DOT/FAA/AR-xx/xx

Federal Aviation Administration
William J. Hughes Technical Center
Aviation Research Division
Atlantic City International Airport
New Jersey 08405

The FAA's Center of Excellence for UAS Research
ASSURE
Alliance for System Safety of UAS through Research Excellence

Secure Command and Control (C2) Link with Interference Mitigation

December 2017

Final Report

U.S. Department of Transportation
Federal Aviation Administration

NOTICE

The FAA's Center of Excellence for UAS Research
ASSURE
Alliance for System Safety of UAS through Research Excellence

Technical Report Documentation Page

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
DOT/FAA/AR-xx/xx		

4. Title and Subtitle	5. Report Date
A9 Secure Command and Control (C2) Link with Interference Mitigation	December 2017
	6. Performing Organization Code

7. Author(s)	8. Performing Organization Report No.
Principal Investigator: John Volakis (co-PIs: C. Emre Koksal, James Gregory), Ohio State Univ. Research Team: Abe Akhiyat – Oversees day to day activities Sam Mensah – Graduate Student Researcher Hari Indukuri – Graduate Student Researcher Halit Bugra Tulay – Graduate Student Researcher	

9. Performing Organization Name and Address	10. Work Unit No. (TRAIS)
The Ohio State University, Columbus Ohio	11. Contract or Grant No.

12. Sponsoring Agency Name and Address	13. Type of Report and Period Covered
The Federal Aviation Administration	Final Report
	14. Sponsoring Agency Code

15. Supplementary Notes

The Federal Aviation Administration Aviation William J. Hughes Technical Center Research Division COR was

16. Abstract

See Proposal titled "A9 Secure Command and Control (C2) Link with Interference Mitigation"

17. Key Words	18. Distribution Statement
	This document is available to the U.S. public through the National Technical Information Service (NTIS), Springfield, Virginia 22161. This document is also available from the Federal Aviation Administration William J. Hughes Technical Center at actlibrary.tc.faa.gov.

19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of Pages	22. Price
Unclassified	Unclassified		

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS

ACM	Adaptive Coding and Modulation
AG	Air-Ground
ASSURE	Alliance for System Safety of UAS through Research Excellence
AWGN	Additive White Gaussian Noise
BER	Bit Error Rate
BLOS	Beyond Line of Sight
BPSK	Binary Phase Shift Keying
C2	Command and Control
CNPC	Control and Non-Payload Communications
CRC	Cyclic Redundancy Check
FAA	Federal Aviation Administration
FDD	Frequency Division Duplexing
FEC	Forward Error Correction
FER	Frame Error Rate
FSK	Frequency Shift Keying
GMSK	Gaussian Minimum Shift Keying
GS	Ground Station
LOS	Line of Sight
MCS	Modulation and Coding Schemes
MIMO	Multiple Input Multiple Output
MOPS	Minimum Operational Performance Standards
NAS	National Airspace System
PSK	Phase Shift Keying
QPSK	Quadrature Phase Shift Keying
RF	Radio Frequency
RTCA	Radio Technical Commission for Aeronautics
SC	Special Committee
SDR	Software Defined Radio
SIMO	Single Input Multiple Output
SJR	Signal to Jammer Raito
SNR	Signal to Noise Ratio
TIM	Technical Interchange Meeting
TDD	Time Division Duplexing
UA	Unmanned Aircraft
UAS	Unmanned Aerial System
UAV	Unmanned Aerial Vehicle

EXECUTIVE SUMMARY

The UAS control and non-payload communications (CNPC) physical layer is envisioned to be infrastructure-free and thus it is susceptible to multi-user interference and a wide variety jamming signals. As UAS air traffic density increases, the hazard posed by multiple users in the same airspace also increases. Spectral interference can result in total loss of link, increased power consumption, packet delays, or bit errors – all of which degrade the reliability of the control link and pose significant risks to safety of flight. Therefore, interference cancellation and mitigation techniques are required to establish secure and robust communication between unmanned aircraft and control station.

The main objective of this research is to develop and implement/test multi-user interference cancellation and jamming mitigation techniques with large coding gain for handling different interference and jamming scenarios. Our goal is to implement transceivers for unmanned aircraft systems (UAS) communications, evaluate signal gain under various interference/jamming scenarios, and develop robust architectures to suppress different types of interference in a wide variety of settings. This goal is achieved by combining adaptive channel coding techniques to realize large coding gain and jamming mitigation. Furthermore, we introduce novel mitigation techniques based on multiple-input and multiple-output (MIMO) strategies as well as exploiting the strong line of sight (LOS) character of UAS to ground station communications.

This research assesses and effectively mitigates multi-user interference as well as jamming in the evaluated RF waveforms. This is done through analysis and testing on frequency bands of interest to the RTCA SC-228 Phase 1 MOPS, for UAS C2 data link physical security protection.

The original scope of this research was for a 3-year program, and included the realization and testing of Phase I MOPS as well as the examination of Phase II MOPS. However, the project was not extended beyond its first year; therefore, this report does address all of the original objectives set forth at the outset of this work. Nevertheless, since the research was proceeding ahead of schedule on all tasks, additional work for some of the out-year objectives are also included here. These additional results include testing and evaluations for the Phase I MOPS, along with security recommendations.

1. INTRODUCTION.

The UAS control and non-payload communications (CNPC) physical layer as well as any other wireless communication technology is vulnerable to multiuser interference, as well as jamming-based attacks in which an interferer purposefully or unintentionally launches a signal or noise that corrupts RF communications. Several undesirable scenarios can occur as a result, that include total loss of communication link, an increase in power consumption, data packets delay and degradation in bit error rates. Therefore, in order to maintain safety of flight, interference cancellation and mitigation techniques are required to establish secure communication between unmanned aircraft(s) and control station(s).

The FAA and Radio Technical Commission for Aeronautics (RTCA) SC-228 have identified physical layer security risks associated with CNPC systems that support the operation of unmanned aerial systems (UAS). With this in mind, the primary objective of this research is to develop, test, and evaluate secure communication links between unmanned aircraft(s) and ground control station(s) for line of sight (LOS) links in phase 1 and beyond line of sight links (BLOS) in phase 2. The research supports the development of a testbed for C2 communication links, and provides the necessary security insights and interference/jamming mitigation solutions to ensure the CPNC radio link in point-to-point configuration. To this end, mechanisms to address interference were developed as well as robust architectures to suppress different types of jammers in a wide variety of settings are investigated. Adaptive coding and modulation is used in combination with multiuser communication techniques, multiuser detection, and MIMO to achieve reliable communication between all ground stations and associated UAVs. Ultimately the goal of this work is to contribute to the current MOPS and expand its capability for safer UAV communication protocols.

Note:
The original proposed task list is shown in Table 1. It was initially designed for the duration of three years. However, due to the funding agency's decision to refocus and reprioritize, this work was only funded for phase 1. As a result, we were not able to see through subsequent phases of the proposed work, draw major conclusions or deliver complete solutions. The majority of the accomplished work was attributed to understanding the Minimum Operational Performance Standards (MOPS) and working with the governing parties to pin its underlying issues as we completed build of a hardware and software testbed environment. This was accomplished before the end of phase 1 as we started work on envisioned solutions projected in phases two and three of the project. Nevertheless, this report highlights the work that was completed.

Table 1: Detailed Task Schedule (Only Phase 1 was Accomplished (T+15))

Proposed Outcomes	Description	Date Due
Characterize and Implement Operational Constraints of Existing MOPS Based Radios	**Work with FAA engineers to characterize and implement operational constraints of existing MOPS based radio; as well as the constraints the proposed research solutions would pose to the NAS.**	**T+3**
Test and evaluation of security schemes for SC-228 Phase 1 at C band	**Develop a hardware and software set-up for testing and evaluation SC-228 Phase 1 MOPS terrestrial links for point-to-point operations. Evaluate security schemes for various modulated signals (GMSK, PSK, BPSK/QPSK, and FSK)**	**T +15 months**
Test and evaluation security Schemes for SC-228 Phase 2	Upgrade SC 228 Phase 1 hardware and software set-up for testing and evaluation SC-228 Phase 2. Carry out analysis and demonstrate anti-jamming techniques for satellites CNPC and terrestrial links	**T+27 months**
Test and evaluation of new secure wideband communications	Examine new security approaches for communication links; Exploit wideband RF and MIMO communication systems for higher-level security.	**T+ 35 months**
Technical Interchange Meeting (TIM)	Review progress via TELECON or Video Teleconference. Minimum quarterly. Will provide slides on technical progress, budget, schedule and risks.	**Quarterly**
Technical Report	The report will provide the status of the research desired products, schedule, budget and risks.	**Bi-annually**
Minutes/Notes	Minutes/Notes capturing the discussions and action items form each Technical Interchange Meetings (TIMS)	**3 days after the TIM**
Final Report	**Final report, detailing key safety characteristics and their thresholds for levels of safety operating in the NAS.**	**Before Grant Ends**

2. WORK SUMMARY

During the course of this project, regular meetings were held with the project sponsor to communicate project progress and ensure mutual understanding of project goals and deliverables.

All tasks and deliverables related to Phase 1 of this project were completed as scheduled and the team was able to complete testing and evaluation of Phase 1 MOPS at C band. Below, we briefly discuss the tasks that were accomplished during the first phase of this project.

Task 1: Literature Review and Testbed Design

Extracted MOPS requirements relevant to the construction of the CNPC physical layer. By doing so, we identified suitable hardware, and developed software required to implement C2 waveform links. A flexible testbed was designed, built and validated with each of the four data classes described in the baseline MOPS [1].

Task 2: Synchronization and Receiver Design

Completed synchronization and correction of channel imperfections in the developed software and hardware testbeds. Pilot-aided frame synchronization algorithms were then created and used for frequency and phase offset corrections.

Task 3: Software Optimization

Optimized software algorithms to provide flexibility for future modulation and channel coding schemes. Specifically, Gaussian Minimum Shift Keying (GMSK), Binary Phase Shift Keying (BPSK), and Quadrature Phase Shift Keying (QPSK) modulations were tested in our testbed along with convolutional turbo codes with various rates and puncture patterns for forward error correction (FEC).

Task 4: Initial Signal Analysis

BER curves were generated for un-coded and coded transmission of baseline MOPS signals. These were used to assess performance of GMSK modulated signals in an Additive White Gaussian Noise (AWGN) channel. Performance curves were used in conjunction with constellation diagrams and RF power spectrum to characterize signal and channel performance.

Task 5: Identification and Implementation of Scenarios of Interest

Interference scenarios with high probability of occurrence for UAV C2 links operating in point-to-point C2 links were identified. The physical layer conditions defining these scenarios were modeled and used to begin our security examination.

Task 6: Security Evaluation of MOPS Waveforms

Flexible software models and hardware experimental setups were developed to enable performance evaluation of C2 links in undesired operating conditions. BER curves were completed to characterize the effect of specific interferers on the CNPC link physical layer, and quantify their impact in various UAV operating conditions.

Task 7: Assessment of Jamming Mitigation Strategies

Proposed techniques were examined as potential solutions for enabling reliable communication links in low Signal to Noise (SNR) operating conditions. As part of this examination, optimization studies were completed to determine how to best employ these techniques for UAV use.

A brief summary of the above accomplishments are provided below in Table 2. Further details are provided in the subsequent sections of this report.

Table 2: Key Accomplished Tasks

Accomplished Tasks	Date Completed
• Completed Detailed Project Research Plan	October 2016
• Extracted pertaining requirements from MOPS for CNPC links	November 2016
• Designed comprehensive hardware and software testbed for implementation of CNPC Physical Layer	December 2016
• Completed Software Algorithms for Coding/Structuring of all four Data Classes specified in Baseline MOPS	December 2016
• Completed Receiver Synchronization and Correction of Initial Channel Imperfections	February 2017
• Evaluated Bit Error Rate (BER) performance of CNPC waveforms in testbed	March 2017
• Optimized Software Algorithms to provide flexibility for future Modulation and Coding Schemes (MCS)	April 2017
• Advanced testbed capabilities for security evaluation of C2 link at C band • Capabilities of interest: 1. Jamming and Channel Interference 2. Fading and Multipath 3. Multiuser, MIMO communication	April 2017
• Completed Bi-Annual Technical Report for Quarters 1&2	May 2017
• Completed preliminary study on Adaptive Coding + Multiple Antenna techniques as solution to Near-Far problem	July 2017
• Engaged SC-228 WG2 Members in meetings discussing: 1. Near Far Problem 2. Adaptive Coding + expansion of MOPS coding schemes 3. MIMO Techniques as solution to Near-Far Problem	July 2017
• Completed BER evaluation with Narrowband and Wideband Jammer	August 2017
• Final Report	December 2017

3. TECHNICAL DESCRIPTION

3.1 C2 DATA LINK MOPS OVERVIEW AND TESTBED BUILD

The first three months of this project were focused on communicating with FAA engineers and industry partners to characterize operational constraints surrounding existing UAS technology. An in depth literature review was completed focusing on the current state of UAS technology, with special emphasis on standards currently in place to ensure the security of the physical layer. As part of this review we examined the 'Command and Control (C2) Data Link Minimum Operational Performance Standards (MOPS) for Verification and Validation (Terrestrial)' [1] document released on April 1st, 2016 by Special Committee 228.

At the end of the three month study period, MOPS requirements relevant to the construction of the CNPC physical layer were extracted and used to identify necessary hardware and software capabilities for C2 waveform links. Subsequently, we proceeded with the development of a flexible testbed. This testbed was then validated for the four baseline waveforms described in the MOPS, before expanding its capabilities to permit testing of interference scenarios of primary interest to this study.

3.1.1 Key CNPC Physical Layer Requirements from MOPS

The CNPC physical layer requirements fall into two categories: (1) Baseline MOPS Requirements, and (2) System Manufacturer Requirements. The baseline conditions were developed by industry partners and SC-228 members for verification & validation of the MOPS document. These baseline MOPS can be adopted by manufacturers who develop radios for use in communication networks intended for CNPC operation within the National Airspace System (NAS). However, system manufacturers are provided with greater flexibility to create their own waveform standards for use with CNPC radios, provided they comply with standards set in the MOPS. A table summarizing both sets of requirements is provided in Table 3.

A key aspect of the transmitted waveforms is compliance with a 50 millisecond time-division duplex (TDD) frame structure. This TDD structure divides all data into message packets. Notably, the 50 ms TDD frame is comprised of two 23 ms subframes used for uplink and downlink transmission, and includes guard times to protect against potential timing delays. Uplink refers to communication from the ground transmitter to the airborne receiver while downlink describes transmission that originates at the airborne transmitter and is received by the ground receiver. Figure 1 below depicts this TDD frame structure.

Table 3: Key CNPC Link Requirements

Specifications	System Manufacturer	Baseline MOPS Requirements
Operational Freq.	C band –[5030 5091 MHz]	C band –[5030 5091 MHz]
Max Load VSWR	Not Specified	2:0:1
TX Output Power	0.5 Watts to 10 Watts	100mW or less in low power mode 10W or less in high power mode
Max Input RX Input	-30 dBm to +20 dBm	-10dBm (shall not exceed +20dBm)
Airborne RX Sensitivity	-126 dBm to -96 dBm	-118 dBm to -114 dBm
Ground RX Sensitivity	-126 dBm to -96 dBm	-119 dBm to -113 dBm
Multiplexing Tech.	Uplink[TDMA] Downlink [FDMA]	Uplink [TDMA] Downlink [FDMA]
Duplexing Structure	TDD – 50 ms (24.3 for Uplink;25.7 for Downlink)	TDD – 50 ms (24.3 for Uplink;25.7 for Downlink)
Symbol Rate	5 to 500 ks/s	34.5 to 138 ks/s
Modulation Type	1 to 3 bits per symbol	1 bits per symbol – GMSK Modulation Index = 0.5, BT=0.2
Freq. Capture Range	0 to ±15 kHz	0 to ±15 kHz
Doppler Correction Range	0 to ±15 kHz	0 to ±15 kHz
RF Power Rise Time	Not Specified	4 symbol periods starting prior to the beginning of each of the uplink and downlink TDD sub frames
RF Power Fall Time	Not Specified	4 symbol periods for data class 2&4 4.5 symbol periods for data class 1&3
Modulation Distortion	Not Specified	5 degrees rms or 20 degrees peak

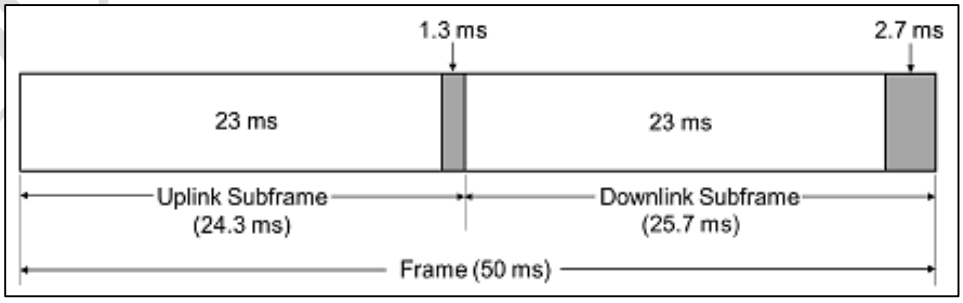


Figure 1: 50 ms TDD Frame Structure

The remaining portion of these requirements include channel correction codes used for these communication links. These are discussed in the Preliminary Signal Analysis section of the report. MOPS define four data frame structures, each having different message size, bandwidths and symbol rates. The key characteristics defining each of these four data classes are provided in Table 4.

Table 4: Baseline Data Class Characteristics

Parameter	Data Class 1	Data Class 2	Data Class 3	Data Class 4
Total Symbols	790.5 sym	1584 sym	2376.5 sym	3173 sym
Data Segment	622 bits	1352 bits	2112 bits	2846 bits
Data Payload	384 bits	832 bits	1312 bits	1760 bits
Slot Duration	23 ms	23 ms	23 ms	23 ms
Symbol Rate (ksym/sec)	34.5	69	103.5	138
Channel Bandwidth	30 kHz	60 kHz	90 kHz	120 kHz
Modulation	GMSK	GMSK	GMSK	GMSK
Bits/Symbol	1	1	1	1
BT Product	0.2	0.2	0.2	0.2

3.1.2 Testbed Build and Validation Tests

After extracting the key CNPC link requirements, the focus shifted to replicating MOPS baseline CNPC links to model single UAV operation for point-to-point communication. A software simulation model was created along with a hardware testbed to perform testing of the MOPS waveforms in addition to signal and channel analysis using developed post-processing capabilities. The main components of the hardware testbed consists of the following equipment:

- Keysight PXB Baseband Generator and Channel Emulator (Model: N5106A)
- Keysight MXG Vector Signal Generator (Model: N5182A)
- Keysight PXA Signal Analyzer (Model: N9030A)
- Keysight Infiniium High Definition Oscilloscope (Model: DSO9204H)
- National Instrument Software Defined Radios (SDR)

A diagram illustrating the hardware setup of the assembled testbed is shown in Figure 2, while a picture of this equipment used in this setup is provided in Figure 3. The available SDRs used over the course of this project are pictured in Figure 4. Finally, for Figure 5 illustrates the hardware testbed in use to replicate a communication signal. Notably, this testbed permits evaluation of all existing CNPC links at C band along with security schemes proposed during Phase 1 of this research.

