CALIFORNIA POLYTECHNIC STATE UNIVERSITY

Spread Spectrum Jamming

Part 2

Casey Burke, Christian Hume, Javier Meza

6/12/2013

Table of Contents

Acknowledgements

We would first like to acknowledge John Jacobs Ph.D. from Raytheon Space and Airborne Systems for providing the most guidance with this senior project as well as keeping us on track over three quarters of developing and working on this project. Furthermore, we would also like to thank our professors over the years for instilling us with extensive electrical engineering knowledge and, particularly for this project, the understanding of communication systems. And, of course, special thanks goes out to the individuals who comprised last year's spread spectrum jamming team, whose work provided the foundation for this project and allowed us to continue our exploration into the field of communication system jamming.

Abstract

Direct-sequence spread spectrum (DSSS) is a special modulation technique used in many telecommunication devices which uses a wide bandwidth relative to single-frequency carrier modulation techniques. Like the name suggests, the spectral content of wireless signals are spread across a range of frequencies to increase the security of transmitted signals by reducing the potential impact of outside interference (i.e. noise, jamming). This resistance against outside interference and jamming has particular application in the field of electronic warfare where spread spectrum jamming techniques may prove to be an effective way of shutting down remotely controlled enemy vehicles.

Last year, a group of students at Cal Poly attempted to jam a remotely controlled car that utilized a DSSS communications system. While they were successful in implementing a jammer that blocked the input signals to the RC car, they were constrained by the jammer's limited range of less than 1 inch between the jammer and the car and they were uncertain of the specific effect the jammer caused on the receiver electronics. This project calls for further investigation into the

spread spectrum jammer’s effects on the RC car, in addition to making improvements to the jammer to increase the effective jamming range.

List of Tables and Figures

Tables

Figures

Introduction

Recently, wireless technology has begun to utilize spread spectrum techniques in order to mitigate signal interference for security and reliability purposes. Remotely controlled vehicles, such as cars and airplanes, can utilize such techniques. The possibility of remote controlled vehicles that are resistant to jamming is of particular interest to national security. Remotely controlled airplanes could be used to launch weapons at a nation's civilian populations or its strategic holdings. The increased technological sophistication of wireless communication demands equally sophisticated countermeasures to ensure that potentially dangerous enemy vehicles can be checked and stopped.

Direct-sequence spread spectrum is a modulation technique by which an information signal may span the entire spectrum of a transmitted signal. The transmitted signal, therefore, has higher bandwidth which contains the information signal. The DSSS process modulates a sine wave using a pseudo-random chip sequence. Each information bit is modulated by chips which operate at a higher rate than the signal bit rate, ensuring that each bit is modulated by multiple chips. The transmitter sends out the modulated signal multiplied by the pseudo-random noise signal, then the receiver uses the same chip sequence to reconstruct the information signal. DSSS is just one method of producing anti-jam signals. Another popular spread spectrum method is frequency-hopping spread spectrum (FHSS) by which the carrier signal frequency is switched using a pseudo-random sequence, and the bits of the information signal are scattered on the different frequency carrier signals. Both forms of spread spectrum transmission contain major advantages over fixed-frequency transmission. One of the major advantages is the improvement of the security of the information signal, making it more difficult to intercept. This concept is invaluable to the military because they can use this method of spread spectrum transmission to prevent the enemy from jamming and either intercepting or interrupting their transmitted signals. A diagram showing a visual representation of how DSSS communication systems work is shown in figure 1 below.

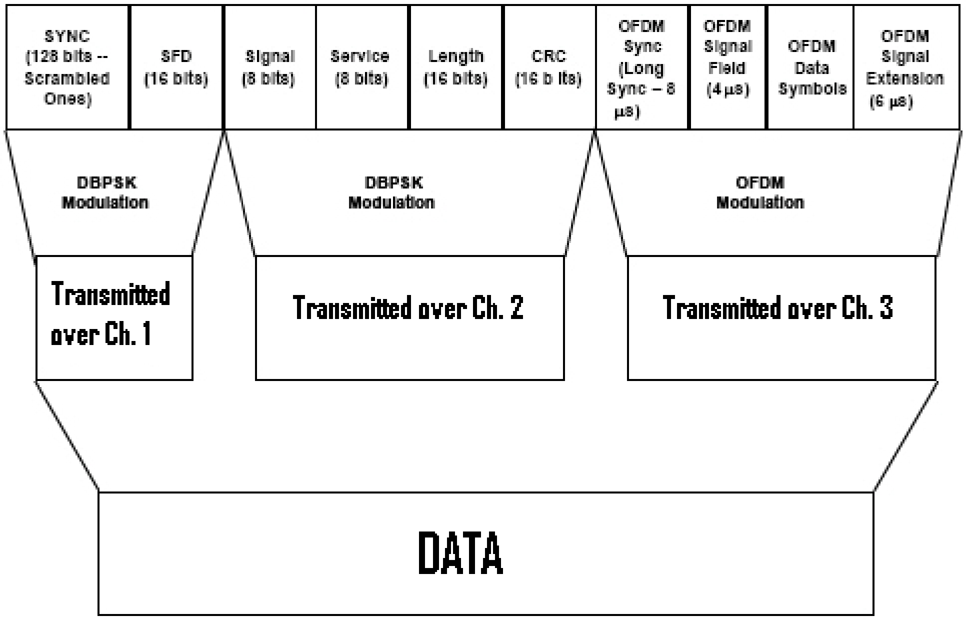
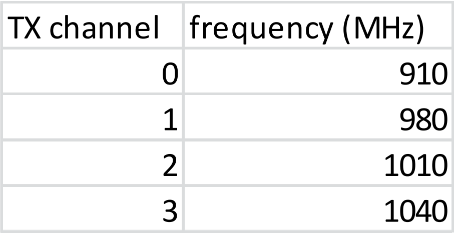


Figure 1: Visual Diagram of how DSSS communication systems work

In DSSS systems, information is broken up into "frames". As shown in the figure 1 above, the frame becomes divided into 3 blocks which represent the preamble, header, and data. These blocks of information are then modulated using different digital modulation schemes over specified sections of the spread spectrum band (i.e. channels 1-3). These blocks are sent to the input of the receiver system where they become demodulated and reassembled back into the original frame of data. By having the data broken up into subdivisions and transmitting using multiple modulation schemes, there is protection against unwanted third parties interfering with the data link.

Furthermore, the reverse is also true: having a better understanding of spread spectrum transmission and jamming techniques could enable the military to jam enemy vehicles. The other existing solution to stopping attacks is shooting down remotely controlled enemy vehicles. While this may be a feasible option on the battlefield, this may prove unfeasible in civilian populations. For example, if the enemy deploys a UAV filled with a biological weapon into a populated area of the country, shooting down the vehicle would still cause major damage. Jamming the signal and shutting down the device would be the ideal option to prevent any major damage from occurring.

The source of the jamming in this project is a camera transmitter which is capable of blocking incoming signals to a Traxxas RC car's 2.4 GHz radio which utilizes a spread spectrum communication system. However, the jamming capability of the camera transmitter is limited in some regards. For example, the camera transmitter has four separate channels shown in table 1.



TX channel	frequency (MHz)
0	910
1	980
2	1010
3	1040

Table 1: Camera transmitter channel listing with corresponding frequency allocations

Channel 0 never jammed the car, channels 2 and 3 jammed the car intermittently, and channel 1 consistently jammed the car. Also, as mentioned before, the operating range of the jammer requires that it is used within 1 inch of the car antenna. Despite these difficulties, the camera transmitter still managed to prevent the car from being controlled reliably while it was simultaneously transmitting a video feed. The previous group was unable to understand the specific impact of the jammer on the car. This project calls for an in-depth investigation into the effects of the jammer in addition to improving the jammer's performance. Figures 2 and 3 below show both test configurations that were used for this project.

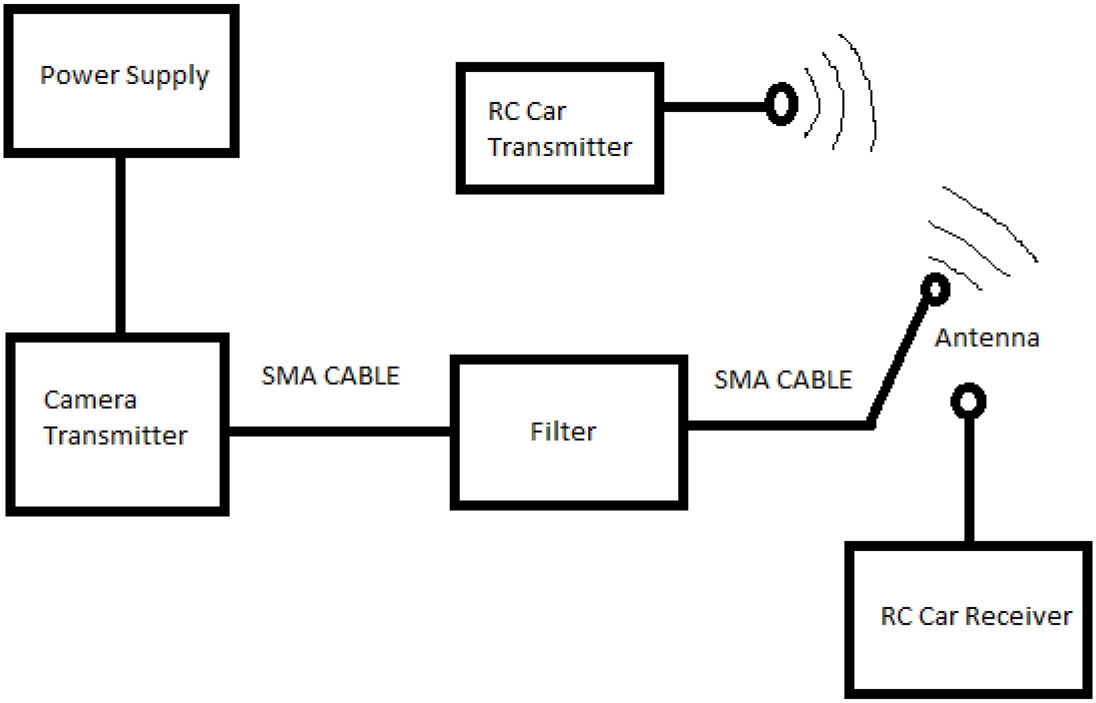


Figure 2: Test Configuration using Camera Transmitter to jam the car

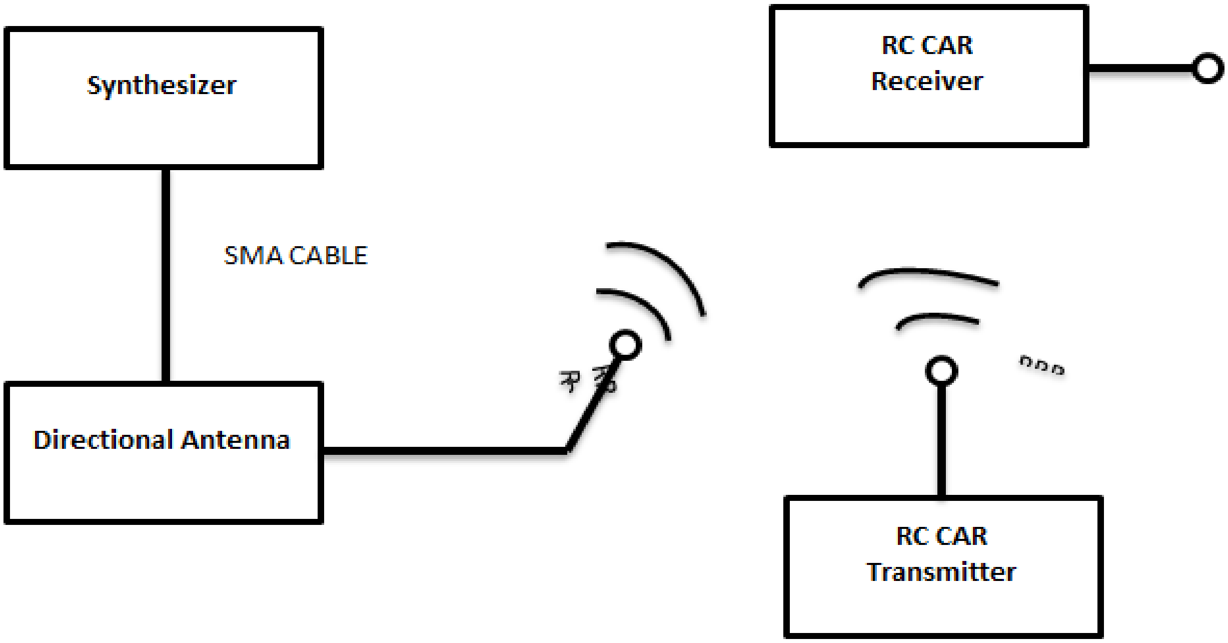


Figure 3: Test Configuration using the frequency synthesizer and directional antenna to jam the car

To investigating the effects on the jammer, measurement devices are required to probe into the car's electrical hardware. These devices include oscilloscopes, network analyzers, and spectrum analyzers which can be found in the various engineering labs on campus. A directional antenna was purchased to help isolate the effects of the jammer on the car by boosting the transmitted signal power. A reference to the antenna datasheet is included in the Bibliography/References section of this report.

