UNIVERSITY OF OKLAHOMA

GRADUATE COLLEGE

EFFECTIVENESS OF ELECTRONIC COUNTER MEASURES (ECM) ON SMALL UNMANNED AERIAL SYSTEMS (SUAS): ANALYSIS AND PRELIMINARY TESTS

A THESIS

SUBMITTED TO THE GRADUATE FACULTY

in partial fulfillment of the requirements for the

Degree of

MASTER OF SCIENCE

By

CHARLES WARREN THUMANN
Norman, Oklahoma
2018

EFFECTIVENESS OF ELECTRONIC COUNTER MEASURES (ECM) ON SMALL UNMANNED AERIAL SYSTEMS (SUAS): ANALYSIS AND PRELIMINARY TESTS

A THESIS APPROVED FOR THE
SCHOOL OF ELECTRICAL AND COMPUTER ENGINEERING

BY

____
Dr. Yan Zhang, Chair

____
Dr. J. R. Cruz

____
Dr. John W. Dyer

Table of Contents

List of Tables

List of Figures

Abstract

Small unmanned aerial systems (sUAS) have become more common and affordable for government, commercial, and private use. There are several counter sUAS products that employ electromagnetic counter measures to disrupt the communications link of sUAS. However, most of these solutions are limited in efficacy to specific sUAS types due to the sophisticated control and communications link technologies utilized by sUAS which make it challenging to effectively jam. To address these challenges, a Drone Detection and Mitigation Radar (DDMR) concept was developed. The jamming component of the DDMR used wideband noise combined with random sweeping of the noise to jam the communications link. This thesis research was predicated by a laboratory experiment which used the DDMR system to successfully jam an sUAS's communications link. This particular experiment did not (1) provide any theoretical analysis, (2) simulation analysis to determine the effective jamming probabilities, or (3) conduct additional experiments to find the optimal sweeping frequency for the jamming component of the DDMR. This thesis focuses on the optimization of the sweeping noise jamming solution of the communications link by examining the theoretical and simulation analysis as well as the results of further experimental studies. The findings are presented in this thesis paper.

Chapter 1: Background

1.1 Overview of sUAS

The increasing affordability of small unmanned aerial systems (sUAS), also known as drones, has resulted in significant interest from individuals and businesses. The sUAS offers distinct advantages, such as reducing hazardous risks to individuals or performing specific functions which might otherwise be impossible to complete. For example, a drone can be placed in a radioactive environment and provide immediate feedback without jeopardizing an individual's safety. A sUAS, or drone, can also be considered a threat or nuisance when it is not operated in a responsible manner. The rapid increase in drone sales could be problematic for many commercial, private, military and government entities. Figure 1 shows how the consumer drone market has grown significantly over the past several years.

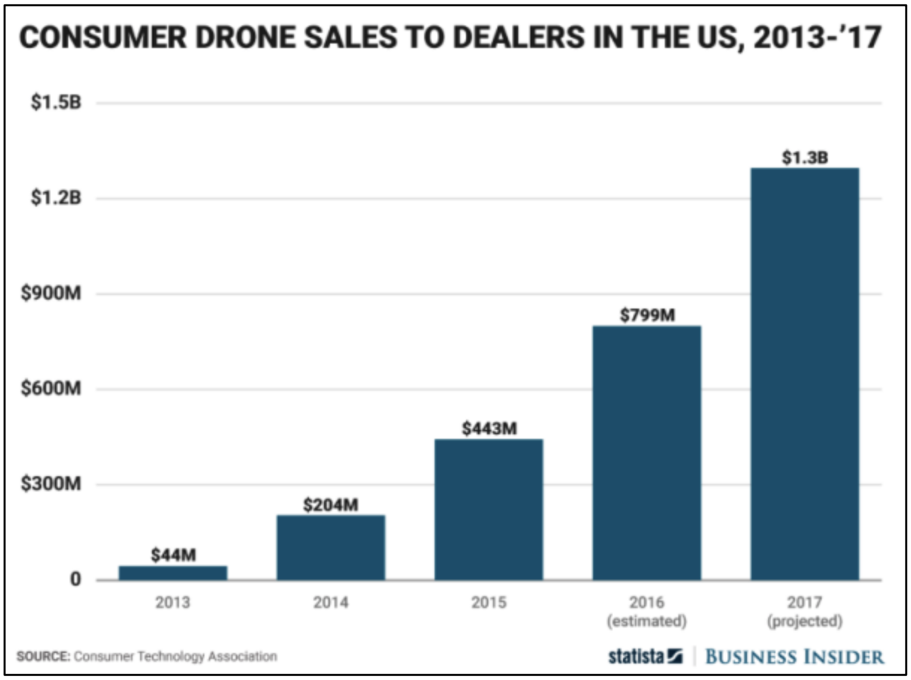


Figure 1. Drone Sales in the U.S. [1]

Some sUAS will pose a security threat for critical infrastructures and venues, such as sports stadiums, military facilities, and airports. Military personnel and law enforcement are faced with the difficult task of protecting infrastructure and venues from any security threats. There are significant challenges encountered when attempting to protect each of these venues. The challenges are not just technological, they are also legal. Military installations abroad are not always subject to the same laws as military bases physically located in the United States. Currently, within the U.S. the Federal Aviation Administration (FAA), Federal Communications Commission (FCC), and various federal statutes prohibit any jamming, or electronic counter measures (ECM), that could otherwise take place outside the United States. These federal agencies recognize the increasing threats created by drone proliferation and are attempting to create new rules and regulations to allow the military and law enforcement to employ ECM to protect critical infrastructures and susceptible venues from drone threats without violating federal laws.

1.2 Applicable Laws that Prohibit ECM (Radar Jamming) in the U.S

The FAA is the governing body that is ultimately responsible for the management of the National Airspace System (NAS) and civilian aircraft operations under Title 49 United States Code (U.S.C.) § 40103, sovereignty and use of airspace [2]. Additionally, sUAS are defined within Title 14 of the Code of Federal Regulations (C.F.R.) 1.1, which states "unmanned aircraft mean an aircraft operated without the possibility of direct human intervention from within or on the aircraft. [3]" In June 2014, the FAA published additional guidance for hobby or recreational use of sUAS. The guidance states the FAA, consistent with the FAA Modernization and Reform Act of 2012, has the authority to undertake enforcement actions against any violators who endanger the safety of the NAS [4].

The FCC is the governing agency responsible for the management of communications within the United States. This responsibility involves ensuring the integrity of radio frequency (RC) communications, to include those communications used by sUAS. The FCC prohibits the act of jamming or intentionally interfering with any communication signals because it is considered a potential public safety risk. The FCC does not want a situation where an individual attempts to seek emergency assistance but is unable to do so because their communications were jammed. The FCC has implemented the following rules concerning the jamming of communications:

- "Title 47 C.F.R. § 2.803 – prohibits the manufacture, importation, marketing, sale or operation of these devices within the United States.
- Title 47 C.F.R. § 2.807 – provides for certain limited exceptions, such as the sale to the U.S. government.
- Title 47 U.S.C. § 301 – requires persons operating or using radio transmitters to be licensed or authorized under the Commission's rules.
- Title 47 U.S.C. § 302(b) – prohibits the manufacture, importation, marketing, sale or operation of these devices within the United States.
- Title 47 U.S.C. § 333 – prohibits willful or malicious interference with the radio communications of any station licensed or authorized under the Act or operated by the U.S. Government.
- Title 47 U.S.C. § 503 – allows the FCC to impose forfeitures for willful or repeated violations of the Communications Act, the Commission's rules,

regulations, or related orders, as well as for violations of the terms and conditions of any license, certificate, or other Commission authorization, among other things.

- Title 47 U.S.C. § 510 – allows for seizure of unlawful equipment. [5]"

In addition to the policies and procedures enacted by the FAA and FCC, the United States Department of Justice (DOJ) also prohibits the active jamming or the use of ECM within the United States. The FAA and FCC can levy fines and seize drones, but the DOJ can criminally prosecute persons who are charged with violating the following federal laws:

- "Title 18 U.S.C. § 1362 – prohibits willful or malicious interference to US government communications; subjects the operator to possible fines, imprisonment, or both.
- Title 18 U.S.C. § 1367(a) – prohibits intentional or malicious interference to satellite communications; subjects the operator to possible fines, imprisonment, or both. [5]"

Currently, due to the aforementioned regulations and laws, domestic law enforcement agencies can only passively monitor drones through radar technology. The radar technology will alert law enforcement to an unauthorized drone in its area of responsibility. There is a possibility that law enforcement may be exempt from these laws in the future and therefore be allowed to utilize jamming technology to ensure particular venues and critical infrastructures can be secured against any drone threats.

1.3 Current Drone Threat Problems

There are several civilian counter-drone products available which use radar and ECM technology. These counter-drone solutions are limited by both the particular type of detection techniques used as well as the ECM deployed. The present solutions are therefore usually restricted to specific drone types. The communications technologies used in RC drones have become more sophisticated in the last few decades, making sUAS more difficult to detect and decode. The sophisticated communication signals can create challenges when attempting to deploy effective counter measures against sUAS. The research, simulations, and experiments associated with this thesis are focused on mass marketed, commercial drones (e.g. DJI Phantom as shown in Figure 2). The majority of commercial drones operate on the 2.4GHz to 2.5GHz frequency range.

Figure 2. Common Commercial Drone Manufactured by DJI Innovations

Some drone enthusiasts operate drones on frequency bands dedicated to other technologies. Furthermore, with improved accuracy in global positioning systems (GPS), some individuals are foregoing traditional radio frequency (RF) technology and operating their drones via GPS. A flexible and robust tracking and jamming system will be necessary to effectively neutralize these evolving technologies.

Since 2014, there have been hundreds of events where drones interfered with restricted airport airspace. These are instances where the drone enthusiast unintentionally flew too close to airplanes and caused a public safety risk. The FAA monitors these events and publishes the results within the UAS Sightings Report [6]. As commercial drones become more affordable and popular, it is highly likely these incidents will continue to increase in frequency.

1.4. Proposed Solution

The Drone Detection and Mitigation Radar (DDMR) system [7] was designed to detect drones and, simultaneously, deploy ECM technology in order to adversely affect a drone's flight. DDMR has several distinct advantages when compared to existing radar jamming technologies on the market:

- DDMR is a low-cost and portable jamming system (small size, weight, and power) operating on the 2.4 GHz to 2.5 GHz, ISM (industrial, scientific, and medical) band frequencies.
- The system can be mounted on an assault rifle style platform for quick and easy deployment. As such, this system will be very familiar to military and law enforcement users who currently utilize this type of weapon platform.
- DDMR can be used to analyze the RC communications signal for the majority of drone products on the market. DDMR is capable of generating optimal transmitting waveforms based on analyzing these common frequencies.
- DDMR transmits multi-functional waveforms that perform both drone jamming and radar localization.

- Through polarimetric radar signature and Doppler features, DDMR can discriminate drones from other objects in the same airspace.

It is important to understand that each entity, commercial, private, military and government, will have a different objective related to the implementation of DDMR technology. Under current law, only the federal government, in a very limited capacity, would be allowed to employ the use of the DDMR system. If the government decided to make changes to current regulations and laws, law enforcement agencies might be allowed to protect particular venues and facilities. For example, local law enforcement constantly faces threats from drones that drop contraband over prison walls. As another example, in the past year, there have been several instances where pilots flew commercial drones over NFL stadiums [6]. Even though this activity is prohibited under current law, law enforcement could not take any actions against the pilots until after the incidents occurred. In the latter example, the pilots were merely a nuisance, but the situations could have been much worse if the pilots had intended to cause harm to civilians at the venues. Most law enforcement agencies use passive radar systems to secure critical infrastructures or at high-profile venues (targets). An example of a high-profile venue is the Super Bowl, the World Series, or a Presidential movement.

The military does not have any restrictions on active jamming outside the continental United States. The military is more concerned about a potential security threat from a drone. There have been instances where drones have dropped improvised explosive devices on military personnel overseas (Non-U.S.). A military installation could benefit from DDMR, and military personnel would likely find its small form factor, light weight, and portability advantageous. Having an effective and reliable DDMR system on a military base's perimeter would help protect the base against adversarial threats.

The front end of the DDMR will utilize polarimetric radar signature and Doppler features in order to identify and discriminate drones from other objects, such as birds. However, this separate and distinct section of the system is outside the scope of this thesis. This thesis will focus solely on the jamming mitigation part of the DDMR system [7]. The following diagram demonstrates the fundamental concepts and components of the mitigation section of the DDMR system:

[Microcontroller] → [Direct Digital Synthesizer] → [Op Amp] → [Voltage Controlled Oscillator] → [Directional Antenna] → [Drone Jamming]

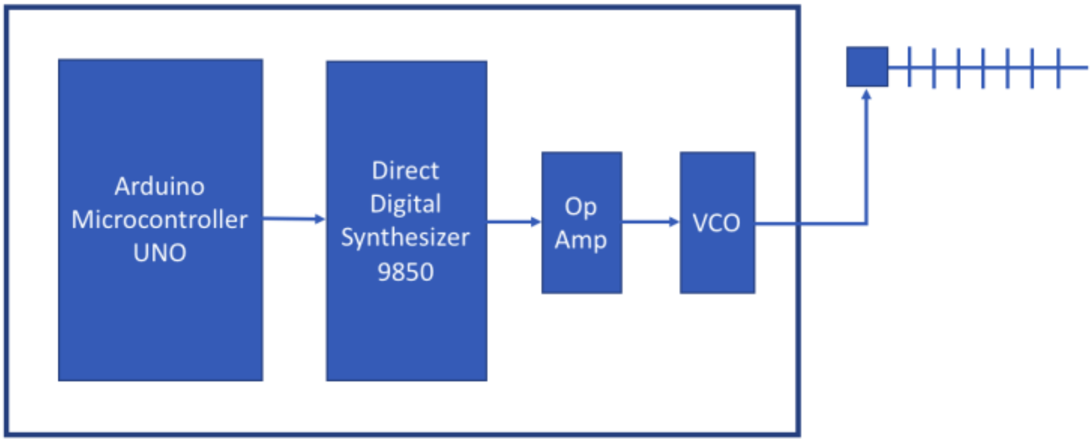


Figure 3. General Concept of the Mitigation Section of the DDMR System

1.5 Thesis Statement

The purpose of this thesis is to determine the optimal jamming sweeping frequency for the 2.4GHz to 2.5Ghz frequency band, also known as the ISM Band, while maintaining a sufficient power level at each frequency within this frequency bandwidth in order to effectively disrupt the communications link with the majority of commercial drones operating on this carrier frequency. This thesis includes an analysis of the optimal sweeping frequency's power spectrum, simulation, and experimentation of the sweeping jamming frequency. This thesis considers an optimal sweeping jamming frequency as one that has the highest hit rate and requires the least amount of power for the jamming system to operate effectively. The thesis requires the design and implementation of an electronics circuit that created a variable voltage offset and sinusoidal waveform function generator in order to achieve the optimal sweeping jamming frequency waveform.

Chapter 2: Control and Communication Links of sUAS

2.1 Spread Spectrum Systems

There are two common types of communications signals used to secure the communications links of a drone or sUAS – direct sequence spread spectrum and frequency hopping spread spectrum. Spreading the communications signal over the spread spectrum offers several distinct advantages as compared to the communicating over fixed frequencies.

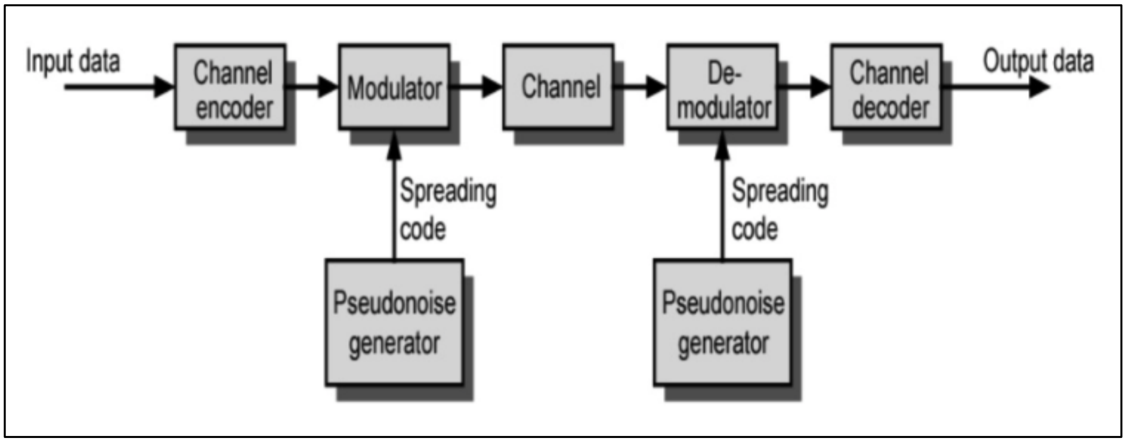


Figure 4. Basic Block Diagram of the Digital Spread Spectrum [10]

First, spread spectrum signals are much more resistant to interference and jamming. Second, the spread spectrum signals can be very difficult to intercept. The spread spectrum affords the ability to share a wider bandwidth without sacrificing interference of the signal. These are a few reasons why the military has implemented spread spectrum techniques since World War II and also why, within the last few decades, it is more commonplace in the civilian marketplace.

2.2 Direct-Sequence Spread Spectrum

Direct-Sequence Spread Spectrum (DSSS) is a type of spread spectrum modulation developed by the U.S. Department of Defense (DOD) in response to ECM technology.

Initially, DSSS was limited to military applications before being adopted into the commercial domain. DSSS spreads the digital signal across a broad bandwidth and occupies the entire bandwidth simultaneously as the signal is hopping across various frequencies within the bandwidth [10] (See Figure 4). This allows the DSSS signal to operate efficiently at higher data rates with a lower signal-to-noise (SNR) ratio compared to the Frequency Hopping Spread Spectrum (FHSS). DSSS technology allows the user of an sUAS to communicate securely with a low probability the signal will be interfered or jammed by an ECM.

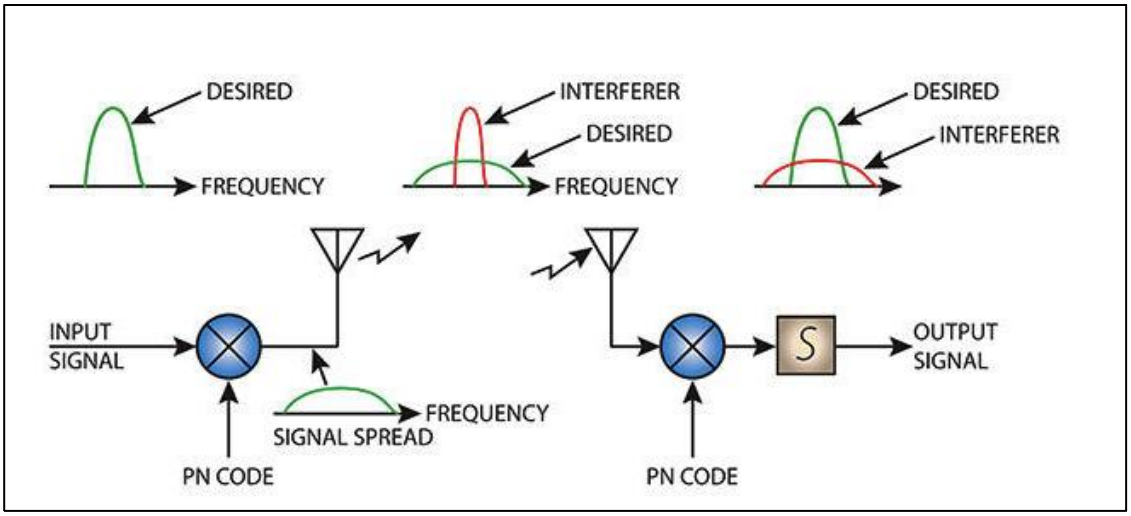


Figure 5. General DSSS Process [13]

DSSS signal is modulated through a redundant bit sequence known as pseudorandom noise, or PN code. The transmitters and receivers of the communications signal know the sequence of the PN code [14]. The PN code is independent of the data in the communications signal. The PN code allows the signal to be spread through a much wider bandwidth. This spread spectrum technique will make interfering with or jamming the signal more challenging because it uses a wider bandwidth. Since the receiver knows the

PN code, or spreading code, it will be removed in order to reconstitute the communications signal to its original form [14].

2.3 DSSS General Parameters

Each DSSS channel is 22 MHz wide in bandwidth and is separated by at least 5 MHz from any other channel. This means there are only three unique, non-overlapping bands within the 2.4 GHz to 2.5 GHz ISM band [15]. If the bands are non-overlapping, there is 3 MHz bandwidth between each band. Dwell time is not a concern with DSSS communications, as the basic principle with this spread spectrum technique requires a shift of phase rather than a shift of frequency [16]. Two common DSSS phase shift keying modulation techniques include binary phase shift keying (BPSK) and differential phase-shift keying (DPSK).

