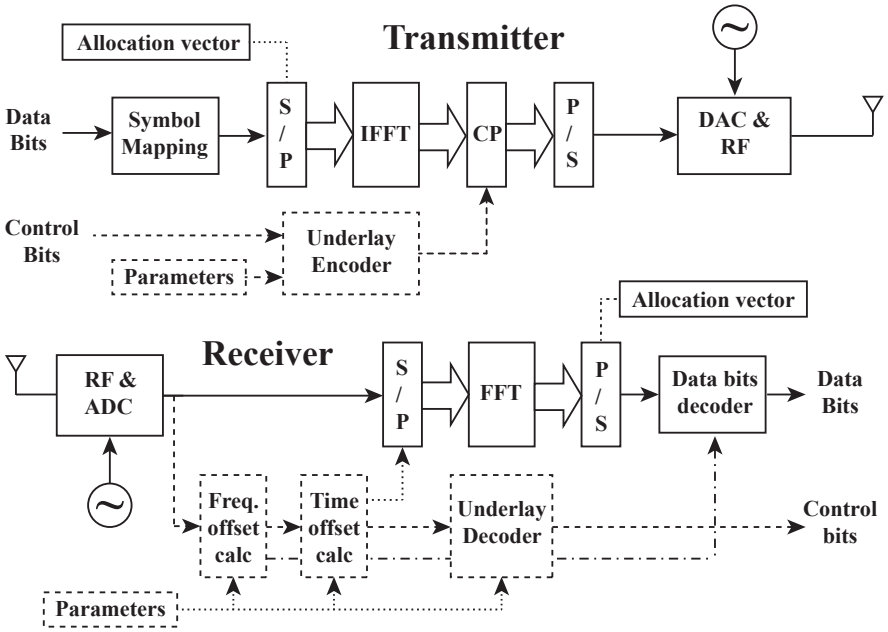


Figure 5.5: Implementation of the transmitter and the receiver on USRP N210 radio nodes using GNU Radio.

5.4 Experimental Setup

5.4.1 Topology

To test the performance of the proposed UCC, we perform a set of experiments on two particular network topologies, as shown in Fig. 5.4. In the single-link topology, the transmitter uses all available subcarriers to communicate with the receiver. In the two-link topology, the two links use two disjoint sets of subcarriers for communication. The UCC spans the whole bandwidth in both the cases. In the two-link topology, the control channels for the two links use orthogonal PN-sequences in both the modes. Note that

from the UCC standpoint, the single-link topology is a more challenging environment to operate in than the two-link topology as the overlay interference in the two-link case gets split between two sources, with one being further away. Hence, we use results from the single-link topology as the basis for the choice of parameters for the UCC.

5.4.2 Platform and Implementation

In our experiments the transmitter and receiver nodes shown in Fig. 5.4 are USRP N210 radio nodes [54], that are part of the larger ORBIT testbed [83]. The USRP N210 radios used in the experiment use the SBX transceiver daughter-card that can operate anywhere from 400 MHz to 4.4 GHz, provide a maximum bandwidth of 40 MHz and transmit up to 100 mW of power. GNU Radio is a free and open-source SDR framework that provides the application programming interface (API) for several hardware platforms, including many USRP devices [71]. The NC-OFDM data paths and the corresponding UCC paths are implemented in C++ and Python in GNU Radio. Fig. 5.5 shows the block diagram of the transmitter and receiver in our experimental setup. All the necessary parameters for the configuration are provided to the transmitter and receiver by an outside controller. The transmit chain has a control path that runs parallel to the data path, however, since the control also aids timing recovery, the two paths are merged at the block where cyclic prefix is added to the NC-OFDM signal.

At the receiver, the incoming stream of symbols is used as input to two parallel chains. The first chain is used for timing recovery, frequency offset estimation, and decoding of control data as described in Section 5.2.2, while the second chain is used to decode the NC-OFDM signal. We use the adaptive thresholding procedure outlined in Section 5.3.1 to set the threshold for the long correlation while using a small, fixed threshold to identify short correlation peaks.

5.4.3 Transmission Parameters

In all the experiments the UCC's power is set to be at noise floor i.e., underlay-to-noise-ratio (UCNR) = 0 dB, while the transmit overlay-signal-to-noise ratio (OSNR) is varied from 4 to 10 dB. Experiments are conducted to study (a) the accuracy of the timing

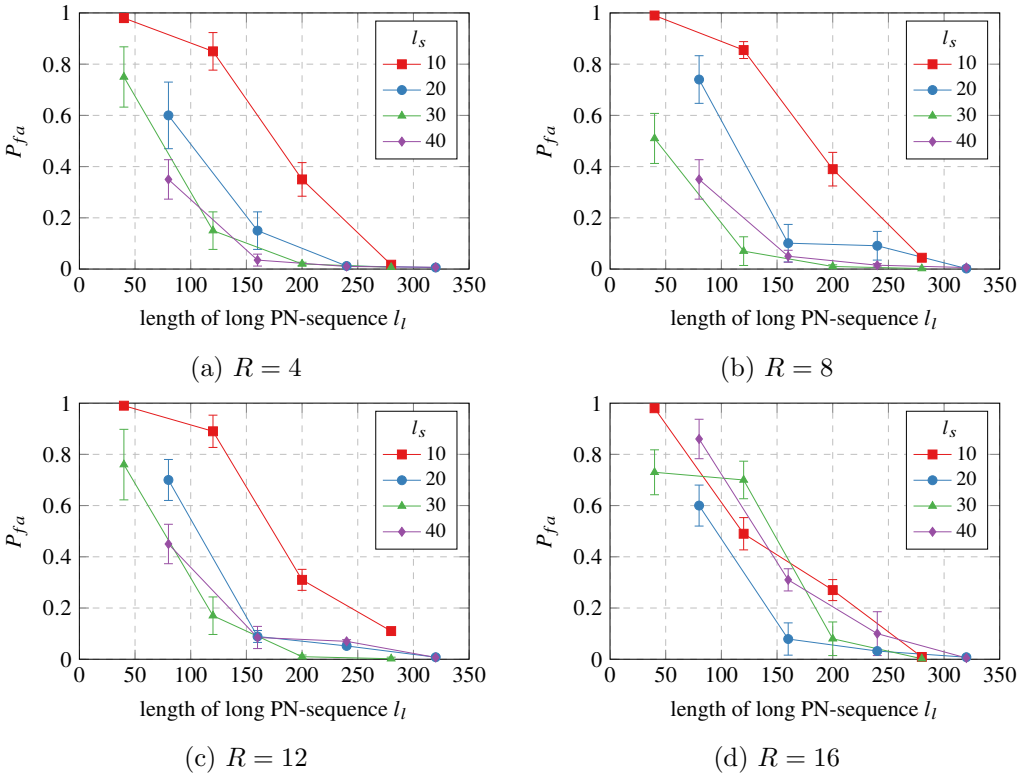
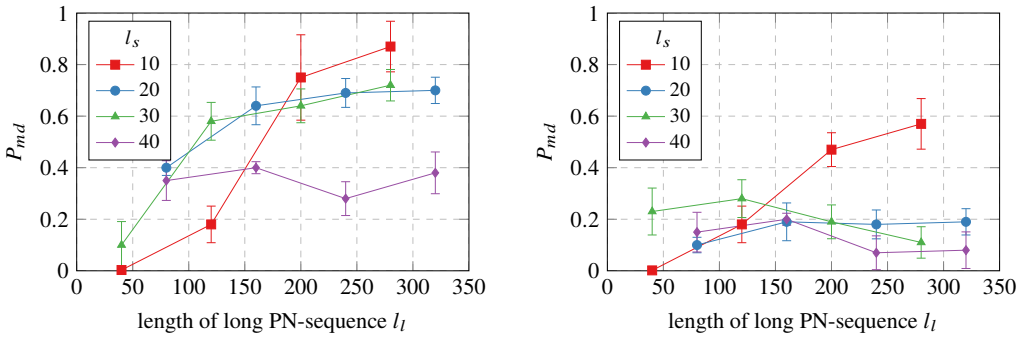


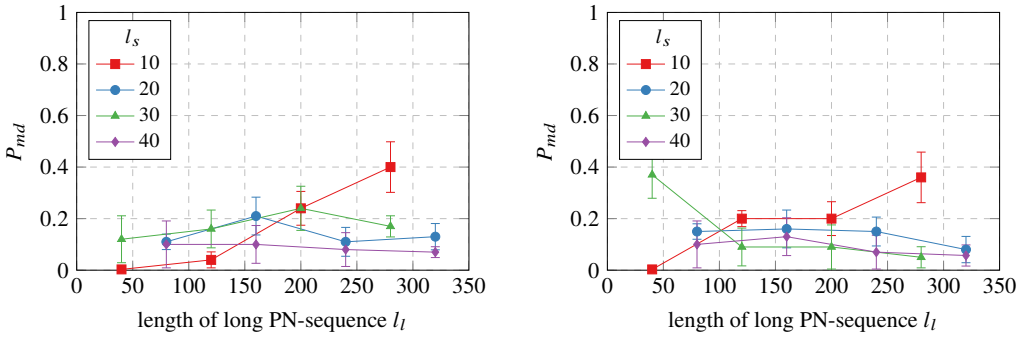
Figure 5.6: Probability of false alarm P_{fa} for various combinations of the parameters l_s, l_l and R.

offset estimation and (b) the symbol error rate (SER) of the UCC as a function of the strength of the overlay NC-OFDM signal. The various design parameters involved in the UCC are designed assuming a transmit OSNR of 10 dB.

In all experiments, we use a 1 MHz bandwidth and divide this bandwidth between $N = 64$ subcarriers. We set the cyclic prefix length to be $N_{cp} = 16$, resulting in a total NC-OFDM symbol length of $N + N_{cp} = 80$. For the two-link topology, subcarriers 1–15 and 34–48 are assigned to link 1, subcarriers 17–31 and 50–64 are assigned to link 2 and subcarriers 16, 32, 33 and 49 are used as guard bands. The NC-OFDM subcarriers are modulated using the QPSK constellation and the control data using BPSK. Timing and frequency offset recovery are only performed periodically, after the transmission of multiple NC-OFDM symbols, we thus ensure that $l_l + Rl_s + Vl_d$ is an integer multiple of 80, where V is the number of control data symbols transmitted in mode 2. To analyze the performance of the timing and frequency offset estimation we vary the values of l_s, l_l and R, while keeping all other parameters constant. Similarly, to calculate the bit



(a) $R = 4$ (b) $R = 8$



(c) $R = 12$ (d) $R = 16$

Figure 5.7: Probability of missed detection P_{md} for various combinations of the parameters l_s, l_l and R.

error rate for UCC we vary the value of l_d and transmit OSNR while keeping UCNR at 0 dB and all other parameters constant.

