COMMUNICATION AND JAMMING BDA OF OFDMA COMMUNICATION SYSTEMS USING THE SOFTWARE DEFINED RADIO PLATFORM WARP

THESIS

Kate J. Yaxley, FLTLT, Royal Australian Air Force

AFIT-ENG-MS-15-M-073

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

AFIT-ENG-MS-15-M-073

COMMUNICATION AND JAMMING BDA OF OFDMA COMMUNICATION SYSTEMS USING THE SOFTWARE DEFINED RADIO PLATFORM WARP

THESIS

Presented to the Faculty

Department of Electrical and Computer Engineering

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

in Partial Fulfillment of the Requirements for the

Degree of Master of Science in Electrical Engineering

Kate J. Yaxley, B.E. (Elec) Hons Div II Class I

FLTLT, Royal Australian Air Force

March 2015

AFIT-ENG-MS-15-M-073

COMMUNICATION AND JAMMING BDA OF OFDMA COMMUNICATION SYSTEMS USING THE SOFTWARE DEFINED RADIO PLATFORM WARP

THESIS

Kate J. Yaxley, B.E. (Elec) Hons Div II Class I
FLTLT, Royal Australian Air Force

Committee Membership:

Dr. Richard K. Martin
Chair

Dr. Julie Jackson
Member

Dr. Jason Pennington
Member

AFIT-ENG-MS-15-M-073

Abstract

The aim of this research is to demonstrate and evaluate the ability to eavesdrop and interfere with orthogonal frequency division multiple access-down link (OFDMA-DL) signal features utilising Wireless Open Access Research Platform (WARP) boards. The OFDMA-DL waveforms have been developed with 64 sub carriers and have guards and pilots as comparable to the 802.11a WiFi standard.

An eavesdropper/interferer (*ExJx*) is used to estimate signal features, remotely gaining intelligence without alerting the communication system. This research also demonstrates how estimated signal features can be used to interfere with an established communication system.

Methods used to perform the signal feature estimation exploit the cyclostationary nature of the OFDMA-DL waveform, with higher order cumulants utilised to classify modulation schemes.

To assess the ability of the *ExJx* system to eavesdrop (*Ex*), Communication Battle Damage Assessment (CBDA) techniques are used. To assess the ability of the *ExJx* system to interfere (*Jx*), Jamming Battle Damage Assessment (JBDA) techniques are used.

For Grandpa.
Beloved Husband, devoted Dad, loved Grandpa, cherished Great-Grandpa.

Acknowledgments

I would like to thank my advisor, Dr. Richard Martin for his patience and excellent advice throughout my course, but especially during my thesis.

I also thank my committee, Dr. Julie Jackson and Dr. Jason Pennington for their helpful comments and to Dr. Pennington for his introduction to WARP boards.

I also wish to acknowledge FLTLT Nicholas Rutherford for his work on *Blind demodulation of pass band OFDMA signals and Jamming Battle Damage Assessment utilizing Link Adaptation*, the methods of which have been used throughout this research.

Thank you to the WARP project team for providing an excellent resource for all users of WARP, as well as the photos of hardware available at the WARP repository, some of which have been used in this document.

To the IMSO, Ms. Annette Robb, and her support staff, thank you for ensuring our transition to the United States went as smoothly and easily as possible.

To Capt. Van, Capt. Bailey and Capt. Abeita, thank you for the great friendship and help with homework throughout this Masters program.

Finally to my friends, family, and especially my husband and daughters, thank you for supporting me throughout this experience.

Kate J. Yaxley

Table of Contents

Page

Abstract iv

Dedication v

Acknowledgments vi

Table of Contents vii

List of Figures ix

List of Tables xii

List of Acronyms xiii

I. Introduction 1

1.1 Motivation 1
1.2 Background 1
1.3 Problem Statement 2
1.4 Assumptions and Resources 2
1.5 Thesis Organization 3

II. Background 5

2.1 Introduction to Orthogonal Frequency Division Multiplexing (OFDM) and Orthogonal Frequency Division Multiple Access (OFDMA) 5
2.1.1 Waveform model 8
2.2 Wireless Open Access Research Platform (WARP) board characterisation 11
2.2.1 Baseband up-sampling and filtering 13
2.2.2 WARP Carrier Frequency Offset (CFO) 13
2.2.3 Timing and synchronisation 14
2.2.4 WARP Channel State Information (CSI) 14
2.3 Signal feature estimation 15
2.3.1 Estimating number of OFDM bursts 15
2.3.2 Estimating CFO 16
2.3.3 Detecting sub-carrier modulation 17
2.4 Interference waveform 22
2.5 Battle damage assessment 23
2.6 Related research. 24

Page

III. Constructing a communication link using WARP 25

3.1 WARP board components 25
3.2 Hardware 26
3.2.1 WARP Field Programmable Gate Array (FPGA) board 26
3.2.2 WARP radio board daughtercard 27
3.3 WARPLab 28
3.4 Communication model 28
3.5 Characterising the communication channel 31

IV. Methodology 43

4.1 Waveform characteristics 43
4.2 System model 43
4.2.1 WARPLab implementation 43
4.3 Signal estimation 44
4.3.1 Estimating OFDMA-Down-Link (DL) features 44
4.3.2 Estimating CFO 45
4.3.3 Detecting sub-carrier (SC) modulation type 46
4.4 Interference techniques 46
4.5 Conducting Communications Battle Damage Assessment (CBDA) 48
4.6 Conducting Jamming Battle Damage Assessment (JBDA) 49

V. Results and Analysis 51

5.1 Estimating OFDMA-DL features 51
5.2 Estimating CFO 53
5.3 Detecting SC modulation 58
5.4 Implementing interference techniques 63
5.4.1 Interference techniques with $N_B = 95$ 71

VI. Summary 76

6.1 Conclusion 76
6.2 Future work 77

Bibliography 78

List of Figures

Figure		Page
2.1	Preamble block diagram	8
2.2	Transmitted OFDM burst block diagram	9
2.3	Transmitted OFDM word block diagram	11
2.4	OFDMA-DL frequency domain structure	11
2.5	Battle Damage Assessment (BDA) functional block diagram	23
3.1	WARP FPGA board version 2.2 [1]	26
3.2	WARP radio board version 1.4 and system architecture block diagram [1]	26
3.3	WARP FPGA board user interfaces [1]	29
3.4	WARPLab Reference Design modules [1]	30
3.5	Quadrature Phase Shift Keying (QPSK) constellation plot, with corresponding histogram plot of real QPSK data, for communication between WARP *Tx* Node 1 radio board RFA to WARP *Rx* Node 2 radio board RFA.	33
3.6	QPSK constellation plot, with corresponding histogram plot of real QPSK data, for communication between WARP *Tx* Node 1 radio board RFD to WARP *Rx* Node 2 radio board RFA.	33
3.7	WARP communication system experimental setup	34
3.8	Effects of varying *Tx* Node Radio Frequency (RF) gain, when transmitting to *Rx* node radio board RFA	35
3.9	Effects of varying *Tx* Node RF gain, when transmitting to *Rx* node radio board RFB	36
3.10	Effects of varying *Tx* Node RF gain, when transmitting to *Rx* node radio board RFC	37
3.11	Effects of varying *Tx* Node RF gain, when transmitting to *ExJx* node radio board RFC	38
3.12	Effects of varying *ExJx* Node RF gain, when transmitting to *Rx* node radio board RFA	39
3.13	Effects of varying *ExJx* Node RF gain, when transmitting to *Rx* node radio board RFB	40
3.14	Effects of varying *ExJx* Node RF gain, when transmitting to *Rx* node radio board RFC	41
4.1	Wireless communication network experimental setup	44

Figure Page

4.2 SISO OFDM receive block diagram [1] 45

4.3 Signal estimation block diagram 45

4.4 Interference signal generation block diagram 47

4.5 CBDA functional block diagram 48

4.6 JBDA functional block diagram 50

5.1 Plot of intercepted Bit Error Rate (BER) using CFO estimation and received user BER using Long Training Sequence (LTS) CSI estimation with $N_G = 16$ 54

5.2 Plot of intercepted BER using CFO estimation and received user BER using LTS CSI estimation with $N_G = 8$ 55

5.3 Plot of intercepted BER using CFO estimation and received user BER using LTS CSI estimation with $N_G = 4$ 56

5.4 Plot of intercepted BER using CFO estimation and received user BER using LTS CSI estimation with $N_G = 2$ 57

5.5 Sub carrier estimation for 95 OFDM bursts using fourth order cumulants 59

5.6 Sub carrier estimation for 95 OFDM bursts using sixth order cumulants 59

5.7 Sub carrier estimation for 75 OFDM bursts using fourth order cumulants 60

5.8 Sub carrier estimation for 75 OFDM bursts using sixth order cumulants 60

5.9 Sub carrier estimation for 50 OFDM bursts using fourth order cumulants 61

5.10 Sub carrier estimation for 50 OFDM bursts using sixth order cumulants 61

5.11 Sub carrier estimation for 25 OFDM bursts using fourth order cumulants 62

5.12 Sub carrier estimation for 25 OFDM bursts using sixth order cumulants 62

5.13 Probabilty of correct SC modulation detection for 95 OFDM bursts using sixth order cumulants during interference techniques 72

5.14 Ability of *ExJx* node to demodulate intercepted OFDMA-DL waveform, with 95 bursts, prior to jamming 73

5.15 Ability of *Rx* node to demodulate transmitted OFDMA-DL waveform, with 95 bursts, without jamming 74

Figure Page

5.16 Ability of *Rx* node to demodulate transmitted OFDMA-DL waveform, with 95 bursts, with jamming 75

List of Tables

Table		Page
2.1	OFDM and OFDMA MATLAB SC assignment	10
2.2	OFDMA-DL SC user assignment	11
2.3	Theoretical cumulant statistics for C_{40}, C_{42} and C_{63} for OFDM modulation types, in a noise free scenario with signals of unit energy [2]	19
2.4	Decision regions for Maximum Likelihood Estimator (MLE) classifier [3]	20
2.5	Binary Phase Shift Keying (BPSK) encoding and normalisation	21
2.6	QPSK encoding and normalisation	21
2.7	Quadrature Amplitude Modulation (QAM)-16 encoding and normalisation	21
2.8	QAM-64 encoding and normalisation	22
3.1	WARP gains, controlled using WARPLab interface group module [1]	31
3.2	WARP Node set up	34
4.1	OFDMA-DL waveform characteristics	44
4.2	CBDA metrics to assess eavesdropping techniques	49
5.1	Probability of correct estimation (P_c) of number of OFDMA-DL bursts (N_B) and Cyclic Prefix (CP) length (N_G) over entire *Tx* node RF gain range	52
5.2	Effects of applying interference techniques to OFDMA-DL waveform with 95 bursts	64
5.3	Effects of applying interference techniques to OFDMA-DL waveform with 75 bursts	66
5.4	Effects of applying interference techniques to OFDMA-DL waveform with 50 bursts	68
5.5	Effects of applying interference techniques to OFDMA-DL waveform with 25 bursts	70

List of Acronyms

Acronym Definition

ADC Analog to Digital Converter

AGC Automatic Gain Control

BDA Battle Damage Assessment

BER Bit Error Rate

BPSK Binary Phase Shift Keying

BW Bandwidth

C2 Command and Control

CBDA Communications Battle Damage Assessment

CFO Carrier Frequency Offset

CP Cyclic Prefix

CSI Channel State Information

DAC Digital to Analog Converter

DFT Discrete Fourier Transform

DL Down-Link

FDM Frequency Division Multiplexing

FDMA Frequency Division Multiple Access

FFT Fast Fourier Transform

FPGA Field Programmable Gate Array

IDFT Inverse Discrete Fourier Transform

IFFT Inverse Fast Fourier Transform

IP Internet Protocol

Acronym Definition

IQ In-phase Quadrature

ICI Inter-Channel Interference

ISI Inter-Symbol Interference

ISM Industrial, Scientific, and Medical

JBDA Jamming Battle Damage Assessment

LED Light Emitting Diode

LSB Least Significant Bit

LTI Linear Time Invariant

LTS Long Training Sequence

MAC Medium Access Control

MIMO Multiple-Input Multiple-Output

MLE Maximum Likelihood Estimator

NIC Network Interface Controller

OFDM Orthogonal Frequency Division Multiplexing

OFDMA Orthogonal Frequency Division Multiple Access

OOD Object Orientated Design

RF Radio Frequency

PAPR Peak to Average Power Ratio

PLL Phase-Locked Loop

PHY Physical

PP-SNR Post-Processing Signal to Noise Ratio

PSK Phase Shift Keying

QAM Quadrature Amplitude Modulation

Acronym Definition

QPSK Quadrature Phase Shift Keying

RSSI Received Signal Strength Indication

SC sub-carrier

SISO Single-Input Single-Output

SNR Signal to Noise Ratio

STS Short Training Sequence

TDD Time Division Duplex

UDP User Datagram Protocol

USB Universal Serial Bus

WARP Wireless Open Access Research Platform

COMMUNICATION AND JAMMING BDA OF OFDMA COMMUNICATION SYSTEMS USING THE SOFTWARE DEFINED RADIO PLATFORM WARP

I. Introduction

This chapter outlines the basis of this research, including motivation, background, goals, assumptions and an outline of the thesis.

1.1 Motivation

The mastery of the RF spectrum is considered a key objective in military operations. Part of this mastery is the ability to intercept combat or intelligence information, as well as denying the adversary's ability to communicate using the RF spectrum. An emerging communication scheme, utilised both in the battlefield and within the civilian sector, is orthogonal frequency division multiplexing (OFDM) and its multiple access scheme orthogonal frequency division multiple access (OFDMA). OFDM is utilised widely within modern communication systems, such as 4G, 802.11a WiFi, 802.16 WiMAX and HDTV [4]. Furthermore, it is being widely used for such applications as communication between ground stations and unmanned vehicles [5]. As such, exploiting such waveforms allows for more complete utilisation of the RF spectrum.

1.2 Background

Research conducted in *Blind demodulation of pass band OFDMA signals and Jamming Battle Damage Assessment utilizing Link Adaptation*, by FLTLT N.A. Rutherford [3], developed methodology to enable estimation of OFDMA waveforms at both passband and baseband. This research demonstrates experimentally that such baseband methodologies can be utilised to both estimate signal features and interfere with a communication system.

The software defined radio platform selected to conduct this research is the Rice University developed WARP, encompassing both hardware, commonly referred to as WARP boards, and online

support [6]. The WARP boards have been developed to operate utilising the 2.4 and 5 GHz Industrial, Scientific, and Medical (ISM) bands [1], and enable signal manipulation at baseband using the reference design, WARPLab.

1.3 Problem Statement

Investigating the effects of interference in communications systems has been the focus of many research institutions, however, most research focuses on the effects in a simulated environment, utilising such programs as MATLAB [7]. Whilst on-site testing of wireless communication testing can be expensive, use of the WARP allows for investigations using a combination of hardware and software. Using the WARP boards in conjunction with the reference design WARPLab allows for a communication systems to be simulated using both the program MATLAB and hardware to emulate the signals with a wireless link. A communication system can be simulated using a number of boards, called a node, with up to four RF daughter cards. Therefore, using three nodes, each with RF daughter cards installed, a transmitter, receiver and interferer/listener can be constructed.

Given the robust nature of OFDM and OFDMA, it is desirable to gain further understanding of the effects of interference, as well as the ability to estimate and classify key features of waveform properties. Using the proposed WARP communications network above, the ability to estimate waveform properties such as number of OFDM bursts and basic composition of the bursts, CFO and detection of SC modulation, as well as the effects of interference shall be investigated. To determine the effectiveness of estimation and interference techniques to the communication system, BDA properties are used. In a military sense, BDA enables a commander to determine whether the application of force has been effective. In this research, BDA determines how effective estimation and interference techniques implemented using an third eavesdropping/interfering (*ExJx*) node, has been at eavesdropping (*Ex*), by using estimation techniques, and interfering (*Jx*), by using interference techniques.

1.4 Assumptions and Resources

A wireless communication network shall be constructed using two WARP v2.2 boards. A third v2.2 board will be used to perform the role of an eavesdropper (*Ex*) and interferer (*Jx*), with the

intent of disrupting communication between the transmitter (Tx) and receiver (Rx), after estimating signal features of the transmitted OFDM word. The three WARP boards will be fitted with four RF daughter cards, allowing for communication on the ISM band. The communication system will be communicating using OFDM and OFDMA waveforms. The communication network shall operate on an available ISM channel.

Whilst the WARP boards operate at pass band, waveform manipulation, investigation and assessment occurs at baseband, which is part of the design feature and utilisation of the WARPLab Reference Design. Waveforms are generated in MATLAB, upconverted to passband by a WARP board configured to transmit. A WARP board configured to receive, downconverts the received passband signal to baseband, after which investigation and assessment can occur. Certain baseband and passband WARP board features will be controlled using WARPLab, including gains and carrier frequency.

Modulation schemes investigated shall be binary phase shift keying (BPSK), quadrature phase shift keying (QPSK), quadrature amplitude modulation (QAM)-16 and QAM-64.

As with many wireless communication networks, a preamble will be used to allow for waveform synchronisation. This preamble is known to all WARP boards.

To ensure accurate timing between the wireless communication network, as well as allowing for rapid configuration of the WARP boards, a computer and 1 gigabit Ethernet switch will be used, with the trigger manager module of WARPLab responsible for all signal timing. Software installed on the computer includes MATLAB, with the reference design WARPLab version 7.4, downloaded from the WARP on-line repository, as well as XiLinx.

1.5 Thesis Organization

The thesis has been organised in six chapters. Chapter II provides the basic concept of OFDM and OFDMA, as well as blind demodulation and previous work in interference techniques. Chapter III presents the methodology for constructing a WARP communication network and characterising the wireless channel. Chapter IV presents the methodology for constructing the interference/listener network and interference models implemented, as well as blind demodulation techniques used. Chapter V provides evaluation results for the interference model implemented and effects on the

wireless communication network. Chapter VI presents the conclusions, summarises the thesis and provides future areas for research.

II. Background

This chapter provides the background for the topics involved in this research. Firstly, OFDM and OFDMA signal properties are discussed, as well as the method used to generate the multi-carrier signals. Next, the hardware platform, WARP boards, shall be discussed, including methods used to estimate the channel and what methods and software are used to ensure generated OFDM waveforms are successfully transmitted and received. Next, the theory behind signal estimation is discussed and what methods used presented, as well as how to implement the estimated data to interfere with a communication system. Lastly, relevant prior research is discussed.

2.1 Introduction to OFDM and OFDMA

OFDM is a multi-carrier modulation scheme, whereby a single data stream is transmitted using a number of lower rate SCs [8], and was presented by R.W. Chang in his application for patent and later paper, discussing the concept of using parallel data transmission and Frequency Division Multiplexing (FDM) [9, 10]. Chang presented the principle of orthogonal multiplexing for transmitting multiple channels simultaneously, which would also eliminate Inter-Channel Interference (ICI) and Inter-Symbol Interference (ISI), whilst occupying a narrower band than conventional FDM. In 1971, Weinstein and Ebert presented how the Fourier transform could be used as a modulator and demodulator to produce FDM waveforms that were orthogonal and removed the requirement for individual sub channel processors [11], giving rise to the use of Fast Fourier Transform (FFT) and digital modulators and demodulators (MODEMs).

OFDMA differs from OFDM as it allows a number of users multiple access to a single burst, by providing each user access to a fraction of the number of SCs [8]. In this way, OFDMA is equal to ordinary Frequency Division Multiple Access (FDMA), yet without large guard bands between users, thereby providing a more efficient use of the RF spectrum. Like OFDM the orthogonal relationship between each of the SCs eliminates ICI and ISI. The idea of OFDMA was proposed as a way to allow more mobiles access to available spectrum by exploiting timing and frequency re-use by way of orthogonal latin squares [12].

In classical FDM, the frequency spectrum is divided into N frequency sub-channels, however in an effort avoid ICI, the sub channels are separated, therefore increasing the amount of Bandwidth (BW) the signal requires [8]. It was proposed by Chang that using the mathematical principal of orthogonality, it would be possible to reduce the amount of BW required by the signal, but also eliminate such effects as ICI and ISI [10].

An OFDM signal allows for multi-carrier transmission, where all the SCs are orthogonal to each other [13, 14]. A key feature of OFDM is that during the modulation process the channel is equally divided into N sub bands, each with a relatively flat frequency response, resulting in a signal which is resistant to multi-path effects (commonly referred to as delay spread effects) [4]. These sub bands, more generally referred to as SCs, can then be used to transmit information.

OFDM is popular given its robustness against frequency selective fading or narrow-band interference [8], which is possible due to the multi-carrier nature of generated signals. Since information is transmitted on individual SCs, of which there are N, only a small percentage are affected by signal fade or an interferer, ensuring the number of errors in data transmission is minimised.

To generate an OFDM signal, information is modulated and resultant symbols formed in the frequency domain one symbol at a time. The size of the frequency domain information is limited by the number of SCs. The frequency information is then modulated using an Inverse Fast Fourier Transform (IFFT), creating N time domain signals. Parallel to serial conversion is then used to produce the resultant OFDM burst [14].

A mathematical expression for OFDM is shown in Equation (2.1) below, where d_m are the complex symbols, N_{SC} is the total number of SCs and T_b is the OFDM burst duration.

$$s(t) = \sum_{m=-\frac{N_{SC}}{2}}^{\frac{N_{SC}}{2}-1} d_{m+\frac{N_{SC}}{2}} \exp\left(j2\pi\frac{m}{T_b}(t-t_s)\right) \tag{2.1}$$

$$t_s \leq t \leq t_s + T_b$$

$$s(t) = 0, t < t_s \wedge t > t_s + T_b$$

Once generated, each SC has exactly an integer number of cycles within the interval T_b. The number of cycles between adjacent SCs differs by exactly one, accounting for orthogonality [8].

Equation (2.1) is a complex baseband expression of an OFDM signal. In this expression, the real and imaginary components correspond to the in-phase and quadrature parts of the signal, which must be multiplied by a cosine and sine of desired carrier frequency (f_c) to produce the final OFDM signal for transmission [8]. Equation (2.2) below expresses the relationship between the complex baseband signal and the transmitted RF signal,

$$s_{RF}(t) = Re\left\{s(t)\exp(j2\pi f_c t)\right\} \tag{2.2}$$

where $Re\{\cdot\}$ represents the real part of the complex variable.

Once the OFDM signal has been received and the p^{th} subcarrier demodulated back to baseband with frequency $\frac{p}{T_b}$, integrating over T_b seconds, assuming perfect Carrier Frequency Offset (CFO) phase correction, the complex symbol represented on the subcarrier can be retrieved, as shown in Expression (2.3) below.

$$\begin{aligned}
&\int_{t_s}^{t_s+T_b} \exp\left(-j2\pi\frac{p}{T_b}(t-t_s)\right) \sum_{m=\frac{-N_{SC}}{2}}^{\frac{N_{SC}}{2}-1} d_{m+\frac{N_{SC}}{2}} \exp\left(j2\pi\frac{m}{T_b}(t-t_s)\right) dt \\
&= \sum_{m=\frac{-N_{SC}}{2}}^{\frac{N_{SC}}{2}-1} d_{m+\frac{N_{SC}}{2}} \int_{t_s}^{t_s+T_b} \exp\left(-j2\pi\frac{m-p}{T_b}(t-t_s)\right) dt \\
&= T_b d_{p+\frac{N_{SC}}{2}}
\end{aligned} \tag{2.3}$$

As shown in Expression (2.3), the complex symbol representation ($d_{p+\frac{N_{SC}}{2}}$) is retrieved, scaled by T_b.

