Dual Band Mobile Jammer for GSM 900 & GSM 1800

Introduction

Communication jamming devices were first developed and used by military. This interest comes from the fundamental objective of denying the successful transport of information from the sender (tactical commanders) to the receiver (the army personnel), and vice-versa. Nowadays, mobile (or cell) phones are becoming essential tools in our daily life. Needless to say, the wide use of mobile phones could create some problems as the sound of ringing becomes annoying or disrupting. This could happen in some places like conference rooms, law courts, libraries, lecture rooms and mosques. One way to stop these disrupting ringing is to install a device in such places which will inhibit the use of mobiles, i.e., make them obsolete. Such a device is known as **cell phone jammer** or "**GSM jammer**", which is basically some kind of electronic countermeasure device. The technology behind cell phone jamming is very simple. The jamming device broadcasts an RF signal in the frequency range reserved for cell phones that interferes with the cell phone signal, which results in a "no network available" display on the cell phone screen. All phones within the effective radius of the jammer are silenced. It should be mentioned that cell phone jammers are illegal devices in most countries. However, recently, there has been an increasing demand for portable cell phone jammers.

A **mobile phone jammer** is an instrument used to prevent cellular phones from receiving signals from or transmitting signals to base stations. When used, the jammer effectively disables cellular phones. These devices can be used in practically any location, but are found primarily in places where a phone call would be particularly disruptive because silence is expected.

Principle of Jamming

Jammers block cell phone use by sending out radio waves along the same frequencies that cellular phones use. This causes enough interference with the communication of cell phones and the towers to render the phones unusable. On most retail phones, the network would simply appear out of range. Most cell phones use different bands to send and receive communications from towers. Thus jammers can work by either disrupting phone to tower frequencies or tower to phone frequencies.

Jamming Techniques

There are several ways to jam an RF device. The three most common techniques can be categorized as follows:

1. Spoofing

In this kind of jamming, the device forces the mobile to turn off itself. This type is very difficult to be implemented since the jamming device first detects any mobile phone in a specific area, then the device sends the signal to disable the mobile phone. Some types of this technique can detect if a nearby mobile phone is there and sends a message to tell the user to switch the phone to the silent mode (Intelligent Beacon Disablers).

2. Shielding Attacks

This is known as TEMPEST or EMF shielding. This kind requires closing an area in a faraday cage so that any device inside this cage cannot transmit or receive RF signal from outside of the cage. This area can be as large as buildings, for example.

3. Denial of Service

This technique is referred to DOS. In this technique, the device transmits a noise signal at the same operating frequency of the mobile phone in order to decrease the signal-to-noise ratio (SNR) of the mobile under its minimum value. This kind of jamming technique is the simplest one since the device is always on. Our device is of this type.

Design Parameters

Based on the above, our device which is related to the DOS technique is transmitting noise on the same frequencies of the two bands GSM 900 MHz, and GSM 1.8 GHz (known also as DCS 1800 band). We focused on some design parameters to establish the device specifications. These parameters are as follows:

1. The distance to be jammed (D)

This parameter is very important in our design, since the amount of the output power of the jammer depends on the area that we need to jam. Later on we will see the relationship between the output power and the distance D. Our design is established upon D=10 meters for DCS 1800 band and D=20 meters for GSM 900 band.

2. The frequency bands

	UPLINK(Handset Transmit)	DOWNLINK (Handset Receive)
GSM 900	890-915 MHz	935-960 MHz
GSM 1800	1710-1785 MHz	1805-1880 MHz

Table 1: Operating frequency bands.

In our design, the jamming frequency must be the same as the downlink, because it needs lower power to do jamming than the uplink range and there is no need to jam the base station itself. So, our frequency design will be as follows:

GSM 900 ⟶ 935-960 MHz
GSM 1800 ⟶ 1805-1880 MHz

3. Jamming–to-signal ratio {J/S}

Jamming is successful when the jamming signal denies the usability of the communication transmission. In digital communications, the usability is denied when the error rate of the transmission cannot be compensated by error correction. Usually, a successful jamming attack requires that the jammer power is roughly equal to signal power at the receiver (mobile device).