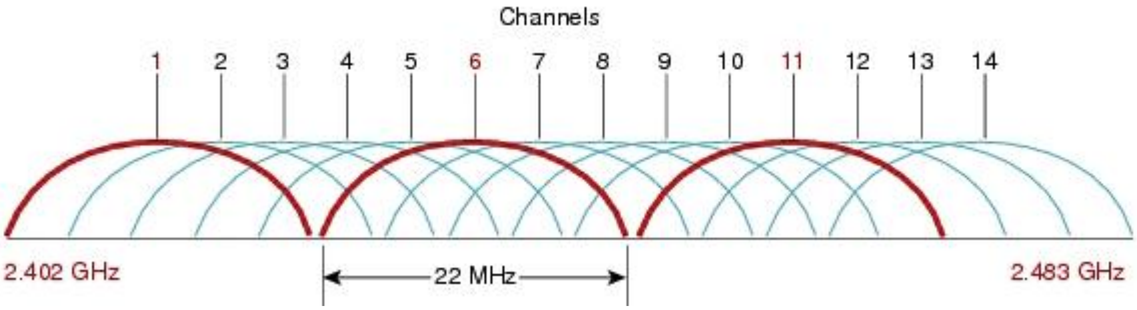


Figure 6. DSSS Channel Concept [15]

2.4 Frequency Hopping Spread Spectrum

The other commonly used anti-jamming technique is achieved through frequency hopping spread spectrum (FHSS). Similar to the DSSS, the transmitter and receiver must have some predetermined knowledge of the communications signal in order for the link to be successful. In the FHSS case, the transmitter and receiver know the frequency hopping sequence. This technique requires the signal to rapidly change frequencies at higher energy levels and narrower bandwidth as compared to the DSSS. The dwell time is how long the signal is present at a particular frequency. The hop time is the length of time it takes to change frequencies. Both the dwell time and hop time must be considered when utilizing this anti-jamming technique.

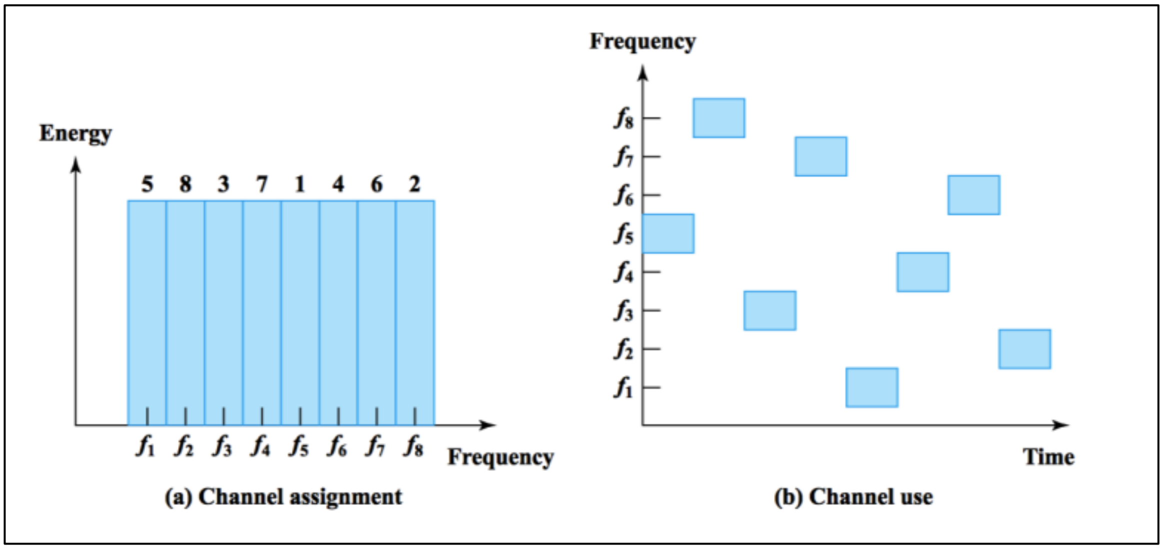


Figure 7. General FHSS Channel Concept [17]

2.5 FHSS General Parameters

Within the ISM band, which is approximately from 2.4 GHz to 2.5 GHz, there are at least 75 channels, or carrier frequencies, and each channel is typically 1 MHz to 2 MHz wide. According to the FCC, the minimum bandwidth between channels on the ISM band is 25 kHz [18]. However, it is common practice for an sUAS to have a larger hop between its carrier frequencies of approximately 6 MHz to 10 MHz to allow the communications signal to utilize more of the bandwidth available in the ISM band. Unlike the DSSS signals, a FHSS signal does not use overlapping channels per the FCC § 15.247 [18]. Furthermore, the FCC has limited the maximum dwell time for any frequencies on a channel to 400 ms [18]. Most commercial drones that use FHSS communications have a dwell time of 100 ms to 200 ms.

Chapter 3: General Analysis of Frequency Sweeping Jamming and Its Effectiveness

3.1 Probability of Intercept

A critical component of jamming a drone requires the ability to effectively intercept its communications link. Low-probability-of-intercept (LPI) radar was developed to intentionally make detection and interference difficult through DSSS and FHSS techniques. Typically, there are four kinds of intercept for consideration: spatial domain, frequency domain, time domain, and others [19, 20]. This thesis and the proposed DDMR solution focused on the time domain, for which the minimum intercept duration time is needed to disrupt the communications link of a drone. Within the FHSS context, this means the number of "hits" or the coincidences when the jamming frequency overlaps the communication frequency. If the jamming spectrum "hits" on the communications spectrum with enough energy and incidents, the jamming frequency will interrupt the communications link between the transmitter and drone. There are a few hypothesized methods on how best to calculate an effective hit rate, or probability of intercept (POI), through computer simulations and experimentation.

3.2 Self and Smith Model

The most common method to find the POI is a model developed by A.G. Self and B.G. Smith, *Intercept Time and Its Prediction* [21]. Self and Smith continued and improved upon the original theory from B.R. Hatcher's *Probability of Intercept and Intercept Time* [22]. The Self and Smith method is often found in textbooks and articles that discuss electronic warfare, and it is considered the standard for finding the POI for ECM technology. The Self and Smith [19, 21] method analyzed the communications frequency and the jamming frequency as two independent window functions, and it identified the overlapping coincidences within the respective pulse trains. The method is versatile and applicable in situations where there are three or more windows functions, also referred to as pulse trains.

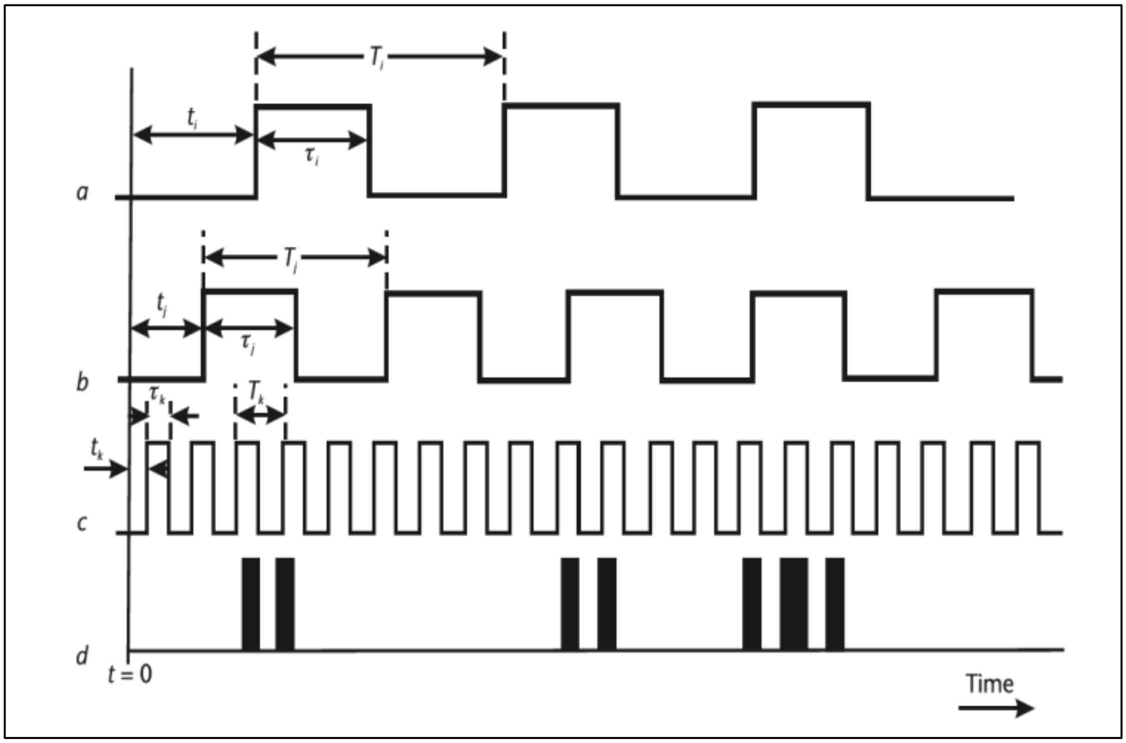


Figure 8. Basic Windows Functions: “a” is pulse train i, “b” is pulse train j, “c” is pulse train k, “d” is pulse train of overlaps [19]

“The key formulae are summarized:

$$T_0 = \frac{\prod_{j=1}^{M}(\frac{T_j}{\tau_j})}{\sum_{j=1}^{M}\left(\frac{1}{\tau_j}\right)} \qquad (1)$$

The mean period between M window functions of pulse train overlaps is T_0, and the mean window period is T_j. For M = 1, 2, and 3, this equation becomes the following explicit form:

M = 1 $$T_0 = T_1 \tag{2}$$

M = 2 $$T_0 = \frac{(T_1 T_2)}{(\tau_1 + \tau_2)} \tag{3}$$

M = 3 $$T_0 = \frac{(T_1 T_2 T_3)}{(\tau_1 + \tau_2 + \tau_3)} \tag{4}$$

where T$_1$, T$_2$, and T$_3$ are the periods for each of the window functions whereas τ$_1$, τ$_2$, and τ$_3$ are the window durations. For all pulse train overlaps M, the mean duration, τ$_0$, is given by:

$$\frac{1}{\tau_0} = \sum_{j=1}^{M} \frac{1}{\tau_j} \tag{5}$$

which, for M = 1, 2, and 3, becomes

M = 1 $$\tau_0 = \tau_1 \tag{6}$$

M = 2 $$\tau_0 = \frac{1}{(\frac{1}{\tau_1} + \frac{1}{\tau_2})} \tag{7}$$

M = 3 $$\tau_0 = \frac{1}{(\frac{1}{\tau_1} + \frac{1}{\tau_2} + \frac{1}{\tau_3})} \tag{8}$$

For the probability of at least one intercept in time, T, is

P(T) = 1 - K$e^{-(T/T_0)}$, where K = 1 – P$_0$ (9)

And the probability of intercept occurring at the first instant, is given by

$$P_0 = \prod_{j=1}^{M} \left(\frac{\tau_j}{T_j}\right) \tag{10}$$

Declaration of an adequate intercept may require at least *m* pulses. Thus, if the pulse rate interval (PRI) of the received signal is T2, then

$$d = mT_2 \tag{11}$$

$$T_0 = \frac{\prod_{j=1}^{M}(\frac{T_j}{(\tau_j - d)})}{\sum_{j=1}^{M}\left(\frac{1}{(\tau_j - d)}\right)} \; where\, \tau_j > mT_2\text{" [16]} \tag{12}$$

3.3 Other Probability of Intercept Analysis Methods

A new methodology, developed by Harri Saarnisaari, is described in the 2016 article *Jamming Hit Rate Analysis for Frequency Agile Communications* [20]. Saarnisaari's method expanded upon Self and Smith's method and proposed a new analysis to more accurately calculate the hit rate. Saarrnisaari recognized the Self and Smith model underestimated the hit rate, particularly when there are spectral mismatches. A spectral mismatch occurs when one signal pulse is much larger than another. If a short jamming pulse is used to sweep quickly across the communications signal, it may hit on the communications signal several times due to the much longer dwell time of the hopping frequency. The original model compared these two signal pulses and calculated a single hit when, in reality, there could have been multiple hits to the communications signal. Saarnisaari [20] agreed with Self and Smith's [21] original theory for the average hit duration:

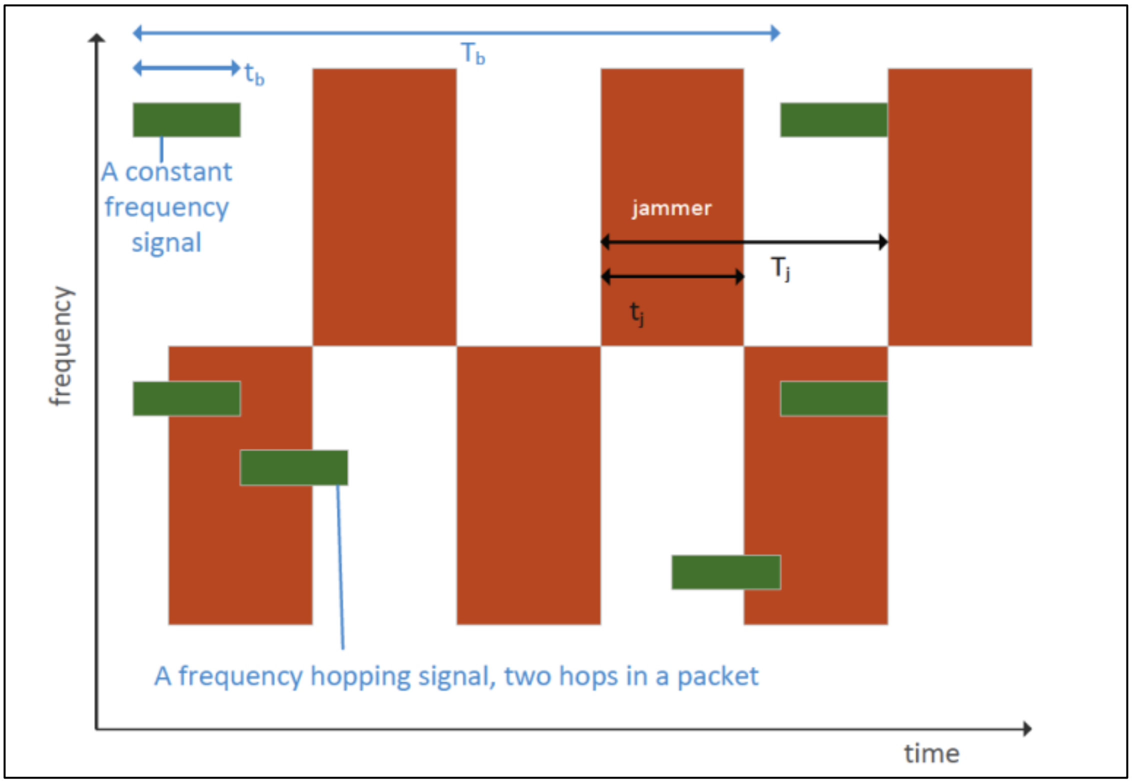
$$\mathrm{t}_0 = \frac{1}{(\frac{1}{t_b} + \frac{1}{t_j})} \tag{13}$$

where t_b is the duration of the frequency hopping communications signal and t_j is the duration of the jamming signal. The average interval between hits is:

$$\mathrm{T}_0 = \frac{T_b T_j}{(t_b + t_j)} \tag{14}$$

where T_b is the average interval length of the repeatable communications signal and T_j is the period of the jamming signal. Furthermore, in a frequency hopping scenario, the average interval length between transmissions is:

$$\mathrm{T}_b = N_b t_b, \text{ where } N_b \text{ is the number of different frequencies} \tag{15}$$



T_b
t_b
A constant frequency signal
jammer
T_j
t_j
frequency
A frequency hopping signal, two hops in a packet
time

Figure 9. Jamming Analysis Based on Saarnisaari's Methodology [20]

One of the critical components to Saarnisaari's [20] solution was calculating the spectral matching, S_M, parameters using the following:

$$\mathrm{S}_M = \min\{1, \frac{W_J}{W_S}\} \tag{16}$$

where W_J is the total bandwidth of the jamming signal and W_S is the total bandwidth of the communications signal.

When considering a spectral mismatch with a short jamming signal, the burst hit rate from the jamming signal is:

$$\mathrm{P}_I = \min\{1, \frac{T_b}{max\{T_b, T_0\}}\} \tag{17}$$

and there is a fraction of the communication signal that hits with the jamming burst:

$$\varepsilon = \mathrm{M}\frac{t_0}{t_b} \tag{18}$$

Where M is the number of hits the jamming signal has during the communications signal interval:

$$\mathrm{M} = \max\{1, \frac{t_b}{T_J}\} \tag{19}$$

With $\in$ and $\mathrm{P_I}$ known, a new hit rate, ρ, can be calculated with the following equation:

$$\rho = S_M \varepsilon P_I \tag{20}$$

Comparing the two methods can yield significantly different hit rates. For the Self and Smith model [21], which analyzed the hit rate at fast sweeping frequencies, it is intuitive that the number of hopping frequencies limit the hit rate. From the Self and Smith model [21], the hit rate is found from:

$$\rho = \frac{t_0}{T_0} \tag{21}$$

where the average hit duration, t_0, is divided by the average interval between hits, T_0.

$$\mathrm{t}_0 = \frac{1}{(\frac{1}{t_b} + \frac{1}{t_j})} \tag{22}$$

$$\mathrm{T}_0 = \frac{T_b T_j}{(t_b + t_j)} \tag{23}$$

For example, if there are 10 hopping channels, where $N_b = 10$, and assuming $t_j << t_{b,}$ $T_b = N_b t_b = 10t_b$ and $t_0 = 1$. In this case where $t_j = T_j$, $\rho_{max} = 0.10$ or 10%. The hit rate, ρ, will be reduced at a linear rate to zero as the duty cycle ratio between t_j and T_j are reduced from 100 percent to zero. For instance, if there were 8 hopping channels this would yield a hit rate of $\rho_{max} = 0.125$, or 12.5%. This model provided an upper bound limit based on the number of hopping channels utilized by the drone's communications link. The hit rate's upper bound limit will be reduced by the same factor as the number of hopping channels in the system.

The Self and Smith model [21] is limited when there are large discrepancies between the duration of the coincidental overlapping signals. In most cases, the model will underestimate the hit rates when there is a large spectral mismatch. The spectral mismatch creates an increase to the burst hit period that results in a lower burst hit rate. Saarnisaari's method [20] addressed the limitations of the Self and Smith model [21].

Contrasting Saarnisaari's methodology with the same fast sweeping frequencies considered within this thesis, the spectral matching coefficient, S_M, would be 1 because the jamming bandwidth exceeds the communications bandwidth. The burst hit rate, P_I, will be 1 because the average interval length between repeating communication transmissions, T_b, will be much greater than average interval between hits, T_0. Also, T_b and t_b will remain the same for the purposes of this example. Therefore, it is only necessary to find ε for the hit rate. The distinct difference between the two methodologies was that Saarnisaari considered the number of hits the jamming signal has during the communications signal interval. This produced a higher upper bound limit when compared to Self and Smith. Using the same parameters studied for Self and Smith [21], the hit rate using Saarnisaari's method [20] is $\rho_{max} = S_M \varepsilon P_I$. Again, this was due to the fast sweeping frequencies and can be observed below where $t_j << t_b$.

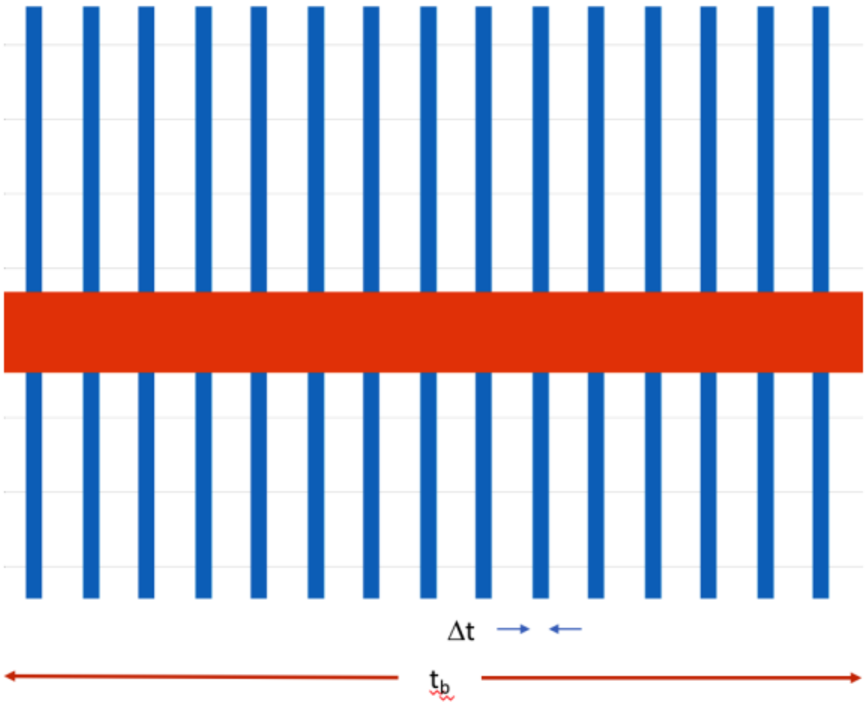


Figure 10. General Jamming Analysis with Fast Sweeping Jamming

Figure 10 is an example of the burst communications frequency (represented in orange) and the sweeping jamming frequency (represented in blue). The average hit duration, t_0, is the sum of all Δt's divided by the length of the hopping frequency, t_b. This is a better visual representation of the hit rate with fast sweeping jamming frequencies.

