Tri-band Mobile Jammer for 2G, 3G, and 4G Cellular Communications

Jarvas Wilderness

Ian McNicholas

Oscar Lopez

Academic Advisor: Khair Al Shamaileh

Departments of Engineering

College of Engineering, Mathematics, and Sciences

Purdue University Northwest

December 7, 2016

Executive Summary

A Tri-Band mobile jammer is designed to jam the 2G, 3G, and 4G cellular networks for four major cell phone carriers: Sprint®, Verizon®, AT&T®, and T-Mobile®. The jammer disrupts the signal between the cell phone and the serving base station by transmitting noise at the downlink frequencies of the above-mentioned networks such that the signal-to-noise ratio (SNR) falls below a predefined minimum threshold for acceptable functionality. This jammer is designed to block signals within a radius of 15 meters from the device.

The design, development, and validation of this device are carried out in three main phases: 1) the intermediate frequency (IF) design phase, which includes the theoretical design of a triangle wave and noise generators, a mixer/summer, clampers, and amplifiers; 2) the radio frequency (RF) design phase, which includes voltage control oscillators (VCOs), power amplifiers (PAs), and antennas; and 3) the power supply design phase which consists of transformers, rectifiers, filters, and regulators.

Upon the verification of the design phases, the overall circuitry is implemented on a designed and fabricated printed circuit board (PCB), and enclosed by a 3D printed case.

It is noteworthy to point out that this project is for educational purposes only as mobile jammers are illegal devices in the United States. As a result, this project, along with its schematics and hardware implementation, will not be advertised, sold, distributed, or otherwise marketed to consumers.

Abstract

The development of a Tri-Band Mobile Jammer is achieved by designing and implementing a jamming device that can disrupt cellular communications within a 15-meter radius from the device. The jammer impacts 2G GSM (Global System for Mobile), 3G W-CDMA (Wideband Code Division Multiple Access), and 4G LTE (Long-Term Evolution) cellular frequency bands used by Sprint®, T-Mobile®, AT&T®, and Verizon® cellular service providers.

The final device circuitry consists of three sections on the printed circuit board which are the IF, RF, and power. The IF section consists of a triangle wave generator that outputs is a 10 KHz triangle waveform with an amplitude of ±2 volts in combination with a noise generator that is sent through a series of amplification. These two signals from the noise generator and triangle wave are combined through a summer section of the circuit. The outputted signal from the summer is separated into two different signal paths. The first signal path is sent directly into the RF section of the circuit into voltage controlled oscillator 1. The second signal path is biased clamped then sent into voltage controlled oscillator 2. These two signals were designed to be sent into the RF power amplifier section of the circuit. Due to a manufacturing error in the printed circuit board, the two signal paths from the voltage controlled oscillators bypassed the power amplifiers and are sent into the SubMiniature version A (SMA) connectors to output the signal through the antennas. The power section of the device used a twelve-volt wall supply that is combined with a voltage line regulator in the circuit to provide the different voltages.

The completed device successfully transmits noise signals over the downlink frequencies of the above mentioned providers to create interference and cancel out the signal received by the cell phones.

This report illustrates a detailed explanation of the key points and strategies used to design and build this device. The report highlights the achievements and progress made during construction of the Jammer.

Table of Contents

List of Figures

List of Tables

Introduction

Electronic jamming systems play a key role in neutralizing. Military and law enforcement originally developed devices to jam or disrupt cell phone signals to stop communications by terrorists and criminals. Cell phones are used to trigger explosives such as IED's (improvised explosive devices) used against military in Iraq. Law enforcement can use these devices in hostage situations and raids to stop suspects from communicating outside the area. "The bombs that blew up commuter trains in Spain in March 2004, as well as blasts in Bali in October 2002 and Jakarta in August 2003, all relied on cell phones to trigger explosives" [1:17]. On President Obama's first Inauguration Day, federal authorities were authorized to jam signals at some locations in downtown Washington, according to current and former federal official [2:17].

Cell phone jamming devices can also find applications in controlling signal transmissions in chemical storage facilities where radio transmissions can be dangerous. Corporations use jammers to stop espionage by blocking voice and photo transmission to protect valuable data. Furthermore, cell phone jammers may also be useful in areas where cell phone use is unwanted, such as court rooms, conference rooms, class rooms, and libraries.

Background

The following list of classes prepared the team to have the necessary tools to be able to research and design this project.

Table 1. List of ECE courses referred to throughout the progress of this project.

Electrical and Computer Engineering Courses	
1. Linear Circuits Analysis I	2. Linear Circuits Analysis II
3. Analog and Digital Electronics	4. Signals and Systems
5. Electronic – Systems	6. Digital Signal Processing
7. Introduction to Communication Systems	

The theory of mobile communications was explored throughout this project. Utilized formulas, including the signal to jamming ratios and free space loss, have been used as a foundation to our designs. Moreover, the team valued the Communications Engineering course entitled "ECE448: Introduction to Communication Systems" that had the direct correlation to the theories of the design approach.

Objectives

The goal of this project was to research, design, construct, and test a cellular jammer that will disrupt all cellular communications of the 2G GSM, 3G W-CDMA, and 4G LTE frequency bands of Sprint®, T-Mobile®, AT&T®, and Verizon® cellular providers.

Constraints

This project is limited to only jamming cellular frequencies with no other frequencies beyond that range (e.g., Wi-Fi, Bluetooth, AM radio, GPS).

This senior design group was granted an amount of $100 from the ECE department and a Research Grant of the amount of $247.72 for the purchase of the components needed to fulfil this project. Some of the costlier components and fabrication costs are listed below in table 2. A full budget list can be referred to in appendix E.

Table 2. Costlier Components and Fabrication.

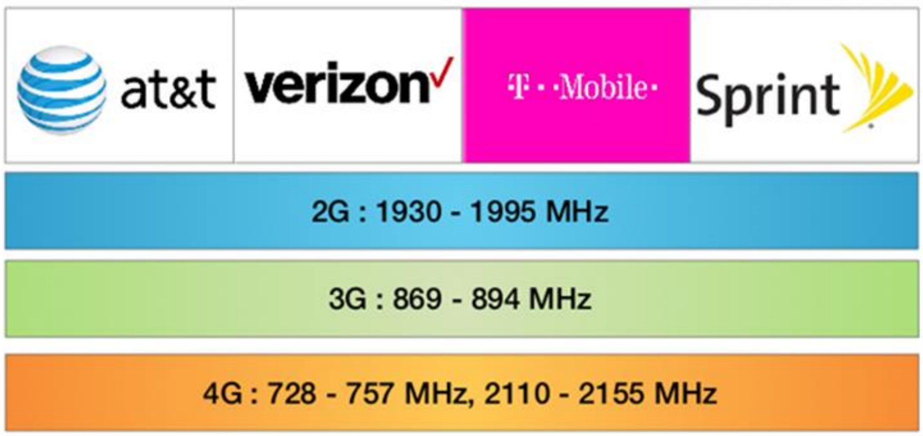
Component	Description	Price (in USD)
VCO CVCO55BE-1550-2500	Voltage Controlled Oscillator 1 (QTY-2)	$25.96
VCO CVCO55BE-0400-0800	Voltage Controlled Oscillator 2 (QTY-2)	$25.96
WTR7270|LTE/4G Multiband Multiposition	Antenna (QTY-2)	$6.75
TQP9309|High Efficiency 0.5W Small Cell	Power Amplifier	$11.88
TQP9321|High Efficiency 0.5W Small Cell	Power Amplifier	$11.88
12V Wall Adapter	Power Supply	$26.99
Printed Circuit Board	PCB Fabrication	$79.99
3D Printer Filament	3D Printed Case	$29.99

Legal constraints of this project prohibit the operation of cellular jamming equipment. As a result, the device cannot be tested in public domains. The device can only be tested within a pre-determined area of the campus. This device will only be used for educational purposes and will not be marketed, sold, or advertised.

Approach

The first step in designing the jamming device is determining the frequency range of the networks. Table 3 showcases the frequency range determined from research.

Table 3. Cellular Network Downlink Frequencies.



at&t	verizon	T-Mobile	Sprint
2G : 1930 - 1995 MHz			
3G : 869 - 894 MHz			
4G : 728 - 757 MHz, 2110 - 2155 MHz			

Next, the parameters of the DOS (Denial of Service) jamming technique for the distance to be jammed, D, are considered. To determine such parameters, the following equations/constraints need to be established:

- Jamming–to-signal ratio {J/S}.
- Free space (Path Loss) {F}.
- Power calculations and considerations

Jammer to signal ratio

Jamming is achieved by transmitting an electromagnetic wave in order to disrupt communication at a targeted receiver. Figure 1 shows that the base station is communicating with the cell phone. The goal of the jammer is to transmit a noise signal at the targeted cell phone using the same carrier frequency as the signal being transmitted from the base station. Jamming signal power needs to be strong enough to cancel out the base station signal in order for the jammer to be effective.

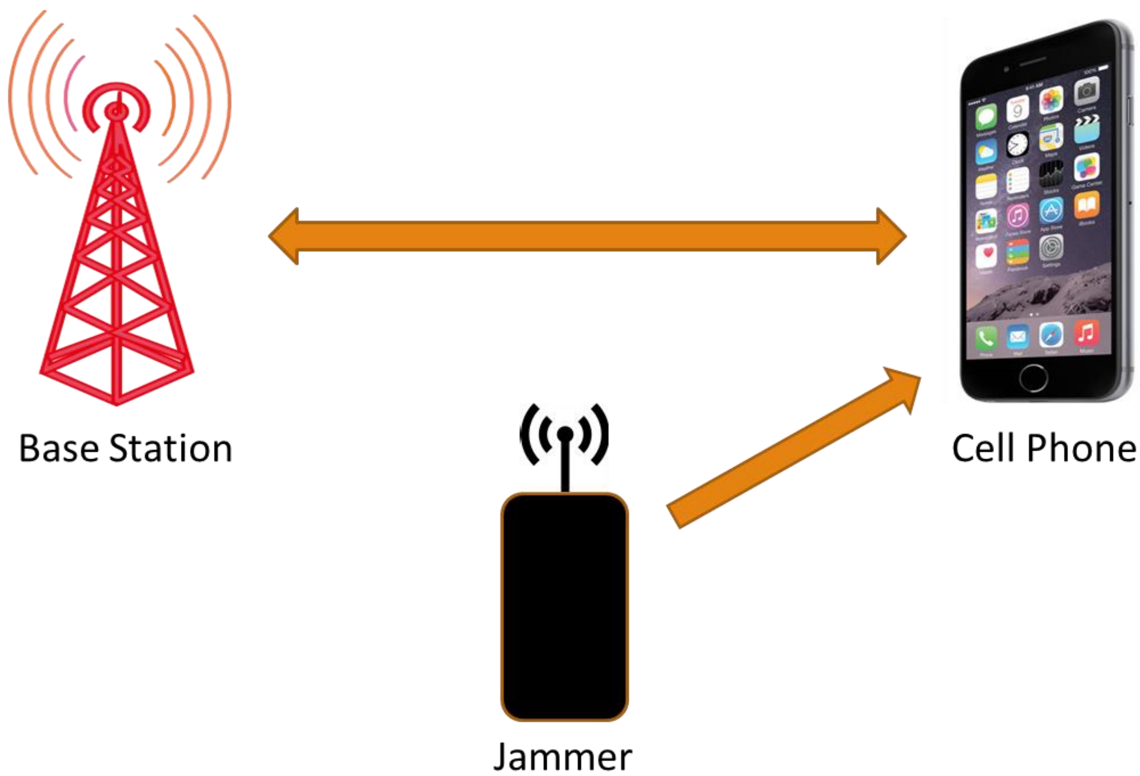


Figure 1. (DOS) Jamming Theory.

Below is the Jammer to Signal Ratio formula.

$$\frac{J}{S} = \frac{P_j G_{jr} G_{jr}^2 R_{tr} L_r B_r}{P_t G_{tr} G_{tr}^2 R_{jr} L_j B_j}$$

P_j= jammer power
P_t = transmitter power
G_{jr} = antenna gain from jammer to receiver
G_{rj} = antenna gain from receiver to Jammer
G_{tr} = antenna gain from transmitter to receiver
G_{rt} = antenna gain from receiver to transmitter
B_r = communications receiver bandwidth
B_j = jamming transmitter bandwidth
R_{tr} = range between communications transmitter and receiver
R_{jt} = range between jammer and communications receiver
L_j = jammer signal loss (including polarization mismatch)
L_r = communication signal loss

The analysis of the above equation reveals the effect of distance between the jammer and the receiver. For example, Doubling the distance between the jammer and the receiver will require a quadrupling the output from the jammer to maintain the same effect. In the designed device, it is assumed that the SNR is 6 dB; while the maximum transmitted signal power is -15dBm. These values are used to represent the worst case (from the jammer perspective) and the best case (from receiving mobile perspective) scenarios.

Free space loss

In this project the free space (Path Loss) model is used. This model assumes a line of sight environment between the transmitter and the receiver. All absorbing and reflective surfaces such as trees and buildings are ignored if this model is adopted. The free space model in dB is given as:

$$Freespace_{PL}(dB) = 20\log_{10}(d) + 20\log_{10}(f) + 32.44$$

{*d*} = distance in kilometers

{*f*} = frequency in megahertz

To calculate the maximum free space loss, the highest targeted frequency was used for {*f*} as well as a distance of 15 meters for {*d*}. The result was 62.6 dB.

$$Freespace_{PL}(dB) = 20\log_{10}(0.015) + 20\log_{10}(2155) + 32.44 = 62.6\ dB$$

Power Calculation

In order to find the jamming power, we must first find the amount of power at the mobile receiver. This is represented below by "*J*". S_{max} equals to -15 dBm (equivalent to -45 dB) and SNR is set to 6dB.

$$J = \frac{S_{max}}{SNR} = \frac{-45dB}{6dB} = \frac{10^{-4.5}}{10^{0.6}} = -21dBm$$

The total output is a combination of free space loss and *J*.

$$Output\ Power = \ -21\ dBm + 62.6\ dB = 42\ dBm$$

The cellular jammer was designed and constructed in three phases: power supply, IF-phase, and RF-phase. Figure 2 shows a simplified block diagram of the proposed design.

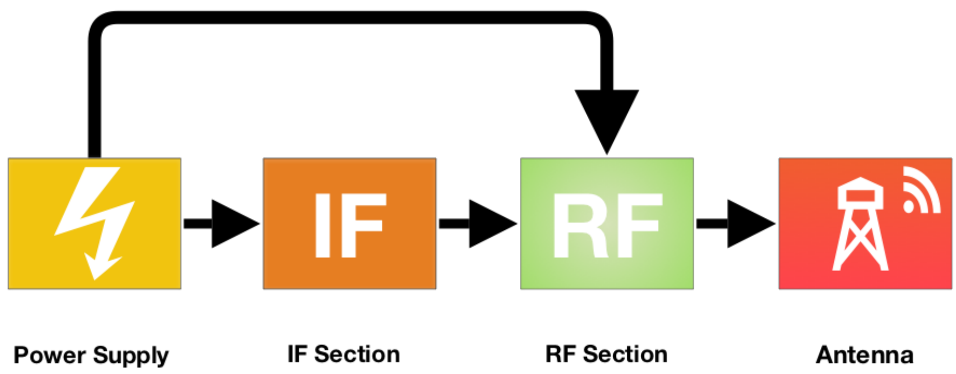


Figure 2. Jammer section breakdown.

Power Supply

The power supply will provide both IF- and RF-Sections with the required voltages. The power supply essentially consists of four parts as described below.

1. Transformer – Transforms AC voltages to DC voltages needed to supply components.
2. Full-Wave Rectification - Obtains negative and positive output voltages from both positive and negative cycles of input AC voltage.
3. DC Blocking Capacitors – Eliminate the fluctuations in the output of the full-wave rectifier so a steady DC voltage is provided.
4. Regulators – Provide the desired DC voltages to other components.

IF-Section

In the IF-Section, both noise and triangular waveforms which are used to sweep the VCOs output frequencies will be generated. Intermediate processing including mixing noise with the rectangular sweep as well as amplifying noise will take place. The IF-Section consists of five main parts:

1. Triangle wave generator – tunes the VCOs that are used in the RF-Section.
2. Noise generator – provides the noise signal.
3. Mixer/Summer – mixes the triangle and noise signals together.
4. Clampers – bound the output signal from the mixer/summer within the specific voltages needed for the VCO's to operate.
5. Amplifiers – provide a suitable gain to the sweep signals.

RF-Section

The RF-Section will receive input signals from the IF-Section and transmit the high power noise at the specified frequencies to complete a denial of service attack on the receiver. The RF-Section consists of six basic components:

1. Two VCO's – generate radio signals at frequencies similar to those of the downlink ones. The triangle wave generated in the IF-Section will vary the input voltage of the VCO to span

each frequency band for each Technology (2G, 3G, and 4G) used by the specific cellular providers.

2. Two power amplifiers – the output power each VCO provides is not enough for jamming, so RF power amplifiers will be needed to amplify the output power just before the antennas interface.
3. Two Antennas – transmit the jamming signal to cancel out cellular communication within a 20-meter radius.

Results

The design of the Tri-Band Mobile Jammer was split into 3 major parts:

1. Power Section
2. IF Section
3. RF Section

Power Supply Section

A 12-volt wall adapter was chosen to power this device due to its availability and ability to reduce the size of the device. The wall adapter only provides a positive 12 volts to the circuit. The circuit design requires 5 volts as well. Research conducted showed that there are two options for addressing this issue: 1) using a DC to DC converter. The DC to DC convertor was a viable option except for the RFI (radio frequency interference) emitted from high frequency switching. The design of our device is based on transmitting specific frequencies, and radio frequency interference is not acceptable. This lead us to the second option, which is 2) using a voltage line regulator, this method worked well with only one concern: the voltage line regulator produces more heat than the DC to DC convertor. As such, the design of the voltage line regulator was implemented on a bread board. Testing was done to measure the heat output from the circuit figures 3 and 4 show the circuit design and output measurements. Table 4 below shows that after two hours of continuous operation, the heat output from the circuit remained within a range that was acceptable for the design.