In 1971, Weinstein and Ebert published the use of the Discrete Fourier Transform (DFT) to perform parallel FDM, producing waveforms with orthogonal sub channels and suggesting the use of computers implementing the FFT to perform the role of modulator and demodulator [11]. A key advantage of utilising the FFT as opposed to the DFT is the reduction in computations required from $O(N^2)$ to $O(N \log N)$ [8].

Referring to Equation (2.1), it can be recognised as an Inverse Discrete Fourier Transform (IDFT) of N_{SC} QAM input symbols [8],

$$s(n) = \sum_{b=0}^{N_{SC}-1} d_b \exp\left(j2\pi\frac{bn}{N_{SC}}\right), \tag{2.4}$$

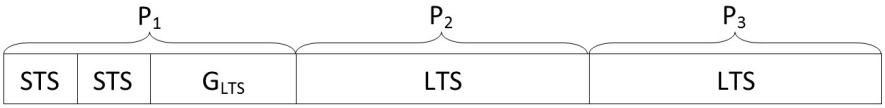

Figure 2.1: Preamble block diagram

where n is the sample of time.

When implementing baseband OFDM waveform generation, zeros are inserted to the middle of the data vector. This ensures the zero data values are mapped to frequencies close to $\pm\frac{1}{2}$ sampling rate and non-zero values are mapped to SCs around zero Hertz. As an OFDM waveform is essentially formed in the frequency domain, an IFFT is performed prior to transmission. Once received, an FFT is performed prior to demodulation of the received signal.

The method above creates a simple OFDM burst. To improve properties of the burst, properties of the SCs can be modified, such as including cyclic redundancy, spectral confinement and synchronization [4, 15]. Cyclic redundancy is achieved by repeating a ratio of the SCs at the beginning of the OFDM burst and is called the CP, used to combat ISI [4, 14]. To achieve spectral confinement, guard bands are used, whereby a number of the SCs are set to null and do not carry any information [15]. Introduction of pilot SCs, so called, as they are set to $[-1, +1]$, can be used for synchronisation and phase correction.

2.1.1 Waveform model.

In this thesis, the OFDM and OFDMA bursts have been created with reference to the IEEE 802.11 WiFi Standard and therefore have $N_{SC} = 64$ SCs [15], equating to a FFT size of 64. Whilst the IEEE 802.11 Standard does not address OFDMA, the same N_{SC} is used, however, the transmitted waveform is intended for multiple users. In this way, the burst is similar to an OFDMA-DL waveform used in such systems as IEEE 802.16 WiMax [16].

As with IEEE 802.11 WiFi Standard, a preamble, or training sequence, is included at the beginning of the transmitted signals. The preamble consists of both a Short Training Sequence

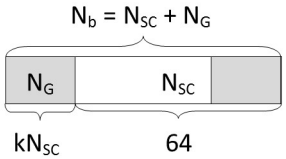

Figure 2.2: Transmitted OFDM burst block diagram

(STS) and LTS. The STS is intended for signal detection only, whilst the LTS is used for signal synchronisation, coarse CFO correction and channel estimation. The STS and LTS sequences used in the preamble are the same as what has been defined in the IEEE 802.11 WiFi standard. However, the structure has been reduced, so only two STS bursts are used, followed by an LTS guard (G_{LTS}) and finally two LTS bursts. The preamble used is illustrated in Figure 2.1 below. Each preamble piece (P_1,P_2,P_3) has a total of 64 SCs. Whilst the two LTS (P_2,P_3) are a total of 64 SCs, P_1 is made up of two STS, each with 16 SCs and the G_{LTS}, which has 32 SCs, totaling 64 SCs for the P_1 element of the preamble.

As shown in Figure 2.1, the total length of the preamble is equal to three OFDM bursts. G_{LTS} is constructed using the last half of the LTS preamble[15]. The two LTS bursts are identical and each span the length of a single OFDM burst, allowing for simpler synchronisation, coarse frequency estimates and channel estimates. It is important to note, however, that due to WARP board timing being controlled by the WARP trigger manager (see Chapter 3), the first OFDM burst is not utilised for any signal demodulation or synchronisation. Preamble burst P_1 is retained to ensure any potential timing delay does not compromise LTS synchronisation or coarse CFO correction.

As discussed in Section 2.1, OFDM and OFDMA waveforms are more robust to channel conditions when such properties as cyclic redundancy are introduced. Shown in Figure 2.2 is the OFDM burst model, where k is the fraction of the FFT size N_{SC}. The CP sizes used in this research are $N_G = [16, 8, 4, 2]$, equating to ratios of $k = [\frac{1}{4}, \frac{1}{8}, \frac{1}{16}, \frac{1}{32}]$ of an OFDM FFT size, respectively. The cyclic redundancy acts as a guard time between each successive OFDM burst, reducing ISI and it is a fractional repetition of the original OFDM signal [8]. The fraction determines the length of the CP used in the guard time. Using a repetition of the signal prevents ICI, as the presence of no

Table 2.1: OFDM and OFDMA MATLAB SC assignment

SC Type	Index	Value	Purpose
DC	1	0	-
Pilot	[8,22,44,58]	1	Phase correction
Guard	[28:38]	0	Spectral confinement
Data	[2:7,9:21,23:27,39:43,45:57,59:64]	*	Information carrier

signal would cause this [8]. As shown in Figure 2.2, N_{SC} is a repetition of the end samples of the OFDM waveform.

With the size of the OFDM burst now defined (N_b), the duration of the signal can be determined as

$$T_b = T_s N_b$$
$$T_b = T_s(N_{SC} + N_G) \tag{2.5}$$

where T_s is the symbol period.

Keeping with the IEEE 802.11 WiFi Standard, the SCs of an OFDM burst are assigned in MATLAB as per Table 2.1, where * indicates the value is determined by data modulation type used.

The buffer size of the WARP boards restricts the total OFDM bursts, with $N_{SC} = 64$, to a maximum of 102 bursts. To ensure the preamble shown in Figure 2.1 can be utilised, gain of the WARP boards is controlled manually. Use of the in-built WARP Automatic Gain Control (AGC) requires a larger preamble to enable AGC settling, as such, the AGC is not used and gain controlled manually. In this research, OFDM word sizes of $N_B = [25, 50, 75, 95]$ are investigated. Whilst up to 99 OFDM bursts could be transmitted in one complete OFDM word, it was found this could not be achieved consistently without error, due to suspected latency from the laptop to the nodes. An example of an OFDM word is shown in Figure 2.3.

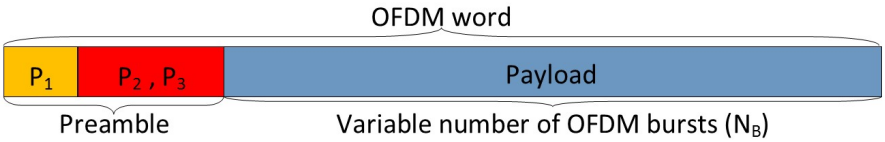

Figure 2.3: Transmitted OFDM word block diagram

Table 2.2: OFDMA-DL SC user assignment

User	*Rx* RF card	Index
1	RFA	[2:7,23:27,53:57]
2	RFB	[9:13,39:43,59:64]
3	RFC	[14:21 45:52]

When the payload of an OFDM word is configured to emulate an OFDMA-DL, the data SCs are assigned as per Table 2.2. The SC assignments were selected to emulate Time Division Duplex (TDD) OFDMA-DL, as described in [16]. The users are assigned to *Rx* RF daughter cards, based on investigations of WARP board channel estimates, described in Section 2.2. Figure 2.4 illustrates the SC assignments for an OFDMA-DL word, once processing has occurred.

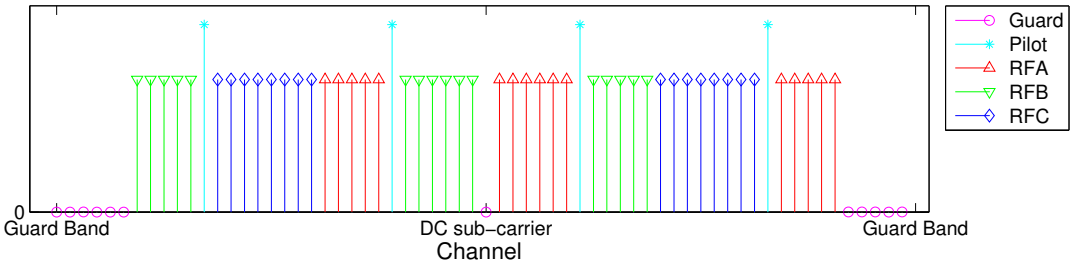

Figure 2.4: OFDMA-DL frequency domain structure

2.2 WARP board characterisation

At the 2006 European Signal Processing Conference in Italy, the design of WARP was presented [6]. Rice University developed the project, known as Wireless Open Access Research

Platform (WARP), encompassing both hardware, commonly referred to as WARP boards, and online support. The WARP boards have been developed to operate utilizing the 2.4 and 5 GHz ISM bands [1], "providing a scalable and configurable platform designed to prototype wireless communication algorithms for educational and research orientated applications" [17]. Whilst they are capable of configuration to IEEE 802.11 Physical (PHY) and Medium Access Control (MAC) standards, it is also possible to implement any form of wireless network design. Since inception, three versions of WARP boards have been developed [1].

The WARP boards were developed by RICE University to enable wireless research [1, 6]. Whilst there are three versions of the WARP board [1], the boards used during this research are Version 2.2. The WARP boards shall be used in conjunction with the WARPLab Reference Design. A full description of the WARP boards, WARPLab Reference Design and method to construct a wireless communications link is detailed in Chapter 3.

Like any wireless communication system, common difficulties encountered when attempting to synchronise and demodulate a signal include

- baseband up-sampling and filtering,
- CFO,
- timing and synchronisation and
- Channel State Information (CSI).

Given waveforms captured using WARP boards will be realistic, it is necessary to define a metric in order to characterise channel quality. Throughout this research, Post-Processing Signal to Noise Ratio (PP-SNR) is the metric used and is defined as the ratio of signal power to signal error, specifically,

$$\text{PP-SNR} = \frac{||x^2||}{||x - \hat{x}||^2} \tag{2.6}$$

where x is the transmitted signal and $\hat{x}$ is the received estimate of x. PP-SNR is similar to Signal to Noise Ratio (SNR), but sources of error affecting PP-SNR include nonlinear distortion in the WARP boards, error in channel estimation, and noise enhancement from equalisation. As a result, PP-SNR is a more hardware-specific description of SNR [18].

2.2.1 Baseband up-sampling and filtering.

To ensure WARP board transmitted OFDM words emulate the IEEE 802.11 Standard it is necessary to up-sample and filter generated bursts. In [15], the framework for which OFDM bursts have been based, up-sampling and filtering of baseband bursts is achieved using square-root raised cosine filters. However, it was found an up-sampling factor of eight was required [19], significantly reducing the capability of transmitting a larger number of bursts. Fortunately, with the release of WARPLab 7.4, a SISO OFDM example was made available to WARP board users [1]. In this example, up-sampling of two is achieved using zero padding, such that $x[nL] = x[n]$, where $L = 2$ [20]. Once the two times interpolation is complete, a half-band interpolation filter is used.

The half-band interpolation filter was designed for the WARP 802.11 Reference Design and has now been made available to all users with the release of WARPLab Reference Design 7.4. This method of up-sampling and baseband filtering is used throughout this research.

2.2.2 WARP CFO.

Local oscillator offsets and Doppler shift are the main source for CFO [20]. In order to successfully demodulate a signal, an accurate CFO estimation is required, which can be performed in either the time or frequency domain using, for example, a specialised training sequence [21]. Failure to successfully estimate CFO introduces such effects as reduction in signal amplitude and introduction of ICI. Since OFDM and OFDMA waveforms implement data carriers which are very close in frequency compared to the BW, only a small variation in frequency offset is tolerable.

Utilising WARP boards for standalone communications over a wireless channel, that is in the absence of a channel emulator or common Phase-Locked Loop (PLL), the frequency of the generated carrier varies with the frequency of the local reference [22]. As such, when using multiple nodes with independent local references, large CFOs are introduced, which must be addressed by physical layer algorithms.

When constructing cooperative communication systems, such as WiFi, beacons [22] or CSI sharing between nodes is employed [23] to combat CFO and hence minimise errors. Regardless of how CFO estimation is addressed, timing synchronisation is non-trivial in standalone communications [22].

Work in [22] demonstrated the importance of CFO estimation and application, noting that if the offset is too large, "the baseband will be forced into the low pass filter stop-band". As a result of [22], methodologies and tips for combating CFO on WARP boards are available at [1], which have been used in this research.

2.2.3 Timing and synchronisation.

OFDM timing and syncronisation using WARP boards is achieved using LTS correlation whereby cross correlator searches for the 64-sample LTS in the preamble [1]. Once both LTS peaks have been identified, timing for the rest of the reception occurs by identifying the index of the payload.

To account for imperfect synchronisation, portion of the CP is used during the synchronisation process, thereby reducing the possibility of ISI [1]. This methodology is contained within the WARPLab SISO OFDM example and has been used in this research.

2.2.4 WARP CSI.

To determine the CSI of the WARP boards, again, the two LTS are used. Channel estimation occurs after coarse CFO estimation, again using the LTS, but prior to phase correction using the pilots.

The channel estimate ($\hat{H}$) is found using Equation (2.7), which assumes any noise has zero mean,

$$\hat{H}_{LTS} = Y_{LTS}.X_{LTS}^{-1} \tag{2.7}$$

where X^{-1} denotes the inverse of the frequency domain defined LTS and Y is the received frequency domain LTS. This method of channel estimation is included in the WARPLab SISO OFDM example.

Equation 2.7 is a zero forcing equaliser and has been retained as the statistics of the channel are not yet understood. As noted in [24], this estimation technique is suitable for such a situation, however, has the disadvantage of introducing a high SNR for frequency selective channels. As denoted in Equation 2.7, the channel estimate is calculated using the frequency domain information of the actual LTS and received, yielding a complex coefficient, which can be effectively applied to each non-zero SC [1].

This method of CSI is used throughout this research.

2.3 Signal feature estimation

Due to the WARP boards operating at baseband, when used in conjunction with WARPLab, the following signal features can be estimated by a listener

- number of OFDMA bursts,
- CFO,
- SC modulation.

The above estimates are achieved using methodology developed in [3].

2.3.1 Estimating number of OFDM bursts.

Given a varying number of OFDM bursts append a preamble, it is necessary for the listener to be able to estimate how many bursts are present (N_B), size of each burst (N_{SC}) and length of the CP (N_G) for highest success of further estimation of signal properties and potential information gathering. To estimate these signal properties, the estimator exploits cyclostationarity due to the CP extension [3].

In [25], it was shown OFDM remains cyclostationary, with a period of T_b, where $T_b = T_{SC} + T_G$, when passed through an Linear Time Invariant (LTI) channel, meaning a received OFDM signal is also cyclostationary. Exploiting the cyclostationarity of a received OFDM waveform allows for estimation of the desired OFDM properties.

To first find the number of OFDM bursts present, repetition due to CP is exploited, using discrete correlation of signals [25]

$$R_y[\tau] = \sum_{i=1}^{D-\tau} y[i]y^*[i+\tau] \tag{2.8}$$

where D is the number of samples. Assuming statistical averaging, the correlation is obtained as [25]

$$R_y[\tau] = \begin{cases} \sigma_s^2 + \sigma_w^2, & \tau = 0 \\ \frac{N_G}{N_{SC}+N_G}\sigma_s^2, & \tau = N_{SC} \\ 0, & \text{otherwise} \end{cases} \tag{2.9}$$

where σ_s^2 and σ_w^2 are signal and noise variances. When $\tau = N_{SC}$, auto-correlation is the signal power of CP. By exploiting this property, the delay of the maximum of the auto-correlation, for correlation delays $\tau > 0$, will yield N_{SC} as [25]

$$\hat{N}_{SC} = \arg\max_{\tau>0}(|R_y[\tau]|) \tag{2.10}$$

The estimator developed in [3] was reduced in complexity by bounding the auto-correlation delays searched to be possible OFDM and OFDMA FFT sizes of $[64, 128, 256, 512, 1024, 2048]$. Given this research uses FFT sizes of $N_{SC} = 64$, this estimator is suitable for use.

Following the estimation of N_{SC}, the CP duration is found by testing for different N_G values[3]. Again, the estimator assumes standard CP orders of $[\frac{1}{4}, \frac{1}{8}, \frac{1}{16}, \frac{1}{32}]$ are employed. By implementing this assumption, this bounds the searching values to $N_G = [\frac{1}{4}\hat{N}_{SC}], \ldots, [\frac{1}{32}\hat{N}_{SC}]$. Given this research implements these standard CP lengths, this estimator is suitable for this implementation.

To estimate N_G, the estimator exploits the fact that maximum correlation will occur only between the CP samples and their copy [3]. Correlation is performed for all possible OFDM bursts for a given CP length. The estimator in [3] is also designed to estimate any delay θ and uses this estimation jointly to estimate N_G. Since the preamble is known to all nodes in this research, this feature of the estimator is not implemented and waveform synchronisation is achieved using LTS correlation. The CP estimator is defined as [25]

$$\hat{N}_G = \arg\max_{N_G,\theta}\left(\left|\sum_{m=0}^{\frac{D}{N_{SC}+N_G}}\sum_{p=1}^{N_G} y[m(\hat{N}_{SC}+N_G)+p+\theta]\cdot y^*[m(\hat{N}_{SC}+N_G)+\hat{N}_{SC}+p+\theta]\right|\right) \tag{2.11}$$

Following the estimation of the symbol parameters, the number of received OFDM bursts, N_B, can be estimated by summing the number of correlated CP instances present in the received burst [3].

2.3.2 Estimating CFO.

As discussed in Section 2.2, the estimation of CFO is essential to ensure received signals can be correctly demodulated. In order to estimate CFO without utilising a known training sequence, a time domain CP estimator was developed in [3], utilising techniques described in [21]. The method exploits that under negligible channel effects, the phase difference between CP and corresponding

original sequence of the OFDM burst, spaced N_{SC} samples apart, caused by CFO, the phase difference (ϵ) is $\frac{2\pi N_{SC}}{N_{SC}} = 2\pi\epsilon$. As such, the CFO can be estimated as the mean phase angles between the product of the CP samples and corresponding original samples, for all OFDM bursts as [21]

$$\hat{\epsilon} = \frac{1}{2\pi}\arg\left(\sum_{n=0}^{N_b}\sum_{m=-N_G}^{-1} y_\epsilon^*[n+m]y_\epsilon[n+m+N_b]\right) \tag{2.12}$$

where y_ϵ is the received baseband signal. Since the *arg()* operator is performed using $\tan^{-1}()$, the range of the normalised CFO estimate is bounded by $\frac{1}{2\pi}\cdot\pm\pi = \pm 0.5$, so that $|\epsilon| < 0.5$ [21].

Whilst $\hat{\epsilon}$ was normalised in [3], the non-normalised estimate $\frac{\hat{\epsilon}}{N_{SC}}$ is used for CFO estimation of the *Ex* waveform. This is to allow for similar channel estimate methods to be utilised with already established WARP methodology.

2.3.3 Detecting sub-carrier modulation.

To detect how the information carried on the data SCs has been modulated, fourth and sixth order cumulants are calculated and a simple MLE is used to classify which data modulation scheme has been used. The development of the fourth and sixth order cumulants is based on work by Swami and Sadler [2] and Shi [26]. It was shown in [2] that regardless of CFO and phase offsets, modulation identification using statistical pattern recognition is possible regardless of a priori knowledge. To compensate for susceptibility to multi-path, techniques from [26] have been adopted to enable blind equalisation and modulation classification [3].

Given the detection of SC modulation is optimal at baseband [2], implementation using WARP boards is possible. To detect SC modulation, first consider a received complex baseband OFDM signal (an extension on Expression (2.3)), with unknown amplitude factor A, residual channel effects ($h(\cdot)$), timing errors (ϵ_T), residual CFO ($f_{\delta c}$), phase jitter (θ_n) and additive noise ($w(p)$),

$$r(p) = Ae^{j2\pi f_{\delta c}T_p + j\theta_p}\cdot\sum_{l=-\infty}^{\infty} x(l)h(pT-(T+\epsilon_T T)+w(p), \tag{2.13}$$

where T is the symbol spacing and $x(l)$ is drawn from one of four constellations (K = {BPSK, QPSK, QAM-16 and QAM-64 }), where $k\{\mu_k \ldots s_k\}$, with s_k representing the number of symbols in the k^{th} signal constellation. It is not assumed each symbol is equiprobable [2].

To determine whether $\{r(p)\}_{p=1}^{N_{SC}}$ has been drawn from one of the K equally likely constellations and given $w(p)$ is, in general, Gaussian (shown in Chapter 5), the MLE classifier exploits that $r(p)$

will have up to eight finite moments, so that sample estimates of fourth and sixth order cumulants have finite variance [2, 26].

