Summer 6-15-2011

STUDY OF CELLULAR PHONE DETECTION TECHNIQUES

Nicholas W. Scott
University of Nebraska, osscottn@gmail.com

STUDY OF CELLULAR PHONE DETECTION TECHNIQUES

by

Nicholas W. Scott

A THESIS

Presented to the Faculty of

The Graduate College at the University of Nebraska

In Partial Fulfillment of Requirements

For the Degree of Master of Science

Major: Telecommunications Engineering

Under the Supervision of Professor Hamid Sharif

Lincoln, Nebraska

April, 2011

STUDY OF CELLULAR PHONE DETECTION TECHNIQUES

Nicholas W. Scott, M.S.

University of Nebraska, 2011

Advisor: Hamid Sharif

This thesis studies techniques for detecting cellular phones. It examines existing technology currently available on the open market, an existing design that utilizes mostly discrete components, and a design approach using a down converter in conjunction with a bandpass filter.

The existing technologies available on the open market are examined and discussed. These technologies are not adequate, because they are inaccurate and expensive.

The first signal detection technique, an existing design utilizing discrete components is difficult to implement. They are very affordable to construct, but require precision tuning. This design is analyzed and found to be inaccurate.

The second signal detection technique, a design using a down converter, voltage controlled oscillator (VCO), and a bandpass filter was investigated for cellular phone detection. The performance of this technique through hardware and computer modeling is discussed and the results are presented. The new system is accurate and a practical solution for detecting cellular phones in a secure facility.

Acknowledgments

I would like to express my sincere appreciation to Dr. Hamid Sharif for his direction and patience during this project. Dr. Sharif has a vast understanding of engineering subject matter, and thoroughly conveys this knowledge. When working on this project with Dr. Sharif, he provided guidance with thought-provoking objectives.Dr. Sharif was always available to answer questions despite an extremely demanding schedule. I gained a wealth of engineering knowledge from him and highly recommend his classes to my colleagues.

I also want to thank Dr. Michael Hempel for his input into this project. He provided some great advice and was very helpful when I ran into problems.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

1.1 Example of Need for Better Cellular Phone Detection Technology

Imagine you are an IT security consultant for pharmaceutical companies.Recently a company hired you to find out why their latest drug leaked to one of their competitors prior to release. The company has many labs, each with sensitive drug information stored on computers that are closely monitored by cameras. The building they are housed in has security guards at every entrance and every employee is required to wear ID. Visitors must be escorted to ensure that no drug information leaks out.

You meet with the head of security and go over the security procedures. After a little digging you find that employee-owned electronic devices such as cellular phones are allowed in and out of the facility. The company feels that the non-disclosure agreements in combination with security personnel monitoring everything on camera are strong enough to keep employees honest and that the cost of screening for electronic devices is too high. You tell the head of security that tomorrow morning security must seize every employee's electronic device as they enter the building.

The next morning you show up early and post yourself outside the entrance to the building. As people start to come into work their electronic devices are taken away. Eventually, you notice that someone walking up to the entrance immediately turns around and walks back to their car. You alert security and they find the person trying to stash away a cellular phone.

Later that morning, you download the contents of the cellular phone and find the files that were recently leaked. The employee confesses to everything and gives the details of how they did it. The files were stolen by transferring from the computers via a Bluetooth connection. Evidently, some of the computers came with Bluetooth and wasn't disabled by IT security. Using a Bluetooth connection didn't look conspicuous on camera, since there were no wires being plugged into the computer.

Therefore the company needs a way to detect cellular phones in the facility. There are a few existing cellular phone detectors on the market today that could of caught the employee prior to the information leaking out. However, this technology still needs a lot of improvement and development.

1.2 Cellular Phone Technology

Cellular phonetechnology is rapidly changing. Features like Bluetooth, USB, high resolution cameras, microphones, Internet, 802.11 wireless, and memory cards are added every year.Also, the communication technology a cellular phone uses such as CDMA, GSM, 3G, and 4G are rapidly changing.

1.2.1 Cellular Phone Features

Bluetooth is a secure wireless protocol that operates at 2.4 GHz. The protocol uses a master slave structure and is very similar to having a wireless USB port on your cellular phone. Devices like a printer, keyboard, mouse, audio device, and storage device can be connected wirelessly.This feature is mainly used for hands-free devices but can also be used for file transfer of pictures, music, and other data.

Universal serial bus (USB) is a way for cellular phones to connect to a computer for data transfer. This feature is very similar to Bluetooth for a cellular phone with the exception of using a cable. On today's cellular phones this feature is mainly used for charging the battery or programming by the manufacturer. It can also be used to transfer pictures, music, and other data.

Cameras on cellular phones are a very popular feature that was added in the last 10 years. In recent years, high resolution cameras have become a standard feature. Most cellular phones will come with at least a 2 mega pixel camera and the more expensive phones can be as much as 8 mega pixels.

Microphones have been featured on cellular phones since they first came out. In the last 10 years the microphones have become dual purpose;now there are programs on the phone that record voice to file such as a simple voice recorder or as part of a video.

Almost every available cellular phone today has a connection to the Internet. This allows users to transfer files and data wherever they are. Cellular phones can send emails, text messages, picture text messages, video text messages, and upload data to the Internet.

Some cellular phones come with 802.11 wireless built in and allows the phone to connect to any nearby wireless networks. This provides an alternate connection method to the Internet and saves money if you're on a limited data plan. Also, connecting with 802.11 is most likely going to provide better throughput than using the cellular phone network.

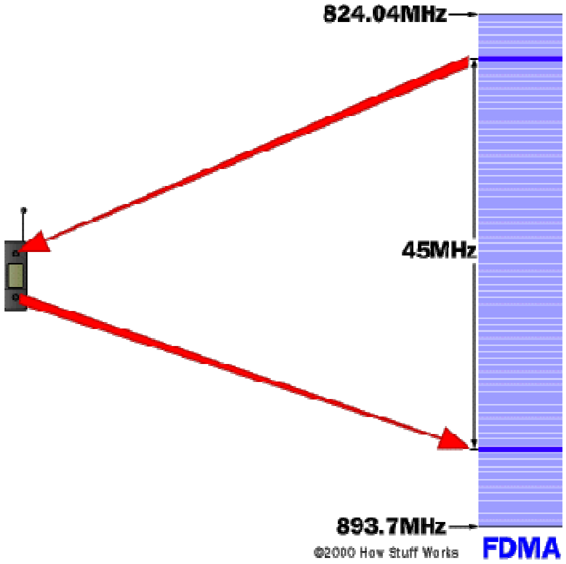
Since cameras and music have become popular features on cellular phones, manufacturers have started adding memory card slots. These memory cards provide expanded memory and allow more pictures to be taken or music files to be stored. Most memory cards can plug directly into the computer for easy data transfer.

All these features make cellular phones today very versatile. They can connect with almost any storage medium or computer. In the years to come, cellular phones will continue to gain more and more features.

1.2.2 Cellular Phone Communication Standards

Currently the three main technologies used by cellular phone providers are 2G, 3G, and 4G. Each generation of technology uses a different transmission protocol. The transmission protocols dictate how a cellular phone communicates with the tower. Some examples are: frequency division multiple access (FDMA), time division multiple access (TDMA), code division multiple access (CDMA), global system for mobile communications (GSM) , CDMA2000, wideband code division multiple access (WCDMA), and time-division synchronous code-division multiple access (TD-SCDMA). All of these protocols typically operate in the 824 - 894 MHz band in the United States. Some protocols, such as GSM (depending on the provider)will use the 1800 - 2000 MHz band [6].

Diagram 1



To provide a good example of how a cellular phone transmission works, take a look at Diagram 1 which shows how FDMA works. Each phone call uses a different frequency within the 45 MHz bandwidth. FDMA is normally used for analog transmissions and is capable of digital transmissions [6].

1.3 Secure Facilities

Many businesses such as psychiatric hospitals, correctional facilities, pharmeseutical companies, government facilities, and military bases rely on keeping information protected. They build security fortresses that shield their money making information from getting to the general public.These facilities have many computers that house the valuable information and are not connected to the Internet. Generally, access is restricted by guards with metal detectors and electronic devices are not allowed in or out without proper approval.

In every secure facility it is hard to ensure that employees and visitors aren't violating the policies. The only way to ensure someone isn't carrying a cellular phone is to search everyone as they enter and exit. This requires a great deal of manpower and most companies can't afford that level of security. Additionally, it will make the employees feel like the company doesn't trust them.

CHAPTER 2

BACKGROUND

2.1 Cellular Phone Detectors Available Today

To get a good grasp on what is available todaylet's take a close look at some off the shelf cellular phone detectors. Most detectors are manufactured with the intent that the cellular phone is stationary and powered on. They generally have the same features and it is questionable whether or not they actually detect a cellular phone.

The two most popular cellular phone detectors available on the market today are produced by Berkeley Varitronics Systems and Mobile Security Products. These companies produce the wolfhound cell phonedetector and Cellbuster respectively.

2.1.1 Berkeley Varitronics Systems Wolfhound Cellphone Detector

Berkeley Varitronics Systems wolfhound cell phone detector will detect PCS, CDMA, GSM, and cellular bands using RF signatures. It also has the capability to directionally find or locate cellular phones that are nearby. The wolfhound, according to the advertisement, can detect phones that are in standby mode, actively using voice, or data transmissions [2].

Wolfhound cell phone detector features [2]:

- 40 to 50 foot radius of coverage
- -60 dBm sensitivity
- Audible alert
- Vibrating alert
- One-handed operation
- Continually scans for cellular phone uplink activity
- Integrated laser-assisted directional antenna
- Estimated battery runtime of 18 hours

The Wolfhound on paper seems to be a great way to detect cellular phones, but may just randomly detect cellular phone communications in the area and not necessarily the phone or device that set it off. A couple of quotes from their advertisement imply this: "It took only two hours to find five cell phones that were either in use at the time or hidden in the jail cells on standby mode ready to take calls[2]" and "With only 30 minutes of operation, the device can detect many cell phones and identify the positions which led the team to find 10 mobile phones[2]." These two quotes suggest that their device is picking up transmissions in the area, but it doesn'tshow that they were directly from the phone they found or a phone at all.

Small print at the bottom of their advertisement reads, "Standby mode (autonomous registration) varies from base station to base station with phones typically registering between once every few minutes to up to 20 minutes. This time varies greatly based upon carriers, distance from base stations and individual handset manufacturer's standards [2]." This again casts some doubt that their equipment is easy to use and won't just be picking up random cellular transmissions or other devices in the area.Also searching the internet for reviews or feedback about the device produces no results. This uncertainty about whether the detecotr works makes the Wolfhound very similar to the Cellbusters cellular phone detector.

2.1.2 Cellbusters Cell Phone Detector

Cellbuster's cellular phone detector provides continuous monitoring for cellular phones and has a voice alert that tells the user to shut their phone off if detected. The Cellbuster only receives and doesn't transmit, making it great for areas sensitive to cellular phone usage. It will also detect phones that are in standby mode [1].

Cellbusters cell phone detector features [1]:

- Detect and prevent unauthorized cellular phone usage
- Detects analog and digital cellular phones CDMA, TDMA, GSM, and PCS/PCN types
- Range adjustment
- Audio alert asks cellular phone users to switch off their phone

- Red alert light flashes brightly to attract attention
- Detects when a phone is switched on and not in use
- Easy to configure and simple to install

This cellular phone detector sounds like it would work wonderfully for keeping people from bringing their phones into a secure facility. However, the advertisement isn't very honest. It doesn't tell you that a cellular phone may take up to 20 minutes to detect if it is in standby and that the phone needs to be on. Also, just like the Wolfhound, it doesn't provide any guarantee that it won't just detect random transmissions in the area.