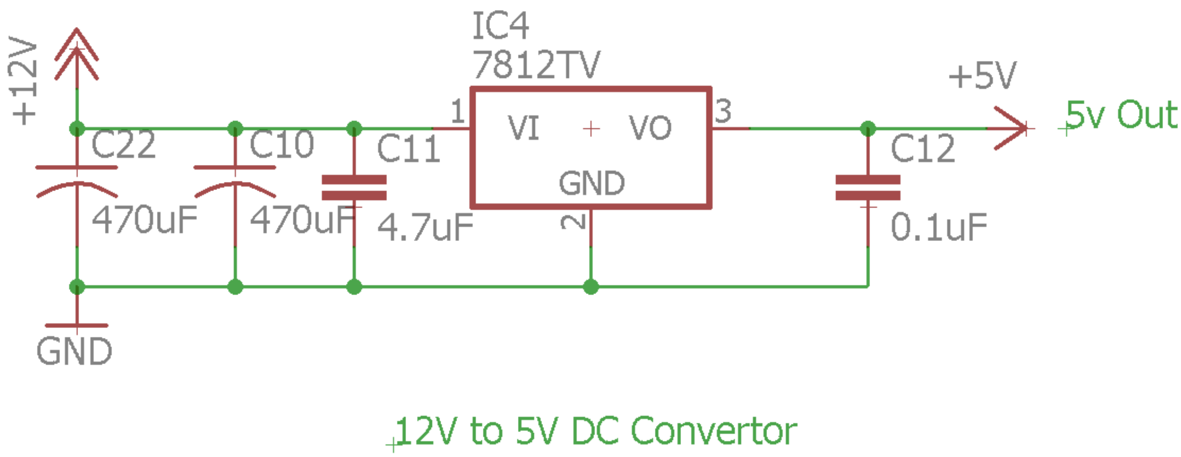


Figure 3. Voltage Line Regulator.

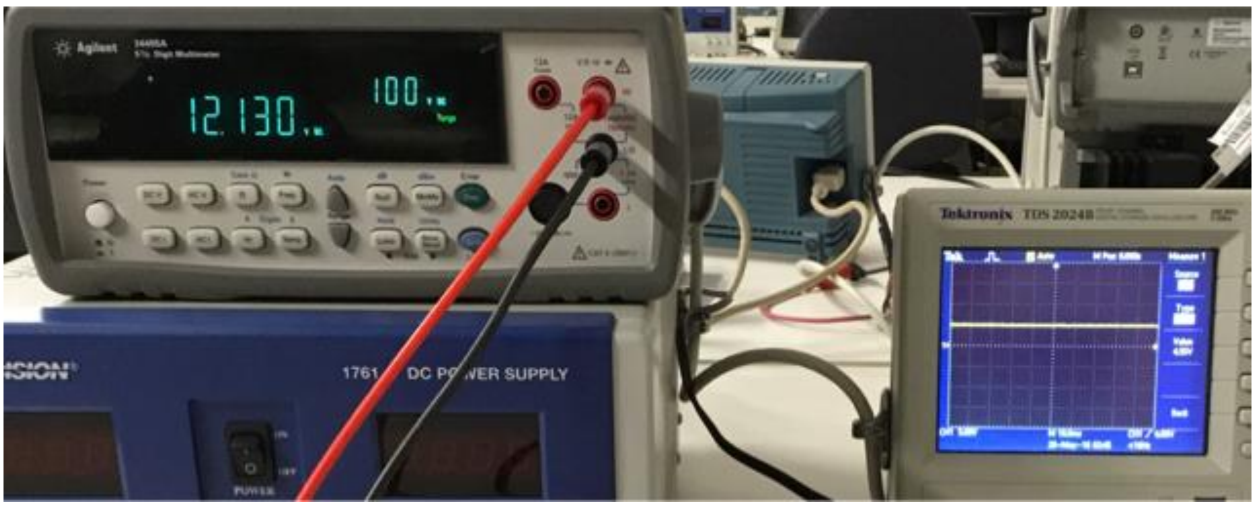


Figure 4. Voltage Output Measurement.

Table 4. Heat Output Test of Power Supply.

Hours	Front (F)	Back (F)
.5	76	76
1	75.6	75.8
1.5	75.4	75.8
2	75.3	75.8

IF Section

This section was divided up into four major parts as described below:

1. Triangle Wave Generator
2. Noise Generator
3. Summer
4. Input to VCOs

Triangle Wave Generator

The purpose of the triangle wave generator is to provide a varying voltage output, which in turn will be used by the VCOs to generate corresponding frequencies. The oscillating frequencies of the VCOs cover the targeted ranges of the 2G, 3G, and 4G networks. A 555 Timer IC (integrated circuit) chip was incorporated in the A-stable mode using resistors and capacitors with pre-calculated values.

As shown in Figure 5, the input of 12V highlighted in red is sent into pin 8 of the 555-Timer. This voltage is divided by the three internal resistances of the 555-Timer resulting in 8V highlighted in yellow, 4V highlighted in blue. The first comparator in the upper left corner monitors the output voltage displayed in green and the internal charge of 4V. This comparator sets the lower limit of the output triangle wave. The lower right comparator sets the upper limit of the triangle wave by comparing the output voltage against 8V. The output of the circuit has a direct relationship of the charging and discharging of the capacitors. When the circuit is initially powered on the capacitors will charge from 0V to 8V.

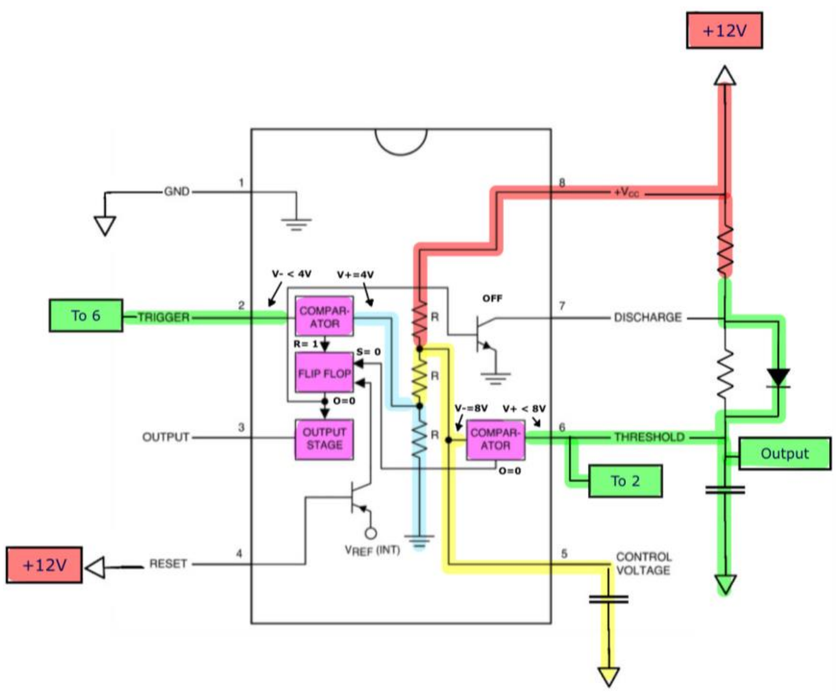


Figure 5. 555-Timer charging of Capacitors.

In Figure 6, at 8V, the upper limit comparator sends a signal of 1 to the flip-flop. Combining the signal of 1 and the lower limit comparator signal of 0 will in turn cause the flip-flop to trigger the BJT (Bipolar Junction Transistor) and discharge the circuit by connecting it to ground. As the voltage drops to a level of 4V the lower limit comparator outputs a signal of 1, this combined with the output signal of 0 from the upper limit will deactivate the BJT and allow the capacitors to charge again.

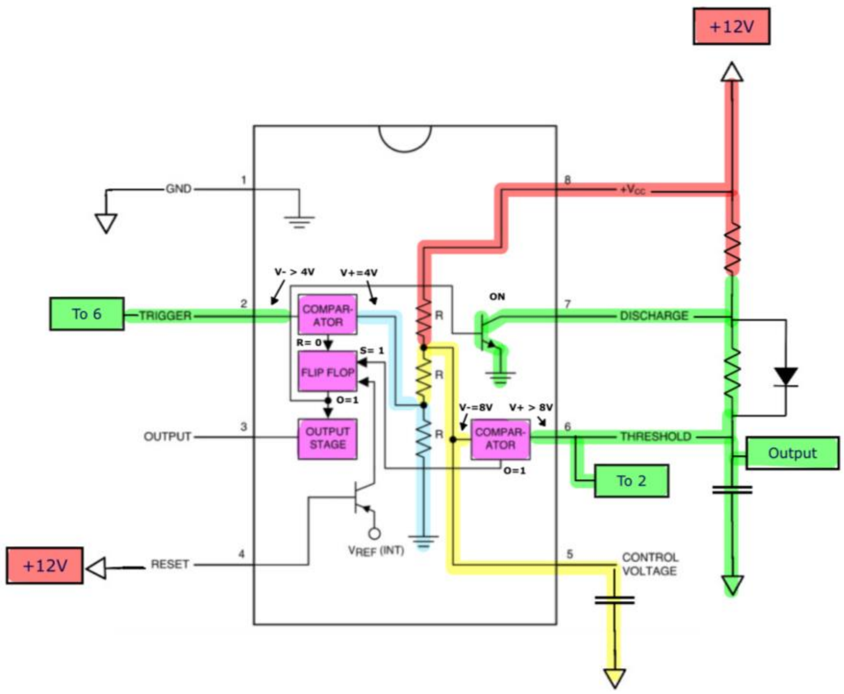


Figure 6. 555-Timer discharging of Capacitors.

The result of this is the obtained output is a 10KHz triangle waveform with an amplitude of ±2 volts varying from 4V to 8V (Fig. 7). Figures 8 and 9 showcase the design of the circuit.

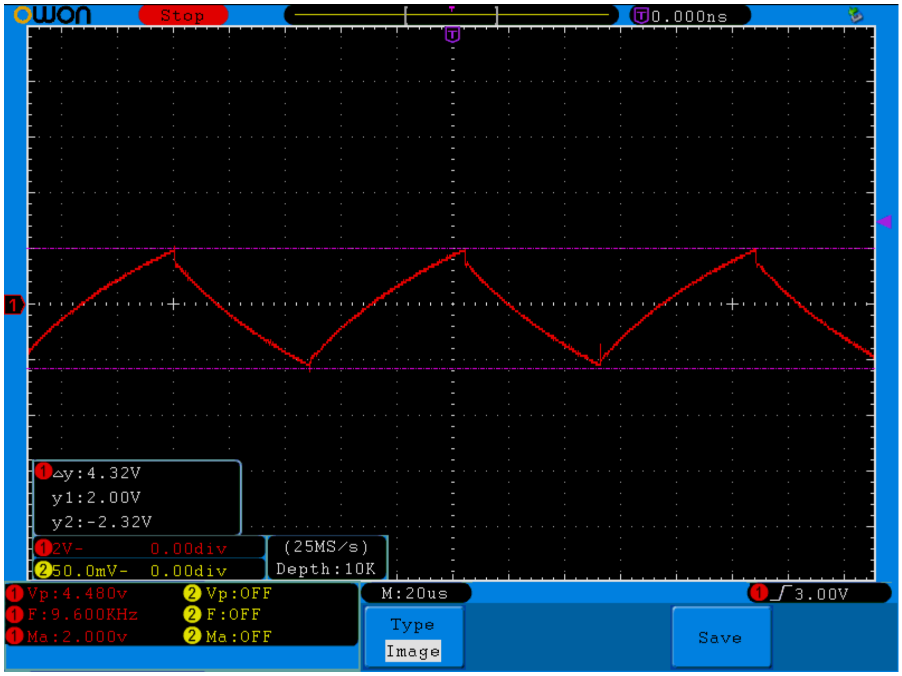


Figure 7. Triangle Wave Generator Output (result is measured after the DC blocking capacitor).

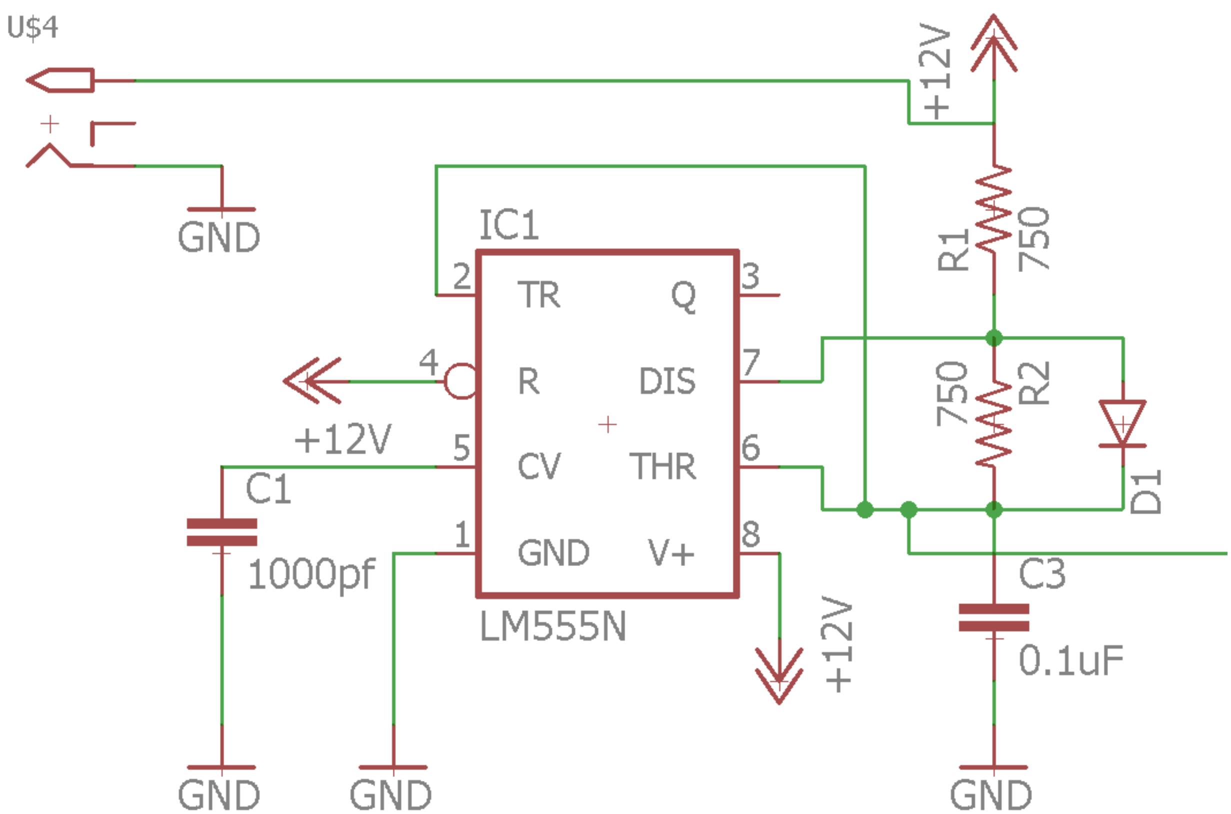


Figure 8. Triangle Wave Generator Schematics.

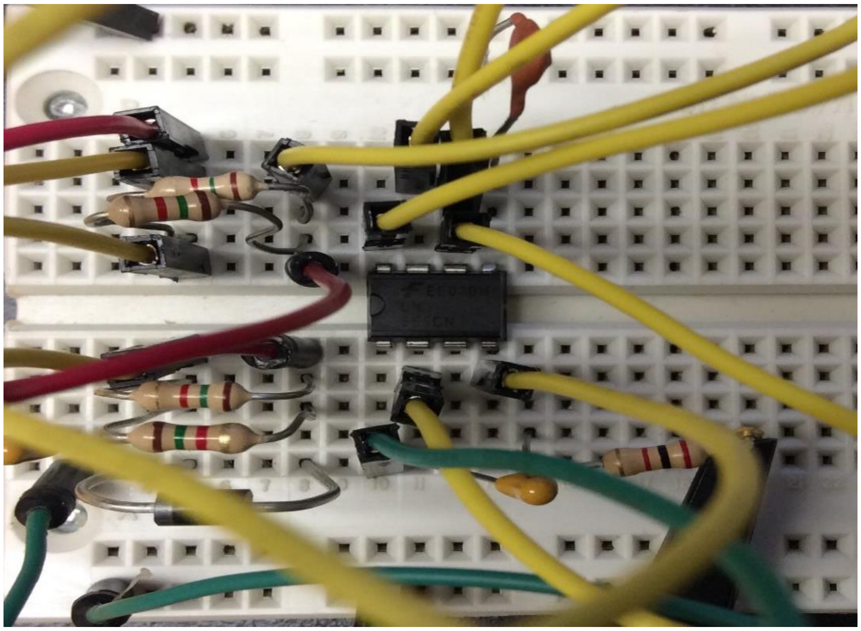


Figure 9. Triangle Wave Generator on bread board.

The output from the triangle wave generator was then sent into the amplifier to achieve a gain of 1.74 (Fig. 10).

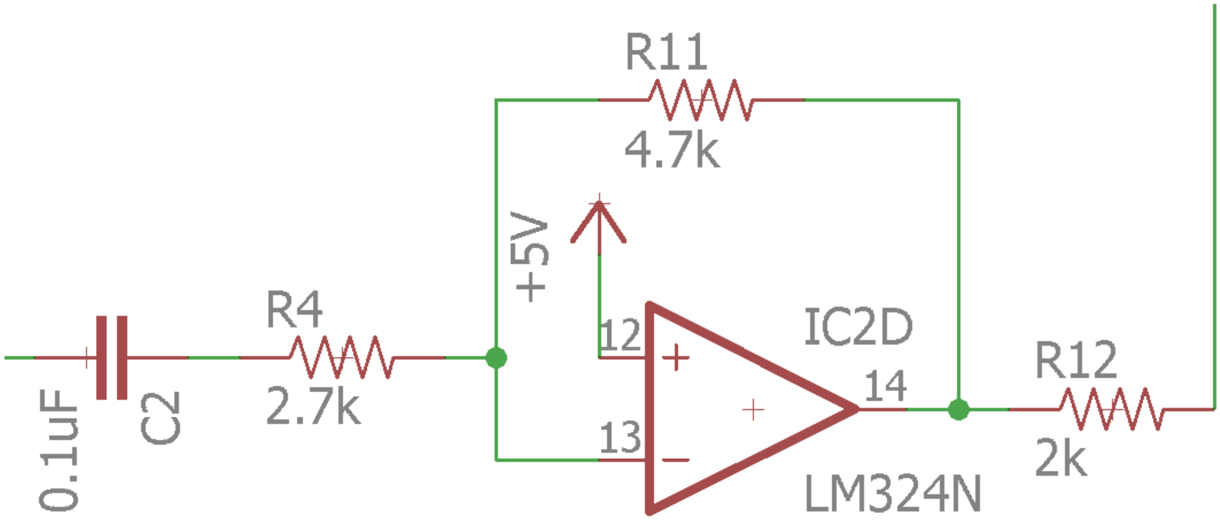


Figure 10. Triangle Wave Amplifier.