The general equation of the jamming-to-signal ratio is given as follows:

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

Where: P_j=jammer power,
G_{jr}= antenna gain from jammer to receiver,
G_{rj}=antenna gain from receiver to jammer,
R_{tr}=range between communication transmitter and receiver,
B_r=communication receiver bandwidth,
L_r =communication signal loss,
P_t=transmitter power,
G_{tr}= antenna gain from transmitter to receiver,
G_{rt}=antenna gain from receiver to transmitter,
R_{jr}=range between jammer and communication receiver,
B_j=jammer bandwidth, and
L_j=jamming signal loss.

For GSM, the specified system SNR_{min} is 9 dB which will be used as the worst case scenario for the jammer. The maximum power at the mobile device P_r is -15 dBm.

4. Free space loss {F}

The free-space loss (or path loss) is given by:

$$\text{Path loss (dB)} = 32.44 + 20 \log d\ (\text{km}) + 20 \log f\ (\text{MHz})$$

The maximum free space loss (worst case F) happens when the maximum frequency is used in the above equation. Using 1880 MHz gives:
F (dB) =32.44+20 log 0.01 + 20 log 1880 which gives F =58 dB.

System Design

Power calculations

Here, we need to find the power that is needed to be transmitted to jam any cell phone within a distance of around 10 meters for GSM 1800. From the above considerations, we can find the required output power from the device, as follows: Using SNR=9 dB and the maximum power signal for mobile receiver=-15 dBm, gives J=-24 dBm. But, our goal is to find the output power from the device, so when we add the free space loss to the amount of power at the mobile receiver we get our target: Output power=-24dBm+58dB = 34 dBm

Parts of the jammer device

Figure 1 shows the block diagram for the jammer to be designed.

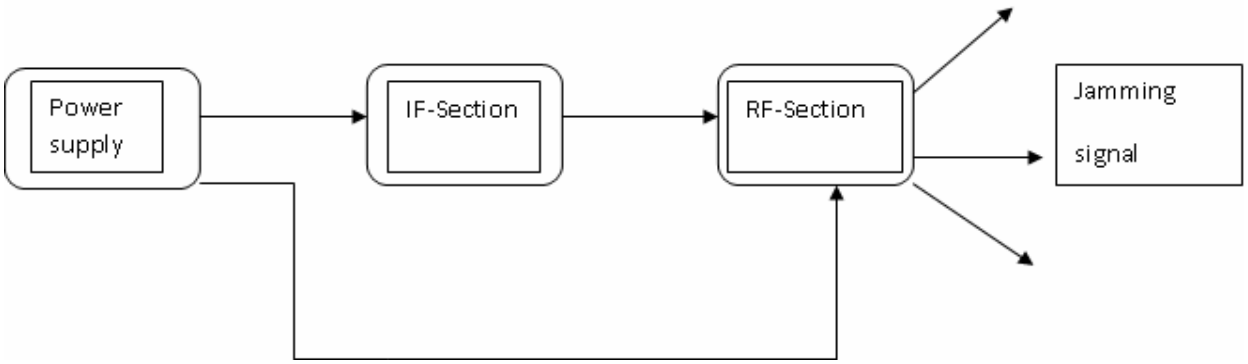

Figure 1 Jammer main blocks.

a) The Power supply

This is used to supply the other sections with the needed voltages. Any power supply consists of the following main parts:

Transformer: - is used to transform the 220VAC to other levels of voltages.

Rectification: - this part is to convert the AC voltage to a DC one. We have two methods for rectification: Half wave-rectification: the output voltage appears only during positive cycles of the input signal. Full wave –rectification: a rectified output voltage occurs during both the positive and negative cycles of the input signal.

The Filter: used to eliminate the fluctuations in the output of the full wave rectifier "eliminate the noise" so that a constant DC voltage is produced. This filter is just a large capacitor used to minimize the ripple in the output.

Regulator: this is used to provide a desired DC-voltage.

Figure 2 shows the general parts of the power supply.