By comparing the results of incoming signals under the influence of the spread spectrum jammer, we can isolate what specifically is being affected in the RC car. This will allow us to come up with a plan to optimize that jamming aspect and increase the effectiveness of the jammer.

Before attempting to jam the receiver system of the RC car, it is important to understand how the system operates. The following diagram in figure 4 shows the logic block diagram of the RC car's receiver followed by a description of its main components. The Integrated Circuit is the Cyprus CYRF6936 2.4GHz Radio System on Chip.

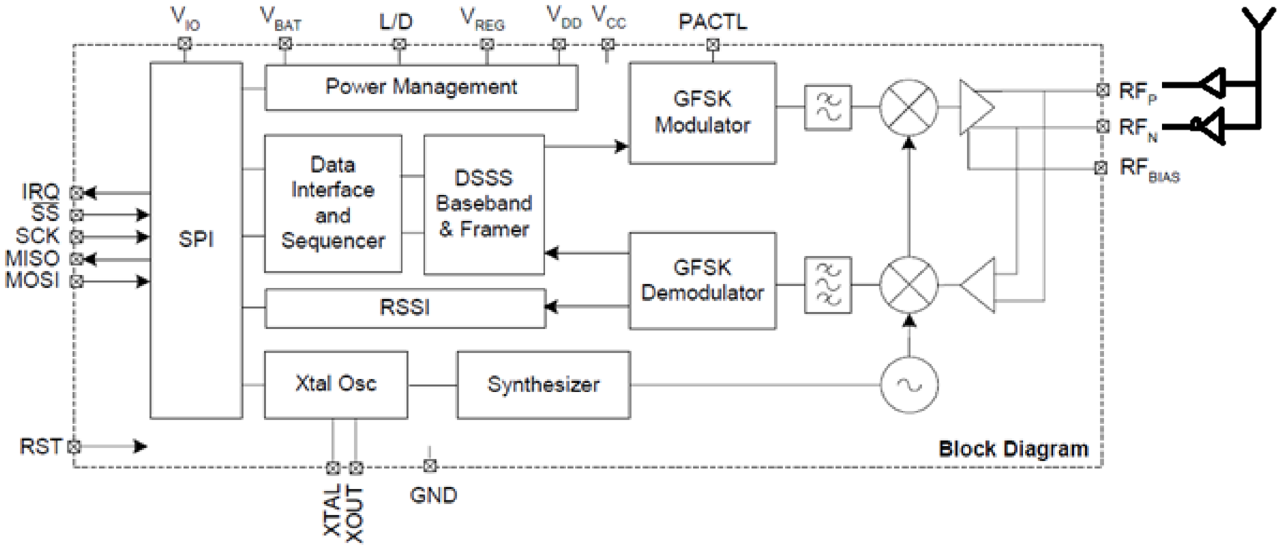


Figure 4: Receiver system of the RC car showing internal subsystems within the CYRF6936 Integrated Circuit

The receiver antenna is connected to the differential RF_P and RF_N inputs. The received signal from the antenna is sent through the RF_P input, while the same signal is inverted and sent to the RF_N input. A differential input is used to eliminate any added noise to the system by adding the normal and inverted signals together. Both signals accumulate the same noise, which is then effectively removed when they are added together.

Breakdown of the individual receiver subsystems:

Amplification

An amplifier is used to boost the power of incoming signals from transmitter sources. This is often necessary due to power losses over free space during the transmission. However, one can see an output amplifier which is used to compensate for the power losses during the signal propagation through the transceiver system.

Mixer + Synthesizer

The synthesizer in conjunction with the mixer is used for frequency shifting. On the receive side, the signal frequency (2.4 GHz) is mixed with a local oscillator frequency (from the synthesizer) to downshift to an intermediate frequency (IF), often in the MHz or kHz range. This is mirrored on the transmit side, where the output data is shifted from the IF frequency and back up to a transmit frequency (most likely 2.4 GHz though it depends on the transmitter).

There are multiple advantages of converting frequencies down to IF. For instance, if several stages of filters are present, they can all be designed around the IF which makes them easier to build and tune. Furthermore, transistors and amplifiers often have higher gains at lower frequencies which serve as an advantage to using IF.

Filtering

Filtering is a key component of telecommunication systems. Filters are typically found to be either lowpass or bandpass filters which allow the desired signal frequency to pass through. Another key use of using filters is that they can help with removing noise that would negatively impact the signal-to-noise ratio of the link. Finally, a filter can also be used for channel selection which can be especially important for switching to other frequencies.

GFSK (Gaussian Frequency-Shift Keying) Demodulator

Because this system is a spread spectrum system and the data is sent across multiple frequencies, the GFSK demodulator helps to smooth out any frequency deviations that may be present in the spread spectrum. This is especially important in the area of digital communications where binary 1s and 0s are specified by changes in the frequency or phase of a carrier wave.

RSSI (Received Signal Strength Indicator)

The RSSI is used to indicate to the receiver system what the received power levels from the antenna are. This is important because the RSSI can help set a threshold for whether or not the SPI or any other DSP system should accept the signal. This can help to filter out low power noise that may be present and also other low power signals on the same receive frequencies.

DSSS Baseband & Framer/Data Interface and Sequencer

As per IEEE 802.11 standards for DSSS systems, information is transmitted in frames. The DSSS baseband & framer block in conjunction with the data interface and sequencer block are responsible for sorting and reassembling the data received into the original signal.

SPI (Serial Peripheral Interface)

The SPI block is responsible for delivering the proper data received to the RC vehicle. It acts as the block that controls the vehicle to move forward, reverse, and turn itself based on the digital data it has received. SPI is often found in systems that fall under IEEE 802.11.

Project Requirements

Our senior project was a continuation off of a previous groups' research; therefore it was pertinent that we learn how communication systems could be jammed. Our job became to investigate the reasons why a previous student's camera transmitter was jamming a spread spectrum communication system.

In 2010, a student had attached a camera to his RC car that transmitted a video feed back to the operator's location. However, it became apparent that this task could not be carried out as the camera transmitter seemed to prevent the RC car from receiving commands from the car's transmitter. This issue was notable due to the fact that the camera transmitter, which uses a single carrier frequency, was able to jam a spread spectrum communication system. This issue became the launching point for a project to investigate the jamming of spread spectrum systems.

A group from the 2011-12 school year accepted the project and proceeded to investigate. Ultimately, they were unsuccessful in identifying the reasons why the camera transmitter seemed to interfere with the RC car's communication system. This required that another group continue their work and investigate the matter further.

As a result, our group entered the 2012-13 school year and decided to replicate the previous group's work and methods to determine whether or not they had made any errors before investigating more possible reasons for jamming. By replicating the previous groups' data ourselves, we were ultimately able to refine our research methods and reach the correct conclusion for why the jamming occurs.

A prediction was made that the camera transmitter's frequency spectrum contained high frequency spurs around 2.4 GHz which could be interfering with the link between the car's receiver and operator's car transmitter by killing the signal-to-noise ratio (SNR). Here, SNR refers to the transmitter signal to jamming signal ratio, since the noise is the jamming signal. SNR will be used to define the transmitter signal to jamming signal ratio from here on. A diagram explaining the noise (or jamming) effect on a data signal is shown in figure 6.

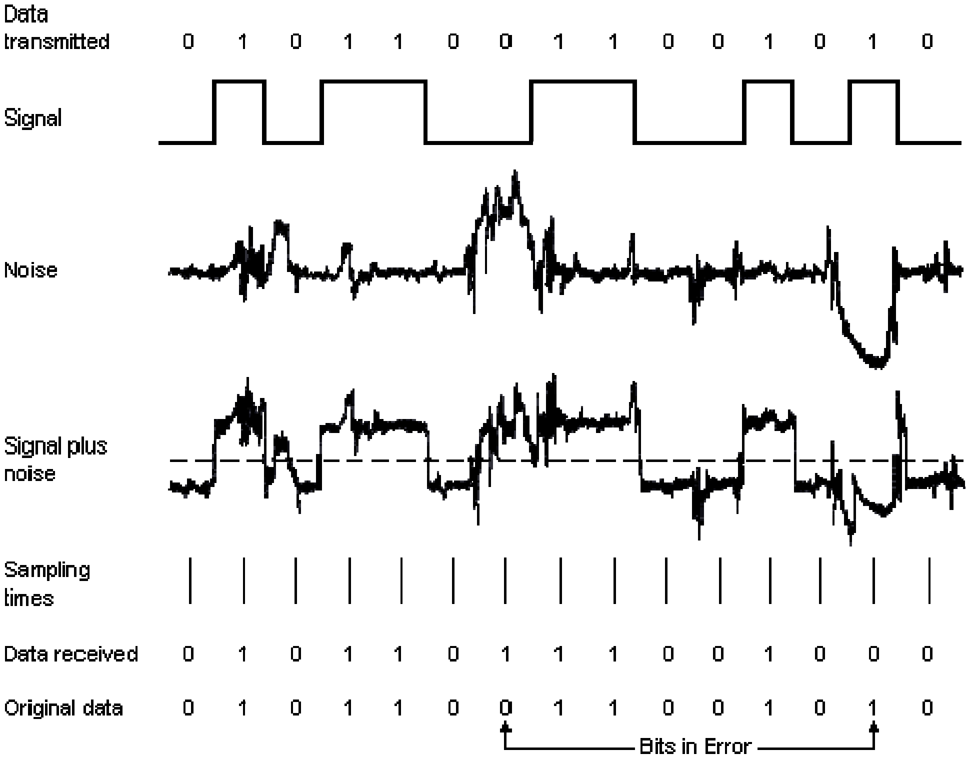
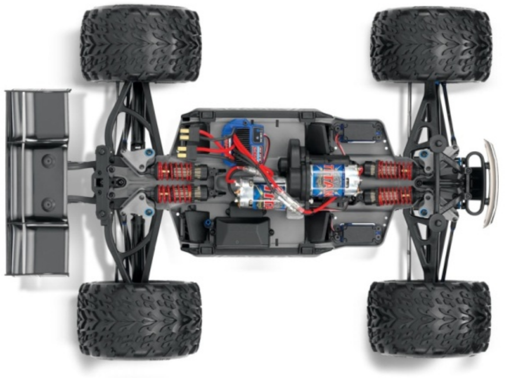


Figure 5: Diagram showing the effects of noise (jamming signal) on transmitted data signals (picture from http://www.technologyuk.net/telecommunications/telecom_principles/noise.shtml)

In the figure above, the channel noise signal disrupts the transmitted data signal by distorting the data stream, causing 2 received bits to be wrong. This is indicated in the diagram. In our experiment, the noise can be referred to simply as the jamming signal, since the effect on the transmitted data signal is the same, just over a concentrated frequency range located at the jammer's frequency. We investigated this possibility of the high-frequency spurs killing the receiver's SNR at 2.4GHz, and if the data confirmed our hypothesis, it could be used to replicate another jamming system based off these principles. If this test was successful, this would allow us to validate our hypothesis and verify our claims.

The ultimate goal of this research is to provide knowledge of how to jam spread spectrum communication systems and to delve further into improving jamming performances and creating new jamming methods. The findings can potentially lead to new countermeasures in electronic warfare, such as taking control over RC vehicles with spread spectrum communication systems.