Noise Generator

The purpose of the noise generator is to create the interference that dominates the transmission between the serving base station and cell phone. Without noise, the output signal from the VCO would be an un-modulated oscillating voltage signal. In order to generate such a noise, a set-up of a reverse biased 5V Zener diode along with a 12V DC voltage was used to achieve an avalanche effect characterized by a wideband noise. Then, this signal is amplified using a two-stage amplifier created from a combination of a BJT and LM386 audio amplifier. Figures 11, 12, and 13 showcase the design of the circuit and the resulting output signal.

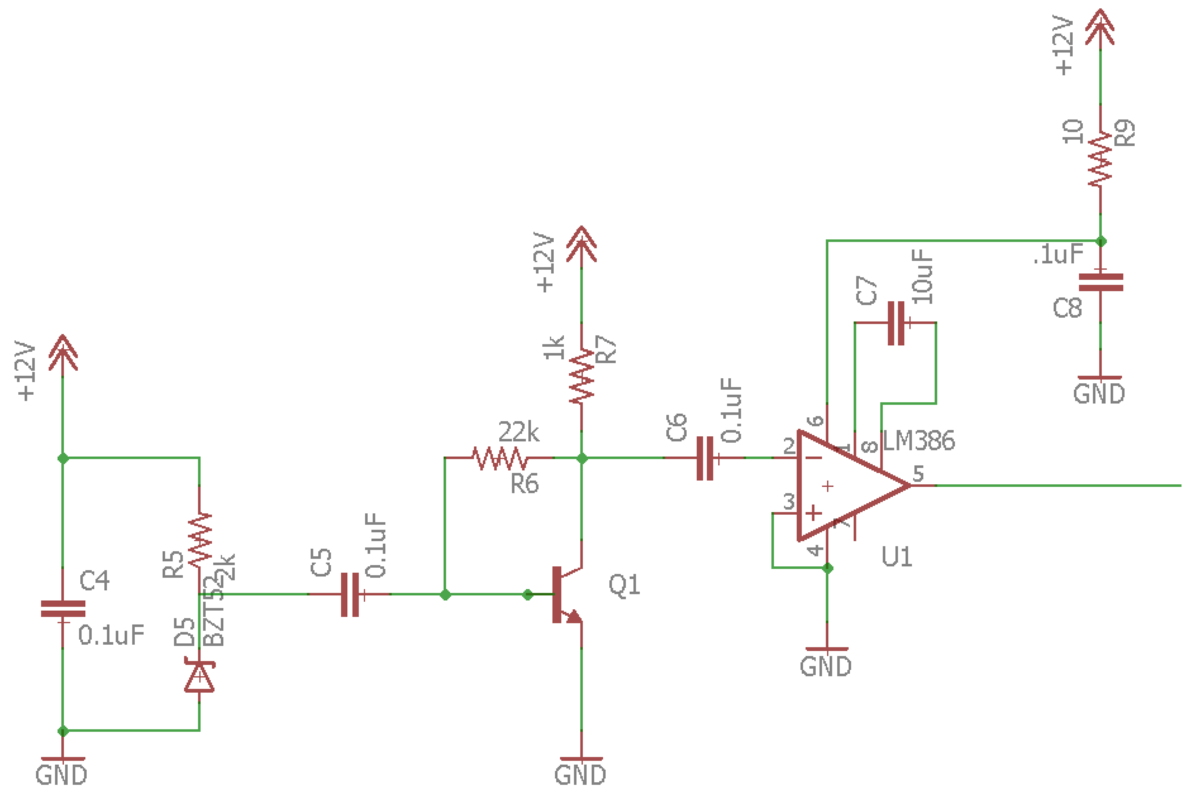


Figure 11. Noise Generator schematic.

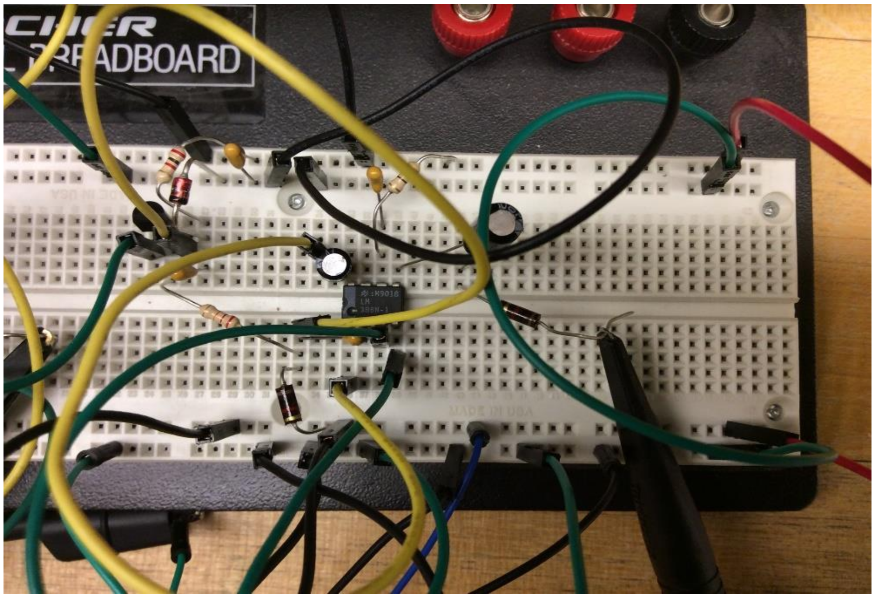


Figure 12. Picture of noise generator.

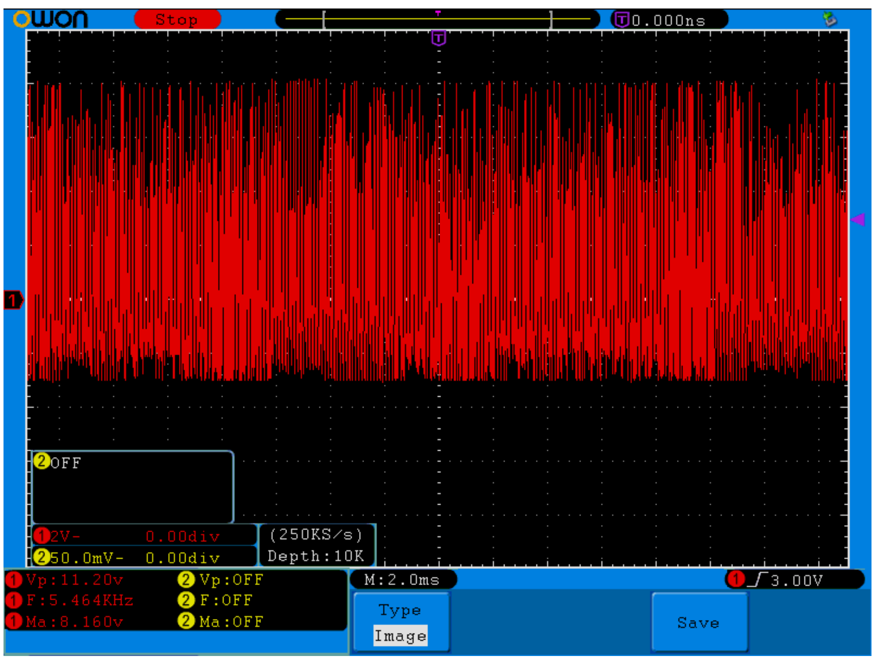


Figure 13. Picture of noise generator output.

Summer

The purpose of the summer is to combine the outputs of both the triangle wave generator and noise generator. This design was achieved by using one of the op amps in the LM324N operational amplifier. Adding a 2K ohm resistor to the triangle wave generator input and a 1k ohm resistor to the noise generator input resulted in a signal to noise ratio of 2 to 1. Figures 14 and 15 showcase the circuit design and the resulting output from the summer.

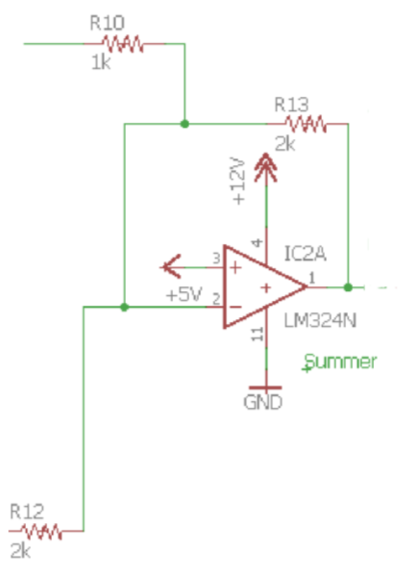


Figure 14. Schematic of summer.

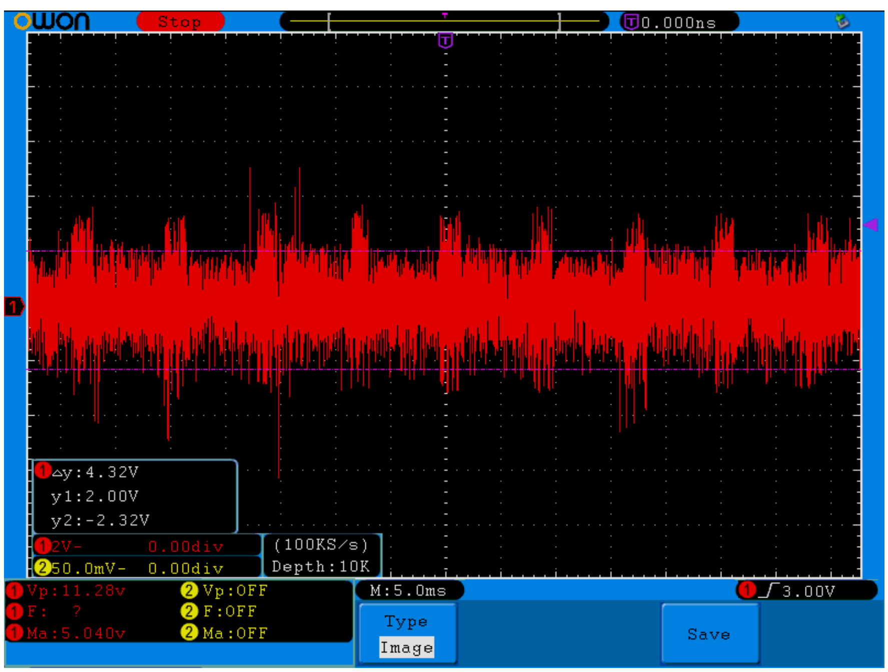


Figure 15. Picture of combined signal.

Input to VCOs

The output signal from the summer has to be modified before it is fed into the VCO2 (Fig. 16). This signal must match the tuning voltages for the VCO2 in order to achieve the desired oscillating frequencies.

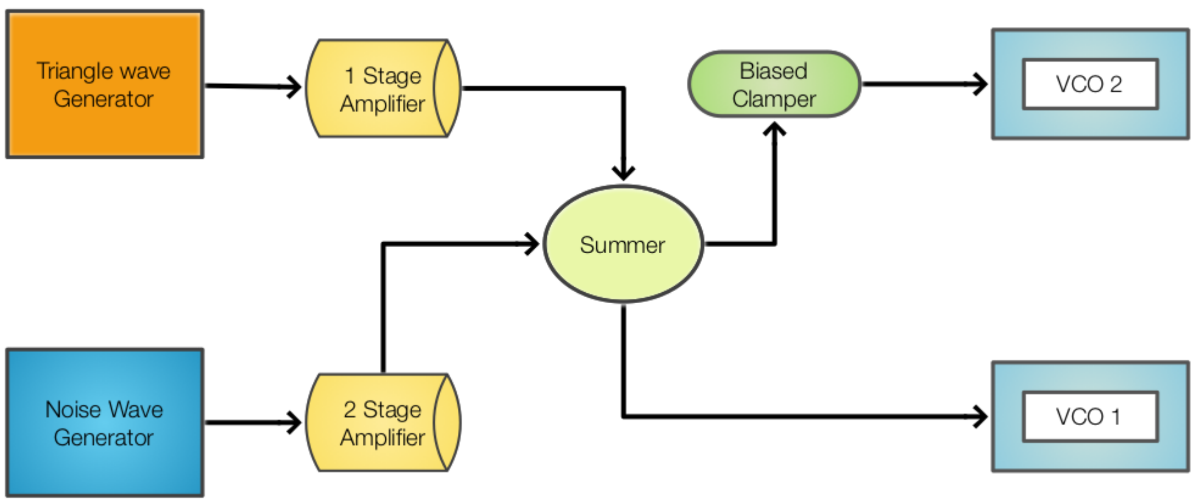


Figure 16. IF-section Flowchart.

VCO2 covers the frequencies ranging from 580 to 920. This signal was sent into a bias clamper circuit using 5V DC which acts as a DC offset to give the resulting signal that sweeps between the range of 3.4V to 12.2V (Figs. 17 and 18).

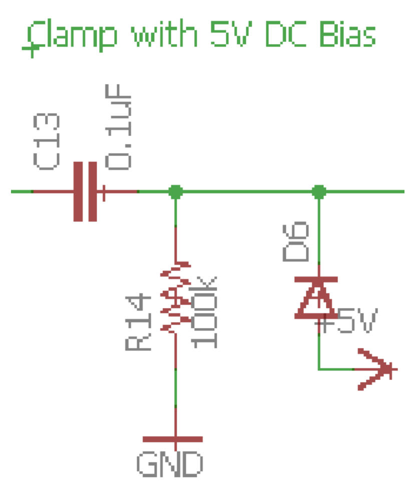


Figure 17. Biased Clamper Schematic.

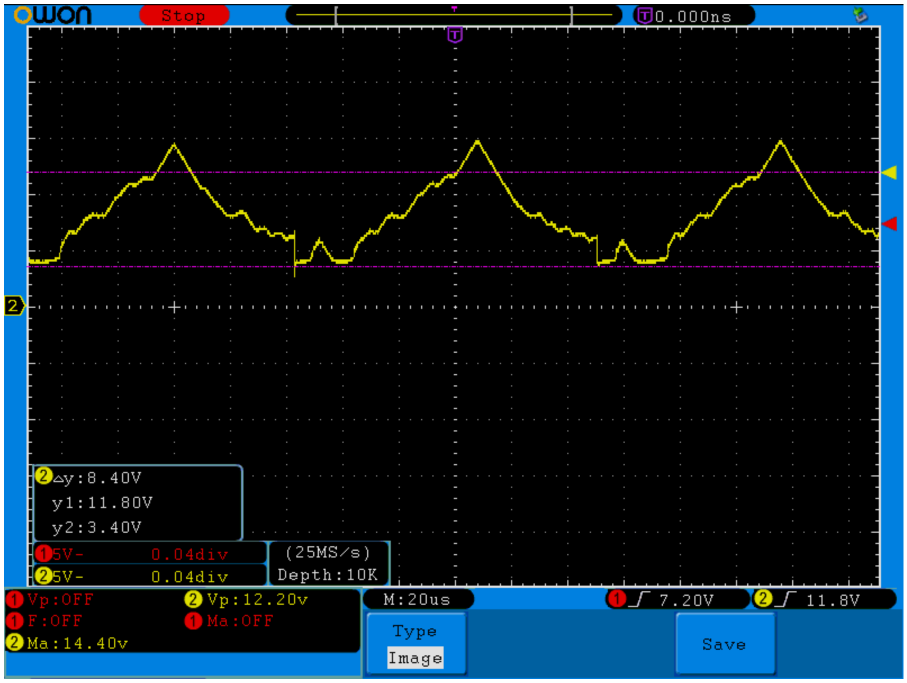


Figure 18. Input signal to VCO2.

VCO1 covers the frequencies ranging from 1930 to 2155. This requires a voltages signal from 3V to 6V according to the VCO data sheet. In order to obtain the desired frequencies, the output signal of the triangle wave amplifier was fed into VCO1 (Fig. 19).

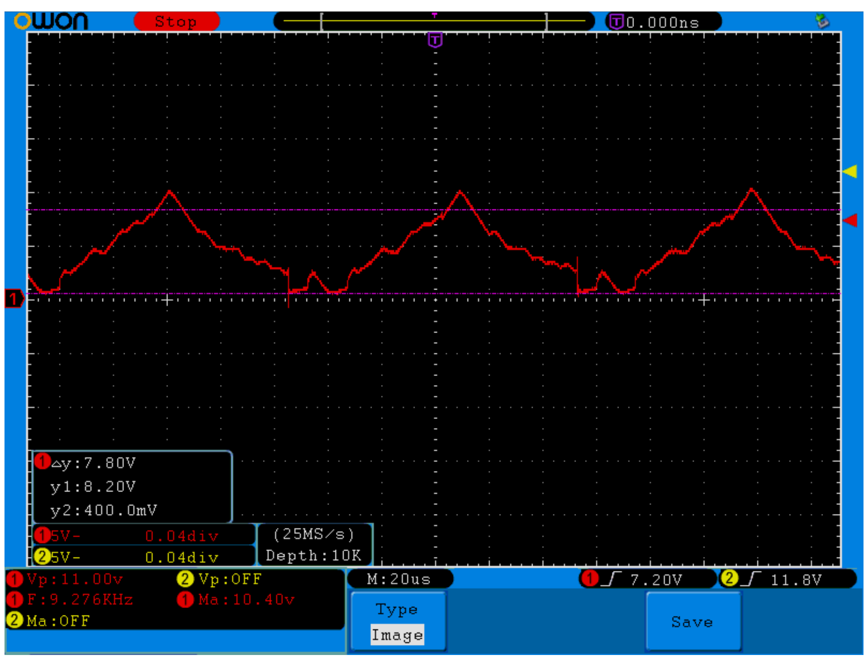


Figure 19. Input signal to VCO1.

RF-Section

For the RF-Section the following list of components where chosen to cover the range of frequencies needed to output the generated frequency signal:

1. VCO1: Voltage Controlled Oscillator-VCO CVCO55BE-0400-0800
2. VCO2: Voltage Controlled Oscillator-VCO CVCO55BE-1550-2500
3. Antennas: WTR7270|LTE/4G Multiband Multiposition Antenna
4. Power Amplifier for VCO1: TQP9309|High Efficiency 0.5W Small Cell Power Amplifier
5. Power Amplifier for VCO2: TQP9321|High Efficiency 0.5W Small Cell Power Amplifier

The components chosen for the RF-section can be referred to in Appendix C.

