900 MHz GSM MOBILE JAMMER

Developed by

Muhammad Nauman Shahid
IS/17119/Aut-07/M
Muhammad Mansoor Ahmed
IS/17118/Aut-07/M
Muhammad Ather Rasool
IS/17115/Aut-07/M

Supervised by
Engr. Jamal Akram

Department of Computer Science
Federal Urdu University of Arts, Science & Technology,
Islamabad

(2011)

Federal Urdu University of Arts, Science & Technology, Islamabad

August 02, 2011

Final Approval

It is certified that we have read the project report titled **"900 MHz GSM Mobile Jammer"** submitted by Mr. Muhammad Nauman Shahid, Mr. Muhammad Mansoor Ahmed and Mr. Muhammad Ather Rasool and it is our judgment that this project is of sufficient standard to warrant its acceptance by the Federal Urdu University of Arts, Science & Technology, Islamabad for the Bachelors Degree in Computer Science.

Committee

External Examiner

_____

Mr. /Dr.
Associate Professor
Faculty of Computer Studies,
..... University,
Islamabad

Internal Examiner

_____

Mr.
Assistant Professor
Department Of Computer Science,
Federal Urdu University of Arts, Science & Technology,
Islamabad

Supervisor

_____

Mr. Jamal Akram
Department Of Electrical Engineering,
Federal Urdu University of Arts, Science & Technology,
Islamabad

A dissertation submitted to the

Department of Computer Science,

Federal Urdu University of Arts, Science & Technology,

Islamabad

as a partial fulfillment of the requirements

for the award of the degree of

Bachelor of Computer Science

DECLARATION

We, hereby declare that this Project, neither as a whole nor as a part thereof has been copied out from any source. It is further declared that we have developed this Project and the accompanied report entirely on the basis of our personal efforts made under the sincere guidance of our teachers. If any part of this report is proved to be copied out or found to be reported, we shall standby the consequences. No portion of the work presented in this report has been submitted in support of any application for any other degree or qualification of this or any other university or institute of learning.

Muhammad Nauman Shahid

Muhammad Mansoor Ahmed

Muhammad Ather Rasool

Dedicated to

Our Loving Parents and Teachers

ACKNOWLEDGEMENT

All praise to Almighty Allah, the most merciful and compassionate, who enabled us to complete this research work.

We express our gratitude to our kind fellow *Muhammad Nauman Shahid* who is behind the idea of ***900 MHz GSM Mobile Jammer*.**

We express our gratitude to our kind supervisor *Engr. Jamal Akram* who kept our morale high by his suggestions and appreciation. He was available to us whenever and for whatever we consulted him. Without his precious guidance and help we could never be able to develop such a system.

To our class fellows and friends, we always remember their cooperation with us. They helped us in our project wherever we needed, especially our friends *Lab Assistant Kashif, Muhammad Umer and Moin ud Din* for providing very good company.

To all our seniors, who helped us to take decisions about this project and provided us technical help.

And last but not the least; we would like to acknowledge the support of our family members. We would like to admit that we owe all our achievements to our truly, sincere and most loving parents, brothers and sisters, who mean the most to us, and whose prayers are a source of determination for us.

Muhammad Nauman Shahid
Muhammad Mansoor Ahmed
Muhammad Ather Rasool

Project in Brief

Project Title	**900 MHz GSM Mobile Jammer**
Organization	Federal Urdu University of Arts, Science and Technology, Islamabad
Undertaken By	Muhammad Nauman Shahid Muhammad Mansoor Ahmed Muhammad Ather Rasool
Supervised By	**Engr. Jamal Akram** Department of Electrical Engineering, Federal Urdu University of Arts, Science & Technology, Islamabad
Tools Used	**Proteus, Electronic Workbench, Oscilloscope**
Date Started	April 10, 2011
Date Completed	July 26, 2011

Abstract

This report presents the design, implementation, and testing of a 900 MHz band Mobile phone Jammer. This jammer works at GSM 900 and thus attains capability to jam all the major GSM cellular operators in Pakistan (Mobilink, Ufone, Telenor, Warid and Zong).

This project went through two phases:

Phase One: Studying the GSM system to find the best jamming technique, establishing the system design and selecting suitable components.

Phase Two: Buying all the needed components, drawing the overall schematics, fabricating the PCB layout, assembling the devices, performing some measurements and finally testing the Mobile Jammer.

The designed jammer was successful in giving a jammed signal as output on the oscilloscope.

TABLE OF CONTENTS

CHAPTER 1
INTRODUCTION

1.1 HISTORY

The rapid proliferation of cell phones in recent years to near ubiquitous status eventually raised problems such as their potential use to invade privacy, contribute to academic cheating, or even aid in corporate espionage. In addition public backlash was growing against the perceived 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 counter-measures.

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.

1.1.1 NEED OF JAMMING

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. Here in Pakistan, for example, with a rather high population (around 80 million), five main cell phone carries are available; namely; Mobilink, Ufone, Telenor, Warid and Zong. All of them use the GSM 900 system. 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 place 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. According to the Federal Communications

Commission (FCC) in the USA: "The manufacture, importation, sale, or offer for sale, of devices designed to block or jam wireless transmissions is prohibited". However, recently, there has been an increasing demand for portable cell phone jammers. We should mention that this project, presented in this report, is solely done for educational purposes. There is no intention to manufacture or sell such devices in Pakistan, or elsewhere. In this project, a device that will jam GSM 900 services will be designed, built, and tested.

1.2 PROJECT SCOPE

Cell phones and radio receivers are used everywhere these days. It's useful to be able to call anyone anytime. But unfortunately, restaurants, movie theatres, concerts, shopping malls and mosques all suffer from the spread of cell phones because not all cell phone users know when to stop talking. While most of us just grumble and move on, some people are actually going to extremes to retaliate. **GSM Jammer** can be one of the solutions to this problem.

1.3 GLOBAL SYSTEM FOR MOBILE COMM

1.3.1 ELEMENTS OF A CELLULAR NETWORK

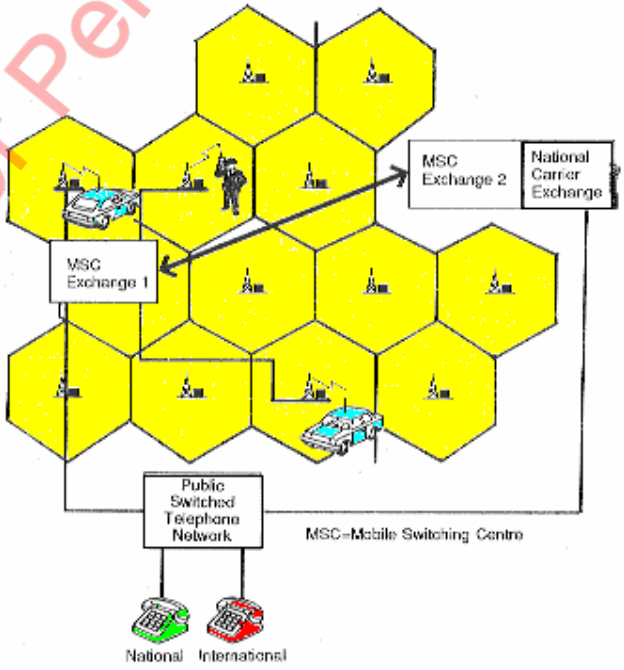
In this section, the ***General* system architecture** of a Global System for Mobile Communication (GSM) cellular network is introduced:

•**Mobile Station (MS):** This is the Mobile Equipment containing the Subscriber Identity Module (SIM).

•**Base Station (BS):** The covered area of a cellular network is divided into smaller areas called cells. Each cell has a base station which communicates simultaneously with all mobiles within the cell, and passes traffic to the Mobile Switching Centre. The base station is connected to the mobile phone via a radio interface.

•**Mobile Switching Centre (MSC):** This controls a number of cells (or cluster), arranges base stations and channels for the mobiles and handles connections.