To show how inaccurate today's cellular phone detectorsare, a Cellbusters detector was borrowed from a local business and tested as part of this study. Using two LG VX11000 GSMcellular phones, this cellular phone detector was tested extensively. Following is a synopsis of the testing:

Test 1 - Outside Faraday Cage at Home with Cellular Phones Turned On

- Tried cell detector sensitivity set low and high for 20 minutes each - detector didn't activate

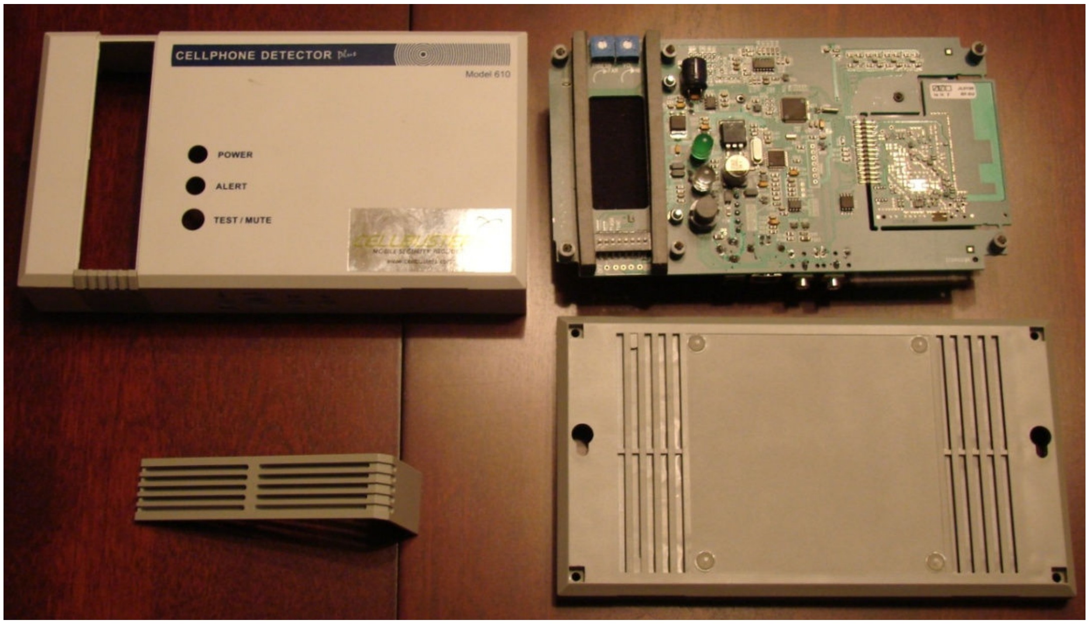
- Called one phone from the other and left on for 5 minutes - detector didn't activate
- Texted one phone from the other - detector didn't activate
- Detector doesn't appear to work in public area with the sensitivity set high or low
- Detector activated randomly and generally not during a phone call

Test 2 - Inside Faraday Cage at University of Nebraska Omaha with Signal Generator Set to 832 MHz

- Tried cellular detector sensitivity set low and high for 10 minutes each - detector didn't activate
- Tried varying the frequency from 100 MHZ to 1 GHz - detector didn't activate
- When set to high and open Faraday cage door it wouldalarm sometimes

Testing this cellular phone detector led to a few conclusions. The Cellbusterscellular phone detector doesn't work very well and it is questionable that the detector works at all. Using this device in a public area the detector just randomly went into alarm and didn't indicate where to go or what to do. Testing indicates that the Cellbusters cell phone detector doesn't work as advertised.

To get an idea of the circuitry required to build a cellular phone detector, it was dismantled. Following are some pictures of the internal components.



After taking a close look at the circuitry used, no conclusions were drawn on exactly what technique of signal detection was used. Cellbusters most likely used some digital signal processing to identify the signal characteristics of a cellular phone.

A study performed by the U.S. Department of Energy pointed out that 2 of the 5 reviewers of the product reported that it didn't work. In October 2007 when the study was performed, the Cellbusterscellular phone detector cost $755 each and were backordered [3].

2.2 Related Work

Since cellular phone detection is a more recent problem, there are only a few articles that have already researched this area. Two articles were published in 2007 and provide good analysis. The first article, "Detecting and Locating Cell Phones in Correctional Facilities," was written by EVI Technology, LLC. The second article, "Cell Phone Detection Techniques," was written by a Contractor hired by the U.S. Department of Energy (DOE).

2.2.1 Detecting and Locating Cell Phones in Correctional Facilities

This article details the growing problem with cellular phones in correctional facilities and lays out the constraints used to develop their solution. According to the research, cellular phones in a correctional facility are used to operate criminal enterprises, threaten witnesses, harass victims, plan uprisings, and undermine security. Their problem is monitoring, controlling, and locating cellular phones in a correctional facility [4].

EVI's possible solutions include physical search, non-linear junction detectors, signal jamming, shielding, network provider location based screening, RF detection, and their custom proprietary solution. They rule out all solutions but their own custom solution that uses a system of networked sensors that are controlled by a central computer. EVI uses proprietary software that determines the cell phone's location and detects any RF emissions. The location of detected cellular devices is displayed on a facility map [4].

This solution was developed for detecting cellular phones in a prison. It relies on the cellular phone remaining stationary which, in prison facilities makes sense since movement is limited. EVI's detection system finds cellular phones after they have already been in the facility for at least 30 minutes or if someone is making a cell phone call.EVI doesn't provide any details on the signal detection technique used since it is all proprietary. Also, there are no reviews or articles stating that this system works as advertised.

2.2.2 Cell Phone Detection Techniques

This study examines detecting cellular phones when a person is entering a secure facility or cellular phone restricted area. The detection technique studied requires measuring a cell phone's electromagnetic properties and determining an identifiable signature. Measuring the RF spectrum around 240 - 400 MHz (outside the cellular phone band) shows the most potential [3].

The DOE Contractor recommends developing a cellular phone detector by measuring the RF spectrum. Spurious emissions from cellular phones are monitored and recorded when the phone is in standby or transmitting [3].

Using this method has some advantages[3]:

- No external signal required for detecting the phone
- The band of frequencies is limited by the FCC and are likely to be used by most manufacturers
- System could potentially detect more than cellular phones

- This method should work on future generations of cellular phones
- System could potentially detect cellular phones even when they are off

The authors lay out a proposed path forward for determining if this technique is possible and perform some preliminary testing of their own. They also provide an alternative path that would detect cellular phones based off of their RF reflecting material in the cellular phone filters on all phones. Cellular phones could then be detected whether they are on or off [3].

This research article also mentioned an evaluation that was conducted in 2003 on the available commercial cellular phone detectors. Bechtel-Nevada and Sandia National Labs found that none of the detectors at the time were effective when the phone was off or in standby mode [3].

CHAPTER 3

PROBLEM STATEMENT

The latest threat to information dependent businesses is the cellular phone. The technology added to cellular phones in the last 15 years has made them a jack-of-all - trades for information storage and transmission. Features like Bluetooth, USB, micro USB, high resolution cameras, microphones, internet, and 802.11 wireless make cellular phones perfect for stealing data.That is why a method to detect cellular phones in a secure facility is needed.

The main problem with ensuring that a cellular phone isn't in a secure facility is that an accurate method for detecting them doesn't exist. The only way to be certain is to perform full body searches on a regular basis.

Most cellular phone detectors available today only alarm if there is a cellular phone or transmission device in the general area. They appear to alarm randomly and aren't very accurate.

Detecting a cellular phone signal using an accurate signal detection technique is the focus of this research and can be solved by using a down converter in conjunction with a bandpass filter. The technique is more accurate and provides signal detection at a lower frequency, making it easier to work with.

If this solution was implemented, it would greatly reduce the risk of cellular phones getting into secure facilities. Businesses and government would save a lot of money on security. The solution would also greatly reduce the risk of their data leaking to the general public and losing even larger amounts of money.

CHAPTER 4

PROPOSED SOLUTIONS

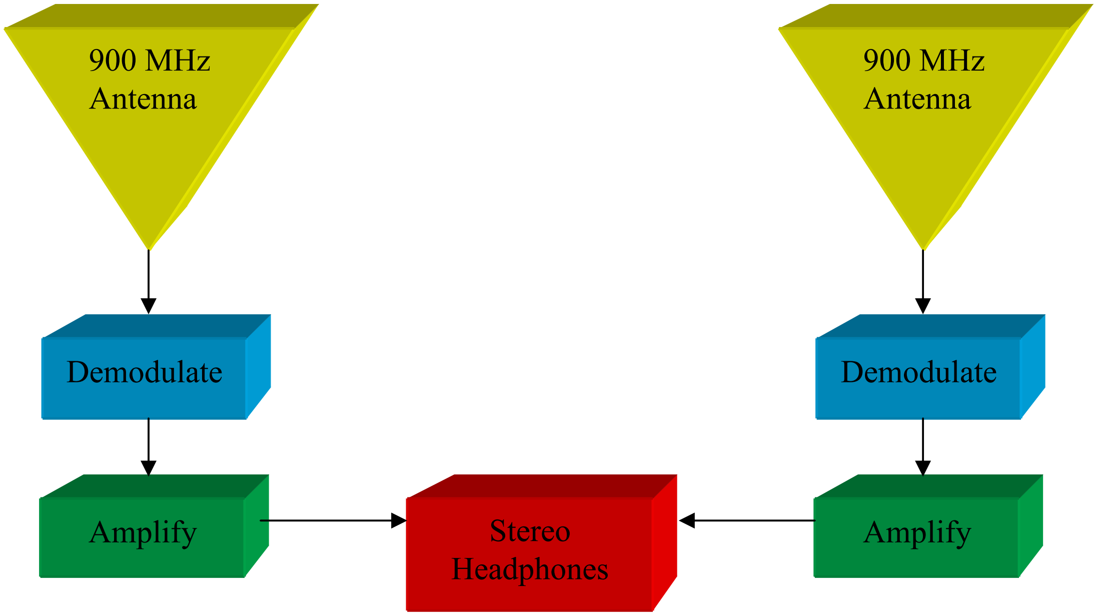
4.1 First Technique -FromCircuit-Projects.com [5]

4.1.1 Design Description

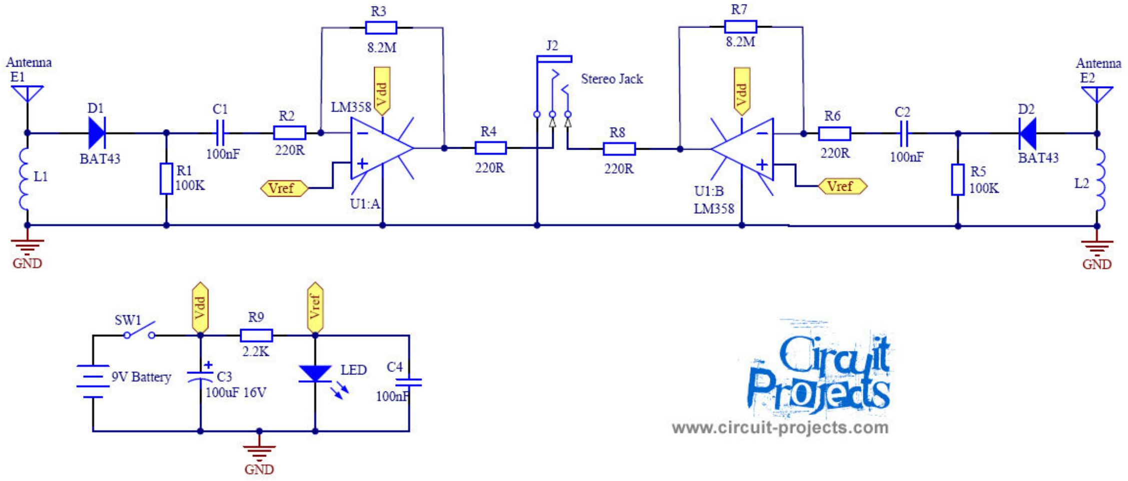
The first techniqueexplored is an existing design from circuit-projects.com. This design can detect Global System for Mobile Communication (GSM) signals at 900 MHz [5].