Figure 20 shows a circuit of the completed IF- and RF-Section components

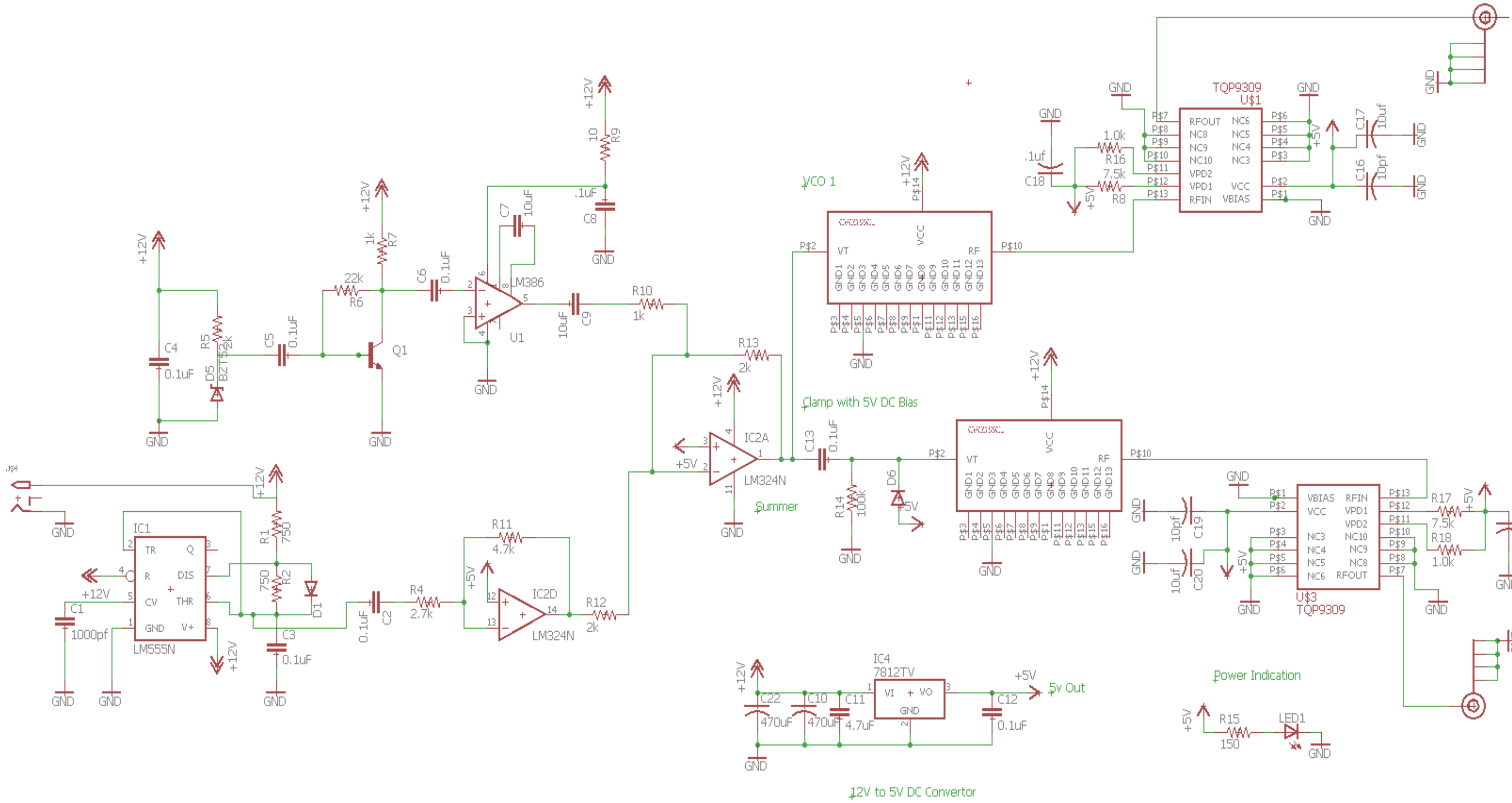


Figure 20. IF-section and RF-section circuit Schematic.

PCB Design

The designed circuit was built and tested on a bread board leading up to the VCO portion of the design. Each VCO component has a 16-pin layout that requires surface mounting and could not be built on the bread board. In order to test the VCOs for functionality, the design of break out boards was performed. . Research was conducted over the summer semester to find the right software to design the required breakout boards and to fabricate them after they were designed. The chosen software program was PCB Eagle®, this program is free as long as the design layout is smaller than 100mm by 80mm.

The initial technique adopted for fabricating the breakout boards was chemical etching, by printing out the circuit layout on the laminate, then transferring the print to the board. After transferring the layout from the laminate to the board, the board was exposed to a mixture of acids to remove the areas of copper around the traces. The following two images to the left show that the process was not as accurate as needed (Fig. 21). Hence, the design team chose to order the printed circuit boards. The design was out-sourced to Oshpark® for fabrication, and the image on the far right shows the fabricated board.

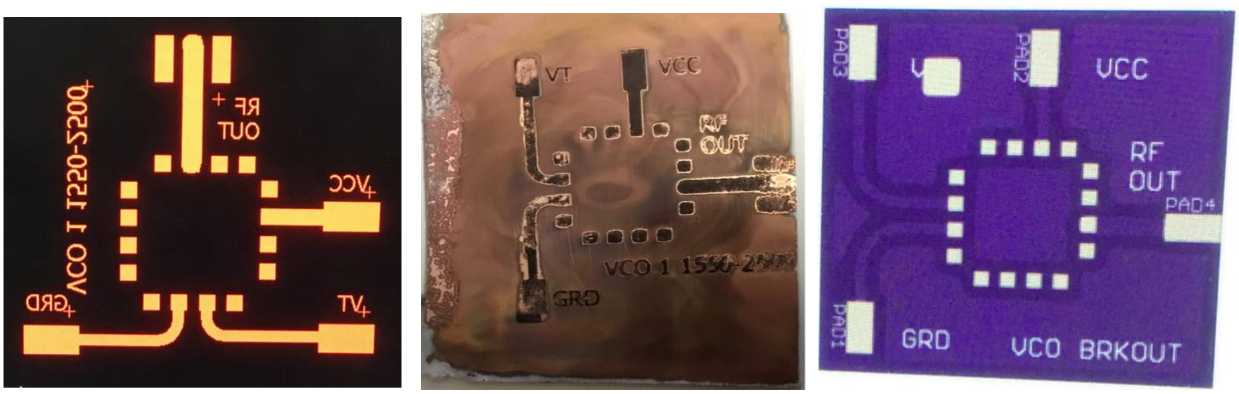


Figure 21. VCO Fabricated Breakout Boards.

In corporation with the head lab technician in the ECE department, the VCOs were soldered on the breakout boards. Figure 22 shows the jammer prototype after installing the VCOs. The completion of the breakout boards allowed the VCOs to be connected to the rest of the circuit.

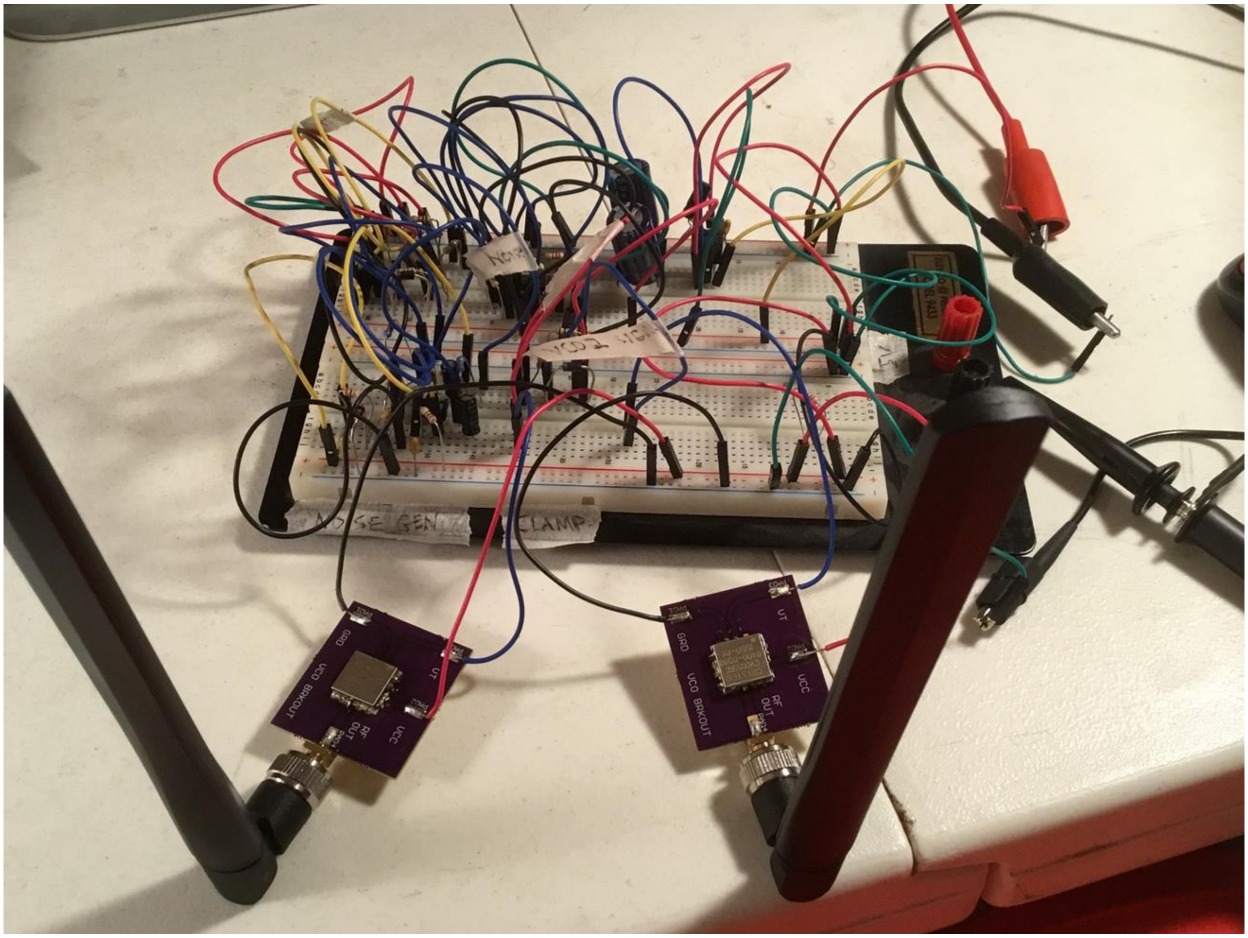


Figure 22. Bread Board Circuit Connected to VCOs.

A test was done on two different cell phones with different carriers in close proximity to the implemented prototype. Referring to Figures 23 and 24, It was proved experimentally that when the built circuit is powered on (the RF power amplifiers), it does indeed jam the cellular networks of the carriers.

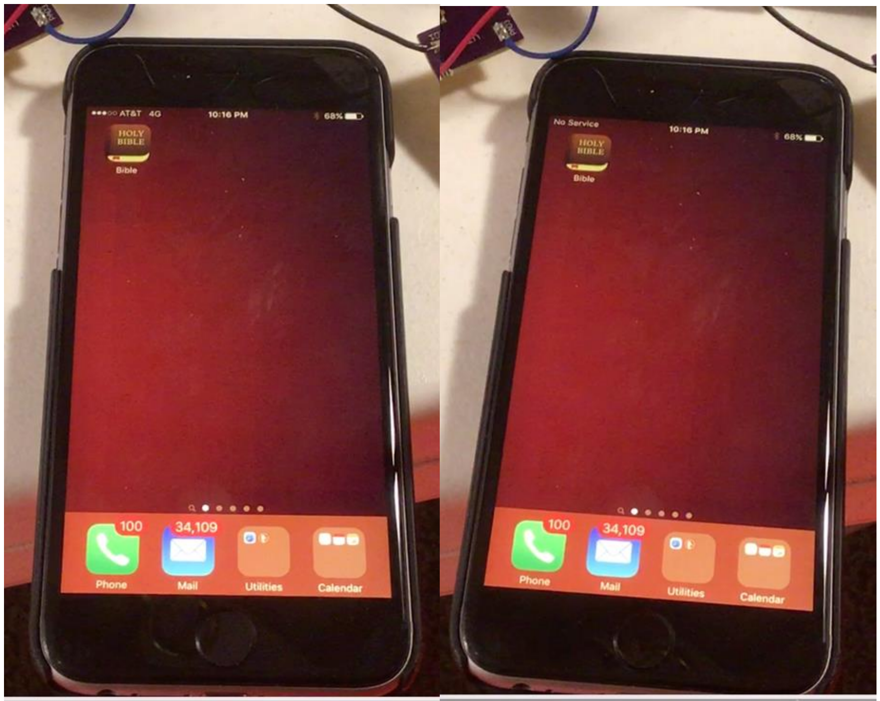


Figure 23. Cell Phone Signal Jam AT&T Network.

Figure 24. Cell Phone Signal Jam T-Mobile Network.

Further testing of the device was done at Purdue Northwest, Westville campus. Testing involved the utilization of a spectrum analyzer to visualize the noise frequency range generated by the two VCOs. The spectrum analyzer displays power versus frequency. This testing verified the successful operation of the device as it clearly transmits on the desired frequency ranges needed to disrupt the networks as can be seen in Figures 25 and 26.

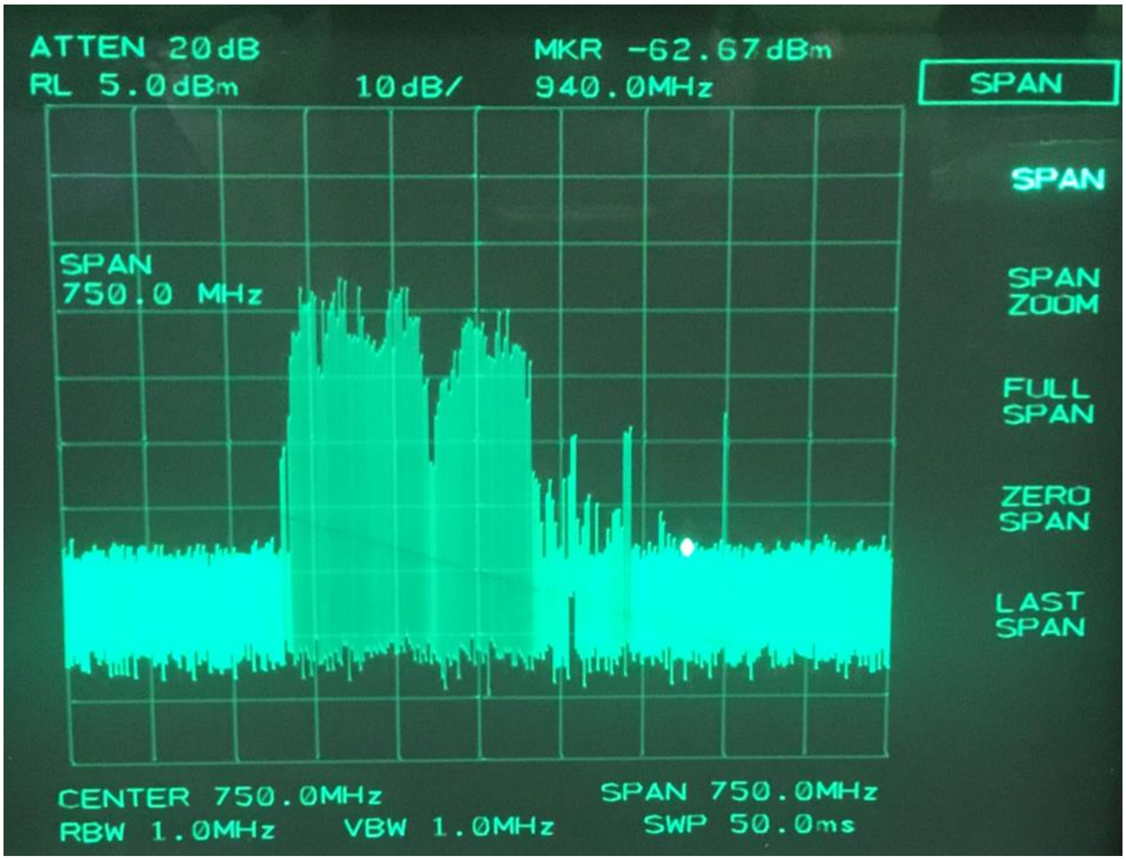


Figure 25. VCO 1 Spectrum Analyzer Output.

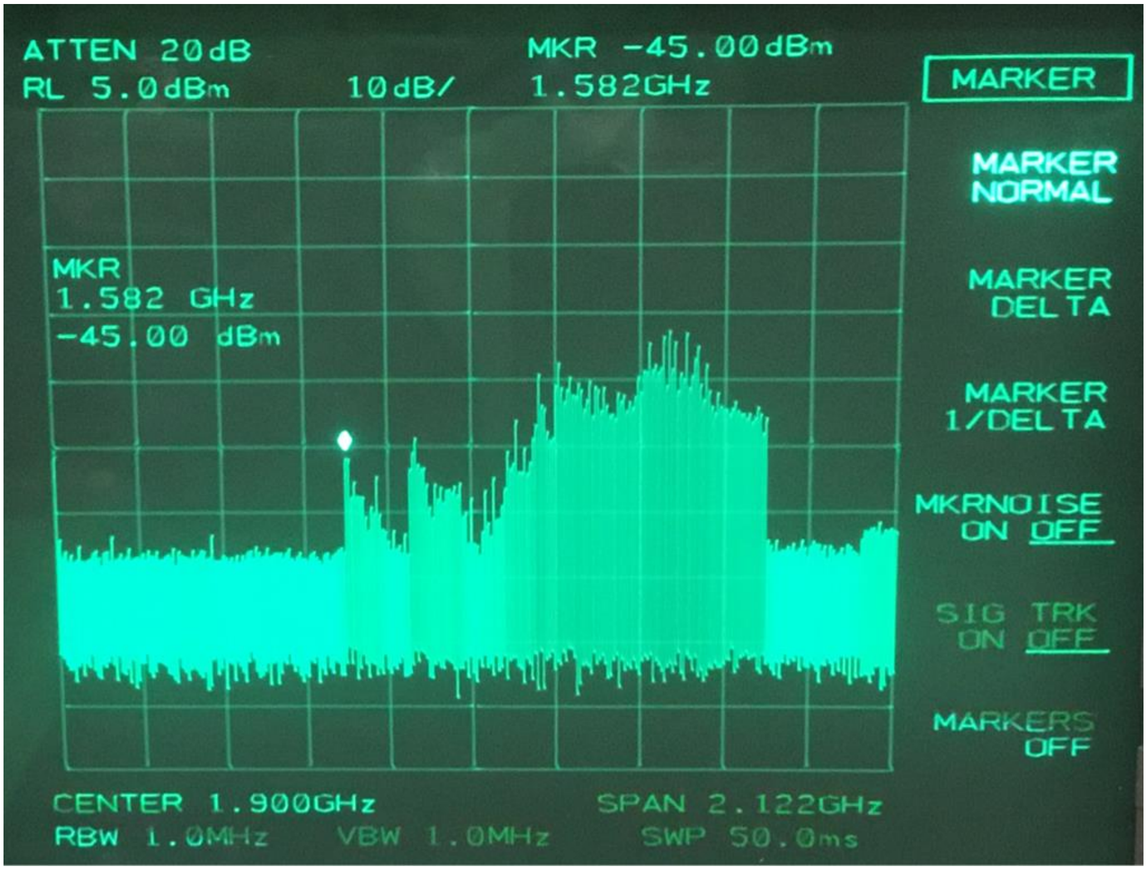


Figure 26. VCO 2 Spectrum Analyzer Output.