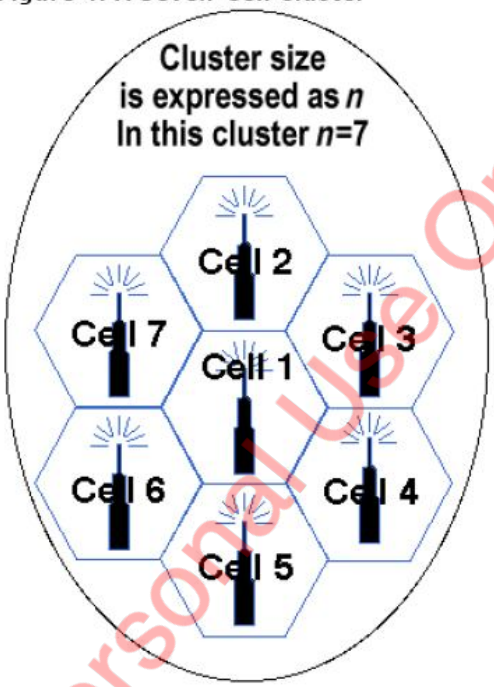
•**National Carrier Exchange:** This is the gateway to the national fixed public switched telephone network (PSTN). It handles connections on behalf of the national communication systems, and is usually integrated with the MSC.



•**Cells:** A cell is the basic geographic unit of a cellular network. The term *cellular* comes from the diamond shape of the areas into which a coverage region is divided. Cells are base stations transmitting over small geographic areas that are represented as hexagons. Each cell size varies depending on the landscape. Because of constraints imposed by natural terrain and man-made structures, the true shape of cells is not a perfect hexagon.

•**Clusters:** A cluster is a group of cells. No channels are re-used within a cluster. Following figure shows a seven-cell cluster.

Figure 4: A Seven-Cell Cluster



The Global System for Mobile Communication (GSM 900) operates on the range of frequencies from 890 MHz to 960 MHz. This range of frequencies is divided into:

•**890 MHz to 915 MHz**: This band of frequencies is known as Uplink Frequency Band and is used by the Mobile Station (cell phone) to communicate with the Base Transceiver Station (BTS).

•**935 MHz to 960 MHz**: This band of frequencies is known as the Downlink Frequency Band and is used by the BTS to communicate with the Mobile Station.

•**915 MHz to 935 MHz**: This band of frequencies is the guard band, separating the Uplink from the Downlink frequencies.

The GSM Network uses two different multiplexing schemes. **Frequency Division Multiple Access (FDMA)** and **Time Division Multiple Access**

(TDMA). Both the Downlink and the Uplink bands are further divided into sets of frequencies 200 KHz wide (FDMA). Each set from the Uplink Frequencies Band is coupled with the corresponding frequency set from the Downlink Frequencies Band to form an Absolute Radio Frequency Channel Number (ARFCN). Communication between the Mobile Station and the BTS takes place on the frequencies allocated to only one ARFCN at a time. This leads to a total of 124 channels for communication (200 KHz set aside as guard band).

Each ARFCN is allocated eight time slots (TDMA) of 4.7 ms duration which gives 577 time slots/s. Each time slot is allotted to communication with a separate Mobile station for the duration of the conversation. This gives a maximum of eight users per ARFCN.

1.3.2 OPERATION OF THE CELLULAR PHONE

When the mobile unit is active (i.e. when a mobile phone is switched on), it registers with the appropriate BS, depending on its location, and its cell position is stored at the responsible MSC. When a call is set-up (when a user makes a call), the base station monitors the quality of the signal for the duration of the call, and reports that to the controlling MSC, which in turn makes decisions concerning the routing of the call.

When a cellular phone moves from one cell to the other, the BS will detect this from the signal power and inform the MSC of that. The MSC will then switch the control of the call to the BS of the new cell, where the phone is located. This is called handover. It normally takes up to 400ms, which is not noticeable for voice transmission.

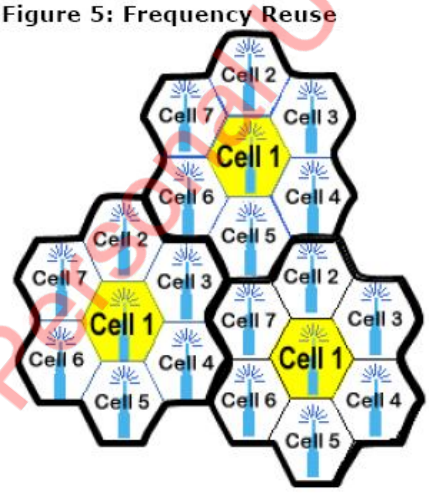
A cellular phone user can only use his/her mobile within the covered area of the network.

1.3.3 FREQUENCY RE-USE

Because only a small number of radio channel frequencies were available for mobile systems, engineers had to find a way to reuse radio channels in order to carry more than one conversation at a time. The solution the industry adopted was called frequency planning or frequency re-use. Frequency re-use was implemented by restructuring the mobile telephone system architecture into the cellular concept.

The concept of frequency re-use is based on assigning to each cell a group of radio channels used within a small geographic area. Cells are assigned a group of channels that are completely different from neighboring cells. The coverage area of cells is called the footprint. The footprint is limited by a boundary so that the same group of channels can be used in different cells that are far enough away from each other so that their frequencies do not interfere.

Figure 5: Frequency Reuse

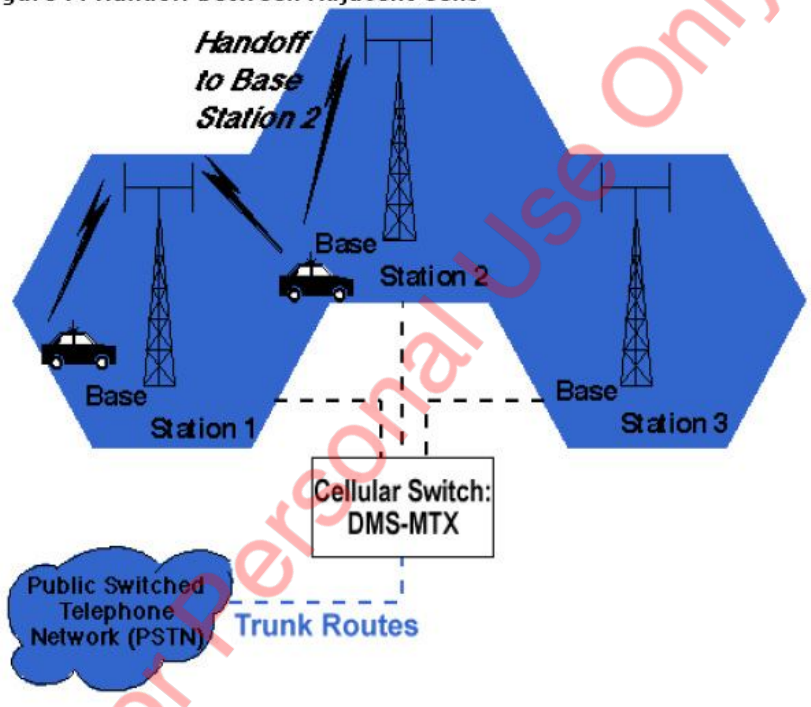


Cells with the same number have the same set of frequencies. Here, because the number of available frequencies is 7, the frequency reuse factor is 1/7. That is, each cell is using 1/7 of available cellular channels.

1.3.4 HANDOFF/HANDOVER

As adjacent areas do not use the same radio channels, a call must either be dropped or transferred from one radio channel to another when a user crosses the line between adjacent cells. Because dropping the call is unacceptable the process of handoff was created. Handoff occurs when the mobile telephone network automatically transfers a call from radio channel to radio channel as mobile crosses the border between adjacent cells.

Figure 7: Handoff between Adjacent Cells



During the call two parties are on one voice channel (ARFCN). When the mobile unit moves out of the coverage area of a given cell site, the reception becomes weak. At this point, the cell site in use requests a handoff. The system switches the call to a stronger frequency channel in a new site without interrupting the call or alerting the user. The call continues as long as the user is talking and the user does not notice the handoff at all.

1.4 WHAT IS A GSM JAMMER?

A GSM Jammer is a device which transmits noise-induced signals at the same frequencies at which a GSM system operates, thus rendering mobile phones in the specified area unusable.

1.5 JAMMING TECHNIQUES

1.5.1 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).

1.7.1 SPOOFING

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 can not transmit or receive RF signal from outside of the cage. This area can be as large as buildings, for example.

1.7.1 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.