The design consists of two signal detectors each with their own dipole antenna, inductor, and diode. Each dipole antenna is tuned to 900 MHz. When the antennas resonate at 900 MHz a charge is induced in the inductor. A diode then demodulates the signal, which is amplified by an op amp and passed along to a 3.5mm headphone jack. The design doesn't describe what sound you will hear when a cellular phone is being used. A schematic and parts list were provided [5].

4.1.2 Block Diagram



4.1.3. Schematic [5]



4.1.4. Component List [5]

R1, R5 : 100K 1/4W Resistor

R2, R6 : 1k 1/4W Resistor

R3, R7 : 8.2M 1/4W Resistor

R4, R8 : 220 Ohm 1/4W Resistor

R9 : 2.2K 1/4W Resistor

D1, D2 : BAT43 Schottky Diode

C1, C2, C4 : 100nF Polyester Capacitor

C3 : 100uF 16V Electrolytic Capacitor

L1, L2 : See Text

U1 : LM358

J1 : 8 Pin Socket

J2 : Stereo Jack

1 x 9V Battery

1 x 9V Battery Socket

1 x LED

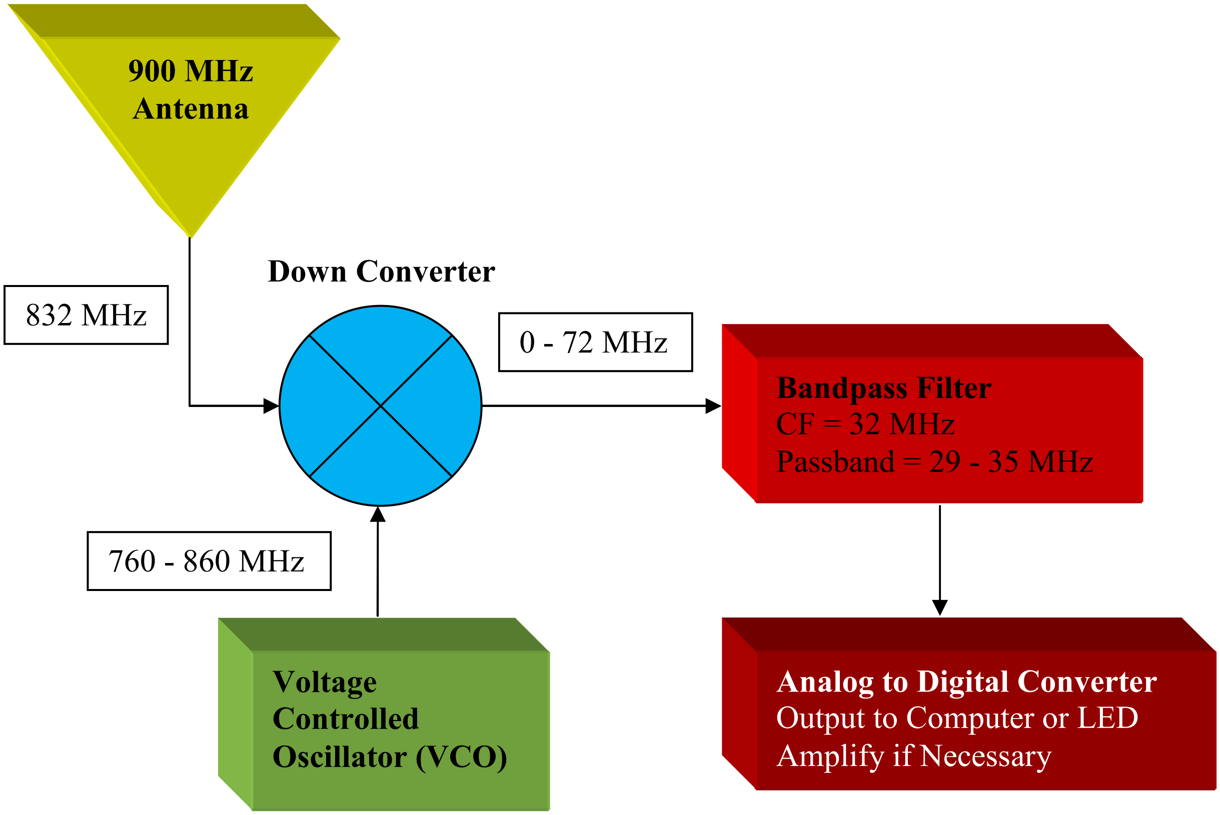
1 x On/Off Switch

4.2 SecondTechnique - Down Converter with Bandpass Filter

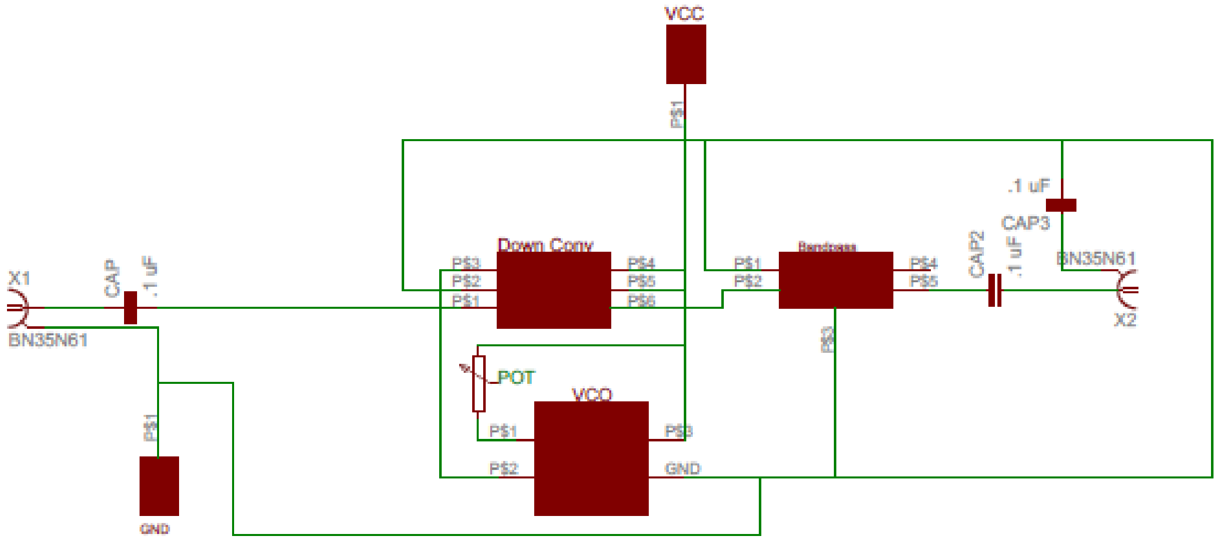
4.2.1 Design Description

Using a down converter, voltage controlled oscillator (VCO), and a bandpass filter is the second technique explored for cellular phone detection. Two signals are inputted into the down converter. The first signal is from the antenna and is between 829 - 835 MHz depending on the cellular phone (832 MHz for this expierment). The other signal is from the VCO, which is tuned to 800 MHz. The down converter multiplies the two signals together producing the sum and the difference. This is then filtered by a bandpass filter with the passband lower and upper edges respectively at 28 MHz and 36 MHz.Filtering eliminates the sum of the signals and any environmental noise. Now all that remains is the difference, a 29 - 35 MHz signal that indicates an active cellular phone is in the area. This can easily be converted using analog to digital converters and output to an alarm or computer.

4.2.2 Block Diagram



4.2.3 Schematic



4.2.4 Component List

SI MMICDownconverter : RF = 0.1 GHz to 2.0 GHz

IF = 20 MHz to 300 MHz

EPCOS SAW Bandpass Filter : BW = 6.0 MHz

CF = 36.125 MHz

Lower Sidelobe = 32 MHz

Upper Sidelobe = 40 MHz

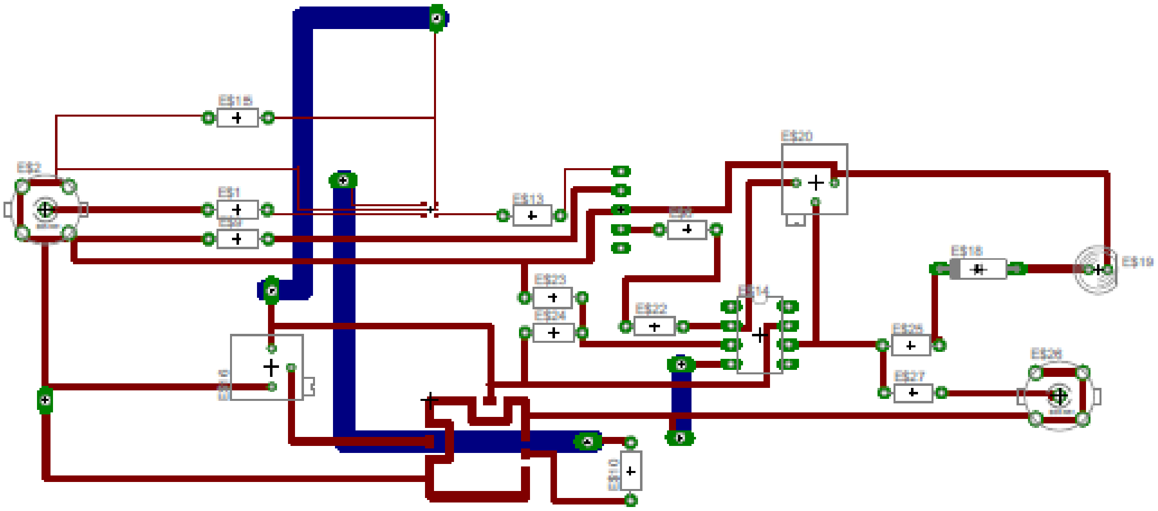
Crysteck Voltage Controlled Oscillator :760 - 860 MHz