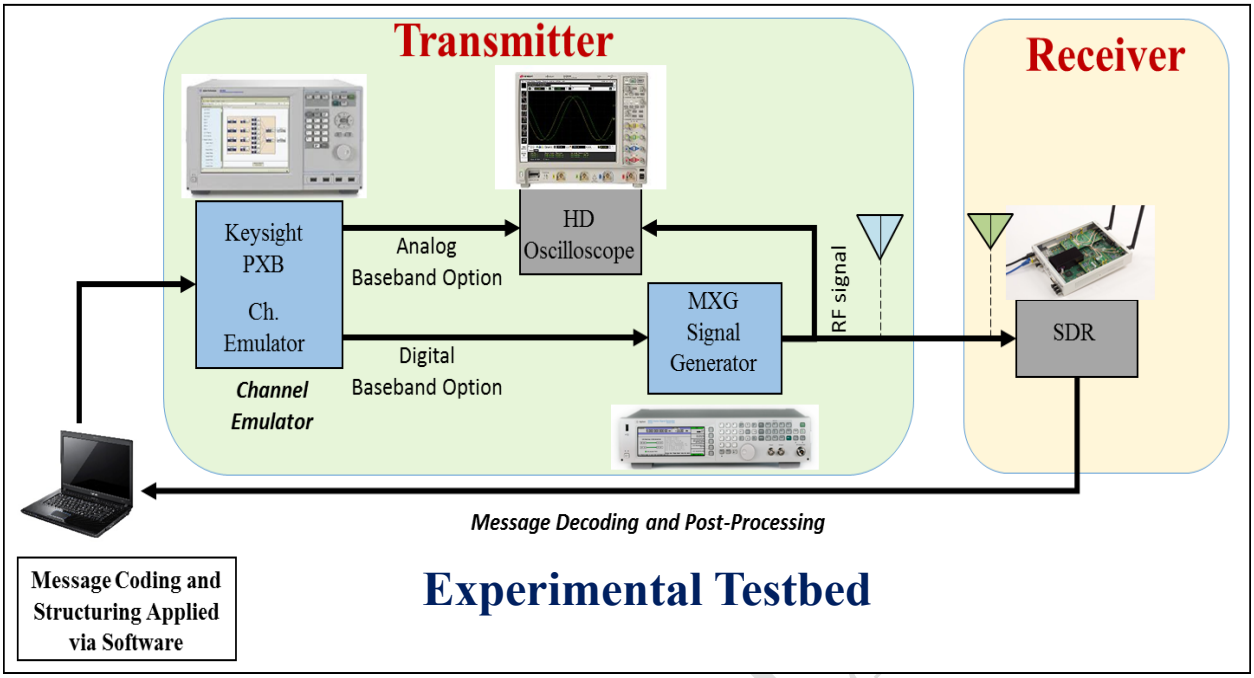


Figure 2: Overall Testbed Block Diagram

Figure 3: Hardware Testbed Setup

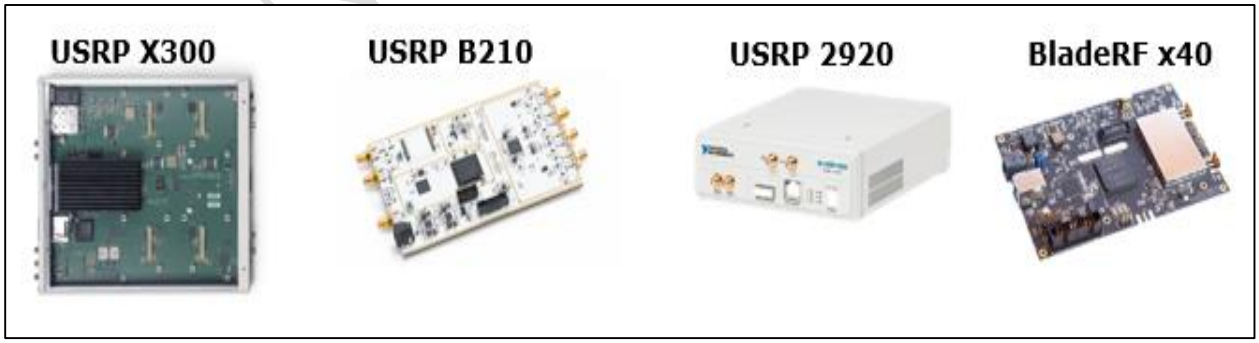


Figure 4: Available SDRs used to emulate and capture CNCP waveforms in C2 link

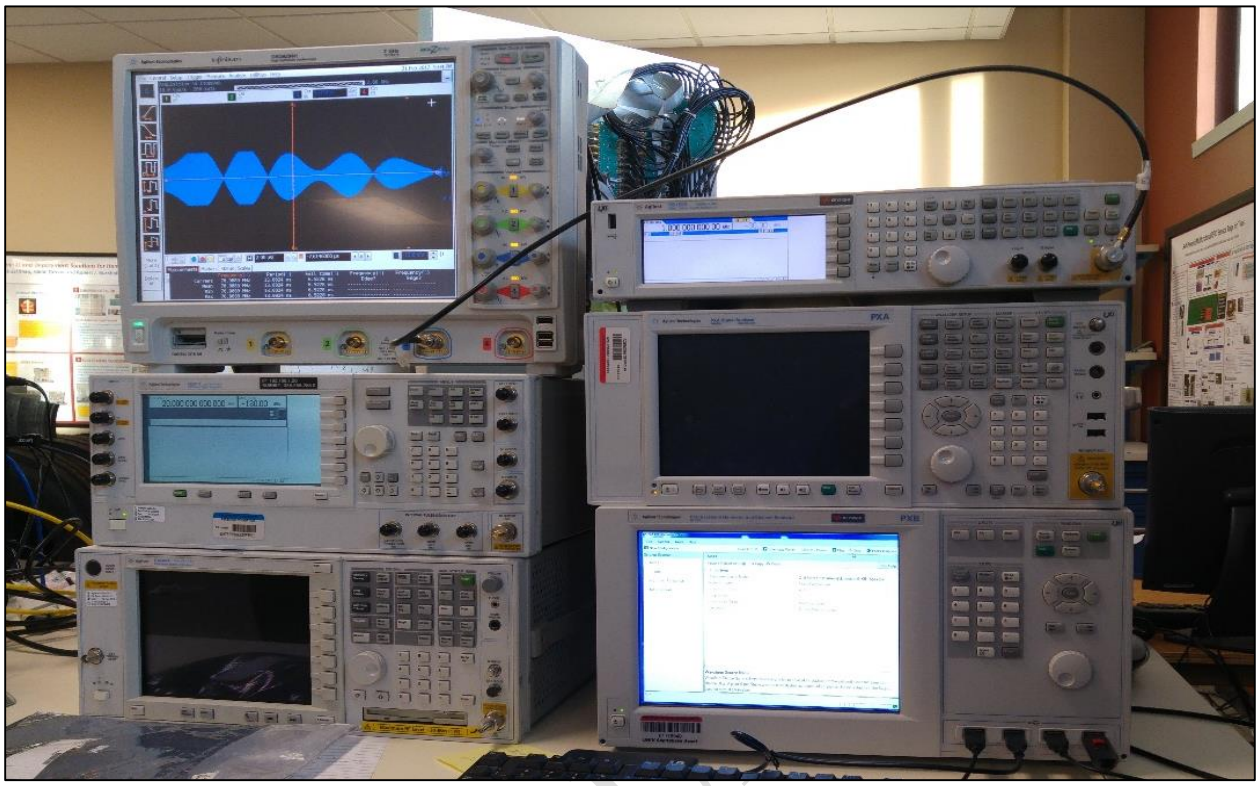


Figure 5: Hardware Testbed in use to Generate CNPC waveforms

In the setup provided in Figure 2, the message is created, conditioned and coded to meet the waveform requirements. Subsequently, the waveform is transferred to the channel emulator where a baseband signal is generated and up-converted to C band using the vector signal generator. This latter RF signal is then transmitted by sending it to an antenna. The RF signal is examined with the aid of an HD oscilloscope and a Signal Analyzer.

The receiver consists of one of many available SDR boards used to capture the RF signal and down-convert it to baseband for post processing. The final step in this process is to employ post-processing techniques to decode the message and complete signal analysis. It is important to note that the testbed has flexibility to be used for both wired and wireless communication by swapping RF cables with antennas. Additional capabilities of this testbed are considered in the Testbed Capabilities section of this report.

To validate the performance of our testbed, the C2 link was tested using all four data classes described in the MOPS. The initial testing consisted of the generation, transmission, and reception of custom messages using each of the four baseline MOPS data classes. The figure of merit for this simple experiment was reliable message recovery while adhering to the TDD frame structure. Ultimately, each of the subframes were tested at 5.06 GHz, the center of the allocated C band. Notably, each message was accurately received, decoded and recovered, thus, completing our initial testbed validation. Again, the goal of this validation test was to demonstrate our capability to reliably implement the CNCP link in point-to-point configurations.

3.2 TESTBED CAPABILITIES

The current testbed allows us to accurately replicate baseline MOPS communication links. However, it expands our testing to additional Modulation and Coding Schemes (MCS) that satisfy the MOPS system manufacturer requirements. Both of these capabilities have already been demonstrated for the four baseline data class waveforms. Future capabilities that will be integrated into the current testbed include introduction of: (1) Jamming and Channel Interference, (2) Fading and Multipath, and (3) Multiuser as well as MIMO communication. The envisioned testbed setup that will be used to emulate each of these capabilities is discussed below:

3.2.1 Jamming and Channel Interference

In order to assess the vulnerability of current C2 links to multi-user interference and various jamming techniques, a few modifications were required to accommodate the addition of these undesired signals. For these scenarios, available hardware was used to emit arbitrary signals and bursts of noise within the spectrum occupied by a user. These undesired signals degrade the performance of the system by causing link losses, packet delays and throughput reduction. A block diagram of the envisioned hardware setup is shown in Figure 6.

The Hardware testbed can accommodate 3 different configurations that allow for injection of undesired interfering signals.

1. Generate using secondary signal generator and couple directly to channel
2. Generate using secondary signal generator and input into Channel Emulator
3. Create in MATLAB and input into Channel Emulator

Each configuration has unique advantages of the others, and can be used to serve different purposes. Preliminary validation was completed for all configurations to verify their functionality.

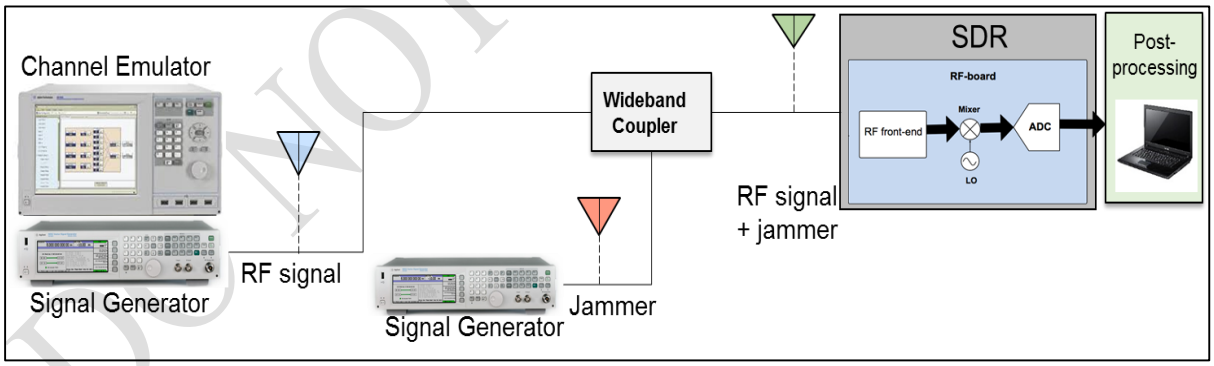


Figure 6: Testbed Setup – Jammer and Channel Interference

A short experiment was designed to demonstrate and validate the setup in Figure 4. Specifically, an undesired single tone jammer was coupled to a generated CNPC waveform. The resulting RF spectrum at various points throughout this experiment is shown below.

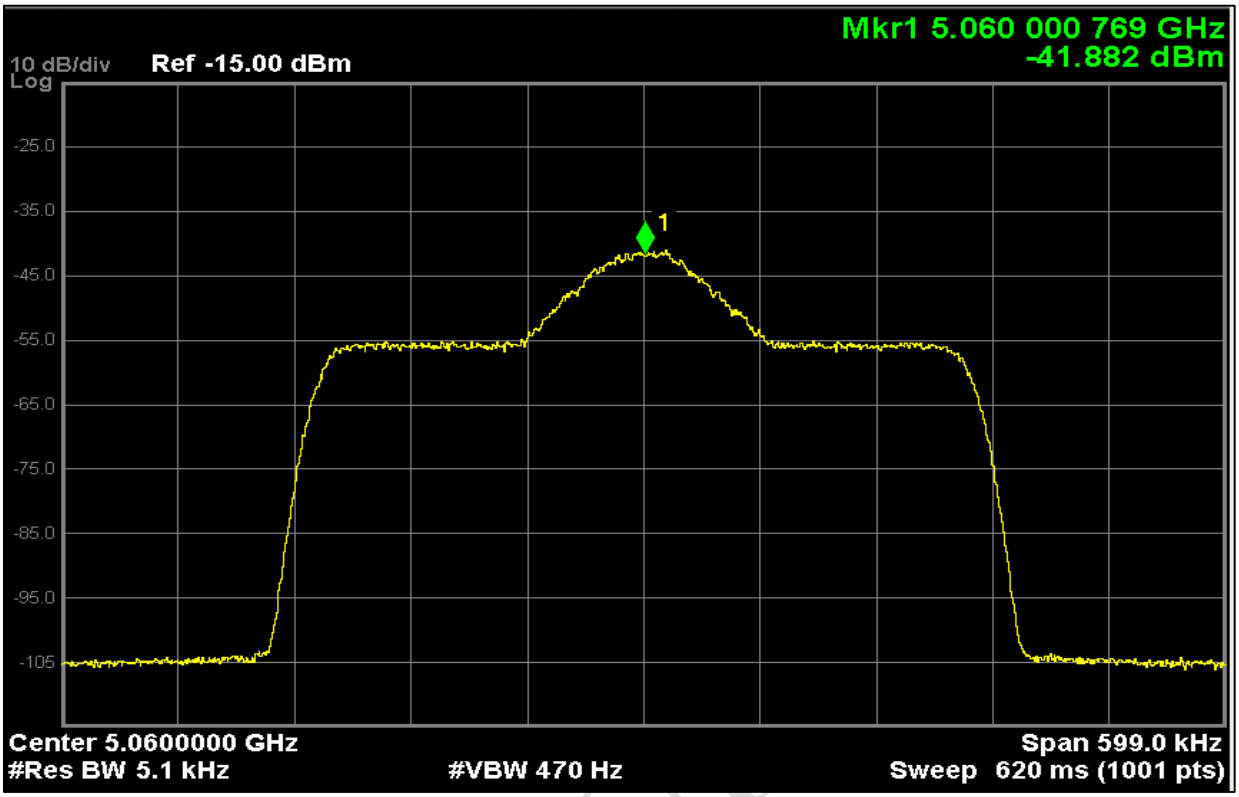


Figure 7: Data Class 4 Signal with the channel noise floor at – 55 dBm

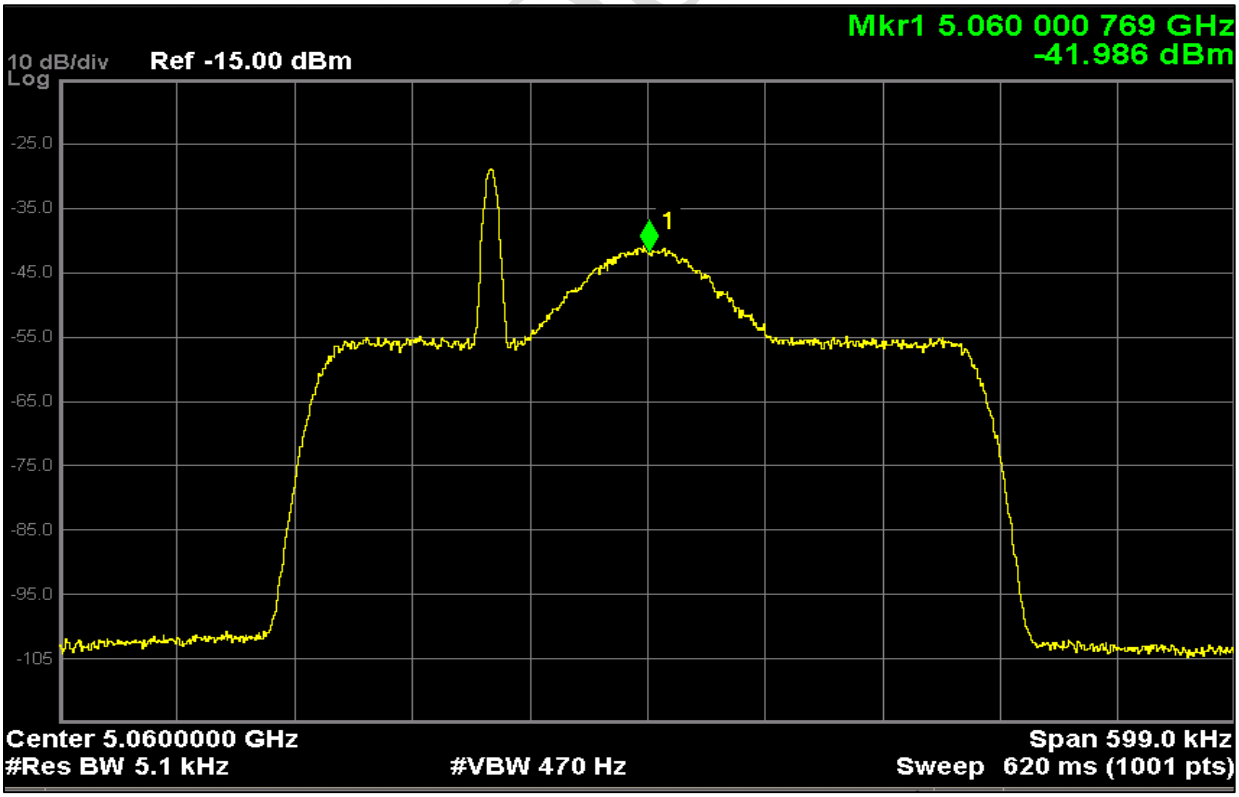


Figure 8: Data class 4 signal in presence of an out-of-band single tone jammer

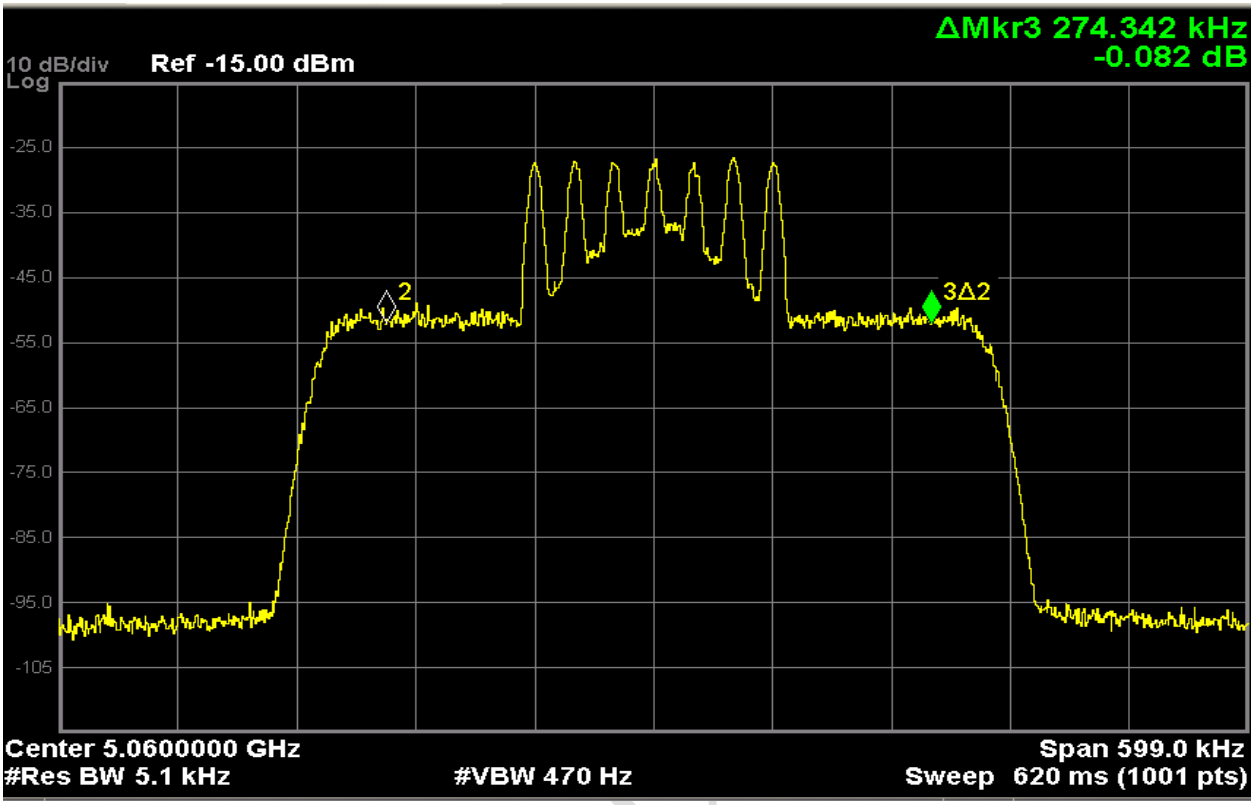


Figure 9: Data class 4 signal (coupled) with swept single tone jammer

Figure 7 represents a CNCP waveform that was created using data class 4, and transmitted at 5.06 GHz with high enough SNR to distinguish the signal from the channel noise floor. In Figure 8 a single tone jammer is introduced just outside the occupied bandwidth of the signal. Figure 9 depicts the CNPC waveform as the single tone jammer is swept across the occupied channel bandwidth.