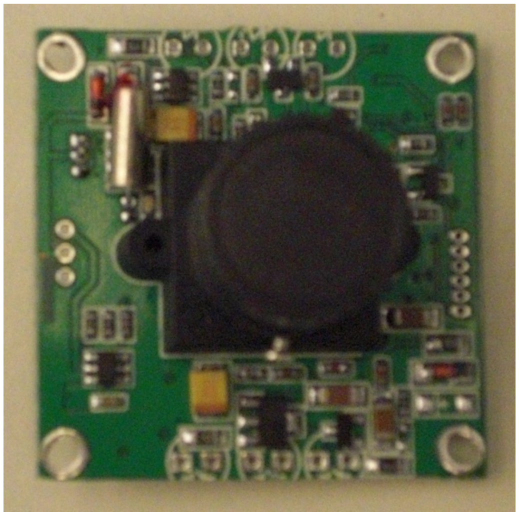
Equipment List



E-Revo Traxxas RC Car (#5603)

Traxxas TQ 2.4 GHz Transmitter

EZ-Peak Plus Battery Charger for Car

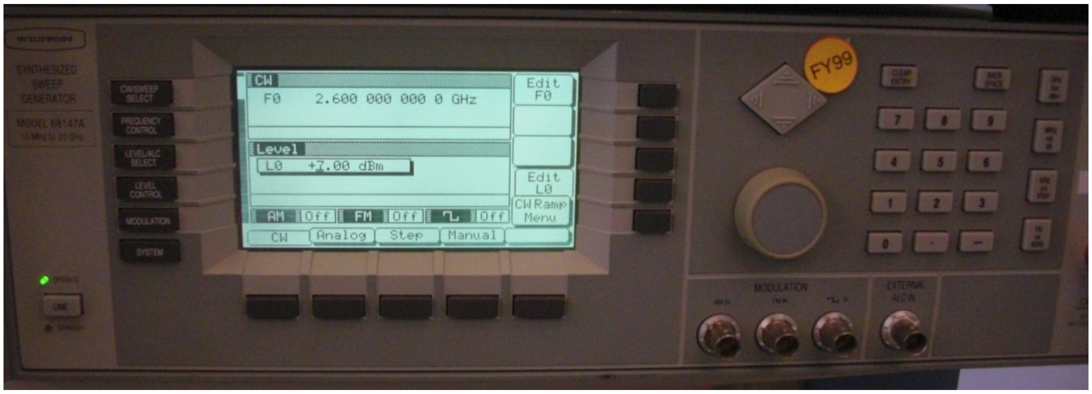


SONY CCD 1/3 inch Camera

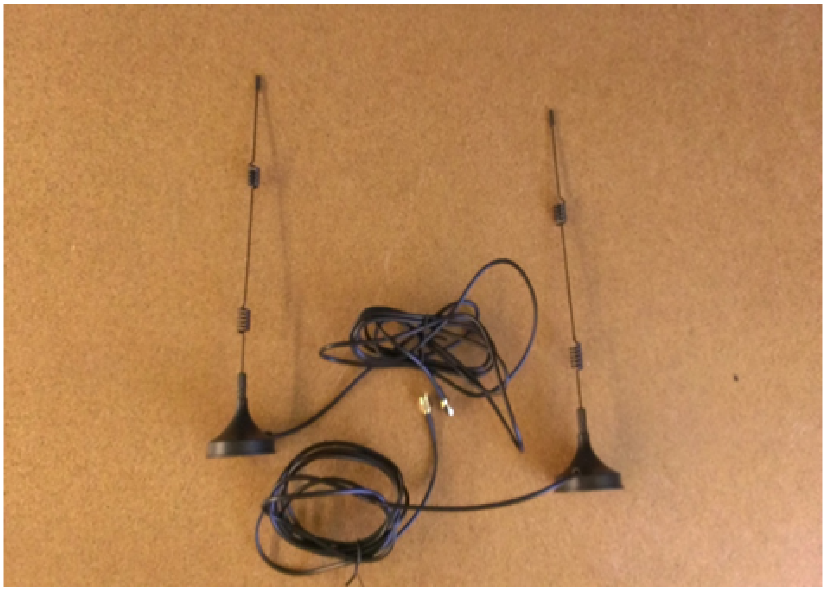
900 MHz 4 Channel Video Transmitter (1500 mW)

Signal Analyzer: 9 KHz-7.5 GHz Agilent

Network Analyzer



Signal Generator



Pair of 2.4 GHz dipole antennas

2.4 GHz Directional Antenna

Test Plans

Because this project is a continuation of the previous year's group, the following investigation is based on their preliminary findings and research. The previous group concluded that the responsible jamming frequencies were from channels 0, 1, 2, and 3 of the camera transmitter, which are 910, 980, 1010, and 1040MHz, respectively. It was suspected that these jamming frequencies were overloading the front end amplifier of the RC car's receiver system (refer to figure 4). Therefore, it was decided to test the hypothesis and prove whether or not this was the cause of the jamming.

However, it was soon discovered during set-up and testing that the amplifier itself could not be tested since it is an internal component inside an IC which contained the entire receiver system. The IC layout did not provide pins which were attached to the output of the amplifier system (see figure 5); thus, we were unable to isolate and directly test the overloading of the amplifier.

However, suspicions arose which debunked the previous group's conclusions that the responsibly jamming frequencies were between 900 and 1100 MHz due to the fact that not all channels of the camera transmitter were jamming the car. Reproducing the previous group's test, we discovered that only channel 1 consistently jammed the car, while channels 2 and 3 jammed intermittently, and channel 0 never jammed.

Further testing concluded that we could not reproduce the jamming response using a synthesizer and a simple dipole: in our reproduced experiment, more power was delivered at the supposed jamming frequencies, but jamming the receiver system was unsuccessful. To see the comparative signal powers at each of the 4 channel frequencies, refer to table 3. As a result, we felt confident that the previous group's conclusions were incorrect, which led us to develop a new experiment.

Therefore, we decided to consider that the receiver system was simply having its data stream interfered with around 2.4 GHz. After isolating the RC car's transmitter's frequency spectrum (which was centered around 2.436 GHz), we looked at the frequency spectrum of each of the camera transmitter's channels around 2.436 GHz. At this point, we discovered that channel 0 had very low power at this frequency, -59.371dBm, whereas channels 1 through 3 had powers of -42.501dBm, -40.513dBm, and -44.602dBm, respectively. See table 5 for data. This somewhat verified our predictions that the jamming frequencies were actually lying directly in the communications channel of the RC receiver/transmitter.

This allowed us to replicate the jamming by hooking up a 2.4 GHz rated antenna to the high frequency synthesizer. We were successful and were able to jam the receiver system. However, our distance was still more or less limited.

Afterwards, we ordered a yagi antenna (directional antenna, vertically polarized) which improved our jamming range dramatically due to the added signal boost of the antenna. The data shown for the effective jamming range is shown in figure 17.

We also noticed inconsistent results in our jamming ability, and concluded that it was due to the fact that our setup between test days was also inconsistent. This is because the relative distances between the car receiver, car transmitter, and jammer were different between the different days. We decided to make graphs depicting the relationship between the jammer and car receiver vs. the distance between the car transmitter and car receiver. This data can be seen in figure 17. Essentially, at this point in the investigation, the data we were after was only the jammer's power, and the SNR of the system was ignored. Later realizations led us to believe that the SNR, not solely the jamming power, but the ratio of that power to the car transmitter power received at the car’s receiver, was the primary cause for whether or not the car would be effectively jammed.

Analysis

Finding Jamming Frequency Range:

The previous group claimed that, based on their research, “the frequencies between 1GHz and 2.4 GHz are most likely responsible for jamming the RC car.” Our experiments narrowed the jamming frequency range to between 2.3GHz and 2.5GHz, with the most effective jamming frequency of 2.436GHz. This frequency range is the same as the communication system of the RC car itself. No other frequencies between 10MHz and 7.5GHz - the testable frequency range limited by the equipment available in the lab - were responsible or capable of jamming the system.

The jamming technique employed in this study is called single tone jamming, or spot jamming for short. In this technique, the jamming signal is a continuous wave (CW) tone placed at a single frequency which aims to overcome the processing gain of DSSS systems (increase the SNR past the critical point at which the jammer’s power is higher than the data stream’s power received at the receiver) at the receiver’s front-end, causing the system to fail. Single tone jamming can be applied to all DSSS systems. Because the signal power is concentrated at a single frequency, single tone jamming signals usually have much higher peak power than multi-tone or broadband jamming signals that are spread over multiple independent frequencies or a continuous frequency range. This increase in power increases the probability that the jamming signal will overpower the receiver’s front end. Thus, this technique was chosen to be used to jam the RC car system. Single tone jamming is explained in figure 6 below:

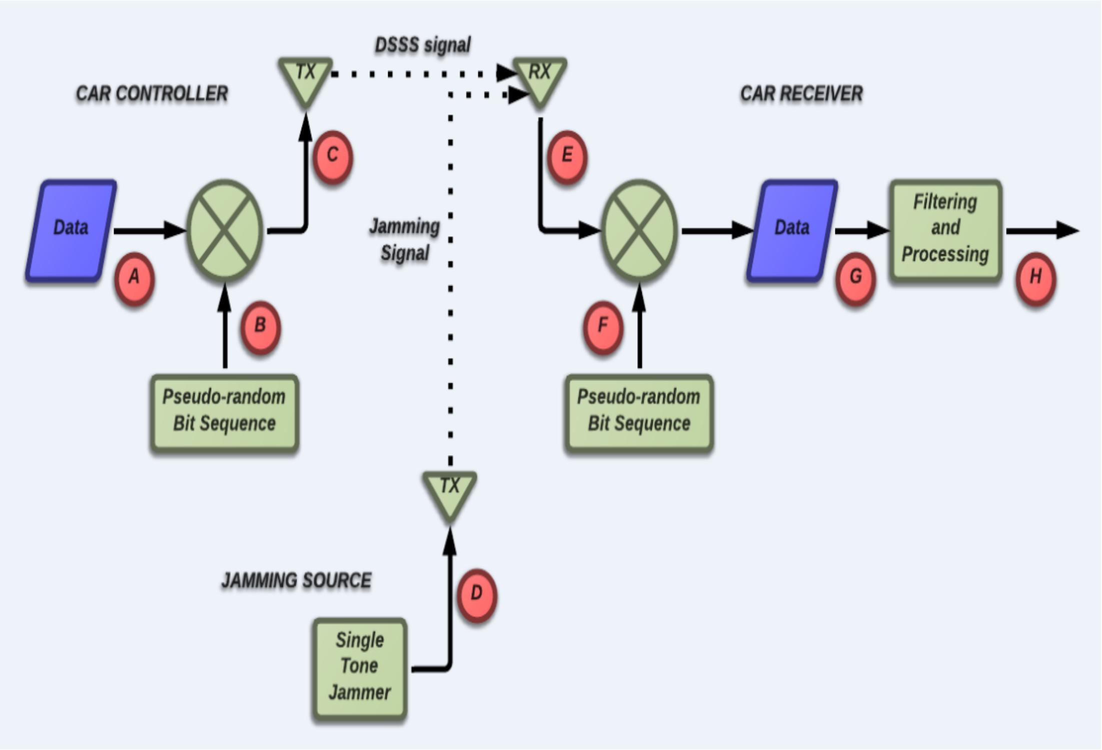
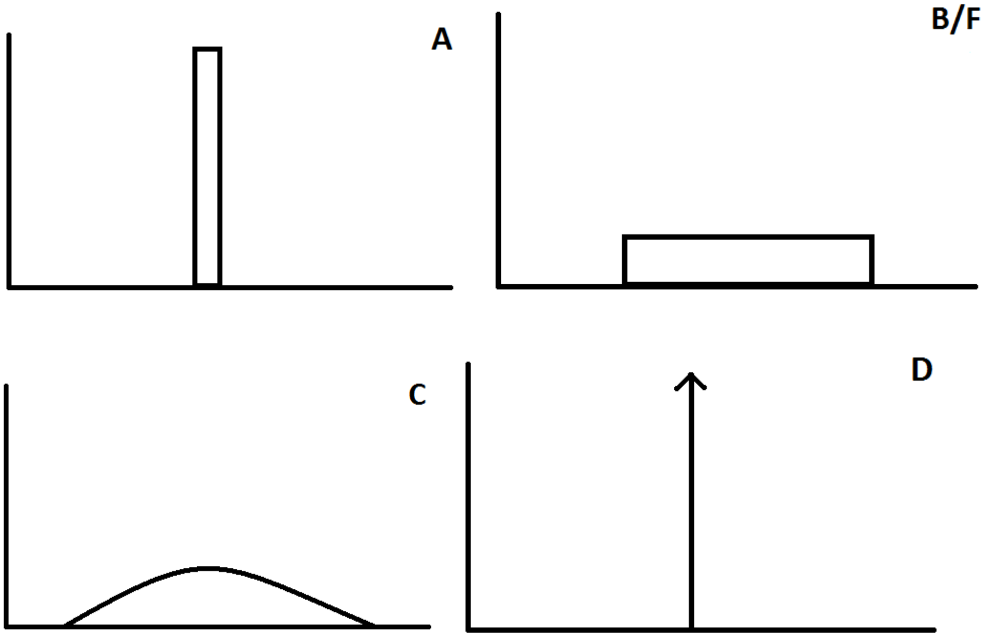


Figure 6: Pictograph of Single Tone Jamming of A DSSS Data Signal

The waveforms at each of the points labeled "A" through "H" are shown below in Figure 7.