Given $r(p)$ is a sequence of samples with a fixed modulation, $r(p)$ is a complex valued stationary process, yielding constant mean and variance over time [2]. Given dependency on conjugation, the second order moment can be defined in two ways

$$C_{20} = E[r^2(p)] \tag{2.14}$$

and

$$C_{21} = E[|r(p)|^2] \tag{2.15}$$

where $E[\cdot]$ is expectation. Similarly, the fourth and sixth order cumulants can be defined as [3, 2, 26]

$$C_{40} = cum(r(p), r(p), r(p), r(p)) \tag{2.16}$$

$$C_{41} = cum(r(p), r(p), r(p), r^*(p)) \tag{2.17}$$

$$C_{42} = cum(r(p), r(p), r^*(p), r^*(p)) \tag{2.18}$$

$$C_{63} = cum(r(p), r(p), r(p), r^*(p), r^*(p), r^*(p)) \tag{2.19}$$

Given the received OFDM burst has no DC offset, $r(p)$ has zero mean, with $cum()$ defined using the joint $cum()$ formula below [3]

$$cum(r_1 \dots r_n) = \sum_{\pi} (|\pi| - 1)!(-1)^{|\pi|-1} \prod_{B \in \pi} E\left[\prod_{i \in B} R_i\right] \tag{2.20}$$

where π runs through all partitions of $\{1, \dots n\}$, B runs through all blocks of the partition π and $|\pi|$ is the number of parts in the partition. For example, the fourth order cumulant is defined as [2]

$$cum(wxyz) = E[wxyz] - E[wx]E[yz] - E[wy]E[xz] - E[wz]E[xy]. \tag{2.21}$$

The above cumulants shown in Equations (2.14) through (2.19) can be estimated from the sample estimates of each moment. Again, accounting for no DC offset and therefore zero mean of $r(p)$, the sample estimates are [2]

$$\hat{C}_{20} = \frac{1}{N} \sum_{n=1}^{N} r^2(p) \tag{2.22}$$

$$\hat{C}_{21} = \frac{1}{N} \sum_{n=1}^{N} r(p) r^*(p) \tag{2.23}$$

Table 2.3: Theoretical cumulant statistics for C_{40}, C_{42} and C_{63} for OFDM modulation types, in a noise free scenario with signals of unit energy [2]

Constellation	$\lvert C_{40}\rvert$	C_{42}	C_{63}
BPSK	2	-2	16
QPSK	1	-1	4
QAM-16	0.68	-0.68	2.08
QAM-64	0.62	-0.62	1.797

where N is the number of samples. This leads to [2]

$$\hat{C}_{40} = \frac{1}{N}\sum_{n=1}^{N} r^4(p) - 3\hat{C}_{20}^2 \tag{2.24}$$

$$\hat{C}_{41} = \frac{1}{N}\sum_{n=1}^{N} r^3(p)r^*(p) - 3\hat{C}_{20}\hat{C}_{21} \tag{2.25}$$

$$\hat{C}_{42} = \frac{1}{N}\sum_{n=1}^{N} |r(p)|^4 - |\hat{C}_{20}|^2 - 2\hat{C}_{21} \tag{2.26}$$

$$\hat{C}_{63} = \frac{1}{N}\sum_{n=1}^{N} r^3(p)r^*(p)^3 - 9\hat{C}_{42}\hat{C}_{21} - 6\hat{C}_{21}^2. \tag{2.27}$$

Given the average power of the signal is the second moment of the signal ($\hat{C}_{21}$), cumulants are typically normalised as [2]:

$$\hat{C}_{4k} = \frac{\hat{C}_{4k}}{\hat{C}_{21}^2}, k = 0, 1, 2 \tag{2.28}$$

and

$$\hat{C}_{63} = \frac{\hat{C}_{63}}{\hat{C}_{21}^3}. \tag{2.29}$$

Using Equations (2.28) and (2.29), the theoretical cumulant statistics C_{40},C_{42} and C_{63} are displayed in Table 2.3 [2]. Given the goal of this research is to determine whether the modulation of data SCs can be identified, it is not necessary to consider cumulants for pilot or guard SCs.

The MLE classifier determines what modulation scheme is implemented by using decision regions set as the mid point between each successive constellation value from Table 2.3, except for between BPSK and QPSK of C_{63}, which is distributed differently [3]. The decision regions for MLE classifier are shown in Table 2.4.

Table 2.4: Decision regions for MLE classifier [3]

$\hat{C}_{42}$	Constellation	$\hat{C}_{63}$
$-\infty < \sigma_{42} \leq -1.5$	BPSK	$\infty > \sigma_{63} \geq 6$
$-1.5 < \sigma_{42} \leq -0.840$	QPSK	$6 > \sigma_{63} \geq 2.75$
$-0.840 < \sigma_{42} \leq -0.6496$	QAM-16	$2.75 > \sigma_{63} \geq 1.9385$
$-0.6496 < \sigma_{42} \leq -\infty$	QAM-64	$1.9385 > \sigma_{63} \geq -\infty$

It was shown in [3], the defined MLE performs well at distinguishing between Phase Shift Keying (PSK) and QAM, however, due to small decision regions, differentiating between QAM modulation types was difficult. It is presumed similar performances shall be observed attempting to classify data SCs on a transmitted OFDMA-DL. In this research, the assumed average power of the modulated SCs is one, therefore normalisation of cumulants is not required. To ensure the average power of each signal is one, information is normalised at the time of data modulation, as per Tables 2.5 through 2.8., where P_N is the scaling factor to ensure power is normalised to one, I_N-out is the normalised I-out representation of each bit and Q_N-out is the normalised Q-out representation of each bit.

Table 2.5: BPSK encoding and normalisation

b_0	I-out	Q-out	P_N	I_N-out	Q_N-out
0	-1	0	1	-1	0
1	1	0	1	1	0

Table 2.6: QPSK encoding and normalisation

b_0	I-out	P_N	I_N-out	b_1	Q-out	P_N	Q_N-out
0	-1	$\frac{1}{\sqrt{2}}$	-0.707	0	-1	$\frac{1}{\sqrt{2}}$	-0.707
1	1	$\frac{1}{\sqrt{2}}$	0.707	0	1	$\frac{1}{\sqrt{2}}$	0.707

Table 2.7: QAM-16 encoding and normalisation

b_0,b_1	I-out	P_N	I_N-out	b_2,b_3	Q-out	P_N	Q_N-out
00	-3	$\frac{1}{\sqrt{10}}$	-0.949	00	-3	$\frac{1}{\sqrt{10}}$	-0.949
01	-1	$\frac{1}{\sqrt{10}}$	-0.316	01	-1	$\frac{1}{\sqrt{10}}$	-0.316
11	1	$\frac{1}{\sqrt{10}}$	0.316	11	1	$\frac{1}{\sqrt{10}}$	0.316
10	3	$\frac{1}{\sqrt{10}}$	0.949	10	3	$\frac{1}{\sqrt{10}}$	0.949

Table 2.8: QAM-64 encoding and normalisation

b_0,b_1,b_2	I-out	P_N	I_N-out	b_3,b_4,b_5	Q-out	P_N	Q_N-out
000	-7	$\frac{1}{\sqrt{42}}$	-1.080	000	-7	$\frac{1}{\sqrt{42}}$	-1.080
001	-5	$\frac{1}{\sqrt{42}}$	-0.772	001	-5	$\frac{1}{\sqrt{42}}$	-0.772
011	-3	$\frac{1}{\sqrt{42}}$	-0.463	011	-3	$\frac{1}{\sqrt{42}}$	-0.463
010	-1	$\frac{1}{\sqrt{42}}$	-0.154	010	-1	$\frac{1}{\sqrt{42}}$	-0.154
110	1	$\frac{1}{\sqrt{42}}$	0.154	110	1	$\frac{1}{\sqrt{42}}$	0.154
111	3	$\frac{1}{\sqrt{42}}$	0.463	011	3	$\frac{1}{\sqrt{42}}$	0.463
101	5	$\frac{1}{\sqrt{42}}$	0.772	101	5	$\frac{1}{\sqrt{42}}$	0.772
100	7	$\frac{1}{\sqrt{42}}$	1.080	100	7	$\frac{1}{\sqrt{42}}$	1.080

2.4 Interference waveform

Once the above signal features have been estimated, the research will attempt to show the effects of constructing an interfering OFDM waveform using the estimated parameters. Given N_B, N_{SC} and N_G will have been estimated, an OFDM waveform with these features can also be constructed. In an attempt to further interfere with the signal, the calculated CFO will be applied to the signal. Regardless of sub carrier modulation, however, the *Jx* signal will be modulated with QAM-64 random data. This modulation scheme has been chosen as it is easily implemented and appear as noise to PSK modulation schemes.

2.5 Battle damage assessment

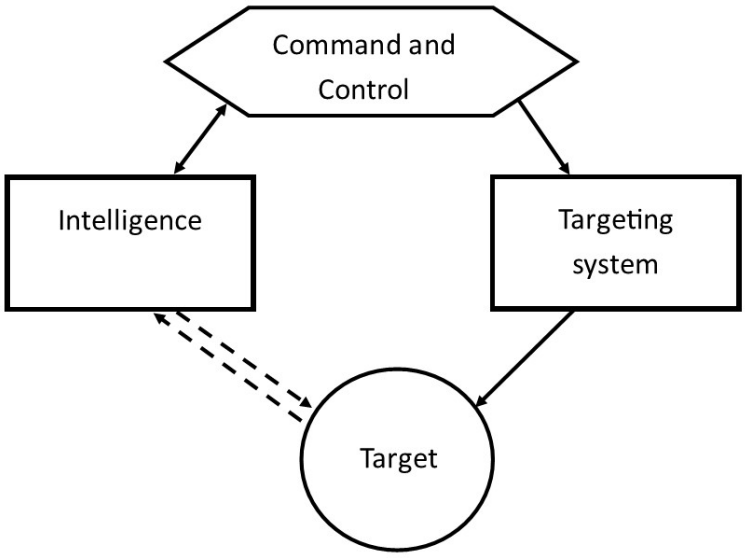

Figure 2.5: BDA functional block diagram

BDA is defined as ”The estimate of damage composed of physical and functional damage assessment, as well as target system assessment, resulting from the application of lethal or nonlethal military force” [27]. Shown in Figure 2.5 is the functional block diagram to conduct BDA, whereby Command and Control (C2) uses intelligence to determine what targeting system should be used to apply military force to a target. Intelligence is used to not only gather information about the target, but also to determine what impact the military force has had on the target.

In this thesis, BDA is applied to a target communication system. The assessment is an estimate of the effectiveness of eavesdropping carried out by an *ExJx* node, as well as an estimate of the effectiveness of the jamming carried out by the same node. Whilst this assessment is not physical, it is a functional damage assessment on a target communication system. The targeting system in this thesis is the *ExJx* node and intelligence is achieved using developed methodologies. Given the purpose of the *ExJx* node, when eavesdropping on the target communication system, is to intercept the communication between the *Tx* and *Rx* nodes, this is measured in terms of CBDA. Specifically how accurately the *Ex* function was able to demodulate the communication with minimal error. The purpose of the *ExJx* node when jamming the *Tx* and *Rx* nodes is to interfere with communications

between the nodes and is measured in terms of JBDA. JBDA assesses how effective the interfering waveform was at reducing the *Rx* node's ability to accurately receive and demodulate the signal with minimal error, when compared to normal operation.

2.6 Related research.

This research utilises research and methodologies developed in [3]. Whilst estimation of OFDM baseband parameters has been widely researched [2, 21, 24, 25, 26], use of such estimations simultaneously for use in an *Ex*, *Jx* environment has not been widely researched. Work in [23] investigates the effect of intercepting CSI between a wireless *Tx* and *Rx* when the two nodes share CSI information. That is, an *Ex* intercepts the *Rx* CSI information when it relays it to the *Tx* node. In this research, however, the *Ex* is attempting to estimate *Tx* CSI in order to interfere with the transmitted signal using a *Jx* emulating the *Tx* CSI. This research also further builds upon CSI interception by attempting to estimate the SC modulation of the intercepted *Tx* signal.

Use of WARP boards as a wireless communications link, however, has been widely implemented [1], with many available support and resources for users. Use of the WARP boards to estimate signal parameters has also been implemented, using such aids as a RF combiner [28].

III. Constructing a communication link using WARP

This chapter details the components of an end-to-end communication link, constructed using WARP boards, including how the components on each board work, how they interface, how MATLAB code is loaded and retrieved from the boards and how the communication channel can be characterised.

3.1 WARP board components

Each WARP board consists of a FPGA and four slots for peripheral daughtercards [1, 17], which can be configured for up to a 4 x 4 Multiple-Input Multiple-Output (MIMO) communication system. Figure 3.1 shows a WARP FPGA board, version 2.2, with the four daughtercard peripherals empty [1].

To enable the WARP boards to perform as a wireless communication link, the daughter cards required are radio boards. Each WARP radio board consists a Digital to Analog Converter (DAC) for transmitted digital In-phase Quadrature (IQ) signals, two Analog to Digital Converter (ADC) for received digital IQ and digital Received Signal Strength Indication (RSSI) respectively, a RF transceiver for transmitted and received analog IQ and received analog RSSI signals, a dual-band power amplifier for transmitted RF, an antenna switch for transmitted and received RF and a port for an antenna [1]. Figure 3.2 shows a WARP radio board (daughtercard) and corresponding system architecture. Inserting four radio boards into the WARP FPGA board enables up to 4 x 4 MIMO wireless communications.

An end to end wireless communication link can be created by using 2 WARP boards, each with minimum of 2 radio daughtercards, inserted in slots 2 and 3 [1]. However, given the scalable nature of the WARP boards, a board with 4 daughter cards can be configured to not only enable up to 4 x 4 MIMO wireless communication, but also Single-Input Single-Output (SISO) wireless communication. Section 3.2 details the hardware for construction of a wireless communication link using WARP boards. Section 3.4 details how 2 version 2.2 WARP boards, each with 4 radio

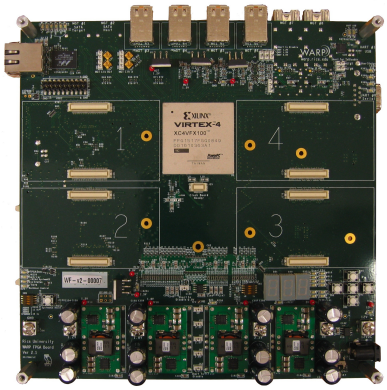

Figure 3.1: WARP FPGA board version 2.2 [1]

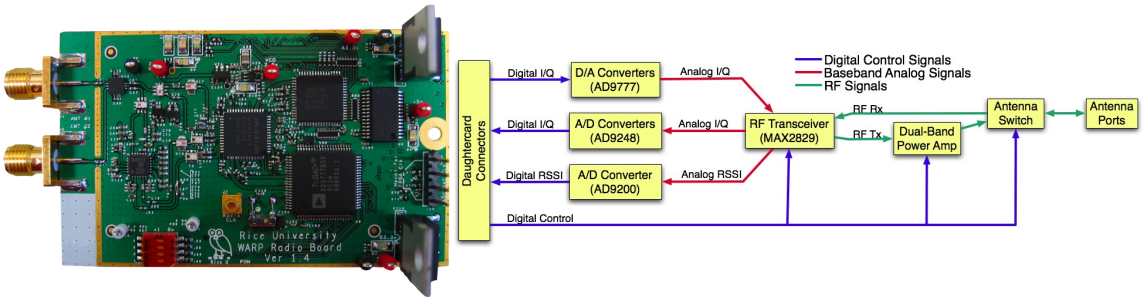

Figure 3.2: WARP radio board version 1.4 and system architecture block diagram [1]

boards, can be configured for MIMO wireless link communication, using MATLAB to load signals of interest onto the board and later, back into MATLAB.

3.2 Hardware

3.2.1 WARP FPGA board.

Power to the WARP boards is provided by an external 12 V power supply. The board enables 5 V to be supplied to each daughtercard slot, from which regulators on the radio board derive the required power supplies for individual components [1]. The FPGA installed on the WARP boards is a Xilinx Virtex-4 11 speed (mid-grade) FPGA [1], requiring an input voltage of 4.4 Volts (V) [29].

Configuration of the FPGA can be achieved using either CompactFlash card or, as recommended on the WARP repository, the on-board Universal Serial Bus (USB) configuration

circuit. The USB circuit emulates a Xilinx Platform USB Cable [1]. The USB port (J52) for the configuration circuit, is located on the same side of the board as the Ethernet port and CompactFlash Slot.

The Ethernet used on the board uses Marvel PHY functionality and TEMAC for the MAC layer [1]. Use of Ethernet allows for good timing between the boards when configured as a wireless communication link.

The daughtercard slots on the WARP board are electrically and mechanically identical, allowing up to 4 radio boards to be connected to the board at any time [1]. Whilst there are other daughtercards available, only the radio boards are considered in this thesis.

3.2.2 WARP radio board daughtercard.

Incorporated onto the Radio Board are three user Light Emitting Diodes (LEDs), which provide a status indication to the user; red, when the PLL is not locked to reference; yellow, when the receiver is enabled; green, when the transmitter is enabled [1].

The RF section of the board uses a Maxim MAX2829 dual-band transceiver [1], which is designed specifically for OFDM 802.11 applications [30]. The dual-band feature allows for operation over both ISM bands and provides up to a 40 MHz bandwidth. The MAX2829 control interfaces are connected to the daughtercard heads, to enable direct control from the FPGA, whilst the IQ interfaces are connected directly to the board's ADC and DAC.

Due to the direct conversion architecture of the radio board, the MAX2829 is sensitive to DC offsets in the transmitted signal [1], with any DC components in the transmit waveform resulting in carrier leakage. Further, the board itself also introduces a small DC offset due to variations in component values and board assembly. As such transmit waveforms should have a zero DC component. To further alleviate DC offsets, the WARP radio board can be calibrated using files available from the WARP repository.

Each Radio board has two standard polarity female SMA jacks, each connected to an RF switch [1], which is driven by the FPGA.

3.3 WARPLab

The reference design which enables rapid PHY prototyping and designs is WARPLab, the most up to date version of which is WARPLab 7.4 [1]. WARPLab uses MATLAB to control nodes and perform signal processing, as well as FPGA programming for time critical processing.

As mentioned in Section 3.2, the easiest way to program the FPGA is using the USB interface. Prior to interfacing with the WARP FPGA board, the Xilinx software program must be installed on the interfacing computer [1]. Tools and instructions required to configure the software as well as program the board is available on the WARP repository. It is important to note that, when using version 2.2 WARP FPGA boards, the intended WARPLab reference design for use in MATLAB must also be loaded on the FPGA. The WARPLab reference design is not backwards compatible, therefore it is essential the same WARPLab reference design used with MATLAB is programmed onto the board.

The WARPLab reference design is intended to provide rapid configuration of multiple WARP FPGA radio boards, collectively referred to as WARP Nodes[1]. Each node can be configured to operate as either a wireless transmitter, receiver or transceiver. Using two version 2.2 WARP nodes and the WARPLab 7.4 reference design, a method for constructing an end-to-end communication link is presented in Section 3.4.

3.4 Communication model

To enable MIMO wireless communication, the equipment required is:

- 2× WARP FPGA version 2.2 boards,
- 4× WARP radio board daughtercards,
- 1Gb Ethernet switch
- A computer installed with MATLAB 2009b or later, Xilinx tool iMPACT, and dedicated Network Interface Controller (NIC) for WARPLab network communications, utilizing the 10.0.0.X subnet.
- WARPLab 7.4 reference design

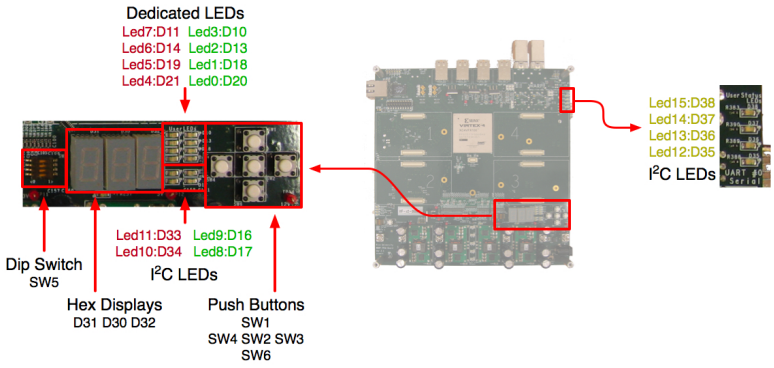

Figure 3.3: WARP FPGA board user interfaces [1]

The Xilinx tool iMPACT allows for downloading of the WARPLab reference design onto the WARP hardware [1]. The reference design is downloaded via a USB cable from the computer to each individual board. Prior to downloading the WARPLab reference design, it is important to note the position of the user dip switch mentioned in Section 3.2.1. If the switch is positioned identically for both WARP boards, the boards will be assigned the same network address, resulting in collisions. WARPLab convention assigns the transmitter node with Internet Protocol (IP) address 10.0.0.001, achieved by positioning the dip switch to all logic lows. The receiver node is conventionally assigned IP address 10.0.0.002, achieved by positioning the dip switch with Least Significant Bit (LSB) to logic high. Figure 3.3 shows the location of the dip switch, and other user interfaces, on the WARP FPGA board [1].

Once the dip switches have been correctly positioned, the boards and user computer must be connected to the Ethernet switch [1]. The boards are now ready to be programmed, individually, with WARPLab 7 reference design, using a standard USB. Once programmed, the board will display its node ID (001 for transmitter node and 002 for receiver node) on the hex display. Whilst the Ethernet link is setting up, the bottom LED will blink with all four LEDs blinking once the node is ready to accept commands from MATLAB.

The WARPLab reference design has modules allowing control of the nodes, MAX2829 radio cards, buffers, User Datagram Protocol (UDP) Ethernet and triggers [1]. This is achieved thanks to

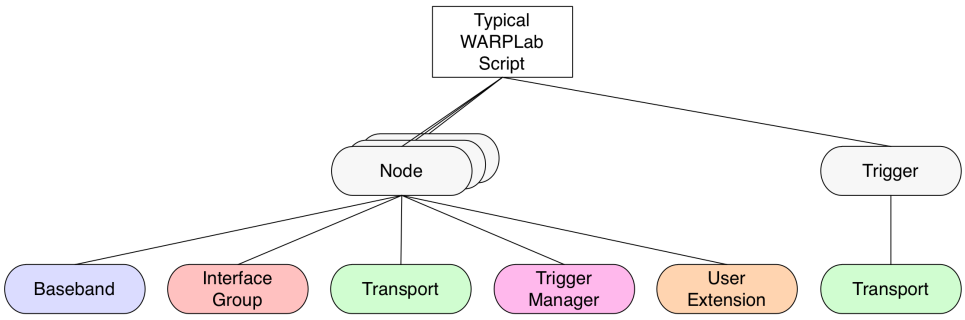

Figure 3.4: WARPLab Reference Design modules [1]

the Object Orientated Design (OOD) nature of MATLAB and the WARPLab 7.4 Reference Design. Figure 3.4 shows the hierarchy of WARPLab Reference Design modules.

The node module of the WARPLab 7.4 reference design is responsible for commands to other modules within the node, as well as collecting responses and delivering them back to the user [1]. It is also responsible for specific set up commands of the node itself.

The baseband module is responsible for the delivery and reception of samples being sent to and from the radio interfaces made available on each node [1]. In this case, MIMO communications on a WARP FPGA board with four radio cards, the baseband module is responsible for sending and receiving samples to all four radio cards. The baseband buffers module allows a user to set the length (up to 2^{14} samples) of the transmission, and subsequent reception, as well as any transmit or receive delay.

The interface group module configures the four radio boards [1]. By using the command string `RF_ALL`, all radio boards can be configured simultaneously. However to allow for customization, each radio board can be called individually. By individually calling each radio card, communications can be established on different channels using different baseband and passband gains. Shown in Table 3.1 are the baseband and passband WARPLab levels and corresponding approximate MAX2829 amplifier gains.

The transport module is responsible for handling messages to and from the WARP hardware with UDP Ethernet traffic [1].

Table 3.1: WARP gains, controlled using WARPLab interface group module [1]

	Tx gains		*Rx* gains	
Baseband	$[0, 1, 2, 3]$	$[-5, -3, -1.5, 0]$dB	$[0 : 31]$	$[0 : 63]$dB
Passband	$[0 : 63]$	$[0 : 31]$dB	$[0, 1, 2]$	$[0, 15, 30]$dB

The trigger manager module is responsible for managing how and individual node action is coordinated with other nodes that are in an experiment [1]. In this case, the trigger module would handle the synchronization of actions between the transmitter node and receiver node. Each node is assigned an ID, which in this case, due to the configuration of the dip switch, `nodes(1)` is the transmitter and `nodes(2)` is the receiver.