1.6 WORKING OF A JAMMER

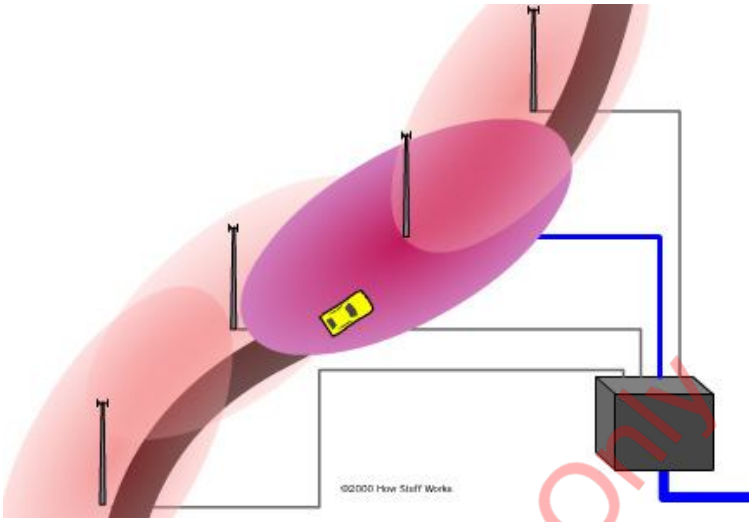
Jamming devices over power the cell phone by transmitting a signal on the same frequency as the cell phone and at a high enough power that the two signals collide and cancel each other out. Cell phones are designed to add power if they experience low- level interference, so the jammer must recognize and match the power increase from the phone.

Cell phones are full-duplex devices, which means they use two separate frequencies, one for talking and one for listening simultaneously. Some jammers block only one of the frequencies used by cell phones, which has the effect of blocking both. The phone is tricked into thinking there is no service because it can receive only one of the frequencies.

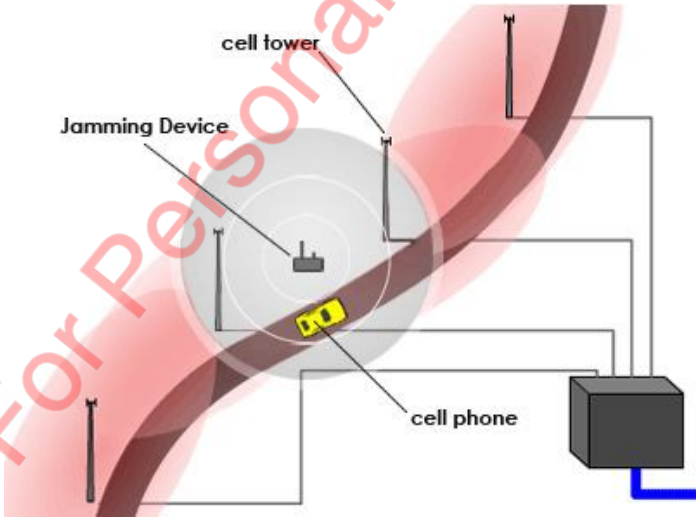
Less complex devices block only one group of frequencies, while sophisticated jammers can block several types of networks at once to head off dual-mode or tri-mode phones that automatically switch among different network types to find an open signal. Some of the high-end devices block all frequencies at once, and others can be tuned to specific frequencies.

To jam a cell phone, all you need is a device that broadcasts on the correct frequencies. Although different cellular systems process signals differently, all cell-phone networks use radio signals that can be interrupted. GSM, used in digital cellular and PCS-based systems, operates in the 900-MHz and 1800-MHz bands in Europe and Asia and in the 1900 MHz (sometimes referred to as 1.9 GHz) band in the United States. Jammers can broadcast on any frequency and are effective against AMPS, CDMA, TDMA, GSM, PCS, DCS, I-DEN and Nextel systems. Old-fashioned analog cell phones and today's digital devices are equally susceptible to jamming.

Disrupting a cell phone is the same as jamming any other type of radio communication. A cell phone works by communicating with its service network through a cell tower or base station. Cell towers divide a city into small areas, or cells. As a cell phone user drives down the street, the signal is handed from tower to tower.



A jamming device transmits on the same radio frequencies as the cell phone, disrupting the communication between the phone and the cell phone base station in the tower.



Older jammers sometimes were limited to working on phones using only analog or older digital mobile phone standards. Newer models such as the double and triple band jammers can block all widely used systems (AMPS, I-DEN, GSM, etc) and are even very effective against newer phones which hop to different frequencies and systems when interfered with. As the dominant network technology and frequencies used for mobile phones vary worldwide, some work only in specific regions such as Europe or North America.

The power of the jammer's effect can vary widely based on factors such as

proximity to towers, indoor and outdoor settings, presence of buildings and landscape, even temperature and humidity play a role.

There are concerns that crudely designed jammers may disrupt the functioning of medical devices such as pacemakers. However, like cell phones, most of the devices in common use operate at low enough power output (<1W) to avoid causing any problems.

1.7 TYPES OF MOBILE JAMMERS

There are many different approaches to jamming a cellular device in a specific area but the five main approaches used or being developed are described in the RABC (Radio Advisory Board of Canada) Mobile & Personal Communications Committee's (M&PCC) meeting of June 22, 1999. These techniques are as discussed below:

1.7.1 TYPE "A" DEVICE: JAMMERS

This type of device comes equipped with several independent oscillators transmitting 'jamming signals' capable of blocking frequencies used by paging devices as well as those used by cellular/PCS systems control channels for call establishment. When active in a designated area, such devices will (by means of RF interference) prevent all pagers and mobile phones located in that area from receiving and transmitting calls. This type of device transmits only a jamming signal and has very poor frequency selectivity, which leads to interference with a larger amount of communication spectrum than it was originally intended to target.

This technique could be implemented without cooperation from PCS/cellular providers, but would negatively impact PCS/cellular system operation. Once jamming begins, escalation to counter-jamming may result, either by deliberate action or by autonomous response of power control systems within a PCS/cellular system.

One other area of concern is the raising of the general RF noise floor in the neighborhood as a result of a Type "A" device. Many communication systems are required to work in all types of buildings under very low signal conditions and the raising of the noise floor by various jamming transmitters in the same band and vicinity could make the difference between receiving or not receiving a crucial message.

1.7.2 TYPE "B" DEVICE: INTELLIGENT CELLULAR DISABLERS

Unlike jammers, Type "B" devices do not transmit an interfering signal on the control channels. The device, when located in a designated 'quiet' area, functions as a 'detector'. It has a unique identification number for communicating with the cellular base station. When a Type "B" device detects the presence of a mobile phone in the quiet room; the 'filtering' (i.e. the prevention of authorization of call establishment) is done by the software at the base station.

When the base station sends the signaling transmission to a target user, the device after detecting simultaneously the presence of that signal and the presence

of the target user, signals the base station that the target user is in a 'quiet' room; therefore, do not establish the communication. Messages can be routed to the user's voice mail box, if the user subscribes to a voice-mail service. This process of detection and interruption of call establishment is done during the interval normally reserved for signaling and handshaking.

For 'emergency users', the intelligent detector device makes provisions for designated users who have emergency status. These users must pre-register their phone numbers with the service providers. When an incoming call arrives, the detector recognizes that number and the call is established for a specified maximum duration, say two minutes. The emergency users are also allowed to make out going calls, similarly, the system is capable of recognizing and allowing all emergency calls routed to "911".

It should be noted that the Type "B" detector device being an integral part of the cellular/PCS systems, would need to be provisioned by the cellular/PCS service providers or provisioned by a third-party working cooperatively with full support of the cellular/PCS service providers.

1.7.3 TYPE "C" DEVICE: INTELLIGENT BEACON DISABLERS

Unlike jammers, Type "C" devices do not transmit an interfering signal on the control channels. The device, when located in a designated 'quiet' area, functions as a 'beacon' and any compatible terminal is instructed to disable its ringer or disable its operation, while within the coverage area of the beacon. Only terminals which have a compatible receiver would respond and this would typically be built on a separate technology from cellular/PCS, e.g., cordless wireless, paging, ISM, Bluetooth. On leaving the coverage area of the beacon, the handset must re-enable its normal function.

This technology does not cause interference and does not require any changes to existing PCS/cellular operators. The technology does require intelligent handsets with a separate receiver for the beacon system from the cellular/PCS receiver. It will not prevent normal operation for incompatible legacy terminals within a "quiet" coverage area, thus effective deployment will be problematic for many years.