Potentiometer : 10K Ohm

BNC Connectors: 2 Surface Mount

100pF Capacitor : 3 for decoupling

4.2.5 PCB Layout



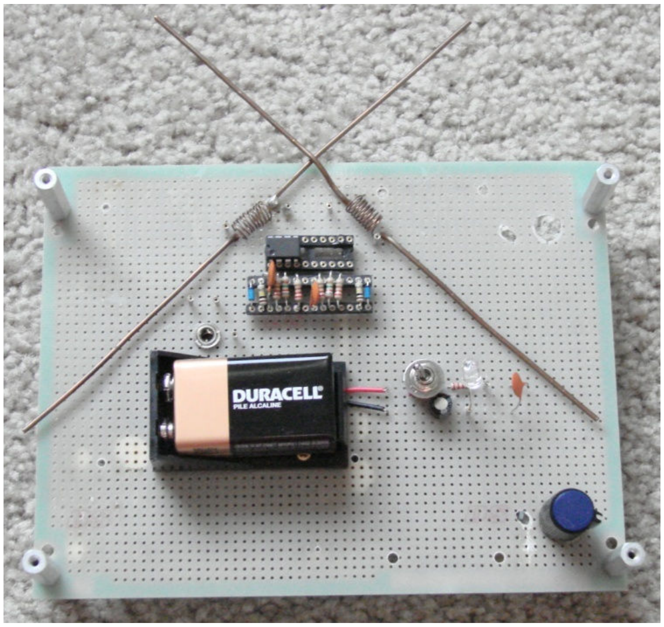
CHAPTER 5

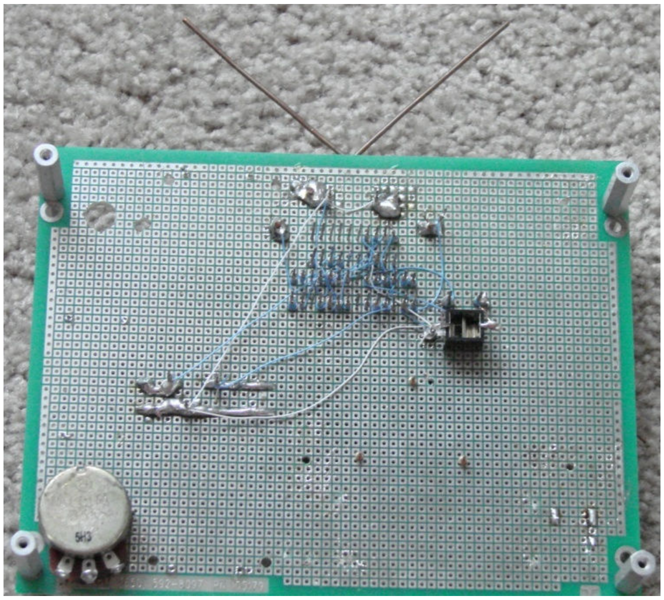
RESULTS

5.1. First Technique - From Circuit-Projects.com [5]

5.1.1. Implementation

For this implementation a breadboard and wire wrapped connections were used. This was done so that it would be easier to change connections later.Following are some pictures of the wire wrapped cellular phone detector that was constructed and tested.





5.1.2. Testing

The first test with this cellular phone detector was to just have an active cellular phone in the room. So the LG cellular phone was turned on and a phone call was placed with the detector nearby. Absolutely nothing came out of the connected headphones. To troubleshoot this problem, the circuit was tested with a spectrum analyzer and signal generator. The antenna was connected to the signal generator at 900 MHz with 10dB of amplitude and the spectrum analyzer was connected to the headphone jack using the available probes (only 500 MHz was available). Injecting the 900 MHz signal into the antennas resulted in a lower amplitude signal on the output.

To test whether the circuit was resonating at 900MHz, a bandpass test was performed by stepping the frequency at 100 MHz intervals from 600 MHz to 1.2GHz. The amplitude changed at each interval, but was actually lower at 900 MHz than anywhere else and didn't have a bandpass response. The wire wrapped connections may have changed the impedance of the circuit.

While testing this cellular phone detectorit was discovered that the spectrum analyzer was able to detect the LG cellular phone only using a 500 MHz probe. When talking on the cellular phone, the spectrum analyzer spiked at 832 MHz. This gavea frequency range to design around for this cellular phone and is in the range of a GSM phone.

5.1.3 Design Conclusions

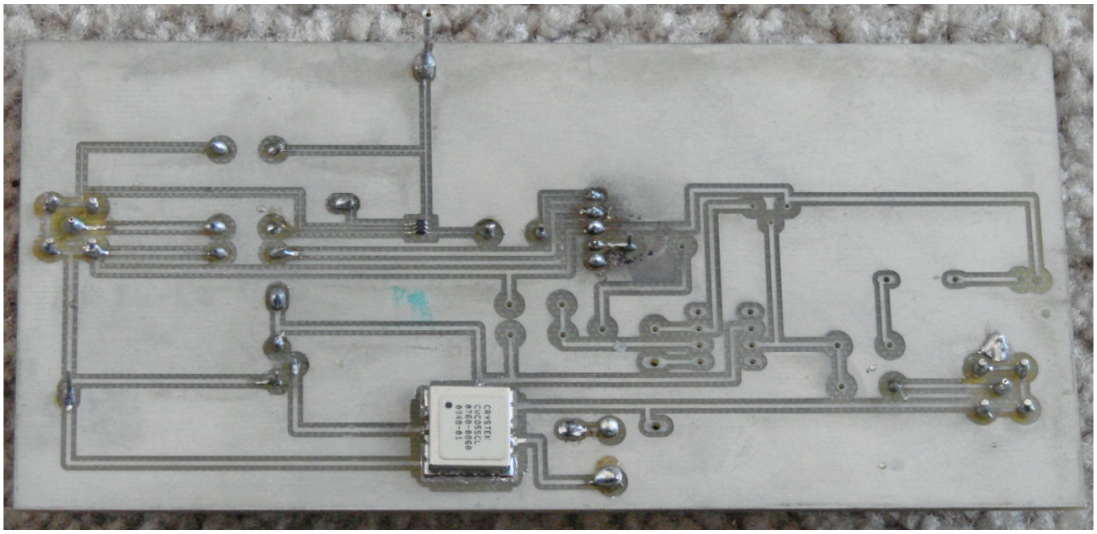
After testing, it was decided that this design was not the most efficient. A better design would have BNC connectors on the input and output for easy connection to antennas, spectrum analyzer, and signal generator. It would also eliminate the need for 1 GHz probes by just using a simple BNC coax cable.

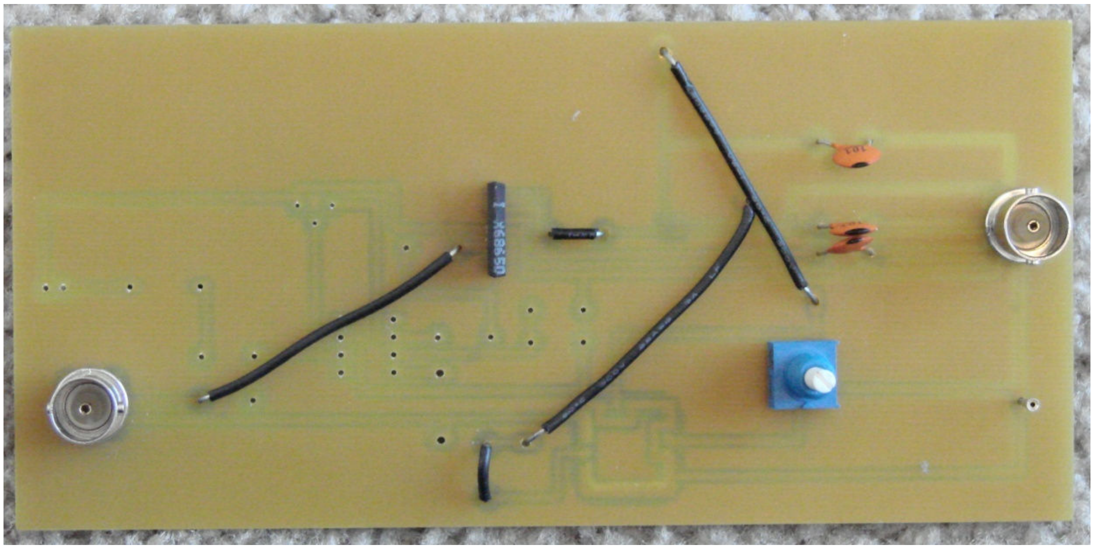
Building this design brought about the decision to go another route and not rebuild the circuit using a PCB. Instead after some more research it was found that using a using a down converter would make the design easier to work with by providing a signal at a lower frequency.

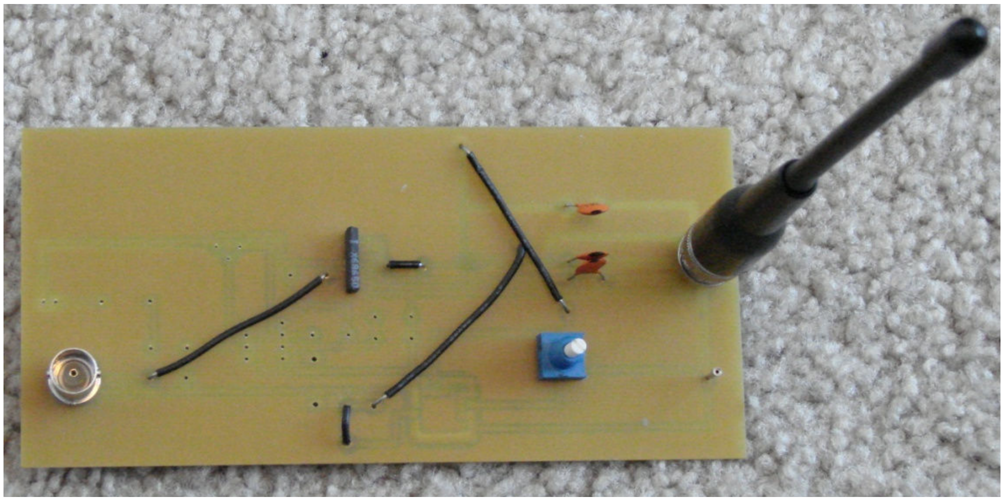
5.2. Second Technique - Down Converter with Bandpass Filter

5.2.1. Implementation

Learning from the first technique, a PCB made more sense for this implementation. This would provide very solid connections and cut down the impedance. Also, surface mounted BNC connectors were used for the input and output to allow easy connection to the spectrum analyzer, signal generator, or antenna. Following are pictures of the board that was constructed.







5.2.2. Testing

This design was tested in the lab and proven by computer simulation. Lab testing was conducted using a spectrum analyzer and signal generator. The computer simulation was done in MATLAB, Advanced Design Software (ADS), and Orcad Cadence PSpice.