This simple experiment confirmed our capability to introduce undesired interferers into the communication link using this modified testbed configuration. With the aid of this initial hardware configuration, we were able to expand our signal processing capabilities for further link/signal/channel analysis to aid in our security evaluation.

3.2.2 Fading and Multipath

Initial testbed capabilities were also expanded to study the effects of multipath signals on the communication link. The purpose of this expansion was to create a platform that could be used to determine how fading conditions affect performance. Additional parameters that are examined include: Doppler spread, propagation path loss, as well as frequency and phase mismatch. A block diagram of this multipath fading setup is provided in Figure 10.

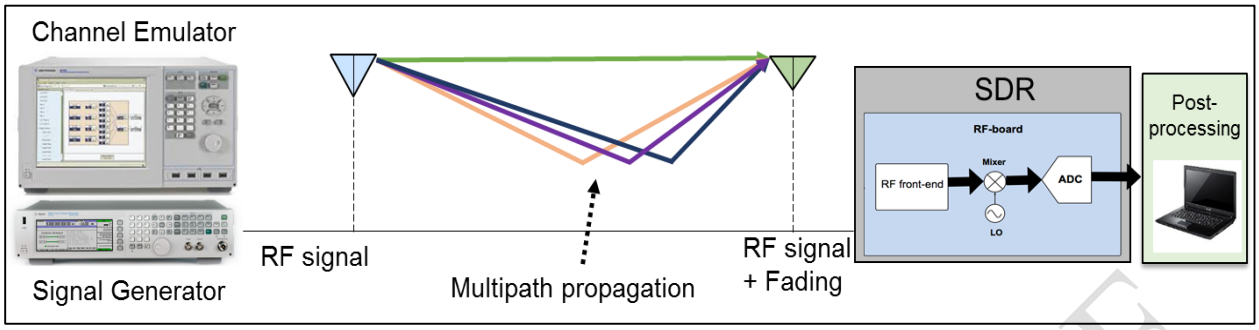


Figure 10: Testbed Setup – Fading and Multipath

3.2.3 Multiuser Communication and MIMO Techniques

Multiuser communication capabilities were also integrated into our testbed. In this effort, MIMO capabilities are implemented at the ground station to exploit beamforming and suppress multiuser interference. MIMO allows for improved security in high data rate environments. In this context, our channel emulator can be used to generate up to 4 baseband channels for MIMO applications. Multiple multi-channel SDRs at the receiver are used for signal capture and post processing. A block diagram of the setup is shown in Figure 11.

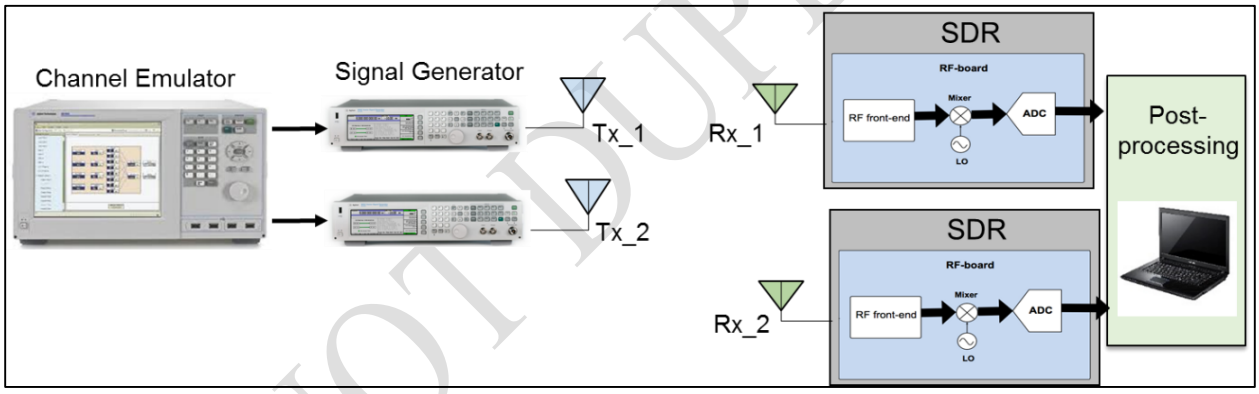


Figure 11: Testbed Setup – Multiuser and MIMO communications

3.3 SYNCHRONIZATION AND RECEIVER DESIGN

Modifications were made to the software algorithms to account for inherent hardware and channel impairments. The corrections were introduced in anticipation of the jamming/interference studies that were carried out during the second half of this project.

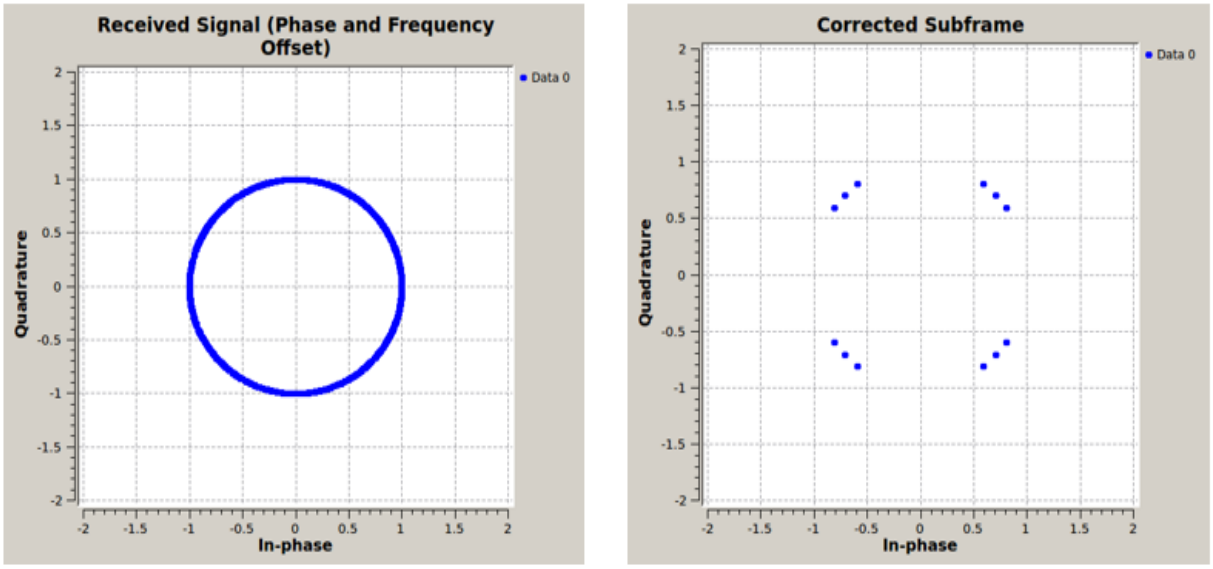
3.3.1 Frame Synchronization Algorithm

We implemented a frame synchronization algorithm using the concept of cross-correlation. In essence, the received signal is cross-correlated with a pilot signal, known to both the transmitter and receiver in order to recover the subframe from the received signal. The pilot-aided frequency and phase offset estimation and correction algorithm is subsequently carried out to correct for offsets caused by hardware synchronization limits and channel impairments. Once the subframe is recovered using our frame synchronization algorithm, the original and recovered pilot signals are

used to estimate the offsets. After estimating these offsets, they are applied to the subframe for correction.

3.3.2 Test Results - Frequency and Timing Synchronization

Correctly estimated and corrected Timing, Frequency and Phase offsets introduced by hardware setup and the channel. These offsets were estimated and used to correct the received subframe with the aid of the algorithms described above. All four data classes were tested and screenshots of this experiment using a data class 4 generated message are given in Figure 12.



(a) (b)

Figure 12: Received Signal with (a) Offsets and (b) Corrected Sub-frame for Data Class 4 Message

3.4 PRELIMINARY SIGNAL ANALYSIS

3.4.1 Bit Error Rate (BER) for Un-Coded Transmission

BER performance evaluation for an un-coded transmission was performed using the data class 4 sub frame structure in MATLAB and in practice. Figure 13 shows the BER curve for the un-coded signal transmission as compared to the theoretical curve for GMSK. Figure 13 also shows the power spectrum at low and high SNR values.

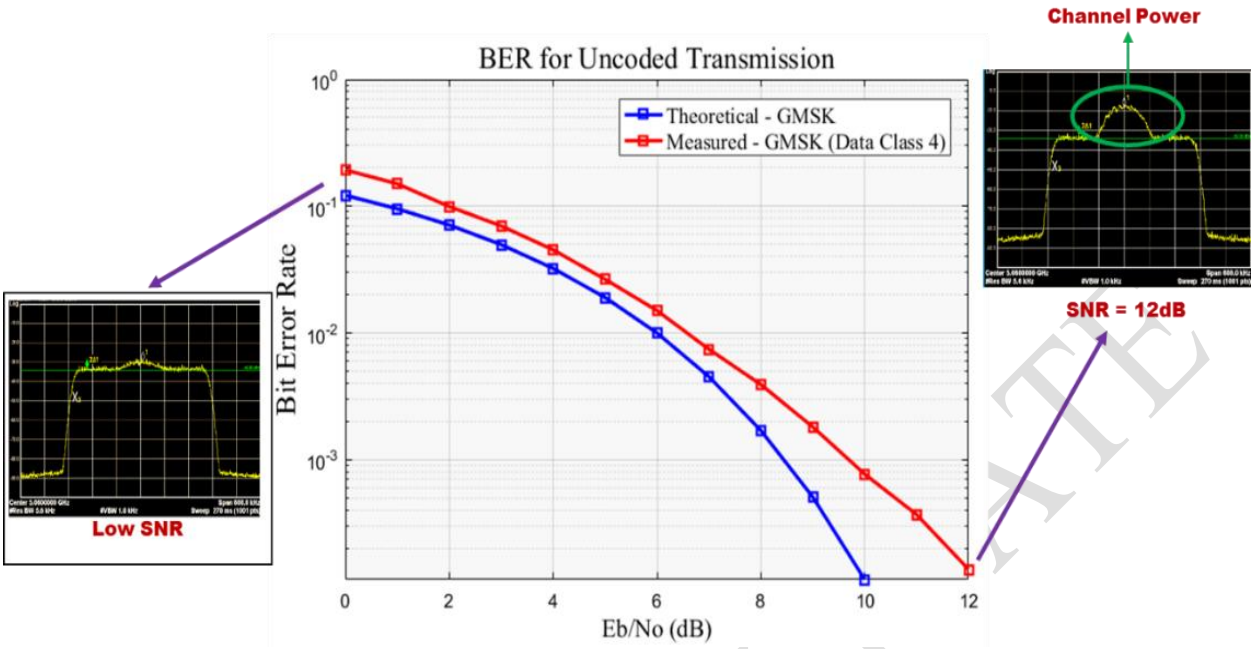


Figure 13: BER curve of Un-Coded Transmission

Figure 13 plots the BER as a function of Eb/No. Eb/No is the normalized signal-to-noise (SNR) measure, also known as the "SNR per bit" given by:

$$\frac{Eb}{No} = \frac{S}{N} \times \frac{Bn}{Rb} \quad (1), \text{ where:}$$

Eb: Energy per bit
No: Noise power spectral density
Bn: Channel bandwidth
Rb: Channel data rate (net bitrate)
S: Signal Power
N: Noise Power

For the experiments, we used Bn=138 kHz and Rb=138 kbps with Bn fixed for the coded and un-coded transmission, but Rb can be varied. As expected, the un-coded transmission gives poor performance as compared to the theoretical curve.

3.4.2 BER for Coded Transmission

Figure 14 illustrates the block diagram for the coded transmission.
To assess the BER performance using coded signals, the baseline MOPS defined Turbo Coding was used at rate 1/3. The coding operation includes steps like Turbo Coding of message bits to be transmitted and puncturing of the coded data. The idea of puncturing is to delete some bits in the coded bit sequence by following a fixed pattern. A 30 bit puncture pattern was used in the baseline MOPS. After puncturing, interleaving was performed on the punctured data. The last step involves pseudo-random overlay of the interleaved data. After the message is coded, the sub-frame is constructed based on requirements dictated by the MOPS. Subsequently, this coded signal is modulated using the GMSK scheme before transmission.

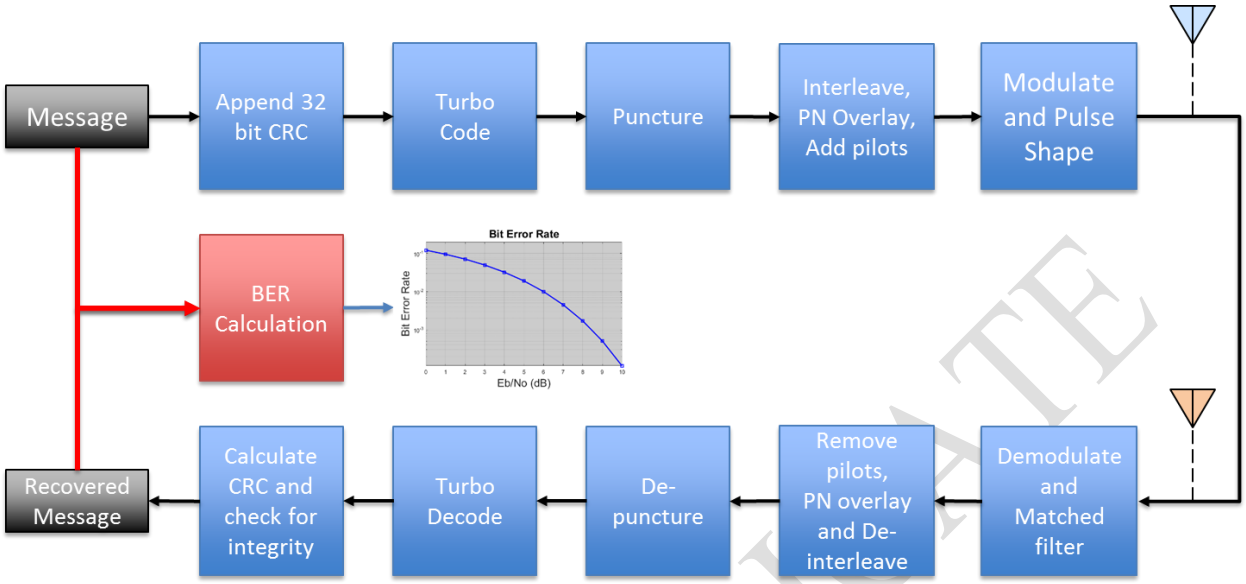


Figure 14: Block Diagram of Coded Transmission

At the receiver, the signal was demodulated and then decoded. The decoding process is the reverse as the coding process. The step by step procedure for decoding is as follows:

1. Demodulated data is XOR'ed with the same pseudo-random sequence used at the transmitter
2. Data from the previous step is passed through the de-interleave algorithm
3. De-interleaved data is then passed through the de-puncturing algorithm
4. De-punctured data is then passed through the turbo decoding algorithm to extract the message bits
5. Cyclic Redundancy Check (CRC) is calculated for the recovered message bits to ensure message integrity

3.4.3 Extension to Frame Error Rate (FER)

Similar to the BER, which used to quantify the performance of communication systems, Frame Error Rate (FER) is another metric that can be employed when applicable. The FER is defined as the ratio of frames received with errors to total frames received. It is used to determine the quality of a signal connection and is defined by the following relationship:

$$FER = \frac{Number\ of\ Frames\ in\ Error}{Total\ Number\ of\ Frames\ Received}$$

Hence, to determine if a given frame is in error, a CRC check of that frame is performed at the receiver to check if there is an error. A sum of total number of frames in error is accumulated to calculate FER at a given SNR value. The normative subframe error rate requirement is defined as 1x10^-3 in the MOPS [1]. However, this requirement varies depending on the operating environment of the radio link. Factors discussed in the MOPS that affect this value include: the

received signal strength, magnitude of fading applied on the channel and the operating terrain, altitude and range.

To demonstrate our capabilities to complete performance evaluations using FER as a figure of merit, a few simulations were completed adhering to MOPS baseline requirements. More specifically, the simulation conditions employed for this evaluation are described in Table 5.

Table 5: Simulation Conditions for Frame Error Rate Performance Evaluation

Simulation/Coding Parameter	Value
MOPS Data Class	Class 4
Modulation	Baseline GMSK
Code Rate	Baseline 5/8 Turbo Code
Delay Elements	3
Generator Polynomial	Constant
Decoding Iterations	6

FER vs SNR curves for all data classes are plotted below and 10,000 frames were transmitted and evaluated to generate a response at each desired SNR value. **Error! Reference source not found.** depicts the results of these simulations.

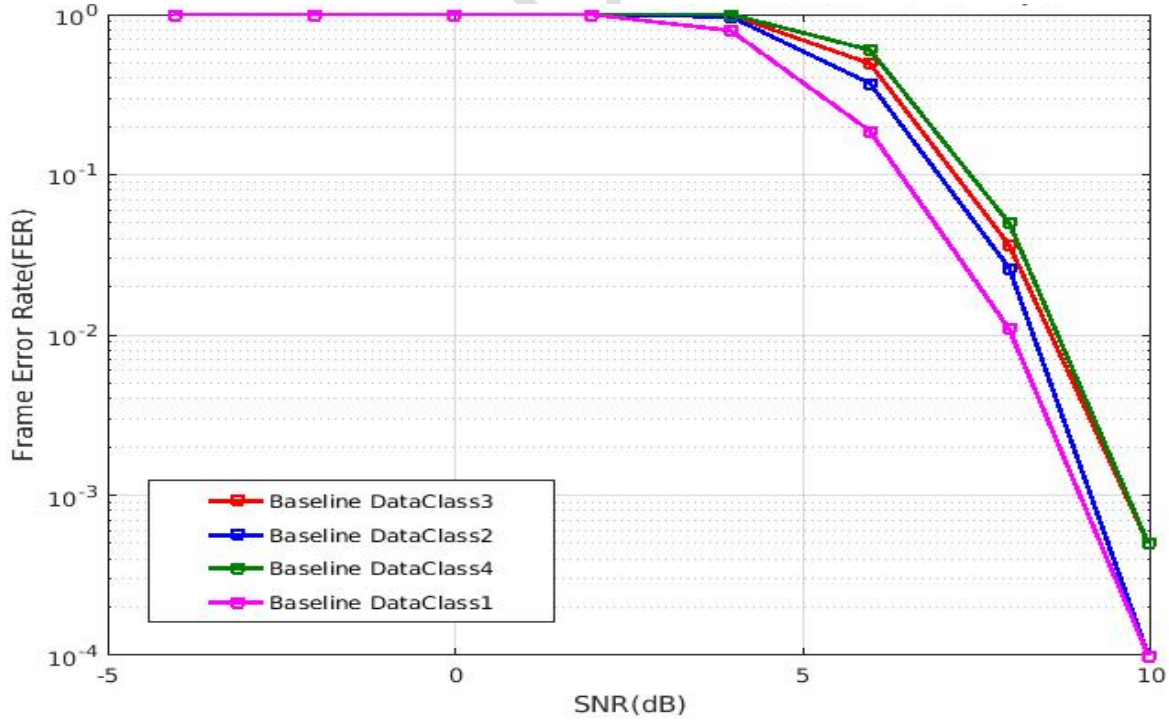


Figure 15: FER curves for all four baseline waveforms

The performance of different data classes are nearly identical when operated at the same code rate. The only difference in these scenarios stems from the different frame lengths of the data classes. Due to the effects of the interleaver used in the turbo encoder, randomness increases when the frame size gets larger. The degrading performance of larger data classes was attributed to the randomness of each data packet. The more randomness the message content within a data class has, the worse FER curve we obtain for this data class. Data class 4 has the largest frame length among the data classes, therefore its FER performance is degraded the most because of its randomness in this specific experiment.