Neither Self and Smith or Saarnisaari provide a method for finding an optimal sweeping frequency, because they simply provide boundary limits as the hit rates remained constant. Saarnisaari stated "if the communication signal duration is much larger than the duration of the jamming signals, then $t_0 = t_j$. Therefore, min $\{t_b, t_j\}$ is the upper bound for the sole hit duration…" [20] Since $t_0 = t_j$, the revised hit rate is a ratio of t_j/T_j. This is true with the large spectral mismatch because $T_0 = T_j$ as long as $t_j << t_b$. In other words, if $t_j = 0.1T_j$, then the hit rate will be approximately 10%. Or if $t_j = 0.5T_j$, then the hit rate will increase to 50%.

3.4 Hit Rate Simulation

A MATLAB simulation was developed in an attempt to follow Saarnisaari's methodology. The communications signal simulated in MATLAB used 8 channels to be consistent with most commercial sUAS, such as the DJI Phantom drones. Some cheaper and less sophisticated drone use fewer channels for their communications links.

The MATLAB simulation jamming frequency utilized a sinusoidal evolution pattern. From previous research and experimentation[1], this waveform is considered a robust and effective modulation pattern to jam a drone communications signal link. A sweeping sinusoidal waveform at high frequency rates will ultimately jam any communications signals, but this process can have unintended consequences by adversely affecting other communications signals. Furthermore, faster sweeping frequencies require more power to operate the components of the DDMR system [7] or any jamming system. The primary objective of creating a MATLAB simulation was to help validate the optimal sweeping jamming frequency.

To mitigate any anomalies of the random set of 8 channels from MATLAB's random number generator, the simulation had a large sample size of 125,000. In other words, an array was created using the *randperm* function in MATLAB to generate 8 random numbers equivalent to frequencies contained within the ISM frequency band. These 8 values were placed in an array in a pattern which repeated 125,000 times, similar to how

[1] In the summer of 2016, the Advanced Radar Research Center at the University of Oklahoma and the Air Force Research Lab from Tinker Air Force Base built and tested an initial prototype DDMR system. These results verified the DDMR system functioned effectively and jammed the communications signal link between the controller and receiver of a commercial drone.

the FHSS works with drones when a known frequency hopping pattern between a drone's transmitter and receiver for 8 channels is repeated continuously.

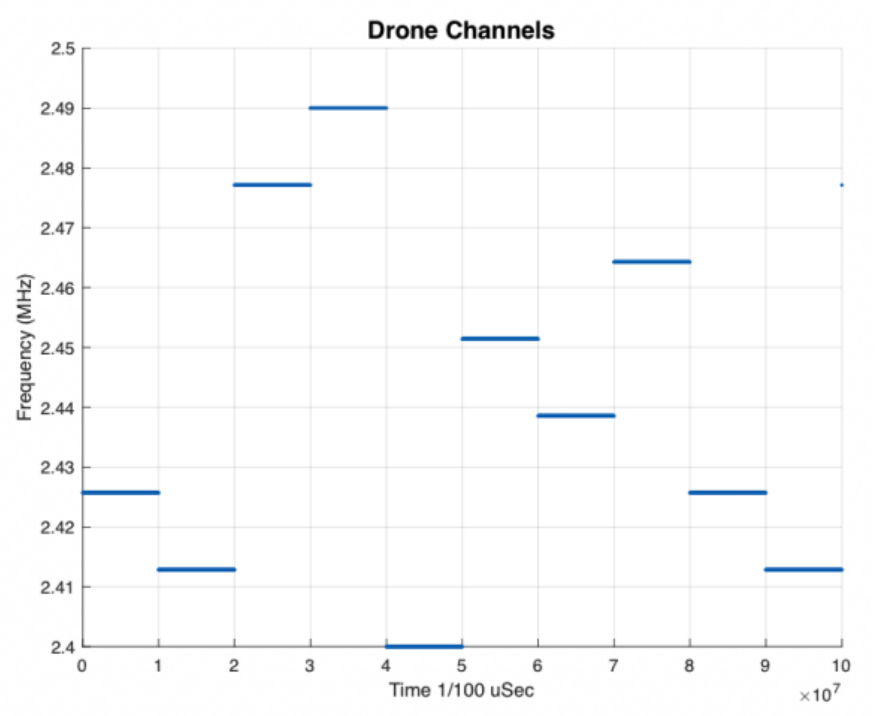


Figure 11. Example of First 8 Channels for FHSS Drone Communications Link Simulation Array with a Dwell Time of 100 Milliseconds

The jamming frequency utilized the *sin* function in MATLAB. An array for the sweeping frequency was created between 100 kHz and 1 MHz. This array was the jamming frequency, and the hit rate can be found from the difference (absolute value) between the jamming frequency and the drone's array table. The following two charts illustrated the hit rates at 100 kHz and 1MHz sweeping frequencies:

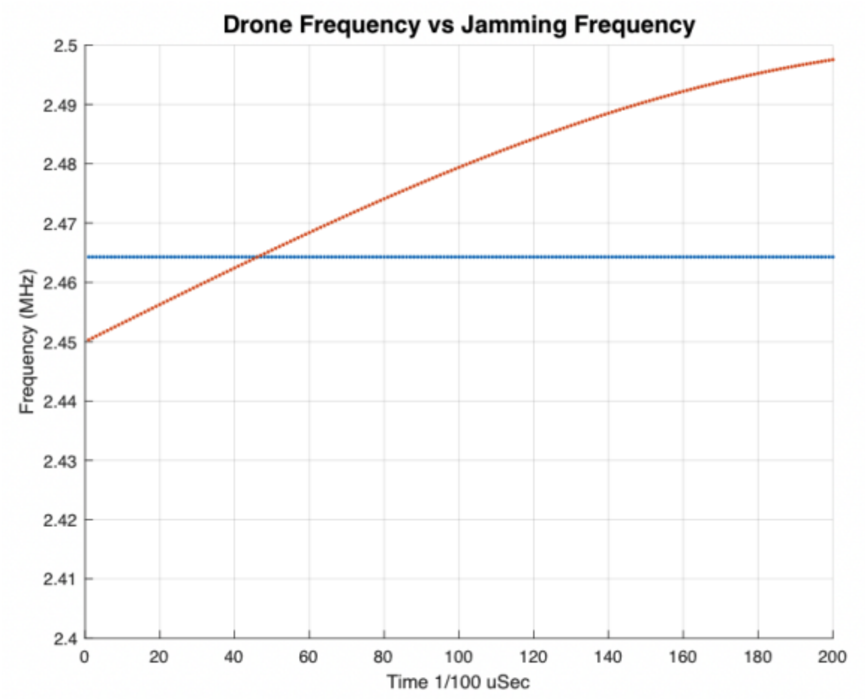


Figure 12. Time-Frequency Spectrum Evolution of Jamming Signal with 100 kHz Sweeping Frequency

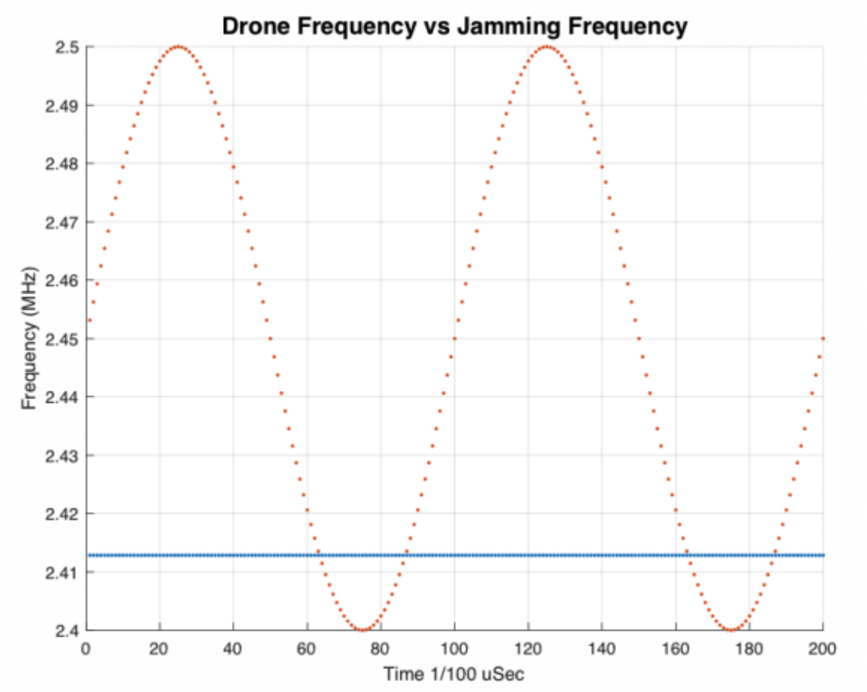


Figure 13. Time-Frequency Spectrum Evolution of Jamming Signal with 1 MHz Sweeping Frequency

Hits were counted anywhere the drone array and the jamming array overlapped within a 3 MHz[2] bandwidth. This ensured any hits on the 1 MHz bandwidth drone array, a typical frequency hopping bandwidth for each communications channel utilizing FHSS in commercial drones, were counted as the jamming frequency swept across the drone's frequency band. The total hit rate was found by adding the total number of hits divided by the length of the drone's non-repeating array table. The simulations can be easily replicated for different bandwidths, sweeping frequencies, and step sizes as appropriate.

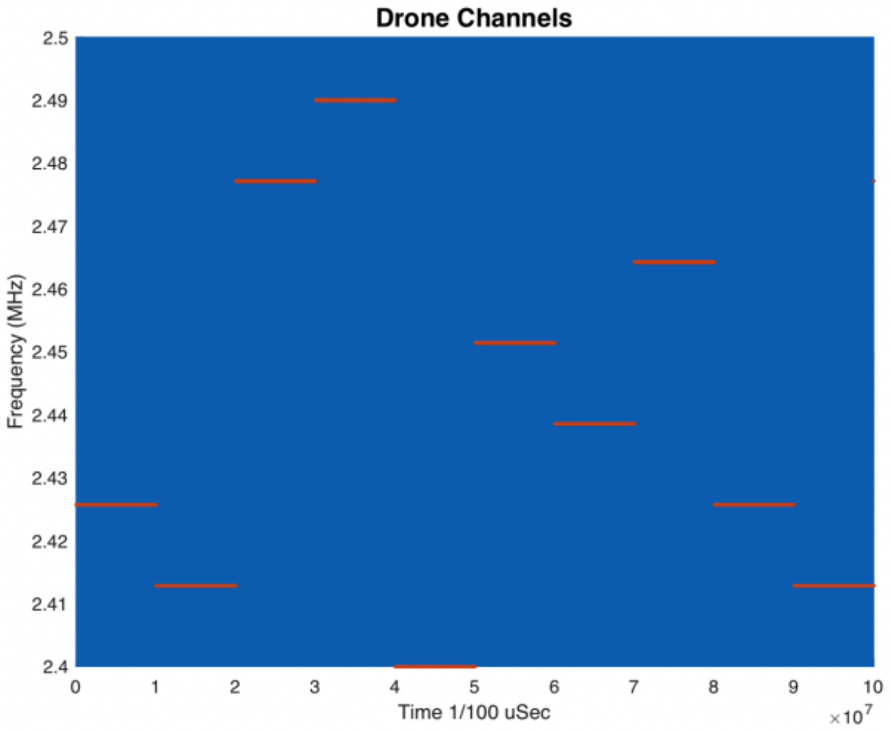


Figure 14. Drone Frequency Hopping Versus 100 kHz Jamming Sweeping Frequency

The jamming sweeping frequency in Figure 14 is sweeping at such a fast rate it appears on the plot as a solid blue background, and the drone channels are represented

[2] Oscilloscope measurements of the VCO from the DDMR prototype demonstrated a 3 dB bandwidth half power point estimated at approximately 5 MHz. Therefore, a 3 MHz boundary window was selected as a reasonable and conservative approach to evaluate hit rate performance with the simulation and experiments set forth in this thesis.

in orange. A much closer view, shown in Figure 15, is needed to observe the sweeping simulated by the MATLAB code.

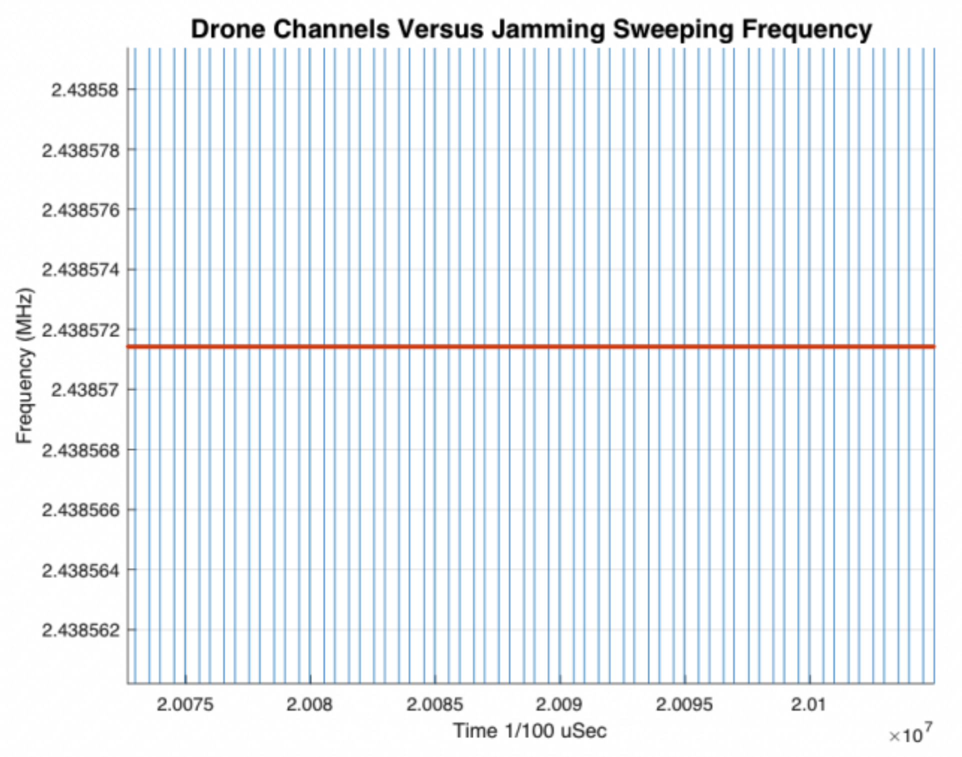


Figure 15. A Close-Up View of Drone Frequency Hopping Versus 100 kHz Jamming Sweeping Frequency

The following chart demonstrates the hit rates at various frequencies between 100 kHz and 1 MHz.

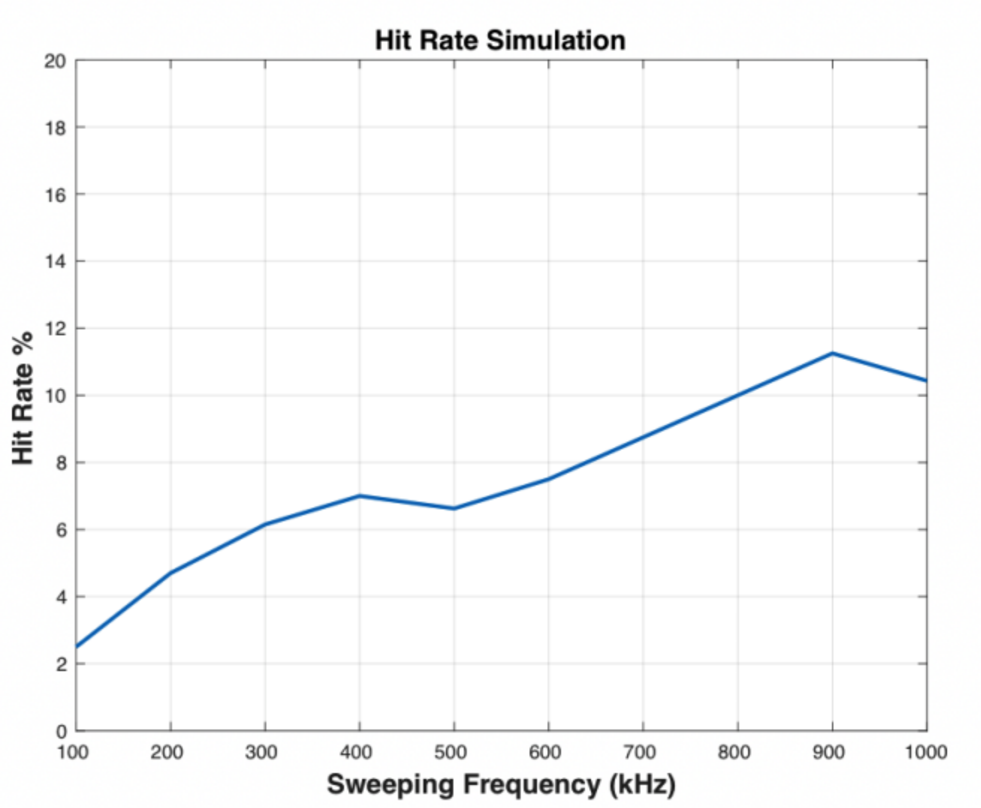


Figure 16. Hit Rate Simulation

The simulations demonstrated a sinusoidal sweeping frequency at 100 kHz had the lowest hit rate of approximately 2.5 percent. This was less than both hit rates suggested by Self and Smith [21] and Saarnisaari's [20] methods. The simulation showed the hit rate increased as the sweeping frequencies increased, peaking at 900 kHz with a hit rate of approximately 11.25 percent. The hit rate decreased to approximately 10.3 percent at a sweeping frequency of 1 MHz. All of these hit rates were less than the upper bound limits calculated using both the Self and Smith and Saarnisaari methodologies.

According to the MATLAB simulations, a sweeping frequency approaching 900 kHz reached the point of diminished return, meaning the hit rate no longer increased. However, this might not be the optimal sweeping frequency. A lower sweeping frequency with a lower hit rate might be sufficient to effectively disrupt any communications signals within the 2.4 GHz frequency band. The higher sweeping frequencies will be more effective but require additional power. Two of the primary concerns in designing the DDMR system were size and weight. Given these considerations, a lower sweeping frequency may afford the system a smaller power source, which would help achieve the overall goal of the system.

3.5 Initial Experiments with Changing Sweeping Frequencies

An experiment to evaluate the optimal jamming sweeping frequency was performed using the Spektrum DX7S (RC drone) transmitting controller and the prototype DDMR (jammer). It was unknown how many frequency hopping channels this controller used or how long the burst communications signals lasted. Over 150 samples were collected with a digitizing oscilloscope and analyzed with MATLAB in an attempt to determine its hopping frequencies. This controller was estimated to use 22 channels to achieve its frequency hopping spread spectrum. While this controller differs slightly from the DJI Phantom controller, specifically regarding the number of frequency hopping channels, the underlying concept of jamming the transmitting communications link remained the same.

The output waveforms from the jammer were also collected with an oscilloscope, using the same sampling rate and time period as the Spektrum's controller. The Spektrum's samples at each of the 22 hopping frequencies were imported into MATLAB and processed at 10 of the jammer's distinct sweeping frequencies between 100 kHz and 1 MHz. The purpose of analyzing each of the 22 hopping frequencies was to maintain an average weighted hit rate in order to best compare the final hit rates at different sweeping jamming frequencies. Otherwise, certain hopping frequencies would have been oversampled, resulting in a skewed final hit rate.