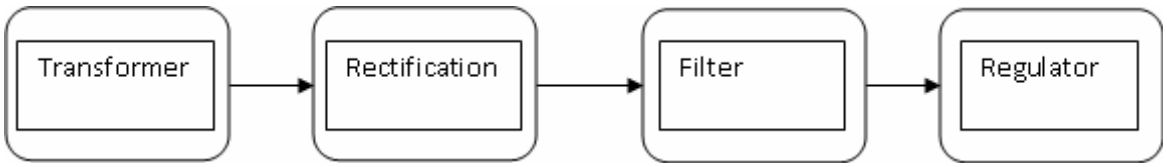

Figure 2 Parts of the power supply.

b) The IF-section

The tuning section of the jammer sweeps the VCO through the desired range of frequencies. Basically, it is just a triangle or saw tooth-wave generator; offset at a proper amount so as to sweep the VCO from the minimum desired frequency to a maximum. The tuning signal is generated by a triangular wave mixed with noise. The IF section consists of three main parts:

- Triangle wave generator. (To tune the VCO in the RF section)
- Noise generator (provides the output noise).
- Mixer "summer" (to mix the triangle and the noise waves).

Triangle wave generator

The main use of the triangle wave is to sweep the VCO through the desired frequency range. We want to cover the downlink through our VCO, i.e., 935-960 MHz for VCO66CL, and 1805-1880MHz for VCO55BE. In our design, we will use 555 IC operating in the a-stable mode to generate the sweeping signal. The output frequency depends on the charging and discharging of the capacitor, resistors values and the power supply for the IC.

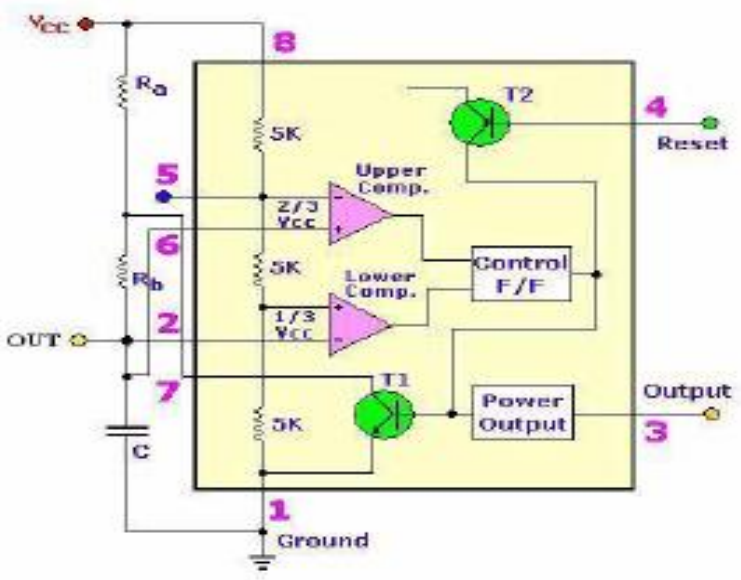

Figure 3 A-stable 555timer.

Noise generation

Without noise, the output of the VCO is just an un-modulated sweeping RF carrier. So, we need to mix the triangular signal with noise (FM modulating the

RF carrier with noise). To generate noise signal, we used the Zener Diode operated in reverse mode. Operating in the reverse mode causes what is called avalanche effect, which causes wide band noise. This noise is then amplified and used in our system. We use two amplification stages: in the first stage, we use NPN transistor as common emitter, and in the second stage, we use the LM386 IC {Audio amplifier}.

Mixer

The mixer here is just an amplifier that operates as a summer. So, the noise and triangular wave will add together before entering the VCO. The LM741 IC was used to achieve this.

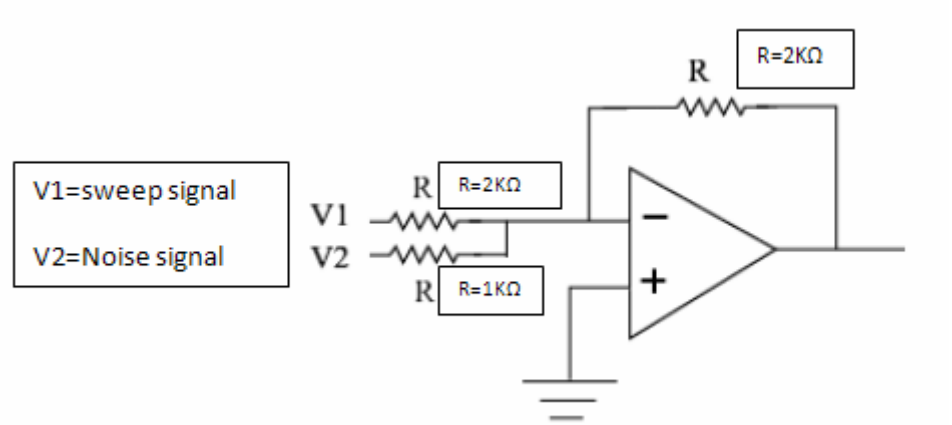

Figure 4 OP-AMP summer circuits

Using R_{noise} =1 KΩ, we amplify the noise signal by 2. In this case, the ratio of the noise to the sweep signal is 2:1.