With the WARP nodes configured for MIMO communication, using the WARPLab reference design, the wireless communication link is now able to operate. A signal, such as a simple sinusoid, or a more complex OFDM waveform, can now be generated in MATLAB. Once generated, the same signal can be transmitted on each of the four radio boards, on four different channels, configured by using all modules. The receiver node will then receive the transmitted signal, which can then be downloaded back into MATLAB for analysis, by using all modules. The module ultimately responsible for loading the signal onto the transmitter and from the receiver back into MATLAB is the transport module. As such, the wireless communication link transmits a digital representation of signals, generated in MATLAB, which is transported to the transmitter (WARP Node 001) using Ethernet, transmitted over a wireless propagation channel to a receiver (WARP Node 002). Once received, the digital representation of signals is transported from the receiver back into MATLAB using Ethernet.

3.5 Characterising the communication channel

With the release of WARPLab 7.4, included an example of OFDM SISO communication, part of which allows for the characterisation of the channel using an interpolation filter [1]. Furthermore, the modulation scheme of the OFDM waveform could be selected, with scaling to to ensure the average power of the signal is one. Aside from channel estimation, output as part of the example

is tracking of CFO and phase error during the transmission, constellation estimates and statistics of the signal, including number of bytes, BER and OFDM signal errors.

The OFDM SISO example utilised only a single node. As such, the example was modified to enable communication between two nodes, thereby creating a wireless communication link as discussed above. That is, on the *Tx* node, a single radio board was nominated to transmit the signal and on the *Rx* node, a single radio board was nominated to receive the transmitted signal. Utilising the code, it was possible to identify which nodes would be suitable to implement as either *Tx*, *Rx*, *ExJx*. Analysis was initially conducted at a WARPLab defined *Tx* baseband gain of two and RF gain of 32 and *Rx* RF gain of two and baseband gain of twelve. These gain levels have been selected as, it is recommended in [1], lower gain levels should be utilised to minimise non-liner distortion effects arising due to such issues as Peak to Average Power Ratio (PAPR). OFDM burst are subject to high PAPR due to the summation of orthogonal waveforms, potentially resulting in OFDM bursts with high peak power levels [14].

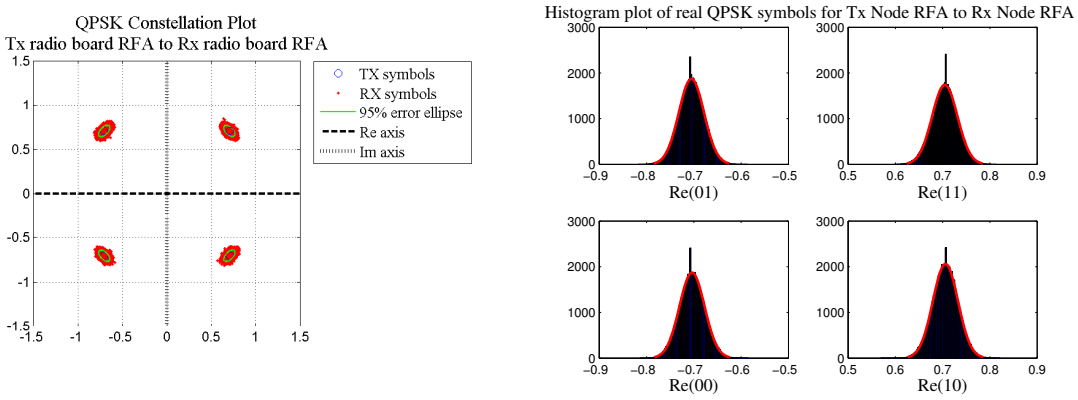

Figure 3.5: QPSK constellation plot, with corresponding histogram plot of real QPSK data, for communication between WARP *Tx* Node 1 radio board RFA to WARP *Rx* Node 2 radio board RFA.

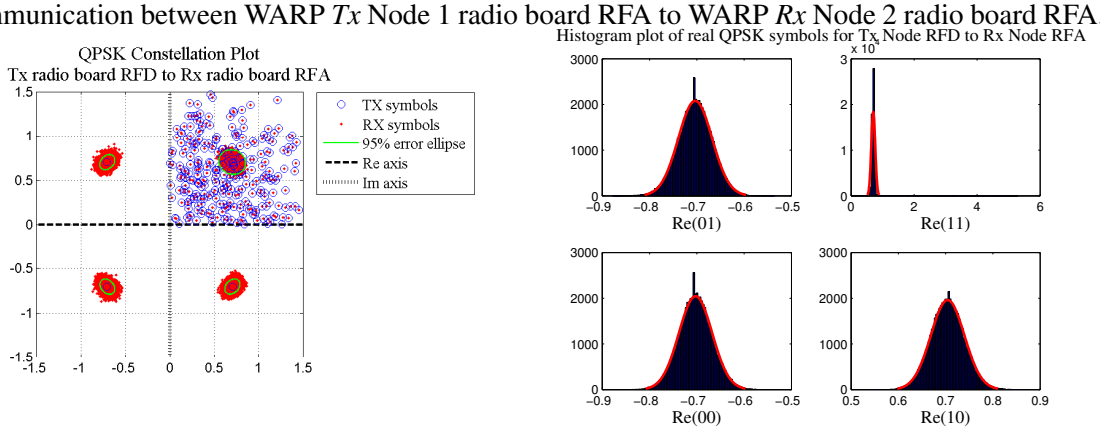

Figure 3.6: QPSK constellation plot, with corresponding histogram plot of real QPSK data, for communication between WARP *Tx* Node 1 radio board RFD to WARP *Rx* Node 2 radio board RFA.

Shown in Figure 3.5 is an example of a good communication link, between the *Tx* node using radio board RFA and *Rx* node also using radio board RFA. Whilst the 95% error ellipse is elongated, showing evidence of phase jitter, the communication link is capable of successfully demodulating the transmitted waveform. However, shown in Figure 3.6 is an example of a poor communications link. Despite using the the same *Tx* and *Rx* nodes used to generate Figure 3.5, errors have been induced by the transmitting node, arising from using a different radio board, RFD. Due to the errors induced by the RFD radio board, which mainly occurred when transmitting symbols corresponding to IQ bits 11, this card was not used. To minimise hardware induced errors during transmission, radio board RFA is selected as the transmitting radio board on the *Tx* node. It is important to note, however, despite the errors induced by the RFD radio board, *Rx* node radio board RFA was still able

Table 3.2: WARP Node set up

Tx Node	*Rx* Node	*ExJx* Node, *Ex*	*ExJx* Node, *Jx*
RFA	RFA, RFB, RFC	RFC	RFA

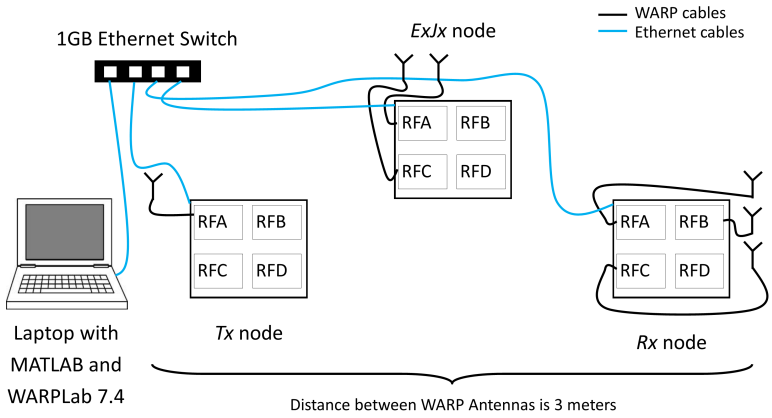

Figure 3.7: WARP communication system experimental setup

to correctly receive the signal. As such, radio board RFA was selected as one of the receiving radio boards on the receiving node.

After completing similar analysis to what is shown in Figures 3.5 and 3.6, the WARP communication system setup shown in Table 3.2 was used throughout this research. The experimental setup is pictured in Figure 3.7

Once WARP nodes were assigned, it was necessary to determine which gains were to be used for signal estimation. The *Rx* gains were fixed, using WARPLab Reference Design, to RF gain of 2 (30 dB) and baseband gain of 12 (30 dB) [1]. Shown in Figures 3.8 - 3.14 are BER vs. PP-SNR plots as a result of varying *Tx* and *Jx* gains.

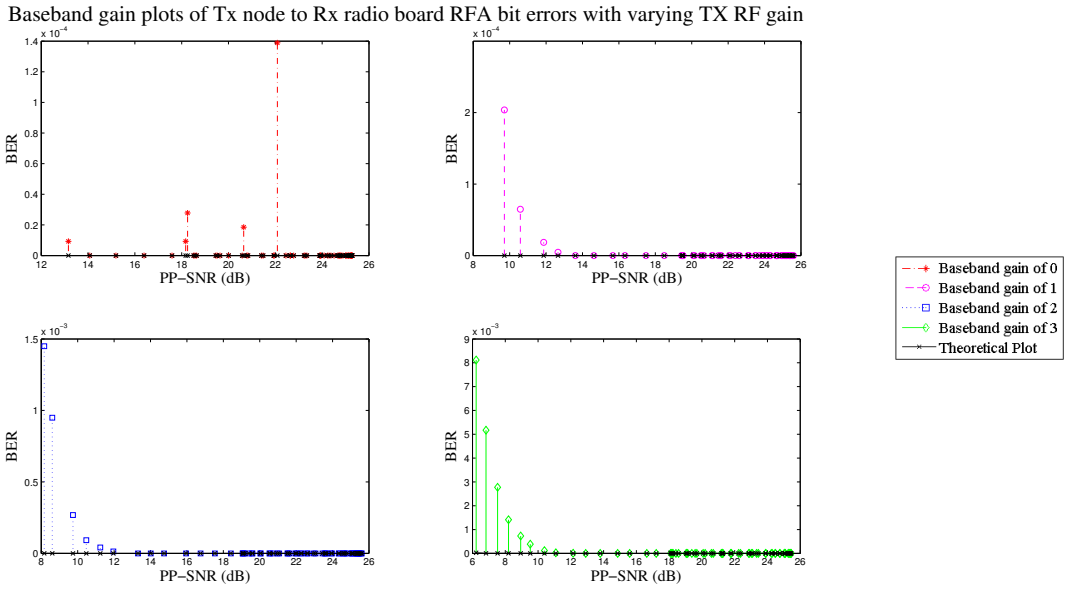

Figure 3.8: Effects of varying *Tx* Node RF gain, when transmitting to *Rx* node radio board RFA

As shown in Figure 3.8, when the WARPLab Reference Design is used to vary the *Tx* node RF gain for all four baseband gain levels, when communicating with *Rx* node radio board RFA, the PP-SNR range achieved at all levels is similar. The baseband power levels have also been set using WARPLab. Differences between responses for the four baseband levels occur when the baseband gain level is set to 0 (corresponding to -5 dB) [1]. With a baseband power level this low, at times spurious non-Gaussian BER responses occur at varying PP-SNR power levels. As a result of this, it would not be suitable to set the baseband gain level to 0 for communications between *Tx* node to *Rx* node radio board RFA.

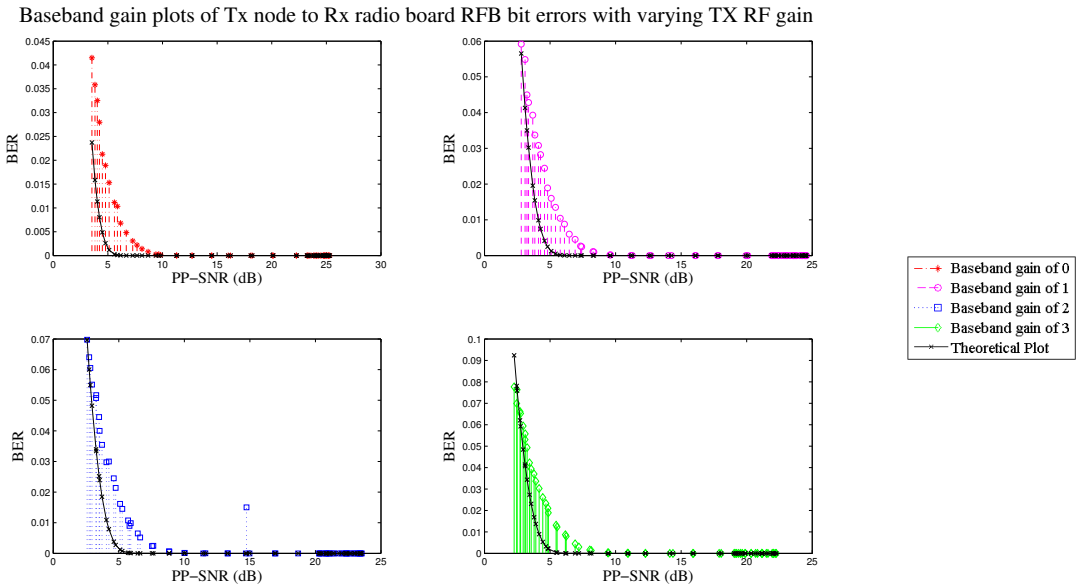

Figure 3.9: Effects of varying *Tx* Node RF gain, when transmitting to *Rx* node radio board RFB

As shown in Figure 3.9, when the WARPLab Reference Design is used to vary the *Tx* node RF gain for all four baseband gain levels, also set using WARPLab, the communication with *Rx* node radio board RFB is more successful when compared to the communication link with *Rx* node radio board RFA. The PP-SNR range achieved at all baseband power levels is similar to each other, yet broader than that achieved between *Tx* node and *Rx* node radio board RFA. This communication link is also able to achieve BER closer to that of the theoretical BER for all baseband gain levels. There is only one single spurious non-Gaussian BER response, which occurs when the baseband gain level is set to 2 (corresponding to -1.5 dB) [1]. These results exhibit the properties of an effective communication link.

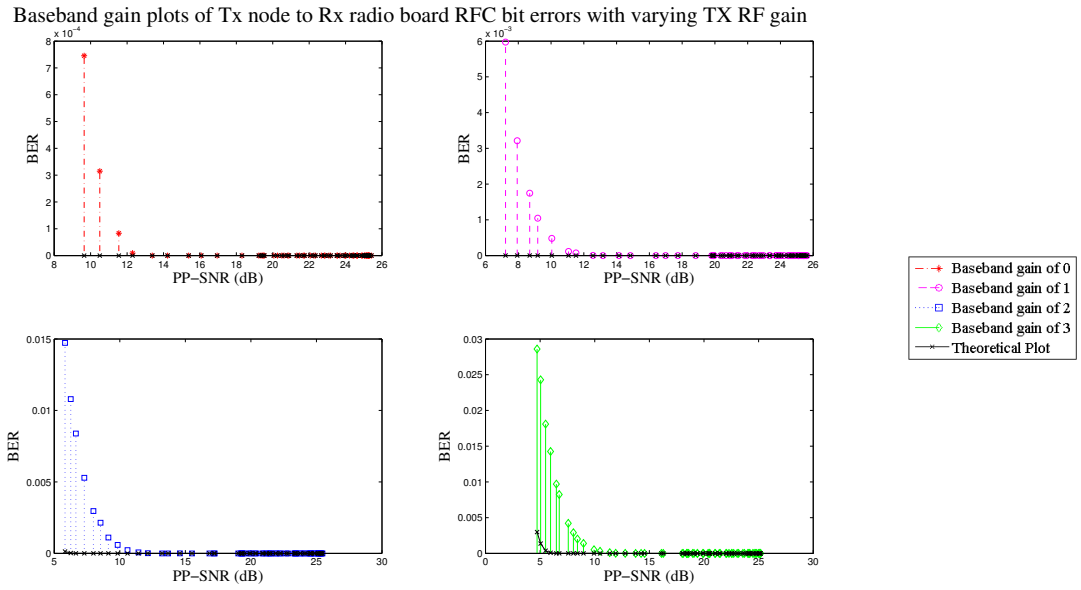

Figure 3.10: Effects of varying *Tx* Node RF gain, when transmitting to *Rx* node radio board RFC

As shown in Figure 3.10, when the WARPLab Reference Design is used to vary the *Tx* node RF gain for all four baseband gain levels, also set using WARPLab, the communication with *Rx* node radio board RFC is capable of achieving a good range of PP-SNR for all baseband gain levels. However, the PP-SNR range for baseband gain levels 2 (corresponding to -1.5 dB) and 3 (corresponding to 0 dB) [1], is broader than that of gain levels 0 (corresponding to -5 dB) and 1 (corresponding to -3 dB). Whilst the BER of baseband gain levels 2 and 3 are poorer than the theoretical BER, the Gaussian response for all baseband gain levels suggests minimal negative hardware influences on the communication channel.

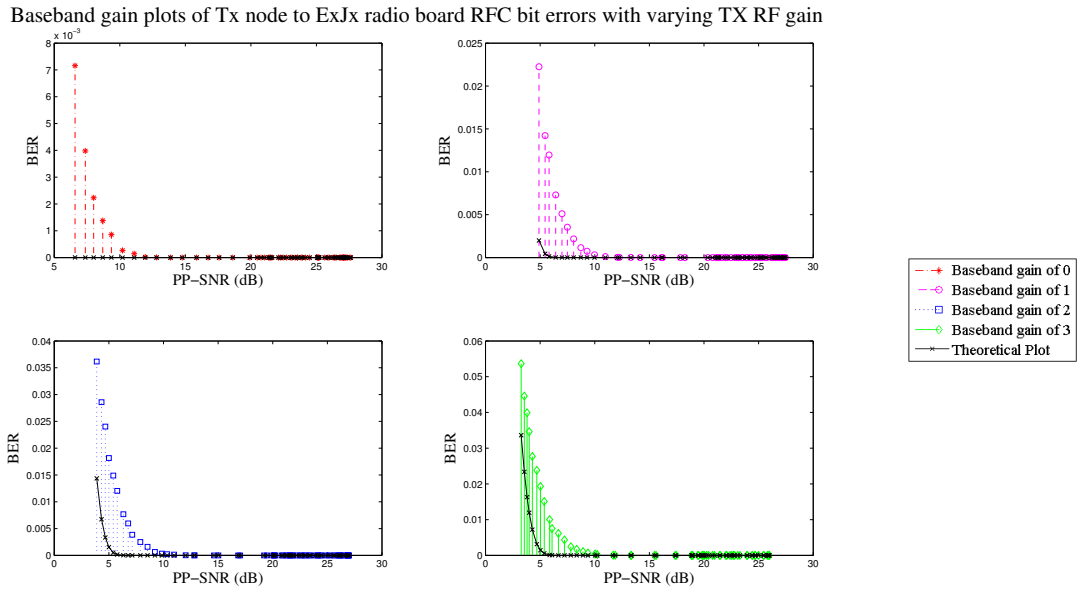

Figure 3.11: Effects of varying *Tx* Node RF gain, when transmitting to *ExJx* node radio board RFC

As shown in Figure 3.11, when the WARPLab Reference Design is used to vary the *Tx* node RF gain for all four baseband gain levels, also set using WARPLab, the communication with *ExJx* node radio board RFC is capable of achieving a good range of PP-SNR for all baseband gain levels. In this configuration the *ExJx* node is using the *Ex* configuration. The purpose of these plots is to determine how effective the application of eavesdropping will be on the communication link. This is important as it will provide an indication on whether CBDA techniques can be utilised. The results displayed in Figure 3.11 indicate eavesdropping may be effective when the *Tx* node is transmitting with a baseband gain level of either 2 (corresponding to -1.5 dB) or 3 (corresponding to 0 dB) [1]. At both of these baseband gain levels, BER performance is acceptable, albeit still poorer than theoretical levels. Given these results, use of CBDA methodology will be effective for determining the ability of *Ex* techniques to extract intelligence from the communication system established between the *Tx* node and *Rx* node.

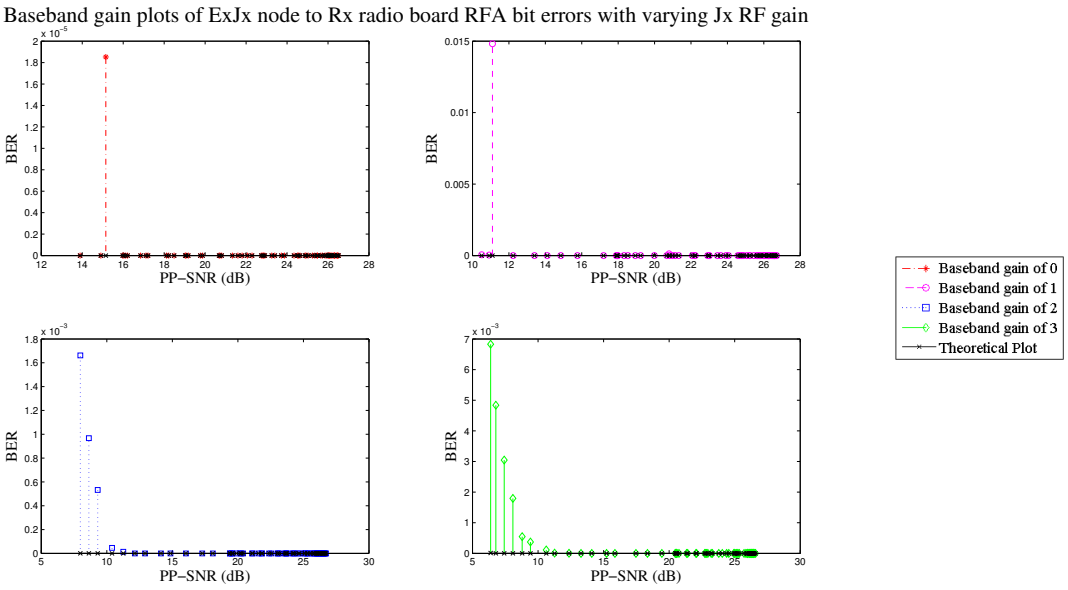

Figure 3.12: Effects of varying *ExJx* Node RF gain, when transmitting to *Rx* node radio board RFA

As shown in Figure 3.12, when the WARPLab Reference Design is used to vary the *ExJx* node RF gain for all four baseband gain levels, also set using WARPLab, the communication with *Rx* node radio board RFA is not consistent for all baseband gain levels, in terms of achieved PP-SNR. That is, the levels achieved vary significantly between the baseband gain levels, however, this is consistent with results displayed in Figure 3.8. Figure 3.8 displays results between the communication link established between the *Tx* node and *Rx* node radio board RFA. Given the similar results displayed in Figure 3.12, the effects are presumably introduced by hardware effects present in *Rx* node radio board RFA. These results are also positive given the *ExJx* node is currently using *Jx* configuration, indicating the application of an interference signal should be able to induce errors into the communication system's ability to effectively receive signals using radio board RFA of the *Rx* node. These results also indicate JBDA methodology shall be appropriate in assessing whether functionality of the communications system has been effected by introduction of an interfering signal.