5.5 Results and discussion

The first set of experiments aims to study the impact of the parameters l_s, l_l and R on the accuracy of timing and frequency offset recovery. We use the single-link topology for this purpose. Fig. 5.6 and Fig. 5.7 show the results of such an experiment where the performance of UCC is measured in terms of the probability of missing a timing instant and the probability of reporting a false timing instant. Figs. 5.6a to 5.6d show the probability of false alarm P_{fa}, while Figs. 5.7a to 5.7d show the probability of missed detection P_{md} for different values of l_s, l_l and R. In all these figures, l_s is chosen from the set $\{10, 20, 30, 40\}$ while the value of l_l is varied between 40 to 320. Focusing on Fig. 5.6a and Fig. 5.7a, we see that although P_{fa} decreases with increasing

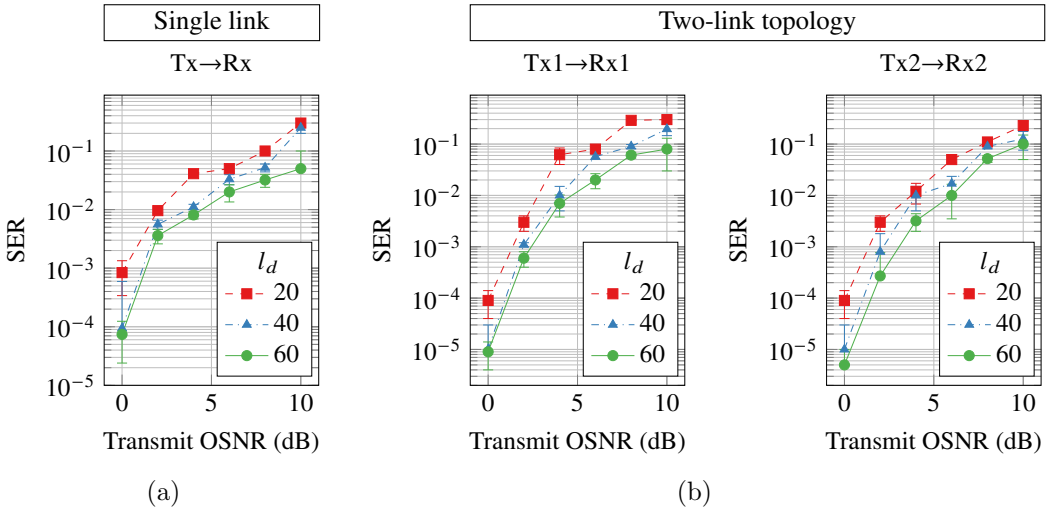


Figure 5.8: SER of UCC as the transmit OSNR is varied. Errors due to false alarms in timing recovery are also counted.

l_l, setting $R = 4$ is insufficient to bring P_{md} to within a reasonable range. A large P_{md} for large values of l_l suggests that a reliable estimate of the frequency offset is difficult to obtain for small values of R. In general it can be noticed that $R \geq 8$ is required to keep both P_{fa} and P_{md} to within acceptable levels. Note also that in Figs. 5.6a-5.6d, P_{fa} appears to increase with R. Although this appears counterintuitive, this can be explained by noting that for small values of R, P_{md} is so high that very few peaks are detected, leading to a low value for P_{fa}. For $R \geq 8$, it is seen that as the value of l_l increases both P_{fa} and P_{md} decrease. Based on these observations, it appears that setting $l_s = 40$, $l_l = 320$ and $R = 8$ provides a good trade-off between reliable timing and frequency offset recovery and transmit overhead incurred in operating the UCC in mode 1 instead of mode 2. We henceforth use these parameter settings for the remaining experiments.

The next set of experiments is performed to measure the SER of the UCC in the presence of overlay NC-OFDM signal. Towards this end, we hold UCNR at 0 dB and vary the transmit OSNR between 0 to 10 dB. All parameters are held constant except for the spreading code length l_d which is chosen from the set $\{20, 40, 60\}$. We conduct these experiments for both single link and two-link topology of Fig. 5.4. Figs. 5.8a and 5.8b show the results from these experiments where Fig. 5.8a shows the SER for the

single link topology and Fig. 5.8b shows the SER over the two links in the two-link topology. We see that overall SER performance is comparable for both topologies. For lower values of transmit OSNR, the two-link topology actually performs better as the received OSNR is slightly lesser in the two-link case due to the difference in the distances to the two transmitters. It is seen that it is possible to achieve an uncoded SER of 10^{-2} even when the transmit OSNR is up to 6-8 dB with $l_d = 60$. Note that these error rates include errors due to false alarms in the timing recovery stage. SER can be further reduced by using a phase-locked loop to improve the accuracy of the timing recovery mechanism. Under the current parameter settings, this translates to a symbol rate of 11 kbps over a 1 MHz channel, assuming the duration of mode 2 is twice the duration of mode 1.

5.6 Chapter Summary

In this chapter, we considered the design of an underlay control channel for a cognitive network consisting of multiple NC-OFDM-based p2p links that operate over a wide bandwidth consisting of multiple disjoint bands. In addition to sharing control data, the proposed underlay control channel based on DSSS transmission is also used for timing and frequency recovery of NC-OFDM transmissions. The control channel operates in one of two modes. The first mode aids timing and frequency recovery through a two-step process, while the second mode is used for control data transmission. Such a control channel was implemented on USRPs in the ORBIT testbed using GNU Radio. Experimental results reveal that such a channel can be relied upon for robust timing and frequency offset recovery while supporting 10 to 20 kbps over a 1 MHz bandwidth at an uncoded symbol-error-rate of about 10^{-2} under typical operating conditions.

Chapter 6

Physical Layer Security Features of NC-OFDM Transmission

6.1 NC-OFDM transmission in presense of evasdropper

Security is an important consideration for wireless communication systems operating in tactical environments [111]. Due to the broadcast nature of the wireless medium, there are multiple facets to securing a communication system, such as resilience to jamming attacks [112], early detection of injection attacks [113], protection of sensitive information from eavesdroppers [114], etc. Focusing on eavesdroppers, strategies at various layers of the communication protocol have been proposed to make it more difficult for the eavesdropper to discern the information being transmitted. While techniques such as encryption, secure routing [115], and frequency hopping [116] are well known, techniques that prevent the eavesdropper from even synchronizing to the transmitted signal offer another line of defense and form the primary focus of this chapter.

6.1.1 Measuring security

Generally, the physical layer security of a transmission is measured using following three parameters.

- Probability of detection $P(D)$: Probability of identifying the presence of the signal by the eavesdropper, commonly using some form of energy or feature detection.
- Probability of interception $P(I) = P(I|D)P(D)$: Probability of detecting and tracking the signal.

- Probability of exploitation $P(E) = P(E|I)P(I|D)P(D)$: Probability of extracting the necessary features from the signal in order to be able to decode it.

Being a multicarrier signal, the NC-OFDM transmission also suffers from the issue of PAPR. Hence, the transmission power requirements for a reasonable BER performance make it very difficult to reduce $P(D)$. In other words, for normal operating conditions the NC-OFDM signal will be detected. Similarly, by observing the spectrum it is possible to determine the range of operating frequency. In this chapter, we specifically focus on features of NC-OFDM transmission which can potentially reduce the value of $P(E)$. Necessary parameters for an eavesdropper to decode an NC-OFDM signal are 1) total bandwidth to determine minimum sampling rate, 2) the total number of subcarriers to determine the size of FFT block to be used, and 3) the set of subcarriers used in the transmission. An LPE-centric design aims to prevent an eavesdropper from recovering the transmitted symbols and is vital in ensuring secure transmission of sensitive information.

6.1.2 LPE-centric design

In particular, we consider a point-to-point communication link designed to use non-contiguous orthogonal frequency division multiplexing (NC-OFDM), and examine its strengths and weaknesses from an eavesdropper's standpoint and presents suggestions for a low-probability-of-exploitation (LPE)-centric design of NC-OFDM-based systems. Two key steps for an eavesdropper to be successful are synchronization and detection. Synchronization requires timing and frequency recovery along with signal parameters such as sampling rate(subcarrier spacing), total bandwidth, list of subcarriers being used, etc. This is followed by detection which requires knowledge of modulation and coding being used. LPE-centric design and analysis of OFDM-based systems [117–121] is well studied and many techniques for waveform feature suppression have been proposed to mask the transmission parameters.

Although NC-OFDM waveform is similar to OFDM waveform, there are several differences that warrant further investigation from an LPE standpoint. The most significant difference emerges from the fact that the total nominal bandwidth (bandwidth

of both active and inactive subcarriers) of an NC-OFDM transmission is not straightforward to infer, thus affecting the ability to sample the received signal at the correct rate. Despite this difficulty, an eavesdropper can use techniques such as cyclostationary analysis [122,123] to infer basic transmission parameters. In this chapter, we focus on a cyclostationary analysis of an NC-OFDM signal and examine how such an analysis can be used by an eavesdropper to infer the transmit parameters. We show that the choice of the active set of subcarriers plays a crucial role in determining the effectiveness of such an analysis.

In addition to such an analysis, we also propose a novel offline timing recovery scheme that can be used by an eavesdropper to identify the start of an NC-OFDM symbol. The proposed approach does not require the knowledge of correct sampling rate, or accurate frequency synchronization. The scheme only requires knowledge of the total duration of an NC-OFDM symbol and is based on principle component analysis (PCA). This method is used as a guidepost to determine the minimum rate at which the active subcarrier set must be refreshed to prevent the eavesdropper from being successful.

The chapter concludes by summarizing the key differences between NC-OFDM and OFDM transmissions from an LPE standpoint and highlights the advantages of using NC-OFDM.

6.2 Signal Model

Consider a point-to-point wireless link operating over a total bandwidth of B and using NC-OFDM. Assuming a total of N subcarriers, NC-OFDM restricts transmission to only a subset of these N subcarriers either to avoid incumbent users or for strategic purposes. Let the subset of active subcarriers be denoted by $\mathcal{S}$. Let the width of each subcarrier be denoted by δf and let the center frequency for each subcarrier be denoted by $f_n = f_o + n(\delta f)$. The transmitted signal can then be written as

$$s(t) = \sum_{m=-\infty}^{m=+\infty} \sum_{n \in \mathcal{S}} s_{m,n} e^{j2\pi f_n (t - mT_o)} g(t - mT_o), \tag{6.1}$$

where $s_{m,n}$ represents the symbol transmitted on the nth subcarrier at the mth time slot, T_o is the total duration of one NC-OFDM symbol and $g(\cdot)$ is a rectangular pulse of width T_o, centered at $T_o/2$. Letting T_u and T_{cp} denote the useful symbol duration and the duration of the cyclic prefix, we note that $T_o = T_u + T_{cp}$. All through this chapter we assume that $T_{cp} \leq T_u$. Further, due to orthogonality of subcarriers, we have $T_u = \frac{1}{\delta f}$. Although not considered here, NC-OFDM also supports concurrent point-to-point transmissions by orthogonally dividing the available subcarriers.