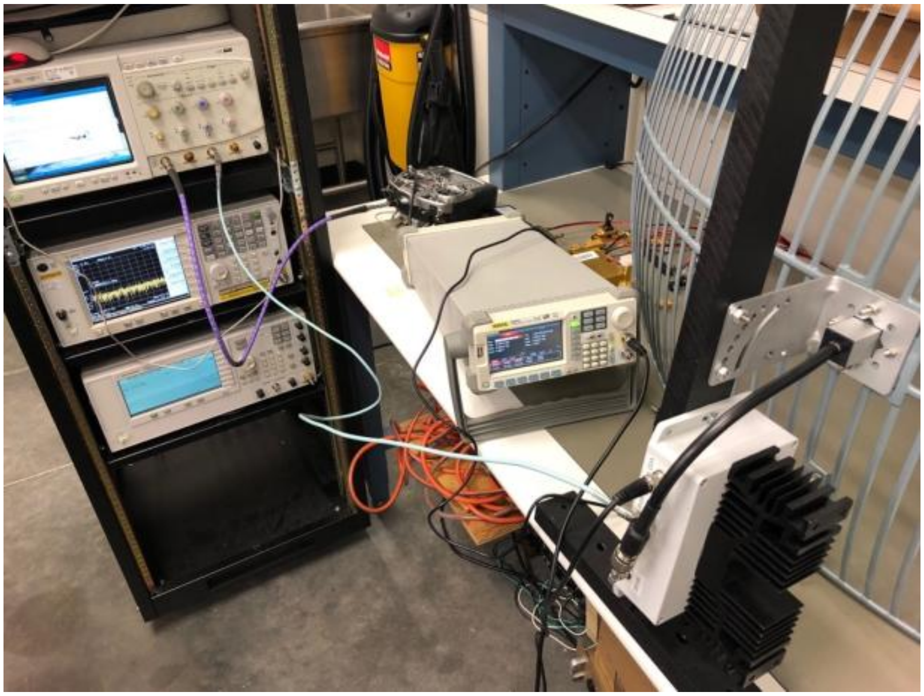


Figure 17. Oscilloscope Data Collection from the RC Drone Transmitter and the DDMR

There is one caveat regarding data collection from the oscilloscope, specifically the memory was limited within the hardware of the oscilloscope. This restricted the amount of data collected from the RC drone's transmitter and jammer's output signal. A sample period of 10 μs was the largest sample time period that could be collected with a sampling rate of 20 Giga samples per second (GSa/s). This does not affect the methodology for calculating or comparing hit rates. As previously stated, commercial drones typically have a dwell time of approximately 100 ms. The data collected can be extrapolated from 10 μs to 100 ms and the hit rate will remain unaffected since the drone's frequency would not have had sufficient time to hop to the next channel in its hopping sequence.

One of the initial observations from the data processing of the jammer's signal was the presence of harmonic waveforms. It appeared there were harmonics at every 2.5 GHz band. The bandwidth of the VCO jamming signal also increased 100 MHz at each respective harmonic. For instance, the VCO signal had a bandwidth of approximately 100 MHz at the 2.4 GHz band, and the signal was approximately 200 MHz at the 4.8 GHz band.

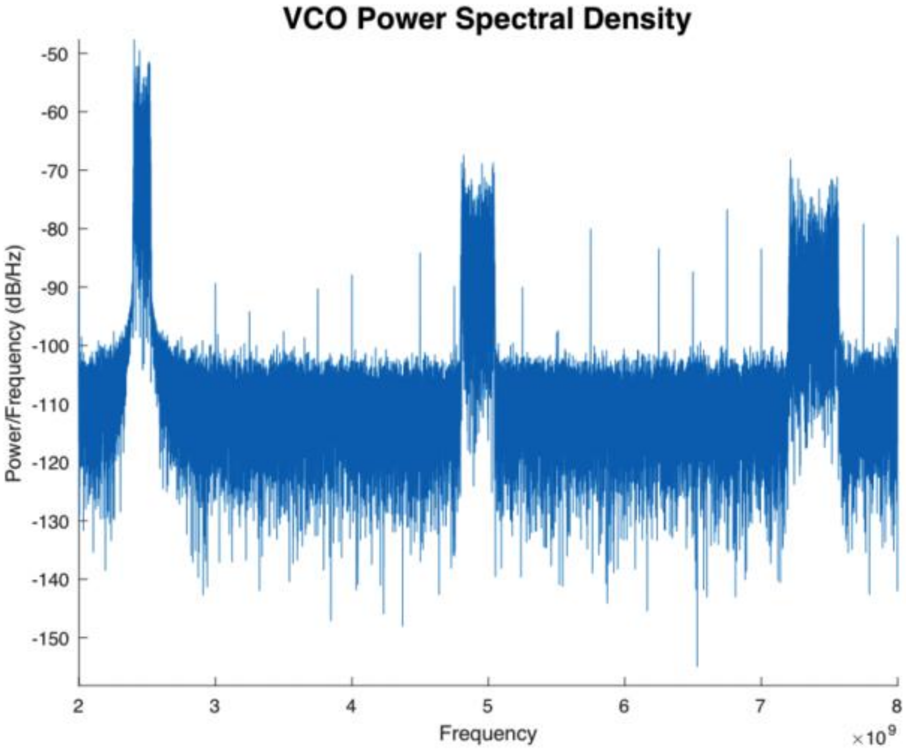


Figure 18. MATLAB Plot of Harmonics with the DDMR VCO Output

The presence of harmonics was confirmed when the jammer's output signal was collected with a spectrum analyzer. Figure 18 from the spectrum analyzer showed harmonics at 2.4 GHz, 4.8 GHz, and 7.2 GHz bands.

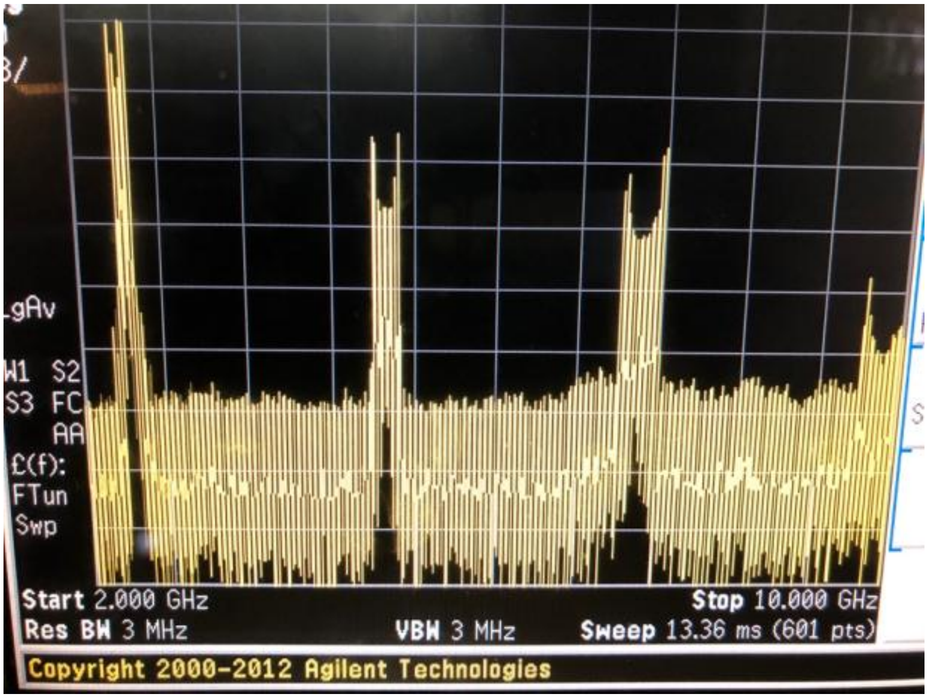


Figure 19. Spectrum Analyzer of DDMR VCO

It was important to eliminate these output frequency signals from the VCO, otherwise there would have been additional undesired frequencies outside the ISM band jammed with the DDMR. A low pass filter and band pass filter were added to the output of the DDMR's VCO to eliminate its harmonic frequencies and to ensure noise is emitted only within the ISM band.

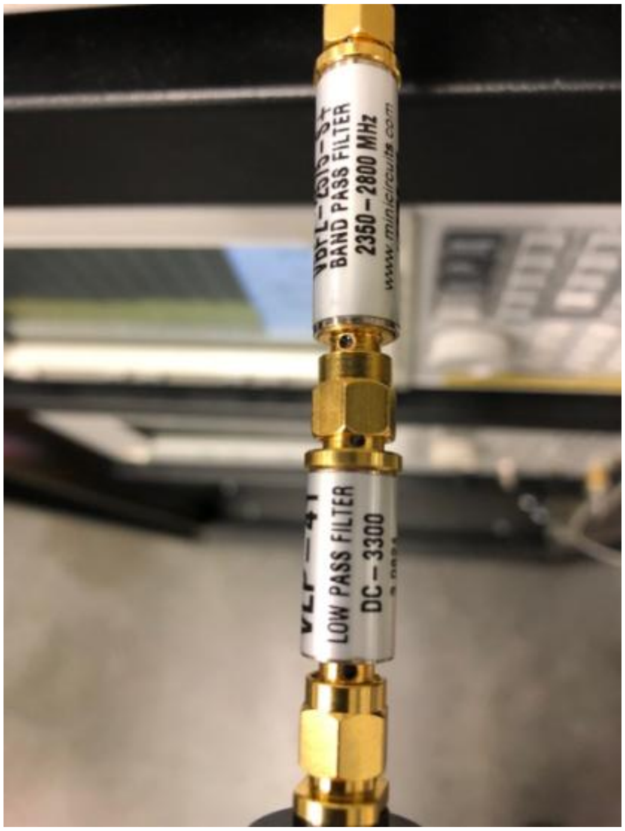


Figure 20. A Low Pass and Band Pass Filter on the DDMR VCO

Following the implementation of the hardware filters, the output signals from the jammer was again collected with an oscilloscope. The following power spectral density plot shows the RC drone's transmitter signal versus the jammer's signal with a 1 MHz sweeping frequency:

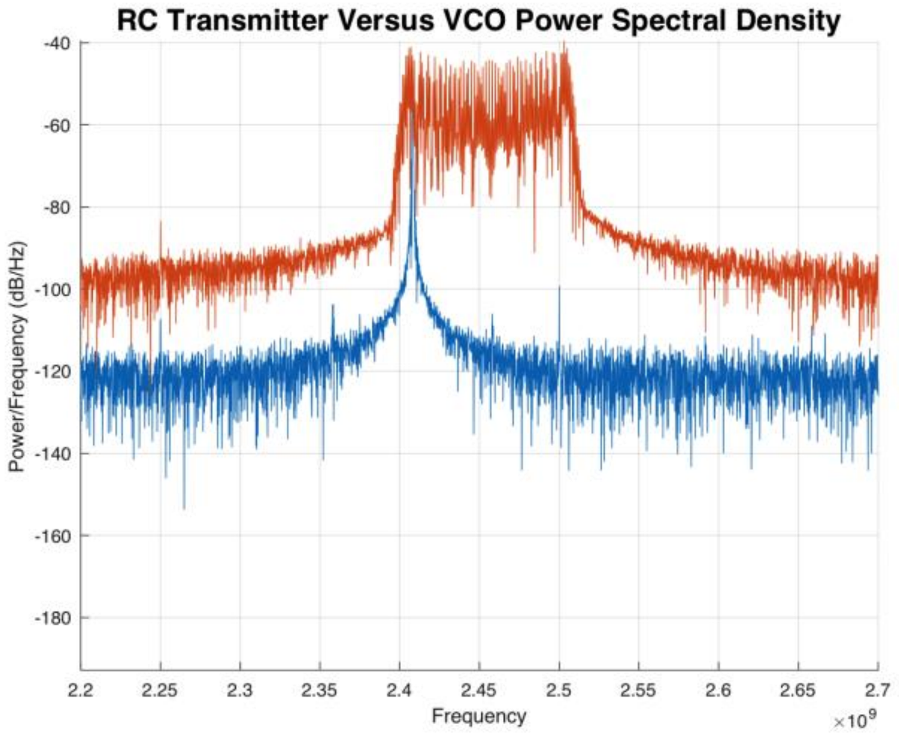


Figure 21. RC Drone Transmitter Signal (Blue) and DDMR VCO Signal Power (Red) Spectral Density MATLAB Plot

Figure 21 shows the 1 MHz sinusoidal wave sweeping frequency covering the ISM band through the DDMR system's VCO. However, in order to accurately calculate the hit rate between the two signals, the time domain must also be considered. MATLAB's spectrogram function plotted the RC drone's transmitter signal and jammer's signal with a time sample time period of 10 μs. The following plot contains the same two signals from the power spectral density plot in Figure 20:

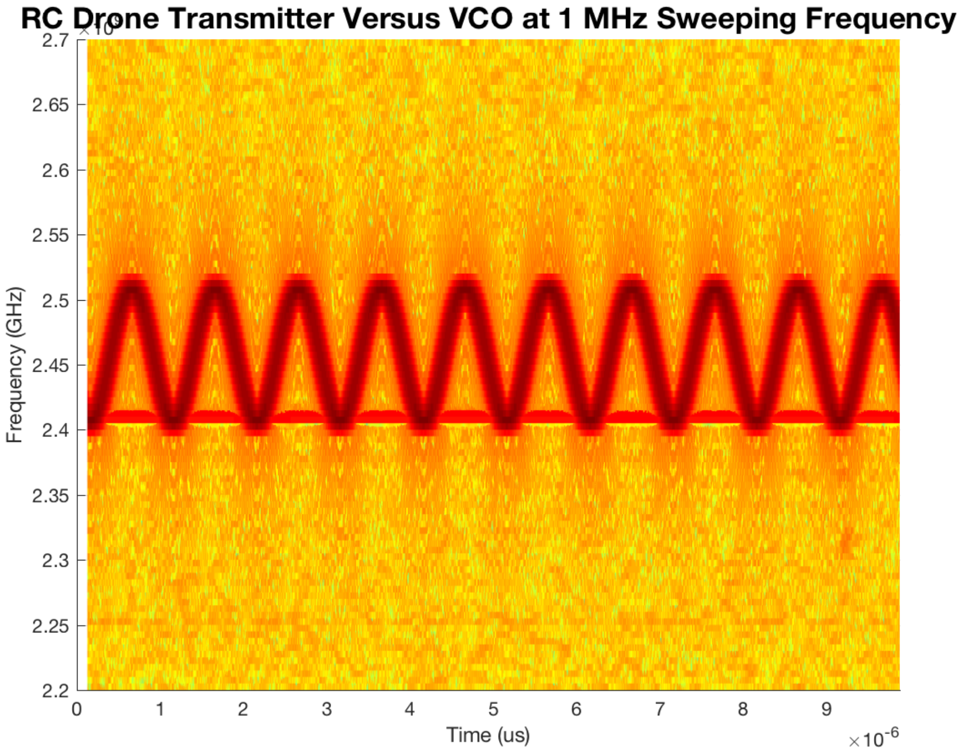


Figure 22. Spectogram MATLAB Plot of the VCO at 1 MHz Sweeping Frequency

It is easy to identify the points of intersection in Figure 22, as these are areas where there are "hits" between the jammer and drone. The duration of these pulse train overlaps were counted and then divided by the entire length (time) of the hopping frequency to determine the hit rate. The following 3D plots further demonstrate the points of intersection, or hits, between the RC drone's signal (in blue) and the jammer's signal (in red).

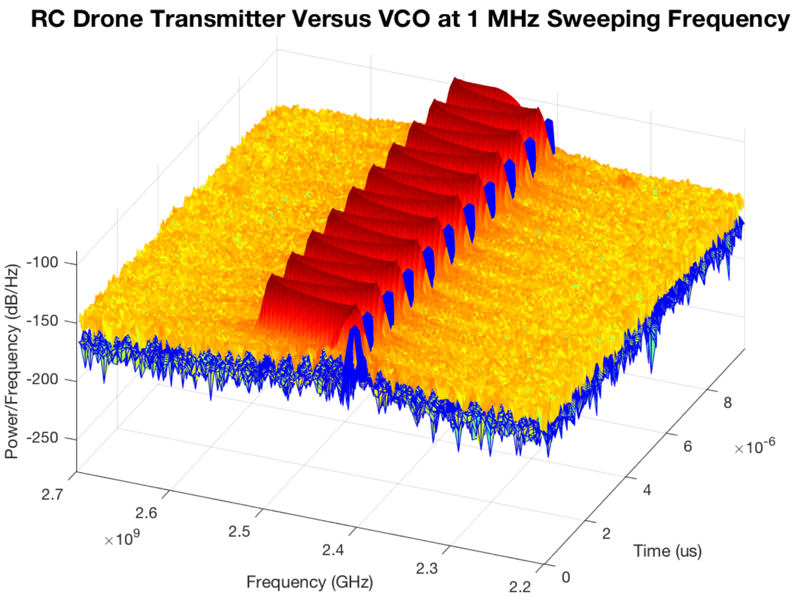


Figure 23. 3D MATLAB Plot of Drone Transmitter (Blue) and VCO (Red) with 1 MHz Sweeping Frequency

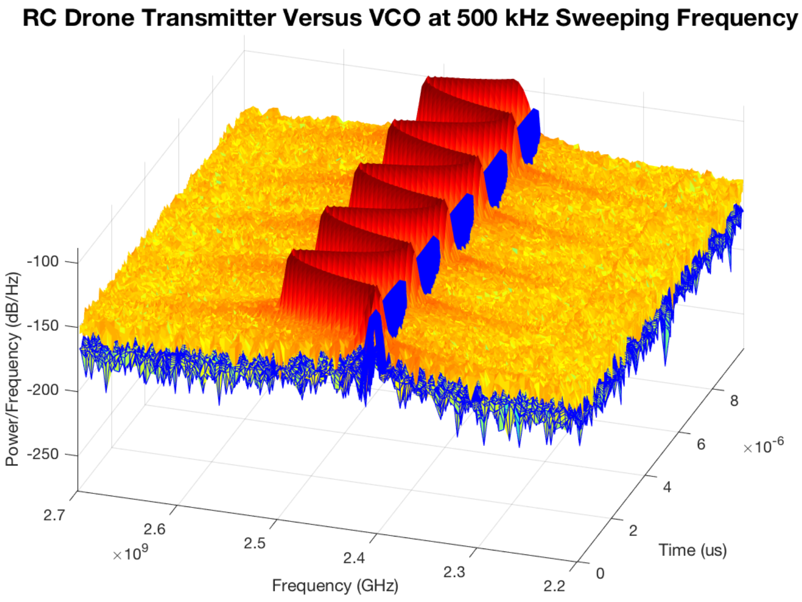


Figure 24. 3D MATLAB Plot of Drone Transmitter (Blue) and VCO (Red) with 500 kHz Sweeping Frequency

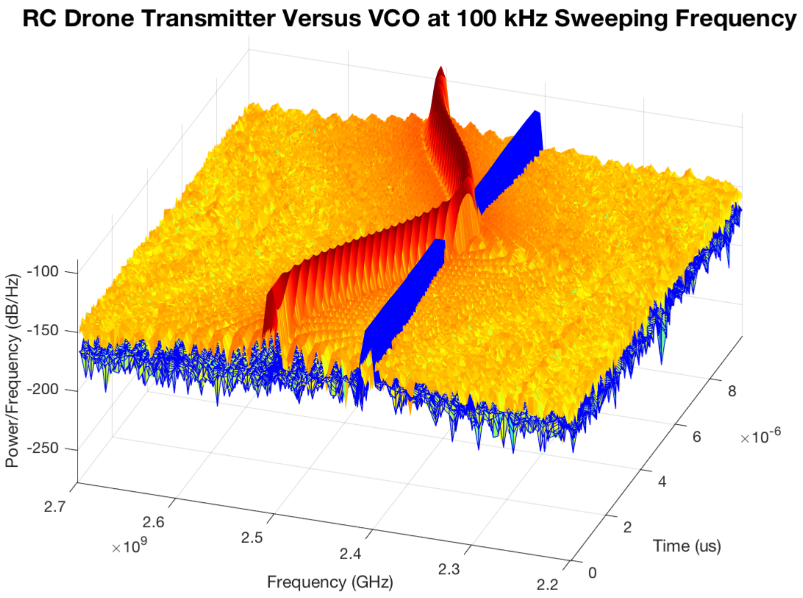


Figure 25. 3D MATLAB Plot of Drone Transmitter (Blue) and VCO (Red) with 100 kHz Sweeping Frequency

In Figures 23 through 25, the probability of intercept (POI) remained relatively constant. The POI was calculated from the Spektrum's 22 hopping channels at each of 10 sweeping frequencies. These results were very close to what Self and Smith proposed in Chapter 3.2, where $\rho_{max} = 1/N_b$ or in this case, 1/22 channels = 4.55%.

Jamming Sweeping Frequency	Average Probability of Intercept
100 kHz	4.60%
200 kHz	4.55%
300 kHz	4.60%
400 kHz	4.40%
500 kHz	4.40%
600 kHz	4.53%

Jamming Sweeping Frequency	Average Probability of Intercept
700 kHz	4.64%
800 kHz	4.59%
900 kHz	4.53%
1 MHz	4.42%

Table 1. POI Rates Calculated from Experiment

The experiment showed the highest probability of intercept occurred at a sweeping frequency of 700 kHz. This does not necessarily mean the optimal sweeping frequency is 700 kHz. The spectrogram signal in Figure 22 was further analyzed to find the maximum values for both waveforms. In Figure 26, the jammer's signal has a +/- 3 MHz bandwidth represented with a green line. Any data points contained on or within these boundary limits, which overlapped the hopping frequency, were considered *hits*, and any data points outside these boundaries were counted as *misses*.