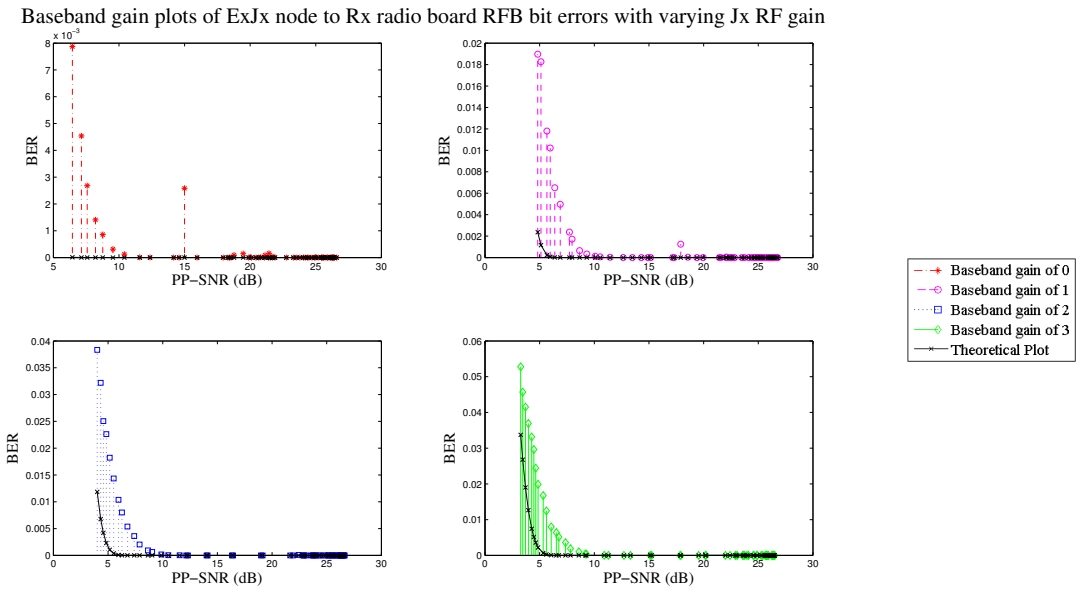

Figure 3.13: Effects of varying *ExJx* Node RF gain, when transmitting to *Rx* node radio board RFB

As shown in Figure 3.13, when the WARPLab Reference Design is used to vary the *ExJx* node RF gain for all four baseband gain levels, also set using WARPLab, the communication with *Rx* node radio board RFB is consistent in terms of achieved PP-SNR. That is, the levels remain relatively consistent between the baseband gain levels. However, unlike results displayed in Figure 3.9, the BER levels are not as consistent for all gain levels. Figure 3.9 displays results between the communication link between the *Tx* node and *Rx* node radio board RFB. Unlike Figure 3.9, Figure 3.13 also shows non-Gaussian responses in baseband power levels 0 (corresponding to -5 dB) and 1 (corresponding to -3 dB) [1]. These results indicate channel effects are being influenced by use of a different source of transmitted waveform, that is the *ExJx* node performing the role of *Jx*. Despite this, the *ExJx* and *Rx* radio board RFB communication link is able to perform effectively at baseband power levels of 2 (corresponding to -1.5 dB) and 3 (corresponding to 0 dB) [1], indicating at either of these baseband gain levels, application of an interference signal should be able to induce errors into the communication system's ability to effectively receive signals using radio board RFB. These results also indicate JBDA methodology shall be appropriate in assessing whether functionality of the communications system has been effected by introduction of an interfering signal.

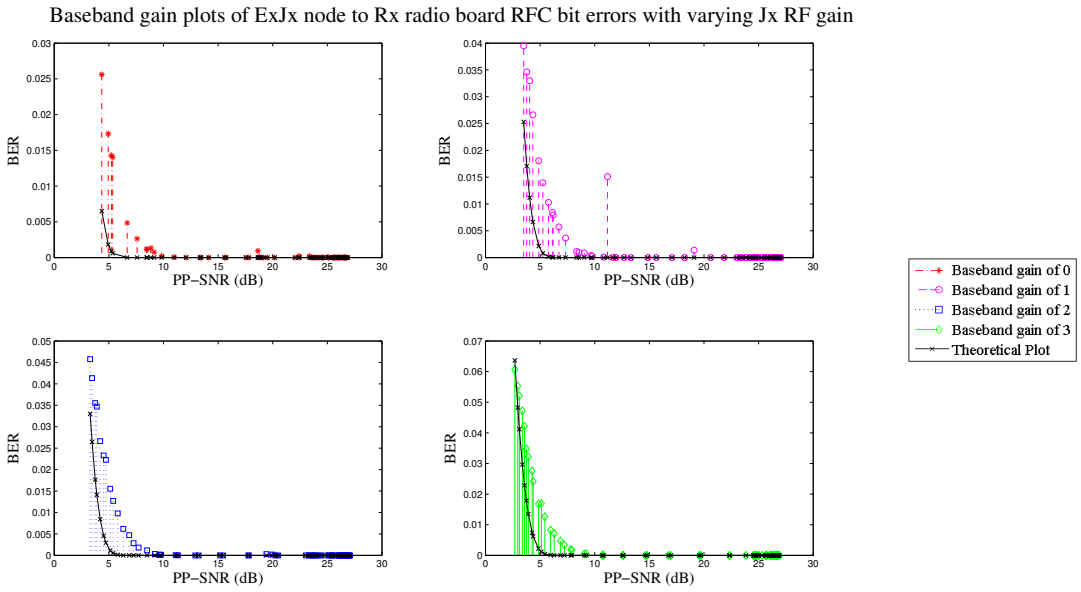

Figure 3.14: Effects of varying *ExJx* Node RF gain, when transmitting to *Rx* node radio board RFC

As shown in Figure 3.14, when the WARPLab Reference Design is used to vary the *ExJx* node RF gain for all four baseband gain levels, also set using WARPLab, the communication with *Rx* node radio board RFC is consistent in terms of achieved PP-SNR. That is, the levels remain relatively consistent between the baseband gain levels. Furthermore, the BER performance displayed in Figure 3.14 indicate a more effective communication link between *ExJx* node and *Rx* node radio board RFC, than between *Tx* node and *Rx* node radio board RFC, displayed in Figure 3.10. In Figure 3.14, the BER displayed for baseband gain levels 2 (corresponding to -1.5 dB) and 3 (corresponding to 0 dB) [1], are close to theoretical and do not display any non-Gaussian effects, such as those seen in baseband gain level 1 (corresponding to -3 dB). These results indicate at either baseband gain level 2 or 3, application of an interference signal should be able to induce errors into the communication system's ability to effectively receive signals using radio board RFC of the *Rx* node. These results also indicate JBDA methodology shall be appropriate in assessing whether functionality of the communications system has been effected by introduction of an interfering signal.

Given the results displayed in Figures 3.8 - 3.14, baseband gain level 2 (corresponding to -1.5 dB) [1], has the least amount of non-Gaussian outliers, whilst also reducing negative OFDM effects such as high PAPR and enabling a greater ranger of PP-SNR. As such, baseband gain level 2 is used throughout this research. With the baseband gain constant, the RF gain level is varied over the entire range to enable analysis of signal estimation techniques.

Whilst the WARP boards can also be used with AGC, this function is not used during this research due to the large preamble required, as discussed in Chapter 2.

IV. Methodology

This chapter describes the methodology to perform signal feature estimation and detection of a wireless communication network, created using WARP boards. Included is the waveform characteristics, system model including how the model is configured, implementation of the signal estimation and evaluation techniques and interference techniques used as a result of signal estimation.

4.1 Waveform characteristics

The OFDMA-DL waveforms are generated as described in Section 2.1.1. The characteristics of the generated waveform are shown in Table 4.1.

4.2 System model

Shown in Figure 4.1, is the experimental setup for the wireless communication network.

The user PC utilises MATLAB to configure the PHY layer of each node, as well as implement *Ex* and *Jx* algorithms. MATLAB is also used to perform post processing analysis of the signals and assess effectiveness of *Ex* and *Jx* techniques using CBDA and JBDA respectively. CBDA methodology is discussed in Section 4.5, whilst JBDA methodology is discussed in Section 4.6

Timing between the different nodes is achieved using the 1Gb Ethernet switch and the trigger manager module in WARPLab. An Ethernet trigger is defined as part of the MATLAB®SISO OFDM script, which is used the synchronise the nodes for transmission and reception.

The ISM channel selected for all experiments conducted is channel 1, equating to a carrier frequency (f_c) of 2.412 GHz.

4.2.1 WARPLab implementation.

As discussed in Section 2.2 the release of WARPLab 7.4 included example file SISO OFDM [1]. Shown in Figure 4.2 is the block diagram for the SISO OFDM example, with the methodology described in Section 2.2. This methodology is retained for signal demodulation of the *Rx* node user cards.

Table 4.1: OFDMA-DL waveform characteristics

Parameter	Symbol	Value	Unit
Bandwidth	BW	20	MHz
Carrier frequency spacing	Δ_F	0.317	MHz
Symbol period	T_s	3.15	μs
STS preamble duration	T_{STS}	20.16	ms
LTS preamble duration	T_{LTS}	40.32	ms

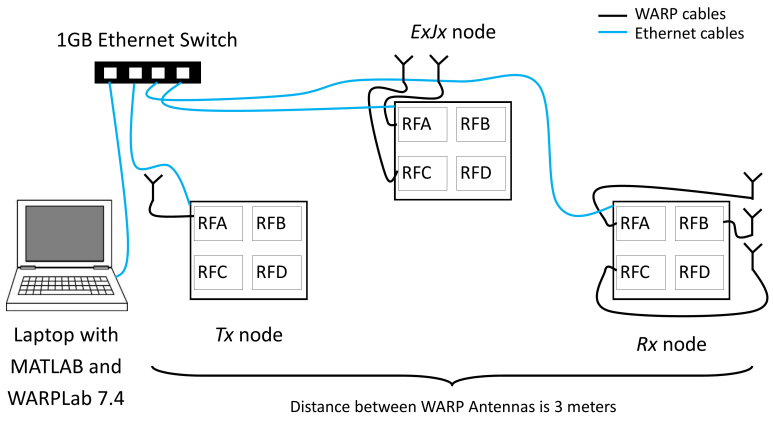

Figure 4.1: Wireless communication network experimental setup

4.3 Signal estimation

To estimate the intercepted OFDM-DL signal features, the block diagram shown in Figure 4.3 illustrates how methods described in Section 2.3 are implemented by the *Ex* daughtercard of the *ExJx* node, where yellow blocks indicate signal features estimated and green blocks indicate retained methods from SISO OFDM.

4.3.1 Estimating OFDMA-DL features.

When estimating the number of OFDM bursts, the estimator exploits cyclostationary properties of CP lengths to determine signal features[3]. To determine the estimator's ability to detect basic features of the OFDM-DL signal, different burst lengths ($N_B = [25, 50, 75, 95]$), with different CP

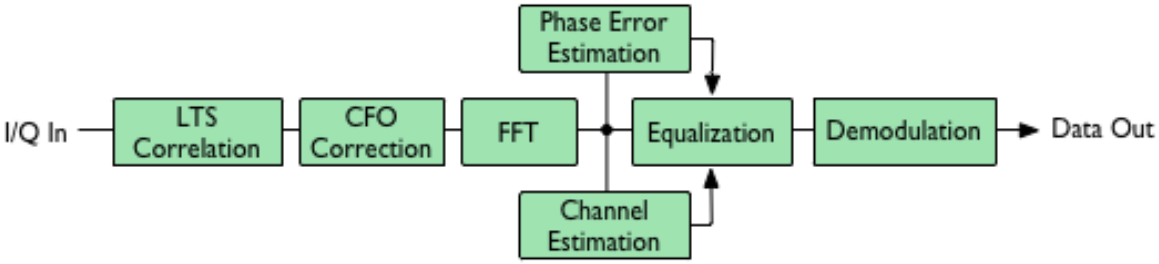

Figure 4.2: SISO OFDM receive block diagram [1]

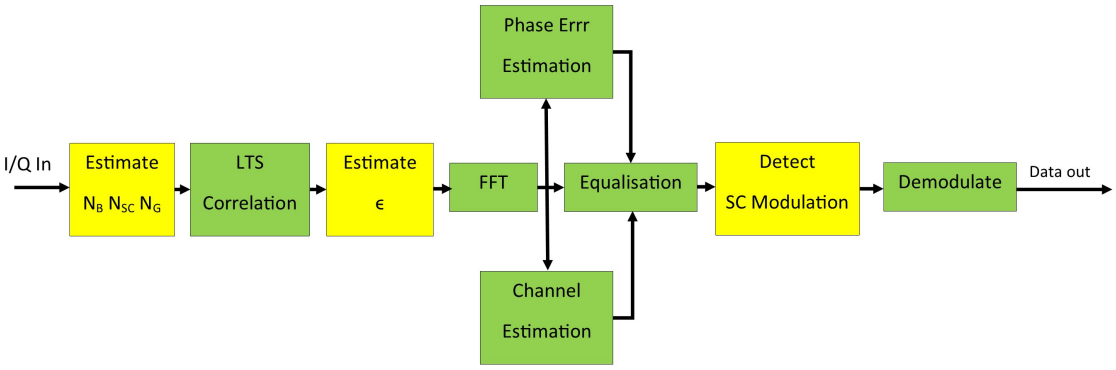

Figure 4.3: Signal estimation block diagram

lengths ($N_G = [16, 8, 4, 2]$) are tested. The number of SCs (N_{SC}) remains constant. This is tested with all waveforms transmitting BPSK modulated data sub carriers for the range of *Tx* RF gain at baseband gain of 2 (corresponding to -1.5 dB) [1]. Estimation was initially only conducted with BPSK modulated data as this is the most robust scheme to channel effects.

4.3.2 Estimating CFO.

The CFO estimator is utilised during LTS correlation. Instead of using the LTS to determine the CFO, the estimator discussed in Section 2.3.2 is used. To test the performance, the CFO is applied to OFDM-DL signals with different burst lengths ($N_B = [25, 50, 75, 95]$) and different CP lengths ($N_G = [16, 8, 4, 2]$). The number of SCs (N_{SC}) remains constant. This is tested with all waveforms transmitting BPSK modulated data sub carriers for the range of *Tx* RF gain at baseband

gain of 2. Again, estimation was initially only conducted with BPSK modulated data as this is the most robust scheme to channel effects.

4.3.3 Detecting SC modulation type.

The SC modulation is detected once equalisation has occurred. Due to use of a zero forcing estimator to estimate the channel during LTS correlation, it was not possible to detect guard SCs. Pilot detection was also not implemented as per assumptions. To determine how effective the detector is, a truth vector from the generated OFDMA-DL waveform is used to obtain the probability of correct detection. Both use of the fourth and sixth order cumulants are compared. Detection of SC modulation type is carried out on OFDM-DL signals with different burst lengths ($N_B = [25, 50, 75, 95]$). The number of SCs (N_{SC}) remains constant. This is tested with all modulation types (BPSK, QPSK, QAM-16, QAM-64), applied to data SCs, with CP length of $N_G = 16$, for the range of *Tx* RF gain at baseband gain of 2.

4.4 Interference techniques

In an attempt to interfere with the OFDMA-DL waveform, the *Ex* estimates and detects signal features, as described above. Once signal features have been estimated and detected, the *Jx* transmits an interfering signal. The signal, regardless of SC detection has been modulated with QAM-64 random data. This has been selected as QAM-64 modulated data resembles noise when compared to such modulation types as BPSK and QPSK, both of which are more robust to channel and interference effects than QAM types [20]. By performing SC detection whilst interfering with the communication system, the *ExJx* node is able to determine whether the communication system has been forced to reduce the modulation order of OFDMA-DL waveforms in order to account for a large amount of interference in the wireless channel, known as link adaptation [3, 31].

Figure 4.4 illustrates how the interference signal is constructed. Yellow blocks indicate information attained from the eavesdropper is what has been used to construct the interfering OFDM-DL waveform. Specifically, the length of the CP, the total number of SCs or FFT size and CFO phase distortion. The addition of phase distortion is applied to each SC in the constructed

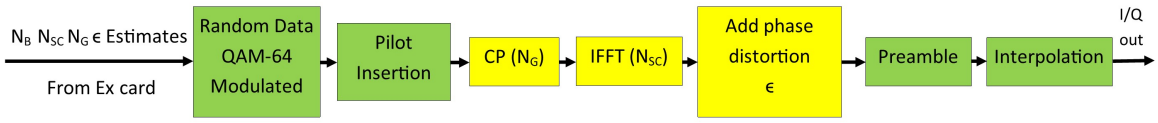

Figure 4.4: Interference signal generation block diagram

Jx OFDMA-DL waveform, with intention to increase the amount of phase distortion experienced by the transmitted waveform.

The constructed interference signal shall be implemented against a varying number of OFDMA-DL, with differing CP lengths. Constructed waveforms transmitted by the *Tx* node were modulated randomly with either BPSK, QPSK, QAM-16 or QAM-64 data. Figure 4.4 illustrates how the interference signal is generated

Due to time constraints, the interference experiment shall initially be applied to a single *Tx* RF gain of 10 (corresponding to approximately 5 dB) [1] and baseband gain of 2 for all burst sizes ($N_B = [25, 50, 75, 95]$). After initial experimentation, WARPLab Reference Design RF power gains from [0 : 5 : 60] shall be applied to OFDMA-DL burst sizes of $N_B = 95$.

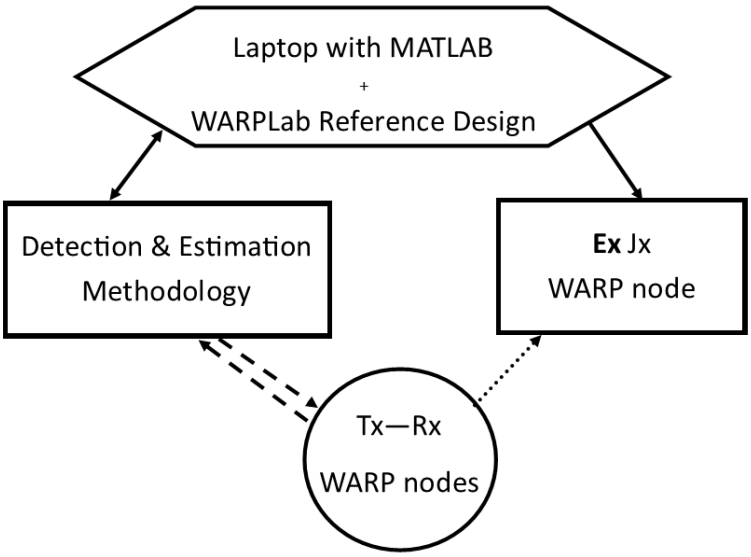

Figure 4.5: CBDA functional block diagram

4.5 Conducting CBDA

Shown in Figure 4.5 is the block diagram representing how CBDA shall be conducted in order to evaluate the ability to perform *Ex* techniques using radio board RFC of the *ExJx* node. Referring to Figure 2.5, which depicts BDA, the role of C2 is performed by the Laptop and WARPLab Reference Design, commanding and controlling the nodes of the communication system. Intelligence is gathered using detection and estimation methodologies described in Sections 4.3.1 - 4.3.3, with assessment conducted by the Laptop with MATLAB. The targeting system is the *ExJx* node intercepting communications between the *Tx* and *Rx* nodes using radio board RFC. Eavesdropping techniques are evaluated based on the probability of correct estimation, or detection, of the intercepted OFDMA-DL waveform transmitted by the *Tx* node, as well as the ability to correctly demodulate the intercepted waveform. Shown in Table 4.2 are the performance metrics used to conduct CBDA, as well as the purpose of the gathered intelligence in relation to *Ex* and *Jx*.

Table 4.2: CBDA metrics to assess eavesdropping techniques

Feature Estimated/Detected	Performance metric	Function
OFDMA-DL Bursts (N_B)	P_c	Enable Ex and Jx
OFDMA-DL SCs (N_{SC})	P_c	Enable Ex and Jx
Size of CP (N_G)	P_c	Enable Ex and Jx
CFO (ϵ)	BER	Enable Ex and Jx
SC Modulation	P_c	Enable Ex

When assessing the ability to estimate OFDMA-DL features, a total of 800 trials is completed at each *Tx* RF gain level, when the baseband gain level is set to 2 (corresponding to -1.5 dB) [1], for each $N_B = [25, 50, 75, 95]$. Results are presented as a probability of correct estimation.

When assessing the ability to estimate CFO, a total of 800 trials is completed at each *Tx* RF gain level, when the baseband gain level is set to 2, for each $N_B = [25, 50, 75, 95]$. Results are presented as the ability of the *ExJx* node radio board RFC to correctly demodulate the intercepted signal.

When assessing the ability to detect SC modulation, a total of 200 trials is completed for each modulation type used at each *Tx* RF gain level, when the baseband gain level is set to 2, for each $N_B = [25, 50, 75, 95]$. Results are presented as the probability of the *ExJx* node radio board RFC to correctly detect the modulation type on each of the data SCs of the intercepted signal.

Once all methods have been assessed and each of the methodologies are used in conjunction with interference techniques CBDA is performed by determining the BER for intercepted waveforms.

4.6 Conducting JBDA

Shown in Figure 4.6 is the block diagram representing how JBDA shall be conducted in order to evaluate the ability to perform *Jx* techniques using radio board RFA of the *ExJx* node. Referring to Figure 2.5, which depicts BDA, the role of C2 is also performed by the Laptop and WARPLab Reference Design, commanding and controlling the nodes of the communication system. Again,

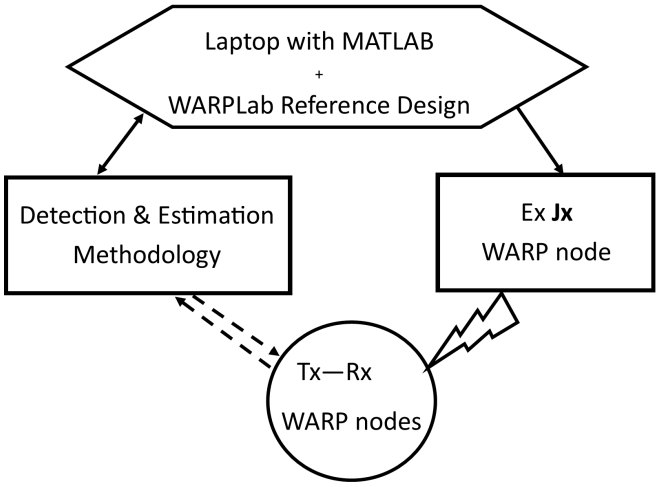

Figure 4.6: JBDA functional block diagram

intelligence is gathered using detection and estimation methodologies described in Sections 4.3.1 - 4.3.3, with assessment conducted by the Laptop with MATLAB. The targeting system is the *ExJx* node interfering with communications between the *Tx* and *Rx* nodes using radio board RFA. Jamming techniques are evaluated based on the BER of the OFDMA-DL waveform transmitted by the *Tx* node. By using link adaptation provided by the *Ex* function detecting changes in SC modulation, the *ExJx* node is able to determine whether the communication system has reduced modulation order to account for interference techniques applied.