While general uninformed users would lose functionality, pre-designated "emergency" users could be informed of a "bypass terminal key sequence" to inhibit response to the beacon. Assuming the beacon system uses a technology with its own license (or in the license exempt band), no change to the regulations are needed to deploy such a system. With this system, it would be extremely difficult to police misuse of the "bypass key sequence" by users.

1.7.4 TYPE "D" DEVICE: DIRECT RECEIVE AND TRANSMIT JAMMERS

This jammer behaves like a small, independent and portable base station, which can directly interact intelligently or unintelligently with the operation of the local mobile phone. The jammer is predominantly in receiving mode and will intelligently choose to interact and block the cell phone directly if it is within close proximity of the jammer.

This selective jamming technique uses a discriminating receiver to target the jamming transmitter. The benefit of such targeting selectivity is much less electromagnetic pollution in terms of raw power transmitted and frequency spectrum from the jammer, and therefore much less disruptive to passing traffic. The jam signal would only stay on as long as the mobile continues to make a link with the base station, otherwise there would be no jamming transmission. The technique forces the link to break or unhook and then it retreats to a passive receive mode again.

This technique could be implemented without cooperation from PCS/cellular providers, but could negatively impact PCS/cellular system operation. This technique, has an added advantage over Type B in that no added overhead time or effort is spent negotiating with the cellular network. As well as Type B, this device could discriminate 911 calls and allow for "breakthroughs" during emergencies.

1.7.5 TYPE "E" DEVICE: EMI SHIELD-PASSIVE JAMMING

This technique is using EMI suppression techniques to make a room into what is called a Faraday cage. Although labor intensive to construct, the Faraday cage essentially blocks, or greatly attenuates, virtually all electromagnetic radiation from entering or leaving the cage or in this case a target room.

With current advances in EMI shielding techniques and commercially available products one could conceivably implement this into the architecture of newly designed buildings for so-called "quiet-conference" rooms.

Emergency calls would be blocked unless there was a way to receive and decode the 911 transmissions, pass by coax outside the room and re-transmitted. This passive configuration is currently legal in Canada for any commercial or residential location insofar as DOC Industry Canada is concerned, however municipal or provincial building code by- laws may or may not allow this type of construction.

1.8 FUTURE ENHANCEMENTS

The successful working of GSM jammers holds its uses in different technologies. In future jamming on 2100MHz band would be possible with the help of same techniques. It will render the cell phones in the effective area unusable.

CHAPTER 2
REQUIREMENT ANALYSIS

2.1 JAMMING METHODOLOGY

2.1.1 THE FREQUENCY ISSUE:

The basic purpose of a GSM Mobile Jammer is to block or hinder communication between the Base Transceiver Station and the Mobile Station. This can only be achieved by rendering the transmission between them incomprehensible. The basic technique for accomplishing this goal is to create disturbance on the GSM transmission frequencies. The question that arises now is on which frequencies should the disturbance be created?

There are three possible answers to this:

•The whole GSM Band (890 MHz - 960 MHz)
•The Uplink frequency band (890 MHz – 915 MHz)
•The Downlink frequency Band (935 MHz – 960 MHz)

The problem with jamming the entire band or the uplink frequencies is that we are aiming to disrupt communication at the Base Transceiver Station. For this we need a very high power transmitter that will create a powerful signal strong enough to reach the BTS. Furthermore, this action will cause the Signal to Noise ratio at the BTS to fall which will, in effect, cause all incoming signals at the BTS to be corrupted. Thus all incoming connections to the BTS will be disturbed which will jam the Mobile Stations throughout the entire coverage region of the BTS i.e. its cell.

In contrast, if we create disturbance over the Downlink frequencies, we only need a transmitter powerful enough to create a signal that disrupts communication in our required area. This causes only the Mobile Stations in the specific area to be jammed and leaves the ones outside it alone.
Summing it all up, we get the following result:

•Jamming the uplink or entire band requires a high power transmitter and disrupts communication over an entire cell.
•Jamming the downlink band requires a transmitter of sufficient power to jam the required area only and does not disturb the communication outside it.

Therefore, our goal is to disrupt communication over downlink frequencies only.

2.2 DESIGN PARAMETERS

Based on the above, our device which is related to the DOS technique is transmitting noise on the same frequencies of the band GSM 900 MHz. We focused on some design parameters to establish the device specifications.

These parameters are as follows:

2.2.1 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 D=20 meters for GSM 900 band.

2.2.2 FREQUENCY BANDS

Table 1: Operating frequency bands.

	UPLINK (Handset transmit)	DOWNLINK (Handset receive)	USED IN JORDAN BY:
GSM 900	890-915 MHz	935-960 MHz	Zain + Orange
DCS 1800	1710-1785 MHz	1805-1880 MHz	Umniah

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 to 935-960 MHz

2.2.3 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 can not 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: Pj= Jammer power, Gjr= Antenna Gain from Jammer to receiver, Grj= Antenna Gain from receiver to Jammer, Rtr= Range between communication transmitter and receiver, Br= Communication receiver bandwidth, Lr= Communication signal loss, Pt= Transmitter power, Gtr= Antenna gain from transmitter to receiver, Grt= Antenna Gain from receiver to transmitter, Rjr= Range between Jammer and communication receiver, Bj= Jammer bandwidth, and Lj= Jamming signal loss.

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

2.2.4 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.

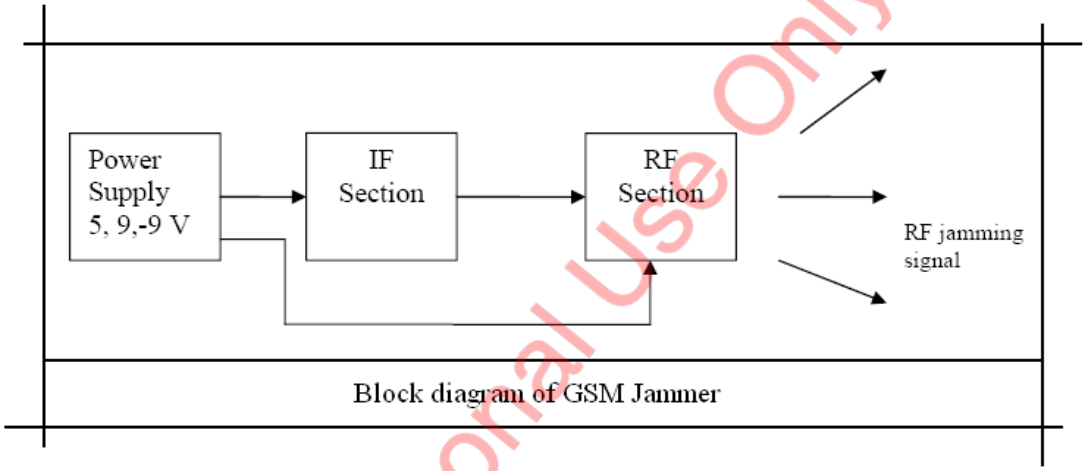
Using 935 MHz gives:
F (Db)= 32.44+20 log 0.01 + 20 log 935 which gives F =51.85 dB.

CHAPTER 3
DESIGN AND IMPLEMENTATION

3.1 JAMMER CONSTRUCTION

The Jammer is divided into three parts, namely:

- The Power Section
- The Intermediate Frequency (IF) Section
- The Radio Frequency (RF) Section