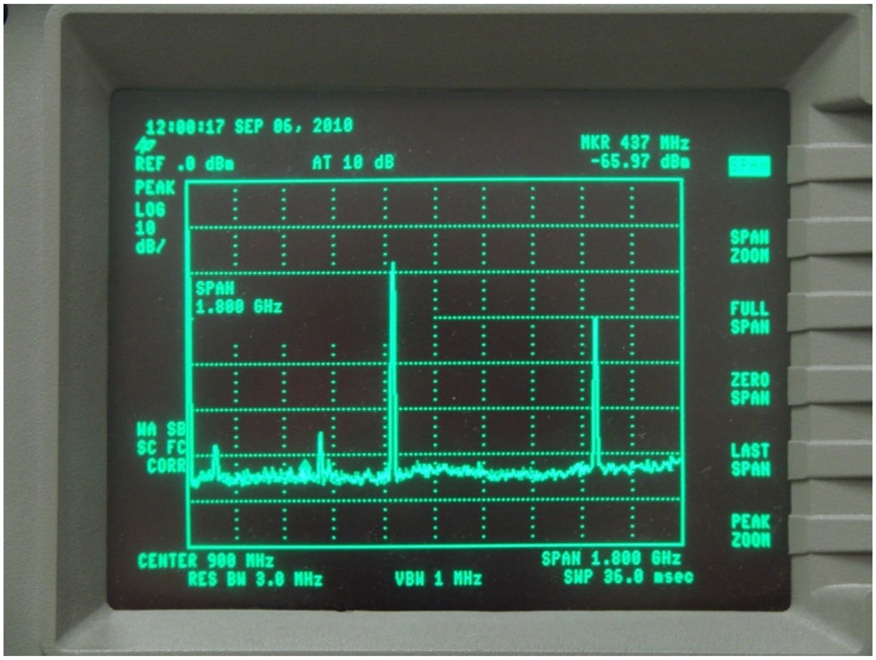
5.2.2.1 Lab Testing

Testing was performed using a signal generator and spectrum analyzer connected respectively to the input and output using BNC coax cables. The signal generator used is aHewlett Packard 8648B capable of signals between 9 kHz - 2000 MHz. As for the Spectrum analyzer, it was an Agilent 8591E capable of detecting signals between 9 kHz - 1.8 GHz.All testing was conducted with the spectrum analyzer set to a center frequency of 900 MHz & span of 1.8 GHz. Three different tests using this equipment were conducted.

The first test checked to see if the VCO was working properly. Figure 1 shows the frequency spectrum with the signal generator turned off.The output of the VCOis at 760 MHz andanother signal is shown around1.5 GHz (the 2nd harmonic of the VCO).

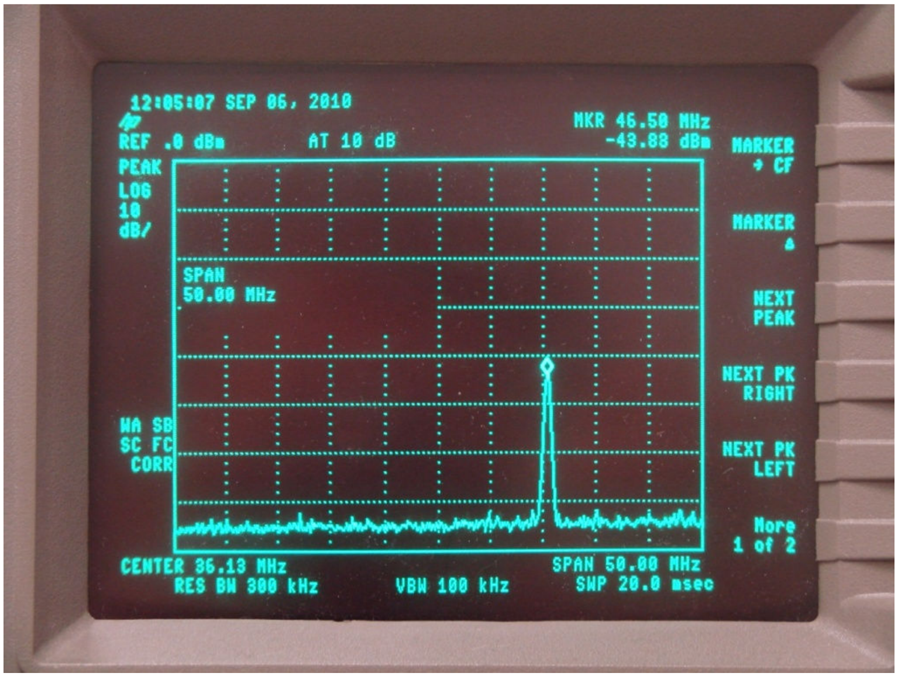
The remaining signals are from environmental noise. According to this data, the VCO is working correctly.

Figure 1



The second test checked to see if the down converter worked in conjunction with the band pass filter. Figure 2 shows the output of the bandpass filter. The expected output should be a bandpass response centered at 36.125 MHz. After adjusting the VCO up and down in frequency, thebandpass response was centered at 46 MHz. This frequency should be getting cut off by the bandpass filter.

Figure 2

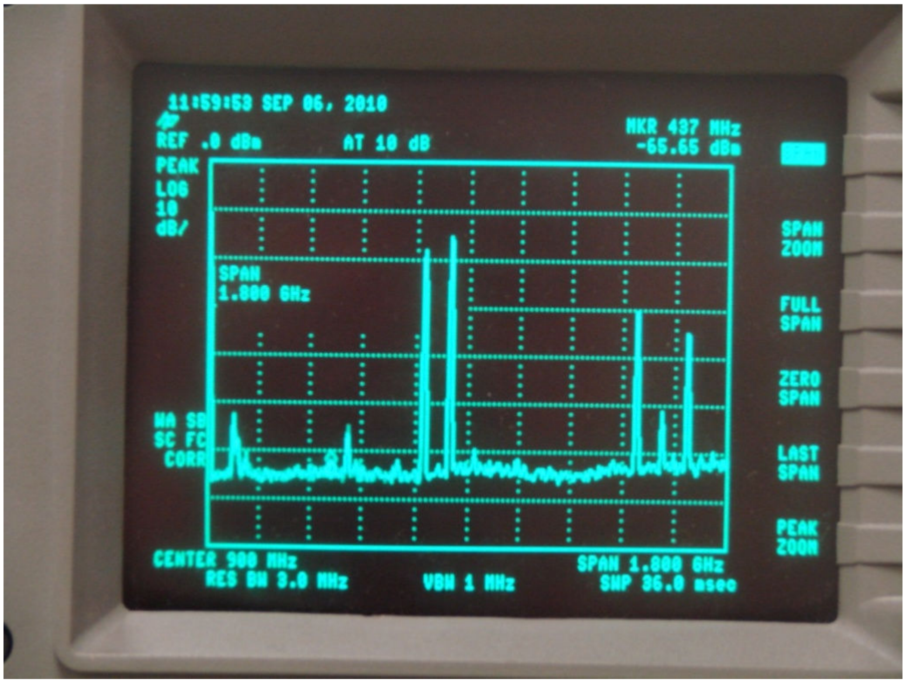


The third test was to see if the bandpass filter was working at all. Stepping the signal generator at 100 MHz increments from .1 to 1.5 GHz confirmed that the bandpass filter is letting everything through. Figure 3 shows the output of the circuit with the signal generator set to 832 MHz.

To remedy this problem the following solutions were attempted: lowering the signal generator's output to 1 dB, replacing the bandpass filter chip, and removing the capacitors between the VCO and bandpass. None of these solutions seemed to fix the problem, so another test on thebandpass filter was performed alone on a breadboard. The test was conducted by slowing increasing and decreasing the signal generators frequency from 1 to 100 MHz. The bandpass once again allowed everything to get through and may have been due to crosstalk between the connections.

According to this data, everything in the circuit was working correctly except for the bandpass filter. After researching this problem further it was determined that a computer simulation at this frequency would be less costly. Since, purchasing a bandpass filter specifically made for this frequency range can cost 500 – 1000 dollars and building one with the available lab equipment would be very time consuming.

Figure 3



5.2.2.2 Computer Simulation

A simulation of the circuit in MATLAB, Advanced Design System (ADS), and OrcadPSpicewas created to show that this technique is very effective. The MATLAB simulation shows that mathematically the circuit work correctly.

5.2.2.2.1 MATLAB Simulation

The following MATLAB code multiplies an 800 MHz sinusoid (VCO) and an 832 MHz sinusoid (input from signal generator) together. It then filters the output using a bandpass filter impulse response with a center frequency of 32 MHz and frequency passband of 29 - 35 MHz.

MATLAB Code

```
Fs = 4000;                    % Sampling frequency
T = 1/Fs;                     % Sample time
L = 1000;                     % Length of signal
t = (0:L-1)*T;                % Time vector

% Product of a 800MHz sinusoid and a 832 MHz sinusoid
X = sin(2*pi*800*t) .* sin(2*pi*832*t);
% Generate bandpass filter response
[b,a] = butter(1,[0.014 0.018]);
% Filter bandpass response from product X
x = filter(b,a,X);

% Plot of bandpass filter impulse response.
figure;
freqz(b,a,L,4000000000);
title('Bandpass Filter Impulse Response')

NFFT = 2^nextpow2(L); % Next power of 2 from length of y
Y = fft(x,NFFT)/L; %Filtered
R = fft(X,NFFT)/L; %Not Filtered
f = Fs/2*linspace(0,1,NFFT/2+1);

% Plot without bandpass filter.
figure(3);
plot(f,2*abs(R(1:NFFT/2+1)));
title('Graph of Frequency Spectrum - Unfiltered')
xlabel('Frequency (MHz)')
ylabel('dB')

% Plot with bandpass filter.
figure(2);
plot(f,2*abs(Y(1:NFFT/2+1)));
title('Graph of Frequency Spectrum - Filtered With Bandpass')
xlabel('Frequency (MHz)')
ylabel('dB')
```

Figure 4 shows the frequency spectrum after the two signals have been multiplied together. This produces the sum and the difference of the signals at 1632MHz and 32 MHz respectively. The output from MATLAB is very similar to the down converter used on the circuit board. Looking at Figure 3 from the output of the bandpass filter, signals in the range of the sum and difference can be seen.

Figure 4

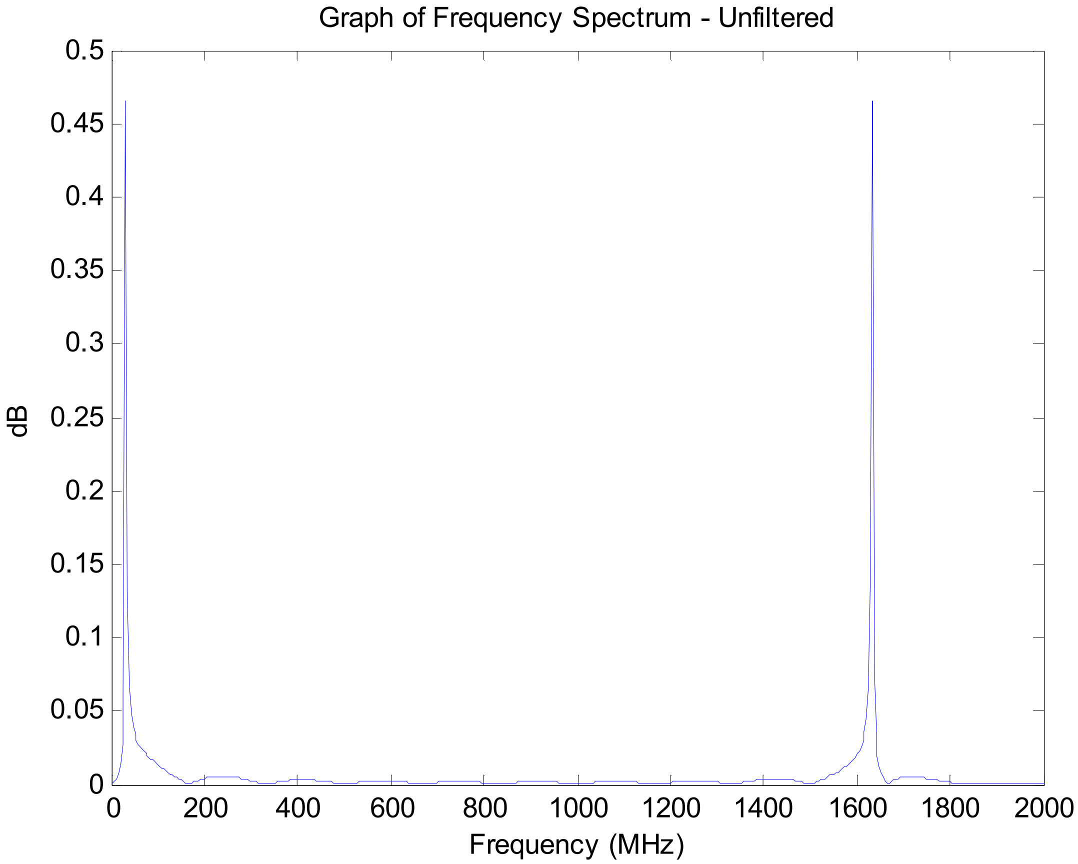


Figure 5 shows the impulse response of the bandpass filter that was designed in MATLAB. The filter peaks at 32 MHz and cuts all other signals down significantly as it increases or decreases in frequency.