3.4.4 Experiments

BER evaluation for the coded and un-coded transmission was performed using the Data Class 4 sub frame structure. The message used is 1728 bits long. Figure 16 gives the BER vs Eb/No for coded and un-coded transmission.

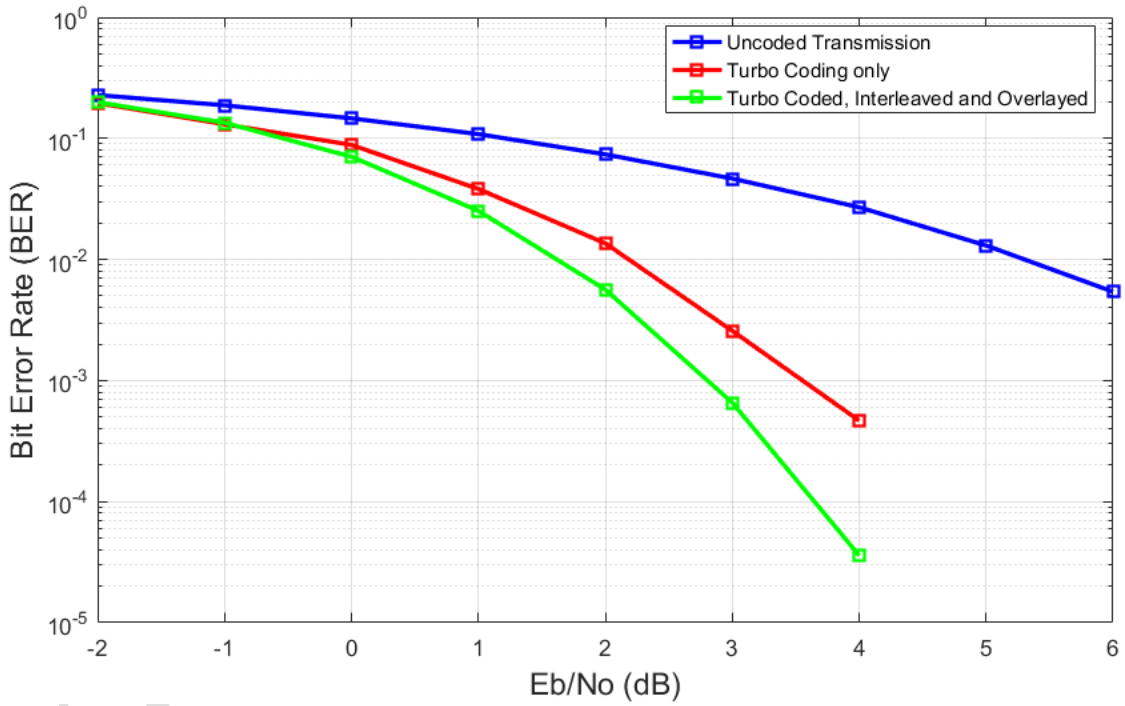


Figure 16: Simulated BER curves for Experiments 1 – 2

When we compare BER curves of uncoded transmission, turbo coded transmission without interleaving and turbo coded transmission with interleaving and overlaying, we see that uncoded transmission gives the worst performance as expected. Interleaving and overlaying slightly increases the performance of turbo coding.

1. Coded Transmission with only Turbo Coding

In this experiment, we compared turbo coded transmitted signals. We observed that BER curve for this experiment outperformed the un-coded signal by at least 3dB. Figure 16 depicts the BER performance curve in red color.

2. Coded Transmission with Turbo Coding, Interleaving and Pseudo-Random overlay

In this experiment, we applied turbo coding with interleaving and pseudo-random overlay. We observed that the BER curve for this experiment outperformed the one where only turbo coding was used. This is because interleaving caused error bursts encountered in the transmission to be spread across multiple code words.

3. Coded Transmission with different Puncture Patterns

A series of experiments were performed using different puncture patterns to observe the BER performance at the receiver. The puncture patterns used for this experiment were selected as follow:

1. Puncture Pattern 279A6D25: Baseline MOPS pattern with 16 bits preserved after puncturing.
2. Puncture Pattern 3FFFFFFF: All bits are preserved after puncturing.
3. Puncture Pattern 35BAEBAE: 20 bits are preserved after puncturing.
4. Puncture Pattern 37DEFDEF: 25 bits are preserved after puncturing.

Figure 17 depicts the BER performance for each of these puncture patterns. We observed that:

1. Puncturing should be uniformly distributed along the message bits to improve BER performance.
2. As more bits are preserved after puncturing, BER performance improves.
3. Puncture patterns that preserves all bits, imply a BER similar to turbo coding alone.

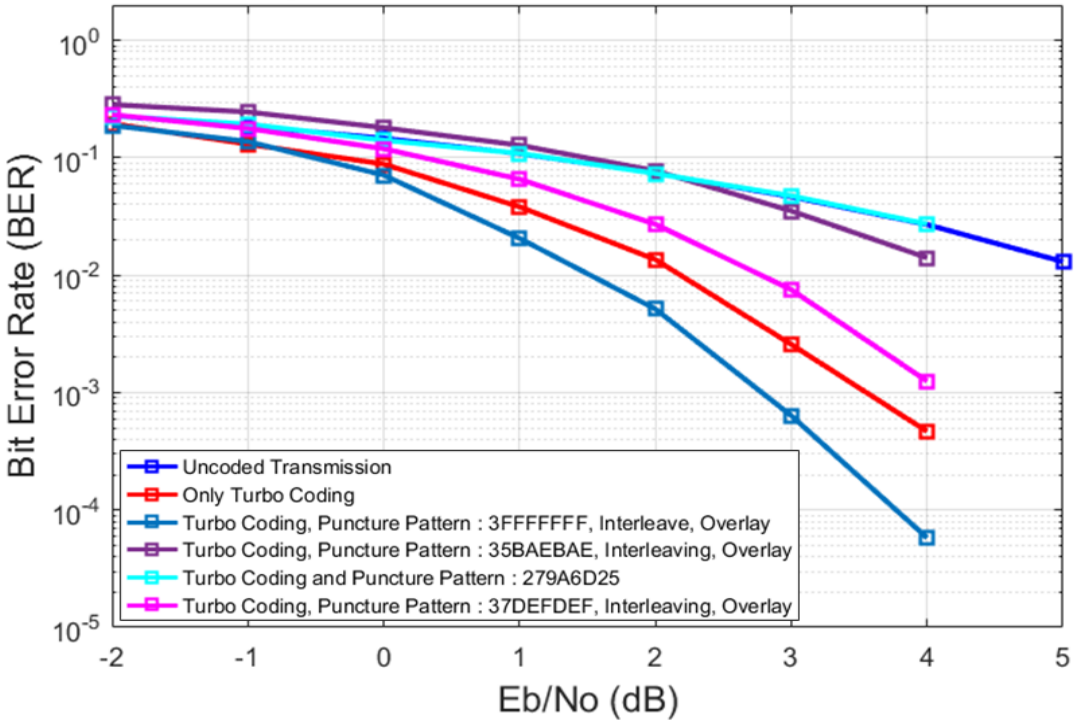


Figure 17: BER Curves for different Puncture Patterns

The above experiments were performed using MATLAB. In the next quarter we will perform these using our hardware testbed and replicate them for various scenarios. This will provide us a baseline for future research.

4. Coded Transmission with different Generator Polynomials Patterns

In this experiment, the generator polynomial used for the turbo encoder is varied. Generator polynomial functions are one of the most important parameters of a Turbo Encoder. Studies in [2] and [3] have suggested that choosing effective generator polynomials would increase the performance of Turbo Codes. Studies also suggested that, for a given constraint length K, there exist few generator polynomials that give optimum BER performance. The effect of these generator polynomials were examined by completing BER performance evaluations for different generator polynomials. The simulation conditions in place for this evaluation are shown below in

Table 6.

Table 6: Simulation Conditions for Generator Polynomial Experiment

Simulation/Coding Parameter	Value
MOPS Data Class	Class 4
Modulation	Baseline GMSK
Code Rate	Baseline 5/8 Turbo Code
Delay Elements	3
Generator Polynomial	Varied
Decoding Iterations	6

The 4 generator polynomials that were selected for use in these simulations are provided below.

1. g1(D) = 1, g2(D) = 1101/1011 = 15/13
2. g1(D) = 1, g2(D) = 1011/1101 = 13/15
3. g1(D) = 1, g2(D) = 1011/1001 = 13/11
4. g1(D) = 1, g2(D) = 1101/1001 = 15/11

The BER performance curves are for each of the examined generator polynomials are included in Figure 18. **In this experiment, 4 different generator polynomials were tested within the turbo encoder. Amongst the 4 generator polynomials tested, generator polynomial 1 resulted in the best performance. This is identical to the structure of the Turbo Encoder defined in the MOPS.**

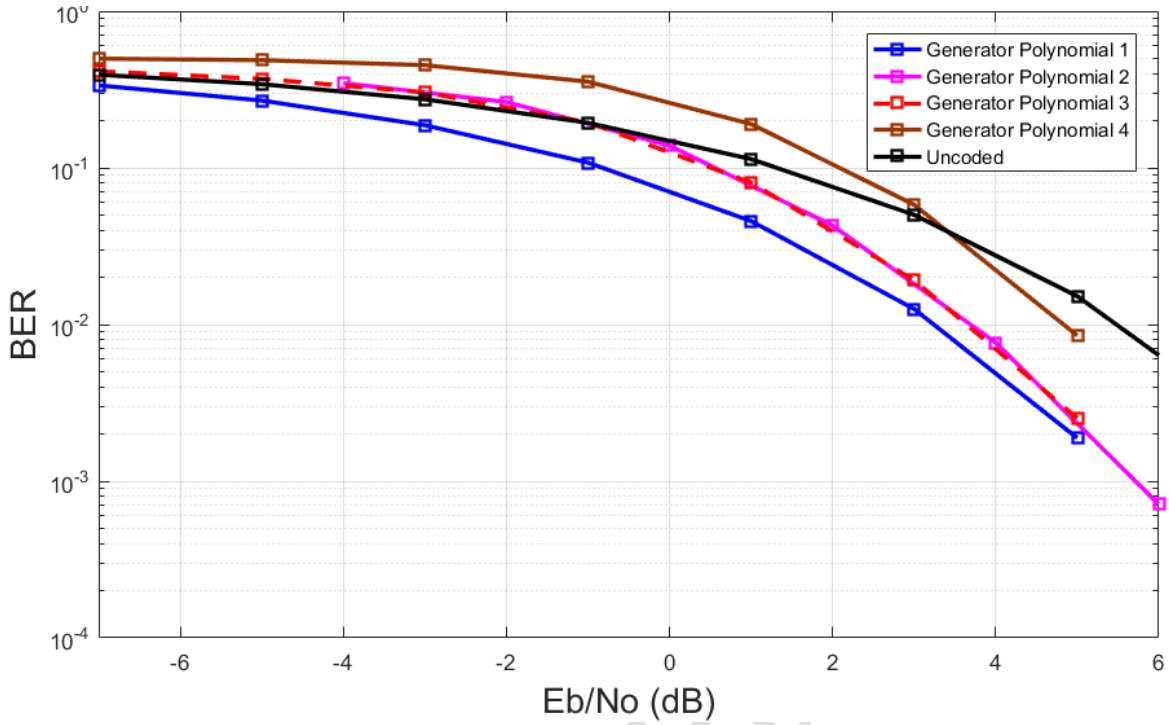


Figure 18: BER Curves for different Generator Polynomials

5. Coded Transmission with different Number of Delay Elements in Turbo Encoder

In this experiment, the number of delay elements used in the Turbo Encoder was varied. Studies in [2] and [4] have suggested that increasing number of delay elements would increase the performance of Turbo codes. However, increasing the number of delay elements increases the decoding complexity and decoding time. It is also important to note that changing the number of delay elements changes the generator polynomial, however, changing the generator polynomial does not necessarily change number of delay elements. The simulation conditions employed to test the effect of varying the number of delay elements are provided in Table 7.

Table 7: Simulation Conditions for Turbo Encoder Delay Elements Experiment

Simulation/Coding Parameter	Value
MOPS Data Class	Class 4
Modulation	Baseline GMSK
Code Rate	Baseline 5/8 Turbo Code
Delay Elements	3, 4, 5
Generator Polynomial	Varies
Decoding Iterations	6

As stated, for each case where the number of delay elements is varied, the generator polynomial used to create the turbo encoder for that specific simulation is varied as well. The BER performance curve for this simulation is shown in Figure 19.

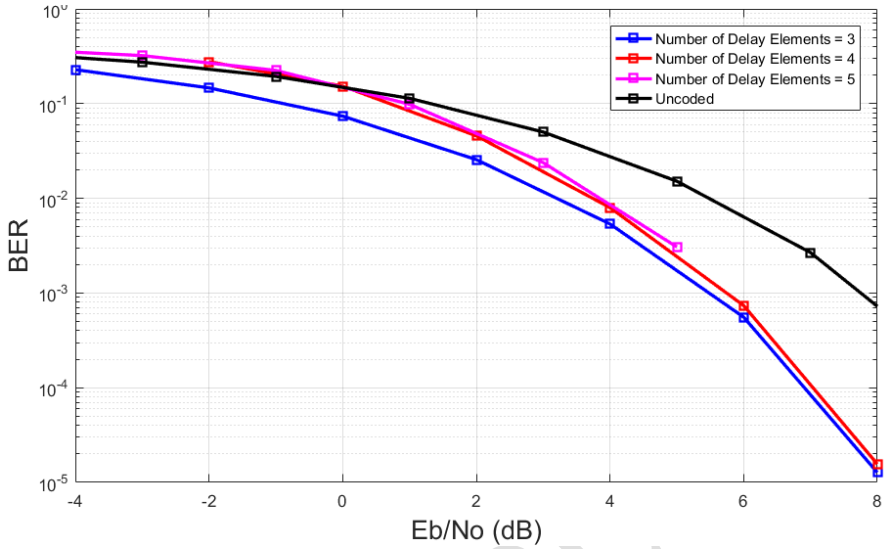


Figure 19: BER Curves for different Number of Delay Elements

After analysis of the BER performances of different turbo encoders using different number of delay elements, it was concluded that 3 delay elements gave the best performance. This is identical to the structure of the Turbo Encoder defined in the MOPS.

4. Coded Transmission with different Number of Decoding Iterations in Turbo Decoder

In this experiment, the number of iterations implemented by the turbo decoder is studied. Turbo Decoders use an iterative decoding process. Studies in [3] and [4] suggested that increasing the number of decoding iterations in an iterative decoding improves the BER performance. However, the improvement in performance for each additional iteration carried out falls as the number of iterations increases. This leads to high number iterations increasing the decoding time and complexity with no significant improvement in performance. So, for complexity reasons usually only about 8 iterations are carried. Figure 20 below illustrates the iterative nature of the turbo decoder used in this study for a 2 stage iterative decoder.

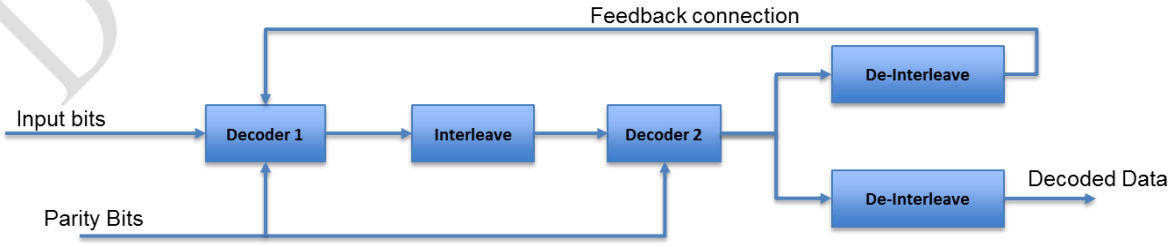


Figure 20: Turbo Decoder with Iterative Decoding

The simulation conditions in place to evaluate the effect of varying the number of decoding iterations is provided below in Table 8.

Table 8: Simulation Conditions for Turbo Decoder Decoding Iterations Experiment

Simulation/Coding Parameter	Value
MOPS Data Class	Class 4
Modulation	Baseline GMSK
Code Rate	Baseline 5/8 Turbo Code
Delay Elements	3
Generator Polynomial	Constant
Decoding Iterations	4, 6, 8, 10, 20

The BER performance curves obtained for this set of simulations are presented in Figure 21.

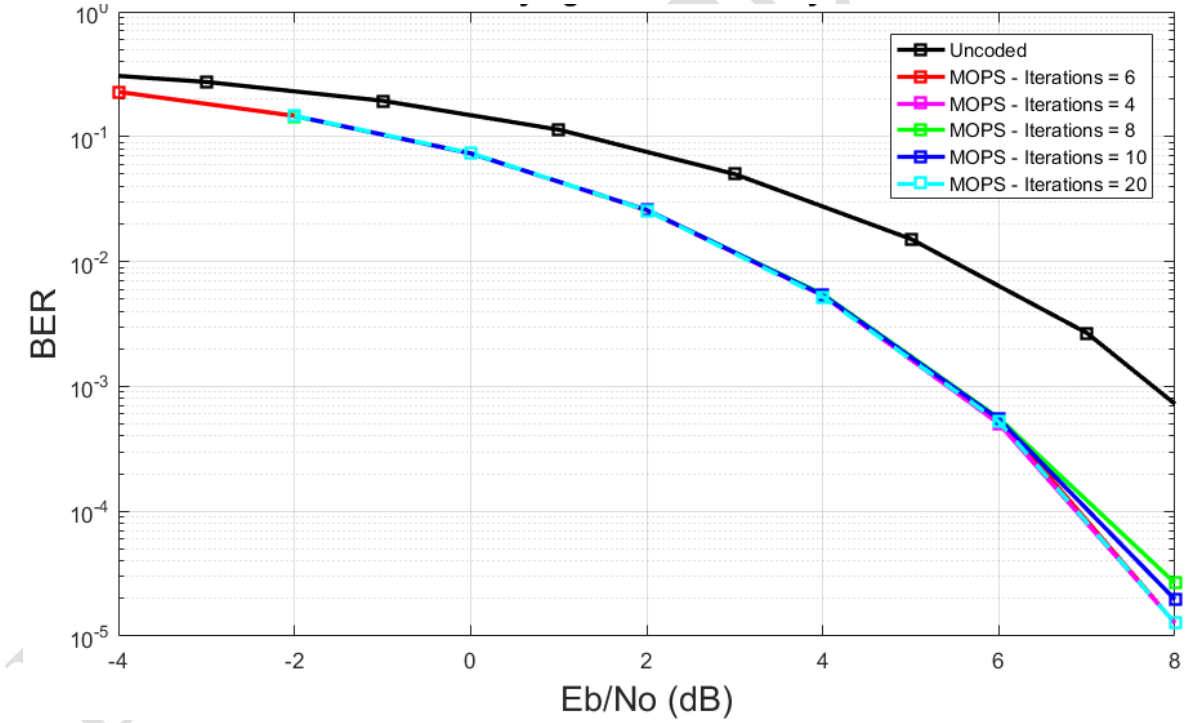


Figure 21: BER Curves for different number of Iterations

In this experiment we tested the number of decoder iterations deployed by the turbo decoder. In our results we saw that increasing the number of decoding iterations did not increase the BER performance. A Turbo decoder with number of iterations of 6 gave the best performance.