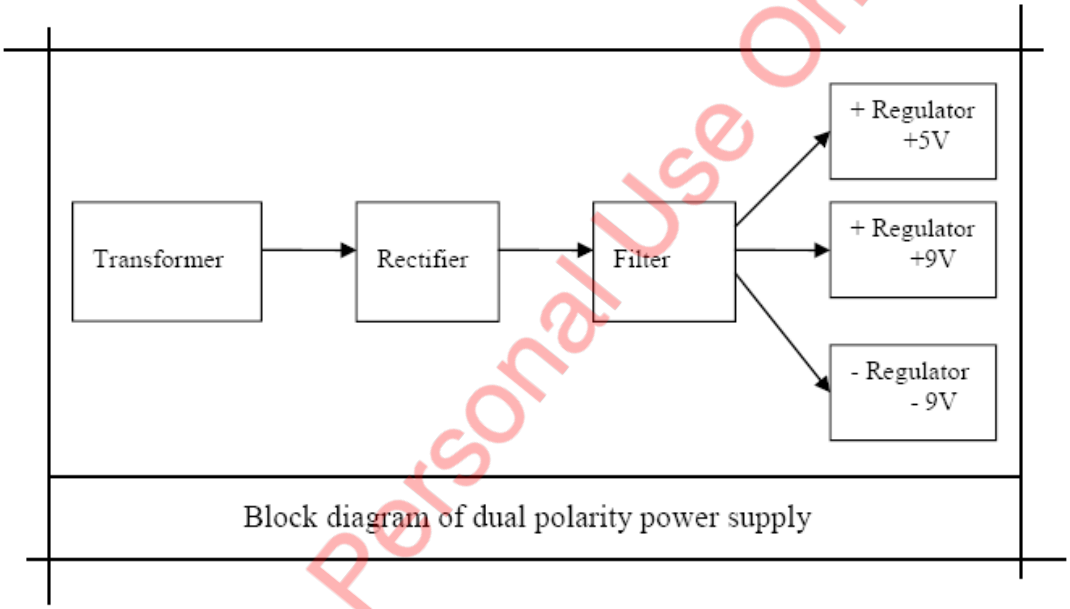
Block diagram of GSM Jammer

3.2 POWER SUPPLY SECTION

The Jammer has been designed to extract power from the regular 220 V AC power outlet. The IF and the RF Sections require +5 V, +9 V and –9 V. The power supply consists of four parts:

•Transformer (220 V to 12 V)
•Rectifier
•Filter
•Regulators (+5 V, +9 V and -9 V)

The block diagram of the power supply is shown below:



Block diagram of dual polarity power supply

The transformer used converts 220 V AC to 12 V AC with a 2A rating. This is then fed to a full-wave bridge rectifier. The out put of the rectifier is given by (V_p – 1.4) V i.e. 16.97– 1.4 = 15.57 V (peak).

The rectifier used is a full-wave bridge rectifier. The rectifier converts the 50 Hz AC signal to a 100 Hz pulsating DC signal. The average value of the output, V_{avg}, of the rectifier is given by:

Where,

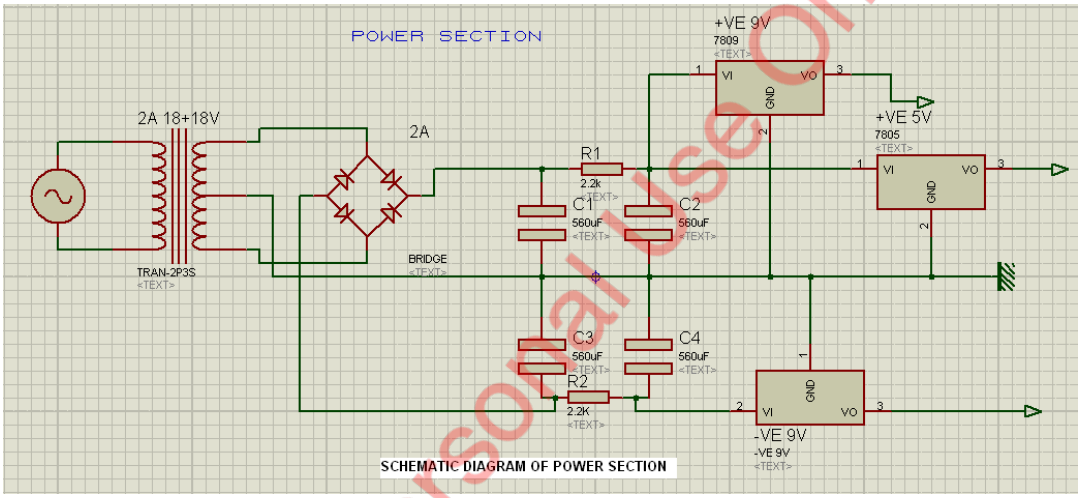
$$V_{av} = \frac{2V_p}{\pi}$$

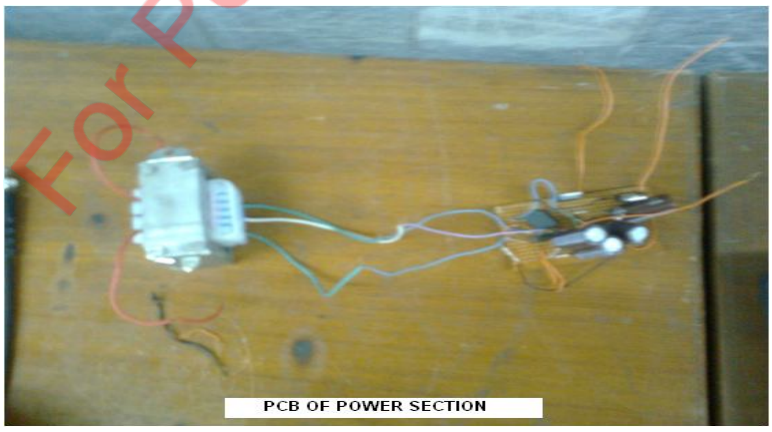
V_p is the value of the peak input voltage to the rectifier.
This implies that V_{avg} = 10.8 V.

Now the output we get from the rectifier is a pulsating DC output with fluctuations between peak value and zero which is undesirable. Therefore we add a capacitive filter to minimize the ripples in the dc voltage. The value of the capacitor is chosen to be as large as possible to minimize the ripples as well as to filter out any high frequency noise.

The final part of the power supply is the regulators. These are used to provide constant voltages of +5, +9 and –9 volts, irrespective of the input voltage. The ICs used for this purpose are LM7805 (+5 V), LM7809 (+9 V) and LM7909 (-9 V).

However, to minimize any unintended fluctuations in regulator output we add more capacitive ripple filters between the regulators and the section's final output.





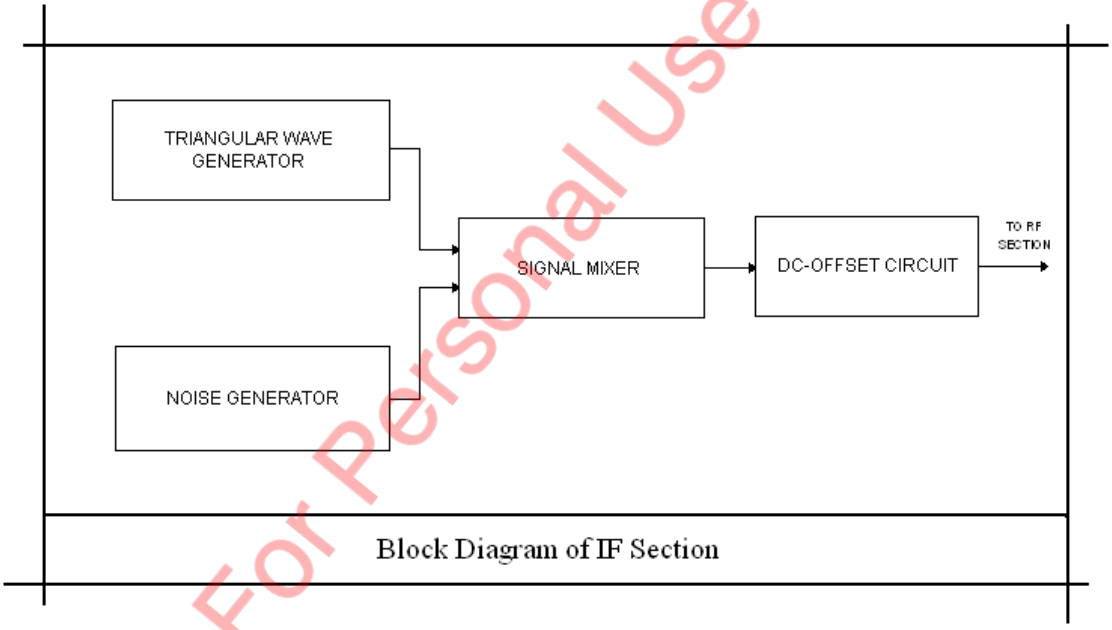
PCB of the Power Supply Section.

3.3 INTERMEDIATE FREQUENCY SECTION

The IF Sections is the section which generates the tuning voltage for the VCO in the RF section so that the output of the VCO is swept through the desired range of frequencies. The output of the IF Section is a triangular wave of frequency 110 KHz to which noise is added and then the signal is offset by a certain DC value to obtain the required tuning voltage.