In such a setting, the received signal at an eavesdropper is given by

$$\tilde{r}(t) = \underbrace{h(t) * s(t)}_{\text{NC-OFDM signal}} + \underbrace{h_p(t) * p(t)}_{\text{incumbent signal}} + \underbrace{n(t)}_{\text{additive noise}}, \tag{6.2}$$

where the various components of the received signal are as labeled and $h(t)$ denotes the time domain channel impulse response. The incumbent primary transmission is denoted as $p(t)$ with $h_p(t)$ denoting the channel impulse response from the primary transmitter. The NC-OFDM signal and the primary transmissions use non-overlapping frequencies and it is assumed that the eavesdropper can effectively filter out the incumbent transmissions to obtain

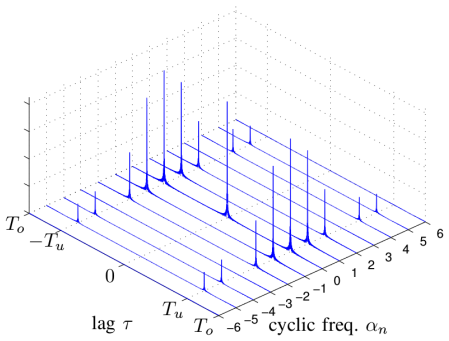
$$r(t) = h(t) * s(t) + n(t). \tag{6.3}$$

The rest of the chapter assumes the incumbent transmission to be filtered out, focuses on the transmitted signal $s(t)$ and examines its features through cyclostationary analysis. Further, since an eavesdropper can potentially be in line of sight of the transmitter, the analysis is presented for an additive white Gaussian noise (AWGN) channel, i.e., $h(t)$ is set to $\delta(t)$. The eavesdropper observes the transmitted NC-OFDM signal over a large window during which the NC-OFDM transmission parameters are assumed to remain constant.

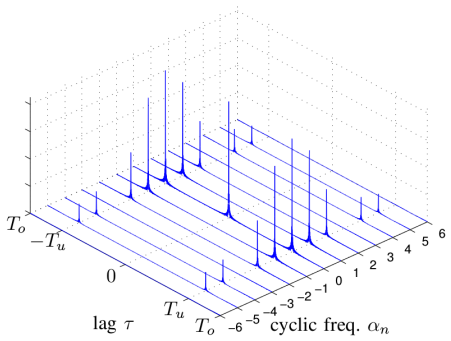
6.3 Cyclostationary Analysis of an NC-OFDM Signal

The autocorrelation $R(t, \tau)$ of the transmitted signal $s(t)$ can be written as

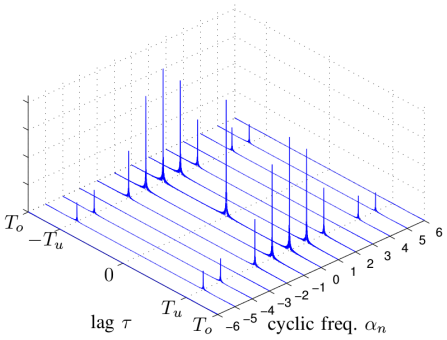
$$R(t, \tau) = E[s(t)s^*(t - \tau)]$$



(a) Contiguous alloc.



(b) Interleaved alloc.



(c) Interleaved alloc.

Figure 6.1: Cyclic autocorrelation function for different types of subcarrier allocation.

$$= \sigma_s^2 \left(\sum_{n \in \mathcal{S}} e^{j2\pi f_n \tau} \right) \sum_m g(t - mT_o) g^*(t - mT_o - \tau)$$
$$= \sigma_s^2 \psi_{\mathcal{S}}(\tau) \sum_m g(t - mT_o) g^*(t - mT_o - \tau), \tag{6.4}$$

where $\sigma_s^2 = E[|s_{m,n}|^2]$ and $\psi_{\mathcal{S}}(\tau) = \sum_{n \in \mathcal{S}} e^{j2\pi f_n \tau}$.

Note that $R(t, \tau)$ is zero whenever $|\tau| > T_o$. Further note that $R(t, \tau)$ is periodic in t with period T_o. This periodicity allows representing the autocorrelation function as a Fourier series sum:

$$R(t, \tau) = \sum_n R(\alpha_n, \tau) e^{j2\pi \alpha_n t}, \tag{6.5}$$

where α_n is the cyclic frequency and is equal to n/T_o, and $R(\alpha_n, \tau)$ is known as the cyclic autocorrelation function (CAF). $R(\alpha_n, \tau)$ is computed as follows

$$R(\alpha_n, \tau) = \frac{1}{T_o} \int_0^{T_o} R(t, \tau) e^{-j2\pi \alpha_n t} dt$$
$$= \frac{\sigma_s^2 \psi_{\mathcal{S}}(\tau)}{T_o} \int_0^{T_o} \left(\sum_m g(t - mT_o) g^*(t - mT_o - \tau) \right) e^{-j2\pi \alpha_n t} dt$$

$$= \frac{\sigma_s^2 \psi_{\mathcal{S}}(\tau)}{T_o} \sum_m \int_{-mT_o}^{-(m-1)T_o} \left(g(t') g^*(t'-\tau) \right) e^{-j2\pi\alpha_n t'} dt'$$
$$= \frac{\sigma_s^2 \psi_{\mathcal{S}}(\tau)}{T_o} \int_{-\infty}^{\infty} \left(g(t') g^*(t'-\tau) \right) e^{-j2\pi\alpha_n t'} dt'. \tag{6.6}$$

It is easy to see that the CAF is non-zero only when $|\tau| \leq T_o$. When $|\tau| \leq T_o$, using the Fourier transform of the rectangular function, this can be further simplified to

$$R(\alpha_n, \tau) = \tfrac{\sigma_s^2 \psi_{\mathcal{S}}(\tau)}{T_o} sinc(\pi\alpha_n(T_o - |\tau|)) e^{-j\pi\alpha_n(T_o+\tau)}. \tag{6.7}$$

It can be seen that there are two components that influence the magnitude of the CAF. The first component, $\psi_{\mathcal{S}}(\tau)$, is only dependent on the lag τ and the active subcarrier set $\mathcal{S}$, while the second component is a sinc function $(\sin(x)/x)$ whose argument includes the cyclic frequencies α_n and the lag $|\tau|$.

Focusing on the $\psi_{\mathcal{S}}(\tau)$, note that

$$|\psi_{\mathcal{S}}(\tau)| = \left| \sum_{n \in \mathcal{S}} e^{j2\pi f_n \tau} \right| \leq \sum_{n \in \mathcal{S}} |e^{j2\pi(f_o + n(\delta f))\tau}| \leq |\mathcal{S}| \tag{6.8}$$

and that irrespective of the choice of $\mathcal{S}$, $|\psi_{\mathcal{S}}(\tau)|$ attains this maximum when $\tau = \pm T_u$ or $\tau = 0$. Additionally, the following observations can be made for specific sets of active subcarriers:

(a) *Contiguous allocation*: When a set of K contiguous subcarriers are used, we have

$$|\psi_{\mathcal{S}}(\tau)| = \frac{|\sin(jK\pi(\delta f)\tau)|}{|\sin(j\pi(\delta f)\tau)|}, \tag{6.9}$$

which attains its maximum value of K whenever $\tau = pT_u$ for some integer p. Since $|\tau| \leq T_o$ and $T_{cp} < T_u$, there are exactly three values of τ where $|\psi_{\mathcal{S}}(\tau)|$ attains its maximum. This is indeed the case with OFDM where all the subcarriers are used and the peaks are observed at $\tau = \pm T_u$ and $\tau = 0$ [117–121].

(b) *Interleaved allocation*: When a set of K interleaved subcarriers, spaced q subcarriers apart are used, we then have

$$|\psi_{\mathcal{S}}(\tau)| = \frac{|\sin(jKq\pi(\delta f)\tau)|}{|\sin(jq\pi(\delta f)\tau)|}, \tag{6.10}$$

which attains its maximum value of K whenever $\tau = pT_u/q$ for some integer p. For $|\tau| \leq T_o$, there are at least $2q+1$ values where this maximum is attained.

(c) *Random allocation*: When subcarriers are chosen at random, $\psi_{\mathcal{S}}(\tau)$ cannot be simplified any further, and except for the maxima that are certain to occur at $\tau = \pm T_u$ and $\tau = 0$, other values where a maximum occurs requires specifying the exact subcarriers being used.

The second component of the CAF is a sinc function involving both τ and α_n. For a fixed α_n, this function is centered at T_o, with a main lobe width of $2T_o/n$ and zeros at $\tau = kT_o/n$ where $k \in \mathbb{Z}$ and $1 \leq |k| \leq |n|$. This suggests that the features of the CAF are most prominent for small values of n (large main lobe width), and taper off rapidly as n increases. Similarly, for a fixed τ, this sinc function is centered at $\alpha_n = 0$, has a main lobe width of $2/(T_o - |\tau|)$ and zeros at $k/(T_o - |\tau|)$, where $k \in \mathbb{Z}$ and $k \neq 0$. This suggests that for a fixed τ, features of the CAF are most prominent close to $|T_o|$ and in fact vanish at $\tau = 0$ for all non-zero n.

The combined effect of these two components is illustrated in Fig. 6.1, where the magnitude of the CAF is plotted for the three different subcarrier allocations considered earlier. From Fig. 6.1a it is seen that CAF in the case of contiguous allocation mirrors the existing observations on the CAF for OFDM with distinct peaks at $(\alpha_n, \pm T_u)$ that decay with increasing n. However, clear differences in the CAF can be observed in Fig. 6.1c when subcarriers are allocated in an interleaved manner. In this case, since alternate subcarriers are used, in addition to the peaks at $\tau = \pm T_u$, peaks are also noticed at $\tau = \pm T_u/2$ and $\tau = \pm 3T_u/2$. Notice that the peaks at $\tau = \pm 3T_u/2$ are more prominent than the other peaks. This is due to the sinc component having a much broader main lobe at $\tau = \pm 3T_u/2$ than at $\tau = T_u/2$ and hence having a lesser impact on the peaks of $|\psi_{\mathcal{S}}(\tau)|$ (main lobe grows larger as τ gets closer to T_o). Finally, when subcarriers are randomly assigned, it is seen that the CAF does not immediately decay as τ moves away from T_u and consequently the peaks at $(\alpha_n, \pm T_u)$ do not stand out distinctly.

The next section investigates how an eavesdropper can learn about the transmission parameters of an NC-OFDM system via a cyclostationary analysis when no strategies to suppress these features are adopted.

6.4 Learning NC-OFDM Transmission Parameters

For an eavesdropper to successfully detect and decode an OFDM/NC-OFDM transmission, the eavesdropper must follow the following steps: (a) identify overall bandwidth B; (b) filter signal of interest by passing through a bandpass filter and down convert to baseband; (c) sample the baseband signal above Nyquist rate; (d) establish timing(start and end of OFDM symbol) and frequency synchronization (e) detect and decode symbols.