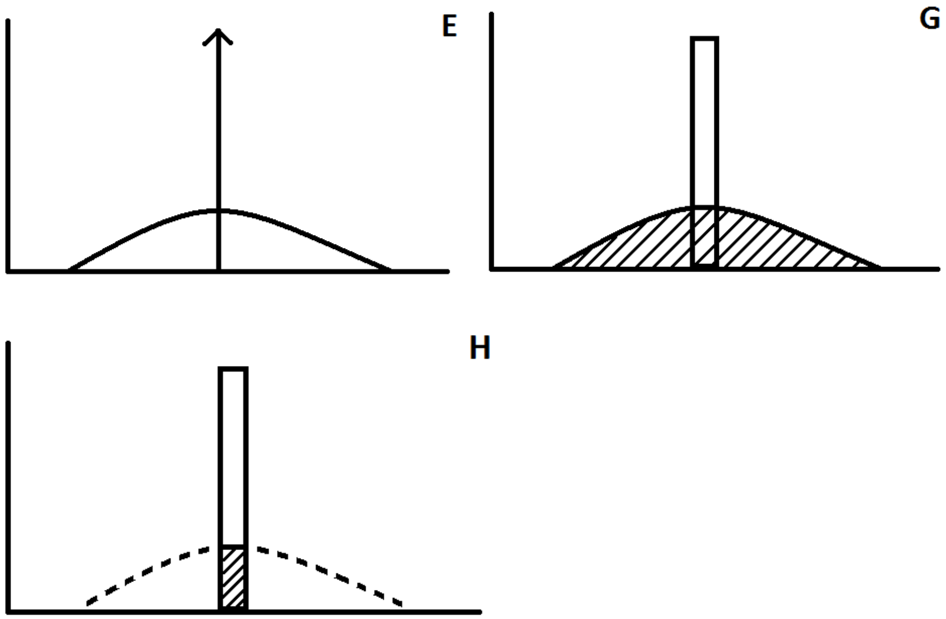
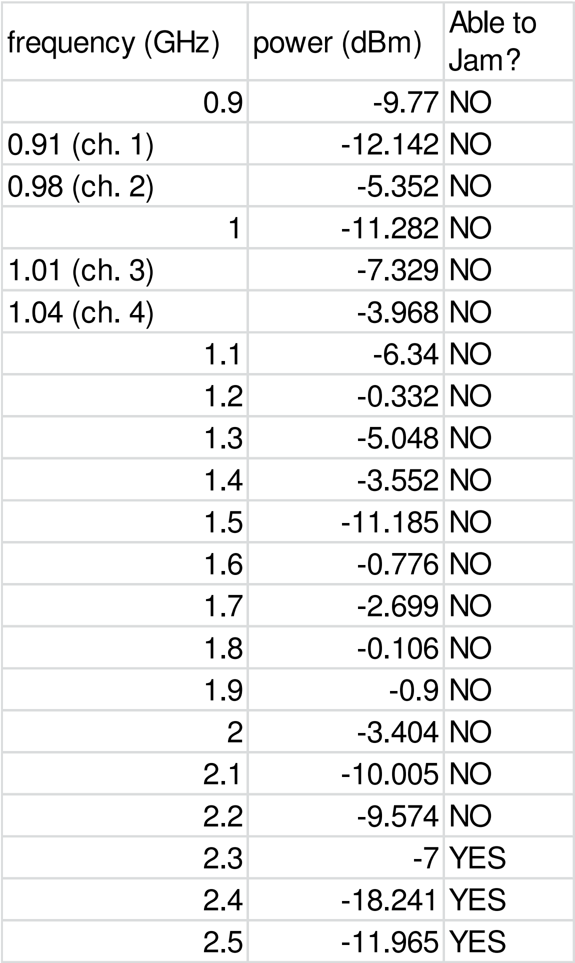


Figure 7:Signal Spectra at points A through H of figure 6

The drawback of single tone jamming is that the frequency of the tone must be very specific to the system that is to be jamming. To find this specific frequency for the RC car system, a frequency synthesizer and directional antenna were used to attempt to jam the RC car at close range. The frequency was manually scanned from 0.9GHz to 2.5GHz. The signal power and frequency were verified using a 2.4GHz receive antenna and the Agilent CXA signal analyzer. The receive and transmit antennas were placed immediately adjacent to each other in this test set-up for the purpose of detecting any possible chance that the system would be jammed since jamming capability increases as distance between the jammer and the system decreases. The power was measured at the fundamental frequencies of each channel of the camera transmitter. These powers are included in table 2 below along with their associated transmitter channel.



frequency (GHz)	power (dBm)	Able to Jam?
0.9	-9.77	NO
0.91 (ch. 1)	-12.142	NO
0.98 (ch. 2)	-5.352	NO
1	-11.282	NO
1.01 (ch. 3)	-7.329	NO
1.04 (ch. 4)	-3.968	NO
1.1	-6.34	NO
1.2	-0.332	NO
1.3	-5.048	NO
1.4	-3.552	NO
1.5	-11.185	NO
1.6	-0.776	NO
1.7	-2.699	NO
1.8	-0.106	NO
1.9	-0.9	NO
2	-3.404	NO
2.1	-10.005	NO
2.2	-9.574	NO
2.3	-7	YES
2.4	-18.241	YES
2.5	-11.965	YES

Table 2: Frequency scan using frequency synthesizer and directional antenna from 0.9 to 2.5GHz along with signal power and jamming capability

The tabular data is plotted in a scatter plot below in figure 8. Looking at the data shown in figure 8, there is no clear relationship between frequency of the signal and power received. The received power varies from as low as -18.241dBm at 2.4GHz to as high as -0.332 at 1.2GHz. Interestingly enough, the RC was only jammed at frequencies between 2.3GHz and 2.5GHz. Outside of this range, no jamming was possible. This range, however, contains the lowest received signal powers. Thus, this experiment concretely disproved the idea that the jamming signal is frequency-independent and is only dependent on the amount of power received. While it is important to transmit enough power to overpower the front end of the receiver, the jamming frequency is clearly frequency-dependent on the system.

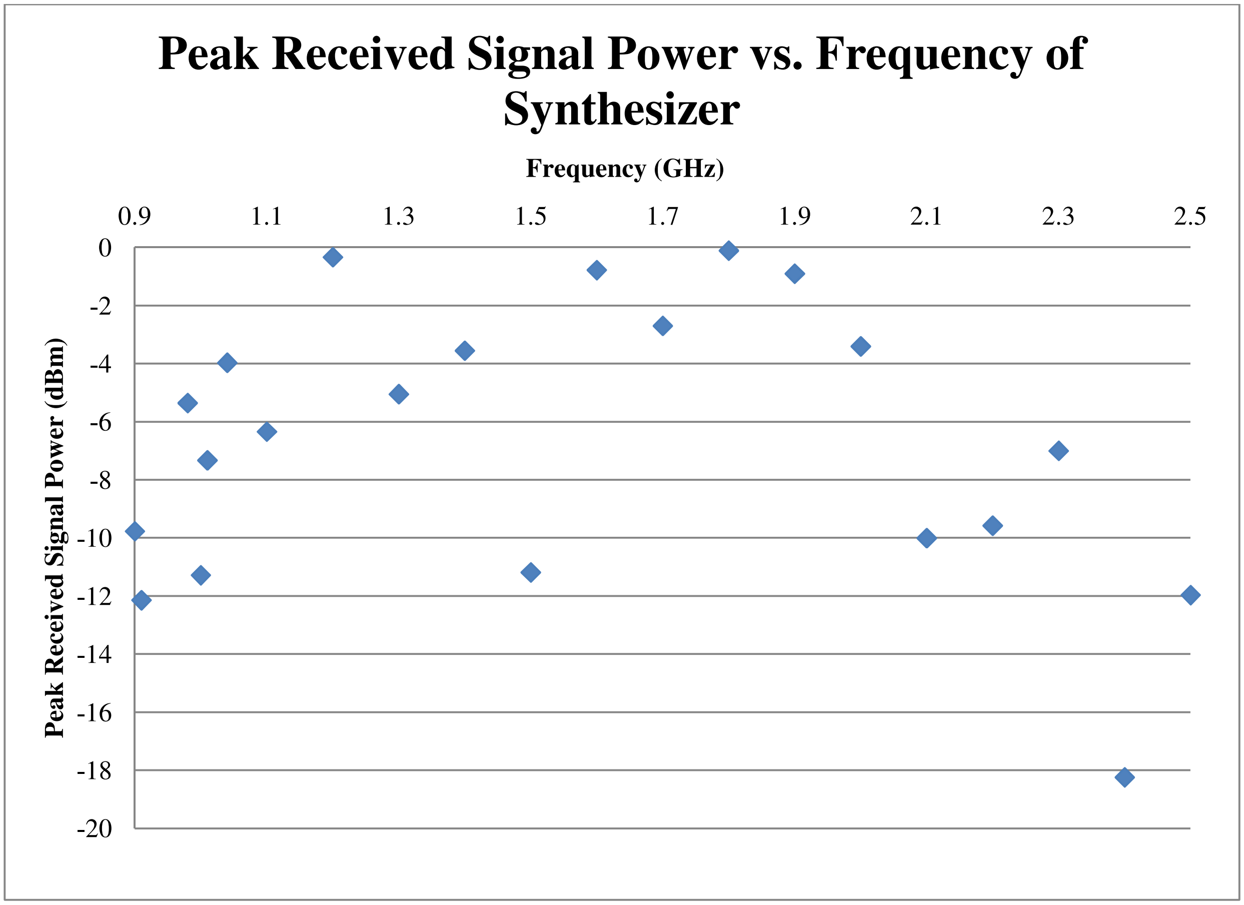


Figure 8: peak received signal power vs. frequency using frequency synthesizer and directional antenna from 0.9 to 2.5GHz

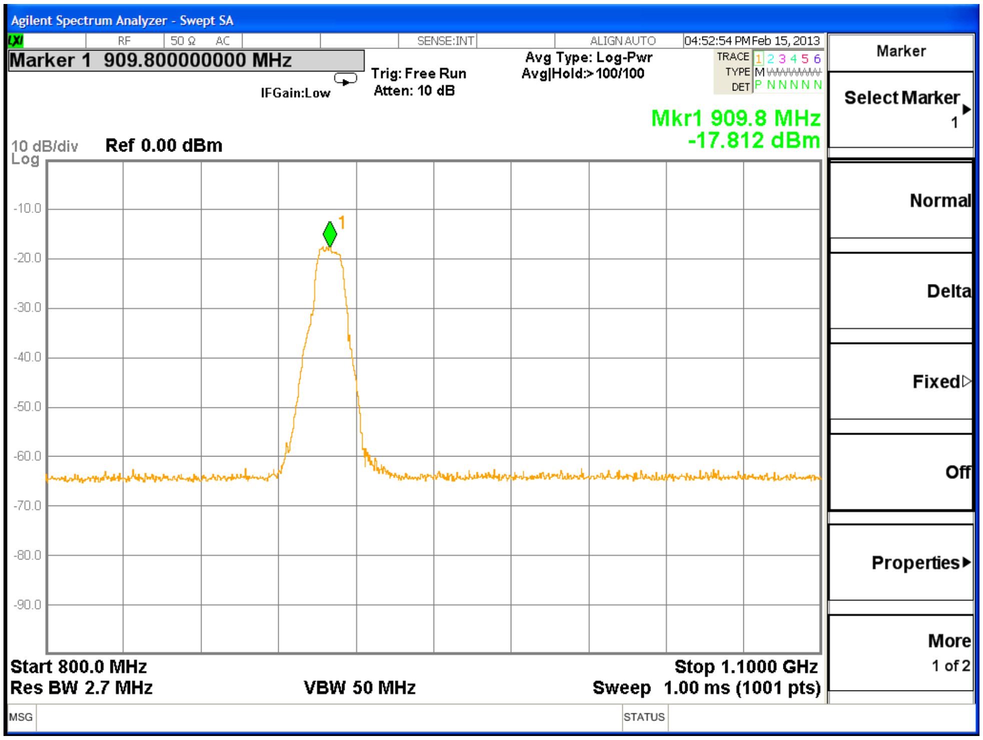
Furthermore, inspecting the signal powers at the fundamental frequencies of the camera transmitter, it is shown that for each of these frequencies listed in table 2, the power received was between 5.67 and 8.618dBm higher than what was being received by the camera transmitter itself; however, no still no jamming occurred. This further disproves the idea that the camera transmitter was jamming the RC car at its fundamental frequencies because boosting the power still did not improve jamming ability. Even for channel 1, at 910MHz, the camera transmitter jammed the car at close range, yet this was not possible to reproduce using the synthesizer and directional antenna, even though more power was added to the jamming signal. This was a previously held belief, that because of the proximity of the camera transmitter to the RC car's receiver antenna, it was responsible for jamming the car at its max power output (its fundamental frequency). Thus, this theory was disproved. This is summarized in table 3 below:

frequency	signal power		Power difference
fundamental frequency (MHz)	camera transmitter signal power (dBm)	synthezizer and directional antenna (dBm)	Power difference (synthesizer power – camera transmitter power) (dBm)
909.8 (910)	-17.812	-12.142	5.67
982.7 (980)	-11.984	-5.352	6.632
1009.7 (1010)	-16.01	-7.329	8.681
1042.6 (1040)	-11.301	-3.968	7.333