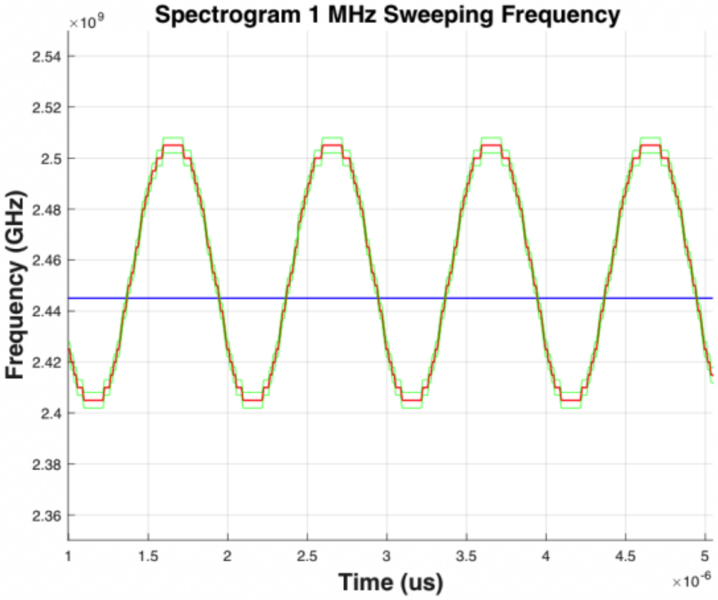


Figure 26. Spectrogram MATLAB Plot of Drone Transmitter (Blue) and VCO (Red)

Figure 27 shows there will be a longer overlapping duration, leading to a higher hit rate when the drone's signal was hopping at either end of the jammer's sweeping frequency. Figure 27 is a plot where the drone's transmitter signal was close to the jammer's lower frequency limit.

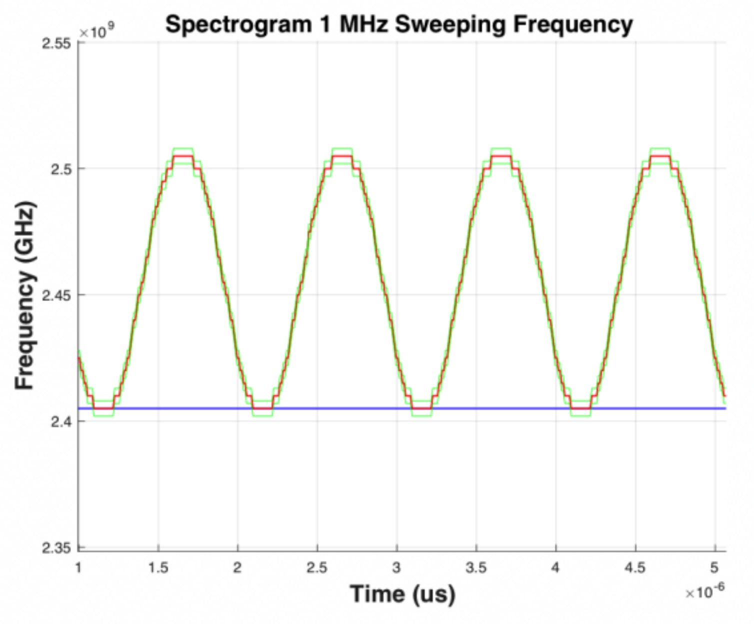


Figure 27. Spectrogram MATLAB Plot of Drone Transmitter (Blue) and VCO (Red) at Higher Hit Rate

A closer look at Figures 28 and 29, respectively, show how the hit rate differed drastically depending on the hopping frequency for the RC drone transmitter.

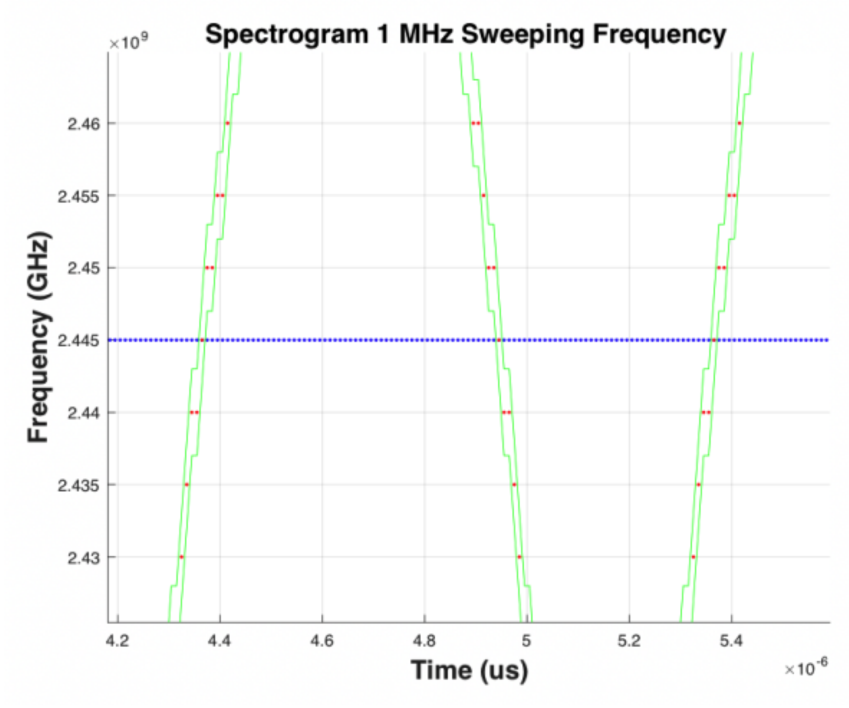


Figure 28. Closer Examination of the Hit Rate from Figure 22

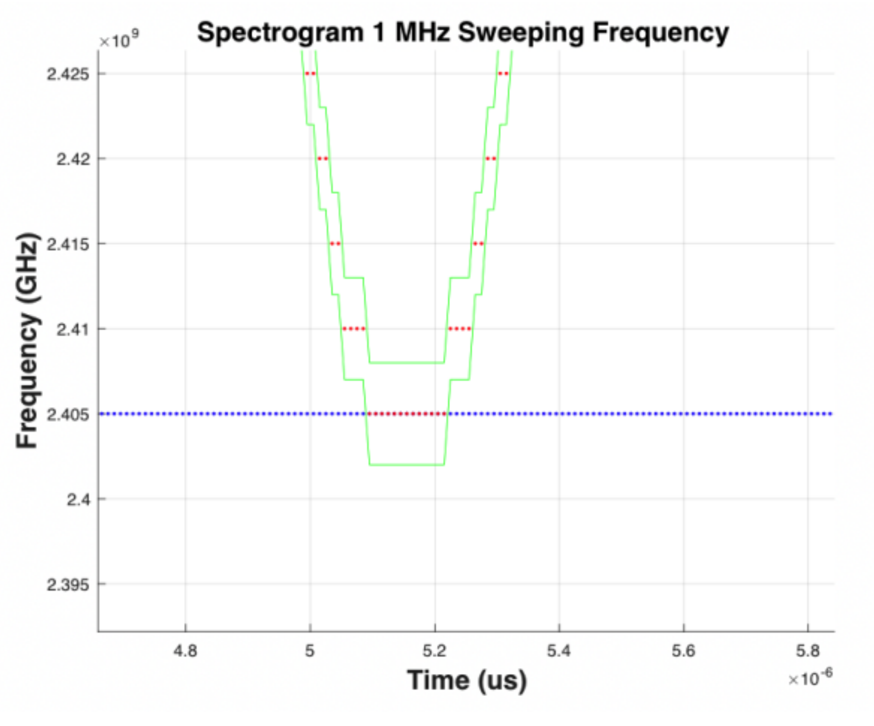


Figure 29. Closer Examination of the Hit Rate from Figure 23

Furthermore, Figures 30 and 31 demonstrate a hit and miss, respectively, between the jamming signal in red and the RC drone transmitter signal blue.

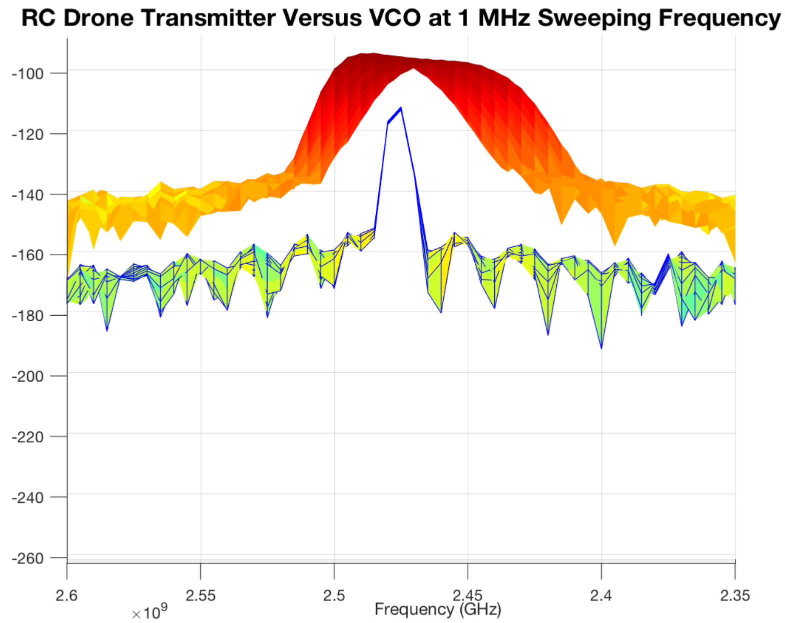


Figure 30. Spectrogram MATLAB Plot of a Hit

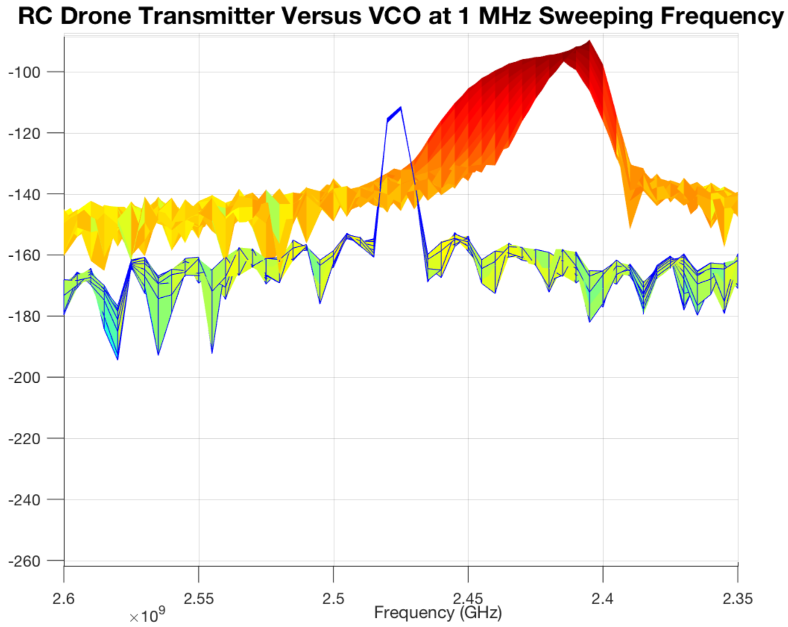


Figure 31. Spectrogram MATLAB Plot of a Miss

Similar to the MATLAB simulation in Chapter 3.4, the hit rate was calculated where the absolute value between the two signals was less than 3 MHz. Based upon the samples analyzed during the experiment, the lowest hit rate was 7.79% and the highest hit rate was 25.10%. The following chart shows the average hit rates for 22 communications hopping frequencies at each of the 10 jamming sweeping frequencies:

Jamming Sweeping Frequency	**Average Hit Rate**
100 kHz	12.72%
200 kHz	12.32%
300 kHz	12.74%
400 kHz	12.19%
500 kHz	12.20%
600 kHz	12.38%
700 kHz	12.66%
800 kHz	12.36%
900 kHz	12.09%
1 MHz	11.92%

Table 2. Hit Rates Calculated from Experiment

The experimental results showed a small deviation in the hit rate as the jamming sweeping frequency was increased from 100 kHz to 1 MHz. The sweeping frequencies appeared to show a general decrease in hit rate as the sweeping frequency increased. According to the experiment, the optimal sweeping frequency was 100 kHz, as this yielded the highest hit rate and required the least amount of energy to produce the waveform.

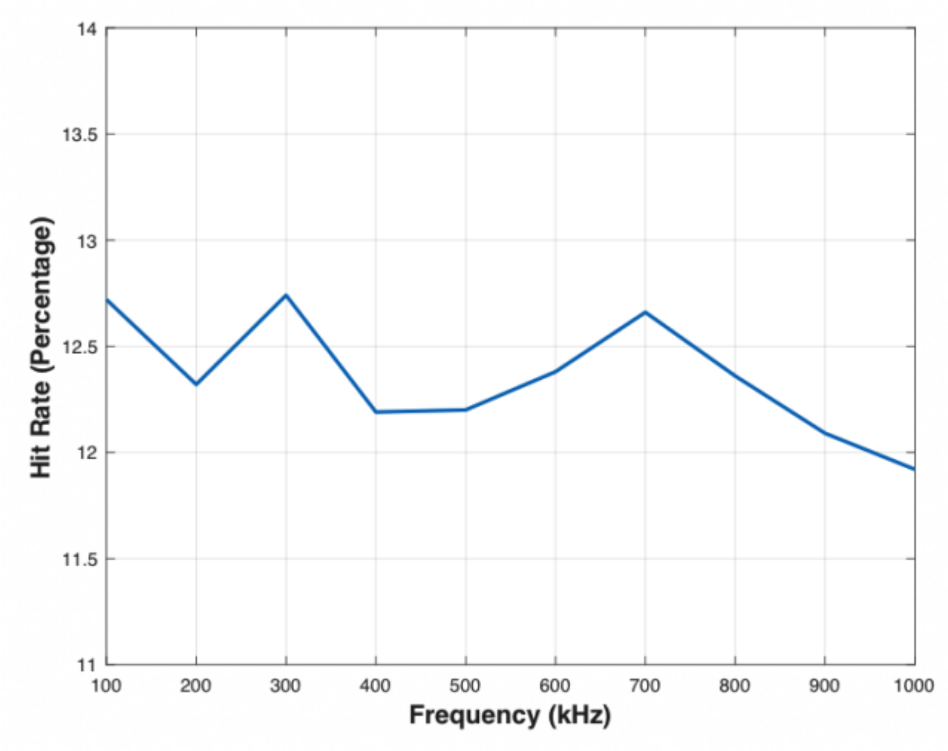


Figure 32. Experimental Hit Rate Illustrates a General Decreasing Trend (Red Line) as the Sweeping Frequency Increases

If the 22 Spektrum channels were simulated in MATLAB it would look like the following:

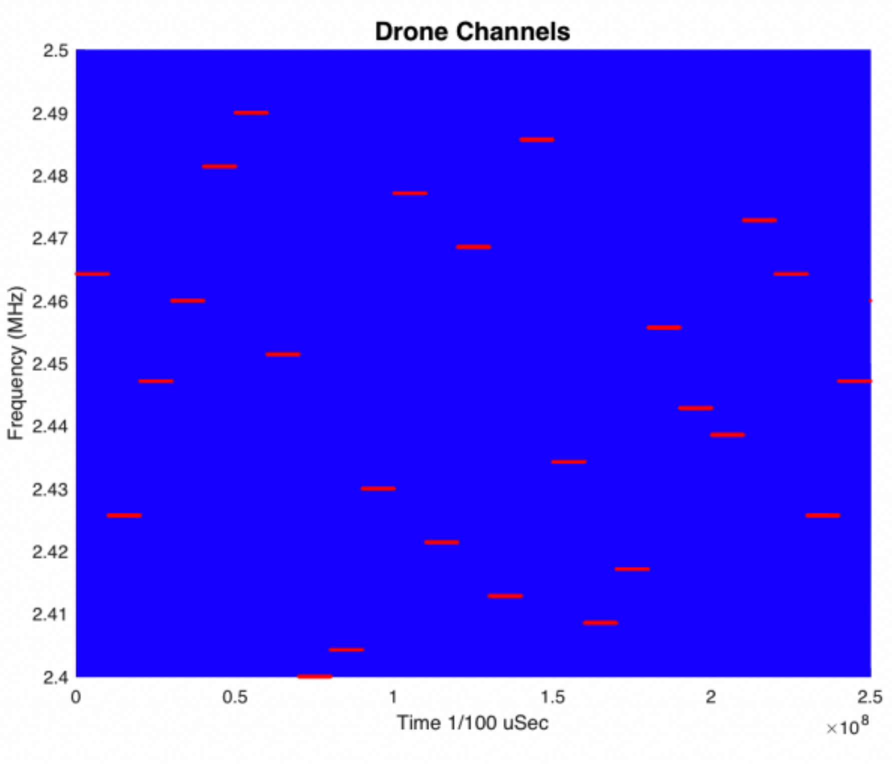


Figure 33. MATLAB Simulation With 22 Frequency Hopping Channels

When the prototype DDMR was tested in the anechoic chamber, there were two frequencies ranges that did not effectively jam the RC drone communications link: (1) sweeping frequencies below 100 kHz and (2) sweeping frequencies over 1.4 MHz. These experimental results allowed the research contained within this thesis to focus on the 100 kHz to 1 MHz sweeping frequency range.

The hit rates from the experimental results fall within the hit rate limits set forth in the theories explained in Chapters 3.2 and 3.3. One of the reasons these hit rates vary is explained with the 3 MHz boundary threshold. Changing this threshold yields different results – increasing the threshold would increase the hit rate while decreasing the threshold would decrease the hit rate. However, the most significant observation from the experiment was the hit rate variation based upon the location of the communications waveform within the ISM frequency band.

A potentially better approach to find an overall hit rate may be considered by modifying Saarnisaari's hit rate. This could be done by calculating the hit rate following Saarinsaari's method, and then further extrapolating the process over the non-repeating hopping channels. The final results would produce an equally weighted hit rate, and they would more accurately reflect the hit rate across the N_b channels. This thesis proposes an alternative method to calculating a new hit rate for a drone communications link using FHSS technology:

$$\text{Proposed New Hit Rate}, \bar{\rho} \; = \frac{\sum_{n=1}^{N_b} S_M \varepsilon P_I}{N_b} \tag{24}$$

The hit rate in jamming theory represents the portion of the communications signal adversely affected by the jamming power. It indicates the average portion of time where the communications hopping frequency and the jamming frequency are overlapping. In terms of the bit-error rate (BER), the common equation [23, 24] is:

$$\bar{P}_b = (1-\rho)P_b\left(\frac{E_b}{N_0}\right) + \rho P_b\left(\frac{E_b}{(N_0 + N_J)}\right) \tag{25}$$

Where E_b is the symbol energy, N_0 is the receiver channel noise power, and N_j is jamming noise power. The precise BER required to disable the communications link for any commercial drone will be manufacture specific. To protect the integrity of its products, this information is not made publicly available by drone manufacturers. Based on the experimental results for both the POI and hit rates as previously cited, the optimal sweeping frequency is approximately 300 kHz as it was found to have the highest hit rate.

Chapter 4: System Implementation and Design Considerations

4.1 Overall ECM System Design

There are only a few companies who manufacture and sell portable drone jamming systems. While these systems are prohibited for sale and use in the United States, the federal government and military can utilize these products outside the United States. An effective ECM system must be versatile and adjust to any radio frequency band on which the drone is operating. This system can be very challenging to create because if the jammer covers more frequency bands it will have greater power requirements. This requires the ECM system to be larger in size, heavy, and possibly less portable. For instance, the following portable jamming system is a versatile system that will jam the 2.4 GHz, 5.8 GHz, GPS, and GLONASS frequency bands. The jammer is larger than others and requires the use of a battery pack that must be attached to the jammer to operate.