The very first step in this process highlights a major difference between NC-OFDM and OFDM. In an OFDM transmission, since all the subcarriers are used, the bandwidth B can be inferred, to within a reasonable accuracy, via a periodogram. However, in the case of NC-OFDM, the actual bandwidth of use (say B_a) that spans all the active subcarriers is not related to the overall bandwidth B except that $B_a \leq B$. While it may be possible to get an estimate of B_a via a periodogram, since B requires knowledge of both active and inactive subcarriers, B is difficult in infer. To further illustrate this, consider the periodogram in Fig. 6.2. While, it can inferred that the underlying transmission occupies a bandwidth of 0.5 MHz, the actual transmission parameters correspond to an NC-OFDM signal with a total of 256 (N) subcarriers spanning 1 MHz (B), of which only 85 ($|\mathcal{S}|$) subcarriers spanning 0.5 MHz (B_a) are actively used. Thus, estimating the overall bandwidth B is a major hurdle that the eavesdropper has to overcome before proceeding with the remaining steps. Since sampling rate is determined by B, the appropriate rate at which the signal is to be sampled is also not known.

Note that lack of knowledge of B and consequently N (assuming subcarrier spacing can be inferred via a cyclostationary analysis) is not theoretically required to recover the transmitted information. From a theoretical perspective, as long as the received signal is sampled at a rate greater than the B_a samples/second, the transmitted symbols must be recoverable. However, sampling at a rate less than B samples/second precludes the use of a simple DFT-based receiver to recover the transmitted symbols. A DFT-based receiver assumes a sampling rate of B samples/second, and with the knowledge

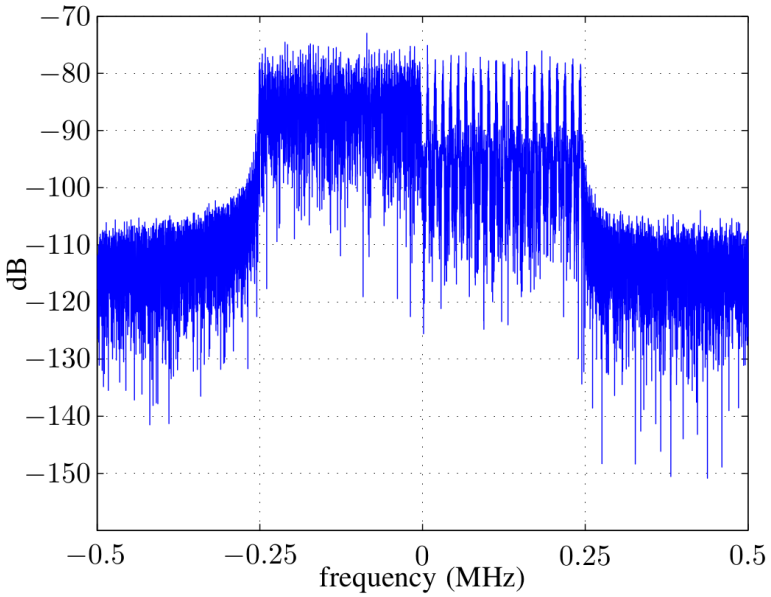


Figure 6.2: Periodogram of an NC-OFDM transmission with a combination of contiguous and interleaved subcarriers.

of the start of an NC-OFDM symbol, collects N samples and puts them through a N-point DFT to obtain $\hat{x}_k = \sum_{n=1}^{N} r[n]e^{j2\pi nk/N}$, where $\hat{x}_k$ is used to recover the symbol transmitted on the kth subcarrier. It is clear that without the correct sampling rate and the knowledge of N, these operations will not be possible and other techniques such as filter banks may be necessary to recover the transmitted symbols.

With the bandwidth B and consequently the correct sampling rate difficult to infer, we simply assume that the eavesdropper samples the received signal at a rate $1/T_s$ that is greater than B and investigate how other transmission parameters can be inferred. The CAF can be estimated from the received samples as

$$\hat{R}(\alpha, \bar{\tau}T_s) = \frac{1}{M}\sum_{n=1}^{M} r[n]r^*[n-\bar{\tau}]e^{-j2\pi\alpha nT_s} \tag{6.11}$$

where M is the total number of samples and $\bar{\tau} \in \mathbb{Z}$. Estimating the autocorrelation function by setting $\alpha = 0$, the peaks of the resulting function can reveal the useful symbol duration. In the case of contiguous or random allocation of subcarriers, the autocorrelation function has peaks only at $\pm T_u$ (ignoring the peak at $\bar{\tau} = 0$) and can be used to estimate the useful symbol duration. If the estimated autocorrelation

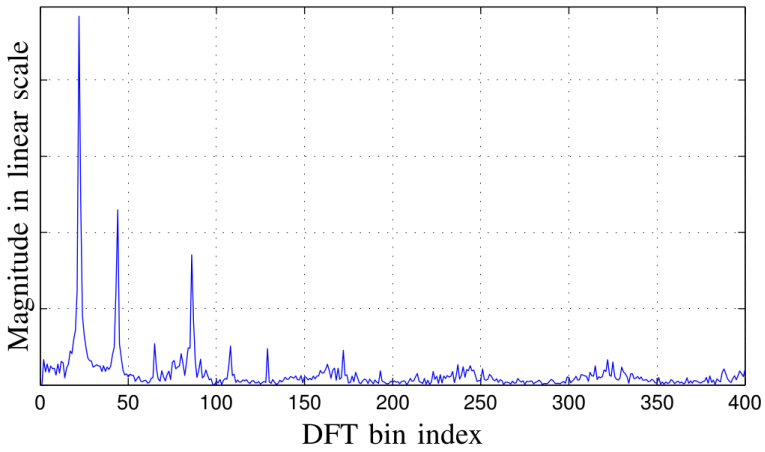


Figure 6.3: Harmonics of the PSD corresponding to interleaved subcarrier allocation.

function has a peak at $\bar{\tau} = \bar{\tau}^*$, then the useful symbol duration of the NC-OFDM transmission is given by $\bar{\tau}^* T_s$ with an accuracy of $\pm T_s$.

When an NC-OFDM transmission uses interleaved subcarriers, the estimation of the useful symbol duration via the autocorrelation function is no longer straightforward. In particular, when every qth subcarrier is used, the autocorrelation function has peaks spaced T_u/q apart until $\tau \leq T_o$. Suppose we see a set of 10 peaks spaced 64 μs apart, such an autocorrelation profile could correspond to the following transmission parameters under the assumption that $T_{cp} \leq T_u$:

T_u in μs	T_o in μs	q
320	$320 \leq T_o \leq 640$	5
256	$320 \leq T_o \leq 512$	4
192	$320 \leq T_o \leq 384$	3

While the outermost peak (largest possible value for T_u) provides an upper bound on q (here $q \leq 320/64$), it also indicates that $T_o \geq 320$. This along with the assumption that $T_{cp} \leq T_u$ implies that $T_u \geq 160$ and provides a lower bound on q by eliminating the choices of $q = 1$ and $q = 2$. Using the CAF alone, range of q cannot be reduced any further. Thus, when interleaved subcarriers are used, interleaving factor q cannot always be precisely determined from the CAF alone and consequently, the useful symbol duration cannot be resolved unambiguously.

The interleaving factor q, however, can be inferred by other means. For example, Fig. 6.2 clearly presents a visual distinction between interleaved and contiguous subcarrier use, suggesting that the periodogram can be used to infer the exact interleaving factor. Focusing on the portion of the periodogram that corresponds to interleaved subcarrier use, estimating q is similar to estimating the duty cycle of a rectangular wave. While there are well established techniques of estimating the duty cycle of a rectangular wave, the noisy nature of the signal under consideration makes estimating the duty cycle significantly more challenging. However, a feature that appears to provide some insight on q is based on the observation that a periodic rectangular wave with duty cycle $1/q$ has the qth harmonic completely suppressed. Thus, for the scenario under consideration, if the qth harmonic of the estimated PSD is suppressed relative to the $(q-1)$th and the $(q+1)$th harmonic, this suggests that the interleaving factor is q. Using this observation suppose one isolates the estimated PSD in Fig. 6.2 between 0 to 250 kHz, treats this as a noisy rectangular wave and computes its harmonics using a DFT, the relative strength of the harmonics obtained through such a procedure is plotted in Fig. 6.3. It can be seen that the third harmonic is suppressed relative to the fourth harmonic, suggesting that the interleaving factor is 3 in Fig. 6.2.

Rather than suggesting the above method as a means to estimate q, the above discussion is intended to highlight the additional complexities of eavesdropping on an NC-OFDM transmission that uses interleaved subcarrier allocation. While a cursory glance at the additional features in the CAF and the periodogram might raise alarm, a closer examination reveals that these features make discerning the actual NC-OFDM transmission parameters significantly harder. Further, choice of multiple interleaving factors along with some contiguous or randomly chosen subcarriers makes a CAF-based analysis extremely challenging.

Proceeding further, assuming that q and T_u are now known, consider estimating the total symbol duration T_o. Assuming $T_{cp} < T_u$, and noting that the CAF has distinct peaks at $(\alpha = n/T_o, \tau = T_u)$, we estimate the CAF as given in (6.11) at $\tau = T_u$ and $0 \leq \alpha \leq 1/2T_u$. Based on the earlier discussion on the CAF, the estimated CAF is expected to peak at exactly one instance in this range of α (assuming T_u was estimated

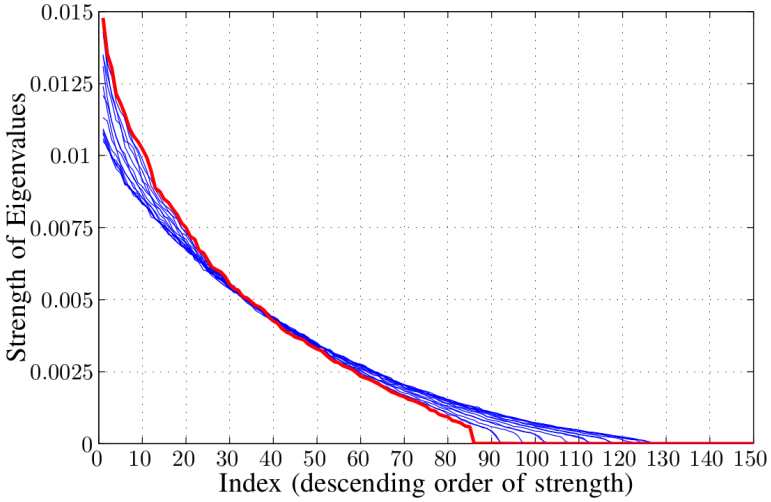


Figure 6.4: Eigenvalues from PCA for different values of δ. Eigenvalues are sorted in descending order.

correctly). Suppose a peak is noticed at $\alpha = \hat{\alpha}$, then $\hat{T_o} = 1/\hat{\alpha}$. This approach holds regardless of subcarrier allocation.