The components of the IF Section are as follows:

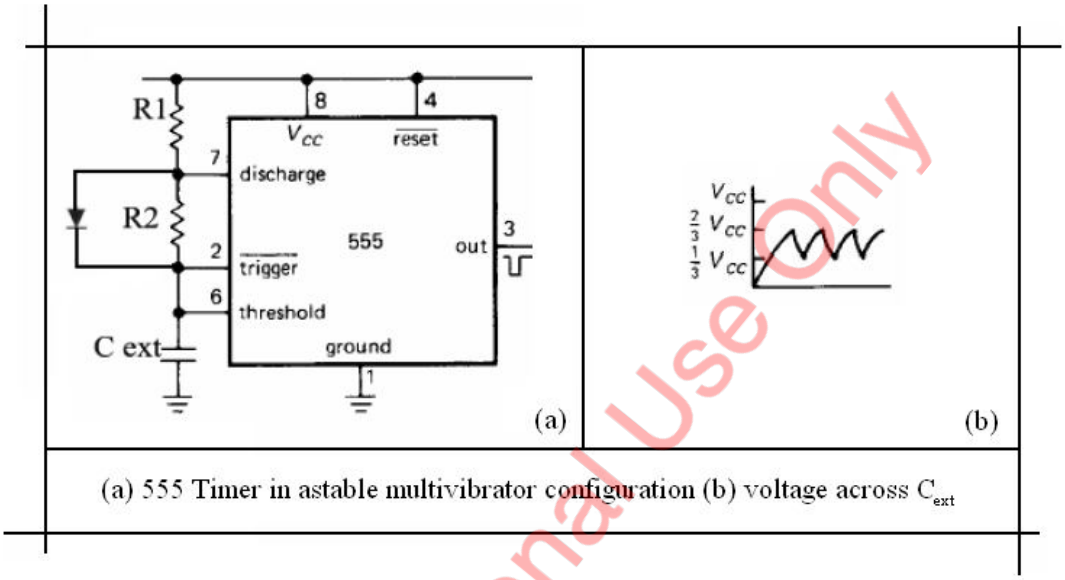
•555Timer IC (Triangular Wave Generator)
•Zener Diode (Noise Generator)
•Op-Amp in Summer Configuration (Signal Mixer)
•Diode–Clamper (Offset Circuit)



Block Diagram of IF Section

3.3.1 TRIANGULAR WAVE GENERATOR:

Our requirement is to have a 110 KHz wave for which we have used a 555 timer IC. The 555 timer is used in the a-stable multi-vibrator mode. It basically consists of two comparators, a flip-flop, a discharge transistors and a resistive voltage divider to set the voltages at different comparator levels. The figure on the next page shows the 555 timer connected to operate in the a-stable multi-vibrator mode as a non-sinusoidal oscillator.



(a) 555 Timer in astable multivibrator configuration (b) voltage across C_{ext}

The following table shows the pin numbers with their respective functions:

Pin Number	Function
1	Ground
2	Trigger
3	Output
4	Reset
5	Control Voltage
6	Threshold
7	Discharge
8	Vcc

The threshold and trigger inputs are connected together. The external resistors R1 and R2 and the capacitor C_{ext} form the timing circuitry that sets the frequency of oscillation. A 0.01 uF has been connected to the Control input of the timer but it is only for decoupling and has no effect on operation.

At the beginning of operation, the capacitor C_{ext} is uncharged and the Trigger input pin is at 0 V, keeping the output of lower comparator to be high and that of the higher comparator to be low, forcing the base of the transistor to be low and keeping it off. Now C_{ext} starts charging through R1 and R2.

The equations for charging and discharging times are given below:

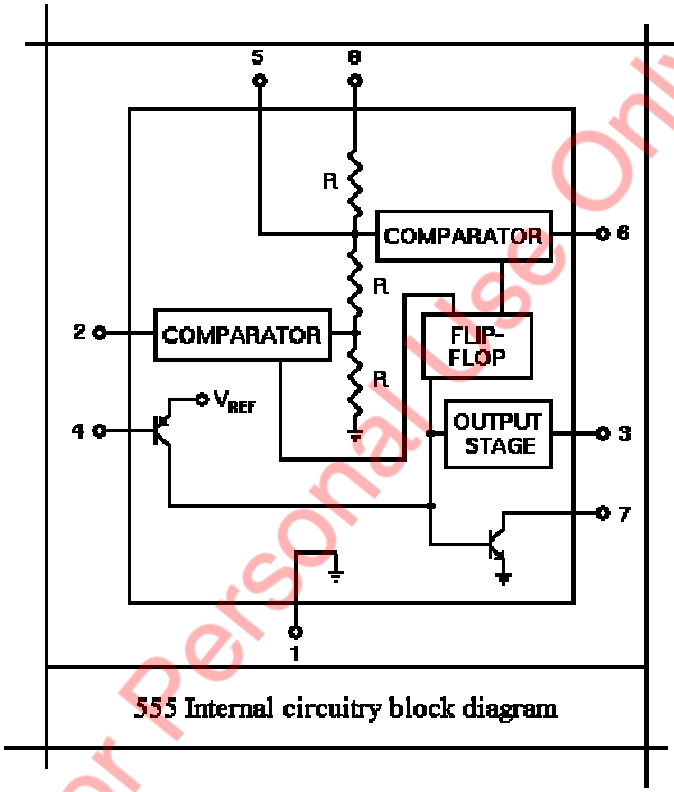
Charging:

$$T_{high} = 0.7(R1 + R2)\, C_{ext}$$

Discharging:

$$T_{low} = 0.7(R2)\, C_{ext}$$

As we need a 50% duty cycle (charging and discharging times to be equal), this is accomplished by keeping R1=R2 and bypassing R2 by a diode during charging.



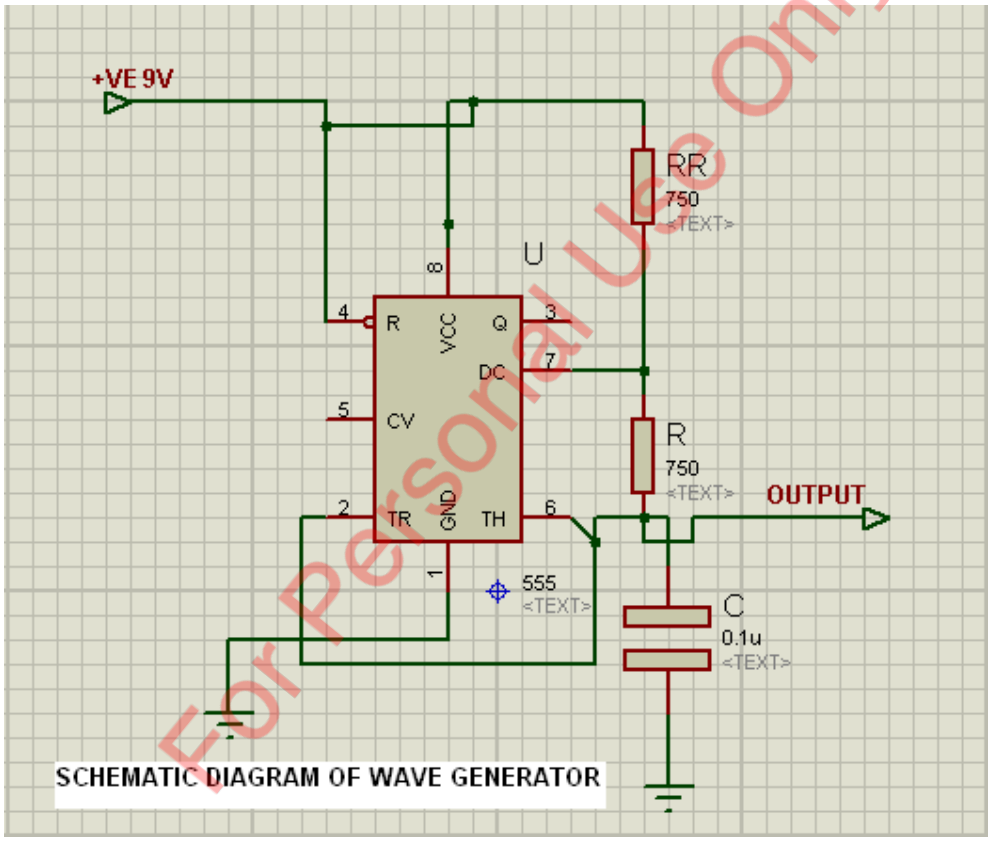
555 Internal circuitry block diagram

As the capacitor charges to $V_{CC}/3$, the output of lower comparator switches to 'low' and as the capacitor charges to $2V_{CC}/3$, the output of higher comparator switches to'high'. The flip-flop is reset by this, causing the base of the discharge transistor to go high and creating a path for the capacitor to discharge through R2 and itself. The capacitor now discharges, causing the output of higher comparator to go low.