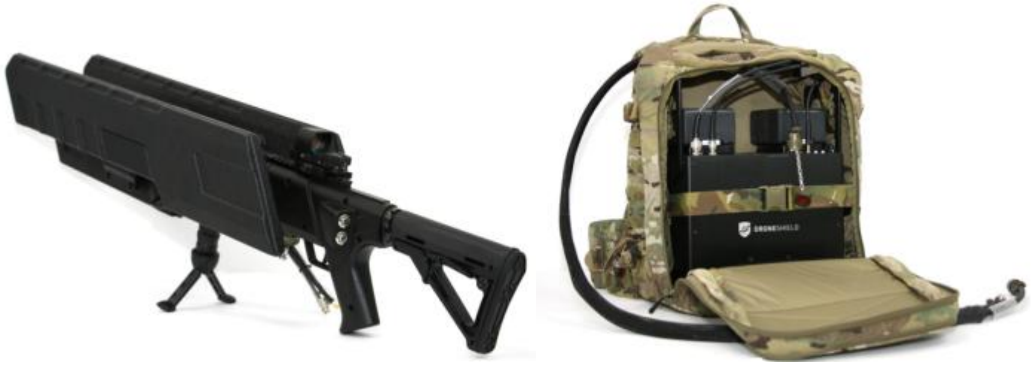


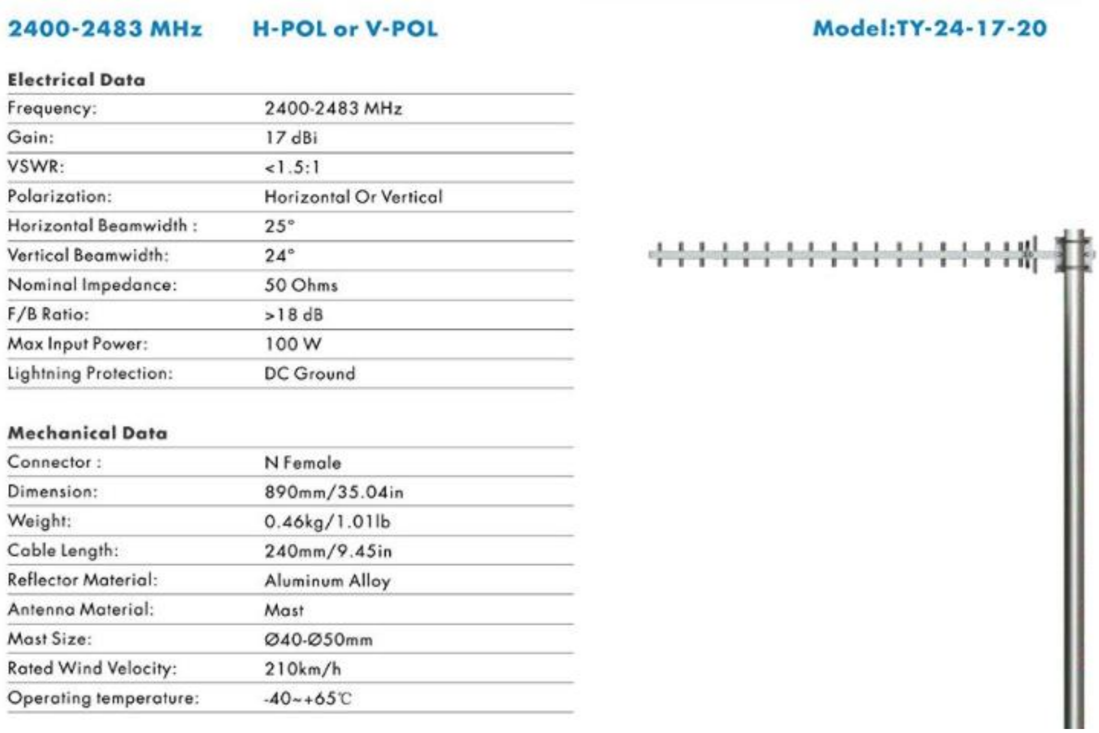
Figure 34. DroneShield DroneGun [28]

The prototype DDMR system was effective at disabling the RC drone's transmitting link in chamber experiments with the assistance of a wave function generator. This is not a practical design outside of a controlled laboratory due to its size and power requirements. This thesis focused on an improved, portable DDMR system which could be implemented outside of the lab. In order to achieve these goals, the system was developed to jam the most common commercial drone communications frequency, the 2.4 GHz band. The DDMR system sacrificed versatility for power, size, and weight.

Once the optimal sweeping frequency was determined for the DDMR's VCO, other important considerations were the antenna selection and power output, or effective range, of the jamming system. There are two general types of antennas used for jammers: parabolic reflective antennas and dipole antennas. Both of these antennas have specific features. "A parabolic antenna is an antenna that uses a parabolic reflector, a curved surface with the cross-sectional shape of a parabola, to direct the radio waves." [29] The dipole antenna essentially consists of two conductive elements that are provided with a signal. "The driving current from the transmitter is, or for receiving antennas the output signal to the receiver is taken, between the two halves of the antenna." [30] A yagi antenna is a common dipole antenna that is the ideal antenna design for any jamming system.

4.2 Impact of Antenna Design and Multipath Issues

The TY-24-17-20 yagi antenna was selected for the prototype DDMR due to its narrow beamwidth and frequency range of 2.4 GHz to 2.48 GHz. This antenna was matched to the design specification of the VCO. The yagi antenna has a gain of 17 dBi and the following characteristics:

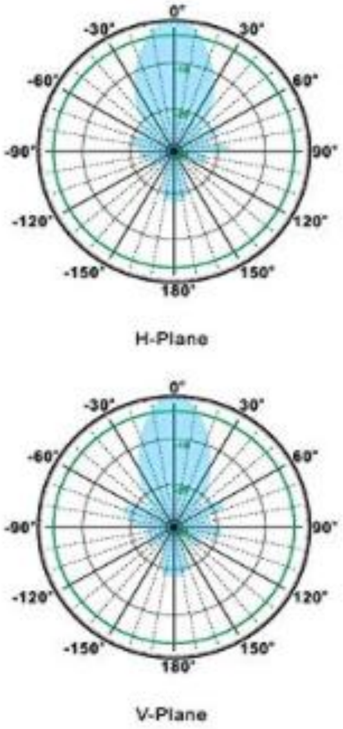


2400-2483 MHz **H-POL or V-POL** **Model:TY-24-17-20**

Electrical Data	
Frequency:	2400-2483 MHz
Gain:	17 dBi
VSWR:	<1.5:1
Polarization:	Horizontal Or Vertical
Horizontal Beamwidth :	25°
Vertical Beamwidth:	24°
Nominal Impedance:	50 Ohms
F/B Ratio:	>18 dB
Max Input Power:	100 W
Lightning Protection:	DC Ground

Mechanical Data	
Connector :	N Female
Dimension:	890mm/35.04in
Weight:	0.46kg/1.01lb
Cable Length:	240mm/9.45in
Reflector Material:	Aluminum Alloy
Antenna Material:	Mast
Mast Size:	Ø40-Ø50mm
Rated Wind Velocity:	210km/h
Operating temperature:	-40~+65℃

Figure 35. Yagi Antenna Characteristics [32]



H-Plane

V-Plane

Figure 36. Yagi Antenna Beamwidth Polarization [32]

When an RC drone's transmitter signal is propagated towards the drone's receiver, the signal will expand the further it travels. The same is true for the DDMR's VCO output signal. If there are obstacles, such as buildings or possible geographical barriers present, the signals are likely going to be reflected, refracted, or somehow interfered with making duplicate waveforms. When there are multiple waveforms present, due to the RF signals taking various paths from the transmitter to the receiver, then multipath propagation occurred. Multipath distortion presents a larger issue for the communications link between the drone's transmitter and receiver. When jamming a drone's communications link, any multipath distortion that may manifest from the DDMR's VCO signal, for instance a large building, will not be significant to its overall effectiveness. By design, the DDMR is trying to corrupt and interfere with the drone's communications link.

4.3 Hardware Design

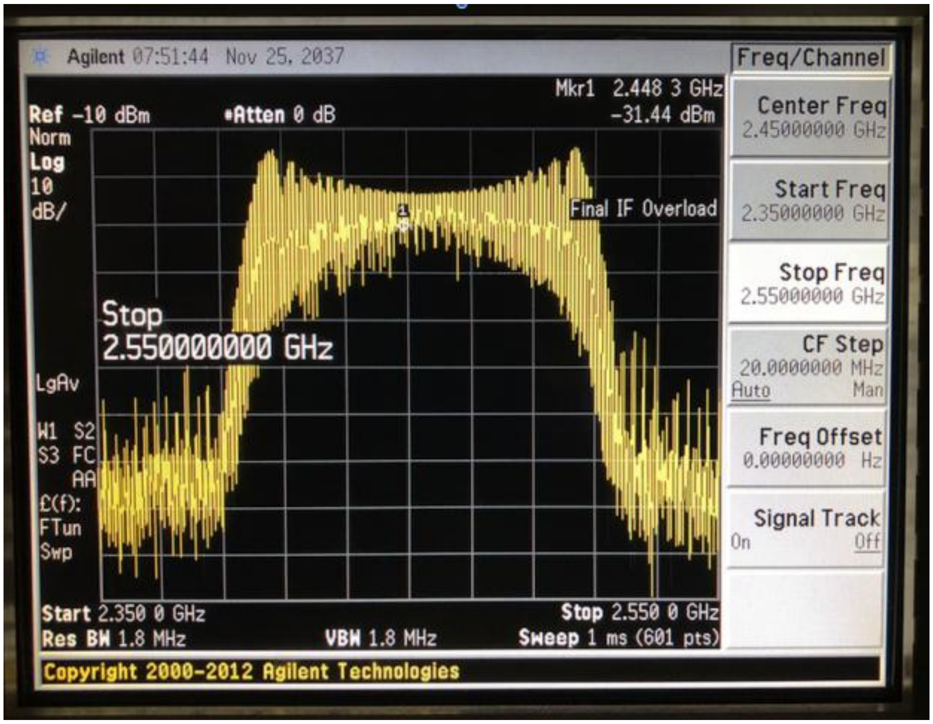
There are several factors to consider when designing the hardware for the DDMR system to make the system small, lightweight, and effective. The particular VCO selected was the ZX95-2490+ with the following performance data characteristics:

Voltage	Frequency (MHz) -55°C	 -25°C	 -85°C
5.50	2415.8	2404.3	2394.4
6.00	2433.0	2421.7	2411.9
6.50	2450.3	2438.7	2428.7
7.00	2466.7	2455.2	2445.1
7.50	2482.9	2471.5	2461.0
8.00	2498.8	2487.1	2476.7
8.50	2513.8	2501.2	2491.8

Table 3. ZX95-2490+ Performance Data [33]

The input voltage of the sine wave supplying the VCO will vary between 5.5 volts and 8.5 volts to ensure the output sweeping frequency is adequately covering the 2.4 GHz band.

A spectrum analyzer was used to measure the effectiveness of the DDMR's VCO. Screenshots were captured for 1 MHz, 500 kHz, and 100 kHz. It should be noted that a 42 dBm attenuator was placed on the output signal of the VCO into the spectrum analyzer for the measurements. The following figures demonstrate how the system covers the 2.4 GHz frequency band:


Agilent 07:51:44 Nov 25, 2037

Mkr1 2.448 3 GHz
-31.44 dBm

Ref -10 dBm
Atten 0 dB
Norm
Log
10
dB/

Final IF Overload

Stop
2.550000000 GHz

Start 2.350 0 GHz
Stop 2.550 0 GHz
Res BW 1.8 MHz
VBW 1.8 MHz
Sweep 1 ms (601 pts)

Freq/Channel

Center Freq
2.45000000 GHz

Start Freq
2.35000000 GHz

Stop Freq
2.55000000 GHz

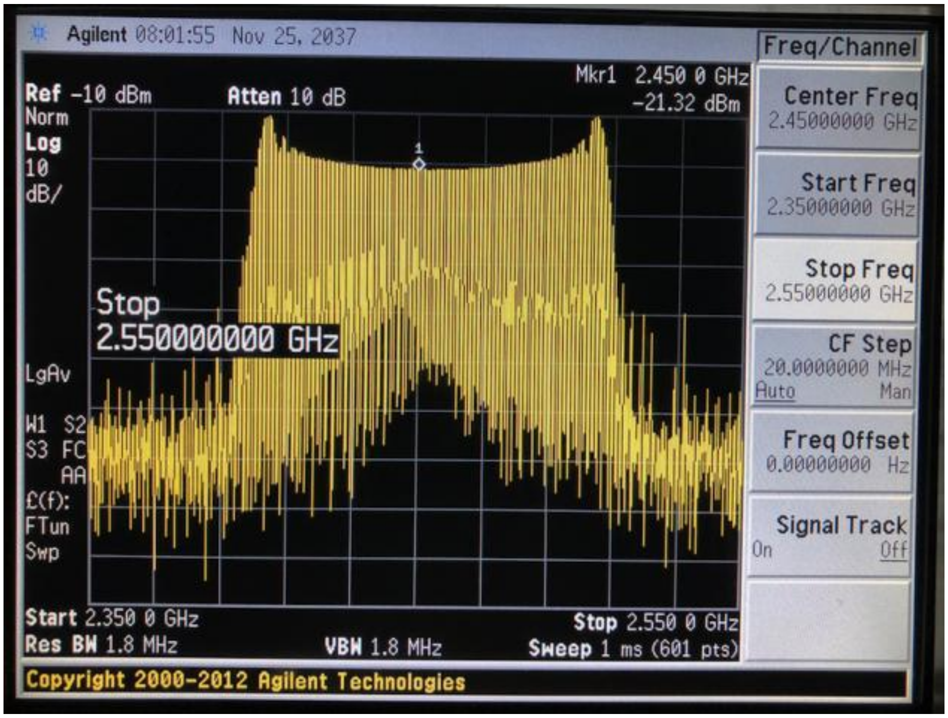
CF Step
20.0000000 MHz
Auto Man

Freq Offset
0.00000000 Hz

Signal Track
On Off

Copyright 2000-2012 Agilent Technologies

Figure 37. Jamming Sweeping Frequency at 1 MHz


Agilent 08:01:55 Nov 25, 2037

Ref -10 dBm Atten 10 dB

Mkr1 2.450 0 GHz
-21.32 dBm

Norm
Log
10
dB/

Stop
2.550000000 GHz

LgAv

W1 S2
S3 FC
AA
£(f):
FTun
Swp

Start 2.350 0 GHz
Stop 2.550 0 GHz

Res BW 1.8 MHz VBW 1.8 MHz Sweep 1 ms (601 pts)

Copyright 2000-2012 Agilent Technologies

Freq/Channel

Center Freq
2.45000000 GHz

Start Freq
2.35000000 GHz

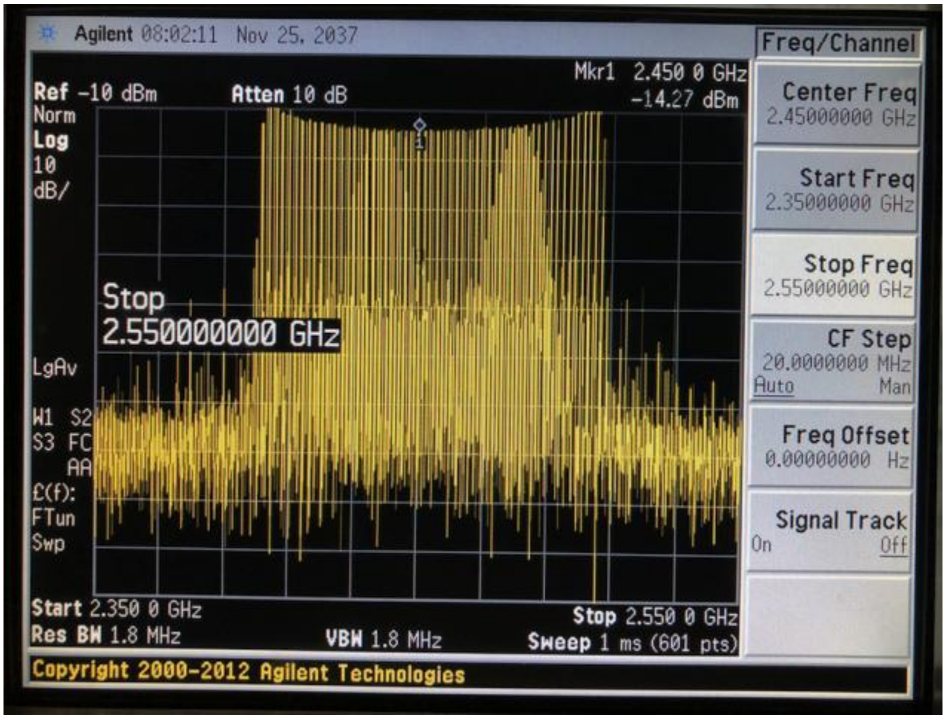
Stop Freq
2.55000000 GHz

CF Step
20.0000000 MHz
Auto Man

Freq Offset
0.00000000 Hz

Signal Track
On Off

Figure 38. Jamming Sweeping Frequency at 500 kHz


Agilent 08:02:11 Nov 25, 2037

Ref -10 dBm Atten 10 dB

Mkr1 2.450 0 GHz
-14.27 dBm

Norm
Log
10
dB/

Stop
2.550000000 GHz

LgAv

W1 S2
S3 FC
AA
£(f):
FTun
Swp

Start 2.350 0 GHz
Stop 2.550 0 GHz

Res BW 1.8 MHz VBW 1.8 MHz Sweep 1 ms (601 pts)

Copyright 2000-2012 Agilent Technologies

Freq/Channel

Center Freq
2.45000000 GHz

Start Freq
2.35000000 GHz

Stop Freq
2.55000000 GHz

CF Step
20.0000000 MHz
Auto Man

Freq Offset
0.00000000 Hz

Signal Track
On Off

Figure 39. Jamming Sweeping Frequency at 100 kHz

The above figures further demonstrate how increasing the jamming sweeping frequency also requires significantly more energy to sufficiently jam the entire ISM band. A jamming sweeping frequency of 1 MHz required approximately twice the energy of a jamming sweeping frequency at 100 kHz.

The Arduino Uno was first studied for use as the microcontroller to control the sinusoidal waveform. The 16 MHz Arduino UNO microcontroller and an operation amplifier design were created to replace the waveform function generator used successfully in previous experimentation. The Arduino UNO output a pulse width modulated (PWM) signal through a high pass filter to create the desired sinusoidal waveform.

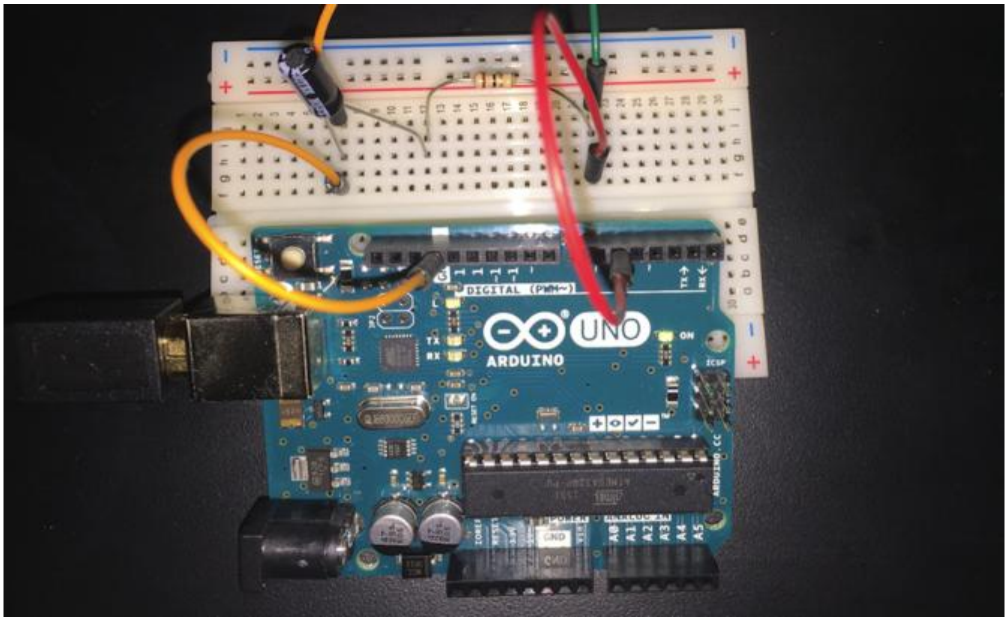


Figure 40. Arduino UNO Hardware Design with High Pass Filter

It was quickly realized, through minor changes to the software code, the sweeping frequency was significantly limited with this particular microcontroller. The fastest frequency the microcontroller could produce was approximately 1.175 kHz. The following screenshots show two different sweeping frequencies:

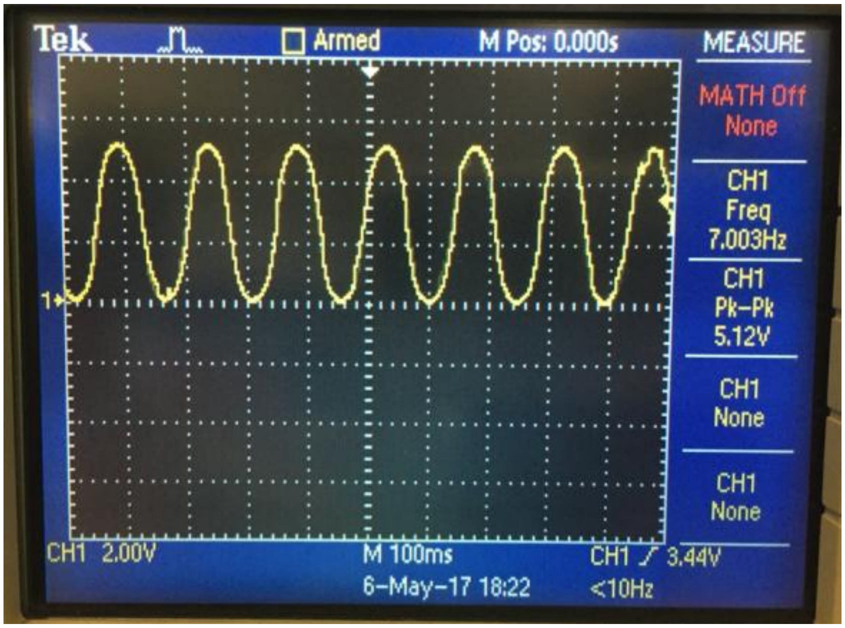


Figure 41. Arduino UNO Sine Wave at 7 Hz

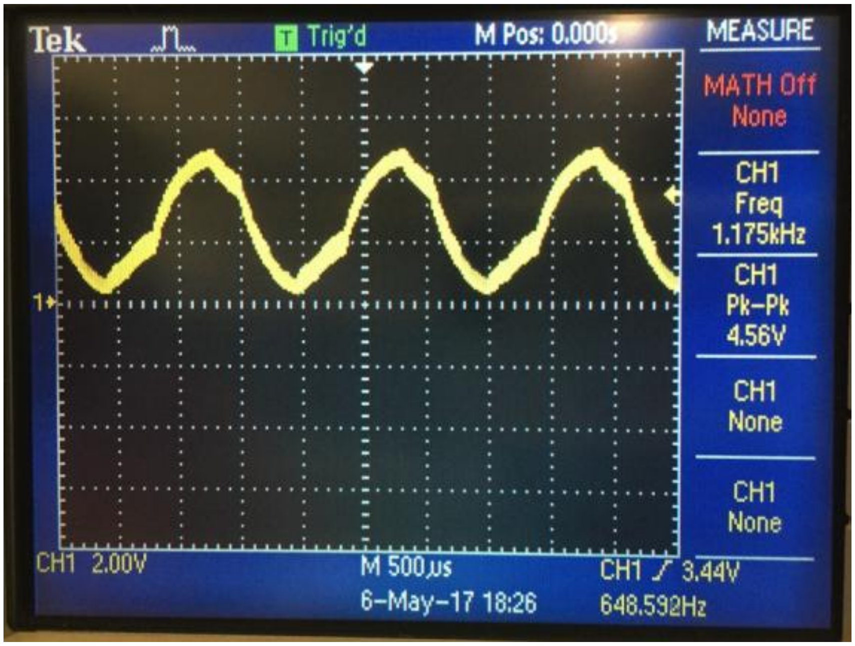


Figure 42. Arduino UNO Sine Wave at 1.175 kHz

An alternative option to the Arduino UNO was the Arduino DUE which has a much faster CPU with an 84 MHz clock. With this microcontroller, there was no need for a high pass filter to produce a sine wave.