Clamper

The input of the VCO must be bounded from 0 to 3.5 V to get the needed frequency range. So, we need to add a clamper to get our goal. The clamper consists of a capacitor connected in series with a resistor and diode, as shown in Figure 5.

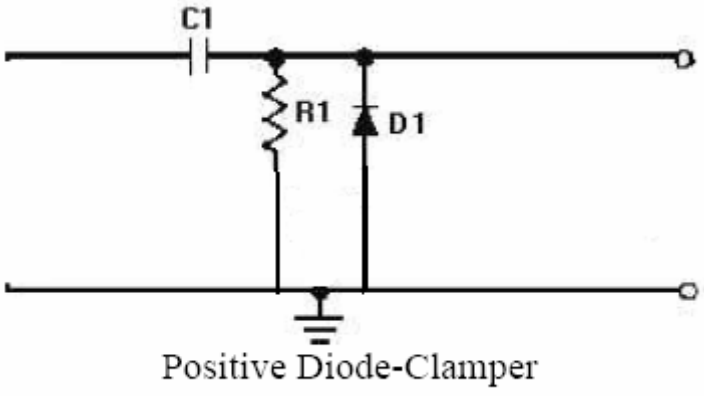

Figure 5 Diode clamper

The IF-section schematic is shown in Figure 6.