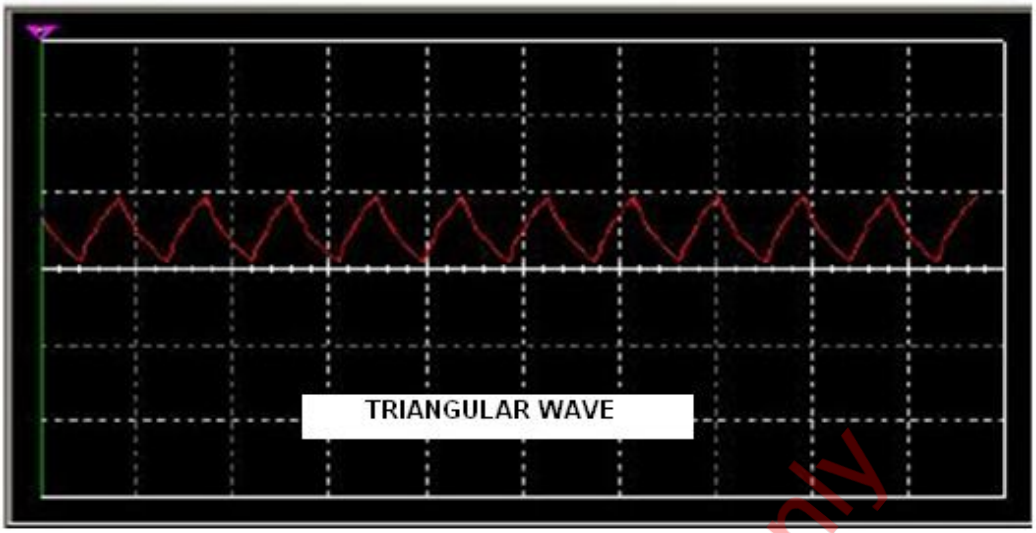
When voltage across C_{ext} reaches $V_{CC}/3$, the output of the lower comparator switches to high, setting the flip-flop and turning off the transistor. This initiates another charging cycle and the process is repeated again and again, resulting in a triangular wave across C_{ext} whose frequency is determined by the formula:

$$f = \frac{1.44}{(R1 + R2)C_{ext}}$$

As we want a 110 KHz triangular wave (requirement of VCO in RF section), we can set the values of R1, R2 and C_{ext} accordingly to get the required output.



SCHEMATIC DIAGRAM OF WAVE GENERATOR



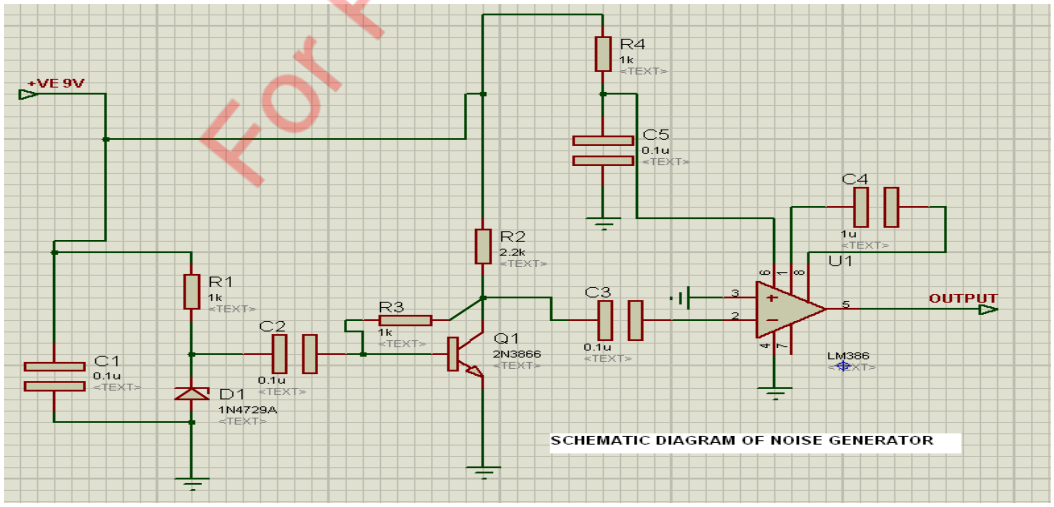
To prevent change in the operating frequency by the loading of timing circuit, the triangular wave from the capacitor was buffered using op-amps.

3.3.2 NOISE GENERATOR:

To accomplish the jamming effect, a noise wave is mixed with the triangular wave to produce the tuning signal for the VCO. The noise masks the jamming signal, making it look like a random noise signal rather than an unmodulated Continuous Wave RF Carrier.

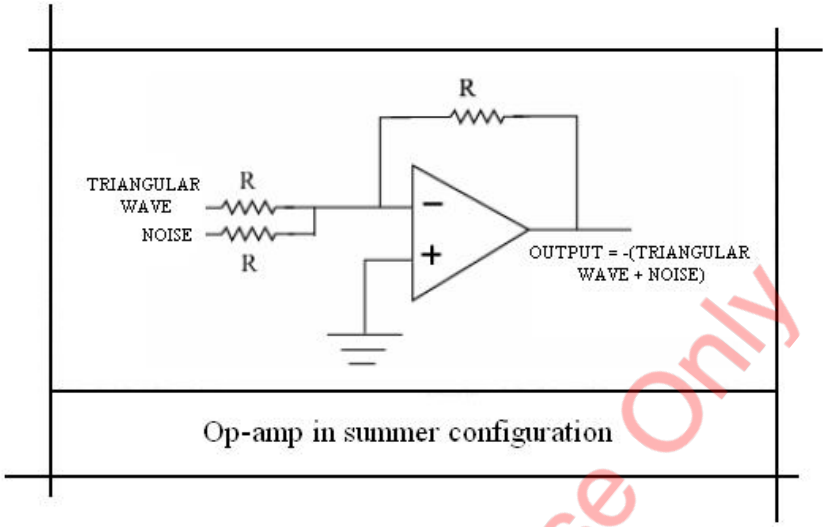
Our noise generator is based on the phenomenon of avalanche noise generated by operating a Zener diode in its reverse breakdown region. Avalanche noise is similar to shot noise but more intense and has a flat frequency spectrum (white noise).

The noise generator circuit consists of a 6.8 V Zener diode with a small reverse current, a transistor buffer, LM386 audio amplifier acting as a natural band pass filter and small signal amplifier.



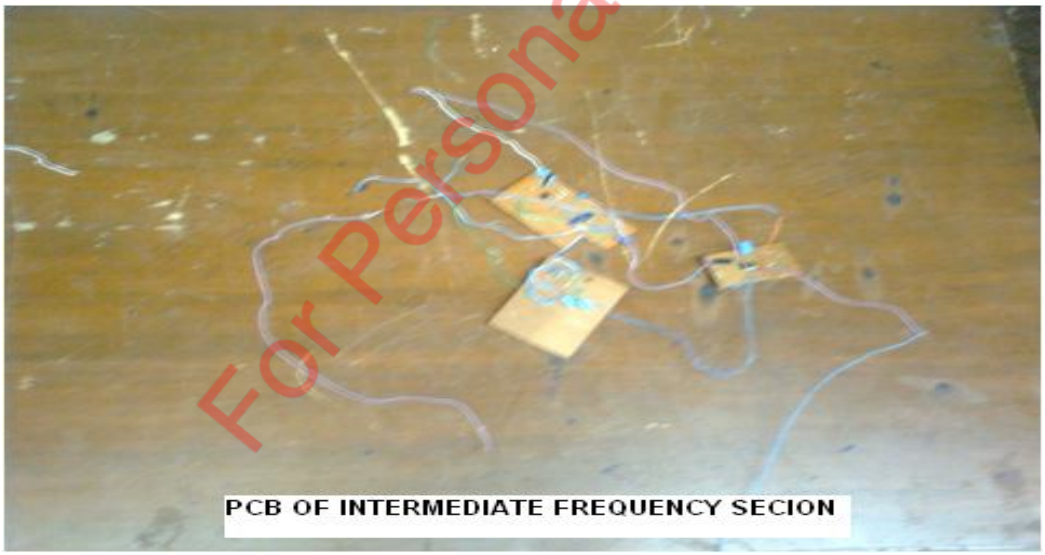
3.3.3 SIGNAL MIXER AND DC OFFSET CIRCUIT:

The triangular wave and the noise wave are summed using an op-amp in a summer configuration.