Figure 5

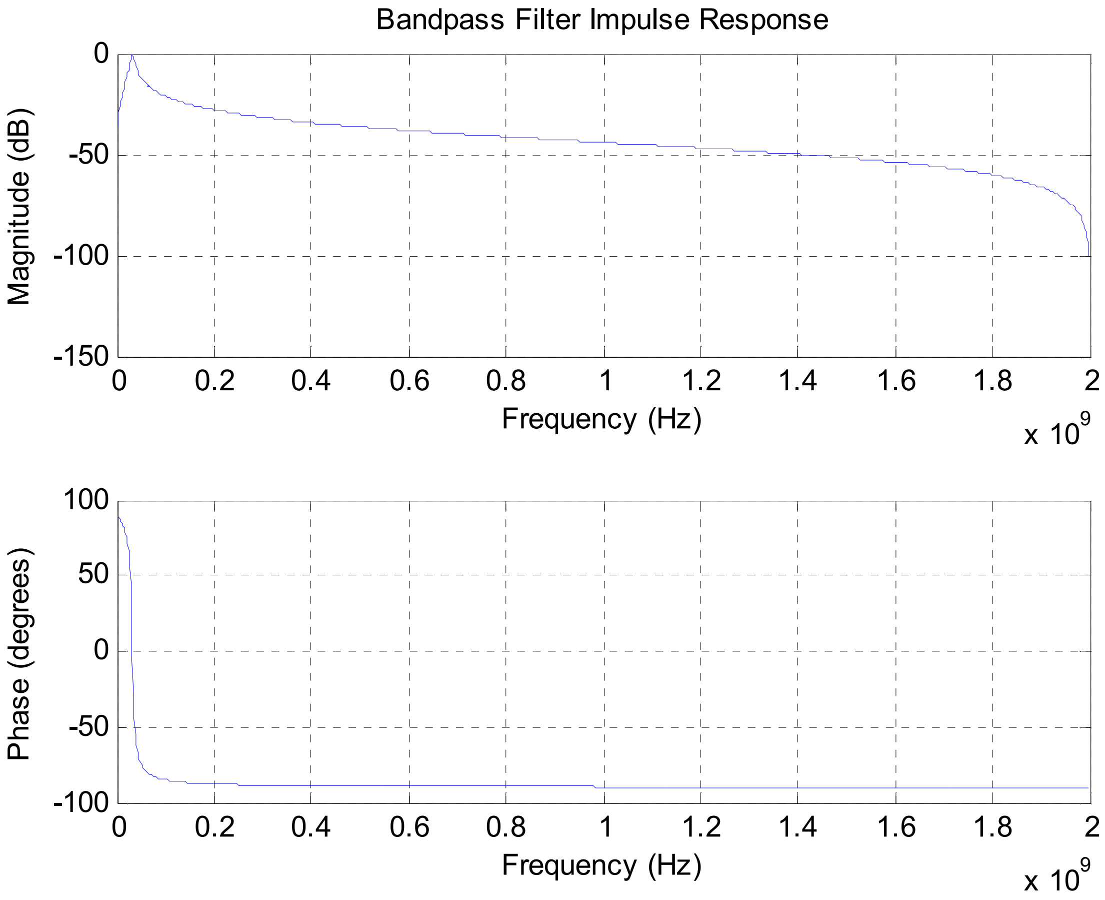
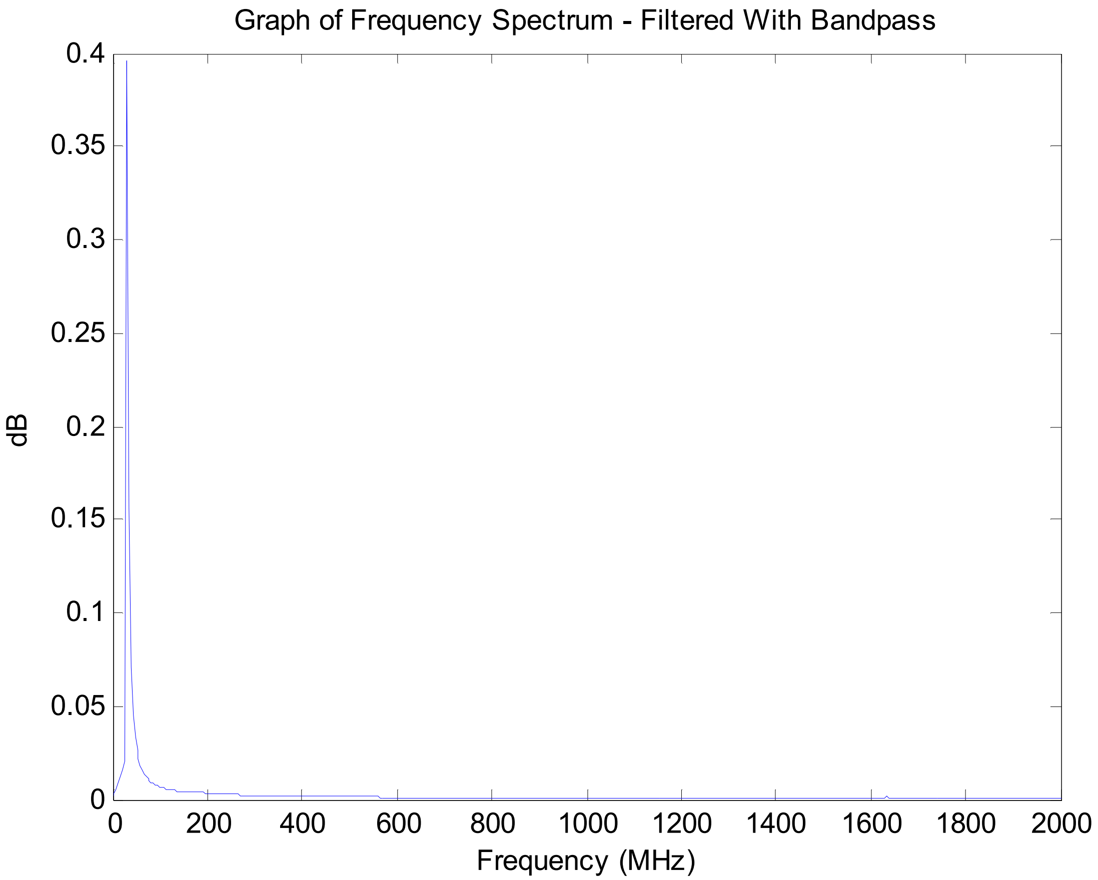


Figure 6 shows the output of the bandpass filter. All signals except for the 32 MHz signal have been cutoff. This proves that a down converter in combination with a good bandpass filter will mathematically work for detecting a cellular phone.

Figure 6



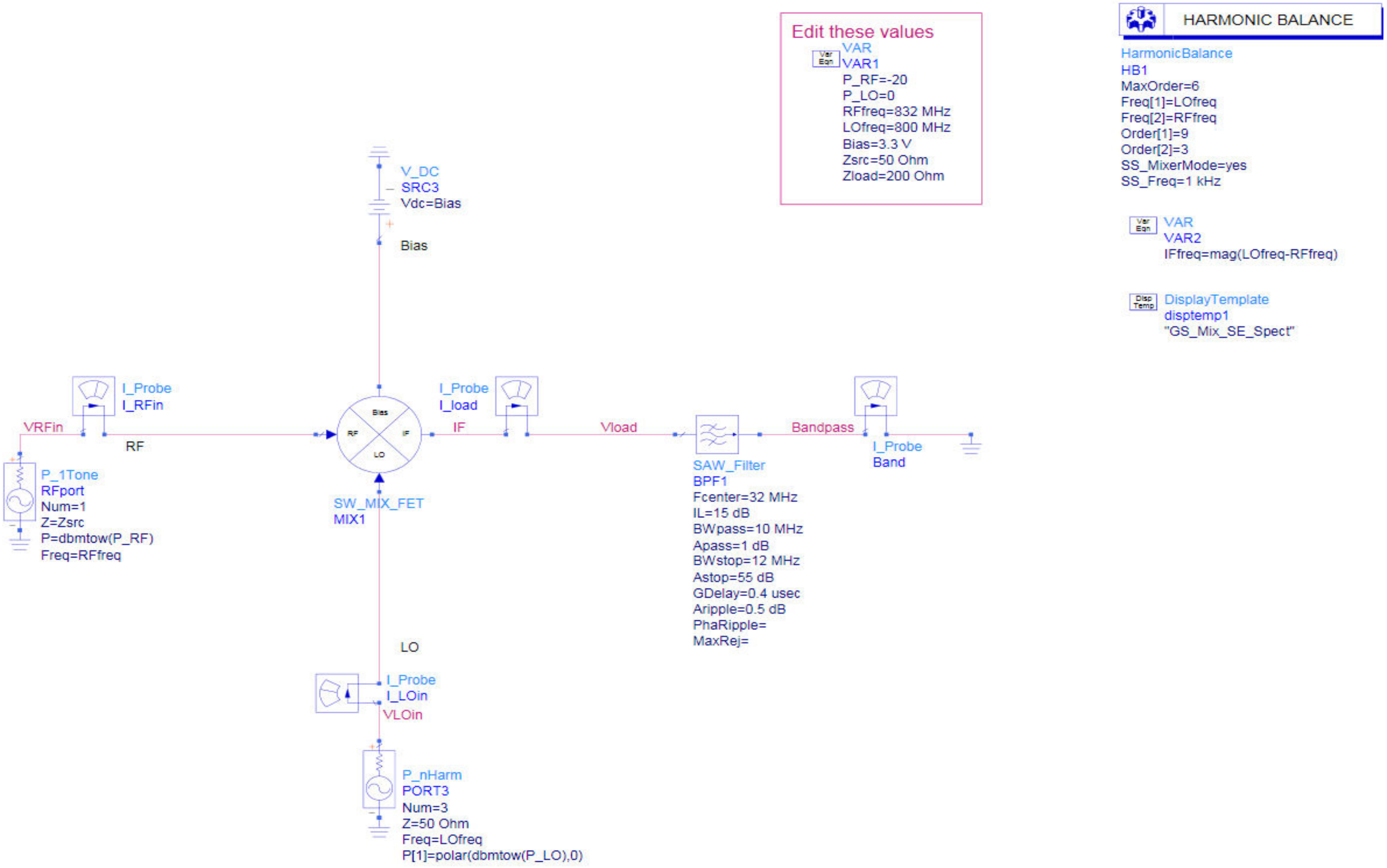
5.2.2.2.2 Advanced Design System(ADS) Simulation

The following simulation in ADS shows how the down converter works with the bandpass filter in a circuit. Figure 7 is a schematic of the simulated circuit which includes an RF input (input from the antenna), a LO input (voltage controlled oscillator input), down converter, and bandpass filter.