Final PCB Circuit Design, Fabrication and Testing

The free version of the software PCB Eagle® that was used to create the breakout boards allows designing only a small PCB area. Hence, the company was contacted by the design team and academic advisor. After conveying that the use of the software would be for a senior design project, the company granted the team a free educational version of the software that allows more square area and more added features. The extra granted area, however, was barely enough to accommodate carbon resistors and ordinary capacitors, as such, we switched to surface mount components.

Designing the overall circuit required careful planning and a deeper understanding of the software. The task of designing the final circuit involved modeling the footprints of the power amps and specific trace widths needed to correctly generate the intended jamming waveform. The trace widths affect the frequency matching, if the width of the waveform is too narrow or too wide it will cause a frequency shift. Figure 27 below shows the final circuit schematic design done in PCB Eagle®. Figure 28 shows the fabricated printed circuit board that measures 2.5 inches by 4 inches.

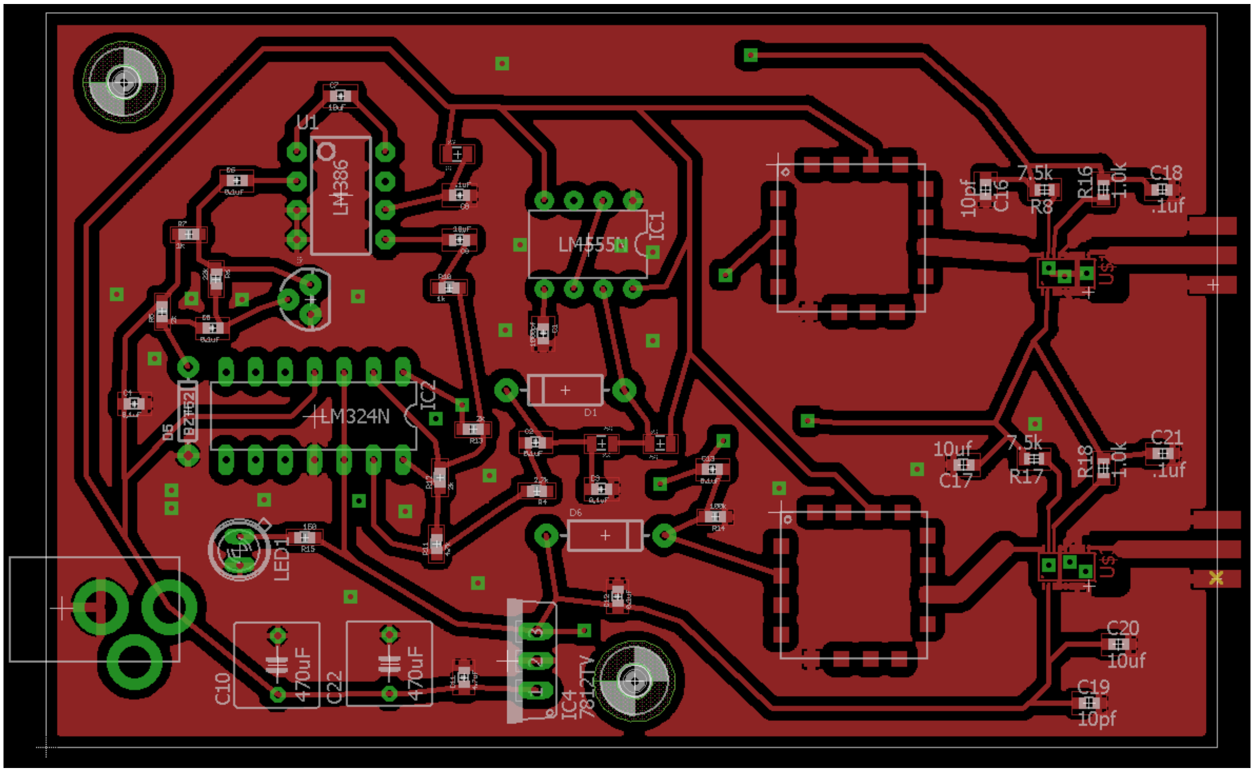


Figure 27. Circuit Schematic.

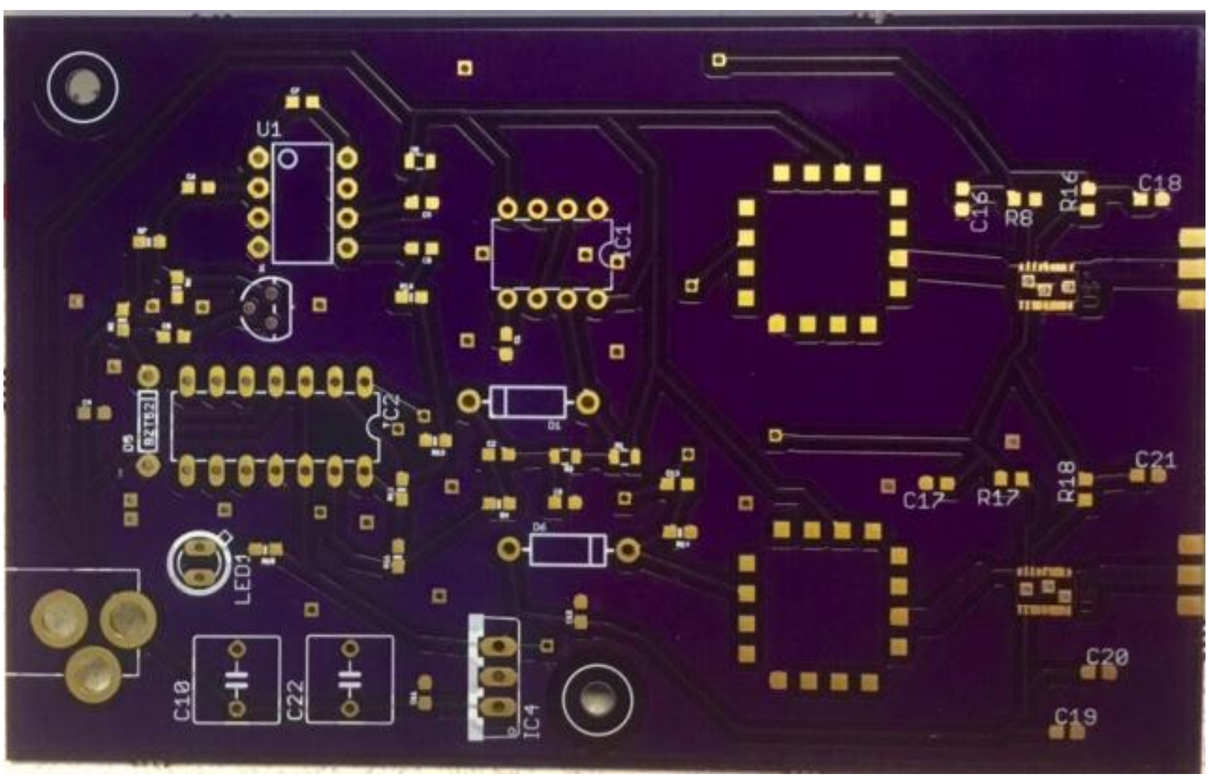


Figure 28. Fabricated Circuit Board.

Since surface mount components are of a very small size (0603 series with 1.6mm×0.8mm dimensions), they require a special attention in terms of soldering. Special tools such as the infrared heater and heat gun were acquired by the ECE department (Fig. 29 and 30). The surface mount components were carefully placed on the printed circuit board using soldering paste. After placing components, the infrared heater was set to a predefined temperature curve according to the solder paste manual, and placed inside to oven (Fig. 31, 32, 33, 35, 36 and 37). Figure 38 displays the completed soldered circuit board.

Figure 29. Infrared IC Heater.

Figure 30. Hot Air Gun Rework Soldering Station.

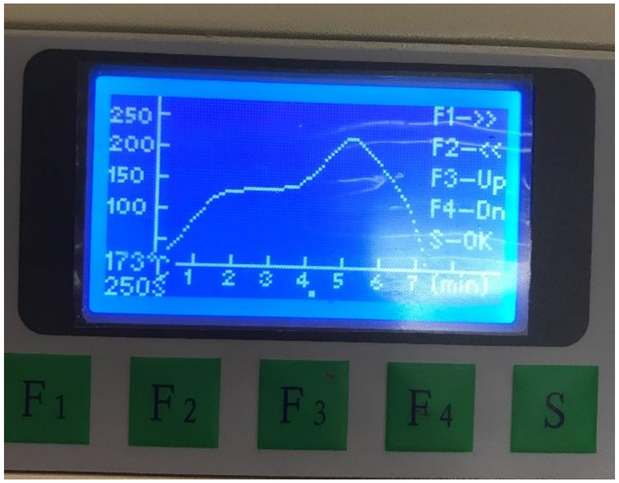


Figure 31. Infrared Heater Temperature Curve.

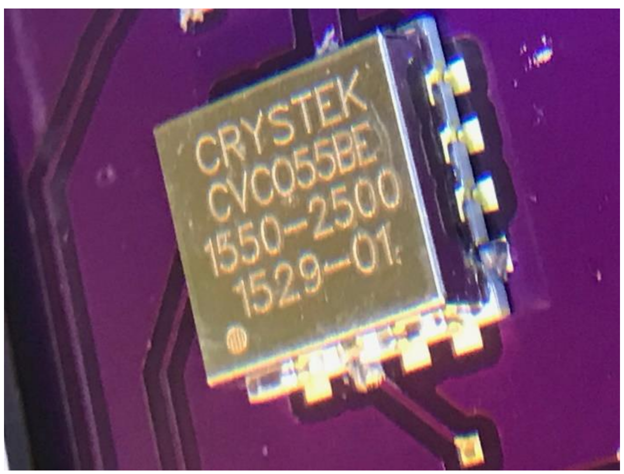


Figure 32. VCO Placement considering ×6 magnification.

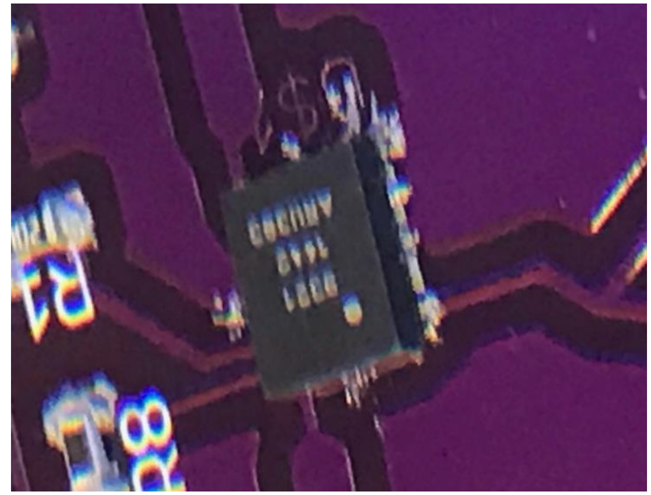


Figure 33. Power Amp Placement (considering ×6 magnification).

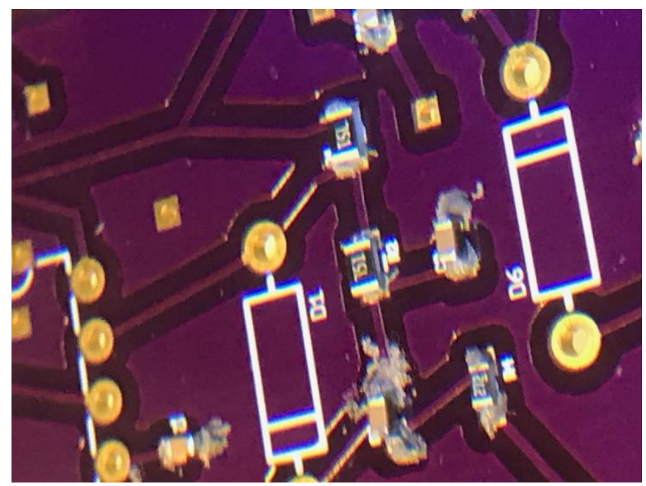


Figure 34. Resistor and Capacitor Placement considering ×6 magnification.

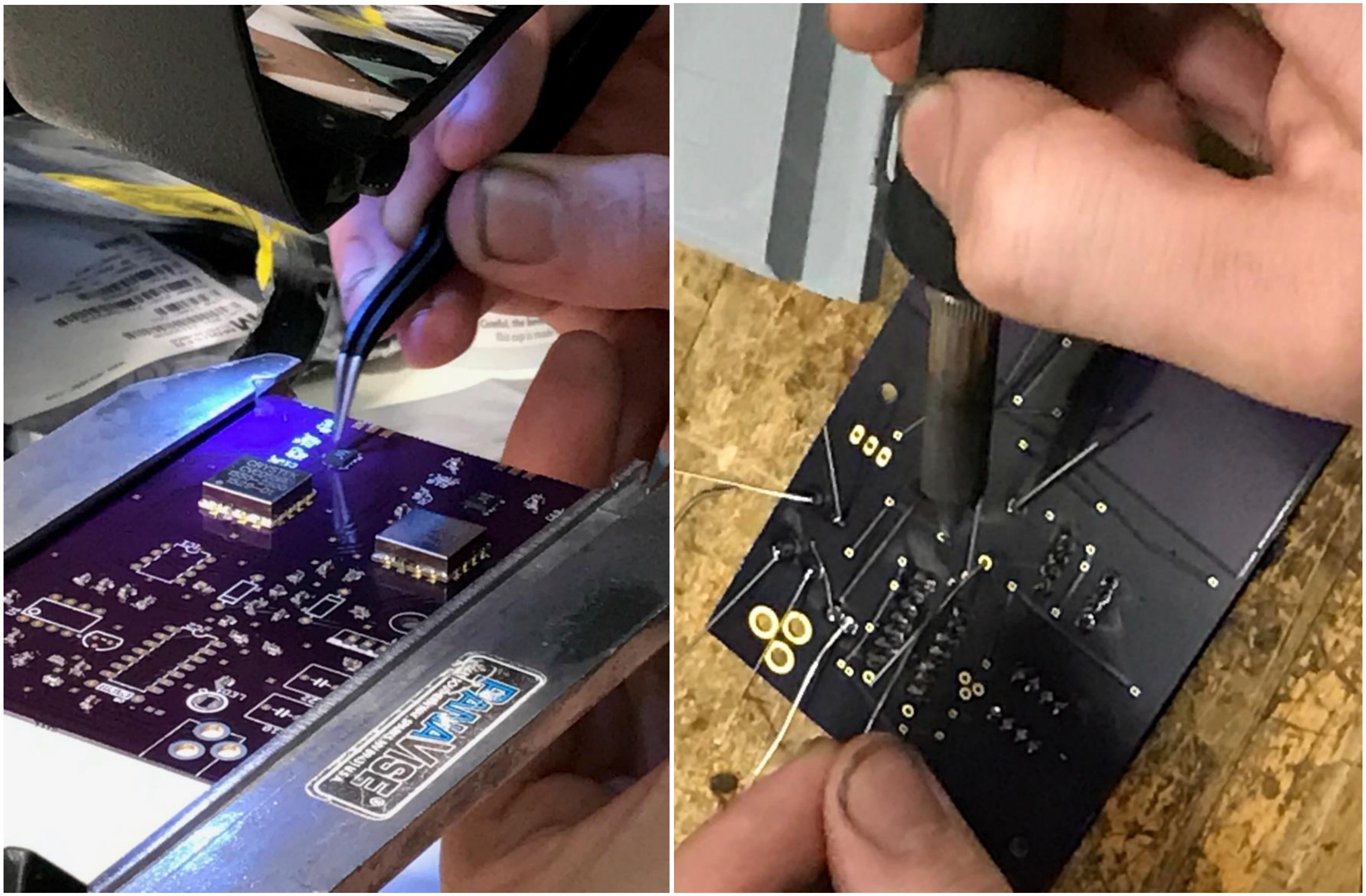


Figure 35. Placement of Components.