V. Results and Analysis

This chapter evaluates the overall performance of the *Ex* signal estimation and *Jx* signal interference techniques.

5.1 Estimating OFDMA-DL features

As discussed in Section 4.3.1, the ability of the *Ex* to estimate basic signal parameters was evaluated with different number of OFDMA-DL bursts (N_B), changes in CP length (N_G), whilst the FFT (N_{SC}) size and modulation scheme (BPSK) remained the same. Shown in Table 5.1 is the probability of correct detection (P_c) for each of the assessed OFDMA-DL word sizes (N_B). It is important to note the estimator was able to correctly identify the FFT size (N_{SC}) regardless of number of OFDM bursts (N_B) or size of CP (N_G), for each trial, throughout the range of *Tx* RF gain. As a result, the probability for correct detection (P_c) is 1 regardless of any variables within the OFDMA-DL waveform and has not been included in Table 5.1 to enable ease of displaying variation of results due to changes in CP length (N_G).

As shown in Table 5.1 errors occur in the ability to correctly estimate the number of bursts (N_B) as the CP length decreased. This result is significant as simulation results in [3] indicated the estimator would be able to correctly identify both N_B and N_G with a probability of one for all SNR levels above -2 dB, for burst sizes ranging from 25 OFDMA bursts to 250 OFDMA bursts. Recalling Figure 3.11 from Chapter 3, Section 3.5, which shows PP-SNR is not recorded below 5 dB between the *Tx* node and *ExJx* node radio board RFC, it was presumed estimation could be achieved regardless of N_B or N_G. Acknowledging that PP-SNR is different to SNR, it was still presumed unlikely the reduced performance would be observed over the entire *Tx* node gain range of PP-SNR 3.9dB to 27.0dB. It is presumed the decrease in estimator performance is a result of multi-path effects.

Table 5.1 has been generated using methodology described in Section 4.3.1 and CBDA techniques described in Section 4.5.

Table 5.1: Probability of correct estimation (P_c) of number of OFDMA-DL bursts (N_B) and CP length (N_G) over entire *Tx* node RF gain range

	$N_B = 95$		$N_B = 75$		$N_B = 50$		$N_B = 25$	
	P_cN_B	P_cN_G	P_cN_B	P_cN_G	P_cN_B	P_cN_G	P_cN_B	P_cN_G
$N_G = 16$	1	1	1	1	1	1	1	1
$N_G = 8$	1	1	1	1	1	1	1	1
$N_G = 4$	1	1	1	1	1	1	0.998	0.986
$N_G = 2$	0.997	0.982	0.994	0.967	0.966	0.809	0.871	0.180

The ability to correctly identify both the number of OFDMA-DL bursts (N_B) and length of CP (N_G) was reduced significantly when N_G was reduced, as shown in Table 5.1. This is due to the estimator incorrectly identifying cyclostationary properties for assumed CP ratios. Given the estimator attempts to identify the number of OFDMA-DL bursts (N_B) after identifying the CP length, errors occur when the estimator incorrectly estimates N_G as being larger than actually present. This is due to the structure of a single OFDMA-DL burst, which is defined as $N_b = N_{SC} + N_G$ (see Section 2.1.1). As such, with an incorrectly estimated CP size, N_G, the size of a single OFDMA-DL burst, N_b is incorrect, leading to an incorrectly identified total number of bursts (N_B) for the intercepted waveform. The variation in P_c for N_B and N_G is present as these estimates are independent, in that N_G is initially estimated and N_B determined by summation of correlation peaks.

Furthermore, the estimator performance was poorest with the smallest OFDMA-DL word size with $N_B = 25$, however, larger CP lengths (N_G) ensured the *ExJx* node could still accurately estimate the signal features, with performance reduced with smaller N_G.

5.2 Estimating CFO

To determine whether CFO estimates were accurate, CBDA techniques discussed in Section 4.5 were used, specifically a functional assessment of the ability to correctly intercept the transmitted OFDMA-DL bursts using estimated CFO compared to actual communication system ability to receive the transmitted OFDMA-DL waveform. Figures 5.1 to 5.4 display the actual user BER as a result of each user demodulating the received waveform using LTS CSI estimates and the user BER as a result of the eavesdropper demodulating the intercepted waveform using estimated CFO. The actual user message is transmitted on the same OFDMA-DL burst, from the *Tx* node to the *Rx* node and a corresponding radio board; user 1 receives waveforms on radio board RFA; user 2 receives waveforms on radio board RFB; user 3 receives waveforms on radio board RFC.

Figures 5.1 through 5.4 have been generated to compare performance for PP-SNR below 10 dB, as errors above this level are minimal or zero and therefore do not provide an indication of CFO estimation accuracy at lower levels. As discussed in Section 2.2, PP-SNR is a hardware specific performance metric. As such, for the communication link between *Tx* node and *Rx* node radio boards RFA (User 1) and RFC (User 3), PP-SNR below 10 dB was minimal and BERs were also very low due to the good link.

Figures 5.1 through 5.4 all show evidence of non-Gaussian BER responses for both intercepted and received OFDMA-DL waveforms. As discussed in Section 3.5, all communication links exhibit occasional non-Gaussian outliers. Performing analysis with a fixed *Tx* node baseband gain of 2 (-1.5 dB) has been conducted to reduce such events, however, these events still occur and exist in all results shown in Figures 5.1 through 5.4 below. Furthermore, the BER of the intercepted waveform compared to the received waveform, for each user, is poorer, however, both the *ExJx* and *Rx* nodes suffer poor BERs when there are less (25) OFDMA-DL bursts in the transmitted waveform.

To generate Figures 5.1 through 5.4, the only estimation technique used by the *ExJx* node, radio board RFA, was CFO phase estimation.

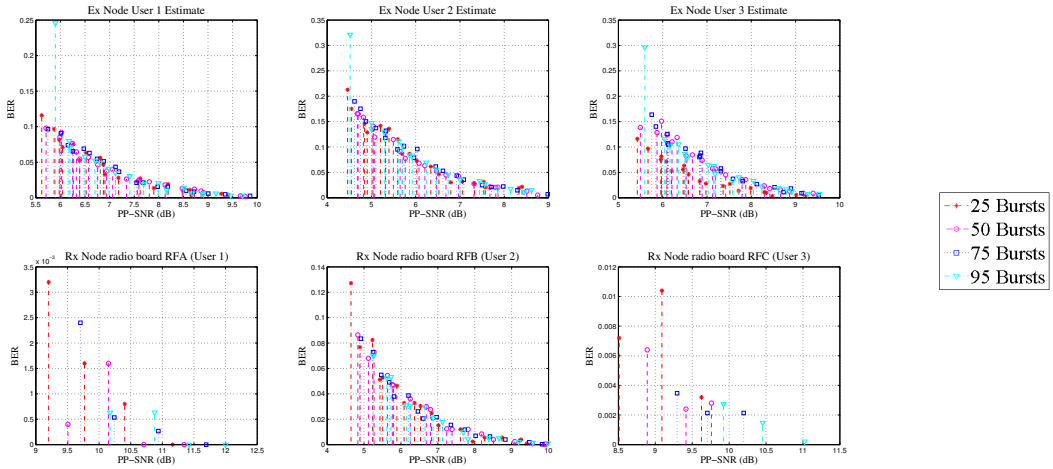

Figure 5.1: Plot of intercepted BER using CFO estimation and received user BER using LTS CSI estimation with $N_G = 16$

Figure 5.1 shows the CBDA of estimating CFO using methods described in Section 2.3.2, for OFDMA-DL bursts of $N_B = [25, 50, 75, 95]$ with a CP length of 16. As discussed in Section 4.5, to assess the ability of the *ExJx* node to successfully intercept the transmitted waveform, the intercepted BER for each user is compared to that of the actual user. The reduced BER is consistent for all OFDMA-DL bursts, albeit with poorer performances when compared to User 1 and User 3. However, the performance of the CFO estimate when compared to User 2 is similar. Whilst the CFO estimate indicates a poorer performance below PP-SNR of 10 dB, given this is a hardware specific metric, what is important is the ability to achieve BERs of 0 for all users above 10dB, which was achieved. Use of the estimated CFO to demodulate the intercepted waveform from *ExJx* node radio board RFC, is viable with $N_G = 16$, albeit with risk of poor performance at lower PP-SNR.

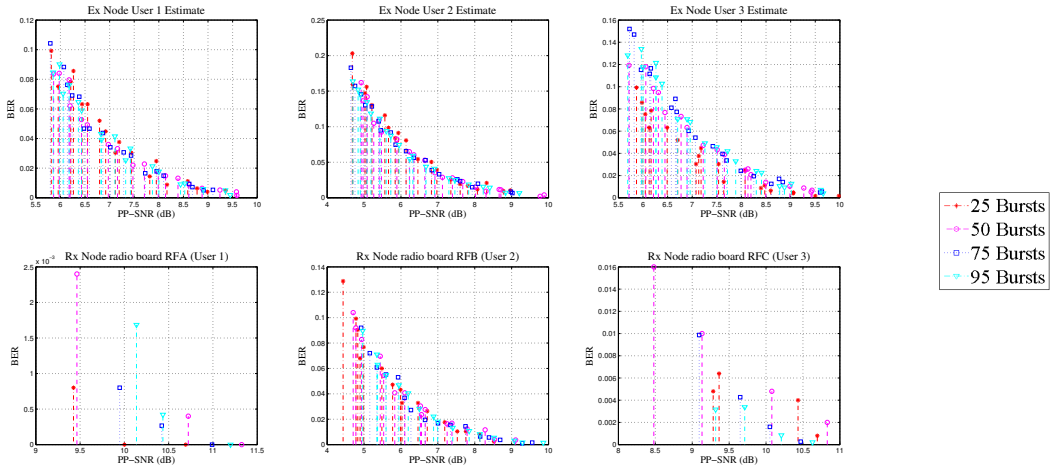

Figure 5.2: Plot of intercepted BER using CFO estimation and received user BER using LTS CSI estimation with $N_G = 8$

Figure 5.2 shows the CBDA of estimating CFO, for OFDMA-DL bursts of $N_B = [25, 50, 75, 95]$ with a CP length of 8. Again, the performance of the CFO estimate when compared to User 2 is similar, yet poorer than that of User 1 and User 3. Importantly, the ability to achieve BERs of 0 for all users above 10dB, which was achieved. Use of the estimated CFO to demodulate the intercepted waveform from *ExJx* node radio board RFC, is viable with $N_G = 8$, albeit with risk of poor performance at lower PP-SNR.

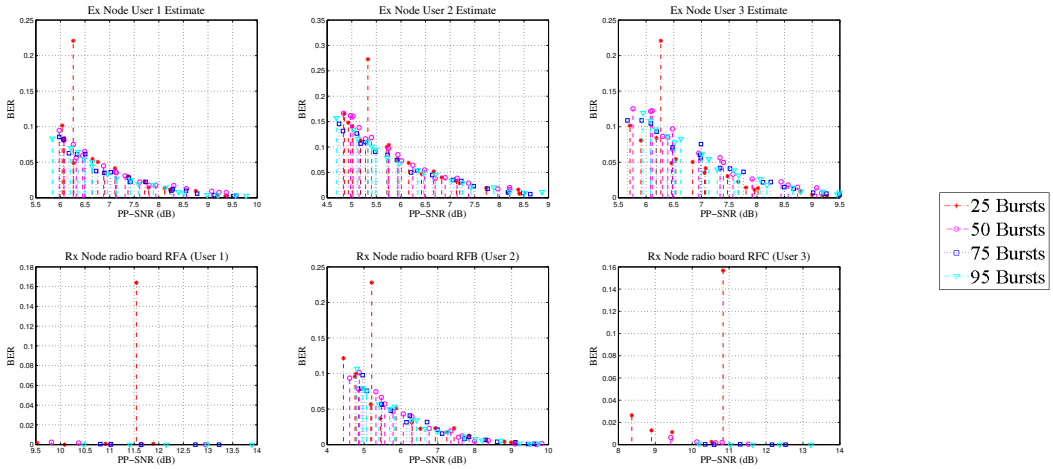

Figure 5.3: Plot of intercepted BER using CFO estimation and received user BER using LTS CSI estimation with $N_G = 4$

Figure 5.3 shows the CBDA of estimating CFO, for OFDMA-DL bursts of $N_B = [25, 50, 75, 95]$ with a CP length of 4. Again, the performance of the CFO estimate when compared to User 2 is similar, yet poorer than that of User 1 and User 3. Importantly, the ability to achieve BERs of 0 for all users above 10dB, which was achieved. With reduced CP length of 4, the number of spurious errors with 25 OFDMA-DL bursts has significantly increased for both the *ExJx* and *Rx* nodes. Given this result, it is unlikely a communications system would implement use of 25 OFDMA-DL bursts with $N_G = 4$, as redundancy measures are nullified resulting in increased errors. Use of the estimated CFO to demodulate the intercepted waveform from *ExJx* node radio board RFC, is viable with $N_G = 4$, albeit with risk of poor performance at lower PP-SNR.

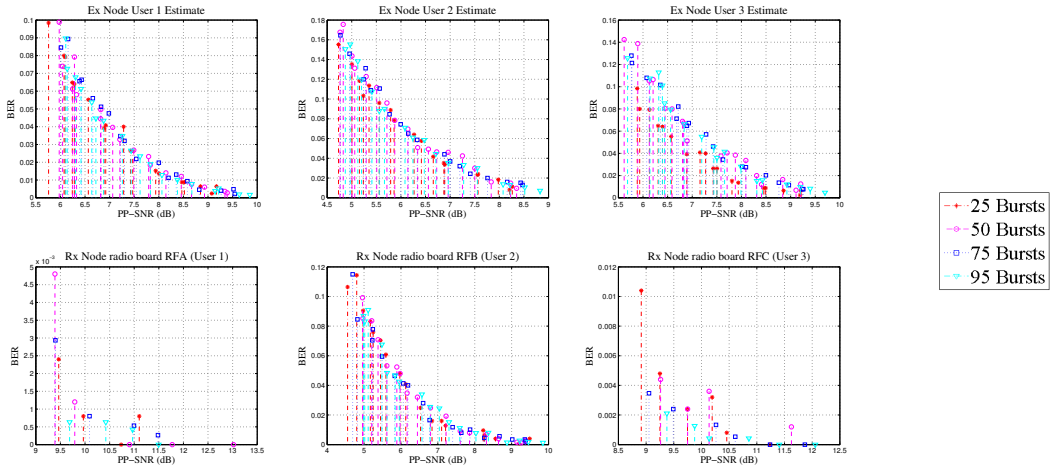

Figure 5.4: Plot of intercepted BER using CFO estimation and received user BER using LTS CSI estimation with $N_G = 2$

Figure 5.4 shows the CBDA of estimating CFO, for OFDMA-DL bursts of $N_B = [25, 50, 75, 95]$ with a CP length of 2. Again, the performance of the CFO estimate when compared to User 2 is similar, yet poorer than that of User 1 and User 3. Importantly, the ability to achieve BERs of 0 for all users above 10dB, which was achieved. With the reduced CP length of 2, the BER for user 2 has increased. Given this result, it is unlikely a communications system would implement use of $N_G = 2$, as measured to reduce effects of ISI are no longer effective and a larger CP is required. Given these CBDA results shown in Figure 5.4, use of the estimated CFO to demodulate the intercepted waveform from *ExJx* node radio board RFC, is viable with $N_G = 2$, albeit with risk of poor performance at lower PP-SNR.

Figures 5.1 - 5.4 show as PP-SNR increases, the *Ex* estimation, using *ExJx* node radio board RFC, is able to perform accurate demodulation. Whilst the estimation of ϵ is bounded by half the sub carrier spacing, actual CFO beyond this bound would exhibit greater interference due to ICI [8].

5.3 Detecting SC modulation

As discussed in Section 4.3.3, sub carrier modulation detection was conducted after applying the channel estimate. The detector's ability to classify modulation was applied to all modulation types with a fixed CP length, however, varying number of OFDMA-DL bursts. Shown in Figures 5.5 to 5.12 are the results for estimating sub carrier modulation with fourth and sixth order cumulants. To supplement these plots, the probability of detection is presented against PP-SNR and *Tx* RF gain. As discussed in Section 3.4, the RF gain is controlled using the WARPLab Reference Design, whilst PP-SNR is a hardware-specific description of SNR, as discussed in Section 2.2. Given hardware factors effecting PP-SNR occurs throughout the entire *Tx* RF gain range, it is possible the same PP-SNR value will be measured more than once. As such, PP-SNR plots shown in Figures 5.5 through 5.12 appear to reach a peak and then begin to decrease again. What has actually occurred is hardware factors and other noise effects have decreased the calculated PP-SNR. Therefore, the *Tx* RF gain plots have also been included to supplement the results and provide further explanation of system performance.

The CBDA shown in Figures 5.5 through 5.12 displays the probability of correct detection (P_c) of modulation types used to modulate data SCs, as discussed in Section 4.5. As with results in [3], the ability to determine whether PSK or QAM modulation has been used to modulate data SCs can be clearly determined. Furthermore, the MLE classifier is also able to, relatively accurately (up to $P_c = 1$), determine whether BPSK or QPSK modulation has been used. The poor performance of QAM modulation types is attributed to the small decision region between QAM-16 and QAM-64, as discussed in [3] and Chapter 2 of this thesis, resulting in incorrect classification between either of the two and resulting in poor P_c.

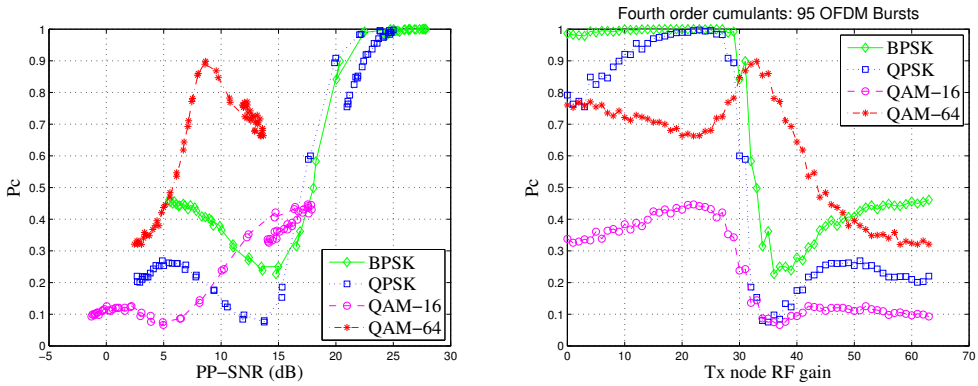

Figure 5.5: Sub carrier estimation for 95 OFDM bursts using fourth order cumulants

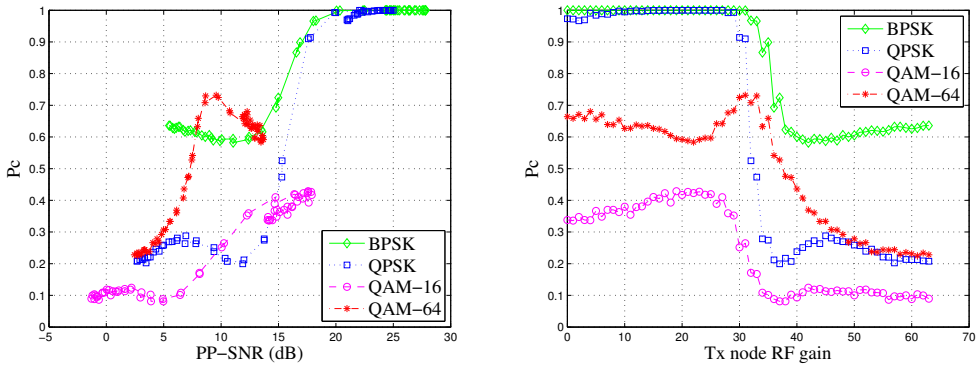

Figure 5.6: Sub carrier estimation for 95 OFDM bursts using sixth order cumulants

Shown in Figures 5.5 and 5.6 is the CBDA of the *ExJx* node to detect SC modulation of data SCs on a transmitted waveform with 95 OFDMA-DL bursts. As shown in Figures 5.5 and 5.6, at the mid range of *Tx* node RF gain, set using the WARPLab Reference Design, both fourth and sixth order cumulant modulation detection schemes begin to perform poorly. Whilst results in [3] did exhibit some of these characteristics, they were recorded as SNR below 0dB. Again, whilst PP-SNR is a hardware specific description of SNR, it is not expected performance to be reduced as PP-SNR, or *Tx* node RF gain increased. A possible explanation for such an occurrence would be non-linear interference being induced into the OFDMA-DL, as a result of PAPR or possible hardware effects. Regardless, at *Tx* node RF gains below thirty, the sixth order cumulant modulation detection method performs better than the fourth order cumulant modulation detection for transmitted OFDMA-DL waveforms with 95 bursts.

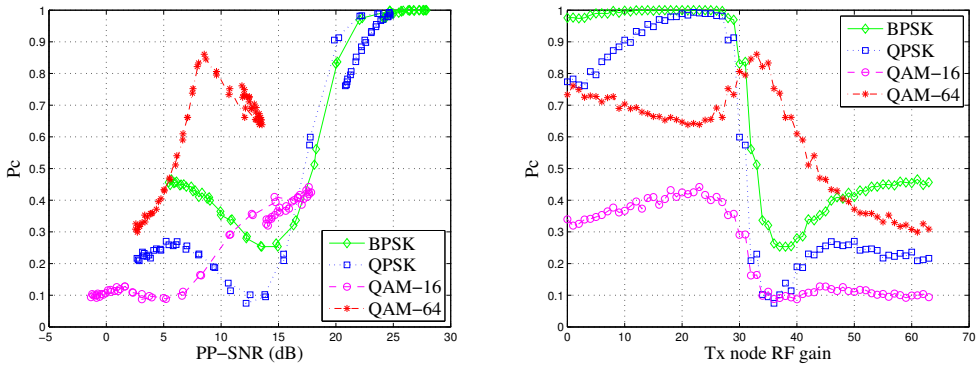

Figure 5.7: Sub carrier estimation for 75 OFDM bursts using fourth order cumulants

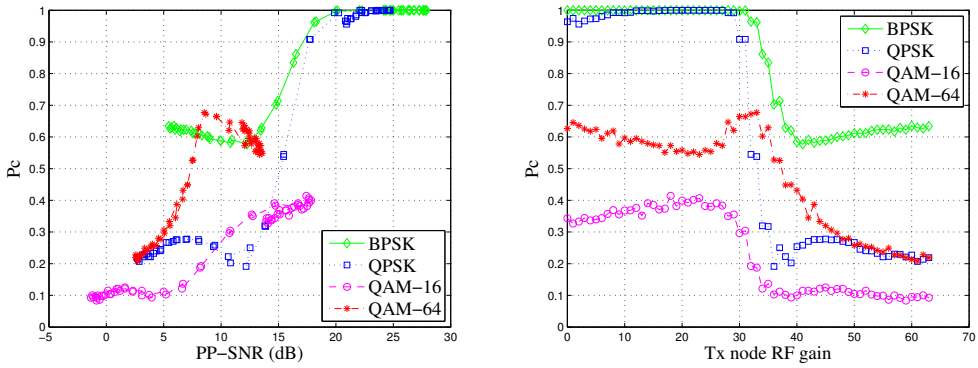

Figure 5.8: Sub carrier estimation for 75 OFDM bursts using sixth order cumulants

Shown in Figures 5.7 and 5.8 is the CBDA of the *ExJx* node to detect SC modulation of data SCs on a transmitted waveform with 75 OFDMA-DL bursts. As shown in Figures 5.7 and 5.8, again at the mid range of *Tx* node RF gain, set using the WARPLab Reference Design, both fourth and sixth order cumulant modulation detection schemes begin to perform poorly. Since the same properties have been exhibited with 75 OFDMA-DL bursts, as what was seen with 95 OFDMA-DL bursts (Figures 5.5 and 5.6), such an occurrence is likely non-linear interference being induced into the OFDMA-DL, as a result of PAPR or possible hardware effects. Similarly, at *Tx* node RF gains below thirty, the sixth order cumulant modulation detection method performs better than the fourth order cumulant modulation detection for transmitted OFDMA-DL waveforms with 75 bursts.