Notice that even if q, T_u, and T_o (and consequently, T_{cp} and subcarrier spacing) are known, the correct sampling rate (or equivalently, B) remains unknown. Next, we switch focus to a novel offline timing recovery method to identify the start of an NC-OFDM symbol.

6.4.1 Timing recovery at the eavesdropper

Timing recovery is a crucial and challenging task for the eavesdropper. Although an online, real-time recovery of the start of an OFDM symbol may not be necessary, the lack of knowledge of the total bandwidth B and other transmission parameters such as signal-to-noise ratio and the presence of frequency offset (down conversion to baseband is non-trivial in NC-OFDM when total bandwidth and center frequency are not known) precludes the use of existing blind mechanisms [124]. With these constraints in mind, we propose a simple principal-component-analysis-based timing recovery mechanism that only depends on the knowledge of the total symbol duration T_o and the assumption that the NC-OFDM symbols are transmitted in a periodic manner. Let $G = \lfloor \frac{T_o}{T_s} \rfloor$, so that

each NC-OFDM symbol spans G samples of the received signal $r[n]$. Timing recovery to identify the start of the NC-OFDM symbol requires segmenting the received signal $r[n]$ into sequences of length G. To accomplish this, we first form the following matrix

$$\mathbf{W}_\delta = [\mathbf{r}_{1\delta}\ \mathbf{r}_{2\delta}\ \mathbf{r}_{3\delta}\ \mathbf{r}_{4\delta}\ \ \ldots\ \ \mathbf{r}_{z\delta}] \tag{6.12}$$

where $\mathbf{r}_{k\delta} = r[(k-1)G + \delta + 1 : kG + \delta]$ and $\delta \in \mathbb{Z}^+$ with $1 \leq \delta \leq G$. Viewing the matrix $\mathbf{W}_\delta$ as representing z independent observations of an underlying system, we aim to identify the number of significant components in these z observations. In the context of an NC-OFDM transmission, the z observations constitute the z transmitted symbols and the active subcarriers are the underlying components generating these observations. The key idea to timing recovery is that, when the received signal $r[n]$ is segmented correctly, then the total number of significant components necessary to sufficiently explain the observed vectors is minimized and further, equal to the total number of active subcarriers. We use principal component analysis (PCA) to identify the total number of dominant components in a given set of observations $\mathbf{W}_\delta$. As δ is varied from 1 to G, the number of dominant components, as identified by the number of significant eigenvalues obtained via PCA varies. Suppose $\delta = \delta^*$ yields the smallest number of eigenvalues above a certain threshold, then δ^* is said to correctly identify the start of an NC-OFDM symbol and each column of $\mathbf{W}_\delta^*$ corresponds to one NC-OFDM symbol.

This approach is used to establish timing recovery in an NC-OFDM transmission similar to that depicted in Fig. 6.2, where a total of 85 subcarriers are used. Fig. 6.4 plots a sorted list of eigenvalues obtained from PCA for various values of δ. It can be seen that there exists a δ such that there are close to 85 dominant components (marked in red). For all other values of δ, more than 85 components are required to sufficiently explain the observations. This illustrates that such an approach can be used for offline timing recovery by the eavesdropper, even when very few transmission parameters are known beforehand. As an added benefit, such an approach also provides an estimate of the total number of active subcarriers, that can then be used to verify the parameters estimated using the CAF, as described in the previous section. Since this chapter

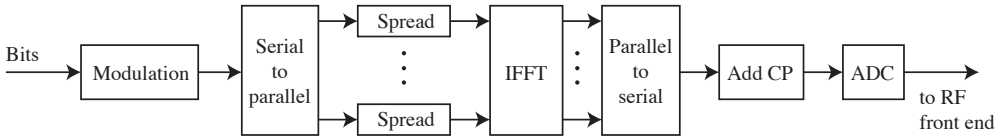


Figure 6.5: Method 1: MC-CDMA implementation by spreading the signal in time domain (also referred to as MC-DS-CDMA).

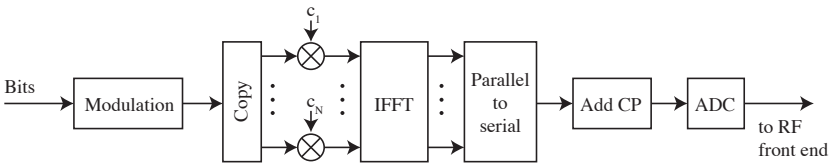


Figure 6.6: Method 2: MC-CDMA implementation by spreading the signal in frequency domain.

focuses on an LPE-analysis of NC-OFDM systems, we do not discuss the performance metrics of the proposed scheme, but instead use this approach as a guidepost for certain key design decisions for NC-OFDM systems.

6.5 Extension to MC-CDMA

Multicarrier-CDMA (MC-CDMA) is a transmission scheme which is derived from OFDM and it can potentially provide some improvement in terms of physical layer security. MC-CDMA spreads the data using spreading code (PN sequence) just before the feeding it to IFFT block in OFDM transmitter chain. MC-CMDA can be implemented in one of the two methods, 1) spreading the data in the time domain, i.e., after spreading the data each chip is sent over a different subcarrier, 2) spreading the data in the frequency domain, i.e., each subcarrier uses a completely separate PN sequence. Block diagram for both of these implementations are highlighted in Figs. 6.5 and 6.6. When MC-CDMA is extended to be used in the noncontiguous spectrum, it retains all the advantages in LPE performance associated with an NC-OFDM transmission. Due to additional use of a PN-sequence in MC-CDMA, it clearly provides another layer of security for an LPE-centric design. If a PN-sequence of length L_{pn} is used then probability of finding

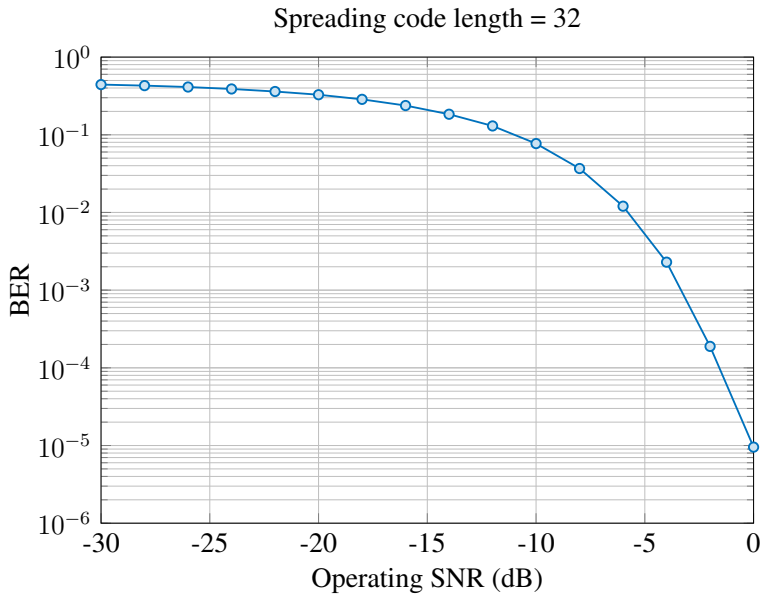


Figure 6.7: BER performance for method 1, spreading code length = 32, number of subcarriers = 32.

this PN-sequence using a brute-force method will be $2^{-L_{\text{pn}}}$ and pose difficulty for the eavesdropper. However, MC-CDMA can also potentially provide security enhancement in terms of probability of detection by lowering the transmission with a cost of reduced data rate. It must be noted that due to the problem of peak-to-average-power (PAPR) associated with OFDM-based transmission, the probability of detection for method 1 of MC-CDMA implementation will not be as low as a regular CDMA transmission for same operating SNR. Fig.6.7 presents the BER performance for MC-CDMA with time domain spreading when the spreading code length is 32, the number of subcarriers is also 32 and the channel is AWGN. It can be observed that such a setting allows the receiver to operate below the noise floor with reasonable BER. However, this comes at a cost of reduction in throughput. A similar trend can be seen for method 2 in Fig. 6.8.

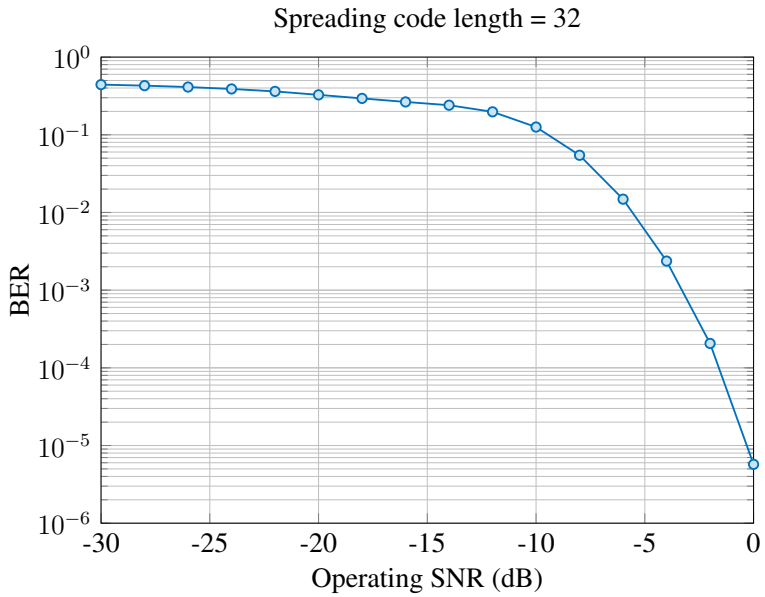


Figure 6.8: BER performance for method 2, spreading code length = 32, number of subcarriers = 32.

6.6 Key Takeaways

It is clear from the discussion in the previous sections that NC-OFDM systems offer significant advantages from an LPE standpoint. The key observations can be summarized as follows:

1. The biggest difference between OFDM and NC-OFDM systems is that the total nominal bandwidth of transmission (B) cannot be directly inferred in NC-OFDM, but is readily known in the case of OFDM. The lack of knowledge of B precludes the use of a traditional DFT-based receiver, and requires a receiver structure based on filter banks or other means to recover the transmitted symbols.

2. The CAF of NC-OFDM systems depends on the set of subcarriers that are used. While a contiguous or a random set of subcarriers results in a CAF that is very similar to OFDM, the CAF has more features when interleaved subcarriers are used. These additional features can make it more difficult to infer the NC-OFDM transmission parameters. Thus, a mixed use of contiguous/random and interleaved subcarriers in NC-OFDM makes a CAF-based analysis significantly more challenging.

3. Previously proposed CAF-suppression techniques such as choosing a random length for the cyclic prefix or adding a random delay between two multicarrier symbols can also be used to suppress the CAF features of NC-OFDM. However, such strategies do not affect the features of the autocorrelation function, which plays a crucial role in inferring the useful symbol duration T_u and further highlights the advantage of the additional ambiguity in the case of NC-OFDM systems.