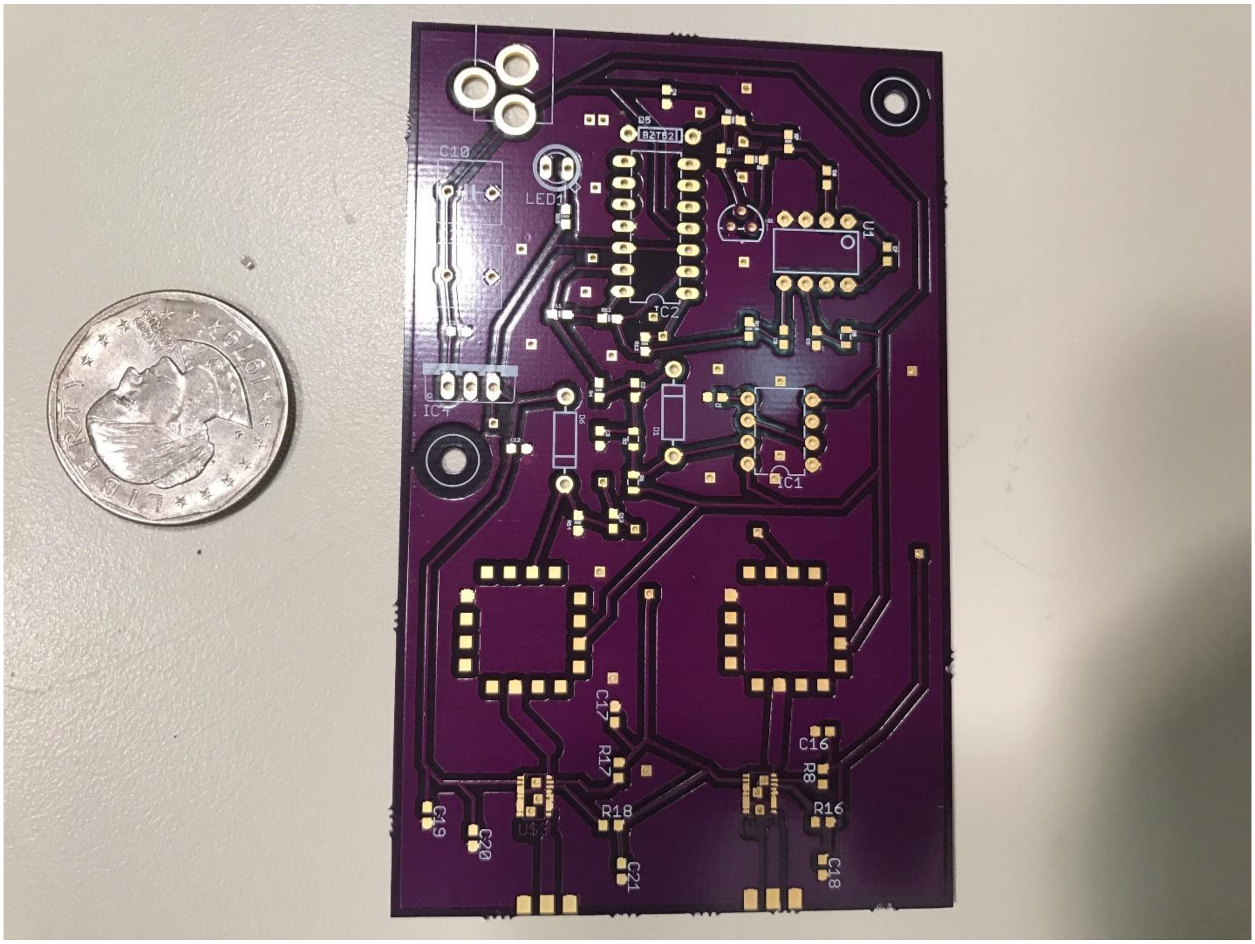


Figure 36. Display of Relative Size of PCB Against Quarter.

Figure 37. PCB Size Comparison.

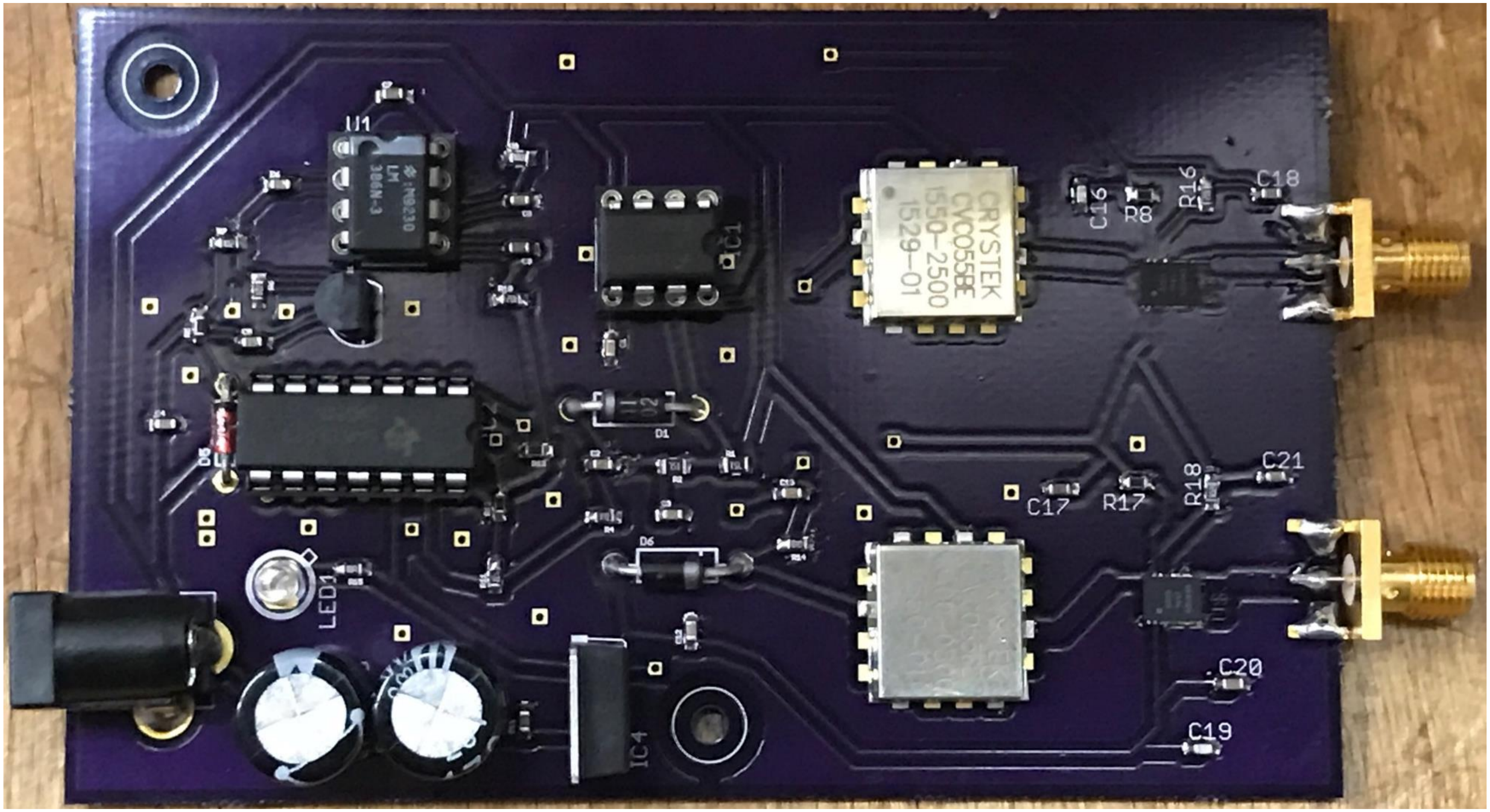


Figure 38. Soldered Circuit Board.

After finishing soldering all components on the board, testing of the board resulted in finding a defect in the manufacturing at the RF power amplifier traces that caused the power amplifier section to short circuit the device. To work around this problem, the power amp section of the board was isolated. The output from the VCOs was routed directly into the SMA connectors to output the signal through the antennas (Fig. 39). The device was then tested on multiple cell phones displaying the device does indeed disrupt the signals of the networks within a short range (Fig. 40). We claim that if range will significantly increase if the RF amplifiers were taken into account as each amplifier provides a gain of 32 dB, which is enough for jamming within 15 meters radius.

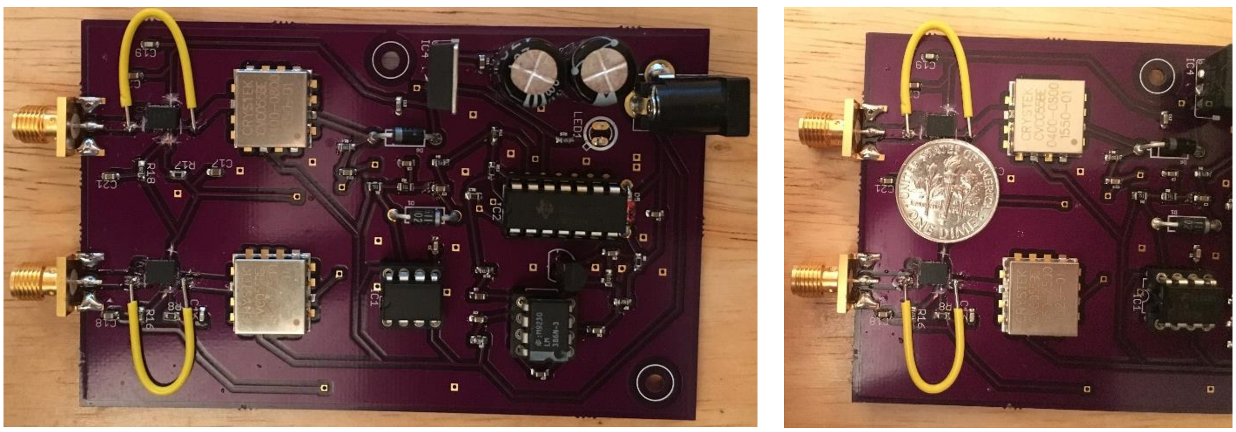


Figure 39. Isolation of Power Amp Section and size comparison versus dime.

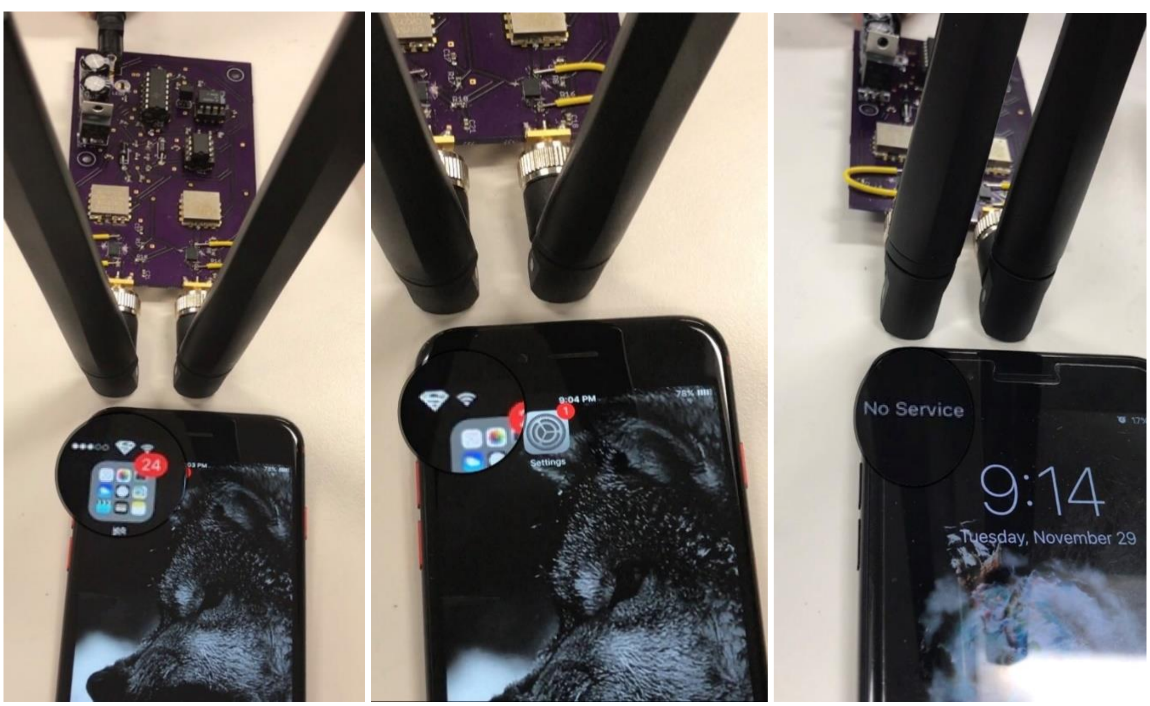


Figure 40. Jammer Test of Disrupting Networks.

Case Design

The enclosure for the device was designed using Microsoft 3D Builder® (Figs. 41 and 42). The file for the enclosure was saved as an STL Standard Tessellation Language file in order to be compatible and printed using the 3D printer from the head technician of the ECE Department (Fig. 43). Figure 44 shows the Case enclosing the jamming device.

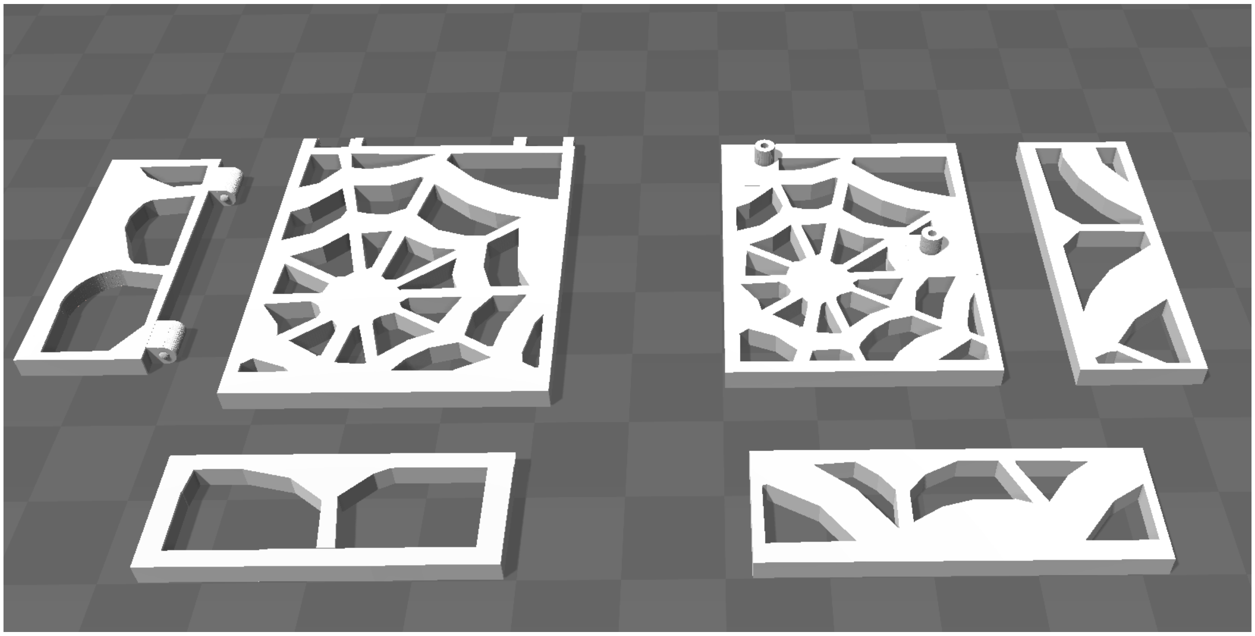


Figure 41. 3D Case Design Sides.

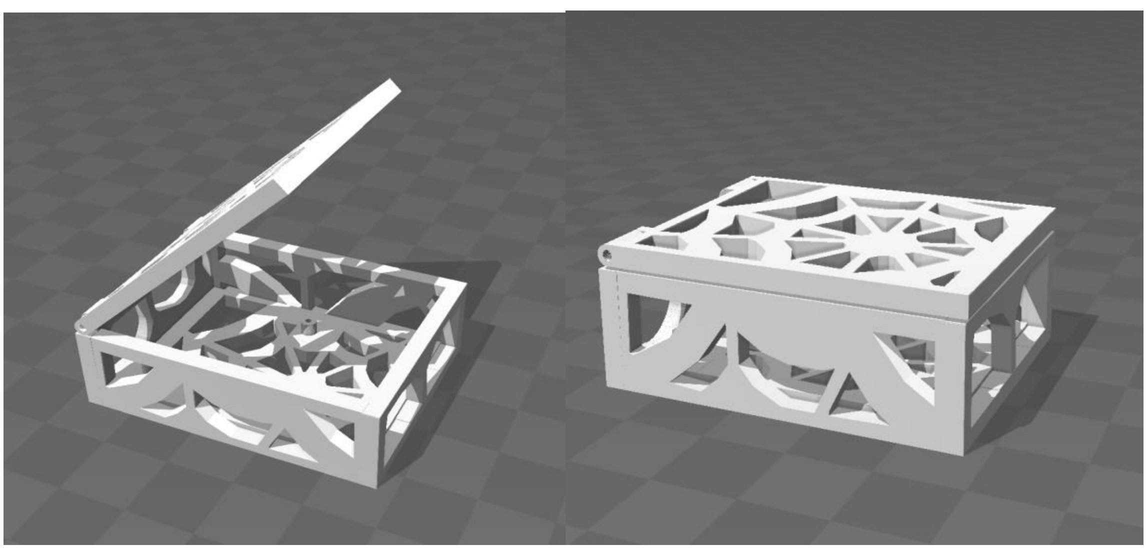


Figure 42. 3D Case Design Assembly.

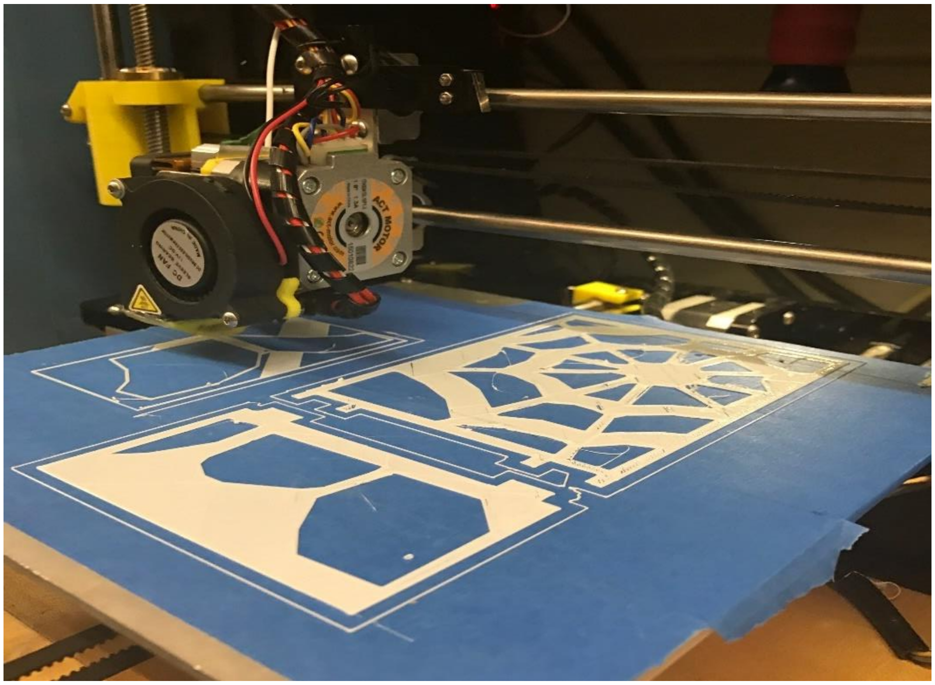


Figure 43. 3D Printing.