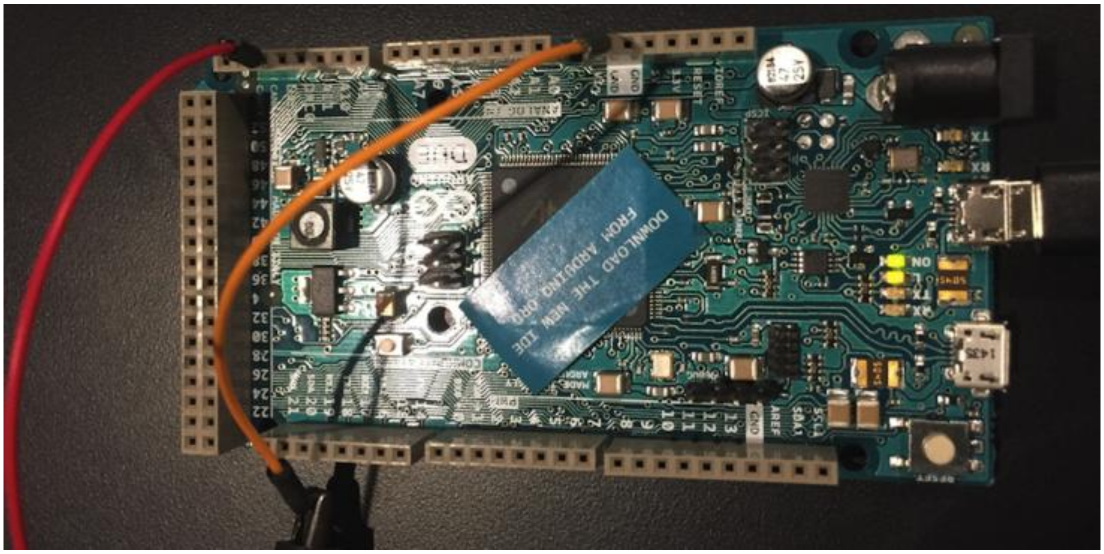


Figure 43. Arduino DUE Hardware Design

This hardware design also faced similar issues, as the sine wave could not be generated at a sufficient frequency. The *analogWriteResolution* function generated a 12-bit waveform and increased the frequency to approximately 32kHz; however, the waveform resolution was very poor, as shown below.

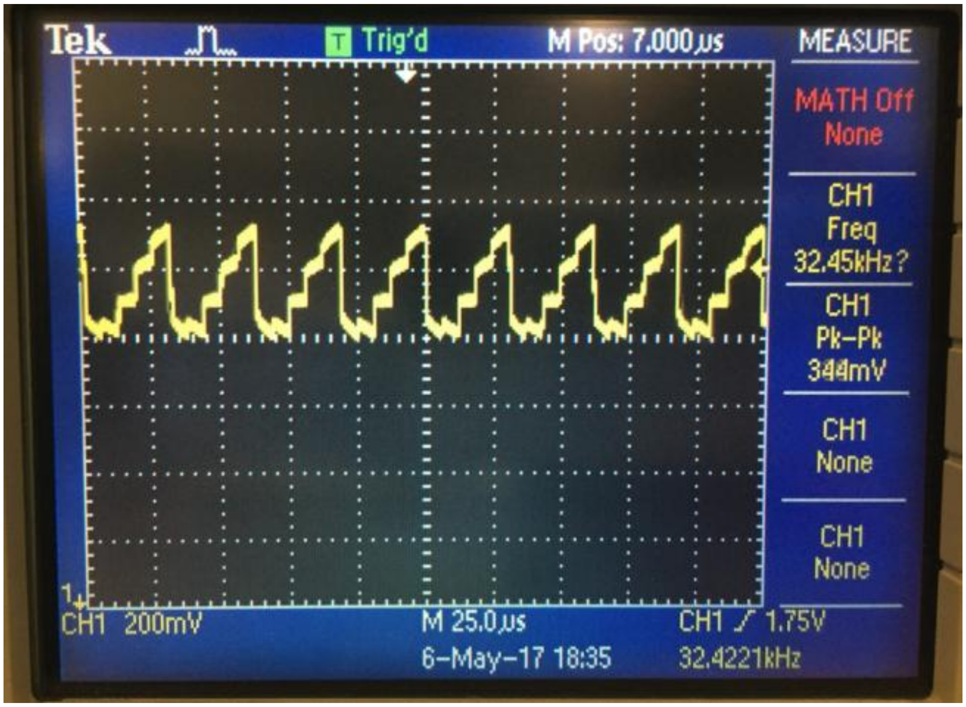


Figure 44. Arduino DUE Sine Wave at 32.45 kHz

After several unsuccessful attempts to use an Arduino microcontroller to generate the sine wave and oscillate it at sufficient frequency, a board from Red Pitaya was selected due to its versatility. This particular platform was considered, as it could potentially replace a waveform function generator, microcontroller, and voltage-controlled oscillator (VCO) all in one design.

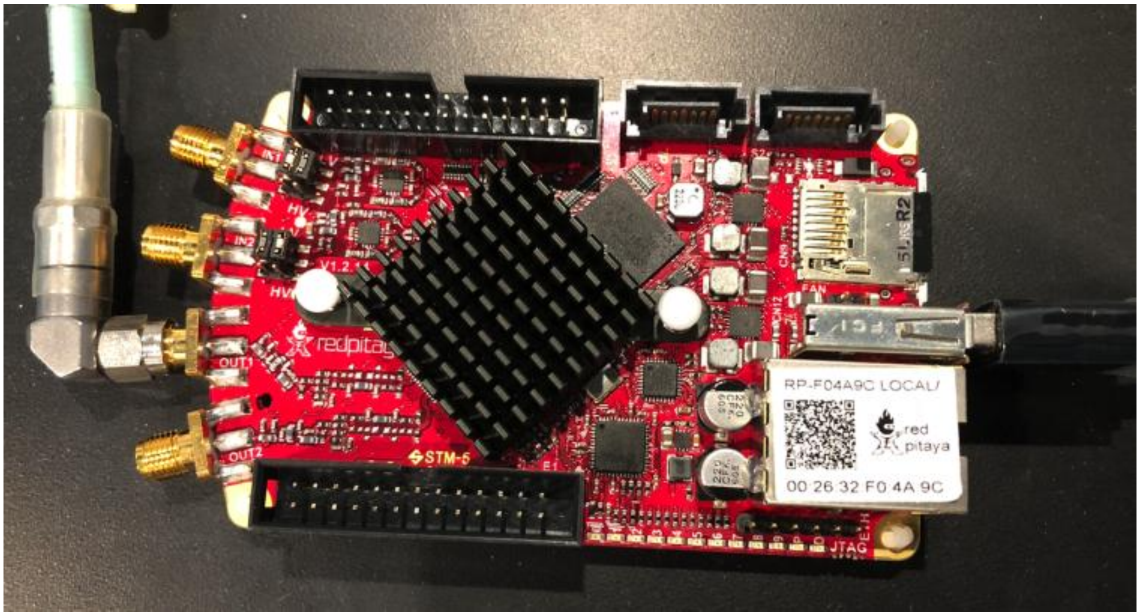
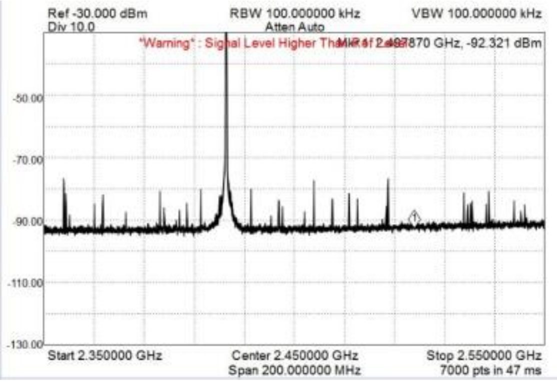


Figure 45. Red Pitaya

However, the Red Pitaya hardware is much more expensive than using an Arduino microcontroller, op amp, and VCO. The Red Pitaya board was very user friendly but suffered problems similar to the Arduino microcontrollers. The following sequential screenshots illustrate the sweeping frequency with a 5 MHz step size through its VCO:



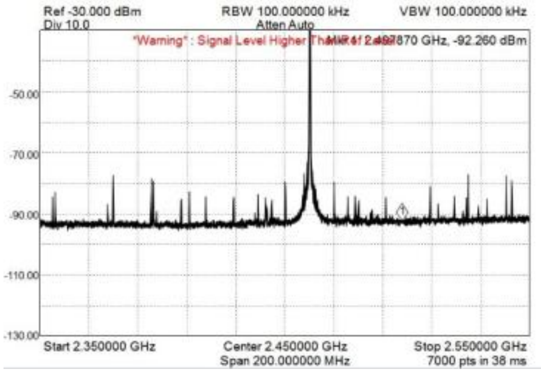


Figure 46. Red Pitaya Step 1

Figure 47. Red Pitaya Step 2

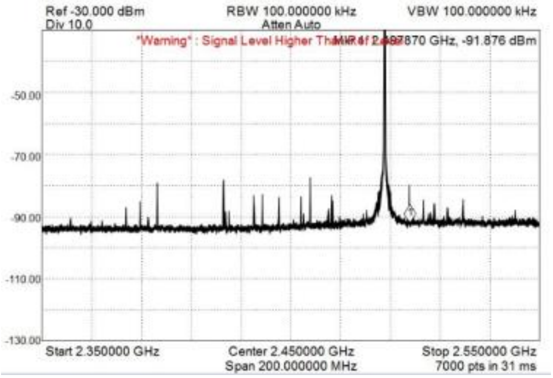


Figure 48. Red Pitaya Step 3

It took several seconds for the hardware to incrementally step through the entire 2.4 GHz to 2.5 GHz frequency range. While this hardware design swept the entire 2.4 GHz band, it did so at such a slow speed that it never effectively jammed the hopping frequency of the drone's communications link. This hardware design performed inferior to the Arduino microcontrollers.

The Arduino UNO microcontroller design was considered again, but with assistance from the AD9850 DDS (direct digital synthesizer). The DDS was added to the microcontroller system to regulate the sweeping frequency. The Arduino UNO was used to output a sine wave signal to the DDS, which then oscillated the waveform to the desired frequency. The sweeping frequency was easily modified through Arduino's open source software code [34].

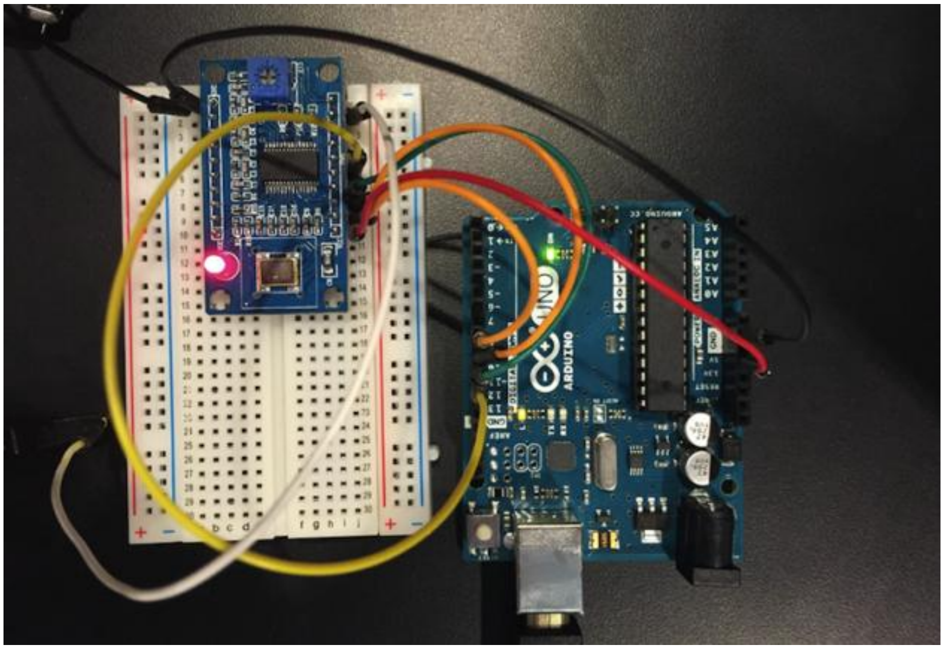


Figure 49. Arduino UNO with AD9850 DDS

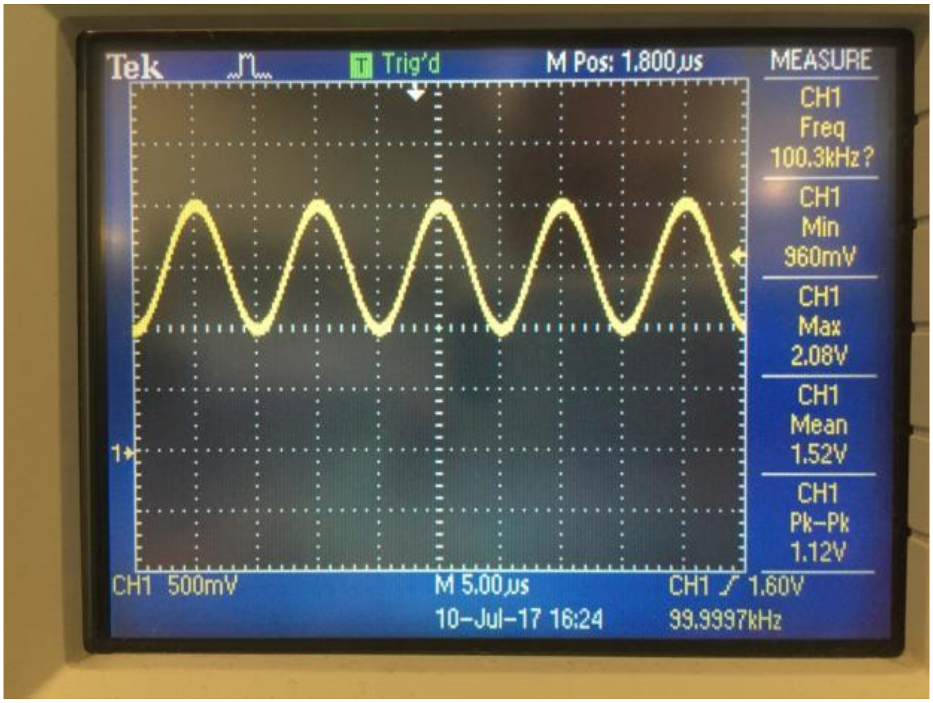


Figure 50. Sine Wave Sweeping at 100 kHz

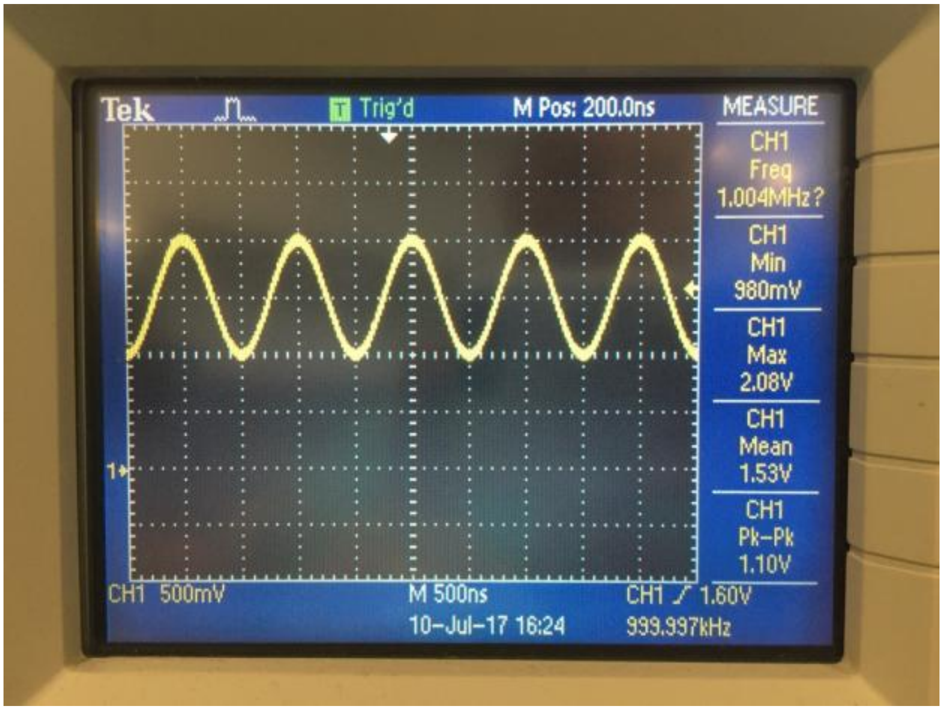


Figure 51. Sine Wave Sweeping at 1 MHz

The output voltage of the jamming sweeping frequency from the Arduino UNO with the AD9850 DDS was not within the specifications for the VCO to effectively jam the ISM band. Again, from the experimental results discussed in Chapter 3.5, the optimal jamming sweeping frequency was approximately 300 kHz. After the optimal sweeping frequency was determined, the resistor values were calculated for the non-inverting operational amplifier. The op-amp was needed to amplify the output waveform from the Arduino UNO as the signal oscillated between 5.5 V and 8.5 V. The amplified waveform was sent to the VCO, which then transmitted the desired jamming frequency via a Yagi antenna.

Chapter 5: DDMR Concept of Operations

5.1 DDMR Low Cost Solution

The DDMR system is an alternative option to other ECMs on the market, and it has the advantage of being a low cost and portable solution to effectively jam sUAS and drones that operate on the 2.4 GHz, ISM carrier frequency. Previous anechoic chamber testing determined the optimal jamming sweeping frequency was within the 100 kHz to 1 MHz frequency range. Theoretical studies helped identify the boundary limits for the POI and hit rates. MATLAB simulations and experimental results yielded the optimal jamming sweeping frequency of 300 kHz, which was critical to the hardware design of the DDMR jamming system.

The hardware for the new DDMR system is contained within the small gray box in Figure 49. The system is powered by a 15 V DC power supply.