4. Noting that the analysis presented here relies crucially on the assumption that the subcarrier allocation remains static over a certain duration and is used over several tens of OFDM symbols, an LPE-centric design requires dynamic use of subcarriers where the active subcarriers are constantly changed either in response to incumbent transmissions or to thwart an eavesdropper from inferring the transmission parameters. While the rate at which the active set is refreshed depends on several system parameters, including rate at which this information can be conveyed to the receiver, changes in incumbent transmissions, etc., some guidance on this issue can be drawn from the offline timing recovery scheme proposed in the previous section. Since a PCA based approach only succeeds if the total number of observations exceed the number of components, an LPE-centric design of an NC-OFDM system must not use an active set of subcarriers $\mathcal{S}$ for more than $|\mathcal{S}|$ NC-OFDM symbols. If the active set is switched at at least this rate, then the proposed timing recovery scheme is guaranteed to fail.

6.7 Chapter Summary

This chapter analyzes NC-OFDM transmissions from an LPE perspective. Using a cyclostationary analysis the various challenges faced by an eavesdropper in learning the transmission parameters are highlighted. Difficulty in estimating the correct sampling rate is identified as a major hurdle for detecting and decoding the transmitted signals. A novel timing recovery mechanism is proposed and used to provide guidance on the rate at which the active subcarrier set is to be refreshed. Key points of difference between NC-OFDM and OFDM system are established and suggestions for an LPE-centric design of NC-OFDM systems are provided. In particular, the ability to harness

fragmented spectrum and dynamically switch frequencies, along with the addition of further complexity to a CAF-based analysis highlight the strengths of NC-OFDM from an anti-jamming and LPE standpoint.

Chapter 7

Conclusion and future work

7.1 Summary of research

The results from this thesis can be broadly categorized into three parts. First, we have highlighted the state of the spectrum as being noncontiguous and motivated its use for opportunistic access. Second, we have proposed the use of noncontiguous OFDM (NC-OFDM) as a potential candidate which can enable such opportunistic access and addressed various issues with the implementation of NC-OFDM. Thirdly, we have explored the inherent security feature present in an NC-OFDM transmission.

7.1.1 Spectrum allocation in noncontiguous spectrum

We explored various aspects of the opportunistic access of a noncontiguous spectrum. We presented scenarios which result in the fragmentation of the spectrum. We also highlighted the motivation for using noncontiguous spectrum by providing TV white space as an example and addressed the problem of spectrum allocation for these cases. We emphasized the significance of considering *spectrum span* as one of the critical parameters for spectrum allocation due to its impact on the system power consumption. This insight can also be extended to the radios with limited ADC/DAC bandwidth which are trying to operate over a much larger bandwidth.

7.1.2 Noncontiguous OFDM as a candidate

Specifically, we proposed the use of noncontiguous OFDM (NC-OFDM) as a multi-carrier transmission method which can be used in these scenarios. In scenarios where noncontiguous spectrum is accessed by multiple NC-OFDM based communication links

which can potentially interfere with each other, we conducted the study to recognize the problems associated with the asynchronous nature of such transmission. We have introduced the use of a decentralized synchronization scheme using low-powered beacons and shown the advantages specifically for the links operating at lower SNR. In cases where such synchronization cannot be achieved, we performed the analysis to identify necessary guard band requirement. Overall these guidelines can be utilized while designing an NC-OFDM-based wireless communication system. We further extended the application of the underlay transmission which is utilized for synchronization to be used as a subsidiary channel which not only supports the NC-OFDM channel in frequency offset estimation and time offset estimation but also to transfer control information between transmitters and receivers. Such an underlay transmission along with an OFDM-based transmission can potentially support a low-rate bursty communication, thus making this underlay transmission a great candidate for supporting Internet-of-Things-like communication.

7.1.3 Security features of NC-OFDM

At last, we studied inherent security features of NC-OFDM transmission and found that NC-OFDM has a good low probability of exploitation characteristics compared to regular OFDM transmission.

7.2 Future work

Based on our analysis a comprehensive spectrum allocation scheme can be designed which not only incorporates the impact on system power consumption but also considers ICI due to asynchronous transmission. When establishing an NC-OFDM-based connection between a transmitter and a receiver, the pair needs to agree on a set of subcarriers to be used. This rendezvous poses an interesting problem to solve. Once the set of subcarrier has been agreed upon, apporpriate allocation of pilot for channel estimation is a challanging problem that needs to be addressed.

References

[1] M. N. Islam, N. B. Mandayam, S. Kompella, and I. Seskar, "Power optimal non-contigous spectrum access," submitted for publication in *IEEE Trans. Wireless Commun.*, 2013. [Online]. Available: http://arxiv.org/abs/1309.0861

[2] "Report of the Spectrum Efficiency Working Group," Federal Communications Commission, Report, Nov 2002. [Online]. Available: https://transition.fcc.gov/sptf/files/SEWGFinalReport_1.pdf

[3] "Second Report and Order and Memorandum Opinion and Order," Federal Communications Commission, Report, Nov 2008. [Online]. Available: https://apps.fcc.gov/edocs_public/attachmatch/FCC-08-260A1.pdf

[4] R. Zhang, M. Wang, L. X. Cai, Z. Zheng, X. Shen, and L. L. Xie, "LTE-unlicensed: the future of spectrum aggregation for cellular networks," *IEEE Transactions on Wireless Communications*, vol. 22, no. 3, pp. 150–159, June 2015.

[5] J. Jeon, Q. C. Li, H. Niu, A. Papathanassiou, and G. Wu, "LTE in the unlicensed spectrum: A novel coexistence analysis with WLAN systems," in *Proceedings of IEEE Global Communication Conference (GLOBECOM)*, 2014, pp. 3459–3464.

[6] J. Mitola and G. Q. Maguire Jr., "Cognitive radio: making software radios more personal," *IEEE Transactions on Professional Communication*, vol. 6, no. 4, pp. 13–18, Aug. 1999.

[7] E. Biglieri, A. J. Goldsmith, L. J. Greenstein, N. B. Mandayam, and H. V. Poor, *Principles of cognitive radio*. Cambridge University Press, 2012.

[8] S. Haykin, "Cognitive radio: brain-empowered wireless communications," *IEEE Journal on Selected Areas in Communications*, vol. 23, no. 2, pp. 201–220, Feb. 2005.

[9] R. Thomas, L. DaSilva, and A. MacKenzie, "Cognitive networks," in *Proceedings of IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN)*, Nov. 2005, pp. 352–360.

[10] O. Ileri and N. B. Mandayam, "Dynamic spectrum access models: toward an engineering perspective in the spectrum debate," *IEEE Communications Magazine*, vol. 46, no. 1, pp. 153–160, Jan. 2008.

[11] Y.-C. Liang, Y. Zeng, E. Peh, and A. T. Hoang, "Sensing-throughput tradeoff for cognitive radio networks," *IEEE Transactions on Wireless Communications*, vol. 7, no. 4, pp. 1326–1337, Apr. 2008.

[12] S. Srinivasa and S. A. Jafar, "Cognitive radios for dynamic spectrum access - The throughput potential of cognitive radio: A theoretical perspective," *IEEE Communications Magazine*, vol. 45, no. 5, pp. 73–79, May 2007.

[13] M. Cesana, F. Cuomo, and E. Ekici, "Routing in cognitive radio networks: challenges and solutions," *Ad Hoc Netw.*, vol. 9, no. 3, pp. 228–248, May 2011.

[14] G. Cheng, W. Liu, Y. Li, and W. Cheng, "Joint on-demand routing and spectrum assignment in cognitive radio networks," in *Proceedings of IEEE International Conference on Communications (ICC)*, Jun. 2007, pp. 6499–6503.

[15] M. N. Islam, N. Mandayam, and S. Kompella, "Optimal resource allocation and relay selection in bandwidth exchange based cooperative forwarding," in *Proceedings of IEEE International Symposium on Modeling and Optimization in Mobile, Ad Hoc and Wireless Network (WiOpt)*, 2012, pp. 192–199.

[16] R. Rajbanshi, A. M. Wyglinski, and G. J. Minden, "An efficient implementation of NC-OFDM transceivers for cognitive radios," in *Proceedings of EAI International Conference on Cognitive Radio Oriented Wireless Network and Communication (CROWNCOM)*, Jun. 2006.

[17] A. Dutta, D. Saha, D. Grunwald, and D. Sicker, "Practical implementation of blind synchronization in NC-OFDM based cognitive radio networks," in *Proc. ACM Workshop Cognitive Radio networks*, 2010.

[18] F. Schaich and T. Wild, "Waveform contenders for 5G – OFDM vs. FBMC vs. UFMC," in *Proceedings of IEEE International Symposium on Communications, Control and Signal Processing (ISCCSP)*, May 2014, pp. 457–460.

[19] F. Schaich, "Filterbank based multi carrier transmission (FBMC)evolving OFDM: FBMC in the context of WiMAX," in *Wireless Conference (EW), 2010 European*, 2010, pp. 1051–1058.

[20] G. Fettweis, M. Krondorf, and S. Bittner, "GFDM-generalized frequency division multiplexing," in *Proceedings of IEEE Vehicular Technollogy Conference (Spring)*, 2009, pp. 1–4.

[21] V. Vakilian, T. Wild, F. Schaich, S. ten Brink, and J.-F. Frigon, "Universal-filtered multi-carrier technique for wireless systems beyond LTE," in *Proceedings of IEEE Global Communication Conference (GLOBECOM) Workshop*, 2013, pp. 223–228.

[22] N. Michailow, M. Matthé, I. S. Gaspar, A. N. Caldevilla, L. L. Mendes, A. Festag, and G. Fettweis, "Generalized frequency division multiplexing for 5th generation cellular networks," *IEEE Transactions on Communications*, vol. 62, no. 9, pp. 3045–3061, 2014.

[23] J. D. Poston and W. D. Horne, "Discontiguous OFDM considerations for dynamic spectrum access in idle TV channels," in *Proceedings of IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN)*, 2005, pp. 607–610.

[24] R. Kumbhkar, M. N. Islam, N. B. Mandayam, and I. Seskar, "Rate optimal design of a wireless backhaul network using TV white space," in *Proceedings of IEEE International Conference Communication System Networks (COMSNETS)*, Jan. 2015.

[25] R. Kumbhkar, T. Kuber, G. Sridharan, N. B. Mandayam, and I. Seskar, "Opportunistic spectrum allocation for max-min rate in NC-OFDMA," in *Proceedings of IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN)*, Sep. 2015, pp. 385–391.

[26] D. Li, X. Dai, and H. Zhang, "Sidelobe suppression in NC-OFDM systems using constellation adjustment," *IEEE Communications Letters*, vol. 13, no. 5, pp. 327–329, May 2009.

[27] A. Ghassemi, L. Lampe, A. Attar, and T. Gulliver, "Joint sidelobe and peak power reduction in OFDM-based cognitive radio," in *Proceedings of IEEE Vehicular Technology Conference (Fall)*, Sep. 2010.