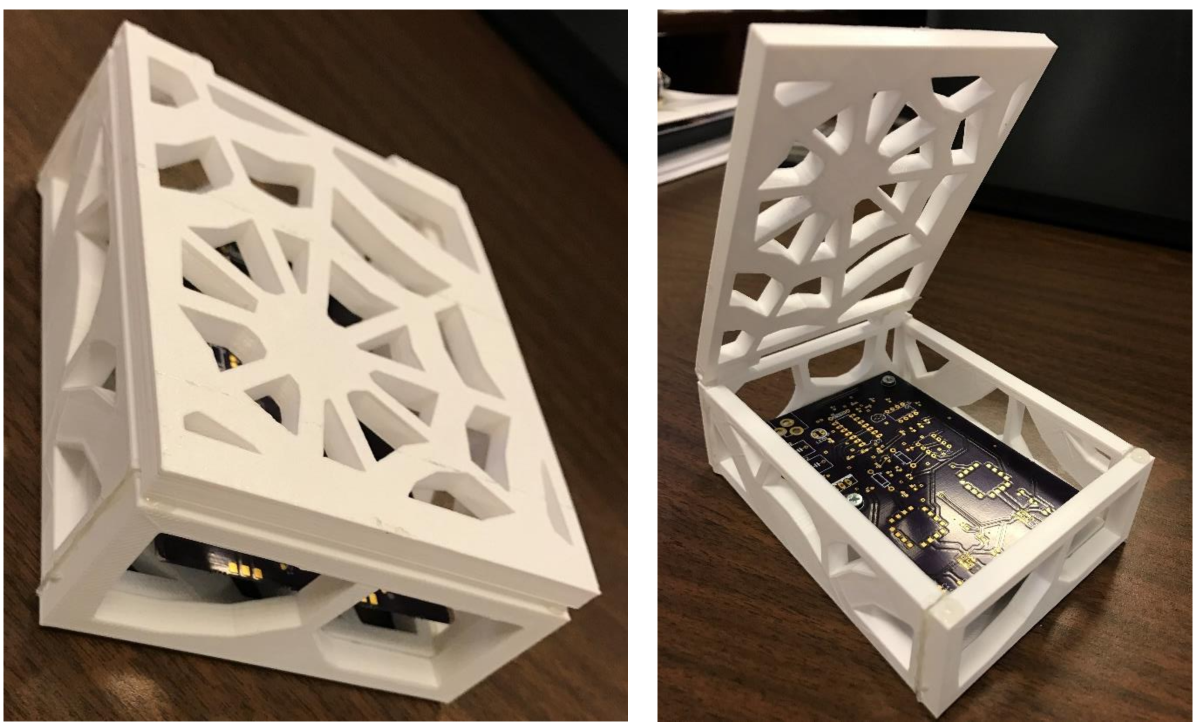


Figure 44. Case Enclosing Circuit.

Conclusion

In conclusion, this project successfully followed the process of researching, designing, constructing, and testing a cellular jammer that disrupted all cellular communications of the 2G GSM, 3G W-CDMA, and 4G LTE frequency bands of Sprint®, T-Mobile®, AT&T®, and Verizon® cellular providers.

The successful design of the IF, RF, and Power sections of the device were implemented onto the combination of a bread board and break out printed circuit boards to test the device. The testing of this prototype device was a success and this design was implemented on a full printed circuit board layout with the incorporation of power amps to get a further jamming distance of the device. After receiving the fabricated printed circuit board and installing the components onto the device, testing resulted in finding a manufacturing error in the power amp section of the PCB. To fix this problem the power amp section of the device was isolated and bypassed. The signal path from the VCOs were sent directly to the SMA connectors and transmitted out through the antennas. The testing of the final device proved full functionality and proof of concept, with a shorter jamming radius due to not getting the gain from the power amp section of the circuit.

Future Work

This project was a success and can be handed down to future design teams to implement the following modifications: 1) Fixing the traces conveying the RF power amps; 2) Making the jammer portable by modifying the power source section; 3) Making adaptive jamming by tuning the input voltage of the VCOs to cover other bands such as wireless local area networks (WLAN) and Bluetooth; and 4) Designing an anti-jamming device that will cancel out the transmitted noise signal from the original Jammer.

References

1. Gary Wollenhaupt "How Cell Phone Jammers Work" 24 March 2005. http://electronics.howstuffworks.com/cell-phone-jammer.htm (3 Feb. 2016).
2. Spencer S. Hsu "Local Police Want Right to Jam Wireless Signals" 1 February 2009. http://www.washingtonpost.com/wp-dyn/content/article/2009/01/31/AR2009013101548.html (3 Feb. 2016).
3. "jamming signal" (n.d.). Collins English Dictionary - Complete & Unabridged 10th Edition. http://www.yourdictionary.com/jamming-signal (23 Apr. 2016).
4. "radio frequency." (n.d.). Collins English Dictionary - Complete & Unabridged 10th Edition. http://www.dictionary.com/browse/radio--frequency (19 Apr. 2016).
5. "intermediate frequency." (n.d.). Collins English Dictionary - Complete & Unabridged 10th Edition. http://www.dictionary.com/browse/intermediate-frequency (19 Apr. 2016).
6. http://www.circuitstoday.com/voltage-controlled-oscillator (19 Apr. 2016).
7. "power amplifier." (n.d.). Collins English Dictionary - Complete & Unabridged 10th Edition. http://www.dictionary.com/browse/power-amplifier (19 Apr. 2016).
8. "antenna." (n.d.). Collins English Dictionary - Complete & Unabridged 10th Edition. http://www.dictionary.com/browse/antenna (19 Apr. 2016).
9. "555 Timer Circuits" http://www.555-timer-circuits.com/an-overview.html (19 Apr. 2016).
10. "Positive Clamper Circuit: Example 1" November 23, 2015 http://youtu.be/b6PNEtG5Edk (23 Apr. 2016).
11. "Introduction to Clamper Circuit, Diode Clamper Circuit Analysis" November 23, 2015 http://youtu.be/XYpY5NdjFxU (23 Apr. 2016).
12. "SureCall Force 5" https://www.repeaterstore.com/collections/verizon/products/surecall-force5 (23 Apr. 2016).
13. "Spectrum Dashboard" http://reboot.fcc.gov/spectrumdashboard/systemInfo.seam?conversationId=15402 (23 Apr. 2016).
14. "Digi-Key Electronics" www.digikey.com (23 Apr. 2016).

Appendix A: Glossary

1. Jammer: In cellphone terminology, a jammer is a device that blocks transmissions by creating interference. The jammer emits signals in the same frequency range that cell phones uses, and within the range of a jammer a cellphone user may lose their signal.
2. RF: radio frequency, a frequency or band of frequencies that lie in the range 10 kilohertz to 300 000 megahertz and can be used for radio communications and broadcasting.
3. IF: intermediate frequency, the frequency to which the signal carrier frequency is changed in a super heterodyne receiver and at which most of the amplification takes place.
4. VCO: Voltage Controlled oscillator, Voltage controlled oscillator is a type of oscillator where the frequency of the output oscillations can be varied by varying the amplitude of an input voltage signal.
5. Power amplifier: (electronics) an amplifier that is usually the final amplification stage in a device and is designed to give the required power output
6. Antenna: a conductor by which electromagnetic waves are sent out or received, consisting commonly of a wire or set of wires;
7. 555 Timer: The 555 Integrated Circuit (IC) is an easy to use timer that has many applications.

Appendix B: Equations

The following formulas were used during the design phase of the device:

- Non Inverting Op Amp Gain formula

$$\beta = 1 + \frac{R_2}{R_1}$$

- Non Inverting Op Amp V_{out} Formula

$$V_{out} = \left(1 + \frac{R2}{R1}\right) . V_{in}$$

- 555 timers formulas output frequency

$$f = \frac{1.44}{(R_a + 2R_b)}$$

- Capacitance charge time

$$T_c = .693(R_a + R_b)C$$

- Capacitance discharge time

$$T_D = .693 R_b C$$

Appendix C: Data Sheets

VCO 1.

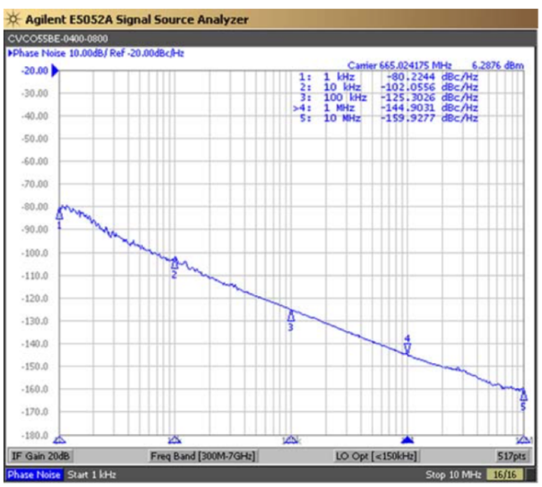
CRYSTEK MICROWAVE
A DIVISION OF CRYSTEK CORPORATION

Voltage Controlled Oscillator-VCO
CVCO55BE-0400-0800

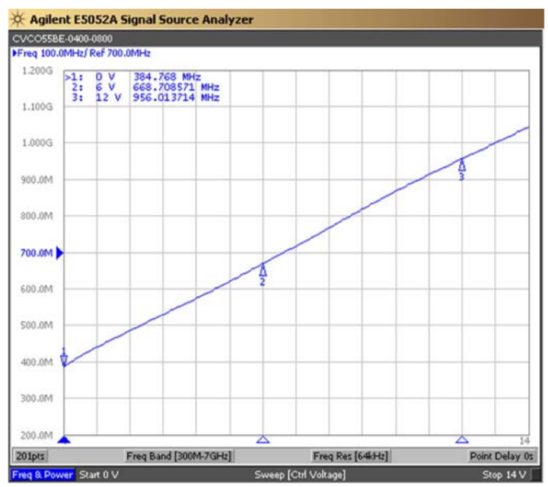
PERFORMANCE SPECIFICATION	MIN	TYP	MAX	UNITS
Lower Frequency:			400	MHz
Upper Frequency:	800			MHz
Tuning Voltage:	0		12	VDC
Supply Voltage:	4.75	5.0	5.25	VDC
Output Power:	0	+5.0	+10.0	dBm
Supply Current:		17		mA
Harmonic Suppression (2nd Harmonic):		-5		dBc
Pushing:			5.0	MHz/V
Pulling, all Phases:			3.0	MHz pk-pk
Tuning Sensitivity:		47		MHz/V
Phase Noise @ 10kHz offset:		-102		dBc/Hz
Phase Noise @ 100kHz offset:		-122		dBc/Hz
Load Impedance:		50		Ω
Input Capacitance:			200	pF
Operating Temperature Range:	-10		+70	°C
Storage Temperature Range:	-45		+90	°C

RoHS Compliant

Phase Noise (1 Hz BW, Typical)



Tuning Curve (Typical)



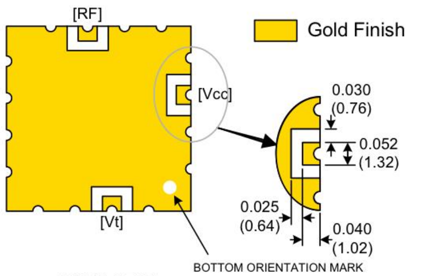
Page 1 of 2

CRYSTEK CORPORATION
12730 Commonwealth Drive • Fort Myers, Florida 33913
Phone: 239-561-3311 • 800-237-3061
Fax: 239-561-1025 • www.crystek.com

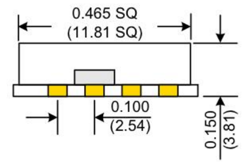
Voltage Controlled Oscillator-VCO
CVCO55BE-0400-0800

CRYSTEK MICROWAVE
A Division of Crystek Corporation

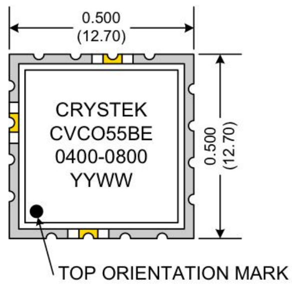
BOTTOM VIEW

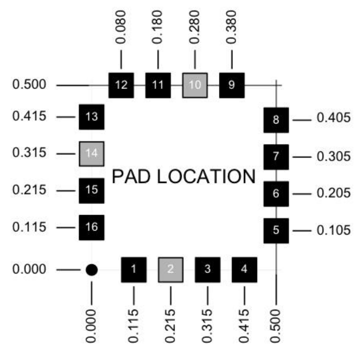


SIDE VIEW



TOP VIEW

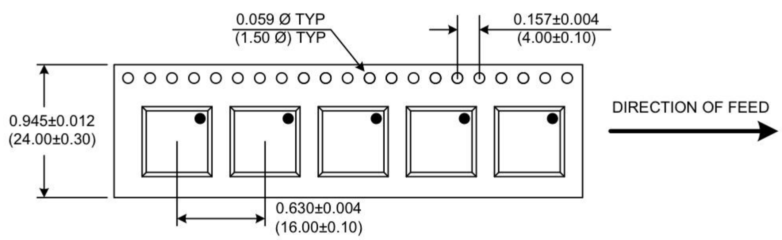




Pad	Connection
2	Vt
10	RF-OUTPUT
14	Vcc
Others	GROUND

- Unless otherwise specified, Dimensions are in: IN / (mm)
- Pad Location Dimensions are in: Inches

TAPE AND REEL



Drawing not to scale

Product Control:			
Crystek Part Number:	CVCO55BE-0400-0800	Release Date:	07-Mar-12
Revision Level:	F	Responsible:	C. Vales

Specification is subject to change without notice

CRYSTEK CORPORATION
12730 Commonwealth Drive • Fort Myers, Florida 33913
Phone: 239-561-3311 • 800-237-3061
Fax: 239-561-1025 • www.crystek.com

VCO 2.

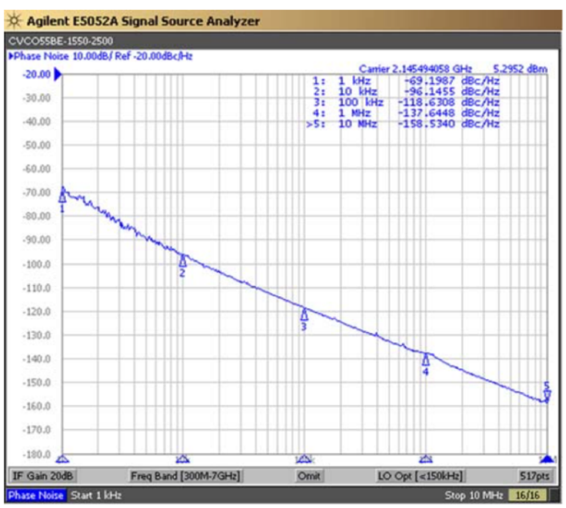
CRYSTEK MICROWAVE
A DIVISION OF CRYSTEK CORPORATION

Voltage Controlled Oscillator-VCO
CVCO55BE-1550-2500

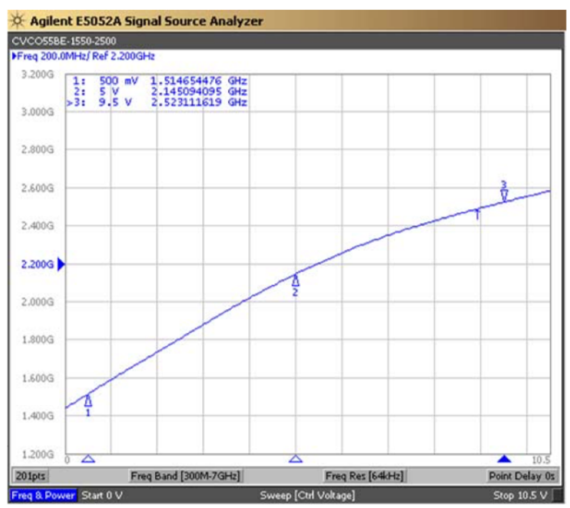
PERFORMANCE SPECIFICATION	MIN	TYP	MAX	UNITS
Lower Frequency:			1550	MHz
Upper Frequency:	2500			MHz
Tuning Voltage:	0.5		9.5	VDC
Supply Voltage:	9.75	10.0	10.25	VDC
Output Power:	+3.0	+6.0	+9.0	dBm
Supply Current:		13		mA
Harmonic Suppression (2nd Harmonic):		-7		dBc
Pushing:			5.0	MHz/V
Pulling, all Phases:			23.0	MHz pk-pk
Tuning Sensitivity:		115		MHz/V
Phase Noise @ 10kHz offset:		-95		dBc/Hz
Phase Noise @ 100kHz offset:		-115		dBc/Hz
Load Impedance:		50		Ω
Input Capacitance:			50	pF
Operating Temperature Range:	-40		+85	°C
Storage Temperature Range:	-45		+90	°C

RoHS Compliant

Phase Noise (1 Hz BW, Typical)



Tuning Curve (Typical)

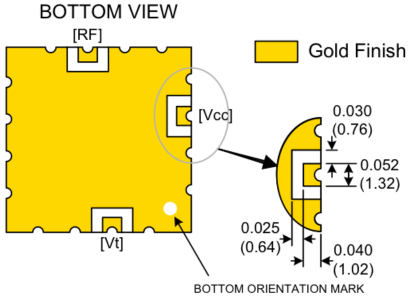


Page 1 of 2

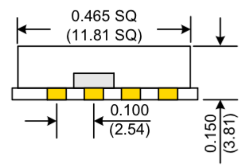
CRYSTEK CORPORATION
12730 Commonwealth Drive • Fort Myers, Florida 33913
Phone: 239-561-3311 • 800-237-3061
Fax: 239-561-1025 • www.crystek.com

Voltage Controlled Oscillator-VCO
CVCO55BE-1550-2500

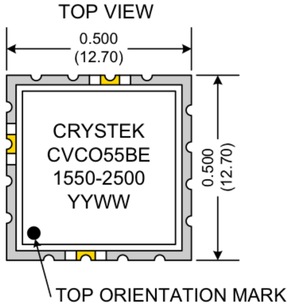
BOTTOM VIEW

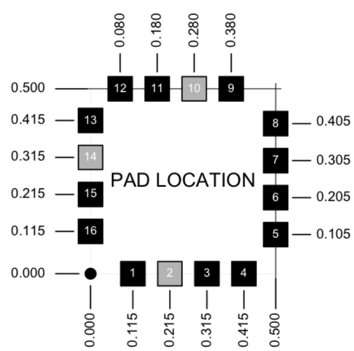


SIDE VIEW



TOP VIEW

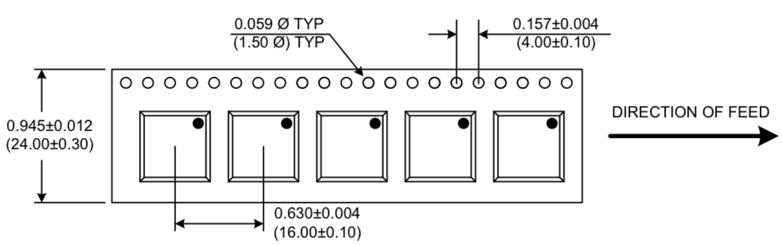




Pad	Connection
2	Vt
10	RF-OUTPUT
14	Vcc
Others	GROUND

- Unless otherwise specified, Dimensions are in: IN (mm)
- Pad Location Dimensions are in: Inches

TAPE AND REEL



Drawing not to scale

Product Control:			
Crystek Part Number:	CVCO55BE-1550-2500	Release Date:	15-Nov-12
Revision Level:	F	Responsible:	C. Vales

Specification is subject to change without notice

CRYSTEK CORPORATION
12730 Commonwealth Drive • Fort Myers, Florida 33913
Phone: 239-561-3311 • 800-237-3061
Fax: 239-561-1025 • www.crystek.com

Power Amp.