3.5 SECURITY EVALUATION OF MOPS WAVEFORMS

3.5.1 Narrowband Jammer

The first jamming scenario examined was that of a proactive single tone narrow band jammer. To do this, we first created accurate software and hardware models to introduce the narrow band jammer into the communication link. Following this, we completed a BER performance evaluation and compared software results with hardware measurements.

The BER performance evaluation was completed for 5 different scenarios representing the jammer power level. These cases along with the corresponding SJR is summarized in .

Table 9.

Table 9: Jammer Cases used for BER performance evaluation of Narrowband Jammer

Case	**SJR (dB)** *(at SNR = 9 dB)*
1	-3
2	0
4	4.5
4	9
5	17.5

For visual illustration these simulation cases are depicted below in Figure 22. The baseline waveform is depicted on the right in blue while the narrow band jammer is depicted on the left in red.

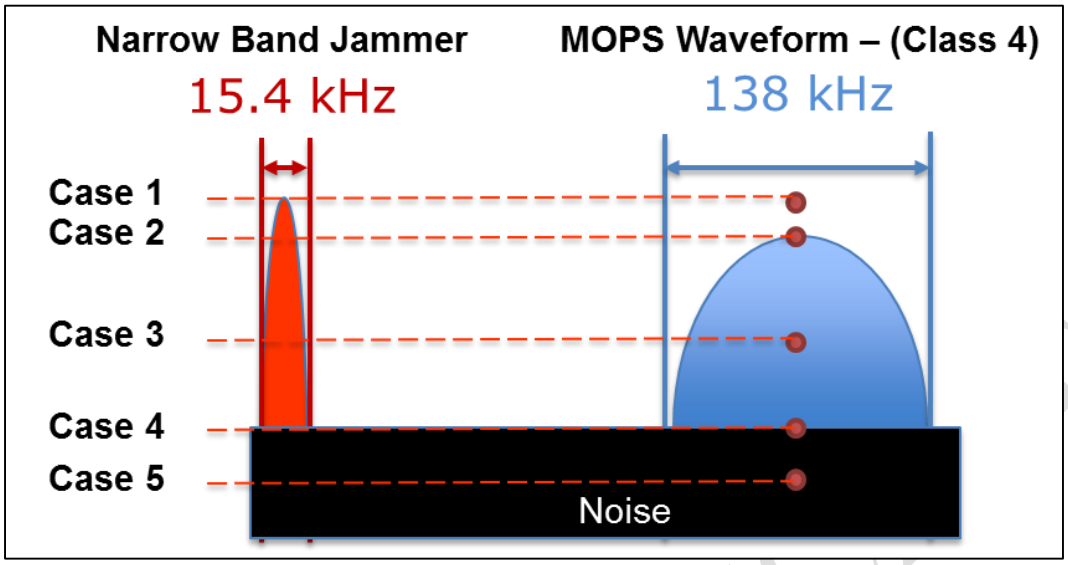


Figure 22: Jammer Cases used for BER performance evaluation of Narrowband Jammer

The baseline data class 4 waveform was used for this initial study. As seen in Figure 22 the 138 kHz bandwidth of this waveform equates to the narrow band jammer occupying roughly 11% of the signal bandwidth when placed within the channel. A software model of this full communication link reflecting this operating scenario was created to perform this interferer assessment. The spectrum response captured at various points in the communication chain is presented in Figure 23.

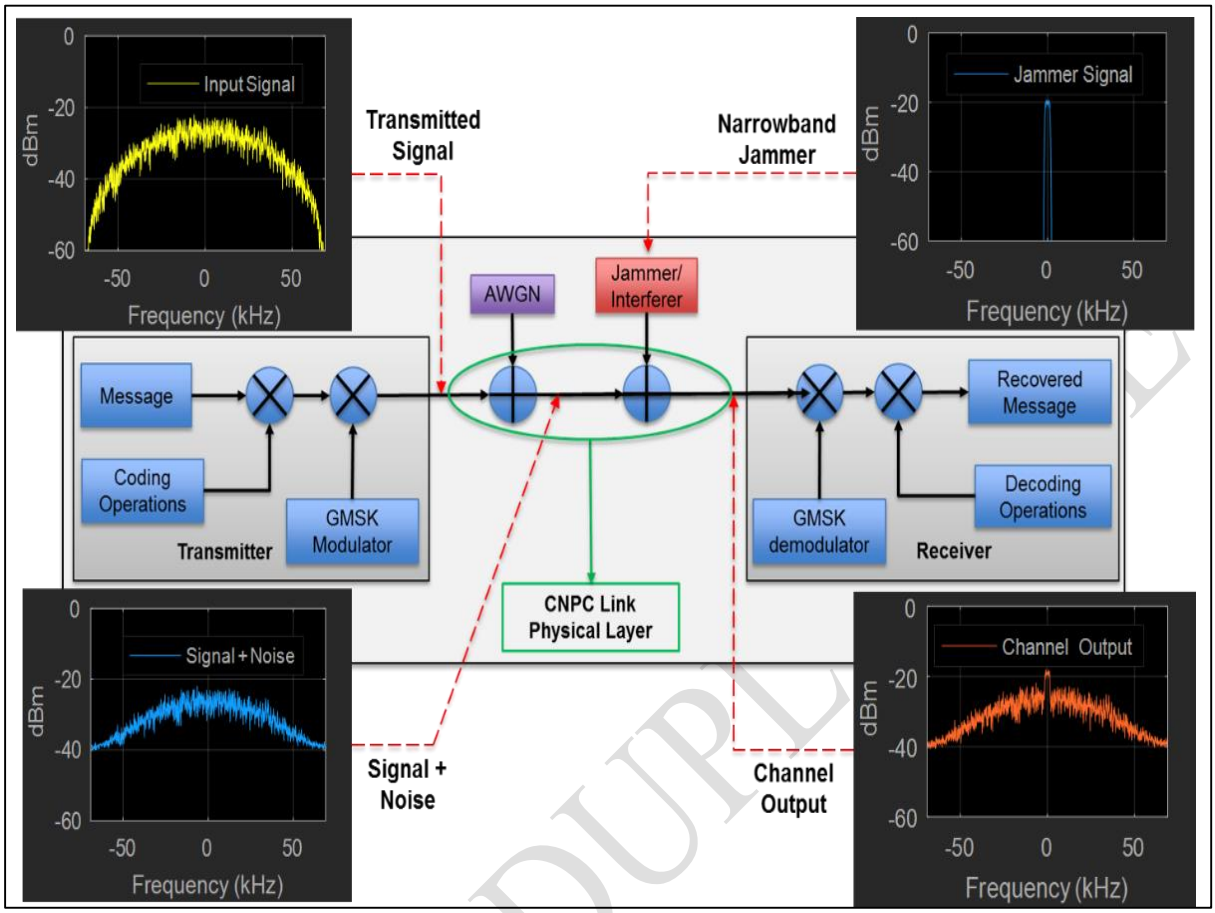


Figure 23: Software Model with Narrowband Jammer and Captured Spectrum Responses

After completion of the software model and examined simulated results, a baseline communication channel was implemented in the hardware testbed described in this report. Figure 24 depicts a narrow band jammer sitting just left of the UAV communication base line channel link described by the MOPS. While Figure 25 below depicts the narrowband jammer inside the communication link. The software MOPS baseline channel model as as well as its implementation into the hardware testbed provided confidence in the path forward and in the capabilities to implement, evaluate and mitigate channel interferers of interest.

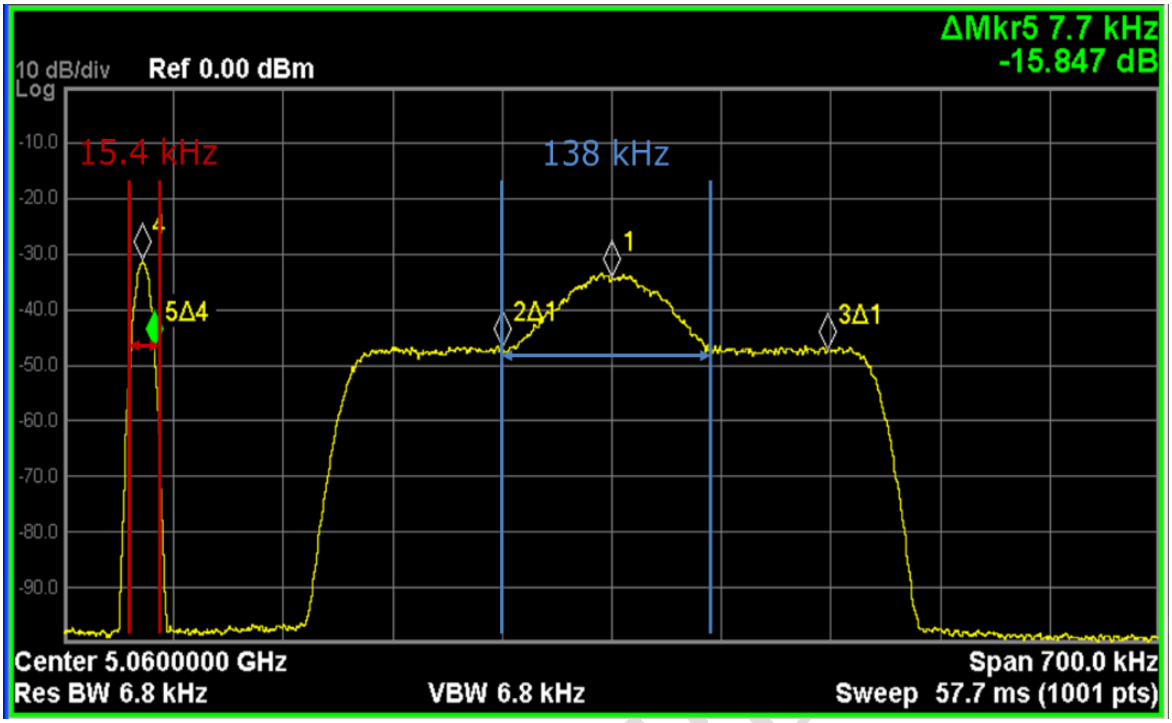


Figure 24: Case 1 Measurement (SJR = -3 dB) with Single Tone Jammer (Outside of Channel)

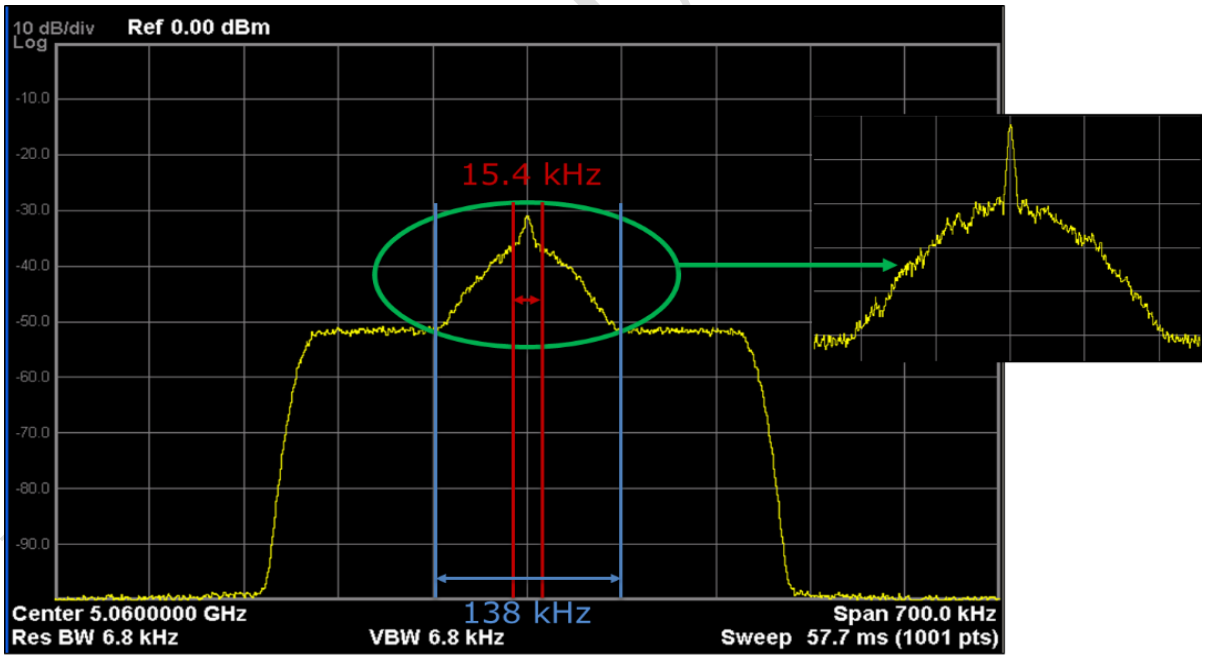


Figure 25: Case 1 Measurement (SJR = -3 dB) with Single Tone Jammer (Inside of Channel)

The next step was to complete an Initial BER performance evaluation of the baseline coded data class 4 waveform in the presence of the Single Tone Jammer. For each BER curve, the jammer power is fixed while the SNR of the waveform is varied over the AWGN channel. Measurement results are compared with simulation results below in Figure 26.

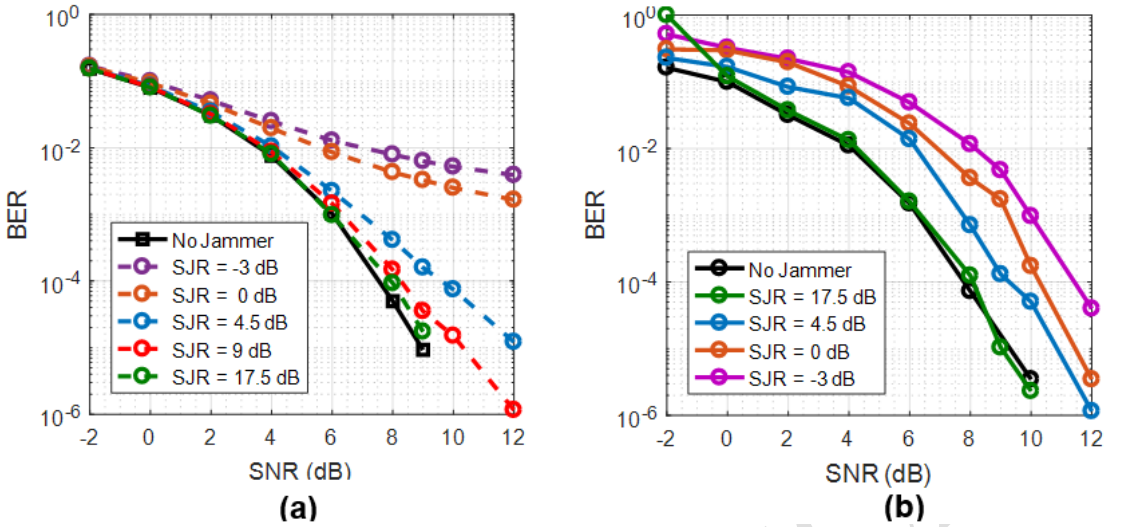


Figure 26: (a) Simulation BER Performance Results. (b) Measured BER Performance Results

For ease of comparison, four of the five cases are isolated in Figure 27 on a case by case representation to compare simulation and measurement results.

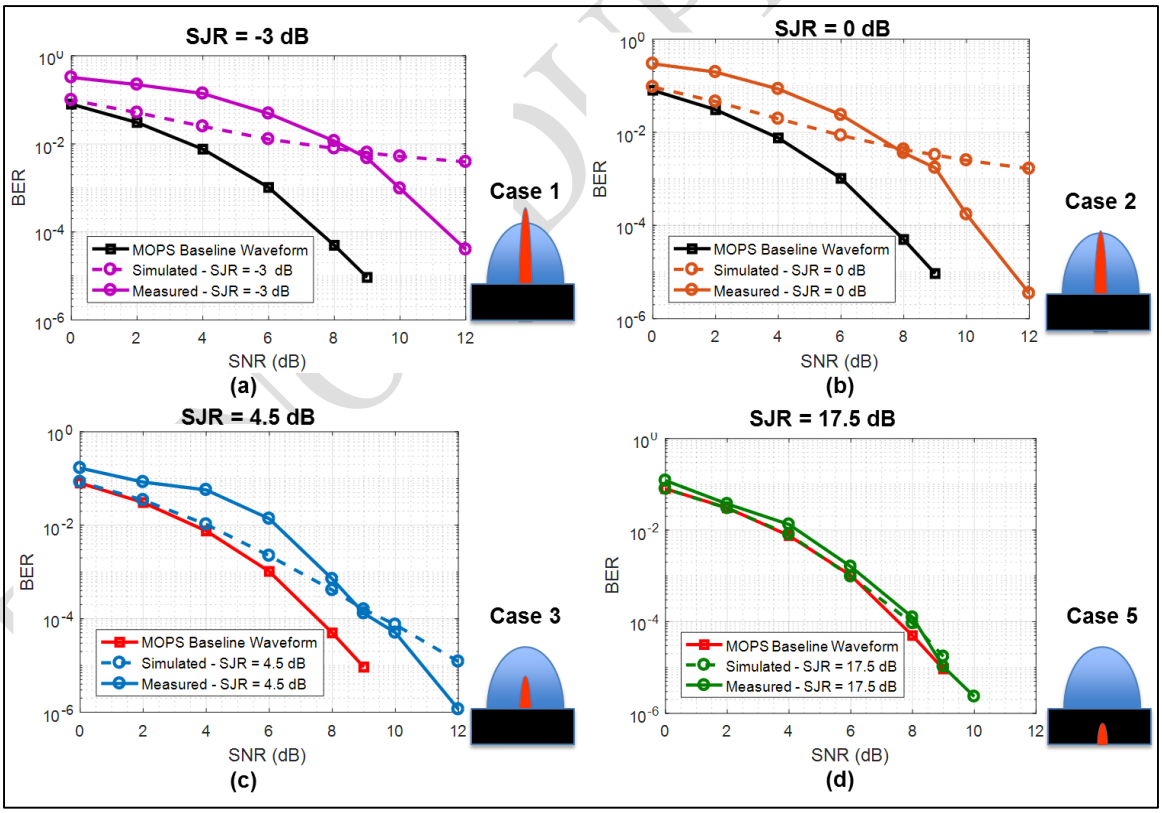


Figure 27: Simulated (dashed non-black) vs Measured (solid non-black) BER performance results of class 4 waveform in presence of Narrowband Jammer for (a) Case 1: SJR = -3dB, (b) Case 2: SJR = 0 dB (c) Case 3: SJR = 4.5 dB, (d) Case 5: SJR = 9 dB

To complete this assessment of the effect of narrow band jammers on the C2 link, 5 cases were studied in detail in both software and hardware setups. In each of the 5 cases the power level of the jammer was varied with respect to that of our Data Class of interest. For high SJR cases, measurement results closely match simulation results. As the SJR ratio decreases, measurements results begin to deviate from simulation results. For low SNR conditions, measurements deviate from simulations. This is primarily because it is difficult in hardware to accurately capture frames and perform synchronization algorithms in low SNR, low SJR conditions. A summary of the conclusion of this study is provided at the end of the Wideband Jammer section of this report.

3.5.2 Wideband Jammer

Following this initial performance assessment with the narrowband jammer, we shifted focus to a wideband jammer. Specifically, a partial channel wideband jammer (~69 kHz bandwidth) was introduced into software model and hardware testbed. Similar to the procedure completed for the narrowband jammer, a BER performance evaluation was completed and software results were compared with Hardware measurements. Similar jamming scenarios completed for the narrowband jammer were modeled for the wideband jammer. Table 10 below summarizes these jammer cases.