Table 3: signal power of each channel of the camera transmitter and signal power of a matched frequency using the frequency synthesizer and directional antenna along with the difference in power

Finding Frequency Spectrum of Camera Transmitter:

Next, the camera transmitter was connected to the camera, and both were powered using the digital power supply set to 11V_{DC}. The camera transmitter was connected directly to its transmit antenna. A 2.4GHz receive antenna was used to receive the signal and was connected directly to the Agilent CXA spectrum analyzer. With the camera transmitter transmitting a signal, both the transmitting and receiving antennas were oriented to find the optimum placement to record the max signal power at the receiving end. The max-hold function was used to record the max signal power. Screen captures were taken for all four operating channels. The fundamental frequency of each channel of the camera transmitter, as well as the corresponding signal power, is shown in Figures 9 through 12 and summarized in Table 4. The following images are focused on the narrow frequency range surrounding each fundamental frequency – shown by the screen marker – to show a clear representation of the frequency spectrum around the main lobe.



Agilent Spectrum Analyzer - Swept SA

RF 50 Ω AC SENSE:INT ALIGN AUTO 04:52:54 PM Feb 15, 2013

Marker 1 909.800000000 MHz

IFGain:Low

Trig: Free Run
Atten: 10 dB

Avg Type: Log-Pwr
Avg|Hold:>100/100

TRACE 1 2 3 4 5 6
TYPE M WWWWW
DET P N N N N N

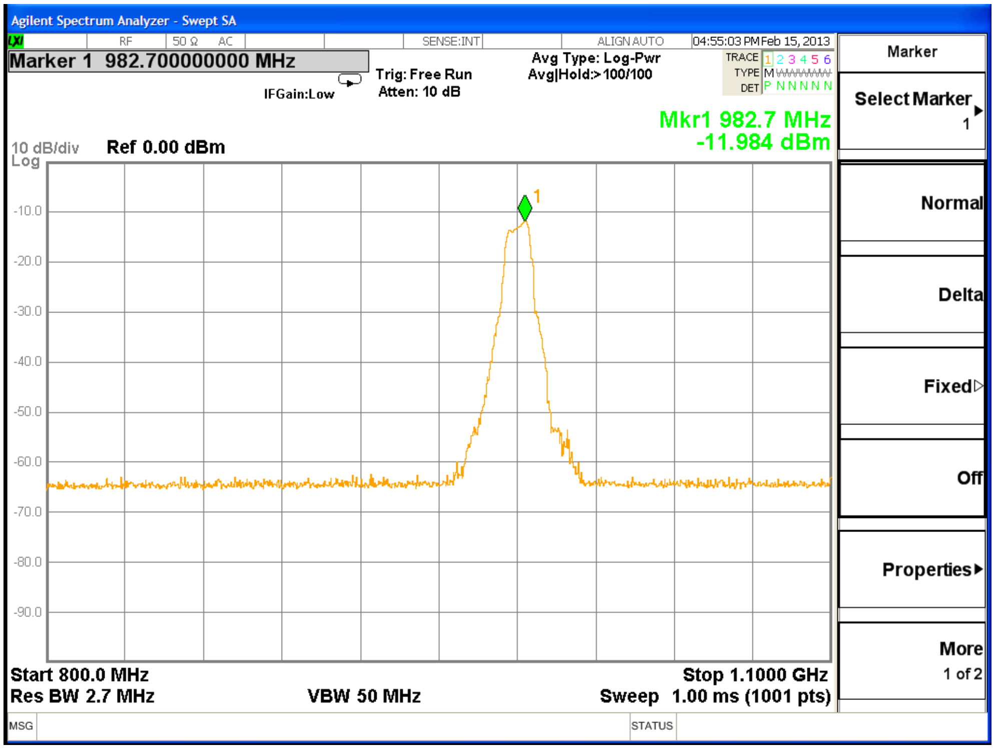
Mkr1 909.8 MHz
-17.812 dBm

10 dB/div Ref 0.00 dBm
Log

Start 800.0 MHz
Res BW 2.7 MHz
VBW 50 MHz
Stop 1.1000 GHz
Sweep 1.00 ms (1001 pts)

MSG
STATUS

Figure 9: camera transmitter - channel 0 at fundamental frequency



Agilent Spectrum Analyzer - Swept SA

RF 50 Ω AC SENSE:INT ALIGN AUTO 04:55:03 PM Feb 15, 2013

Marker 1 982.700000000 MHz

IFGain:Low

Trig: Free Run
Atten: 10 dB

Avg Type: Log-Pwr
Avg|Hold:>100/100

TRACE 1 2 3 4 5 6
TYPE M WWWWW
DET P N N N N N

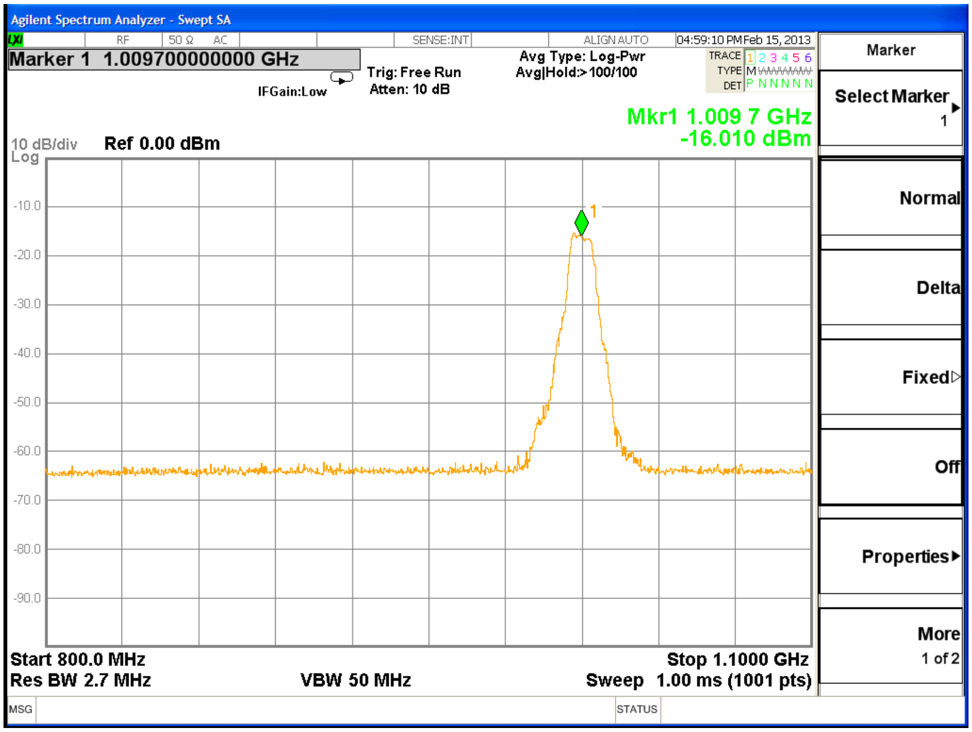
Mkr1 982.7 MHz
-11.984 dBm

10 dB/div Ref 0.00 dBm
Log

Start 800.0 MHz
Res BW 2.7 MHz
VBW 50 MHz
Stop 1.1000 GHz
Sweep 1.00 ms (1001 pts)

MSG
STATUS

Figure 10: camera transmitter - channel 1 at fundamental frequency



Marker 1 1.009700000000 GHz

IFGain:Low

Trig: Free Run
Atten: 10 dB

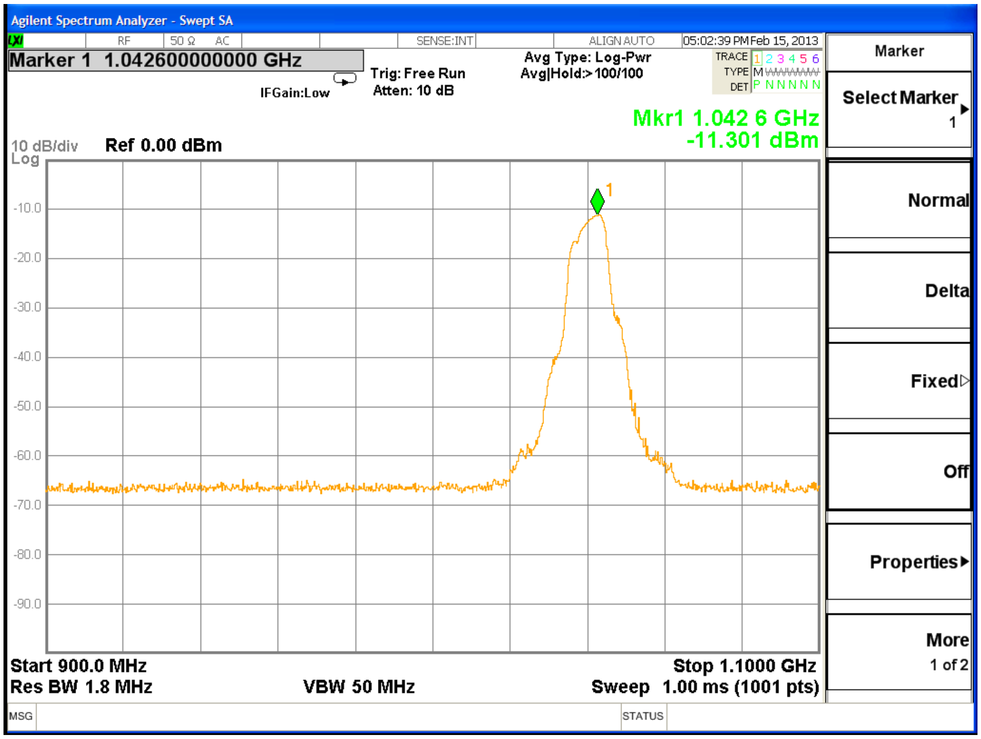
Avg Type: Log-Pwr
Avg|Hold:>100/100

Mkr1 1.009 7 GHz
-16.010 dBm

10 dB/div Log Ref 0.00 dBm

Start 800.0 MHz
Res BW 2.7 MHz
VBW 50 MHz
Stop 1.1000 GHz
Sweep 1.00 ms (1001 pts)