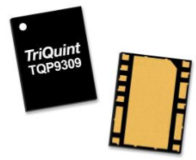
TQP9309

High Efficiency 0.5W Small Cell Power Amplifier

RFMD + TriQuint = Qorvo

Applications

- Small-Cell Basestations
- Enterprise Femtocell
- Bands 5, 6, 8, 12, 13, 14, 17, 20, 26, 27, 28, 29

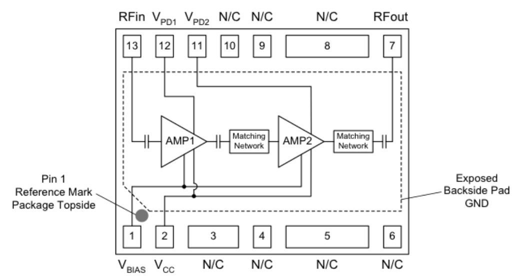


3.5x4.5 mm Leadless SMT Package

Product Features

- Frequency Range : 0.7-1.0 GHz
- Covers multiple bands with one component
- Fully integrated, 2-stage Power Amplifier
- Internally matched 50 Ω input/output
- -50dBc ACLR (corrected) @ +28 dBm Pavg
- 32 dB Gain
- 27% PAE @ +28 dBm Pavg
- In-built Control Bias and Temp. Comp Circuit
- Single Supply Voltage : 5V
- Lead-free / RoHS compliant
- POE Capable

Functional Block Diagram



General Description

The TQP9309 is a high-efficiency two-stage power amplifier in a low-cost surface-mount package with on-chip bias control and temperature compensation circuitry, suitable for small cell base station applications.

TQP9309 provides 32 dB gain and >+28 dBm linear power with pre-distortion correction over the 0.7-1.0 GHz frequency range for Bands 5, 6, 8, 12, 13, 14, 17, 20, 26, 27, 28, and 29. With pre-distortion, the amplifier is able to achieve -50dBc ACLR at 28 dBm output power using a 20 MHz LTE signal.

The TQP9309 integrates two high performance amplifier stages onto a module to allow for a compact system design and requires very few external components for operation. The amplifier is bias adjustable allowing the amplifier's power consumption to be optimized. The TQP9309 is available in a lead-free/RoHS-compliant 3.5x4.5mm surface mount package and is pin-compatible to the 1.8-2.2 GHz TQP9321 and 2.5-2.7 GHz TQP9326.

Pin Configuration

Pin No.	Label
1	Vbias
2	Vcc
3, 4, 5, 6, 8, 9, 10	GND or NC
7	RFout
11	Vpd2
12	Vpd1
13	RFin
Backside Paddle	RF/DC Ground

Ordering Information

Part No.	Description
TQP9309	0.7-1.0 GHz Power Amplifier
TQP9309-PCB	Evaluation board

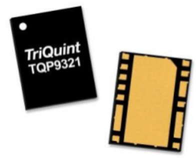
Standard T/R size: 2500 pcs. on a 13" reel

TQP9321

High Efficiency 0.5 W Small Cell PA

Applications

- Small Cell / Picocell
- Enterprise Femtocell
- Bands 1, 2, 3, 4, 10 and 25

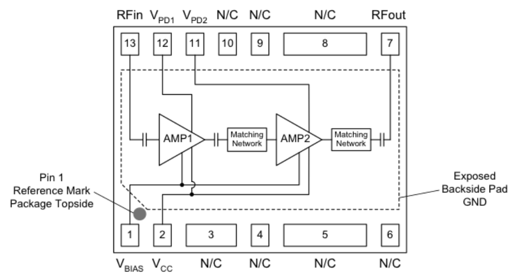


3.5 x 4.5 mm Leadless SMT Package

Product Features

- Frequency Range: 1.8 – 2.17 GHz
- Covers Multiple Bands with One Component
- Fully Integrated, 2-Stage Power Amplifier
- Internally Matched 50 Ω Input/Output
- ACLR: −50 dBc ACLR at Pavg =+27 dBm
- Gain: 30 dB
- High Efficiency: 27% at +27 dBm
- Quiescent Current: 110 mA
- Integrated Bias Control and Temp. Comp Circuit
- Single Supply Voltage: +5 V
- Lead-free / RoHS compliant
- POE Capable

Functional Block Diagram



General Description

The TQP9321 is a high-efficiency, two-stage power amplifier with integrated bias and temperature control circuits in a low-cost surface-mount package. This 0.5 watt power amplifier is ideal for small cell base station applications.

TQP9321 provides high gain (30 dB) and +27 dBm linear power with pre-distortion correction over the 1.8 – 2.2 GHz frequency range for bands 1, 2, 3, 4, 10 and 25. With pre-distortion, the amplifier is able to achieve −50 dBc ACLR at +27 dBm output power using an LTE signal.

The TQP9321 integrates two high performance amplifier stages to allow for a compact system design and requires very few external components for operation. The amplifier is bias adjustable allowing the amplifier's power consumption to be optimized for specific applications. The TQP9321 is available in a lead-free/RoHS-compliant 3.5 x 4.5 mm surface mount package and is pin-compatible to the 0.7 – 1.0 GHz TQP9309 and 2.5 – 2.7 GHz TQP9326.

Pin Configuration

Pin No.	Label
1	V_{BIAS}
2	V_{CC}
3, 4, 5, 6, 8, 9, 10	N/C
7	RFout
11	V_{PD2}
12	V_{PD1}
13	RFin
Backside Pad	RF/DC Ground

Ordering Information

Part No.	Description
TQP9321	0.5 W Small Cell PA
TQP9321-PCB	Evaluation board

Standard T/R size: 2500 pcs. on a 13" reel

Antenna.

Product Specification

WTR7210

Wideband LTE, 4G, 3G & GSM Multiposition Antenna

Features

- Groundplane Independent
- Covers LTE, cellular, GSM and 3G bands
- Locks in three positions for flexibility
- Ideal for fixed and mobile terminals

Specifications	
Radiating element	1/2 Wave Element
Frequency range	690-960/1710-2700MHz
Gain	1 dBi
Polarisation	Linear
VSWR	< 2.0:1
Power rating	10W
Connector	SMA-Male (multiposition)
Dimensions	171 x 18mm (max)

Popular Ordering Options	
FWTR35292-SM-KR	WTR7270 antenna with SMA-Male connector

Specifications subject to change without notice.

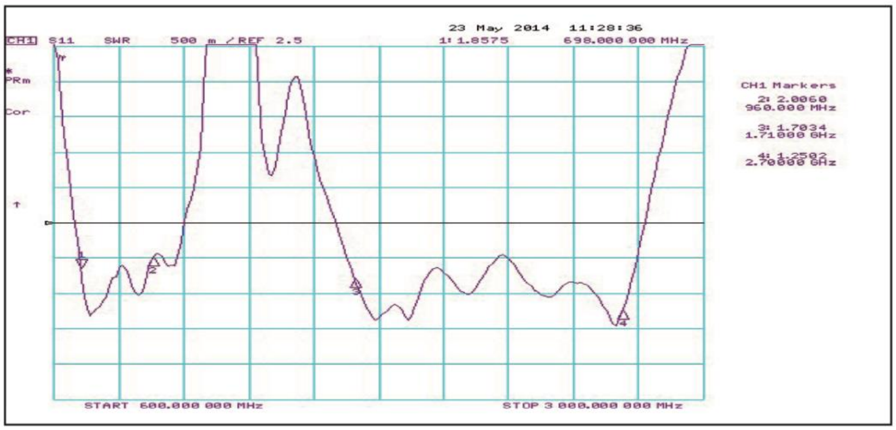
5 Little Balmer
Buckingham Industrial Park
Buckingham
MK18 1TF
UK

Tel: +44 (0)1280 824055
Fax: +44 (0)1280 817179
Email: sales@ead-ltd.com
Web: www.ead-ltd.com

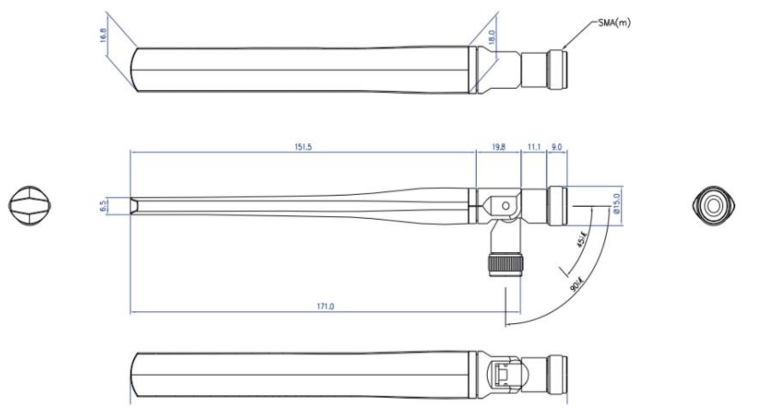
embedded antenna design ltd
Delivering Antenna Innovation

WTR7270| LTE/4G Multiband Multiposition Antenna

VSWR



Outline Drawing



Specifications subject to change without notice.

5 Little Balmer
Buckingham Industrial Park
Buckingham
MK18 1TF
UK

Tel: +44 (0)1280 824055
Fax: +44 (0)1280 817179
Email: sales@ead-ltd.com
Web: www.ead-ltd.com

EAD
embedded antenna design ltd
Delivering Antenna Innovation

Appendix D: Parts List

Part	Value	Device	Package	Description	PROD_ID	VALUE
C1	1000pf	1NF/1000PF-50V-10%(0603)	0603-CAP	CAP-07886	CAP-07886	1nF
C2	0.1uF	0.1UF-25V(+80/-20%)(0603)	0603-CAP	CAP-00810	CAP-00810	0.1uF
C3	0.1uF	0.1UF-25V(+80/-20%)(0603)	0603-CAP	CAP-00810	CAP-00810	0.1uF
C4	0.1uF	0.1UF-25V(+80/-20%)(0603)	0603-CAP	CAP-00810	CAP-00810	0.1uF
C5	0.1uF	0.1UF-25V(+80/-20%)(0603)	0603-CAP	CAP-00810	CAP-00810	0.1uF
C6	0.1uF	0.1UF-25V(+80/-20%)(0603)	0603-CAP	CAP-00810	CAP-00810	0.1uF
C7	10uF	0.1UF-25V(+80/-20%)(0603)	0603-CAP	CAP-00810	CAP-00810	0.1uF
C8	.1uF	0.1UF-25V(+80/-20%)(0603)	0603-CAP	CAP-00810	CAP-00810	0.1uF
C9	10uF	0.1UF-25V(+80/-20%)(0603)	0603-CAP	CAP-00810	CAP-00810	0.1uF
C10	470uF	C-US050-075X075	C050-075X075	CAPACITOR, American symbol		
C11	4.7uF	0.1UF-25V(+80/-20%)(0603)	0603-CAP	CAP-00810	CAP-00810	0.1uF
C12	0.1uF	0.1UF-25V(+80/-20%)(0603)	0603-CAP	CAP-00810	CAP-00810	0.1uF
C13	0.1uF	0.1UF-25V(+80/-20%)(0603)	0603-CAP	CAP-00810	CAP-00810	0.1uF
C16	10pf	C-USC0603	C0603	CAPACITOR, American symbol		
C17	10uf	C-USC0603	C0603	CAPACITOR, American symbol		

Part	Value	Device	Package	Description	PROD_ID	VALUE
C18	.1uf	C-USC0603	C0603	CAPACITOR, American symbol		
C19	10pf	C-USC0603	C0603	CAPACITOR, American symbol		
C20	10uf	C-USC0603	C0603	CAPACITOR, American symbol		
C21	.1uf	C-USC0603	C0603	CAPACITOR, American symbol		
C22	470uF	C-US050-075X075	C050-075X075	CAPACITOR, American symbol		
D1		DIODEPTH	DIODE-1N4001	Diode		
D5	BZT52	DIODE-ZENER	DIODE-BZT52	Zener Diode	DIO-08200	BZT52
D6		DIODEPTH	DIODE-1N4001	Diode		
H1	MOUNT-HOLE2.8	MOUNT-HOLE2.8	2,8	MOUNTING HOLE with drill center marker		
H2	MOUNT-HOLE2.8	MOUNT-HOLE2.8	2,8	MOUNTING HOLE with drill center marker		
IC1	LM555N	LM555N	DIL08-ROUND	TIMER		
IC2	LM324N	LM324N	DIL14	OP AMP		
IC4	7812TV	7812TV	TO220V	Positive VOLTAGE REGULATOR		
J$3	SMA_EDGE	SMA_EDGE	SMA-EDGE	SMA Antenna Connector		
J$4	SMA_EDGE	SMA_EDGE	SMA-EDGE	SMA Antenna Connector		
LED1		LEDSFH482	SFH482	LED		
Q1		TRANSISTOR_NPN2N3904-EZ	TO-92-EZ	Generic NPN BJT	TRANS-08447	

R1	750	RESISTOR0805-RES	805	Resistor		
Part	**Value**	**Device**	**Package**	**Description**	**PROD_ID**	**VALUE**
R2	750	RESISTOR0805-RES	805	Resistor		
R4	2.7k	RESISTOR0603	0603-RES	Resistor		
R5	2k	RESISTOR0603	0603-RES	Resistor		
R6	22k	RESISTOR0603	0603-RES	Resistor		
R7	1k	RESISTOR0603	0603-RES	Resistor		
R8	7.5k	R-US_R0603	R0603	RESISTOR, American symbol		
R9	10	RESISTOR0805-RES	805	Resistor		
R10	1k	RESISTOR0603	0603-RES	Resistor		
R11	4.7k	RESISTOR0603	0603-RES	Resistor		
R12	2k	RESISTOR0603	0603-RES	Resistor		
R13	2k	RESISTOR0603-RES	0603-RES	Resistor		
R14	100k	RESISTOR0603	0603-RES	Resistor		
R15	150	RESISTOR0603	0603-RES	Resistor		
R16	1.0k	R-US_R0603	R0603	RESISTOR, American symbol		
R17	7.5k	R-US_R0603	R0603	RESISTOR, American symbol		
R18	1.0k	R-US_R0603	R0603	RESISTOR, American symbol		
U$1	TQP9309	TQP9309	TQP9309			
U$2	CVCO55CL	CVCO55CL	CVCO55CL	Volatage Controlled Oscillator - VCO		
U$3	TQP9309	TQP9309	TQP9309			
U$4	2.1MMJACKTHM	2.1MMJACKTHM	PJ-102A	2.1mm x 5.5mm THM DCjack with internal		

				switch. Digikey part #PJ-102A, 4UCON part #05537		
Part	**Value**	**Device**	**Package**	**Description**	**PROD_ID**	**VALUE**
U1	LM386	LM386	DIP08	low voltage audio power amplifier		
VCO1	CVCO55CL	CVCO55CL	CVCO55CL	Volatage Controlled Oscillator - VCO		

Appendix E: Budget

Consumable Materials		**137.74**
Power Supply		**25.99**
12 Volt Wall Outlet Adapter	1	25.99
IF Section		**13.33**
Resistors	10	6.99
Capacitors	10	2.99
555 Timer IC	2	0.99
LM741	1	0.75
LM386	1	0.85
Zener Diode 6.8 V	1	0.35
Diode	2	0.41
399-1170-1-ND (10uF)		2.25
RMCF0805JT750RCT-ND (750ohm)		0.4
RMCF0603FT2K70CT-ND (2.7kohm)		0.4
311-10.0HRCT-ND (10 ohm 0603)		0.4
P2.00KHCT-ND (2k ohm 0603)		0.4
311-22.0KHRCT-ND (22k ohm 0603)		0.4
311-1.0KGRCT-ND (1k ohm 0603)		1.1
311-4.70KHRCT-ND (4.7k ohm 0603)		0.4
311-150HRCT-ND (150 ohm 0603)		0.3
311-100KHRCT-ND (100k ohm 0603)		0.4
RF Section		**98.42**
VCO CVCO55BE-0400-0800 - Voltage Controlled Oscillator	1	25.96
VCO CVCO55BE-1550-2500 - Voltage Controlled Oscillator	1	25.96
PCB Copper Clad	1	15.99
WTR7270|LTE/4G Multiband Multiposition - Antenna	2	6.75
TQP9309|High Efficiency 0.5W Small Cell - Power Amplifier	1	11.88
TQP9321|High Efficiency 0.5W Small Cell - Power Amplifier	1	11.88
Fabrication		**109.98**
Printed Circuit Board		**79.99**
PCB Fabrication	1	79.99
3D Printed Case		**29.99**
3D Printer Filament	1	29.99

Appendix F: Operating Manuel and Testing Procedure.

TRI-BAND MOBILE JAMMER

Operating Manuel

WARNING

Legal Consequences:

- Use and distribution of cellular jamming devices is against the law and carries heavy penalties and/or fines.
- This project was just for educational purposes and there is no intent to distribute or remanufacture device.

PROCEDURE TO POWER AND OPERATE DEVICE

In order to operate this device plug the device into a normal 120VAC wall Outlet.

OPERATING RADIUS

The jamming distance ranges within 305mm.

TESTING

Testing procedure:

- This device can be tested by placing a cell phone within the jamming radius of the device.
- A Network Spectrum analyzer can measure the output power and frequency range of the Device.