Table 10: Jammer Cases used for BER performance evaluation of Wideband Jammer

Case	SJR (dB) *(at SNR = 9 dB)*
1	-3
2	0
4	4.5
4	9
5	17.5

Figure 28 illustrates the jammer cases that were studied. The baseline waveform is portrayed in blue on the right, while the wideband jammer is represented in red on the left.

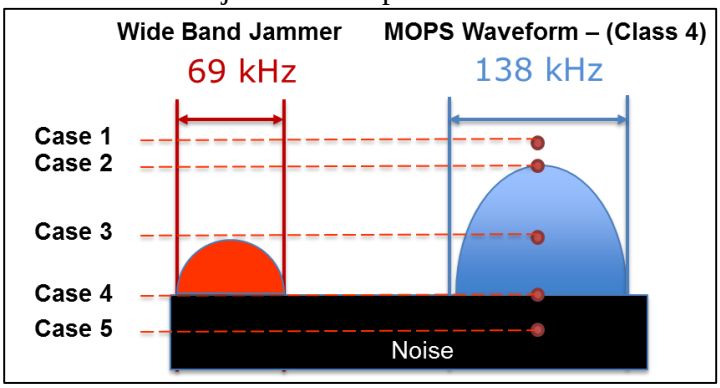


Figure 28: Jammer Cases used for BER performance evaluation of Wideband Jammer

The Spectrum Response captured at various points in communication chain is shown below in Figure 29.

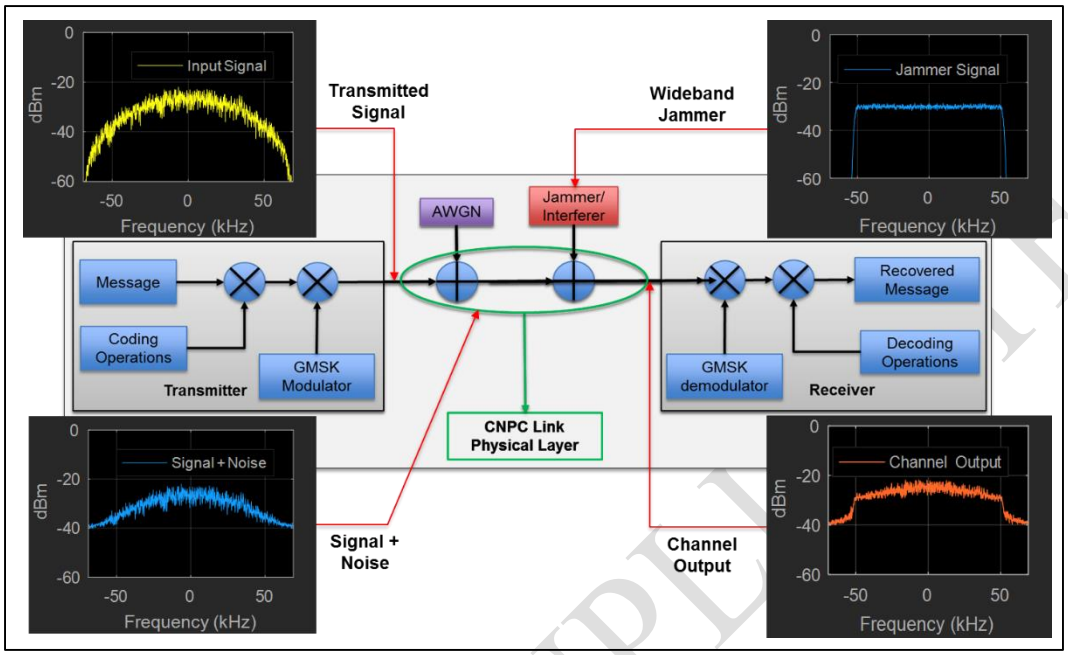


Figure 29: Software Model with Wideband Jammer and Captured Spectrum Responses

The Wideband Jammer in this simulation is implemented using a filtered random noise source. The Key Jammer Signal Parameters that can be varied are the (1) Jammer Power, (2) Jammer Bandwidth, and (3) Jammer Nosie Floor.

Having completed the software model, we then modeled this jammer using our hardware testbed. The resulting spectrum with the wideband jammer placed outside of the channel is shown below in Figure 30.

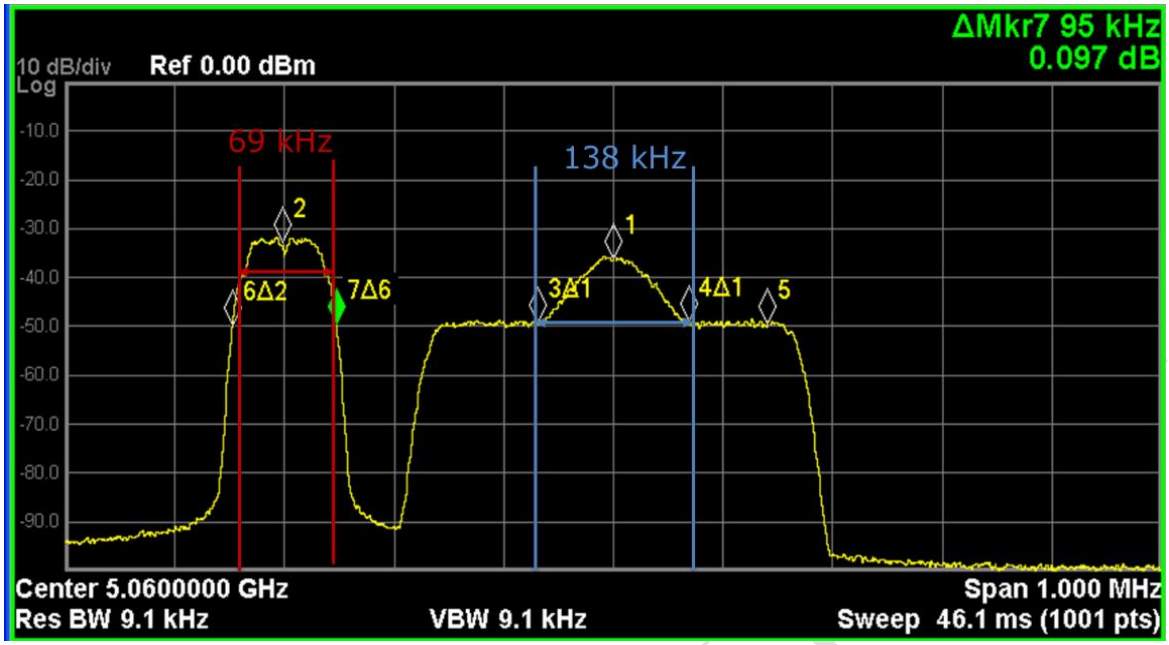


Figure 30: Case 1 Measurement (SJR = -3 dB) with Wideband Jammer (Outside of Channel)

Figure 31 below depicts the resulting spectrum when the wideband jammer is placed within the channel occupied by the MOPS waveform.

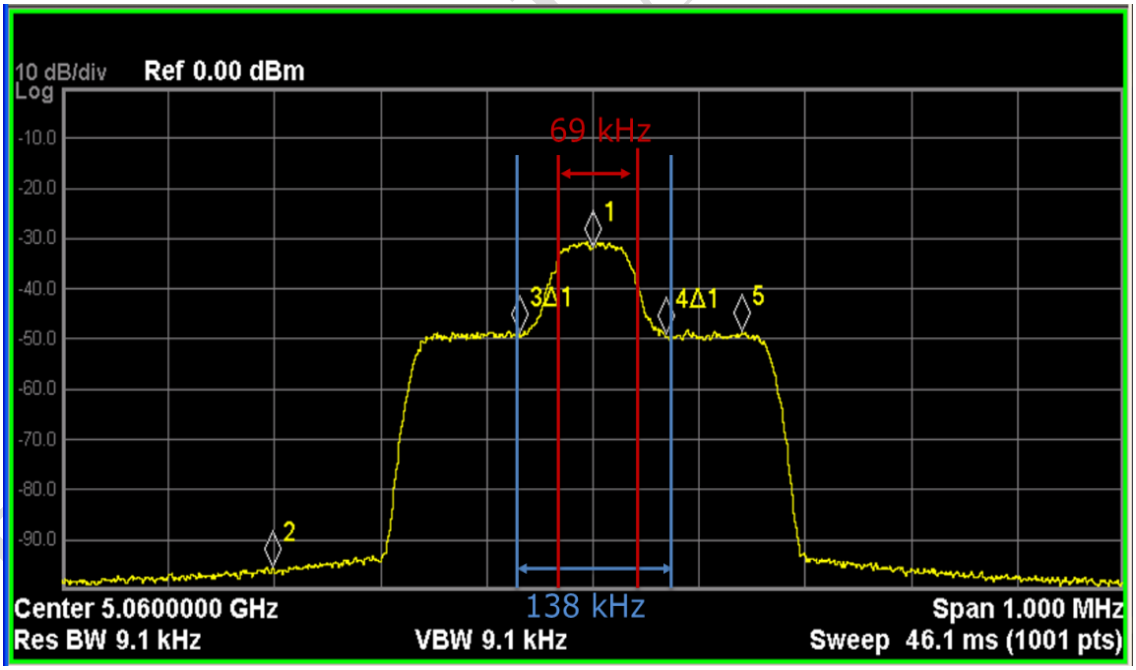


Figure 31: Case 1 Measurement (SJR = -3 dB) with Wideband Jammer (Inside of Channel)

Following the design of these models, an initial BER performance evaluation was completed for both software and hardware models. The baseline coded data class 4 waveform was tested in the presence of the modeled wideband jammer to compute BER curves. For each BER curve, the

jammer power fixed while SNR varied over AWGN channel. Measurement and Simulation results are shown in Figure 32.

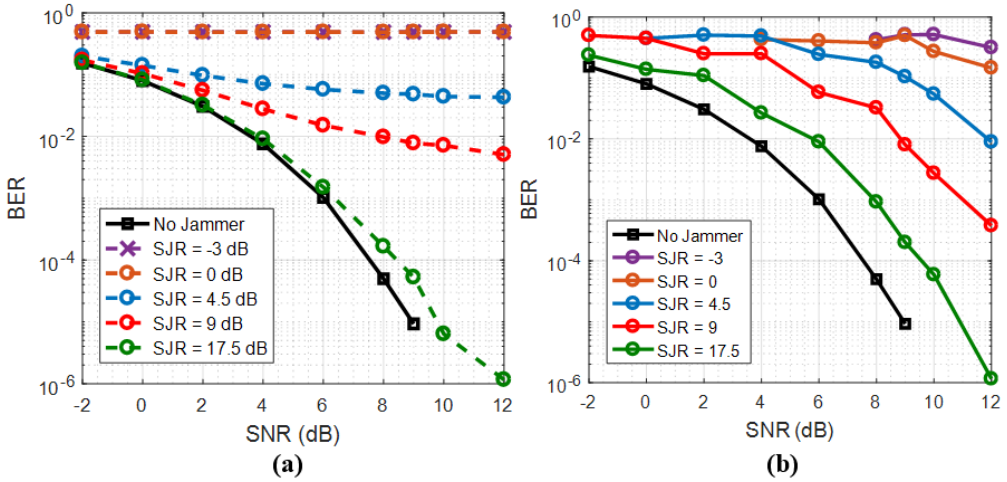


Figure 32: (a) Simulation BER Performance Results. (b) Measured BER Performance Results

For ease of comparison, four of the five cases are isolated below in on a case by case base to compare simulation and measurement results. Figure 33 below illustrates the BER performance curves for each of these cases.

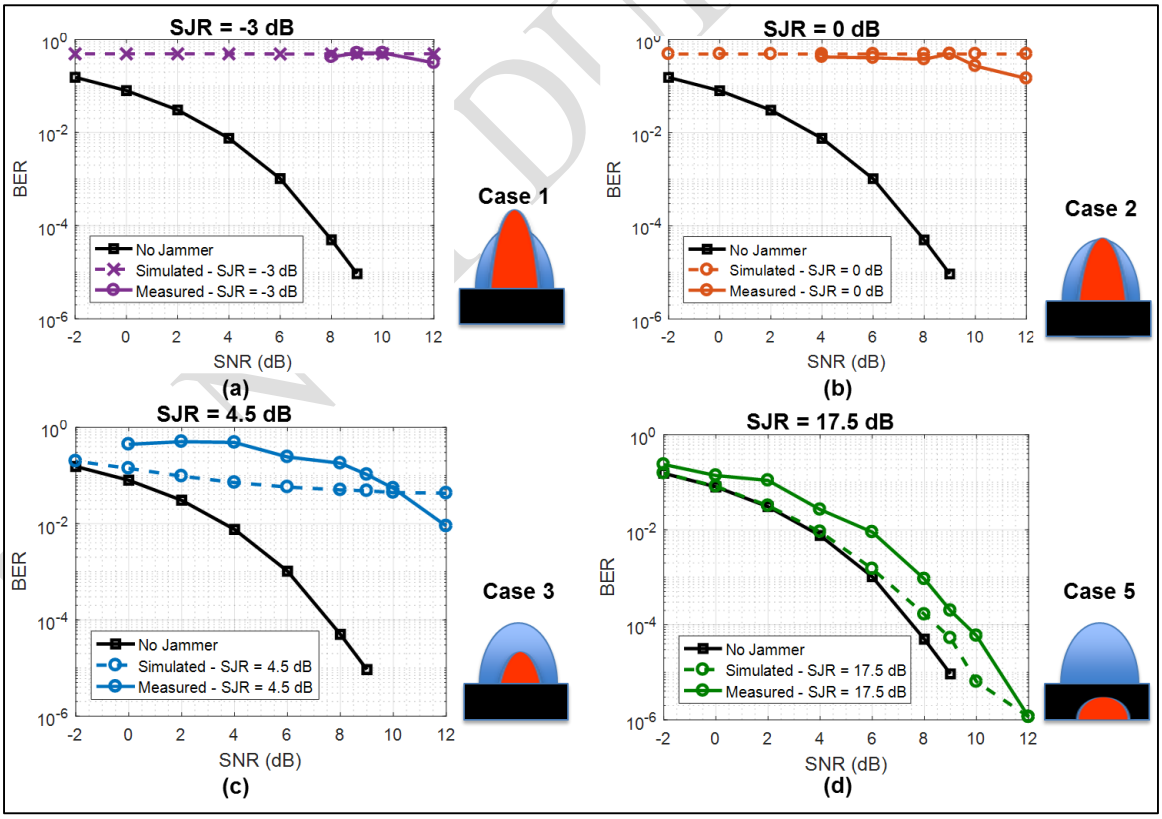


Figure 33: Simulated (dashed non-black) vs Measured (solid non-black) BER performance results of class 4 waveform in presence of Wideband Jammer for (a) Case 1: SJR = -3dB, (b) Case 2: SJR = 0 dB (c) Case 3: SJR = 4.5 dB, (d) Case 5: SJR = 9 dB

To complete this assessment of the effect of wideband jammers on the C2 link, 5 cases were studied in detail in both software and hardware setups. In each of the 5 cases the power level of the jammer was varied with respect to that of our Data Class of interest. Again, For high SJR cases, results from measurements closely match simulation results. As SJR decreases, measurement results deviate from simulation results. The primary reason for this is accurate measurements difficult in high noise environments due to low probability frame capture rates. For low SJR, low SNR conditions BER cannot be completed in hardware as pilot correlation and frame synchronization algorithms cannot be completed.

The effect of all tested jammers is easily interpreted when the BER performance results obtained from both simulations and hardware measurements are consolidated onto one curve. For this case the SNR is fixed at 9 dB, while the SJR for each jammer tested is varied. The BER corresponding to each specific operating environment is then plotted. Figure 34 below illustrates this evaluation method.

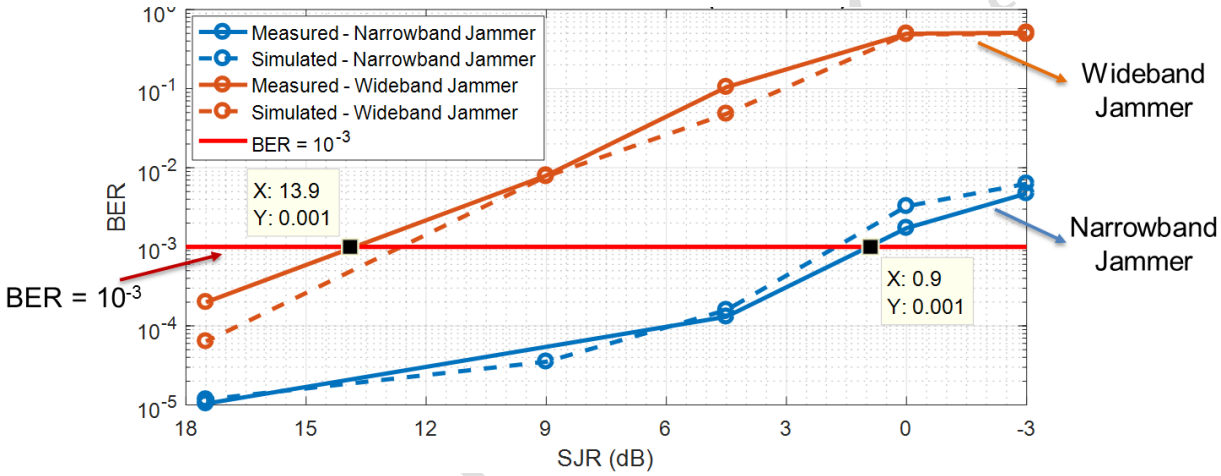


Figure 34: Effect of Tested Jammers at 9 dB SNR. Simulation (Dashed) vs. Measurements (Solid).

As seen from the curve, the Performance decreases as Jammer Power increases (i.e. decreasing SJR). The BER requirement is set at 10^{-3} for this scenario, where the BER value can be adjusted to reflect the communication link requirement. For this desired BER, In the presence of Narrowband Jammers, SJR $\geq$ 0.9 dB to maintain link. In the presence of the tested Wideband Jammer, SJR $\geq$ 13.9 dB to maintain link

In order to conduct this assessment that focused on the effect of intentional jammers on the C2 link, flexible software models were constructed in addition to enhancing the in-lab hardware testbed to accommodate interferers of interest. Testbed and Model flexibility allow for expansion of these tests to all UAV operating scenarios of interest to test link susceptibility. The evaluation in this section was completed for (1) Single Tone Jammer and (2) Wideband Jammer to assess their effect on MOPS baseline waveforms.

3.6 ASSESSMENT OF JAMMING MITIGATION STRATEGY

3.6.1 Adaptive Modulation Coding Schemes

Software algorithms were optimized to provide robustness and flexibility for testing different modulation and channel coding schemes as part of research for interference mitigation. The testbed supports modulation schemes such as GMSK, BPSK and QPSK. These modulations can be changed on-the-fly for future testing. In the future, we also plan to implement different combinations of modulation and coding schemes to assess their performance. By using different coding schemes, BER can be minimized subject to channel state information. In cases of poor channel quality data redundancy can be used to improve BER performance.

The motivation for using Adaptive Modulation and Coding Schemes stems from the fact that Multi-user interference is a major limiting factor in the performance of many multi-user wireless communication systems. Since many users share the same medium, signals from other users will interfere with the reception of desired signals.

Adaptive Coding is a term used to denote matching or changing coding parameters of FEC codes based on the channel conditions (SNR at the receiver). Adaptive Coding systems improve the performance of Bit Error Rate (BER) and Frame Error Rate (FER) by exploiting the channel state information at the transmitter.

The major drawback of this technique is the tradeoff between the information throughput and probability of bit error achieved. Since the redundancy due to coding consumes both bandwidth and energy resources, it is ideal to have FEC codes that achieve error requirements with minimum transmitting power and redundancy. Therefore, it is desirable to employ higher-rate codes when conditions are favorable and lower-rate codes under poor channel conditions.