[28] J. Acharya, H. Viswanathan, and S. Venkatesan, "Timing acquisition for non contiguous OFDM based dynamic spectrum access," in *Proceedings of IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN)*, Oct. 2008.

[29] B. Huang, J. Wang, W. Tang, and S. Li, "An effective synchronization scheme for NC-OFDM systems in cognitive radio context," in *Proceedings of IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN)*, Sep. 2010.

[30] D. Qu, J. Ding, T. Jiang, and X. Sun, "Detection of non-contiguous OFDM symbols for cognitive radio systems without out-of-band spectrum synchronization," *IEEE Transactions on Wireless Communications*, vol. 10, no. 2, pp. 693–701, Feb. 2011.

[31] T. Schmidl and D. Cox, "Robust frequency and timing synchronization for ofdm," *IEEE Transactions on Communications*, vol. 45, no. 12, pp. 1613–1621, Dec. 1997.

[32] H. Minn, V. Bhargava, and K. Letaief, "A robust timing and frequency synchronization for OFDM systems," *IEEE Transactions on Wireless Communications*, vol. 2, no. 4, pp. 822–839, Jul. 2003.

[33] M. Morelli, C.-C. Kuo, and M.-O. Pun, "Synchronization techniques for orthogonal frequency division multiple access (OFDMA): A tutorial review," *Proceedings of the IEEE*, vol. 95, no. 7, pp. 1394–1427, Jul. 2007.

[34] B. Ai, Z.-X. Yang, C.-Y. Pan, J. hua Ge, Y. Wang, and Z. Lu, "On the synchronization techniques for wireless OFDM systems," *IEEE Transactions on Broadcasting*, vol. 52, no. 2, pp. 236–244, June 2006.

[35] S. Feng, H. Zheng, H. Wang, J. Liu, and P. Zhang, "Preamble design for non-contiguous spectrum usage in cognitive radio networks," in *Proceedings of IEEE Wireless Communication Network Conference (WCNC)*, Apr. 2009.

[36] R. Kumbhkar, G. Sridharan, N. B. Mandayam, I. Seskar, and S. Kompella, "Impact of asynchronous transmissions in noncontiguous ofdma," in *Dynamic Spectrum Access Networks (DySPAN), 2017 IEEE International Symposium on*. IEEE, 2017, pp. 1–9.

[37] ——, "Design and Implementation of an Underlay Control Channel for NC-OFDM-Based Networks," in *Proceedings of IEEE International Conference Information Science and System (CISS)*, Mar 2016.

[38] G. Sridharan, R. Kumbhkar, N. B. Mandayam, I. Seskar, and S. Kompella, "Physical-layer security of nc-ofdm-based systems," in *Proceedings of IEEE Military Communication Conference (MILCOM)*, Nov 2016, pp. 1101–1106.

[39] J. M. Chapin and W. H. Lehr, "Mobile broadband growth, spectrum scarcity, and sustainable competition," in *39th Research Conference on Communication, Information and Internet Policy*, Alexandria, VA, September 2011.

[40] G. R. Faulhaber, "The question of spectrum: Technology, management and regime change," in *The Conference on the Economics, Technology and Policy of Unlicensed Spectrum*, East Lansing, MI, 2005.

[41] C. Gerami, N. B. Mandayam, and L. Greenstein, "Backhauling in tv white spaces," in *Proceedings of IEEE Global Communication Conference (GLOBECOM)*, Dec 2010, pp. 1–6.

[42] J. Peha, "Approaches to spectrum sharing," *IEEE Communications Magazine*, vol. 43, no. 2, pp. 10–12, Feb 2005.

[43] M. Kodialam and T. Nandagopal, "Characterizing the capacity region in multi-radio multi-channel wireless mesh networks," in *Proceedings of ACM Annual International Conference on Mobile Computing and Network (MobiCom)*, 2005, pp. 73–87. [Online]. Available: http://doi.acm.org/10.1145/1080829.1080837

[44] P. Kyasanur and N. H. Vaidya, "Capacity of multi-channel wireless networks: Impact of number of channels and interfaces," in *Proceedings of ACM Annual International Conference on Mobile Computing and Network (MobiCom)*, 2005, pp. 43–57. [Online]. Available: http://doi.acm.org/10.1145/1080829.1080835

[45] O.-S. Shin, N. Devroye, P. Mitran, H. Ochiai, S. Ghassemzadeh, H. Kung, and V. Tarokh, "Cooperation, competition and cognition in wireless networks," in *Cooperation in Wireless Networks: Principles and Applications*, F. Fitzek and M. Katz, Eds. Springer Netherlands, 2006, pp. 69–100. [Online]. Available: http://dx.doi.org/10.1007/1-4020-4711-8_3

[46] R. Etkin, A. Parekh, and D. Tse, "Spectrum sharing for unlicensed bands," *IEEE Journal on Selected Areas in Communications*, vol. 25, no. 3, pp. 517–528, April 2007.

[47] N. Clemens and C. Rose, "Intelligent power allocation strategies in an unlicensed spectrum," in *Proceedings of IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN)*, Nov 2005, pp. 37–42.

[48] J. Hicks, A. MacKenzie, J. Neel, and J. Reed, "A game theory perspective on interference avoidance," in *Proceedings of IEEE Global Communication Conference (GLOBECOM)*, vol. 1, Nov 2004, pp. 257–261 Vol.1.

[49] J. Huang, R. Berry, and M. Honig, "Spectrum sharing with distributed interference compensation," in *Proceedings of IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN)*, Nov 2005, pp. 88–93.

[50] D. Zhang, R. Shinkuma, and N. B. Mandayam, "Bandwidth exchange: an energy conserving incentive mechanism for cooperation," *IEEE Transactions on Wireless Communications*, vol. 9, no. 6, pp. 2055–2065, June 2010.

[51] D. Raychaudhuri, N. B. Mandayam, J. B. Evans, B. J. Ewy, S. Seshan, and P. Steenkiste, "CogNet: An architectural foundation for experimental cognitive radio networks within the future internet," in *Proceedings of ACM International Workshop on Mobility in the Evolving Internet Architecture (MobiArch)*, Dec. 2006, pp. 11–16.

[52] Z. Miljanic, I. Seskar, K. Le, and D. Raychaudhuri, "The WINLAB Network Centric Cognitive Radio Hardware Platform - WiNC2R," in *Proceedings of EAI International Conference on Cognitive Radio Oriented Wireless Network and Communication (CROWNCOM)*, Aug 2007, pp. 155–160.

[53] WARP: Wireless Open-access Research Platform. [Online]. Available: http://warp.rice.edu/

[54] USRP software radio systems: Ettus Resarch. [Online]. Available: http://www.ettus.com/

[55] GENI Cognitive Radio Kit. [Online]. Available: http://crkit.orbit-lab.org/

[56] J. D'Ambrosia, "100 gigabit ethernet and beyond [commentary]," *IEEE Communications Magazine*, vol. 48, no. 3, pp. S6–S13, March 2010.

[57] G. Wellbrock and T. Xia, "The road to 100g deployment [commentary]," *IEEE Communications Magazine*, vol. 48, no. 3, pp. S14–S18, March 2010.

[58] E. Amaldi, A. Capone, and F. Malucelli, "Planning UMTS base station location: optimization models with power control and algorithms," *IEEE Transactions on Wireless Communications*, vol. 2, no. 5, pp. 939–952, Sept 2003.

[59] Y. Yu, S. Murphy, and L. Murphy, "Planning Base Station and Relay Station Locations in IEEE 802.16j Multi-Hop Relay Networks," in *Proceedings of IEEE Consumer Communications & Networking Conference*, Jan 2008, pp. 922–926.

[60] L. Yang, Z. Zhang, W. Hou, B. Y. Zhao, and H. Zheng, "Papyrus: A software platform for distributed dynamic spectrum sharing using SDRs," *ACM SIGCOMM Comput. Commun. Review*, vol. 41, pp. 31–37, 2011.

[61] L. Yang, B. Y. Zhao, and H. Zheng, "The spaces between us: Setting and maintaining boundaries in wireless spectrum access," in *Proceedings of ACM Annual International Conference on Mobile Computing and Network (MobiCom)*, Sep. 2010, pp. 37–48.

[62] R. Rajbanshi, A. M. Wyglinski, and G. J. Minden, "An efficient implementation of NC-OFDM transceivers for cognitive radios," in *Proceedings of EAI International Conference on Cognitive Radio Oriented Wireless Network and Communication (CROWNCOM)*, Jun. 2006.

[63] M. Chiang, P. Hande, T. Lan, and C. W. Tan, "Power control in wireless cellular networks," *Found. Trends Netw.*, vol. 2, no. 4, pp. 381–533, Apr. 2008. [Online]. Available: http://dx.doi.org/10.1561/1300000009

[64] R. Yates, "A framework for uplink power control in cellular radio systems," *IEEE Journal on Selected Areas in Communications*, vol. 13, no. 7, pp. 1341–1347, Sep 1995.

[65] C. Saraydar, N. B. Mandayam, and D. Goodman, "Efficient power control via pricing in wireless data networks," *IEEE Transactions on Communications*, vol. 50, no. 2, pp. 291–303, Feb 2002.

[66] Cisco Visual Networking Index. [Online]. Available: http://www.cisco.com/c/en/us/solutions/service-provider/visual-networking-index-vni/index.html

[67] World in 2014: ICT facts and figure. [Online]. Available: http://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx

[68] "Propagation data and prediction methods required for the design of terrestrial line-of-sight systems," International Telecommunication Union, Recommendation. [Online]. Available: http://www.itu.int/rec/R-REC-P/en

[69] CVX Research, Inc., "CVX: Matlab software for disciplined convex programming, version 2.0 beta," Sep. 2012. [Online]. Available: http://cvxr.com/cvx

[70] MOSEK ApS, *The MOSEK optimization toolbox for MATLAB manual. Version 7.1 (Revision 28).*, 2015. [Online]. Available: http://docs.mosek.com/7.1/toolbox/index.html

[71] GNU Radio Website, accessed February 2012. [Online]. Available: http://www.gnuradio.org

[72] Texas Instruments, Inc., "Datasheet for ADS62P4X: Dual channel, 14 bits, 125/105/80/65 MSPS ADC with DDR LVDS/CMOS outputs." [Online]. Available: http://www.ti.com/lit/ds/symlink/ads62p42.pdf

[73] ——, "Datasheet for ADS4249: Dual-Channel, 14-Bit, 250-MSPS Ultralow-Power ADC." [Online]. Available: http://www.ti.com/lit/ds/symlink/ads4249.pdf

[74] Analog Devices, Inc., "Datasheet for AD9777: 16-bit interpolating dual DAC converter." [Online]. Available: http://www.analog.com/media/en/technical-documentation/data-sheets/AD9777.pdf

[75] Texas Instruments, Inc., "Datasheet for DAC3152/DAC3162: Dual-Channel, 10-/12-Bit, 500-MSPS Digital-to-Analog Converters." [Online]. Available: http://www.ti.com/lit/ds/symlink/dac3162.pdf

[76] G. Li, Z. Xu, C. Xiong, C. Yang, S. Zhang, Y. Chen, and S. Xu, "Energy-efficient wireless communications: tutorial, survey, and open issues," *IEEE Transactions on Wireless Communications*, vol. 18, no. 6, pp. 28–35, Dec. 2011.