Figure 11: camera transmitter - channel 2 at fundamental frequency



Marker 1 1.042600000000 GHz

IFGain:Low

Trig: Free Run
Atten: 10 dB

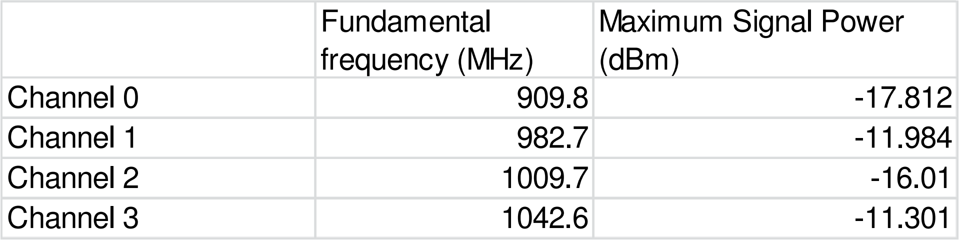
Avg Type: Log-Pwr
Avg|Hold:>100/100

Mkr1 1.042 6 GHz
-11.301 dBm

10 dB/div Log Ref 0.00 dBm

Start 900.0 MHz
Res BW 1.8 MHz
VBW 50 MHz
Stop 1.1000 GHz
Sweep 1.00 ms (1001 pts)

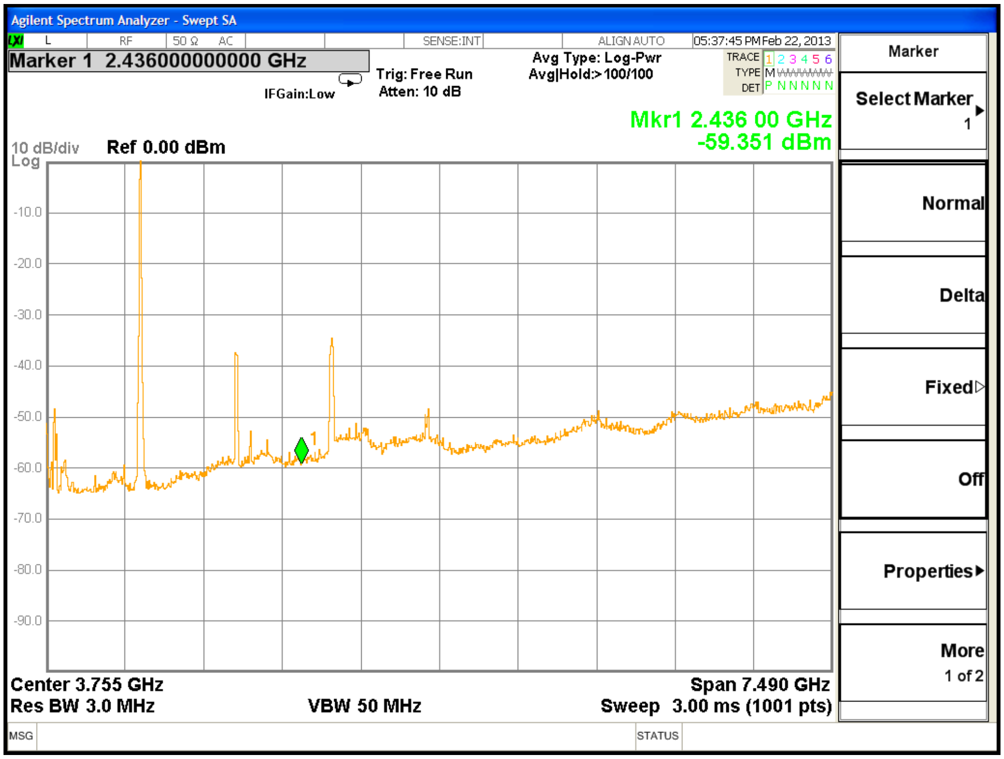
Figure 12: camera transmitter - channel 3 at fundamental frequency



	Fundamental frequency (MHz)	Maximum Signal Power (dBm)
Channel 0	909.8	-17.812
Channel 1	982.7	-11.984
Channel 2	1009.7	-16.01
Channel 3	1042.6	-11.301

Table 4: Summary of fundamental frequency and signal power for channels 1 through 4 (figures 9 through 12) of camera transmitter

To increase the signal power, the camera transmitter was connected directly to the Agilent CXA spectrum analyzer. A broad frequency range (10MHz to 7.5GHz) for each channel of the camera transmitted was captured and is shown in figures 13 through 16 below. This frequency range shows all spurious frequencies occurring within the range. Note that channel 0 contains no spurious frequencies at the marker value of 2.436GHz, while all other channels do. This explains why channel 0 never jams the car, while channels 1, 2 and 3 have jamming capabilities. A summary of the peak signal power of the camera transmitter at 2.436GHz for each channel is given in table 5.



Agilent Spectrum Analyzer - Swept SA

Marker 1 2.436000000000 GHz

IFGain:Low

Trig: Free Run
Atten: 10 dB

Avg Type: Log-Pwr
Avg|Hold:> 100/100

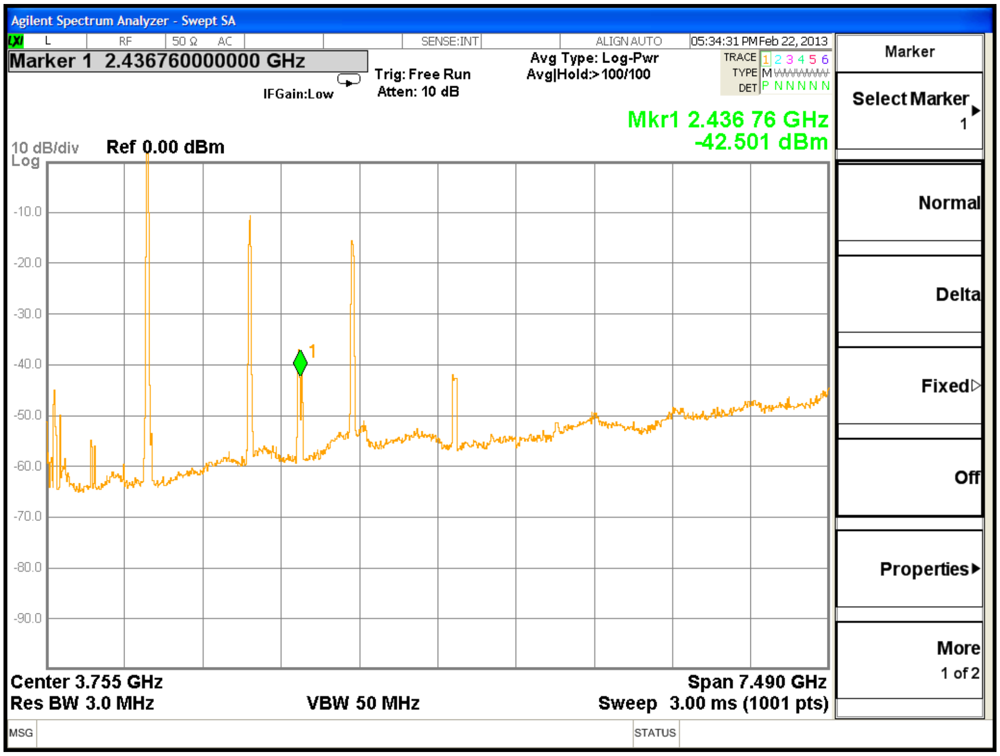
05:37:45 PM Feb 22, 2013

Mkr1 2.436 00 GHz
-59.351 dBm

10 dB/div Log Ref 0.00 dBm

Center 3.755 GHz
Res BW 3.0 MHz
VBW 50 MHz
Span 7.490 GHz
Sweep 3.00 ms (1001 pts)

Figure 13: Broad Frequency Spectrum of Channel 0 (10MHz to 7.5GHz)



Agilent Spectrum Analyzer - Swept SA

Marker 1 2.436760000000 GHz

IFGain:Low

Trig: Free Run
Atten: 10 dB

Avg Type: Log-Pwr
Avg|Hold:> 100/100

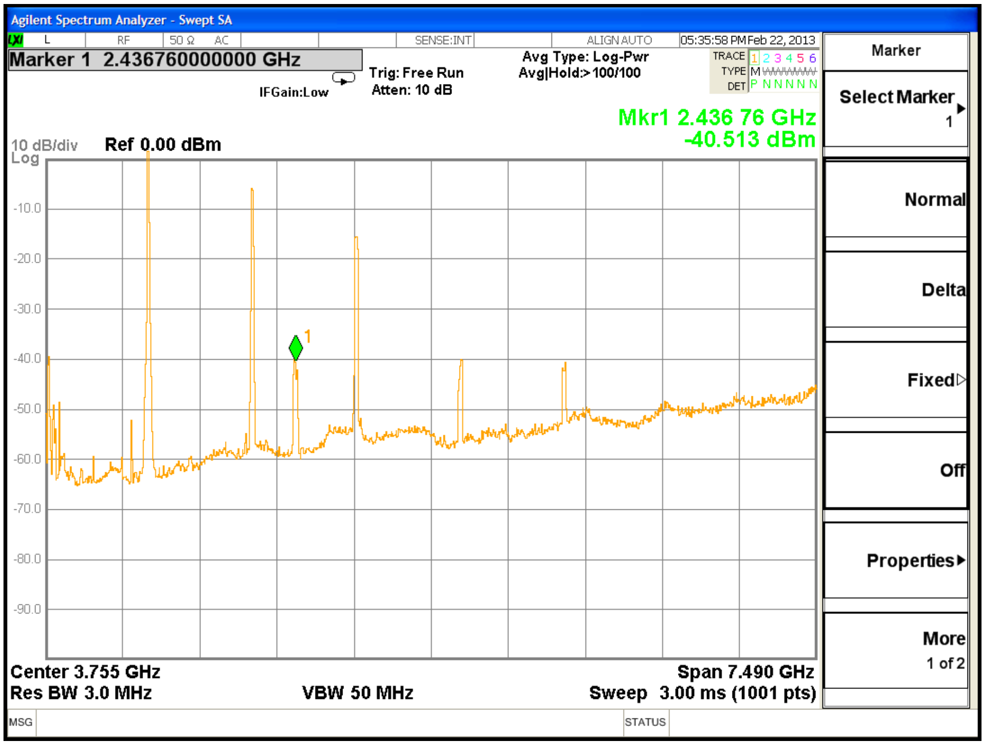
05:34:31 PM Feb 22, 2013

Mkr1 2.436 76 GHz
-42.501 dBm

10 dB/div Log Ref 0.00 dBm

Center 3.755 GHz
Res BW 3.0 MHz
VBW 50 MHz
Span 7.490 GHz
Sweep 3.00 ms (1001 pts)

Figure 14: Broad Frequency Spectrum of Channel 1 (10MHz to 7.5GHz)


Agilent Spectrum Analyzer - Swept SA

L RF 50 Ω AC SENSE:INT ALIGN AUTO 05:35:58 PM Feb 22, 2013

Marker 1 2.436760000000 GHz

IFGain:Low

Trig: Free Run
Atten: 10 dB

Avg Type: Log-Pwr
Avg|Hold:> 100/100

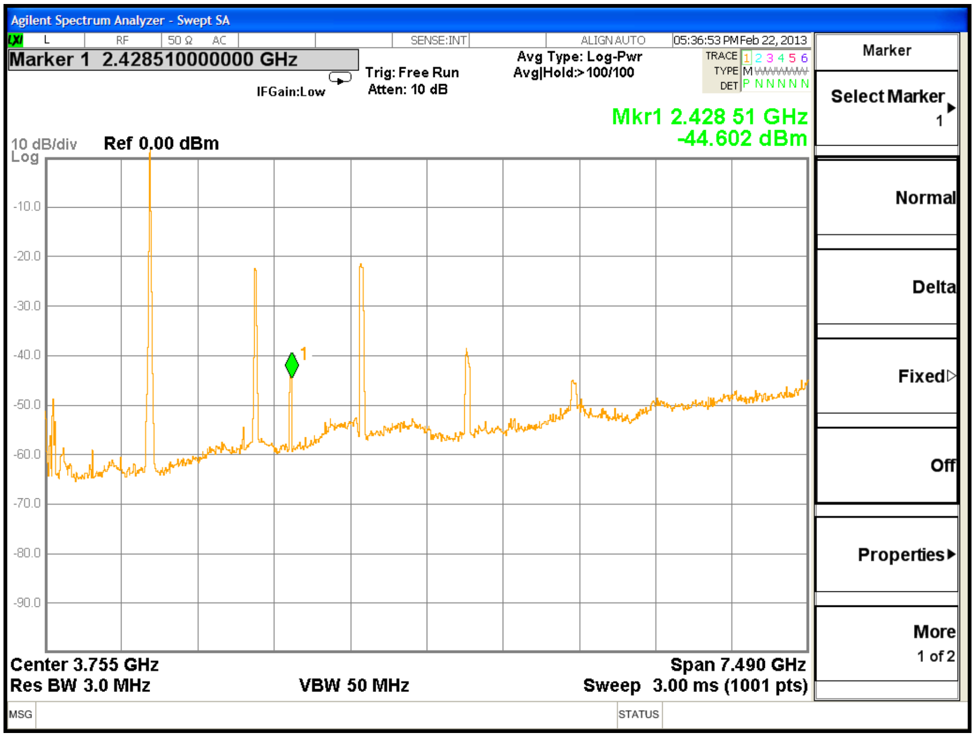
TRACE 1 2 3 4 5 6
TYPE M WWWWW
DET P N N N N N