Three turbo code rates were tested (Rate – 1/3, 1/5, 1/7) for the initial adaptive coding model. For each turbo code, 3 puncture patterns were tested (16, 20 and 25 bit puncture patterns). 9 different code rates are achieved by using the above variations. Table 11 below summarizes all 9 codes. Each code rate yields different coding gain according to the equation below:

$$SNR = \frac{E_b}{N_o} + 10log_{10}(Code\ Rate)$$

Table 11: Initial Turbo Codes Studied for Adaptive Coding Model

Turbo Code Rate	16 bit Puncture Pattern		20 bit Puncture Pattern		25 bit Puncture Pattern	
	Overall Code Rate	Coding Gain	Overall Code Rate	Coding Gain	Overall Code Rate	Coding Gain
1/3	5/8	-2.0412	1/2	-3.0103	2/5	-3.9794
1/5	3/8	-4.2597	3/10	-5.2288	6/25	-6.1979
1/7	15/56	-5.721	3/14	-6.6901	6/35	-7.6592

Study of MOPS channel coding was expanded to develop a preliminary model for adaptive coding scheme implementation in CNPC link. Simulations were completed to assess BER performance of the 9 coded waveforms in an AWGN channel. From these simulations, 6 different code rates that yield distinct BER curves were selected for initial studies. The resulting BER curve is shown in Figure 35.

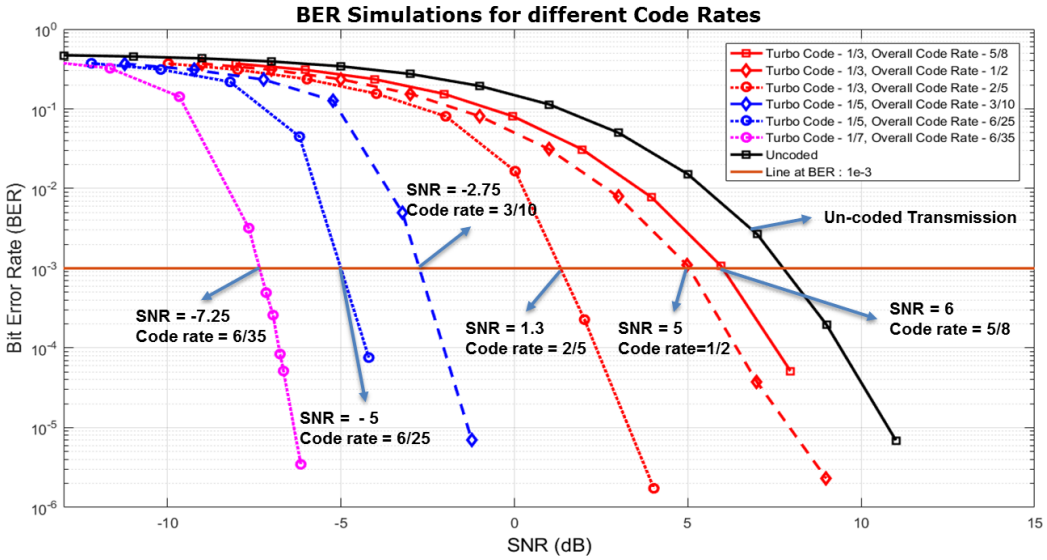


Figure 35: BER Simulation for Initial Turbo Codes selected for Adaptive Coding Model

The 6 data rates corresponding to the 6 turbo code rates were calculated and plotted against different SNR values to get a step curve as shown in Figure 36.

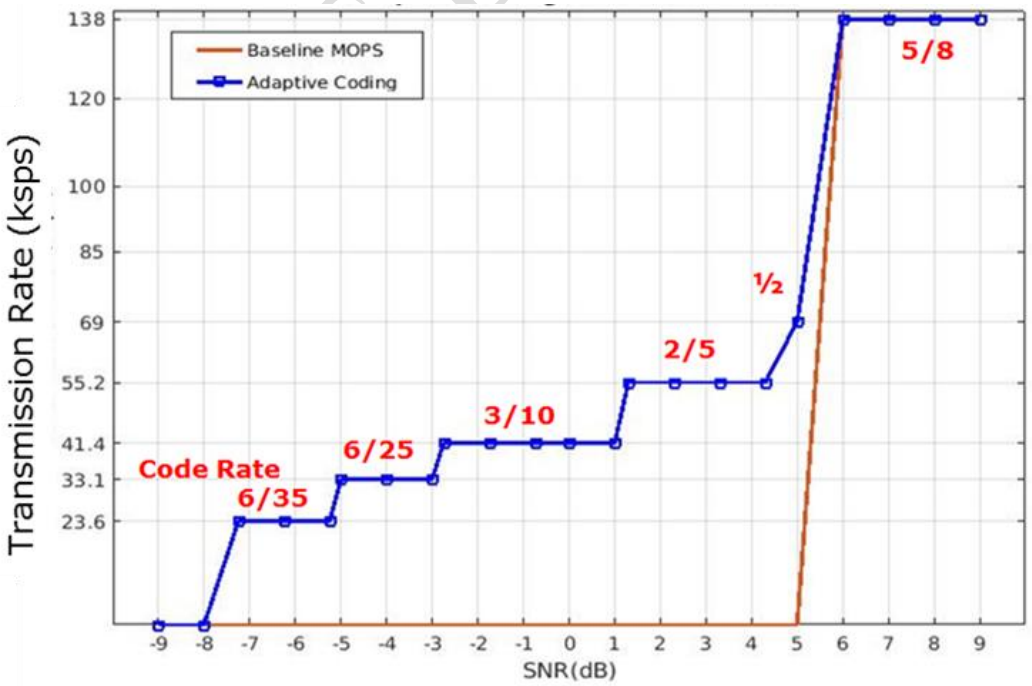


Figure 36: Adaptive Coding SNR Step Curve vs. Transmission Rate

According to channel condition (i.e. SNR at the receiver), a suitable coding scheme can be selected for transmission. Resultantly, communication is achievable at low SNR conditions by exploiting adaptive coding. Figure 37 below depicts this SNR step curve as a function of the code rate to demonstrate the tradeoff between transmission rate, and reliability required for this technique.

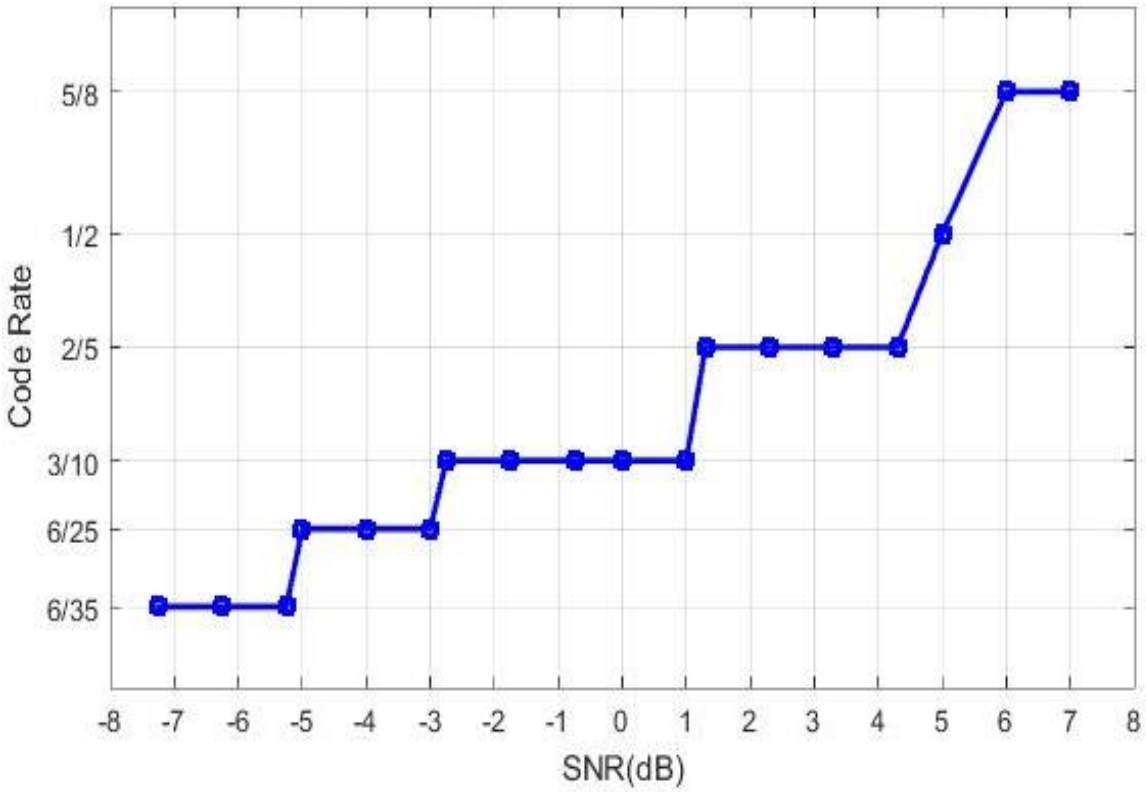


Figure 37: Adaptive Coding SNR Step Curve vs. Code Rate

These SNR step curves in addition to the BER simulations presented in this section demonstrate the utility of Adaptive Coding to improve communication reliability for Air-Ground C2 links. At high SNR values, larger code rates are used as they provides higher transmission rates. While SNR decreases, communication is still maintained by switching to smaller code rates despite this resulting in lower transmission rates. This demonstrates the trade-off between transmission rate and communication reliability.

AIR-GROUND CHANNEL CHARACTERIZATION

The channel over which any communication system operates can significantly degrade performance, therefore accurate models of the channel are necesary for analysis. The channel of interest for phase 1 of this study was the Air-Ground (AG) channel and it's model was important in improving CNPC performance. However, characterization and construction of this model according to different environments is still incomplete in literature. Several efforts focusing on the characterization of AG channels are discussed in [5], [6], [7], and [8]. From these efforts, proposed empirical models are constructed by conducting experiments for over-water scenarios, hilly and mountainous environments, along with sub-urban and urban settings.

For the AG channel characterization, it is also important to construct an earth model which represents the characteristics of ground reflection between aircraft and ground station. A "two ray" model with the LOS component modeled as one ray and the earth reflection as the second ray is a typical path loss model for several scenarios. As the ground station antenna is elevated and the aircraft flies in the sky, a two-ray model is expected to fit the AG channel in many cases [9]. Due to this, the 'Flat Earth Two-Ray Model' was used in the project to characterize the channel that the C2 signals communicate over. The details of the channel model are described in Appendix A.

Different Scenarios using two-ray model

To evaluate the effect of the adaptive coding and multiple antennas at the receiver, we studied 4 different scenarios. In the case of multiple antennas we explore a single input multiple output (SIMO) configuration where the multiple antennas are deployed at the ground station using:

1) No interference in C2 Link with single antenna
2) No interference in C2 Link with multiple antennas (SIMO setting)
3) Interference in C2 Link with single antenna
4) Interference in C2 Link with multiple antennas (SIMO setting)

For each scenario, the probability of outage was evaluated using the code defined in MOPS and adaptive coding. In the case of interference, the interferer power was modeled as one tenth of the main UAV and closer to the ground station than the main UAV. For SIMO scenarios, it was assumed that the receiver has full-CSI and has the ability to apply maximum ratio combining on the received signals.

For the given scenarios, the channel is accepted as a flat fading channel since the data class bandwidths defined in MOPS is smaller than the coherence bandwidth of the channel. Table 12 and Table 13 below show the bandwidths of each of the data classes defined in the MOPS.

Table 12: Ground Radio Transmitter Data Class Bandwidth

Data Class	Channel Width[0.5C] (kHz)	Channel Width[1.0C] (kHz)	Channel Width[1.75C] (kHz)
Data Class 1	15	30	52.5
Data Class 2	30	60	105
Data Class 3	45	90	157.5

Table 13: Airborne Data Class Bandwidth

Data Class	Channel Width[0.5C] (kHz)	Channel Width[1.0C] (kHz)	Channel Width[1.75C] (kHz)
Data Class 1	15	30	52.5
Data Class 2	30	60	105
Data Class 3	45	90	157.5
Data Class 4	60	120	210

According to the given channel impulse expression for two ray model, the frequency response of the channel is defined as:

$$h_{2-ray}(\mathrm{f};\mathrm{t}) = \alpha_0(t)\mathrm{e}^{-j2\pi \mathrm{f}\tau_0(\mathrm{t})} + \alpha_{\mathrm{g}}(\mathrm{t})e^{-j\Delta\theta}\Gamma(\mathrm{t})\mathrm{e}^{-j2\pi \mathrm{f}\tau_{\mathrm{g}}(\mathrm{t})}$$

The delay spread, $\tau_{\mathrm{d}}(\mathrm{t})$, of the channel dictates the frequency coherence and coherence bandwidth [11] which is given by:

$$W_c = \frac{1}{2\tau_d(t)} = \frac{1}{2(\tau_g(t) - \tau_0(t))}$$

Figure 38 below shows the impulse response of the two ray model.

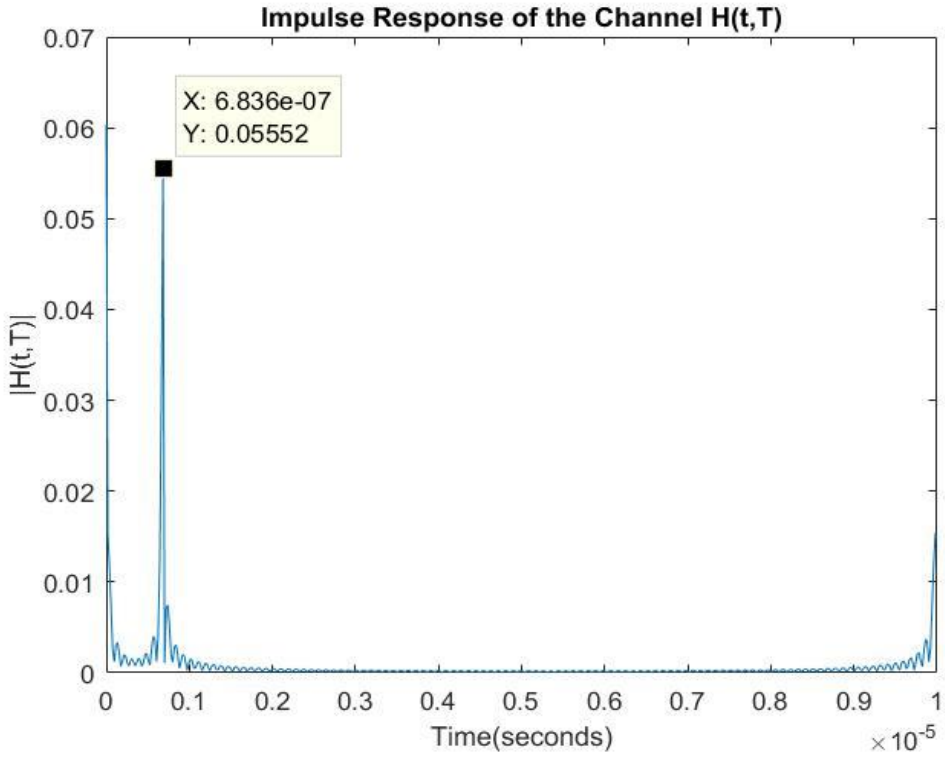


Figure 38: Channel Impulse Response at t = 0

For the scenarios investigated, the delay spread begins from 0.68μs and decreases while the transmitter-receveiver separation is increased. In accordance to the formula above, the coherence bandwidth starts from 750kHz and increase with the latitude. As a result, the channel is a flat-fading channel for the given bandwidths.

Scenario 1: No interference in C2 Link

The first scenario of interest was that of no interference in the C2 link that exists between the UAV and single antenna ground station. There is a strong LOS component between the UAV and ground station in addition to the ground reflection. Figure 39 below depicts this scenario.

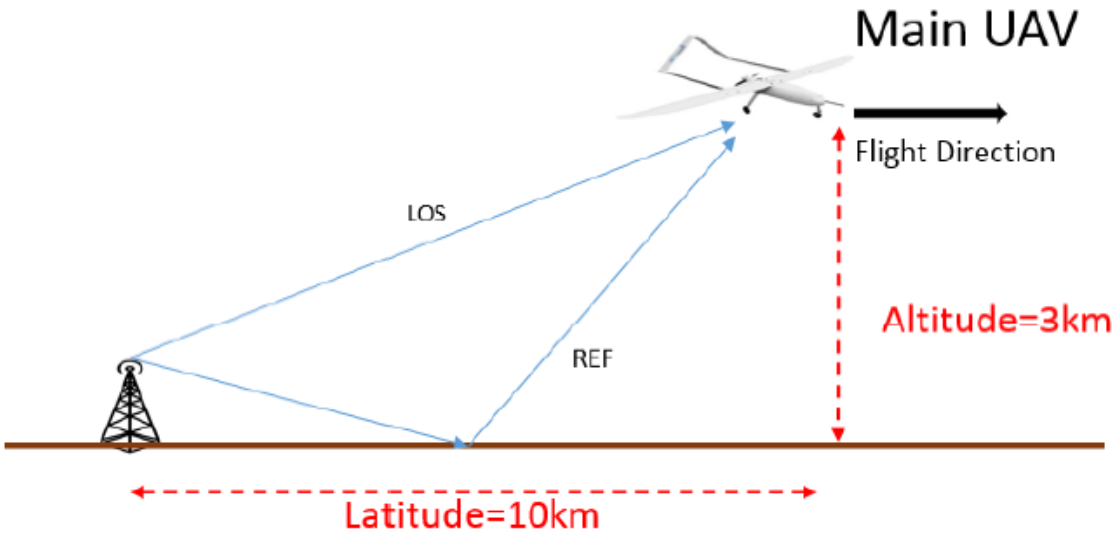


Figure 39: Diagram corresponding to No interference Scenario with Single Antenna

We define the channel matrix **h**[n] as:

$$\mathbf{h}[n] = [h1[n]\ h2[n]\ h3[n]\ h4[n]\ ]^T$$

For this single antenna GS scenario, the received signal y[n],

$$y[n] = h[n]\ s[n] + w[n] \text{ where } w \sim N(0, N_o)$$

and

$$SNR[n] = \frac{E_s|h[n]|^2}{N_o}$$

where E_s is the transmitted symbol energy. The code rate used in MOPS sustains the communication link at SNR values above 6dB while adaptive coding communicates at SNR values above -7dB.

Table 14 compares the average outage probability of the code in MOPS and the adaptive code offered. The probabilities E_s/N_o was calculated for different transmitted power.

Table 14: Outage Probability Corresponding to No Interference Scenario with Single Antenna

$Avg.\ E_s/N_o$ at receiver	Outage Probability of MOPS Code	Outage Probability of Adaptive Code
9 dB	0	0
4 dB	0.678	0
-6 dB	1	0.229

From this experiment, the results show that Adaptive coding increases the SNR range of the communication and allows communication to be maintinained in SNR values that MOPS code is not able to communicate with.

Scenario 2: No interference in C2 Link with multiple antennas

The second scenario studied introduces multiple antennas at the ground station. Again, there is no interference thus we again have a strong LOS component between the UAV and ground station in addition to the ground reflection. Figure 40 below depicts this scenario.