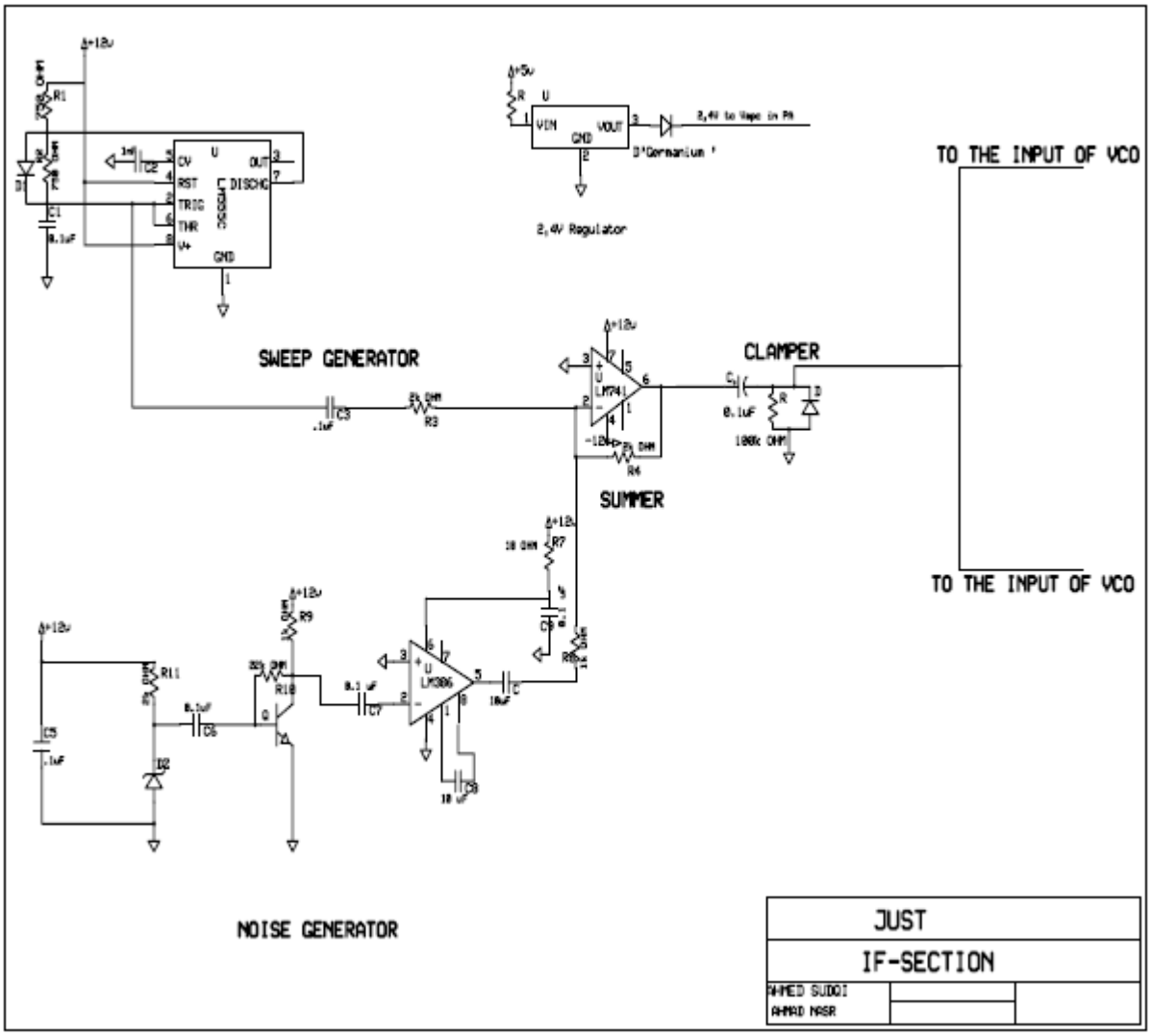

Figure 6 Schematic of the IF-section.

c) The RF-Section

This is the most important part of the jammer, since the output of this section will be interfacing with the mobile. The RF-section consists of three main parts: voltage controlled oscillator VCO, power amplifier and antenna.

The voltage controlled oscillator (VCO) is the heart of the RF-section. It is the device that generates the RF signal which will interfere with the cell phone. The output of the VCO has a frequency which is proportional to the input voltage, thus, we can control the output frequency by changing the input voltage. When the input voltage is DC, the output is a specific frequency, while if the input is a triangular waveform; the output will span a specific frequency range. In our design, we need to find a VCO for GSM 900 and GSM 1800. There are three selection criteria for selecting a VCO for this application. Most importantly, it should cover the bands that we need, secondly, it should be readily available at low cost, and finally, it should run at low power consumption. Moreover, we

need to minimize the size of GSM-jammer. So, we started to search through the internet for VCO's that work for GSM 900 & GSM 1800 bands. The power amplifier: Since 5 dBm output power from the VCO does not achieve the desired output power of the GSM jammer; we had to add an amplifier with a suitable gain to increase the VCO output to 34 dBm. We obtained our amplifier IC from an old mobile as it was the most suitable, cheapest and easiest way to get one.

Antenna: A proper antenna is necessary to transmit the jamming signal. In order to have optimal power transfer, the antenna system must be matched to the transmission system. In this project, we used two 1/4 wavelength monopole antennas, with 50 Ω input impedance so that the antennas are matched to the system. We used monopole antenna since the radiation pattern is Omni-directional.