Mkr1 2.436 76 GHz
-40.513 dBm

10 dB/div Ref 0.00 dBm

Center 3.755 GHz
Res BW 3.0 MHz
VBW 50 MHz
Span 7.490 GHz
Sweep 3.00 ms (1001 pts)

Figure 15: Broad Frequency Spectrum of Channel 2 (10MHz to 7.5GHz)


Agilent Spectrum Analyzer - Swept SA

L RF 50 Ω AC SENSE:INT ALIGN AUTO 05:36:53 PM Feb 22, 2013

Marker 1 2.428510000000 GHz

IFGain:Low

Trig: Free Run
Atten: 10 dB

Avg Type: Log-Pwr
Avg|Hold:> 100/100

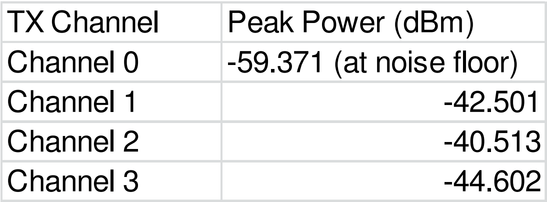
TRACE 1 2 3 4 5 6
TYPE M WWWWW
DET P N N N N N

Mkr1 2.428 51 GHz
-44.602 dBm

10 dB/div Ref 0.00 dBm

Center 3.755 GHz
Res BW 3.0 MHz
VBW 50 MHz
Span 7.490 GHz
Sweep 3.00 ms (1001 pts)

Figure 16: Broad Frequency Spectrum of Channel 3 (10MHz to 7.5GHz)



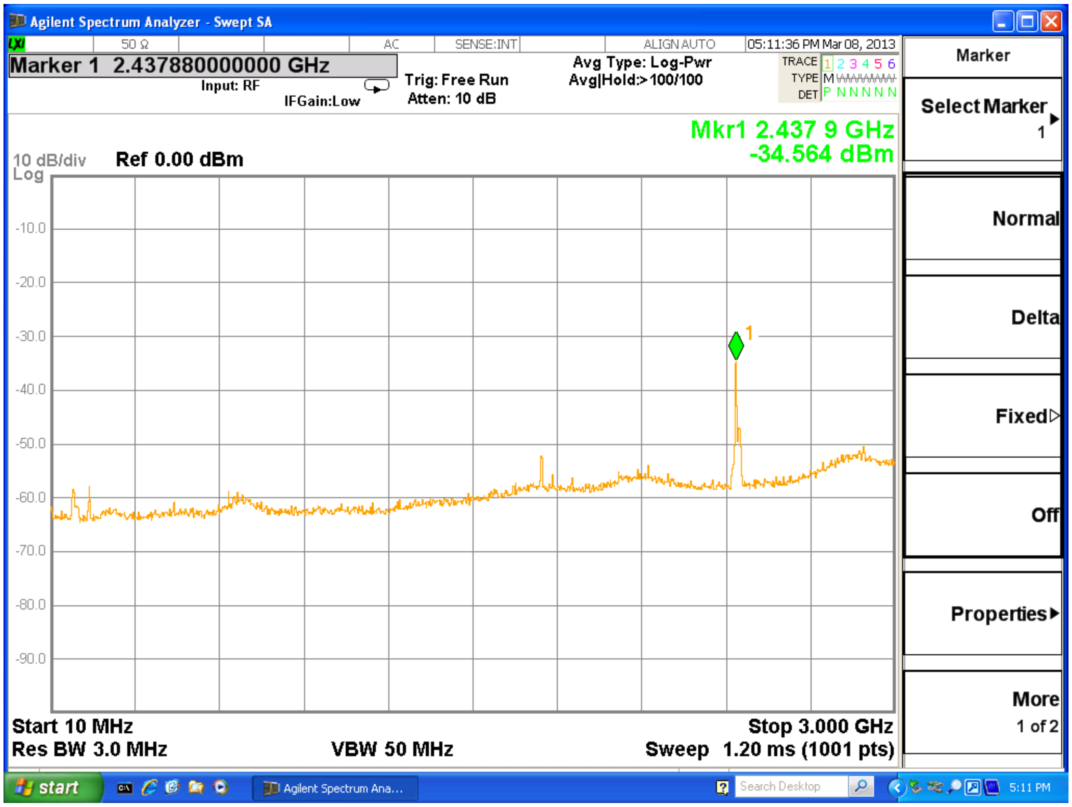
TX Channel	Peak Power (dBm)
Channel 0	-59.371 (at noise floor)
Channel 1	-42.501
Channel 2	-40.513
Channel 3	-44.602

Table 5: Summary of Peak Power of Camera Transmitter at 2.436GHz for channels 0 through 3 (figures 13 through 16)

Isolating A Single Frequency on Frequency Synthesizer

To once again prove that the only frequency capable of jamming the car is the narrow 2.3GHz to 2.5GHz frequency range, a 2.436GHz signal was isolated by eliminating all other frequency spurs from the spectrum. The previous group achieved frequency isolation by applying various filters to the transmitter. Instead, we achieved frequency isolation by using a frequency synthesizer and reducing the power such that any spurs produced were stifled below the noise floor of the spectrum analyzer. The sythesizer was connected to the directional antenna. The synthesizer power was increased to 5dBm, the maximum power at which all unwanted frequency spurs remained below the noise floor. By jamming the car with this transmit spectrum, this proves that only the 2.436GHz peak – and no other spurious frequencies – was responsible for jamming the car because no other frequency was transmitted. At synthesizer powers above 5dBm, spurs began to appear above noise floor.

Additionally, Looking at the data in the jamming distance section, we were able to jam the RC car at powers much less than 5dBm, effectively proving that the 2.436GHz frequency is the jamming frequency. Below is the spectrum of the synthesizer generating a 2.4GHz signal at 5dBm through the directional antenna, being received by a 2.4GHz antenna at the spectrum analyzer.



Agilent Spectrum Analyzer - Swept SA

50 Ω AC SENSE:INT ALIGN AUTO 05:11:36 PM Mar 08, 2013

Marker 1 2.437880000000 GHz

Input: RF

IFGain:Low

Trig: Free Run

Atten: 10 dB

Avg Type: Log-Pwr

Avg|Hold:> 100/100

TRACE 1 2 3 4 5 6

TYPE M WWWWW

DET P N N N N N

Mkr1 2.437 9 GHz

-34.564 dBm

10 dB/div Ref 0.00 dBm

Start 10 MHz

Res BW 3.0 MHz

VBW 50 MHz

Stop 3.000 GHz

Sweep 1.20 ms (1001 pts)

Figure 17: Frequency spectrum of synthesizer showing the isolation of a 2.4379GHz signal with all spurious frequencies at or below the noise floor of the spectrum analyzer

Finding the Maximum Jamming Distance:

The next part of the project involved finding the effective jamming range of the jammer. The previous group was able to jam the RC car within one inch of the car. One of the goals of this project was to increase this range.

Looking into this requirement, it was discovered that the effective jamming range is dependent on the amount of power received by the car's antenna from the jamming signal compared to the car transmitter's signal. The Friis Transmission Formula yields the power received by one antenna (under idealized conditions) from another antenna some distance away transmitting a signal at a known amount of power. The equation is

Where G_T and $G_R$are the antenna gains of the transmitter and receiver respectively, and $\left(\frac{\lambda}{4\pi R}\right)^2$ is the spreading loss of the signal. By inspection of the formula, the power received by the receiver antenna decreases by a factor of R^2 as R is increased. While jamming the RC car, both the car transmitter and the jamming signal are simultaneously being received by the car. Thus, the jamming range is dependent on the distance between the car and the jammer, in addition to the distance between the car and the car transmitter. This means that when the car transmitter is operated close to the car, the effective jamming range decreases; when the car transmitter is operated further from the car, the effective jamming range increases. This is because when the car transmitter is further away, the received signal power is lower at the car's receiver. This enables the jamming signal's power to be decreased and still maintain the same critical SNR needed to effectively jam the car's receiver. Thus, the jamming signal can be generated from further away as well. The jamming range was plotted against the power of the jamming signal for when the car transmitter was 1m away from the car and again when it was 2m away from the car. When the car and car transmitter were separated by 1m, the system is referred to as the 1m system. When the car and car transmitter were separated by 2m, the system is referred to as the 2m system. The data is shown in Figure 18 below.

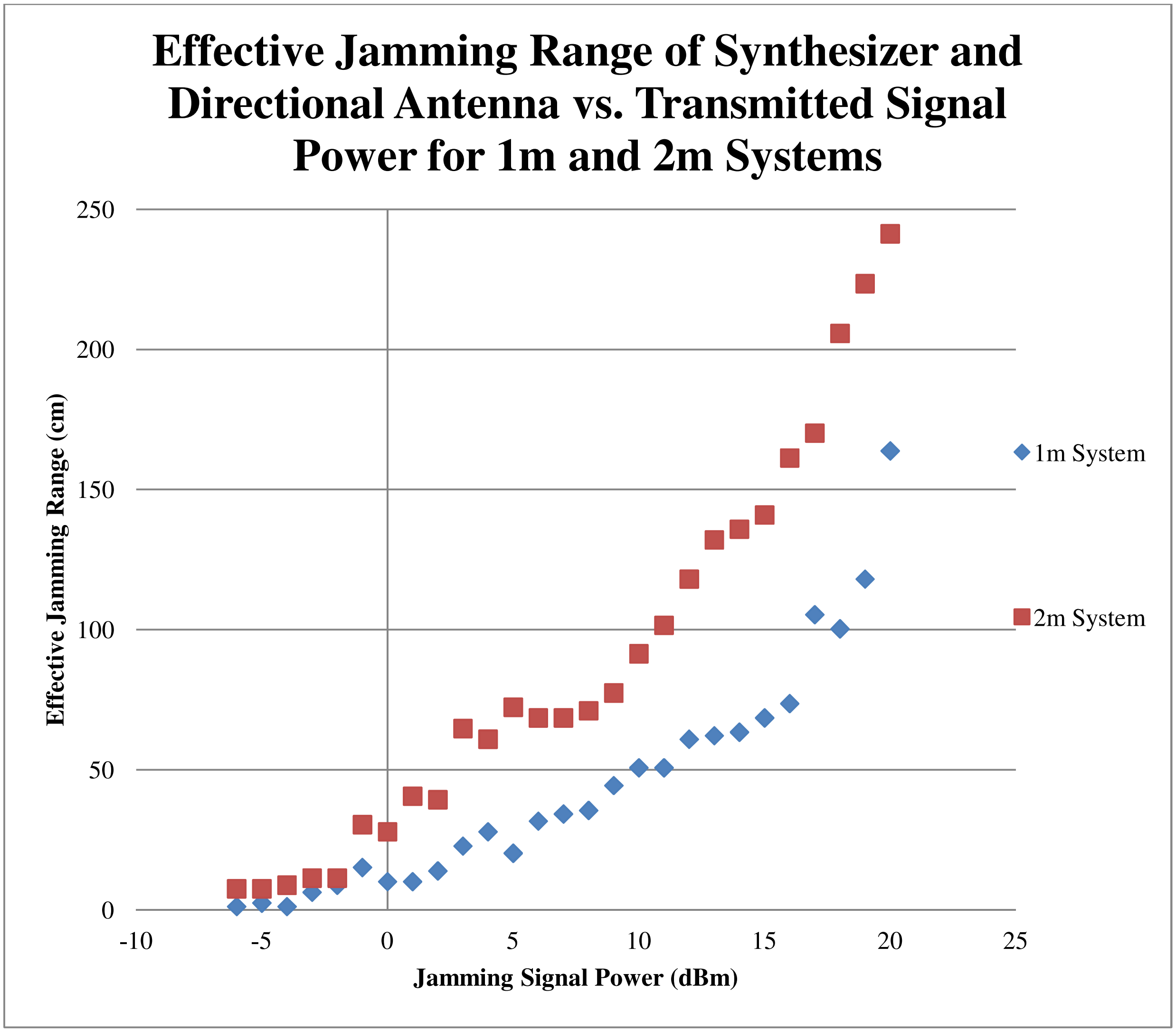
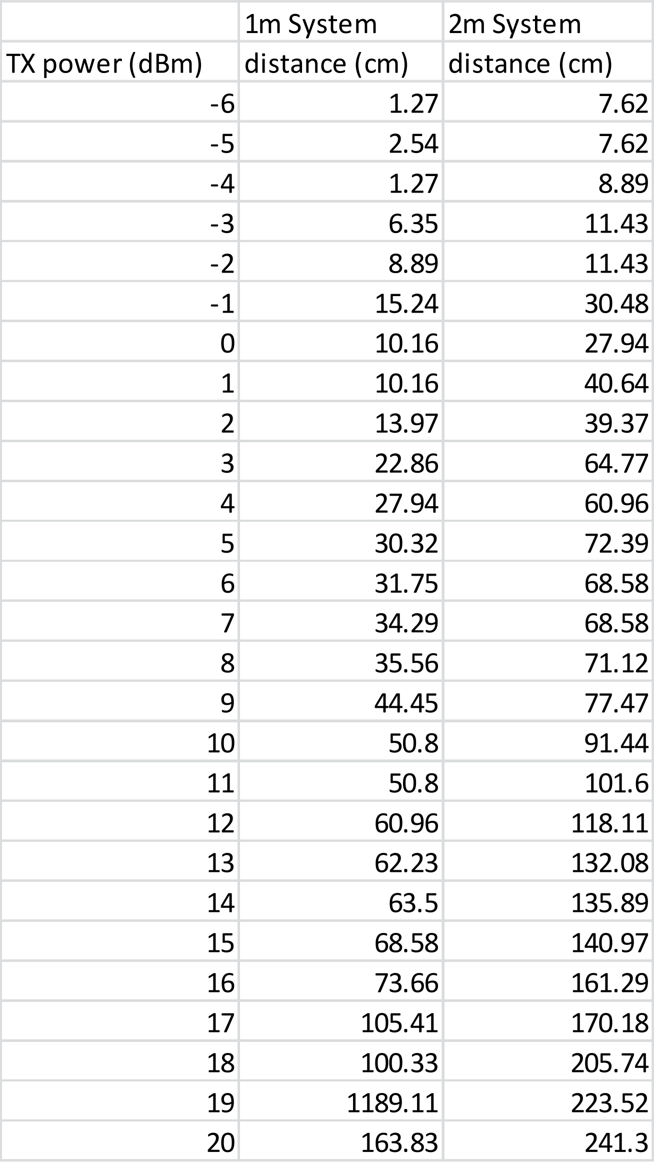