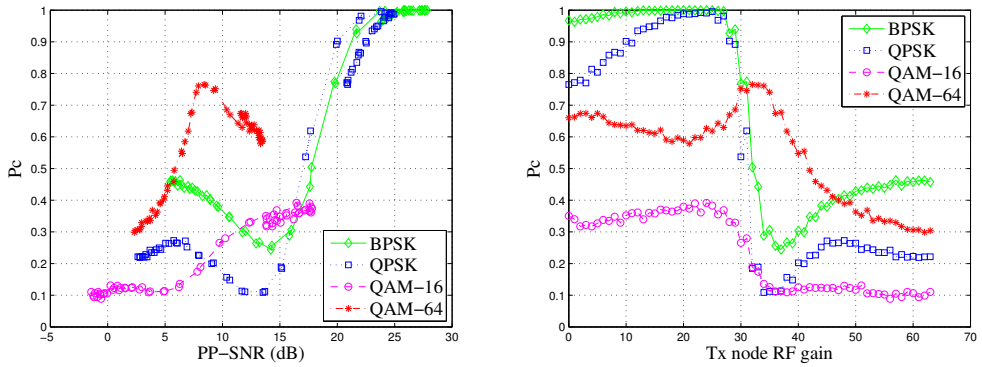

Figure 5.9: Sub carrier estimation for 50 OFDM bursts using fourth order cumulants

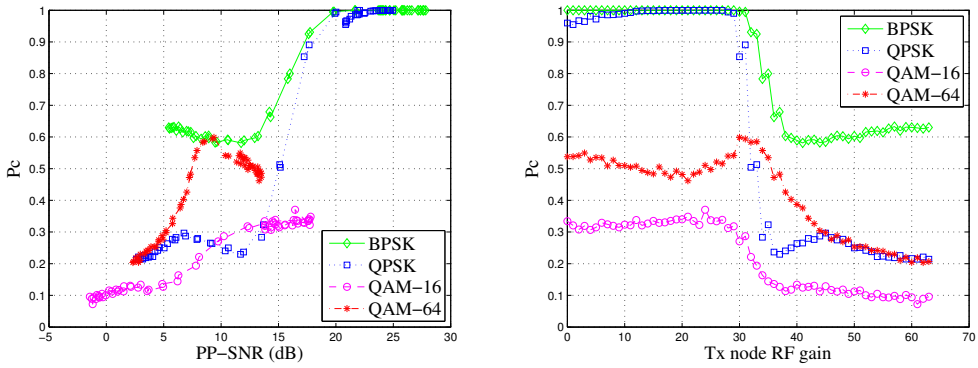

Figure 5.10: Sub carrier estimation for 50 OFDM bursts using sixth order cumulants

Shown in Figures 5.9 and 5.10 is the CBDA of the *ExJx* node to detect SC modulation of data SCs on a transmitted waveform with 50 OFDMA-DL bursts. As shown in Figures 5.9 and 5.10, again at the mid range of *Tx* node RF gain, set using the WARPLab Reference Design, both fourth and sixth order cumulant modulation detection schemes begin to perform poorly. Since the same properties have been exhibited with 50 OFDMA-DL bursts, as what was seen with 75 and 95 OFDMA-DL bursts, such an occurrence is likely non-linear interference being induced into the OFDMA-DL, as a result of PAPR or possible hardware effects. Similarly, at *Tx* node RF gains below thirty, the sixth order cumulant modulation detection method performs better than the fourth order cumulant modulation detection for transmitted OFDMA-DL waveforms with 50 bursts.

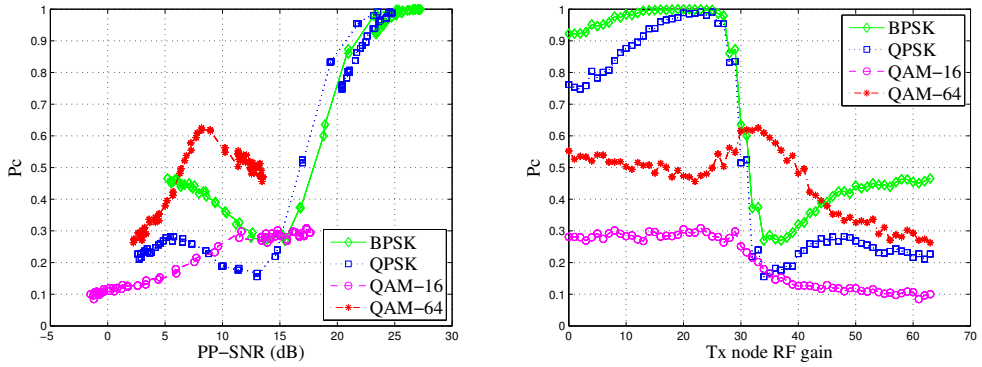

Figure 5.11: Sub carrier estimation for 25 OFDM bursts using fourth order cumulants

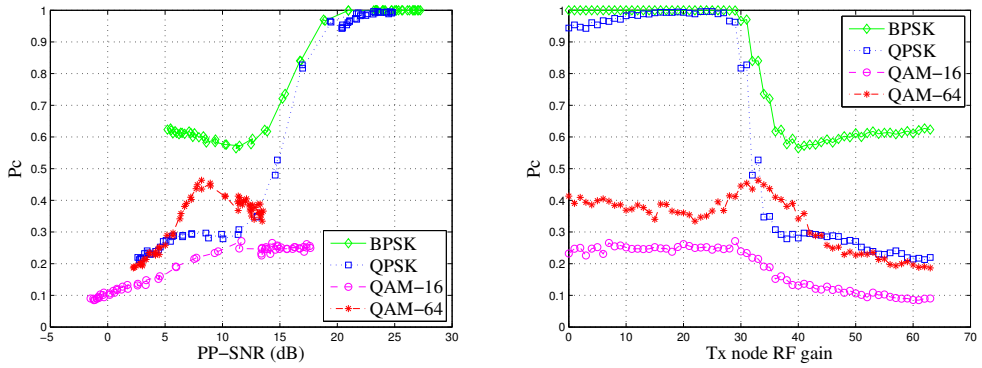

Figure 5.12: Sub carrier estimation for 25 OFDM bursts using sixth order cumulants

Shown in Figures 5.11 and 5.12 is the CBDA of the *ExJx* node to detect SC modulation of data SCs on a transmitted waveform with 25 OFDMA-DL bursts. As shown in Figures 5.11 and 5.12, again at the mid range of *Tx* node RF gain, set using the WARPLab Reference Design, both fourth and sixth order cumulant modulation detection schemes begin to perform poorly. Since the same properties have been exhibited with all OFDMA-DL burst lengths, such an occurrence is likely non-linear interference being induced into the OFDMA-DL, as a result of PAPR or possible hardware effects. Similarly, at *Tx* node RF gains below thirty, the sixth order cumulant modulation detection method performs better than the fourth order cumulant modulation detection for transmitted OFDMA-DL waveforms with 25 bursts.

Given the above results, it can be seen that use of sixth order cumulants enables more accurate sub carrier modulation detection, irrespective of the number of OFDMA-DL bursts. Regardless of what order cumulant is used, however the classifier had difficulty identifying QAM-16 and QAM-64

modulation schemes, although QAM-64 modulation was more accurately classified than QAM-16, this is likely a result of the small decision regions used to determine whether QAM-16 or QAM-64 modulation schemes has been used. Despite this difficulty, the detector is capable of distinguishing between PSK and QAM modulation types.

5.4 Implementing interference techniques

With estimation techniques verified using CBDA, an interference waveform was constructed using estimated signal features and CFO phase estimates, as discussed in Section 4.4. The selected *Tx* RF gain was ten, as estimations at this gain level were most successful.

Tables 5.2 to 5.5 display the results of applying interference techniques after obtaining results of signal feature estimation. Whilst the BER has increased for each situation, the increase is minimal, suggesting communications could continue despite interference attempts. As discussed in Chapter 2, OFDM and OFDMA waveforms are able to maintain data transfer even with changing channel effects. Whilst it was hypothesised introducing CFO effects would have an impact on BER, due to OFDM being sensitive to changes in CFO, this has not been significantly observed.

Displayed in Table 5.2 are the effects of applying interference techniques to a transmitted OFDMA-DL waveform, with 95 bursts, between *Tx* node and *Rx* node, with users demodulating received waveforms from radio boards RFA, RFB or RFC. The ability of the *Rx* node to correctly demodulate the received waveform is displayed in Table 5.2, as an expression of BER for each radio board used to receive the transmitted OFDMA-DL waveform.

To assess the effectiveness of eavesdropping performed by the *ExJx* node radio board RFC, CBDA techniques are used to determine how effectively the *Ex* process was at estimating signal features, CFO and determining SC modulation type. The ability to correctly demodulate the intercepted waveform, with 95 OFDMA-DL bursts, is displayed in Table 5.2, as an expression of BER CBDA for each intended user represented in the OFDMA-DL waveform. The BER CBDA for each user corresponds to the *Rx* node radio board used.

Referring to the CBDA column of Table 5.2, the ability of the *ExJx* node to intercept a transmitted OFDMA-DL waveform with 95 bursts is relatively effective, with relatively small (0.01)

Table 5.2: Effects of applying interference techniques to OFDMA-DL waveform with 95 bursts

	BER RFA	BER CBDA RFA	BER JBDA RFA
$N_G = 16$	0.0725	0.0820	0.1335
$N_G = 8$	0.1045	0.1229	0.1475
$N_G = 4$	0.0610	0.0868	0.1319
$N_G = 2$	0.0820	0.0940	0.1292
	BER RFB	BER CBDA RFB	BER JBDA RFB
$N_G = 16$	0.0723	0.0846	0.1337
$N_G = 8$	0.1045	0.1248	0.1485
$N_G = 4$	0.0611	0.0826	0.1321
$N_G = 2$	0.0812	0.0949	0.1290
	BER RFC	BER CBDA RFC	BER JBDA RFC
$N_G = 16$	0.0725	0.0881	0.1337
$N_G = 8$	0.1047	0.1229	0.1480
$N_G = 4$	0.0608	0.0868	0.1321
$N_G = 2$	0.0824	0.0940	0.1294

increases in BER when compared to the BER column for each user. This is positive given the multi-path, non-linear and hardware effects present in the communication system. In situations where the communication system is poorly performing, likely due to hardware effects or a reduction in CP length, the ability of the *ExJx* node to intercept the OFDMA-DL waveform is similar, with BERs of the same order.

To assess the effectiveness of jamming performed by the *ExJx* node radio board RFA, JBDA techniques are used to determine how effectively the *Jx* process was at interfering with the transmitted OFDMA-DL waveform. The ability to effectively interfere with the waveform is displayed in Table 5.2, as an expression of BER JBDA for each user represented in the OFDMA-DL waveform. The BER JBDA for each user has been determined by calculating the BER after

an interfering transmission. That is, the same technique used to determine the initial user BER is implemented, yet after transmission of the interfering waveform.

Referring to the JBDA column of Table 5.2, the ability of the *ExJx* node to interfere with a transmitted OFDMA-DL waveform with 95 bursts is effective, increasing the BER for each user by approximately 0.06. In situations where the communication system is poorly performing, likely due to hardware effects or a reduction in CP length, the ability of the *ExJx* node to interfere the OFDMA-DL waveform remains similar to a communication link with lower BER. This is an indication of a successful *Jx* technique and effective JBDA.

Table 5.3: Effects of applying interference techniques to OFDMA-DL waveform with 75 bursts

	BER RFA	BER CBDA RFA	BER JBDA RFA
$N_G = 16$	0.0938	0.1190	0.1732
$N_G = 8$	0.0926	0.1148	0.1664
$N_G = 4$	0.0891	0.1167	0.1639
$N_G = 2$	0.1038	0.1205	0.1697
	BER RFB	BER CBDA RFB	BER JBDA RFB
$N_G = 16$	0.0964	0.1135	0.1732
$N_G = 8$	0.0931	0.1066	0.1666
$N_G = 4$	0.0905	0.1129	0.1638
$N_G = 2$	0.1042	0.1174	0.1699
	BER RFC	BER CBDA RFC	BER JBDA RFC
$N_G = 16$	0.0965	0.1179	0.1728
$N_G = 8$	0.0929	0.1119	0.1669
$N_G = 4$	0.0909	0.1129	0.1631
$N_G = 2$	0.1040	0.1172	0.1694

Displayed in Table 5.3 are the effects of applying interference techniques to a transmitted OFDMA-DL waveform, with 75 bursts, between *Tx* node and *Rx* node, with users demodulating received waveforms from radio boards RFA, RFB or RFC. The ability of the *Rx* node to correctly demodulate the received waveform is displayed in Table 5.3, as an expression of BER for each radio board used to receive the transmitted OFDMA-DL waveform.

To assess the effectiveness of eavesdropping performed by the *ExJx* node radio board RFC, CBDA techniques are used to determine how effectively the *Ex* process was at estimating signal features, CFO and determining SC modulation type. The ability to correctly demodulate the intercepted waveform, with 75 OFDMA-DL bursts, is displayed in Table 5.3, as an expression of BER CBDA for each intended user represented in the OFDMA-DL waveform. The BER CBDA for each user corresponds to the *Rx* node radio board used.

Referring to the CBDA column of Table 5.3, the ability of the *ExJx* node to intercept a transmitted OFDMA-DL waveform with 75 bursts is less effective than a waveform with 95 bursts. Whilst the increases in BER are relatively small (0.02), when compared to the BER column for each user, it is not as effective as those results displayed in Table 5.2. This is likely due to a reduction in the ability of the *ExJx* node to effectively intercept OFDMA-DL waveforms with fewer bursts. In situations where the communication system is poorly performing, likely due to hardware effects or a reduction in CP length, the ability of the *ExJx* node to intercept the OFDMA-DL waveform is similar, with BERs of the same order.

To assess the effectiveness of jamming performed by the *ExJx* node radio board RFA, JBDA techniques are used to determine how effectively the *Jx* process was at interfering with the transmitted OFDMA-DL waveform. The ability to effectively interfere with the waveform is displayed in Table 5.3, as an expression of BER JBDA for each user represented in the OFDMA-DL waveform. Again, The BER JBDA for each user has been determined by calculating the BER after an interfering transmission.

Referring to the JBDA column of Table 5.3, the ability of the *ExJx* node to interfere with a transmitted OFDMA-DL waveform with 75 bursts is effective, increasing the BER for each user by approximately 0.06, which is a similar result to that shown in Table 5.2. In situations where the communication system is poorly performing, likely due to hardware effects or a reduction in CP length, the ability of the *ExJx* node to interfere the OFDMA-DL waveform remains similar to a communication link with lower BER. This is an indication of a successful *Jx* technique and effective JBDA.

Table 5.4: Effects of applying interference techniques to OFDMA-DL waveform with 50 bursts

	BER RFA	BER CBDA RFA	BER JBDA RFA
$N_G = 16$	0.1253	0.1575	0.2427
$N_G = 8$	0.1479	0.1705	0.2303
$N_G = 4$	0.1435	0.1872	0.2504
$N_G = 2$	0.1906	0.2177	0.2698
	BER RFB	BER CBDA RFB	BER JBDA RFB
$N_G = 16$	0.1261	0.1505	0.2430
$N_G = 8$	0.1466	0.1683	0.2303
$N_G = 4$	0.1427	0.1787	0.2519
$N_G = 2$	0.1878	0.2190	0.2705
	BER RFC	BER CBDA RFC	BER JBDA RFC
$N_G = 16$	0.1265	0.1509	0.2440
$N_G = 8$	0.1483	0.1687	0.2293
$N_G = 4$	0.1433	0.1744	0.2519
$N_G = 2$	0.1878	0.2169	0.2704

Displayed in Table 5.4 are the effects of applying interference techniques to a transmitted OFDMA-DL waveform, with 50 bursts, between *Tx* node and *Rx* node, with users demodulating received waveforms from radio boards RFA, RFB or RFC. The ability of the *Rx* node to correctly demodulate the received waveform is displayed in Table 5.4, as an expression of BER for each radio board used to receive the transmitted OFDMA-DL waveform.

To assess the effectiveness of eavesdropping performed by the *ExJx* node radio board RFC, CBDA techniques are used to determine how effectively the *Ex* process was at estimating signal features, CFO and determining SC modulation type. The ability to correctly demodulate the intercepted waveform, with 50 OFDMA-DL bursts, is displayed in Table 5.4, as an expression of BER CBDA for each intended user represented in the OFDMA-DL waveform. The BER CBDA for each user corresponds to the *Rx* node radio board used.

Referring to the CBDA column of Table 5.4, the ability of the *ExJx* node to intercept a transmitted OFDMA-DL waveform with 50 bursts is less effective than a waveform with either 95 or 75 bursts. In this case, the increases in BER have increased (0.03), when compared to the BER column for each user. Results shown thus far in Tables 5.2 - 5.3 indicate as the number of OFDMA-DL waveforms decrease, the ability of the *ExJx* node to effectively intercept OFDMA-DL waveforms reduces, regardless of other signal features, such as CP length.

To assess the effectiveness of jamming performed by the *ExJx* node radio board RFA, JBDA techniques are used to determine how effectively the *Jx* process was at interfering with the transmitted OFDMA-DL waveform. The ability to effectively interfere with the waveform is displayed in Table 5.4, as an expression of BER JBDA for each user represented in the OFDMA-DL waveform. Again, The BER JBDA for each user has been determined by calculating the BER after an interfering transmission.

Referring to the JBDA column of Table 5.4, the ability of the *ExJx* node to interfere with a transmitted OFDMA-DL waveform with 50 bursts is effective, increasing the BER for each user by approximately 0.1, which is a significant increase compared to results displayed in Tables 5.2 and 5.3. This is an indication of a successful *Jx* technique and effective JBDA, especially with smaller OFDMA-DL words.

Table 5.5: Effects of applying interference techniques to OFDMA-DL waveform with 25 bursts

	BER RFA	BER CBDA RFA	BER JBDA RFA
$N_G = 16$	0.3913	0.4574	0.5274
$N_G = 8$	0.1917	0.2825	0.4632
$N_G = 4$	0.2531	0.3353	0.4804
$N_G = 2$	0.2432	0.2864	0.3032
	BER RFB	BER CBDA RFB	BER JBDA RFB
$N_G = 16$	0.3879	0.4477	0.5301
$N_G = 8$	0.1828	0.2588	0.4622
$N_G = 4$	0.2561	0.3227	0.4833
$N_G = 2$	0.2448	0.2920	0.3032
	BER RFC	BER CBDA RFC	BER JBDA RFC
$N_G = 16$	0.3923	0.4494	0.5321
$N_G = 8$	0.1970	0.2620	0.4604
$N_G = 4$	0.2549	0.3159	0.4914
$N_G = 2$	0.2344	0.2992	0.3088

Displayed in Table 5.5 are the effects of applying interference techniques to a transmitted OFDMA-DL waveform, with 25 bursts, between *Tx* node and *Rx* node, with users demodulating received waveforms from radio boards RFA, RFB or RFC. The ability of the *Rx* node to correctly demodulate the received waveform is displayed in Table 5.5, as an expression of BER for each radio board used to receive the transmitted OFDMA-DL waveform.

To assess the effectiveness of eavesdropping performed by the *ExJx* node radio board RFC, CBDA techniques are used to determine how effectively the *Ex* process was at estimating signal features, CFO and determining SC modulation type. The ability to correctly demodulate the intercepted waveform, with 25 OFDMA-DL bursts, is displayed in Table 5.5, as an expression of BER CBDA for each intended user represented in the OFDMA-DL waveform. The BER CBDA for each user corresponds to the *Rx* node radio board used.

Referring to the CBDA column of Table 5.5, the ability of the *ExJx* node to intercept a transmitted OFDMA-DL waveform with 25 bursts is less effective than a waveform with either 95, 75 or 50 bursts. In this case, the increases in BER have increased unacceptably to beyond 0.06, when compared to the BER column for each user. This result confirms as the number of OFDMA-DL waveforms decrease, the ability of the *ExJx* node to effectively intercept OFDMA-DL waveforms reduces, regardless of other signal features, such as CP length.

To assess the effectiveness of jamming performed by the *ExJx* node radio board RFA, JBDA techniques are used to determine how effectively the *Jx* process was at interfering with the transmitted OFDMA-DL waveform. The ability to effectively interfere with the waveform is displayed in Table 5.4, as an expression of BER JBDA for each user represented in the OFDMA-DL waveform. Again, The BER JBDA for each user has been determined by calculating the BER after an interfering transmission.

Referring to the JBDA column of Table 5.5, the ability of the *ExJx* node to interfere with a transmitted OFDMA-DL waveform with 25 bursts is effective, increasing the BER for each user greater than 0.1, which is a significant increase. This is an indication of a successful *Jx* technique and effective JBDA, especially with smaller OFDMA-DL words.

It must also be noted, however, that larger errors occurred with the reduction in OFDMA-DL bursts to 25, regardless of CP length, indicating an OFDMA-DL word size this small would not be suitable for effective communications between a communication link.

5.4.1 Interference techniques with $N_B = 95$.

With results obtained for all OFDMA-DL burst sizes, further investigation was carried out with a fixed burst size of $N_B = 95$ and $N_G = [4, 8, 16]$ with *Tx* WARPLab RF gains of $[0 : 5 : 60]$. CP length of 2 was not investigated due to inconsistent results, as shown in Table 5.1, ensuring at all power levels, failures occurred in the ability to consistently construct an interference waveform.