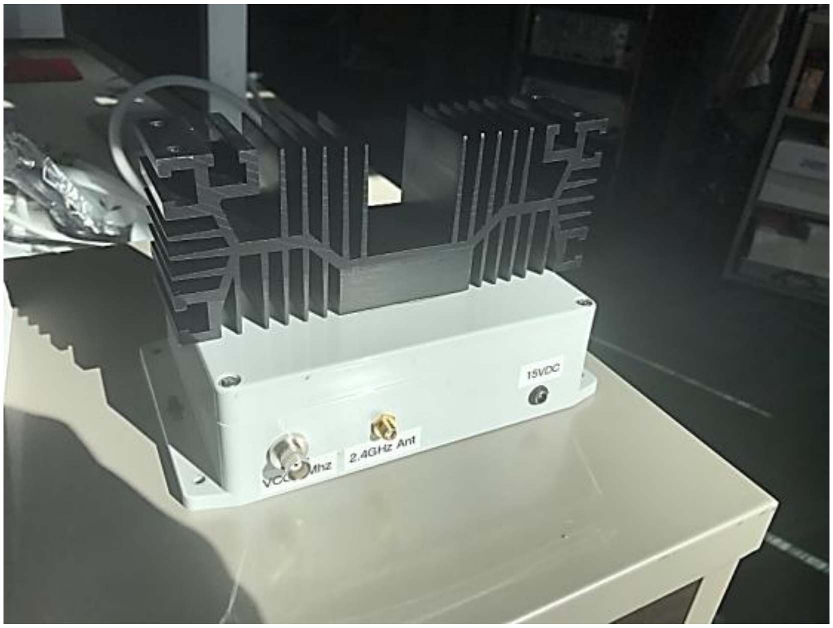


Figure 52. DDMR System

The size, weight, and low cost of the DDMR make it a viable resource for organizations who protect critical infrastructures and venues. The hardware designed for the new DDMR may be further refined to achieve a smaller scale, thus allowing it to be added to existing equipment, such as an assault rifle style platform, for quick and easy deployment. With the addition of an optical (reticle) aiming system, an AR or other similar platform would allow the user to accurately aim the antennae at a sUAS or drone.

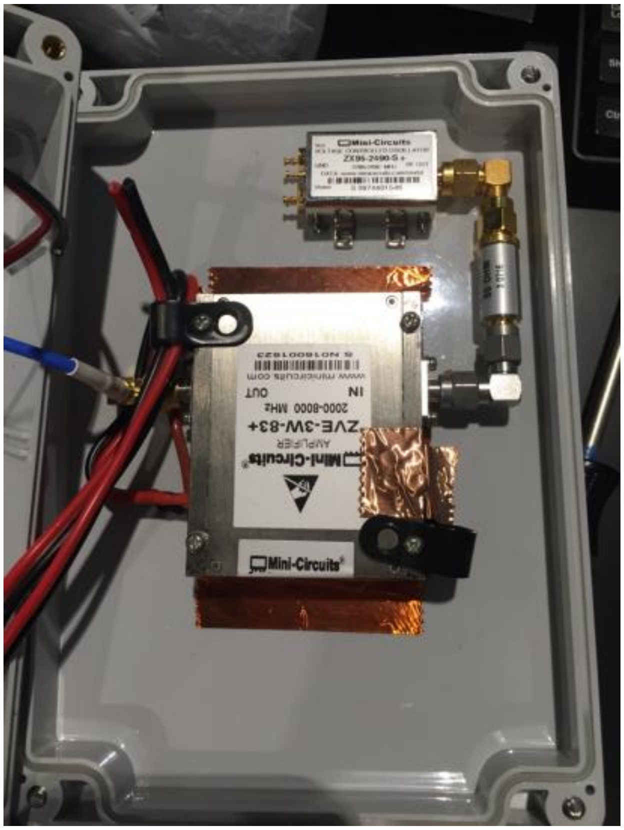


Figure 53. Inside the DDMR

The total cost for all of the parts used in the jamming component of the new DDMR system are less than $150. In comparison, the prototype DDMR system's wave function generator, with no other hardware components considered, far outweighed the cost of this new system. In addition, the prototype DDMR system was not portable due to the wave function generator’s size and power requirements. The original parabolic reflective antenna was also very large and bulky when compared to the new Yagi antenna design.

5.2 Summary and Future Work

One important limitation of this research is the new DDMR system was unable to be evaluated in an outdoor, real-world environment. This was primarily due to the federal laws which prohibit active jamming within the United States, as stated in Chapter 1.2. Since the jammer had the possibility to potentially interfere with other nearby communications signals operating on the 2.4 GHz carrier band, approval from the FCC would have been required. It would have taken a significant amount of time for the FCC to review and approve a proposal. As such, it was not possible to complete experimental hardware testing within the timeframe of this thesis, but the testing should be completed in the future. Obtaining FCC approval would be particularly helpful, as it would further demonstrate the effectiveness of the DDMR system in a real-world environment.

The new DDMR system was designed only to jam the communications link on the ISM band. Future research could be expanded to other common carrier bands, such as the 4.8 GHz band, since drone enthusiasts often modify their drones to operate at other carrier frequencies. As GPS has become commonplace, it must be expected drone users will begin to utilize this technology as well. In particular, as the other designated frequency bands become more crowded with emerging electronic devices (smart cars, smart homes, etc.), drone enthusiasts may opt to operate on less crowded carrier bands.

References

[1] J. Dunn (2017). Available: http://www.businessinsider.com/drone-sales-in-us-chart-2017-5

[2] Legal Information Institute, Cornell Law School. Sovereignty and use of airspace. Available: https://www.law.cornell.edu/uscode/text/49/40103

[3] Legal Information Institute, Cornell Law School. General Definitions. Available: https://www.law.cornell.edu/cfr/text/14/1.1

[4] Federal Register, Interpretation of the Special Rule for Model Aircraft. Available: https://www.federalregister.gov/documents/2014/06/25/2014-14948/interpretation-of-the-special-rule-for-model-aircraft

[5] Federal Communications Commission. Jammer Enforcement. Available: https://www.fcc.gov/general/jammer-enforcement

[6] Federal Aviation Administration. UAS Sightings Report. Available: https://www.faa.gov/uas/resources/uas_sightings_report/

[7] Y. (Rockee) Zhang, Y.R. Huang and C. Thumann, "Noise and LPI radar as part of counter-drone mitigation system measures", in Proceedings of SPIE Defense and Security 2017 Conference-Radar Sensor Technology XX (DS112), Anaheim CA, April 8-13, 2017.

[8] R. Poisel, *Modern Communications Jamming Principles and Techniques*, 2nd Edition, Norwood: Artech House, 2011.

[9] W. Shen, P. Ning, X. He, and H. Dai, "Ally Friendly Jamming: How to Jam Your Enemy and Maintain Your Own Wireless Connectivity at the Same Time", *2013 IEEE Symposium*, May 2013.

[10] Northeastern University College of Computer Information Science. Spread Spectrum Lecture. Available: http://www.ccs.neu.edu/home/rraj/Courses/6710/S10/Lectures/SpreadSpectrum.pdf

[11] H. Shin, K. Choi, Y. Park, and J. Choi, "Security Analysis of FHSS-type Drone Controller", *Information Security Applications, 16th International Workshop, WISA 2015*, pp.240-253.

[12] Z. Kong, P. Li, X. Yan, and X. Hao, "Anti-Sweep Jamming Design and Implementation Using Multi-Channel Harmonic Timing Sequence Detection for Short-Range FMCW Proximity Sensors", *Sensors*, September 2017.

[13] R. Cerda (2014). Summary of wireless formats. Available: https://www.ecnmag.com/article/2014/10/its-wireless-world

[14] J. Meel, "Spread Spectrum (SS)", *nov. 1997 – nov. 1999 a 'Spread Spectrum' project was worked out at the polytechnic 'DE NAYER instituut'*.

[15] Cisco. WLAN Radio Frequency Design Considerations. Available: https://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob30dg/RFDesign.html

[16] Wikipedia. Direct-sequence spread spectrum. Available: https://en.wikipedia.org/wiki/Direct-sequence_spread_spectrum

[17] F. Fund (2017). Frequency hopping spread spectrum. Available: https://witestlab.poly.edu/blog/frequency-hopping-spread-spectrum/

[18] Federal Communications Commission. Operation within the bands, 2400-2483.5 MHz. Available: https://www.gpo.gov/fdsys/pkg/CFR-2013-title47-vol1/pdf/CFR-2013-title47-vol1-sec15-247.pdf

[19] R. G. Wiley, *ELINT: The Interception and Analysis of Radar Signals*, Wiley, 2006.

[20] H. Saarnisaari, "Sweep jamming hit rate analysis for frequency agile communications," *2016 International Conference on Military Communications and Information Systems (ICMCIS)*, Brussels, 2016, pp. 1-6. doi: 10.1109/ICMCIS.2016.7496578

[21] A.G. Self and B.G. Smith, "Intercept time and its prediction", *IEE Proceedings*, Vol. 132, Pt f, No. 4, July 1985, pp. 215-222.

[22] B.R. Hatcher, "Intercept Probability and Intercept Time", *Electronic Warfare*, pp. 95-103, March/April 1976.

[23] C. Thumann, Y. (Rockee) Zhang, Y.R. Huang and, J. Dyer, "Analysis of Transmission and Polarization Optimization of Counter-Small UAS (C-SUAS) Radar and Noise Jamming", in Proceedings of SPIE Defense and Commercial Sensing 2018 Conference, Orlando, FL, April 17-19, 2018.

[24] H.R. Cho, Y.S. Oh, and C.E. Kang, "BIT ERROR RATE IN FH/BFSK SYSTEM UNDER JAMMING ENVIRONMENTS", *1992 IEEE*, pp. 465-469.

[25] N. Harter, J. J. Keaveny, S. Venkatesh and R. M. Buehrer, "Analysis and implementation of a novel single- channel direction-finding method," *IEEE Wireless Communications and Networking Conference, 2005*, 2005, pp. 2530-2533 Vol. 4.doi: 10.1109/WCNC.2005.1424912

[26] M. Ritchie, F. Fioranelli, H. Griffiths and B. Torvik, "Monostatic and bistatic radar measurements of birds and micro-drone," In *Proceedings of 2016 IEEE Radar Conference (RadarConf)*, Philadelphia, PA, 2016, pp. 1-5. doi: 10.1109/RADAR.2016.7485181.

[27] R. Poisel, *Introduction to Communications Modern Warfare Systems*, Boston: Artech House, 2002.

[28] DroneShield. Manufacturer of drone jammer gun. Available: https://www.droneshield.com/dronegun/

[29] Wikipedia. Parabolic antenna. Available: https://en.wikipedia.org/wiki/Parabolic_antenna

[30] Wikipedia. Dipole antenna. Available: https://en.wikipedia.org/wiki/Dipole_antenna

[31] M. K. Simon, J. K. Omura, R. A. Schultz, and B. K. Levitt, *Spread Spec- trum Communications Handbook*, electronic ed. New York: McGraw- Hill, Inc., 2002.

[32] Tupavco. Manufacturer of antennas. Available: https://www.tupavco.com/yagi-wifi-antenna-24ghz-17dbi-angle-20-outdoor-directional-wireless-n-female

[33] Datasheet for voltage-controlled oscillator. Available: https://www.minicircuits.com/pdfs/ZX95-2490+.pdf

[34] Arduino open-source code and pin layout for DDS9850. 2014. Available: https://www.riyas.org/2014/02/quickly-test-ad9850-ebay-module-with-arduino-and-software-defined-radio.html

[35] Avionics Department, Naval Air Warfare Center Weapons Division, *Electronic Warfare Radar Systems Engineering Handbook*, Fourth Edition, October 2013.

[36] J.H. Lee, B.S. Yu, and S.C. Lee, “Probability of error for a hybrid DS/SFH spread-spectrum system under tone jamming”, In *Military Communications Conference, 1990. MILCOM’90, Conference Record, A New Era. 1990 IEEE*, pages 410–414. IEEE, 1990.

Appendix A: Open Source Arduino Code

Arduino UNO code:

```
int value=0;
int i=0;

void setup()
{
  analogWriteResolution(12);  //12 bit very poor resolution; 8 bit better resolution
}

void loop()
{
analogWrite(DAC1, value);

i = i+1;
value = i*10;      //i*10; freq control *1=680Hz; *10=6kHz; *20=12kHz;
if(value>4096)   // 12 bit 4096 very poor resolution at 32kHz; and 8 bit 256 only 3kHz
{
  //i=0;
  //value=0;
}
}
```

Arduino UNO DUE code:

```
int value=0;
int i=0;

void setup()
{
  analogWriteResolution(12);  //12 bit very poor resolution; 8 bit better resolution
}

void loop()
{
analogWrite(DAC1, value);

i = i+1;
value = i*10; //i*10; freq control *1=680Hz; *10=6kHz; *20=12kHz;
if(value>4096)  // 12 bit 4096 very poor resolution at 32kHz; and 8 bit 256 only 3kHz
{
  //i=0;
  //value=0;
}
}
```

Arduino UNO code with AD9850 [20]

```
/*
 * A simple single freq AD9850 Arduino test script
 * Original AD9851 DDS sketch by Andrew Smallbone at www.rocketnumbernine.com
 * Modified for testing the inexpensive AD9850 ebay DDS modules
 * Pictures and pinouts at nr8o.dhlpilotcentral.com
 * 9850 datasheet at http://www.analog.com/static/imported-
files/data_sheets/AD9850.pdf
 * Use freely
 */

#define W_CLK 8       // Pin 8 - connect to AD9850 module word load clock pin (CLK)
#define FQ_UD 9       // Pin 9 - connect to freq update pin (FQ)
#define DATA 10       // Pin 10 - connect to serial data load pin (DATA)
#define RESET 11      // Pin 11 - connect to reset pin (RST).

#define pulseHigh(pin) {digitalWrite(pin, HIGH); digitalWrite(pin, LOW); }

 // transfers a byte, a bit at a time, LSB first to the 9850 via serial DATA line
void tfr_byte(byte data)
{
  for (int i=0; i<8; i++, data>>=1) {
    digitalWrite(DATA, data & 0x01);
    pulseHigh(W_CLK);   //after each bit sent, CLK is pulsed high
  }
}

 // frequency calc from datasheet page 8 = <sys clock> * <frequency tuning word>/2^32
void sendFrequency(double frequency) {
  int32_t freq = frequency * (4294967295)/125000000;  // note 125 MHz clock on 9850
//.24 to send 1MHz output freq(old chip)

  for (int b=0; b<4; b++, freq>>=8) {
    tfr_byte(freq & 0xFF);
  }
  tfr_byte(0x000);   // Final control byte, all 0 for 9850 chip
  pulseHigh(FQ_UD);  // Done!  Should see output
}

void setup() {
 // configure arduino data pins for output
  pinMode(FQ_UD, OUTPUT);
  pinMode(W_CLK, OUTPUT);
  pinMode(DATA, OUTPUT);
  pinMode(RESET, OUTPUT);
  pulseHigh(RESET);
  pulseHigh(W_CLK);
  pulseHigh(FQ_UD);  // this pulse enables serial mode - Datasheet page 12 figure 10
}

void loop() {
  sendFrequency(1000000);  //control output freq
  delay (1000);
  //sendFrequency(10.01e6);  // freq
  //delay(1000);
}
```

Appendix B: MATLAB Simulation Code

```
%VCO 5.5V = ~2.4GHz and 8.5V = ~2.5GHz
%For sine wave sweeping frequency:
%sin(0:(pi/5):2*pi)*(0.1/2)+2.45  2.45 is center frequency and 0.1 is amplitude

clear
close all
%Sample size at 1MHz or 1 uSec for jamming frequency
SS = 100;

%Dwell time of 100 milli-seconds
%uSec -> each step is 10 uSec => 1 millisecond times one thousand uSec times SS
DT = 100 * 1000 * SS;  %DT is 100ms

%random integers for 8 channels in first array and random frequency for 8
%frequencies between 2.4GHz to 2.5GHz in second array
DFT = sortrows([randperm(8)' (2.400: 0.090/7: 2.490)']);
%plot(DFT(:,2), ':')
%Sweeping frequency 0.1=>100Khz 1=>1MHz
%If increase sweeping frequency need to increase the below sample rate
SFreq = 0.100: 0.100: 1.000;

%1,000,000 samples in 1 micro-second length
for j = 1:length(SFreq)
   for i = 1:(SS*1e6*2.5)
%Phantom frequency and creating a Phantom frequency table
%Repeats the hopping frequency table 1,000,000 samples divided by 8 (array
%size)
%mod(i/DT,8)+1 bc the array cannot equal zero --> making array table 1 thru
%8
   DFreq(i) = DFT(floor(mod(i/DT,8)+1),2);
%Jamming frequency
   JFreq(i) = sin((i*(2*pi))/SS*SFreq(j))*(.100/2)+2.450;
   end
   %Abs value between Phantom frequency and Jamming frequency for less
   %than 3 MHz bandwidth increments
   %Hit rate is calculated by taking the absolute value between
   %both arrays for less than 3 MHz (FHSS bandwidth is 1 MHz)
   %Length will give a final count of positive hits
   X = find(abs(JFreq-DFreq) < 0.003);
   %Counter
   x = 1;
   l = 0;
   %Create large array X and count each incremental (small x) within array
   %If length exceeds array X increase count and move to next array X and
```

```
    %continue counting hits
    for k = 1:length(X)
        if X(k)-x > SS
            x = X(k);
            l = l+1;
        end
    end
    %Jamming rate is total counted hits above and divided by the length of
    %Phantom frequency divided by the sample size
    JR(j) = l/(length(DFreq)*8/SS);
end

figure(1)
hold on;
plot(JFreq(1:250000000),'b');
plot(DFreq(1:250000000),'r.');
hold off;
ylabel('Frequency (MHz)')
xlabel('Time 1/100 uSec')
axis([0,250000000,2.4,2.5])
grid on;
title('Drone Channels','FontSize',14,'FontWeight','bold')

figure(2)
plot(JR*100,'LineWidth',1)
ylabel('Hit Rate %','FontSize',14,'FontWeight','bold')
xlabel('Sweeping Frequency (kHz)','FontSize',14,'FontWeight','bold')
set(gca,'XTickLabel',[100: 100: 1000])
axis([-inf,inf,0,20])
grid on;
title('Hit Rate Simulation','FontSize',14,'FontWeight','bold')
```

Appendix C: MATLAB Experiment Code

```
close all
clear

RC = textread('RC Freq3/RC Freq025.txt');
x = RC(:,1);
VCO = textread('VCO/1 MHz Jamming.txt');
y = VCO(:,1);

%Plot input signals
figure(1)
plot(x);
ylabel('Amplitude')
xlabel('Time')
title('Transmitter Input Signal','FontSize',14,'FontWeight','bold')
figure(2)
plot(y);
ylabel('Amplitude')
xlabel('Time')
title('Jammer Input Signal','FontSize',14,'FontWeight','bold')

%FFT
nfft = 131072;  %2^17 less than D=200k
RCfft = fftshift(fft(x,nfft));
VCOfft = fftshift(fft(y,nfft));
fs = 20e9; %sampling frequency 20GSa/s from scope with 10us sample period
n = fs*(-nfft/2:nfft/2-1)/nfft;  %DFT sample points
figure(3)
hold on
plot(n,abs(RCfft)); %double sided fft
plot(n,abs(VCOfft));
hold off
ylabel('Magnitude')
xlabel('Frequency')
grid on
axis([2.3e9,2.6e9,-inf,inf,])
title('RC Transmitter Versus VCO FFT','FontSize',16,'FontWeight','bold')

%PSD
X = fft(x,nfft);
X = X(1:nfft/2+1);
Px = X.*conj(X)/(nfft*nfft); %complex and real numbers
Y = fft(y,nfft);
Y = Y(1:nfft/2+1);
Py = Y.*conj(Y)/(nfft*nfft);
```

```
f = fs*(0:nfft/2)/nfft;
figure(4)
hold on
plot(f,10*log10(Px));
plot(f,10*log10(Py));
hold off
ylabel('Power/Frequency (dB/Hz)')
xlabel('Frequency')
grid on
axis([2.3e9,2.6e9,-inf,inf,])
title('RC Transmitter Versus VCO Power Spectral
Density','FontSize',16,'FontWeight','bold') %Single sided distribution

%Spectrogram
figure(5)
hold on
[s1,f1,t1,p1] = spectrogram(x,5000,4800,4000,fs);
surf(t1,f1,10*log10(abs(p1)),'EdgeColor','b');
[s2,f2,t2,p2] = spectrogram(y,5000,4800,4000,fs);
surf(t2,f2,10*log10(abs(p2)),'EdgeColor','none');
axis xy;
axis tight;
colormap(jet);
view(0,90);
rotate3d on;
hold off
ylabel('Frequency (GHz)')
xlabel('Time (us)')
zlabel('Power/Frequency (dB/Hz)')
grid on
axis([0,inf,2.2e9,2.7e9])
title('RC Drone Transmitter Versus VCO 1 MHz Sweeping
Frequency','FontSize',16,'FontWeight','bold')

%Hit Rate
[q_RC,nd_RC] = max(10*log10(p1));
[q_VCO,nd_VCO] = max(10*log10(p2));
figure(6)
hold on
plot(t1,f1(nd_RC),'b');
plot(t2,f2(nd_VCO),'r');
plot(t2,f2(nd_VCO)+3e6,'g');
plot(t2,f2(nd_VCO)-3e6,'g');
rotate3d on;
hold off
ylabel('Frequency (GHz)')
```

```
xlabel('Time (us)')
axis([0,inf,2.3e9,2.6e9])
grid on
title('Spectrogram 1 MHz Sweeping Frequency','FontSize',16,'FontWeight','bold')
J = length(find(abs((f(nd_VCO)-(f(nd_RC)))) <= 3e5));
HR = (J/length(f(nd_RC)))

%Peak RC frequency
[A,B] = max(10*log10(Px));
RC_Freq_Peak = f(1,B)
```