Figure 18: Comparison of effective jamming range vs. jamming signal power for both the 1m and 2m systems

The data is summarized in table 6 below:



	1m System	2m System
TX power (dBm)	distance (cm)	distance (cm)
-6	1.27	7.62
-5	2.54	7.62
-4	1.27	8.89
-3	6.35	11.43
-2	8.89	11.43
-1	15.24	30.48
0	10.16	27.94
1	10.16	40.64
2	13.97	39.37
3	22.86	64.77
4	27.94	60.96
5	30.32	72.39
6	31.75	68.58
7	34.29	68.58
8	35.56	71.12
9	44.45	77.47
10	50.8	91.44
11	50.8	101.6
12	60.96	118.11
13	62.23	132.08
14	63.5	135.89
15	68.58	140.97
16	73.66	161.29
17	105.41	170.18
18	100.33	205.74
19	1189.11	223.52
20	163.83	241.3

Table 6: Comparison of the effective jamming range vs. jamming signal power for both the 1m and 2m systems

Further Research

Given our findings, further groups can possibly continue working on the project by upgrading from a basic jamming system, to a system that can jam, and control a vehicle. This would prove to be a valuable system that could not only prevent enemies from endangering friendlies, but to even turn weapons against an enemy or even park/land vehicles in order to study enemy technologies.

Unfortunately as of yet there is no jammer that can jam and control an RC car or UAV. There is very little work being done in this field by America's military. America's military prime focus is to use jamming UAV's to effectively jam signals at far distances. Ideally the military targets enemy UAV launch and support facilities and destroys them before the UAV's or other vehicles are used against U.S. forces. The defense department does not focus on attempting to control the vehicles mainly because once remotely controlled UAVs are airborne, command uplink and status or data downlink may be detectable or jamable. Once the communication is jammed, the operator becomes blind and the UAV/vehicle will fly/run around until it crashes or the fuel/battery is gone.

A simple jammer cannot jam and control an RC car. The jammer only blocks the signal from the receiver to the transmitter. One would need another device that can send control signals to the receiver that can drive the motor. Some control signals are forward, reverse, forward and left, etc…This new device/RC transmitter would need a trigger that causes a pair of electrical contacts to touch, completing a circuit connected to a specific pin of an integrated circuit (IC). The completed circuit causes the transmitter to transmit a set sequence of electrical pulses. Each sequence contains a short group of synchronization pulses, followed by the pulse sequence. One may typically need a synchronization segment which alerts the receiver to incoming information.

The new transmitter would need a type of pulse modulation to send radio waves that oscillate at the same frequency as the vehicle, in our case a frequency of 2.4 GHz.

Conclusions

Based on our extensive experimentation, we can safely conclude how the RC car was being jammed by the camera transmitter it was carrying: the signal produced by the camera transmitter contained a large-enough frequency spur at the operating frequency of the RC car, 2.436GHz. This frequency spur can effectively be analyzed as a single-tone noise signal that overcame the critical SNR above which the RC car's communication system cannot function. This explains why the receiver shut down whenever the camera transmitter was set to channel 1, and sometimes when it was set to channels 2 and 3, since these channels contained frequency spurs between approximately 2.2 and 2.5GHz. The spectrum of channel 0 contained no such spurious frequencies. A possible continuation route for this experiment is to analyze and break down the modulation techniques used in the different channels of the camera transmitter to explain why channels 2 and 3 only jammed intermittently while channel 1 always jammed the car. Furthermore, the jamming range of the car was increased from less than one inch to beyond 20 meters. Because of power and space limitations, we were unable to increase this range; however, with less stringent power and space limitations, this range can be increased dramatically. This experiment was successful in both discovering the cause of the jamming as well as subsequently increasing the effective jamming range.

Bibliography/References

1. Poisel, Richard A. *Modern Communications Jamming Principles and Techniques*. Norwood, MA: Artech House, 2004. Print.

2. Hwang, Edward, and Karl Sanders. *Spread Spectrum Jamming*. Senior Project. California Polytechnic State University, 2012. San Luis Obispo, CA: Electrical Engineering Department, Cal Poly, 2012. Print.

3. Schwartz, Sorin."Frequency Hopping Versus Direct Spread Spectrum."*Sorin-Schwardz Seminars*.Web. 19 May 2012. <http://sorin-schwartz.com/white_papers/fhvsds.pdf>.

4. Cyprus CYRF6936 2.4GHz Radio System on Chip Datasheet

http://www.cypress.com/?docID=28606

Analysis of Senior Project

Project Title: Spread Spectrum Jamming – Part 2

Student's Names: Casey Burke, Christian, Hume, Javier Meza

Advisor's Name: Bill Ahlgren

Summary of Functional Requirements:

The spread spectrum jammer uses a camera transmitter to block incoming signals to a Traxxas RC car's 2.4 GHz radio which utilizes spread spectrum signals. The jammer has an operating range of less than 1 inch, meaning it has to be used right next to the car antenna to operate. The goal of this study is to investigate in depth into the effects of the jammer in addition to improving the jammer's range and performance capabilities.

Primary Constraints:

This project is not currently underway, but we anticipate the following major challenges along the way. First, all project members have no hands-on experience with the jammer yet. Also, we need to learn to use and integrate new hardware components into our study such as RF amplifiers and antennas which we have limited exposure to in both theory and practice.

Economic:

Some economic impacts of jamming technology fall on the defense budget of the U.S. and also the taxpayers who fund the U.S. government. Further studies and improvements in jamming technology allow the U.S. military to keep pace with the continuous improvements being made in communications and jamming technology of other nations. The jammer project is not necessarily driven for profiting purposes as much as it is defense. For our customer, Raytheon, and their customer, the U.S. government, the spread spectrum jammer is an investment for the future in order for the U.S. to maintain a military advantage over other nations.

If Manufactured on a Commercial Basis:

This project is sponsored by Raytheon and is intended for use in military and defense applications only. This is not a commercial product and therefore does not have commercial implications. Raytheon would be the sole designer and manufacturer for this jammer and the only customers would be the Department of Defense, along with possibly other governments and private defense firms.

Environmental:

The environmental impacts of the spread spectrum jammer are limited to inadvertently disruption communication links of other users in the EM spectrum. This potential disruption is because the jammer has jamming capabilities around 2.4 GHz, which is a commonplace frequency for other commercial products such as wireless routers and other RC vehicles. In a battlefield location for instance (possibly near a city or populated area), the jammer could also obstruct civilian phone and radio communications. With respect to other environmental concerns, the use of spread spectrum jamming of enemy vehicles and weapons can replace the current method of shooting them down, saving on the costs of missiles and bullets as well decreasing collateral damage to the surrounding environment from the explosions. This would also decrease harm done to animals in the area.

However, there are concerns with EM pollution and its effect on various species. Some have voiced their concerns of bees being affected by the widespread use of antennas and cell phone towers as their use has grown ubiquitous within our society. Therefore, the spread spectrum jammer may contribute to this damage done to wildlife including bees if that is the case. The jammer is meant to be used intermittently when the need arises and will not be running continuously like cell phone towers do, mitigating the possible risk.

Manufacturability:

There does not seem to be any major challenges associated with manufacturing of this product. Because our jammer is a commercially available camera transmitter, the resources and manufacturing technology are already in place to produce the product.

Sustainability:

The main challenges regarding the maintenance and upkeep of the spread spectrum jammer are the proper care of the electronics involved and protection from extreme weather and environmental conditions. Modularity will be taken into account when designing the project. Designing the jammer to be easily repairable and making the electronics accessible would enable the possibility repairs in order to limit the amount of growing electronic waste in the world. A modular design would also help in upgrading the jammer easily while limiting the risk of damage to the product.

Ethical:

The primary ethical implication of using a spread spectrum jammer is the obvious misuse of the product. When used improperly, jammers can be used to obstruct necessary communications in emergency situations, including radio and wireless phone transmissions.

Health and Safety:

There are no significant health and safety concerns associated with the design, manufacture, or use of the project.

Social and Political:

There are many social and political concerns with the issue of spread spectrum jamming, and specifically the use of the spread spectrum jammer in military applications. Anything designed for use in the battlefield raises significant concerns regarding civilian safety, relationship tensions between nations, and moral dilemmas about war and conflict in general. There is much opposition within this country and the world as a whole to U.S. military involvement in other countries, even when protecting the people of those countries from terrorist activities or oppressive regimes. However, the spread spectrum jammer, although intended for military use, is meant for defensive actions only. There is much less opposition to defending our citizens at home and our military personnel abroad. The spread spectrum jammer will be used to identify and shut down enemy vehicles and weapons, thereby protecting people from enemy attacks. Therefore, the intended use of the jammer has minor social and political opposition since most everyone can agree that safety and protection are a good thing. However, as mentioned previously, as with all things in this world, the jammer may be misused if left in the wrong hands. The jammer could be used to disrupt emergency communications or lead to a breach of public or private security. This raises the social opposition to such products when the misuse poses a threat to privacy and security. Because jammer directly impacts the U.S. military, the indirect impact falls on the people who live in the U.S. whose tax money funds such projects. The exchange for taxpayer money towards the military is that our military gains technological superiority over enemies, while our citizens benefit of having a safe country to live in.

Development:

This project is not yet underway, but we anticipate lots of development in both technical and project based skills as we complete our study and analysis. Among the technical skills we will develop are understanding the high frequency behavior of electronics, learning how new hardware pieces (e.g. frequency converters, RF amplifiers, antennas) function, learning to integrate the new hardware onto the existing jammer, and becoming more adept at using frequency test equipment. Among the project based skills we will learn are time and project management to ensure timely completion of deadlines, developing effective research skills, effective technical writing and research documentation, and allocation of specific tasks and work to group members based on individual skill sets and technical strengths.