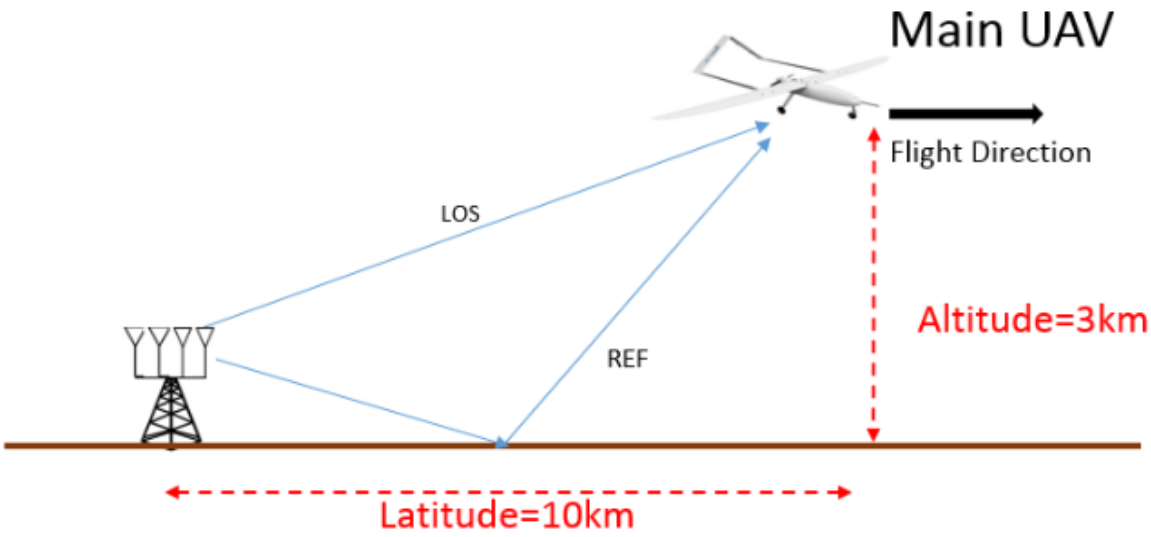


Figure 40: Diagram corresponding to No Interference Scenario with Multiple Antennas

We define the channel matrix **h**[n] as:

$$\mathbf{h}[n] = [h1[n]\ h2[n]\ h3[n]\ h4[n]\ ]^T$$

the received signal y[n] as:

$$\mathbf{y}[n]\ =\ \mathbf{h}[n]\ s[n]\ +\ \mathbf{w}[n] \text{ where } \mathbf{w} \sim N(0, \Sigma)$$

and

$$SNR[n] = \frac{\mathrm{E_s}\|\mathbf{h}[\mathrm{n}]\|^2}{\mathrm{N_o}}$$

Table 15 below below compares the outage probability of the code in MOPS and the adaptive code for multi antennas scenario.

Table 15: Outage Probability corresponding to No Interference Scenario with Multiple Antennas

$Avg.\ E_s/N_o$ at receiver	Outage Probability of MOPS Code	Outage Probability of Adaptive Code
12 dB	0	0
9 dB	0.1264	0
3 dB	0.8064	0

Results from this experiment, confirm that using multiple antennas results in significant increase in SNR. This results in better performance in terms of outage probability and allows communication to be maintained across SNR values that MOPS code is not able to communicate in.

Scenario 3: Interference in C2 Link with single antenna

The third scenario introduces an interfering UAV that disrupts the C2 link between the main UAV and ground station. In addition to the strong LOS component between the UAV and ground station, there is another LOS component that exists between the interfering UAV and ground station. Both LOS components are accomponied with ground reflections. Figure 41 below depicts this scenario.

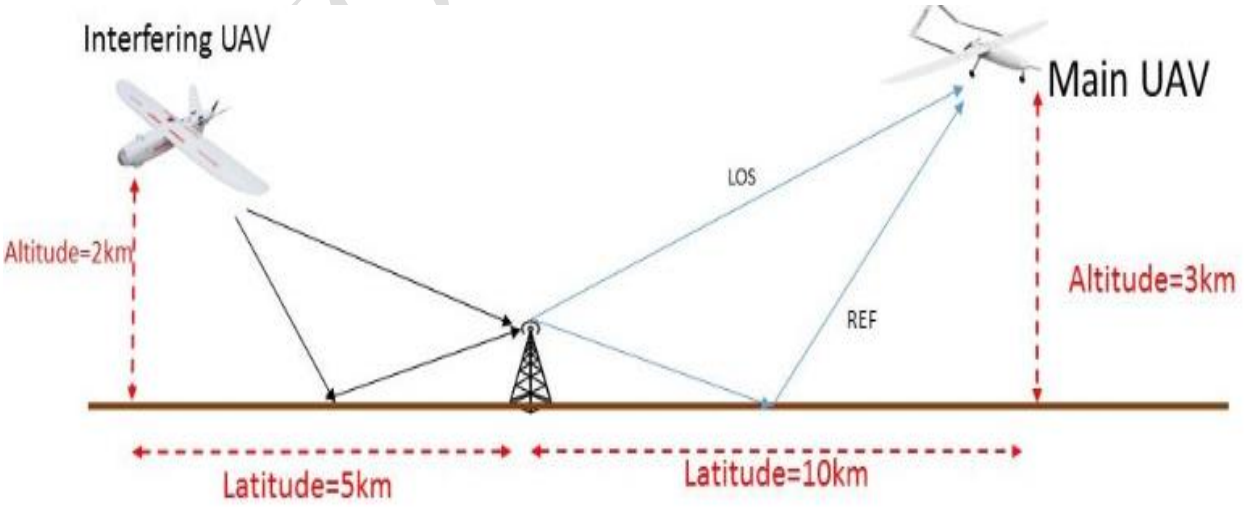


Figure 41: Diagram corresponding to Interference Scenario with Single Antenna

We define the channel matrix **h**[n] as:

$$\mathbf{h}[n] = [h1[n]\ h2[n]\ h3[n]\ h4[n]\ ]^T$$

and the interferer channel matrix $\mathbf{h_{int}}[n]$ as:

$$\mathbf{h_{int}}[n] = [h_{int}1[n]\ h_{int}2[n]\ h_{int}3[n]\ h_{int}4[n]\ ]^T$$

For single antenna under interference , the received signal y[n],

$$y[n] = h[n]s[n] + h_{int}[n]s_{int}[n]\ +\ w[n] \text{ where } w \sim N(0,\ N_o)$$

and

$$SINR[n] = \frac{E_s|h[n]|^2}{N_o\ + E_{int}|h_{int}[n]|^2}$$

where E_s, E_{int} is the transmitted symbl energy of the main UAV and interferer respectively while $E_{int} = 0.1E_s$.

Table 16 below compares the situation under interference

Table 16: Outage Probabilites corresponding to Interference Scenario with Single Antenna

$Avg.\ E_s/N_o$ at receiver	Outage Probability of MOPS Code	Outage Probability of Adaptive Code
3 dB	0.9	0
1 dB	1	0
-6.5 dB	1	0.264

From this experiment, it is seen that the communication link using MOPS code is in outage in the presence of an interferer. Adaptive Coding enables the C2 to communicate with lower code rates and again allows communication to be maintainained across SNR values that MOPS code is not able to communicate in.

Scenario 4: Interference in C2 Link with multiple antennas

The fourth scenario studied builds on scenario three and introduces multiple antennas at the ground station in. Once more, in addition to the strong LOS component between the UAV and ground station, there is another LOS component that exists between the Interfering UAV and ground station. Both LOS components are accomponied with ground reflections. Figure 42 illustrates this scenario.

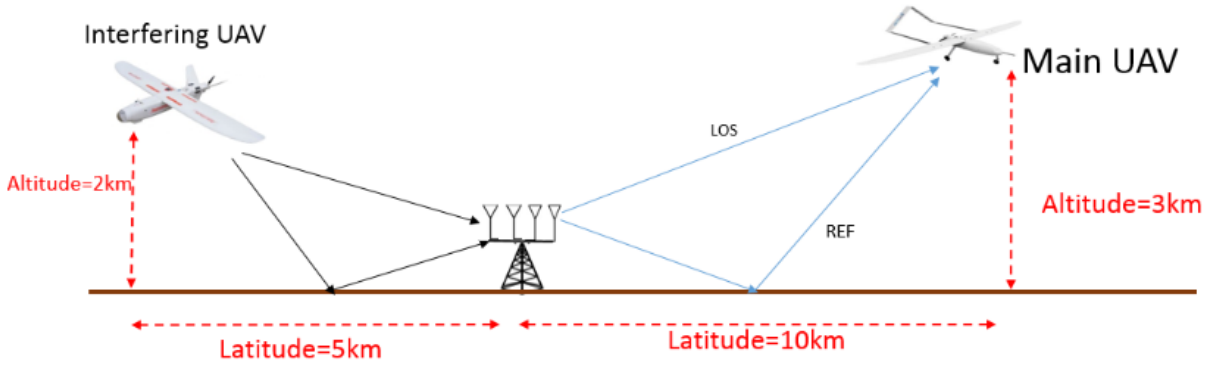


Figure 42: Diagram corresponding to Interference Scenario with Multiple Antennas

We define channel matrix **h**[n] as:

$$\mathbf{h}[n] = [h1[n]\ h2[n]\ h3[n]\ h4[n]\ ]^T$$

and the interferer channel matrix $\mathbf{h_{int}}[n]$ as:

$$\mathbf{h_{int}}[n] = [h_{int}1[n]\ h_{int}2[n]\ h_{int}3[n]\ h_{int}4[n]\ ]^T$$

the received signal y[n] as:

$$\mathbf{y}[n] = \mathbf{h}[n]s[n] + \mathbf{h_{int}}[n]s_{int}[n]\ +\ \mathbf{w}[n] \text{ where } \mathbf{w} \sim N(0, \Sigma)$$

and

$$SNR[n] = \frac{E_s\|\mathbf{h}[n]\|^2}{N_o\ + E_s\|\mathbf{h_{int}}[n]\|^2}$$

Table 17 depicts the outage probability in the SIMO case.

Table 17: Outage Probability corresponding to Interference Scenario with Multiple Antennas

$Avg.\ E_s/N_o$ at receiver	Outage Probability of MOPS Code	Outage Probability of Adaptive Code
6 dB	0.4483	0
5 dB	0.6782	0
2 dB	0.931	0

From this experiment, SIMO enables communication for the MOPS code although there is a high probability of outage in each case and the performance of adaptive code increases with the addition of the antenna gain. However, deploying both SIMO and Adaptive Coding techniques allows communication to be maintainained accross SNR values that MOPS code is not able to communicate with.

4. CONCLUSION

In summary, by the end of phase one of this work we were able to accomplish the following: 1) During the first three months the project we regularly interacted with the governing party and the pertaining industry partners to identify the underlying issues and concerns in the current Minimum Operational Performance Standards (MOPS). 2) Extracted key requirements from the documented Minimum Operational Performance Standards and built communication waveforms to be used as a baseline. 3) Simulated the baseline physical link as prescribed in the MOPS. 4) Built and tested a complete hardware setup that can mimic a real time physical UAV communication link for line of sight in the C frequency band. Some built-in capabilities are: testing of various jamming scenarios (intended and unintended), implementation of various coding communication schemes including adaptive coding, MIMO capabilities for use of multiple antennas, and fading and multipath scenarios. 5) Used designed testbeds (software and hardware) to run baseline measurements as prescribed in MOPS and evaluate their performance. 6) Investigated the adaptive coding scheme as a possible solution for more robust communication links. In doing so, we obtained preliminary results in terms of BER performance and required SNR to maintain C2 link operability.

5. REFERENCES

1. DO-362 “Command and Control(C2) Data Link Minimum Operational Performance Standards (MOPS) (Terrestrial)”
2. Feria, Ying, and Kar-Ming Cheung. "Seamless Data-rate Change Using Punctured Convolutional Codes for Time-varying Signal-to-noise Ratio." Proceedings IEEE International Conference on Communications ICC '95
3. Chatzigeorgiou, I., M.r.d. Rodrigues, I.j. Wassell, and R. Carrasco. "Punctured Binary Turbo-codes with Optimized Performance." VTC-2005-Fall. 2005 IEEE 62nd Vehicular Technology Conference, 2005.
4. Kousa, M.a., and A.h. Mugaibel. "Puncturing Effects on Turbo Codes." IEE Proceedings - Communications 149.3 (2002): 132-38.
5. D. M. R.Sun, "Air-Ground Channel Characterization for Unmanned Aircraft Systems—Part I: Methods, Measurements and Models for Over-Water Settings," IEEE Trans. Veh. Technol., vol. 66, no. 1, pp. 26-44, 2017. Dd
6. D. M. R.Sun, "Air-Ground Channel Characterization for Unmanned Aircraft Systems—Part II: Hilly & Mountainous Settings," IEEE Trans. Veh. Technol., vol. 66, no. 3, pp. 1913-1925, 2017
7. D. M. R.Sun, "Air-Ground Channel Characterization for Unmanned Aircraft Systems—Part III: The Suburban and Near-Urban Environments," *IEEE Trans. Veh. Technol.*, to be published
8. D. M. R.Sun, "Air-Ground Channel Characterization for Unmanned Aircraft Systems—Part IV: Airframe Shadowing," *IEEE Trans. Veh. Technol.*, to be published.
9. R.Sun, Dual-Band Non-Stationary Channel Modeling for the Air-Ground Channel, University of South Carolina, 2015.
10. A. Goldsmith, Wireless Communications, Cambridge University Press, 2005.
11. P. V. David Tse, Fundamentals of Wireless Communication, Cambridge University Press, 2005.
12. E. Haas, "Aeronautical Channel Modeling," *IEEE Trans. Veh. Technol*, vol. 51, no. 2, 2002.

APPENDIX A—DERIVATION OF FLAT EARTH TWO-RAY MODEL

Flat-Earth Two-Ray Model [9]

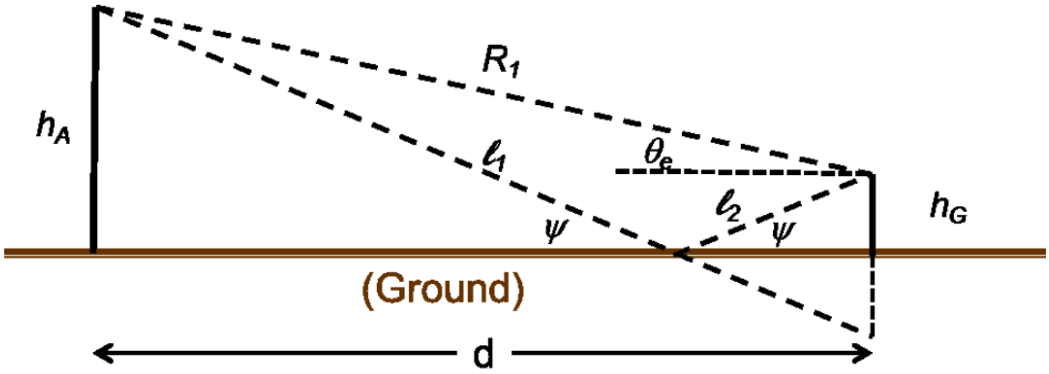


Figure 43: Geometry for flat-earth approximation.

The variables h_G and h_A denote the antenna heights of GS and aircraft, respectively. d represents the distance on the earth between the aircraft and the GS.

The length of LOS path R_1 is expressed as:

$$R_1(t) = \sqrt{d^2(t) + \left(h_A(t) - h_g\right)^2}$$

With c representing the speed of light, the delay of the LOS component is:

$$\tau_o(t) = \frac{R_1(t)}{c}$$

Via the Friis free-space transmission equation, we can find the LOS amplitude coefficient as:

$$\alpha_0(t) = \frac{c}{4\pi f c}\frac{1}{R_1(t)}$$

The length of the reflected path R_2 is:

$$R_2(t) = l_1(t) + l_2(t) = \sqrt{d^2(t) + \left(h_A(t) + h_g\right)^2} = \sqrt{R_1^2(t) + 4h_A(t)h_g}$$

Then, the delay of the earth surface reflection is:

$$\tau_g(t) = \frac{R_2(t)}{c} = \sqrt{R_1^2(t) + 4h_A(t)h_g}\,/c$$

The reflected component's amplitude coefficient is:

$$\alpha_g(t) = \frac{c}{4\pi f c}\frac{1}{R_2(t)}$$

and ψ is the grazing angle calculated as:

$$\psi_k(t) = \tan^{-1}\left(\frac{h_A(t) + h_g}{d(t)}\right)$$

the phase delay between the LOS and the earth surface reflection is:

$$\Delta\theta = \frac{2\pi\Delta R(t)}{\lambda} = 2\pi f_c\left(\frac{R_2(t) - R_1(t)}{c}\right)$$

Using these result, channel impulse response can be expressed as:

$$h_{2-ray}(\tau; t) = \alpha_0(t)\delta(\tau - \tau_0(t)) + \alpha_g(t)e^{-j\Delta\theta}\Gamma(t)\delta(\tau - \tau_g(t))$$

where Γ is the reflection coefficient which depends on the dielectric constant and conductivity of the reflection surface.

The ground reflection coefficient is given in [10]:

$$\Gamma = \frac{\psi_k(t) - Z(t)}{\Psi_k(t) + Z(t)}$$

Where

$$Z(t) = \begin{cases} \sqrt{\varepsilon_r - \cos^2(\psi_k(t))}/\varepsilon_r & \text{for vertical polarization} \\ \sqrt{\varepsilon_r - \cos^2(\psi_k(t))} & \text{for horizontal polarization} \end{cases}$$

ε_r is the dielectric constant of the ground. For earth or road surfaces this dielectric constant is approximately that of a pure dielectric. (for which it is real with a value of about 15).

The received power of the two-ray model for narrowband transmission is:

$$P_r(t) = P_t\left[\frac{\lambda}{4\pi}\right]^2\left|\frac{\sqrt{G_t}}{R_1(t)} + \frac{\Gamma(t)\sqrt{G_r}\, e^{j\Delta\theta(t)}}{R_2(t)}\right|^2$$

Where, G_t, G_r are the transmitter and receiver antenna gains respectively.

It is seen that for large d values, $R_1 \cong R_2 \cong d$, $\psi \cong 0$, $\Gamma = -1$ and assume $\sqrt{G_t} = \sqrt{G_r}$

$$P_r(t) \cong P_t \left[\frac{\lambda\sqrt{G_t}}{4\pi}\right]^2 \left[\frac{4\pi h_A(t) h_g(t)}{\lambda d(t)}\right]^2 P_t$$

Or equivalently, the attenuation in dB is given by:

$$P_r(\text{dBm}) = P_t(\text{dBm}) + 10\log_{10}(G_t) + 20\log_{10}(h_A h_g) - 40\log_{10}(d)$$

Thus, for large d, the received power falls off inversely with the fourth power of d and is independent of the wavelength. The plot of the received power vs distance can be separated into three segments. For small distances, $d < h_A$, the path loss is roughly flat. For distances larger than h_A up to a certain critical distance d_c, the wave experiences constructive and destructive interference of two rays, resulting in a wave pattern with a sequence of maxima and minima.

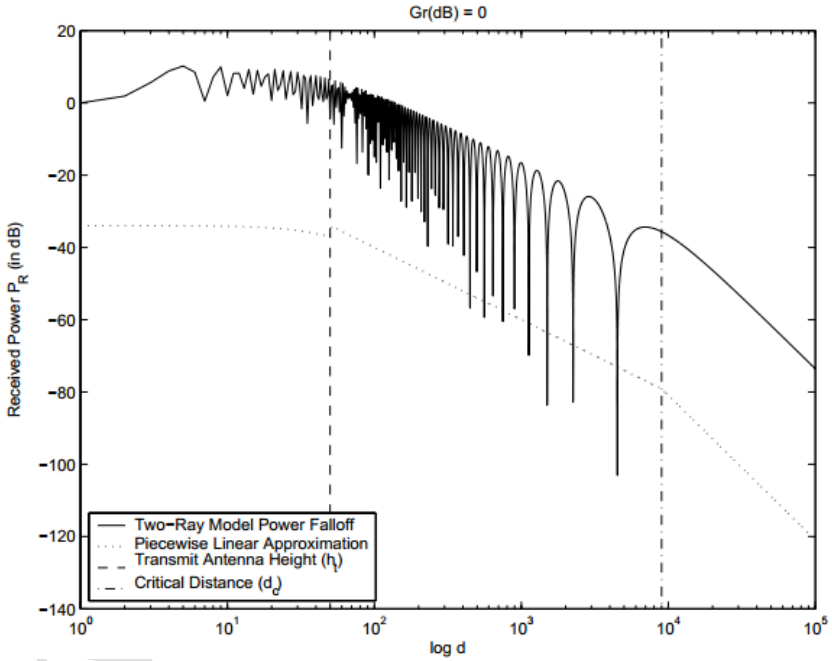


Figure 44: Received Power vs Distance for Two-Ray Model