Figure 8 shows the output of the circuit withan RF input signal at 832 MHz. The input spectrum graph shows a LO signal at 800 MHz and an RF signal at 832MHz. The mixer output spectrum shows the sum inputs, difference of the inputs, and the original input signals. The bandpass output spectrum graph shows the frequency spectrum from 0 – 7.5 GHz. All signals except the 32 MHz difference of the two signals have been eliminated.

Figure 9 shows the output of the circuit with an RF input signal at 900 MHz. The bandpass output spectrum graph shows that all frequencies above 838 MHz are eliminated. Figure 10 shows that all frequencies below 826 MHz are eliminated.

Figure 7 – Advanced Design System Simulation Schematic



Edit these values
VAR
VAR1
P_RF=-20
P_LO=0
RFfreq=832 MHz
LOfreq=800 MHz
Bias=3.3 V
Zsrc=50 Ohm
Zload=200 Ohm

HarmonicBalance
HB1
MaxOrder=6
Freq[1]=LOfreq
Freq[2]=RFfreq
Order[1]=9
Order[2]=3
SS_MixerMode=yes
SS_Freq=1 kHz

VAR
VAR2
IFfreq=mag(LOfreq-RFfreq)

DisplayTemplate
disptemp1
"GS_Mix_SE_Spect"

V_DC
SRC3
Vdc=Bias

I_Probe
I_RFin

I_Probe
I_load

P_1Tone
RFport
Num=1
Z=Zsrc
P=dbmtow(P_RF)
Freq=RFfreq

SW_MIX_FET
MIX1

SAW_Filter
BPF1
Fcenter=32 MHz
IL=15 dB
BWpass=10 MHz
Apass=1 dB
BWstop=12 MHz
Astop=55 dB
GDelay=0.4 usec
Aripple=0.5 dB
PhaRipple=
MaxRej=

I_Probe
Band

I_Probe
I_LOin

P_nHarm
PORT3
Num=3
Z=50 Ohm
Freq=LOfreq
P[1]=polar(dbmtow(P_LO),0)

Figure 8 – 832 MHz RF Frequency

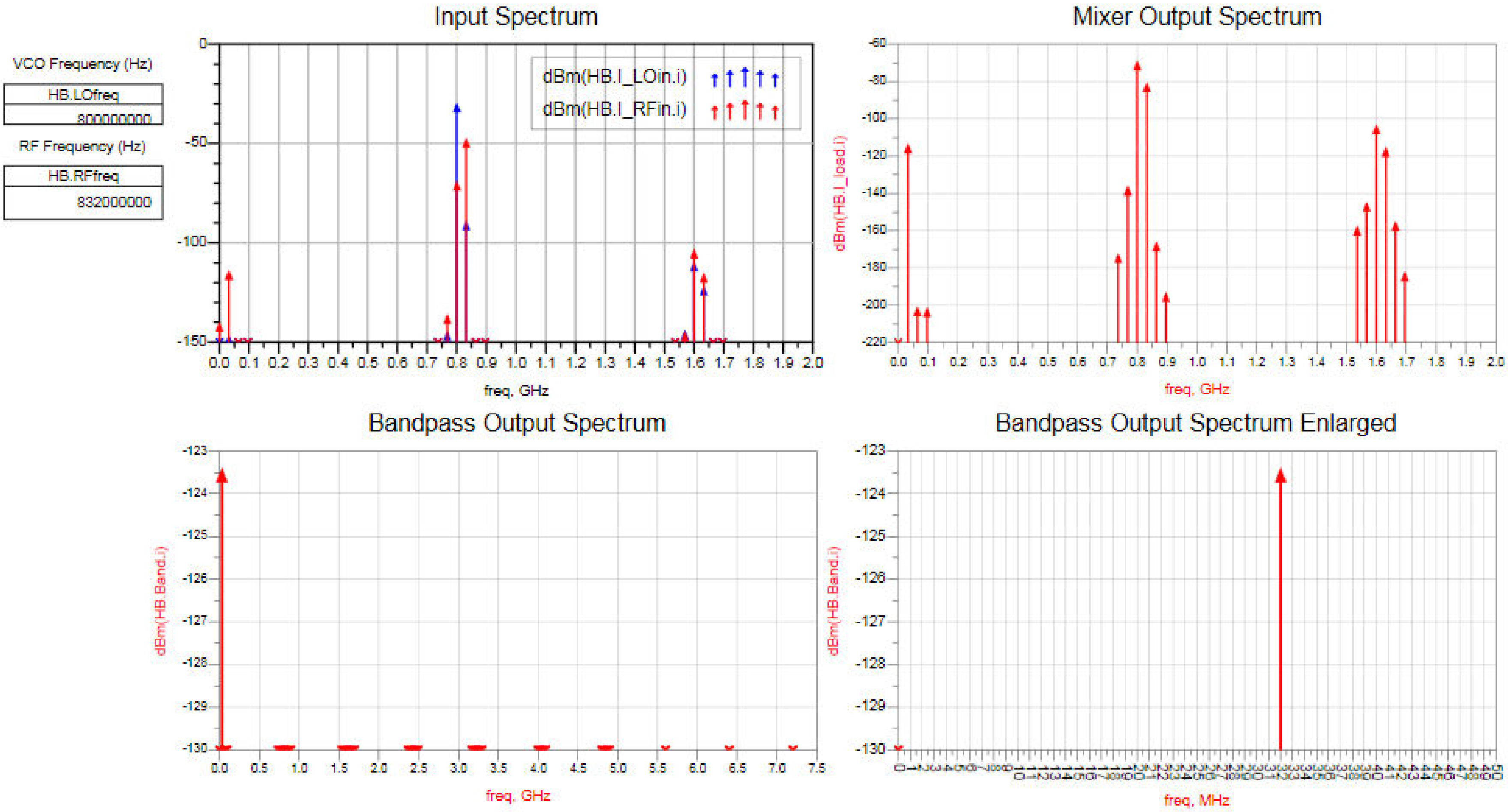


Figure 9 – 900 MHz RF Frequency

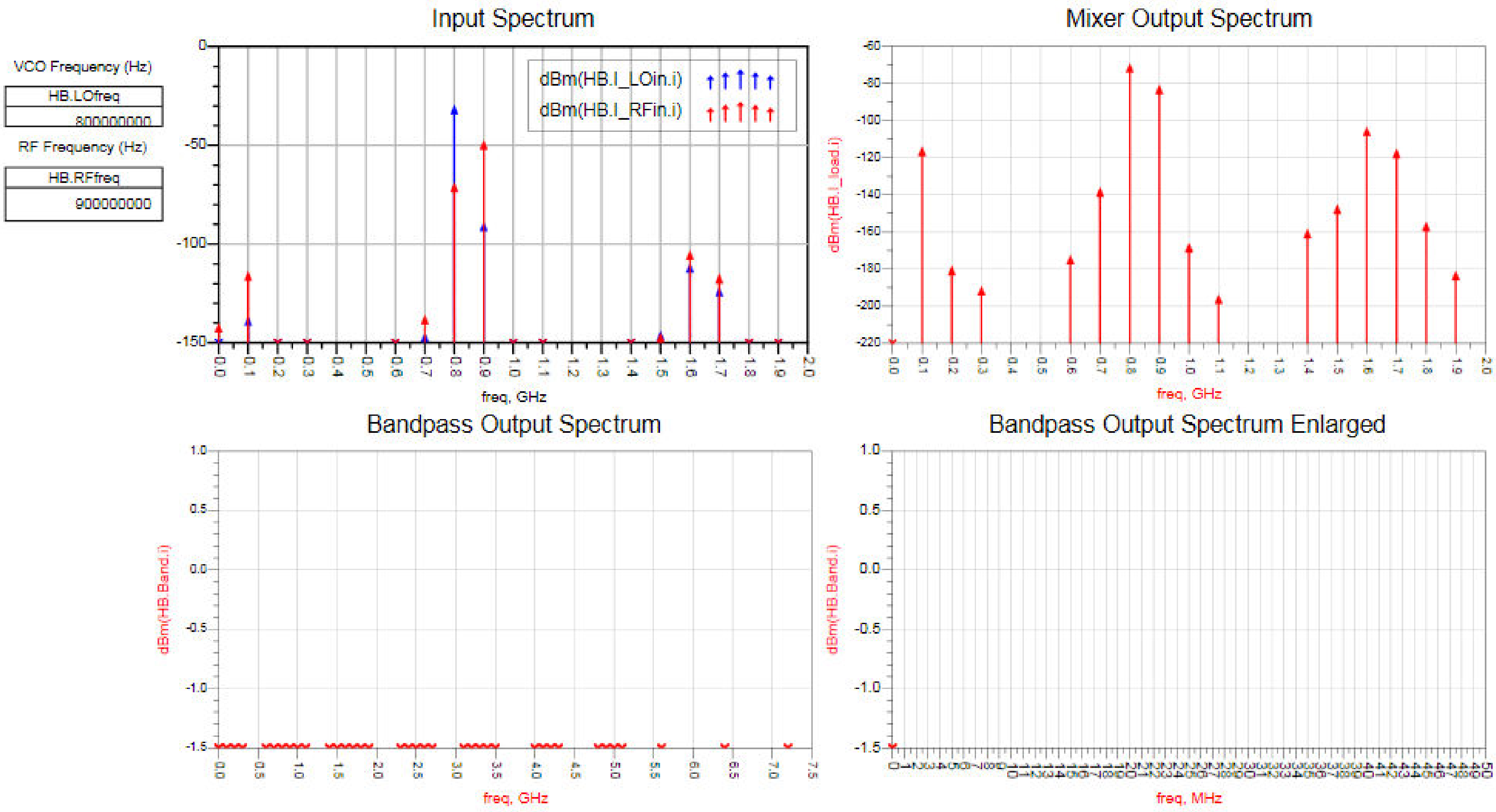
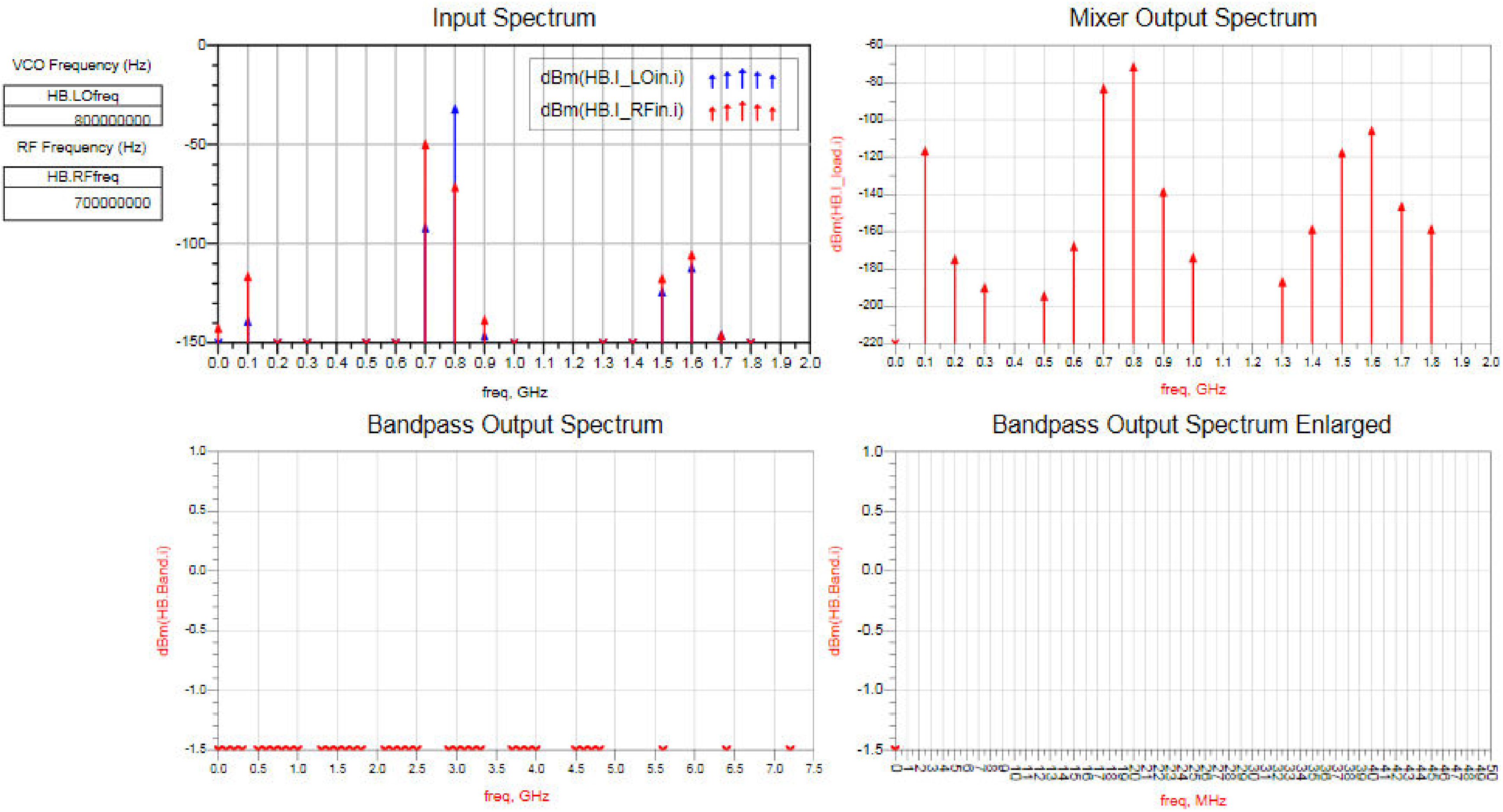