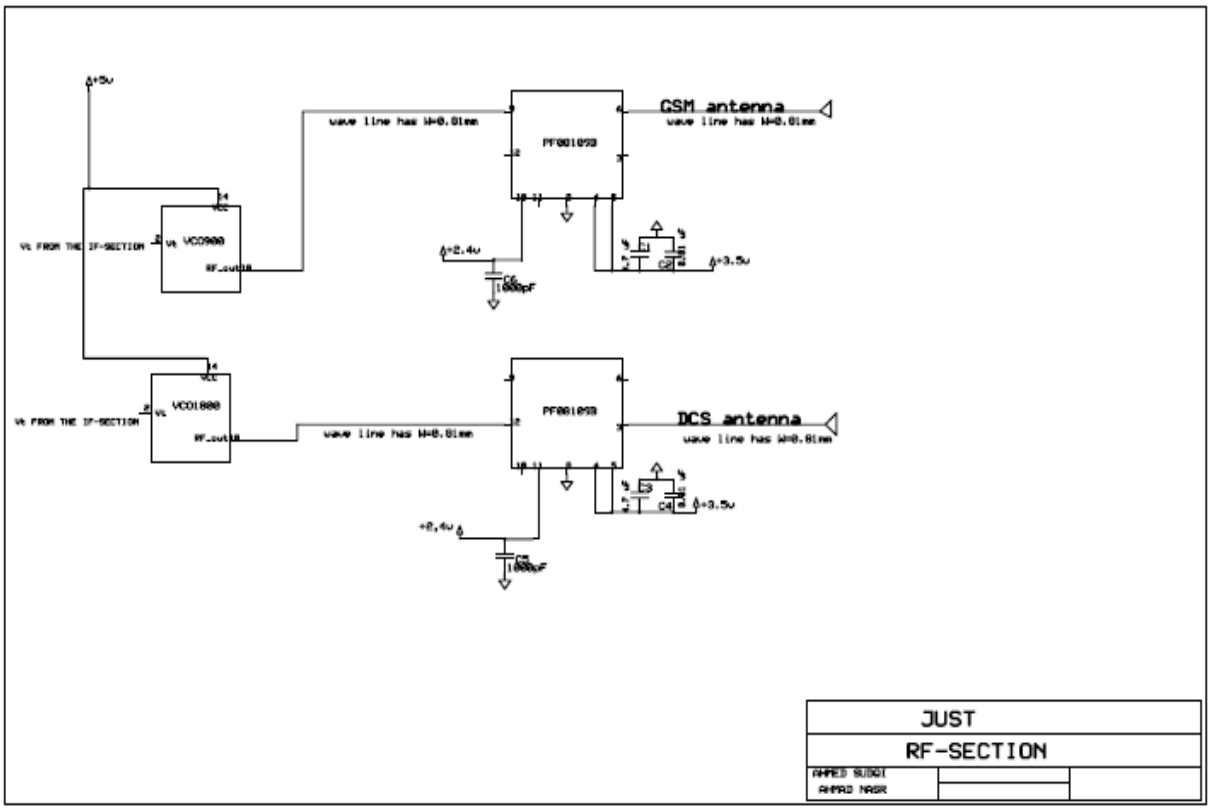

Figure 7 RF-section Schematic.

Applications of GSM Jammer

- Business (conferences, board of directors rooms, seminars, meeting rooms)
- Hospitals
- For ICU & Operation Theatres
- Church/Mosque/Cathedral/ Temple/ Religious establishment
- To keep solemn mode in religious ceremony by removing unwanted noise of mobile phones

- Libraries, Lecture Halls
- Movie Theatres/ cinemas
- To avoid trouble of ringing mobile phones during the movie is on
- Institutes / reading rooms
- To maintain silence for study activities
- Places of Worship (mosques, shrines, churches, temples, etc.)
- Government Buildings
- Recording Studios
- Mobile Phone Free Zones and Prohibited Areas

Conclusions

Cell phones are everywhere these days. According to the Cellular Telecommunications and Internet Association, almost 195 million people in the United States had cell-phone service in October 2005. And cell phones are even more ubiquitous in Europe. It's great to be able to call anyone at anytime. Unfortunately, restaurants, movie theaters, concerts, shopping malls and churches all suffer from the spread of cell phones because not all cell-phone users know when to stop talking. Who hasn't seethed through one side of a conversation about an incredibly personal situation as the talker shares intimate details with his friend as well as everyone else in the area? The rapid proliferation of cell phones at the beginning of the 21st century to near ubiquitous status eventually raised problems such as their potential use to invade privacy, contribute to academic cheating, or even aid in industrial espionage. In addition public backlash was growing against the intrusive disruption cell phones introduced in daily life. While older analog cell phones often suffered from chronically poor reception and could even be disconnected by simple interference such as high frequency noise, increasingly sophisticated digital phones have led to more elaborate counters. Cell phone jamming devices are an alternative to more expensive measures against cell phones, such as Faraday cages, which are mostly suitable as built in protection for structures. They were originally developed for law enforcement and the military to interrupt communications by criminals and terrorists. Some were also designed to foil the use of certain remotely detonated explosives. The civilian applications were apparent, so over time many companies originally contracted to design jammers for government use switched over to sell these devices to private entities. Since then, there has been a slow but steady increase in their purchase and use, especially in major metropolitan areas. In this project, which we think will turn out to be a full success; we designed a device that stops phone ringing. This device could be used in places where ringing is not desired at specific times, as these ringing may disturb people in such places. The designed device works in dual band. It jams both the GSM 900 and GSM 1800 bands.