[77] S. Cui, A. Goldsmith, and A. Bahai, "Energy-constrained modulation optimization," *IEEE Transactions on Wireless Communications*, vol. 4, no. 5, pp. 2349–2360, Sep. 2005.

[78] P. Grover, K. Woyach, and A. Sahai, "Towards a communication-theoretic understanding of system-level power consumption," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 8, pp. 1744–1755, Sep. 2011.

[79] J. Jia and W. Zhuang, "Capacity of multi-hop wireless network with frequency agile software defined radio," in *Proceedings of IEEE International Conference on Computer Communications (INFOCOM)*, Apr. 2011, pp. 41–46.

[80] L. Cao, L. Yang, and H. Zheng, "The impact of frequency-agility on dynamic spectrum sharing," in *Proceedings of IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN)*, Apr. 2010.

[81] G. Zhang and S. Feng, "Subcarrier allocation algorithms based on graph-coloring in cognitive radio NC-OFDM system," in *Proceedings of IEEE International Conference on Computer Science and Information Technology (ICCSIT)*, July 2010, pp. 535–540.

[82] M. Grant and S. Boyd, "Graph implementations for nonsmooth convex programs," in *Recent Advances in Learning and Control*, ser. Lecture Notes in Control and Information Sciences, V. Blondel, S. Boyd, and H. Kimura, Eds. Springer-Verlag Limited, 2008, pp. 95–110.

[83] WINLAB, Rutgers, The State University of New Jersey. ORBIT: Open access research testbed for next-generation wireless networks. [Online]. Available: http://www.orbit-lab.org

[84] P. Murphy, A. Sabharwal, and B. Aazhang, "Design of WARP: A wireless open-access research platform," in *Proc. European Signal Process. Conf. (EUSIPCO)*, Sep. 2006.

[85] Z. Yuan and A. M. Wyglinski, "On sidelobe suppression for multicarrier-based transmission in dynamic spectrum access networks," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 4, pp. 1998–2006, May 2010.

[86] F. Tufvesson, O. Edfors, and M. Faulkner, "Time and frequency synchronization for OFDM using PN-sequence preambles," in *Proceedings of IEEE Vehicular Technology Conference (Fall)*, Sep. 1999, pp. 2203–2207.

[87] A. M. Tonello, N. Laurenti, and S. Pupolin, "Analysis of the uplink of an asynchronous multi-user DMT OFDMA system impaired by time offsets, frequency offsets, and multi-path fading," in *Proceedings of IEEE Vehicular Technology Conference (Fall)*, vol. 3, 2000, pp. 1094–1099 vol.3.

[88] K. Raghunath and A. Chockalingam, "SIR Analysis and Interference Cancellation in Uplink OFDMA with Large Carrier Frequency and Timing Offsets," in *Proceedings of IEEE Wireless Communication Network Conference (WCNC)*, March 2007, pp. 996–1001.

[89] K. A. Hamdi, "Precise interference analysis of OFDMA time-asynchronous wireless ad-hoc networks," *IEEE Transactions on Wireless Communications*, vol. 9, no. 1, pp. 134–144, January 2010.

[90] Y. Medjahdi, M. Terr, D. L. Ruyet, and D. Roviras, "Asynchronous OFDM/FBMC interference analysis in selective channels," in *Proceedings of IEEE Symposium on Personal, Indoor and Mobile Communication (PIMRC)*, Sept 2010, pp. 538–542.

[91] V. Kotzsch and G. Fettweis, "Interference Analysis in Time and Frequency Asynchronous Network MIMO OFDM Systems," in *Proceedings of IEEE Wireless Communication Network Conference (WCNC)*, April 2010, pp. 1–6.

[92] X. Li, F. Ng, and T. Han, "Carrier frequency offset mitigation in asynchronous cooperative ofdm transmissions," *IEEE Transactions on Signal Processing*, vol. 56, no. 2, pp. 675–685, Feb 2008.

[93] D. Marabissi, R. Fantacci, and S. Papini, "Robust multiuser interference cancellation for ofdm systems with frequency offset," *IEEE Transactions on Wireless Communications*, vol. 5, no. 11, pp. 3068–3076, November 2006.

[94] S. Barbarossa, M. Pompili, and G. B. Giannakis, "Channel-independent synchronization of orthogonal frequency division multiple access systems," *IEEE Journal on Selected Areas in Communications*, vol. 20, no. 2, pp. 474–486, Feb 2002.

[95] R. Fantacci, D. Marabissi, and S. Papini, "Multiuser interference cancellation receivers for OFDMA uplink communications with carrier frequency offset," in *Proceedings of IEEE Global Communication Conference (GLOBECOM)*, vol. 5, Nov 2004, pp. 2808–2812 Vol.5.

[96] M. Faulkner, "The effect of filtering on the performance of OFDM systems," *Proceedings of IEEE Vehicular Technollogy Conference (Spring)*, vol. 49, no. 5, pp. 1877–1884, Sep 2000.

[97] H. B. Salameh, M. Krunz, and D. Manzi, "An Efficient Guard-Band-Aware Multi-Channel Spectrum Sharing Mechanism for Dynamic Access Networks," in *Proceedings of IEEE Global Communication Conference (GLOBECOM)*, Dec 2011, pp. 1–5.

[98] M. Bohge, F. Naghibi, and A. Wolisz, "The use of guard bands to mitigate multiple access interference in the OFDMA uplink," in *Proc. International OFDM Workshop.*, 2008, pp. 75–79.

[99] T. M. Schmidl and D. C. Cox, "Robust frequency and timing synchronization for OFDM," *IEEE Transactions on Communications*, vol. 45, no. 12, pp. 1613–1621, Dec 1997.

[100] H. Bolcskei, "Blind estimation of symbol timing and carrier frequency offset in wireless OFDM systems," *IEEE Transactions on Communications*, vol. 49, no. 6, pp. 988–999, Jun 2001.

[101] Ettus Knowledge Base, "SBX — Ettus Knowledge Base," 2016, [Online; accessed 10-October-2016]. [Online]. Available: https://kb.ettus.com/index.php?title=SBX&oldid=3021

[102] B. F. Lo, "A survey of common control channel design in cognitive radio networks," *Elsevier Physical Communication*, vol. 4, no. 1, pp. 26–39, 2011.

[103] M. E. Sahin and H. Arslan, "System design for cognitive radio communications," in *Proceedings of EAI International Conference on Cognitive Radio Oriented Wireless Network and Communication (CROWNCOM)*, 2006.

[104] D. L. Wasden, H. Moradi, and B. Farhang-Boroujeny, "Design and implementation of an underlay control channel for cognitive radios," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 10, pp. 1875–1889, Nov. 2012.

[105] R.-R. Chen, K. H. Teo, and B. Farhang-Boroujeny, "Random access protocols for collaborative spectrum sensing in multi-band cognitive radio networks," *IEEE Journal of Selected Topics in Signal Processing*, vol. 5, no. 1, pp. 124–136, 2011.

[106] K. Bian, J.-M. Park, and R. Chen, "A quorum-based framework for establishing control channels in dynamic spectrum access networks," in *Proceedings of ACM Annual International Conference on Mobile Computing and Network (MobiCom)*, 2009, pp. 25–36.

[107] C. Cormio and K. R. Chowdhury, "Common control channel design for cognitive radio wireless ad hoc networks using adaptive frequency hopping," *Elsevier Ad Hoc Networks*, vol. 8, no. 4, pp. 430–438, 2010.

[108] B. F. Lo, I. F. Akyildiz, and A. M. Al-Dhelaan, "Efficient recovery control channel design in cognitive radio ad hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 9, pp. 4513–4526, Nov. 2010.

[109] M. Petracca, R. Pomposini, F. Mazzenga, R. Giuliano, and M. Vari, "An always available control channel for cooperative sensing in cognitive radio networks," in *Proc. IEEE IFIP Wireless Days Conf.*, 2010.

[110] M. N. Islam, N. B. Mandayam, S. Kompella, and I. Seskar. (2013) Power Optimal Non-contiguous Spectrum Access. [Online]. Available: http://arxiv.org/abs/1309.0861

[111] R. Liu and W. Trappe, *Securing wireless communications at the physical layer*. Springer, 2010, vol. 7.

[112] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proceedings of ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*. ACM, 2005, pp. 46–57.

[113] G. Padmavathi, M. Shanmugapriya *et al.*, "A survey of attacks, security mechanisms and challenges in wireless sensor networks," *arXiv:0909.0576*, 2009.

[114] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," *Communications of the ACM*, vol. 47, no. 6, pp. 53–57, 2004.

[115] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," *Ad hoc networks*, vol. 1, no. 2, pp. 293–315, 2003.

[116] R. K. Nichols and P. C. Lekkas, *Wireless security*. McGraw-Hill New York, 2002.

[117] M. Bouanen, F. Gagnon, G. Kaddoum, D. Couillard, and C. Thibeault, "An LPI design for secure OFDM systems," in *Proceedings of IEEE Military Communication Conference (MILCOM)*, 2012.

[118] Z. Ankaral, M. Karabacak, and H. Arslan, "Cyclic feature concealing CP selection for physical layer security," in *Proceedings of IEEE Military Communication Conference (MILCOM)*, 2014, pp. 485–489.

[119] R. R. Meyer and M. N. Newhouse, "OFDM waveform feature suppression," in *Proceedings of IEEE Military Communication Conference (MILCOM)*, vol. 1, 2002, pp. 582–586.

[120] T. Yucek and H. Arslan, "Feature suppression for physical-layer security in OFDM systems," in *Proceedings of IEEE Military Communication Conference (MILCOM)*, 2007.

[121] G. L. Peng, "Study of cyclostationary feature detectors for cognitive radio," Ph.D. dissertation, 2007.

[122] W. A. Gardner, A. Napolitano, and L. Paura, "Cyclostationarity: Half a century of research," *Signal processing*, vol. 86, no. 4, pp. 639–697, 2006.

[123] A. Punchihewa, Q. Zhang, O. A. Dobre, C. Spooner, S. Rajan, and R. Inkol, "On the cyclostationarity of OFDM and single carrier linearly digitally modulated signals in time dispersive channels: Theoretical developments and application," *IEEE Transactions on Wireless Communications*, vol. 9, no. 8, pp. 2588–2599, Aug. 2010.

[124] H. Bölcskei, "Blind estimation of symbol timing and carrier frequency offset in wireless OFDM systems," *IEEE Transactions on Communications*, vol. 49, no. 6, pp. 988–999, 2001.