Figure 10 – 700MHz RF Frequency



VCO Frequency (Hz)

HB.LOfreq

800000000

RF Frequency (Hz)

HB.RFfreq

700000000

5.2.2.2.3 OrcadPSpice Simulation

After filtering out the signal it needs to be converted to a digital output. This will allow easy connection to a computer or display. Figure 11 is the schematic for the analog to digital converter. It consist of two 100 nF capacitors and a diode. The diode only allows the positive part of the AC wave to pass through while the two capacitors smooth the wave out to a steady DC voltage. The top graph in Figure 12 (voltage vs time) shows the 32 MHz signal as it leaves V1. Figure 12 bottom graph shows the signal after the diode and two capacitors have converted it to a DC voltage around 4 volts.

Figure 11 – Analog to Digital Converter Schematic

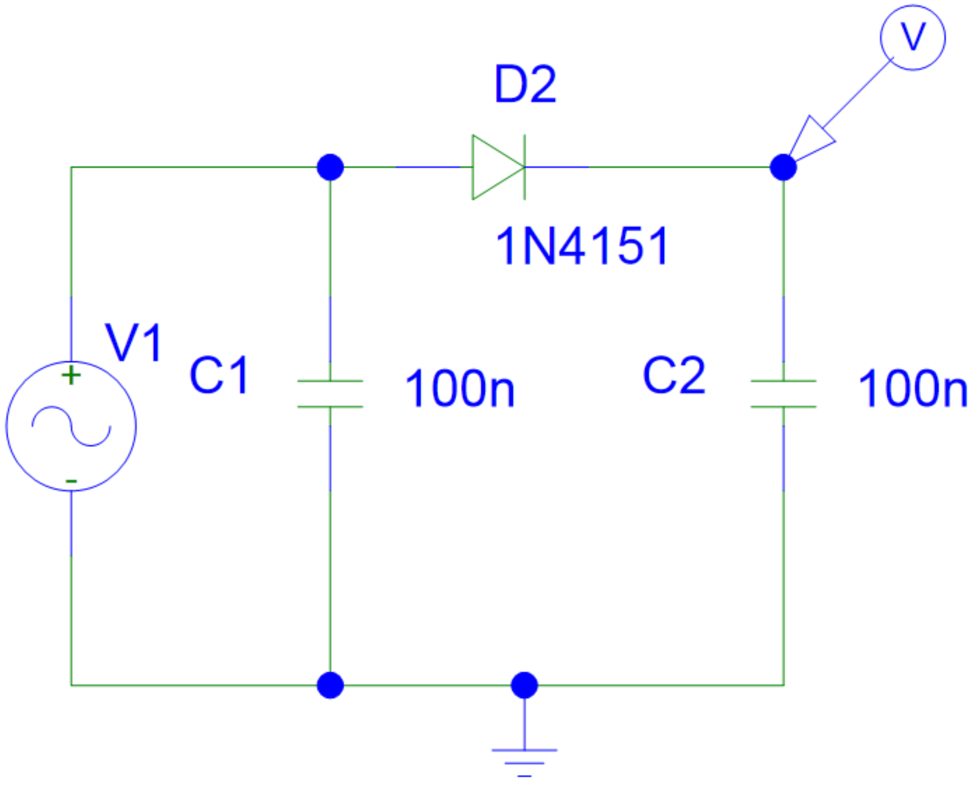
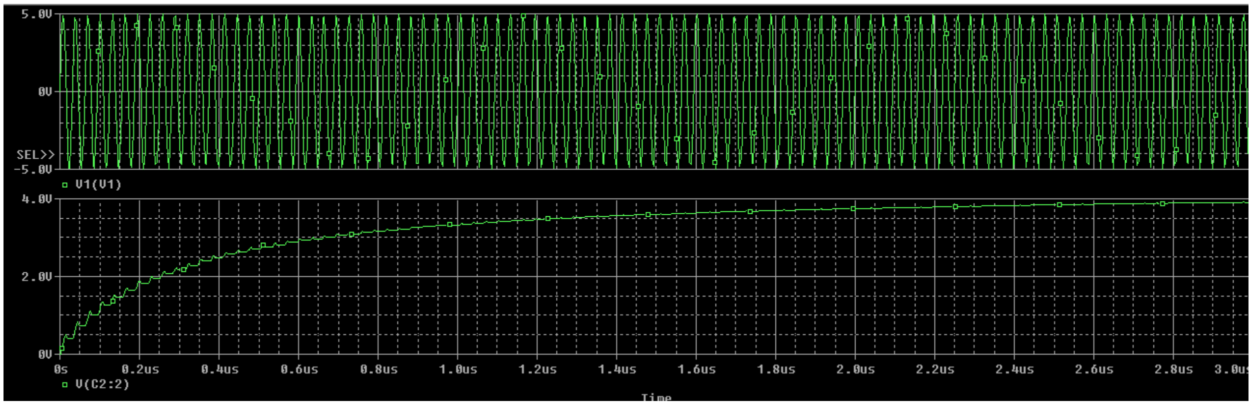


Figure 12 – Analog to Digital Converter Schematic



5.2.3 Design Conclusions

The simulations in MATLAB, ADS, and PSpice prove that using a down converter in conjunction with a bandpass filter can accurately detect a cellular phone that is transmitting in the area. MATLAB proved that it is mathematically possible to multiplying two signals together (downconverter) and filter them with a bandpass impulse response to accurately detect a signal. ADS proved that a circuit consisting of a down converter, bandpass filter, and VCO can accurately detect a signal. PSpice showed that this signal can then easily be converted to digital for input to a computer or display.

CHAPTER 6

SUMMARY/DISCUSSION

Cellular phone technology is gaining new data capabilities very rapidly. New features like Bluetooth, high resolution cameras, memory cards, and Internet make them ideal for getting data in and out of secure facilities. A cellular phone uses many differenttransmission protocols such as FDMA or CDMA. These protocols dictate how a cellular phone communicates with the tower. Typically cellular phones in the United states operate between 824 - 894 MHz.

Many businesses depend on keeping information protected and build fortresses that called secure facilities to protect their investment. Currently the only way to ensure that no one is bringing a cellular phone into a secure facility is to search everyone entering and exiting. This requires a lot of manpower and money to implement.

The existing technology available off the shelf does not accurately detect cellular phones ina secure facility. Detectors like the Wolfhound or Cellbusters sit in the entry way of a facility and randomly detect cellular phones or devices in the area. A better technique for accurately detecting cellular phones is needed.

The first signal detection technique, a design from circuit-projects.com was built and tested. This technique utilizes two antennas that are tuned to 900 MHz. The antennas resonate at this frequency and the signal is then demodulated. After demodulation, the signal is amplified and sent to a pair of headphones for monitoring.

After building the circuit-projects design using wire wrap, two conclusions were made. Using wire wrap at these frequencies changes the impedance of the circuit and BNC connectors make a much better connection. With this new information an even better design was conceived.

The second signal detection technique, a design utilizing a down converter in conjunction with a bandpass filter was built and tested. A VCO at 800 MHz and an 800MHz antenna is fed into the down converter. The VCO frequency is then subtracted from the cellular phone signal coming in around 832 MHz. This produces an output from the down converter around 32 MHz which is sent to a bandpass filter with a pass band of 29 - 35 MHz leaving just the 32MHz signal. It can then be converted to a digital output using an analog to digital converter.

This design was built and tested in the lab and provenMATLAB, ADS, and PSpice simulation software. Lab results show that a down converter and VCO circuit works, but requires a finely tuned bandpasss filter which can cost a lot of time and money. Therefore computer simulation results proved that this design will work with an effective bandpass filter. This technique, if fully implemented would greatly improve cellular phone detection technology. Businesses would save money on security and save money by not allowing any sensitive information to leak out.

REFERENCES

[1] “CellbusterCell Phone Detector”, Cellbusters INC.2004. Accessed September, 2008. Website http://www.cellbusters.com

[2] “Wolfhound Cellphone Detector”, Berkeley Varitronics Systems. 2010. Accessed March, 2009. Website http://www.bysystems.com

[3] “Cell Phone Detection Techniques”, U.S. Department of Energy. October 2007. Accessed January, 2010. Website http://inspire.ornl.gov

[4] “Detecting and Locating Cell Phones in Correctional Facilities”, EVI Technology, LLC. June 2007. Accessed February, 2010. Website http://iiw.itt.com/files/cellHound_wpCellPhonesInPrison.pdf

[5] “Cell Phone Detector”, Circuit-Projects.com Quality Circuits Archive. Accessed March, 2009. Website http://www.circuit-projects.com/rf-radio-frequency-circuits/cell-phone-detector.html

[6] "How Cell Phones Work", How Stuff Works A Discovery Company. Accessed April, 2009. Website http://www.howstuffworks.com/cell-phone.htm/printable

APPENDICES

APPENDIX A:

DATA SHEETS

APPENDIX B:

RELATED ARTICLES