Shown in Figure 5.13 is the probability of correct (P_c) SC modulation detection, performed by the *ExJx* node using radio board RFA. Whilst SC modulation detection is an eavesdropping function, it allows the *ExJx* node to determine whether interference techniques have been effective, as the

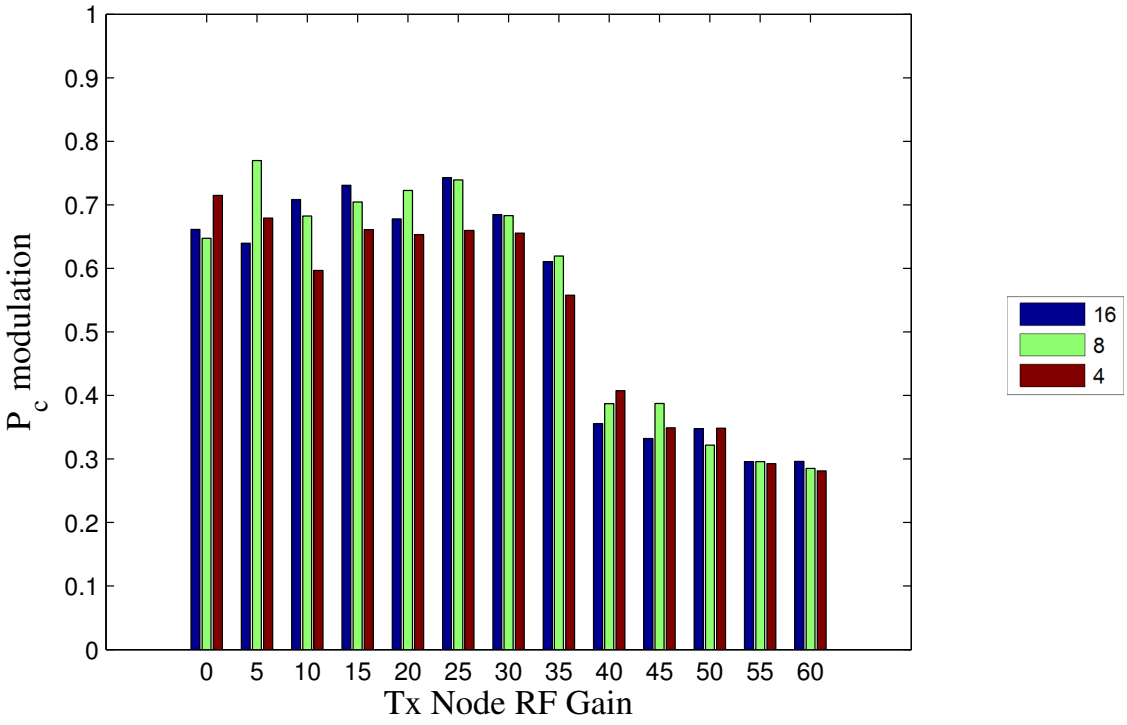

Figure 5.13: Probabilty of correct SC modulation detection for 95 OFDM bursts using sixth order cumulants during interference techniques

communication system will reduce the modulation order in an attempt to reduce communication errors. This is known as link adaptation [3, 31].

Results in Figure 5.13 are similar to what was shown in Section 5.3, in that at lower *Tx* RF gain, the ability to detect SC modulation is greater. The reduction in P_c is due to all modulation schemes being used during the investigation, that is BPSK, QPSK, QAM-16 and QAM-64. Furthermore, as the *Tx* RF gain is increased, the ability to detect the SC modulation decreases, again remaining consistent with results of Section 5.3 and attributed to WARP functionality.

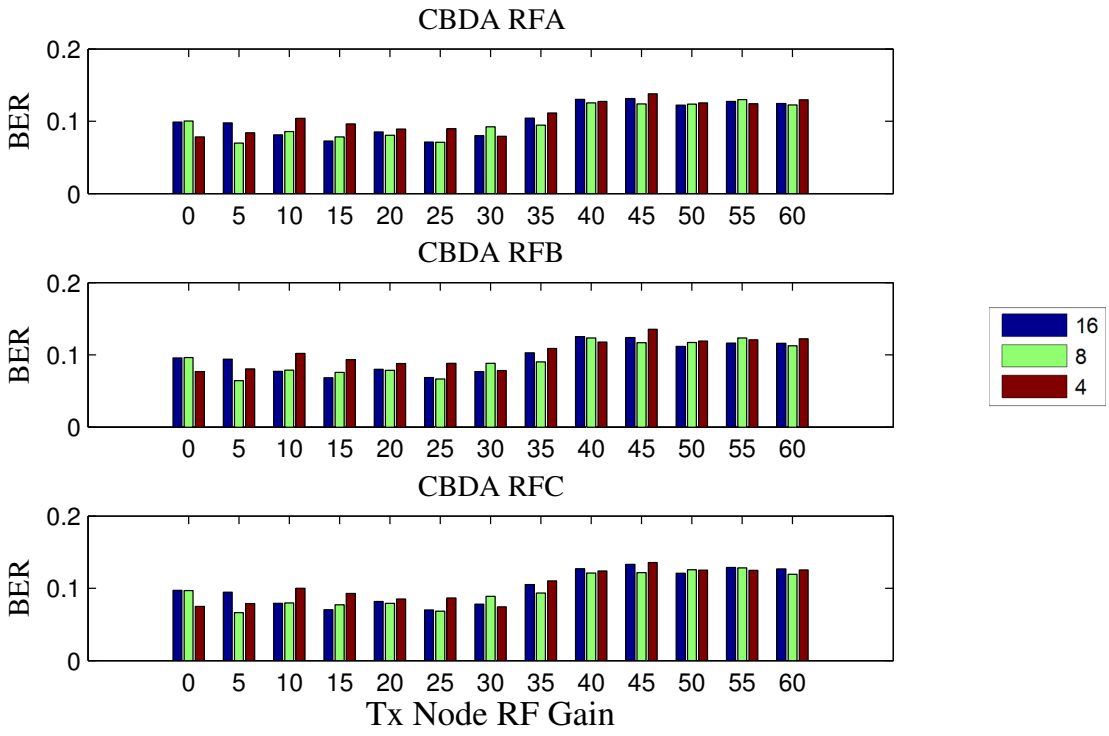

Figure 5.14: Ability of *ExJx* node to demodulate intercepted OFDMA-DL waveform, with 95 bursts, prior to jamming

Shown in Figure 5.14 is the ability to correctly demodulate the intercepted waveform during interference techniques. It is important to note the BER trend for each user follows the trend shown in Figure 5.13, which is to be expected, given demodulation shall be attempted for detected SC modulation. As a result of this, BER for intercepted *Tx* waveforms with RF gains greater than WARPLab setting of 30 (approximately 30 dB) have a poorer performance than those with a lower RF gain. Comparing the results with those shown in Figure 5.15, BER for the lower RF gain is similar to that of the target communication system, confirming *Ex* techniques applied by the *ExJx* node radio board RFA are successful.

Figure 5.14 was generated using CBDA techniques.

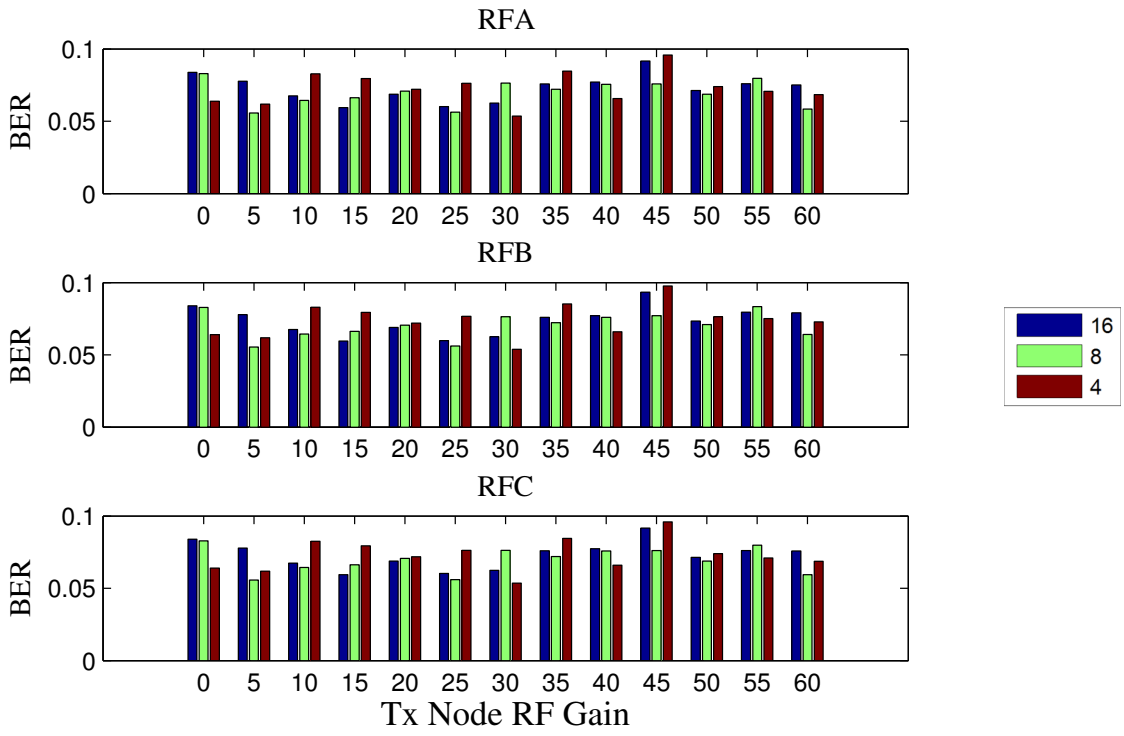

Figure 5.15: Ability of *Rx* node to demodulate transmitted OFDMA-DL waveform, with 95 bursts, without jamming

Shown in Figure 5.15 is the ability of the target communication system to correctly demodulate the transmitted OFDMA-DL prior to application of interference techniques by the *ExJx* node. Regardless of which user is demodulating the OFDMA-DL waveform, the BER level remains below 0.1 for all *Tx* RF gain levels.

Figure 5.15 was generated using CBDA techniques.

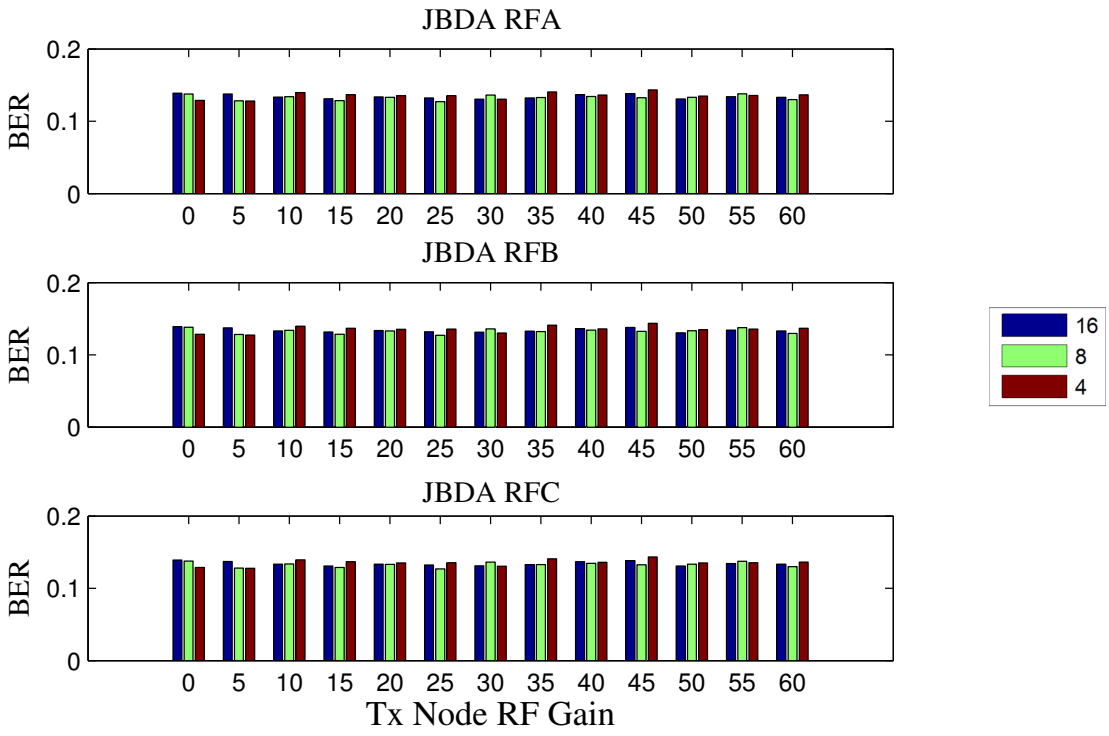

Figure 5.16: Ability of *Rx* node to demodulate transmitted OFDMA-DL waveform, with 95 bursts, with jamming

Shown in Figure 5.16 is the effect to the target communication system's ability to correctly demodulate the transmitted OFDMA-DL with application of interference techniques by the *ExJx* node. For all users, for all *Tx* RF gain levels, the ability to correctly demodulate the received signal is reduced, as evidenced by the increase of BER to greater than 0.1. The consistent increase in BER is attributed to the consistent process used to generate the interference waveform transmitted by radio board RFA of the *ExJx* node, discussed in Section 4.4. Results in Figure 5.16 validate use of estimated signal features to generate an effective interference waveform to disrupt communications between a target communication system.

Figure 5.16 was generated using JBDA techniques.

VI. Summary

6.1 Conclusion

Gaining mastery of the RF spectrum is a key objective of both the US military and its coalition partners. The ability to not only transmit communication and intelligence waveforms uninterrupted as well as intercepting other users information plays a key role into achieving such mastery. This research presents how previously simulated estimation techniques can be applied to estimating information transmitted using a wireless communication link.

Whilst effects such as changes in number of OFDM bursts and CP length did have bearing on performance of each of the estimators, overall, the methodology developed in [3] performs well at baseband when implemented on WARP. Of particular note is how well parameters such as number of OFDM waveforms, FFT size and CP length can be estimated. The ability to detect such parameters allows for further estimation and demodulation of intercepted waveforms.

Given the large variation of CFO witnessed when either estimated or calculated using LTS, larger BER regardless of technique used is not significant. The presence of multipath effects and the simulated performance of the estimator shown in [3], indicate further development of CFO estimation is required.

The ability of the sub carrier modulation detector to identify modulation schemes using sixth order cumulants performed well, despite the introduction of a multi-path environment. The MLE classifier was able to accurately detect PSK modulation schemes, regardless of OFDMA-DL burst sizes, indicating the classifier is robust to such variations. Results in [3] indicated the estimator may have difficulty to correctly identify modulation schemes in a channel with multi-path influences, however, despite multi-path effects being present in this communication system, significantly poor performance was not apparent. Whilst only data sub carriers were considered in this research, the ability of the estimator to correctly identify PSK modulation schemes is better than expected, which would enable pilot SCs to be identified in future research. Further assistance to correctly identify QAM-16 and QAM-64 modulation schemes is required.

Use of the estimated signal features to construct an OFDMA interferer was successful. Whilst the interferer was capable of inducing errors to the transmitted OFDMA-DL waveform, more successful interference is required to successfully cease transmissions. However, the ability of *Ex* to successfully intercept OFDMA waveforms greater than 25 bursts, without intercepting CSI messages between nodes, such as what is implemented in [23], suggests the ability to successfully intercept messages without alerting users of *ExJx* node presence within channel.

6.2 Future work

Given the results presented in this research, further investigation into complete blind estimation would be a possible topic for later research, including demodulation and classification of an actual 802.11 WiFi transmission. It would also be desirable to perform demodulation without use of the preamble.

Given this research only estimates sub carrier modulation on known data SCs, due to use of a zero forcing estimator, investigating the ability of the estimator to distinguish between data SCs and guards in a multi path environment could also be investigated. If the estimator could be shown to achieve this on hardware also, its use could be extended for different FFT sizes with differing waveform structure.

To further enhance the effectiveness of interference jamming, investigation of pilot phase jamming or CP interference could be applied, given they are often used for phase corrections and cyclic redundancy respectively.

Bibliography

[1] WARP Project, "http://warpproject.org," 2014.

[2] A. Swami and B.M. Sadler, "Heirarchical Digital Modulation Classifier using cumulants," *IEEE Transactions on Communications*, vol. 48, no. 3, pp. 416–429, Mar. 2000.

[3] N.A. Rutherford, "Blind Demodulation of Pass Band OFDMA Signals and Jamming Battle Damage Assessment Utilizing Link Adaptation," M.S. thesis, Air Force Institute of Technology, 2014.

[4] R.K. Martin and C.R. Johnson, "Adaptive equalization:transitioning from single-carrier to multicarrier systems," *IEEE Signal Processing Magazine*, vol. 22, no. 6, pp. 108–122, 2005.

[5] J. Porcello, "Designing and implementing OFDM communications for Advanced Multifunction UAV payloads using FPGAs," in *2012 IEEE Aerospace Conference*, Big Sky, MT, 2012, pp. 1–12.

[6] P. Murphy, A. Sabharwal, and B. Aazhang, "Design of WARP: A Wireless Open-Access Research Platform," in *Proceedings of EUSIPCO*, Florence, Italy, 2006.

[7] MATLAB, *version 8.1.0.604 (R2013a)*, The MathWorks Inc., Natick, Massachusetts, 2013.

[8] R. van Nee and R. Prasad, *OFDM for Wireless Multimedia Communications*, Artech House, 2000.

[9] R.W. Chang, "Orthogonal frequency multiplex data transmission system," Jan. 6 1970, US Patent 3,488,445.

[10] R.W. Chang, "Synthesis of Band Limited Orthogonal Signals for Multichannel Data Transmission," *Bell Systems Technical Journal*, vol. 45, pp. 1775–1796, Dec. 1966.

[11] S.B. Weinstein and P.M. Ebert, "Data Transmission by Frequency-Division Multiplexing Using the Discrete Fourier Transform," *IEEE Transactions on Communication Technology*, vol. 19, no. 5, pp. 628–634, Oct. 1971.

[12] G.J. Pottie and A.R. Calderbank, "Channel Coding Strategies for Cellular Radio," *IEEE Transactions on Vehicular Technology*, vol. 44, no. 4, pp. 763–770, Nov. 1995.

[13] M. Marchetti, M. Rahman, S. Kumar, and Prasad R., *New Directions in Wireless Communications Research*, Springer, 2002.

[14] A. Pandharipande, "Principles of OFDM," *IEEE Potentials*, vol. 21, no. 2, pp. 16–19, 2002.

[15] *IEEE Std 802.11-2012 - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, 2012.

[16] *IEEE Std 802.16-2012*, 2012.

[17] K. Amiri, Y. Sun, P. Murphy, C. Hunter, J. R. Cavallaro, and A. Sabharwal, "WARP, a Unified Wireless Network Testbed for Education and Research," in *IEEE International Conference on Microelectronic Systems Education*, San Diego, CA, 2007, pp. 53–54.

[18] K. Wanuga, R. Measel, C.S. Lester, D.J. Bucci, D. Gonzalez, R. Primerano, M. Kam, and K.R. Dandekar, "Performance Evaluation of MIMO OFDM Systems in On-Ship Below-Deck Environments," *IEEE Antennas and Wireless Propagation Letters*, vol. 13, pp. 173–176, Jan. 2014.

[19] J. Pennington, *Scalable system design for covert MIMO communications*, Ph.D. thesis, Air Force Institute of Technology, 2014.

[20] B.P. Lathi and Z. Ding, *Modern Digital and Analog Communication Systems*, Oxford University Press, New York, NY, 4 edition, 2010.

[21] P. Moose, "A technique for orthogonal frequency division multiplexing frequency offset correction," *IEEE Transactions on Communications*, pp. 2908–2914, Oct. 1994.

[22] P. Murphy, A. Sabharwal, and B. Aazhang, "On Building a Cooperative Communication System: Testbed Implementation and First Results," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, June 2009.

[23] Y. Tung, S. Han, D. Chen, and K. Shin, "Vulnerability and protection of channel state information in multiuser mimo networks," in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, 2014.

[24] S. Zettas, S. Kasampalis, P. Lazardis, Z.D. Zaharis, and J. Cosmas, "Channel estimation for OFDM systems based on a time domain pilot averaging scheme," in *2013 16th International Symposium on Wireless Personal Multimedia Communications (WPMC)*, Atlantic City, NJ, 2013, pp. 1–6.

[25] T. Yucek and H. Arslan, "OFDM Signal Identification and Transmission Parameter Estimation for Cognitive Radio Applications," in *IEEE 2007 Global Telecommunications Conference*, Washington, DC, Nov. 2007, pp. 4056–4060.

[26] M. Shi, *Advanced classification of OFDM and MIMO signals with enhanced second order cyclostationarity detection*, Ph.D. thesis, New Jersey Institute of Technology, 2010.

[27] *Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms*, (As Amended Through 15 December 2014).

[28] E.S. Hennessey, "Opportunistic Access in Frequency Hopping Cognitive Radio Networks," M.S. thesis, Air Force Institute of Technology, 2014.

[29] *Virtex-4 FPGA Data Sheet: DC and Switching Characteristics*, Sept. 2009, DS302 (v3.7).

[30] *MAX2828/MAX2829 Single-/Dual-Band 802.11a/b/g World-Band Transceiver ICs*, http://www.maximintegrated.com/en/products/comms/wireless-rf/MAX2829.html.

[31] K. Jayanthi, *Some investigations on quality improvement using link adaptation techniques in cellular mobile networks*, Ph.D. thesis, Pondicherry University, 2006.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704–0188

1. REPORT DATE *(DD–MM–YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From — To)*
26–03–2015	Master's Thesis	Oct 2013–Mar 2015

4. TITLE AND SUBTITLE

Communication and Jamming BDA of OFDMA communication systems using the software defined radio platform WARP

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Yaxley, Kate J., FLTLT, Royal Australian Air Force

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 Hobson Way
WPAFB, OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT-ENG-MS-15-M-073

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Intentionally Left Blank

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

DISTRIBUTION STATEMENT A:
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The aim of this research is to demonstrate and evaluate the ability to eavesdrop and interfere with orthogonal frequency division multiple access-down link (OFDMA-DL) signal features utilising Wireless Open Access Research Platform (WARP) boards. The OFDMA-DL waveforms have been developed with 64 sub carriers and have guards and pilots as comparable to the 802.11a WiFi standard.
An eavesdropper/interferer (*ExJx*) is used to estimate signal features, remotely gaining intelligence without alerting the communication system. This research also demonstrates how estimated signal features can be used to interfere with an established communication system.
Methods used to perform the signal feature estimation exploit the cyclostationary nature of the OFDMA-DL waveform, with higher order cumulants utilised to classify modulation schemes.
To assess the ability of the *ExJx* system to eavesdrop (*Ex*), Communication Battle Damage Assessment (CBDA) techniques are used. To assess the ability of the *ExJx* system to interfere (*Jx*), Jamming Battle Damage Assessment (JBDA) techniques are used.

15. SUBJECT TERMS

OFDMA, WARP, Jamming, Interference assessment.

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Dr. Richard K. Martin (ENG)
U	U	U	UU	96	19b. TELEPHONE NUMBER *(include area code)* (937)785-3636 xx4625 Richard.Martin@afit.edu