Op-amp in summer configuration

A DC voltage is then added to the resultant using a diode-clamper circuit to obtain the tuning voltage for VCO.



PCB OF INTERMEDIATE FREQUENCY SECION

3.4 RADIO FREQUENCY SECTION

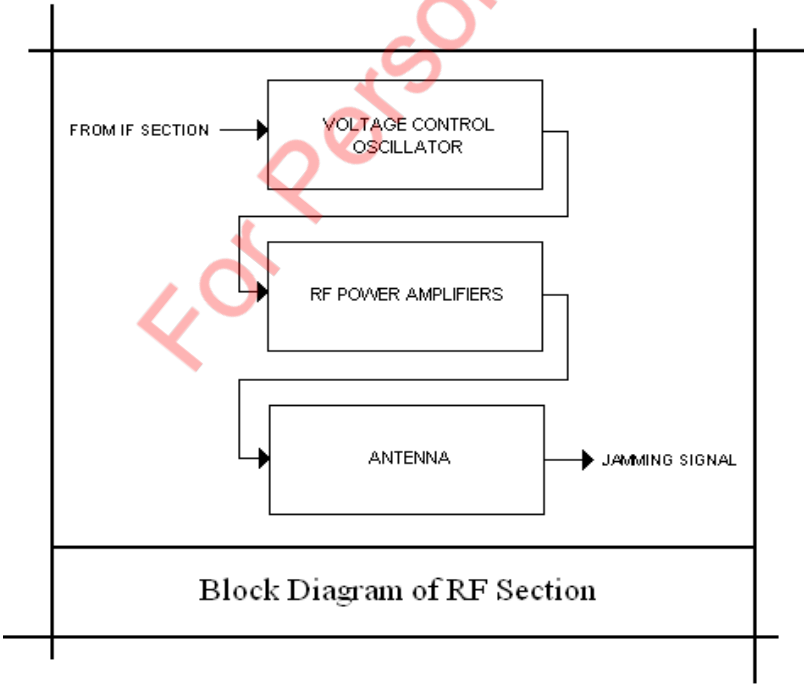
This is the most important part of the Jammer. Its basic components are as follows:

•Voltage Control Oscillator (VCO)
•RF Power Amplifiers
•Antenna

The selection of these components was based on the specification of the jammer such as the desired frequency range and coverage area. All the components used have 50 ohm output impedance, so a 50 ohm micro strip was used for component matching. The width of the micro strip was calculated using the following equations for w/h > 1.

$$Z_0 = \frac{120\pi}{\sqrt{\varepsilon_{eff}}} \times \frac{1}{\left\{\frac{w}{h} + 1.393 + 0.677 \times \ln\left(\frac{w}{h} - 1.444\right)\right\}}$$

$$\varepsilon_{eff} = \left\{\frac{\varepsilon_r + 1}{2} + \frac{\varepsilon_r - 1}{2}\left(\frac{1}{\sqrt{1 + \frac{12h}{w}}}\right)\right\}$$



Block Diagram of RF Section

3.4.1 POWER REQUIREMENTS:

To successfully jam a particular region, we need to consider a very important parameter which is the signal to noise ratio, referred to as the SNR. Every device working on radio communication principles can only tolerate noise in a signal up to a particular level. This is called the SNR handling capability of the device. Most cellular devices have a SNR handling capability of around 12dB. A very good device might have a value of 9dB, although it is highly unlikely. To ensure jamming of these devices, we need to reduce the SNR of the carrier signal to below the 9dB level.

For this, we consider the worst-case scenario from a jammers point of view. This would mean maximum transmitted power S_{max} from the tower, along with the lowest value of the SNR handling capability of a mobile device. So, mathematically,

$$J = -24\text{dBm}$$
$$\text{Since } SNR_{min} = S/J$$

Where, J is the power of the jamming signal.

So we need to have jamming signal strength of -24dBm at the mobile device's reception to effectively jam it. However, our radiated signal will undergo some attenuation in being transmitted from the antenna of the jammer to the antenna of the mobile device. This path loss can be calculated using the simple *free space path loss* approximation:

$$L_p = 32.45 + 20\log_{10}(f.D)$$

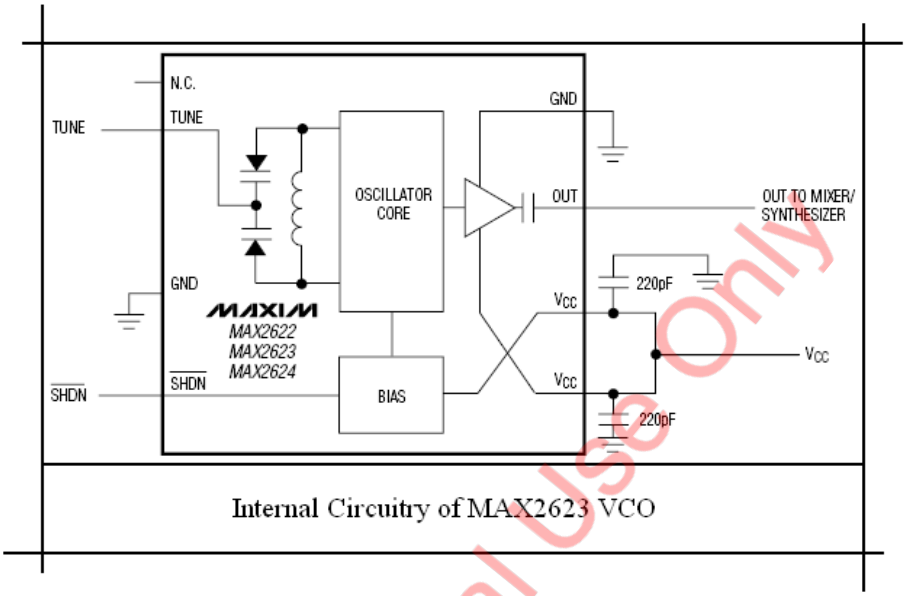
Here f is the frequency in MHz, and D the distance traveled in kilometers. Using the GSM downlink center frequency (947.5MHz) and a jamming radius of 20m, we get the value of path loss to be 58dBm. This ideal path loss is for free space only, and the path losses in air will me much greater. This means that the jamming radius will be less than the 20m used to calculate this value. So, including the power lost in path loss, we need to transmit a signal with strength of:

$$J_T = 58 - 24 = 34\text{dBm}$$

Now, the power output of our VCO is -3dBm, which needs to be amplified by 37dBm to meet our requirements. For this, we used a two-stage amplification mechanism. The first stage is the MAR-4SM pre-amplifier, which provides an 8dBm power gain. This takes the power level to 5dBm. To match the power to the input recommendation of the second amplification stage (the PF08103B); we need to attenuate this by 4dB, for which a pi-attenuator is used. Now the power level is 1dB, which is amplified by a gain of 33dB by the PF08103B to an output power level of 34dBm.

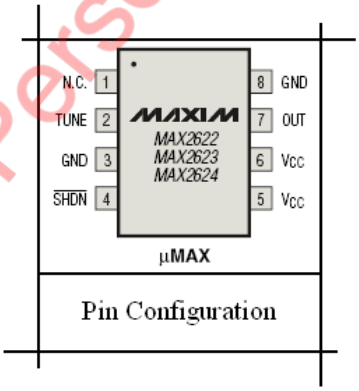
3.4.2 VOLTAGE CONTROL OSCILLATOR (VCO):

This is the main part of the RF Section that is going to generate the required frequency range which will overpower the downlink signals. The main factor that led to the selection of the Max 2623 IC from Maxim IC was the frequency range of the GSM system from 935 MHz - 960 MHz. The second factor was the availability of the chip and was not a big problem.



Internal Circuitry of MAX2623 VCO

The MAX2623 VCO's typical output power is -3 dBm and the output is best swept over the operating range when the input is around 110 kHz.

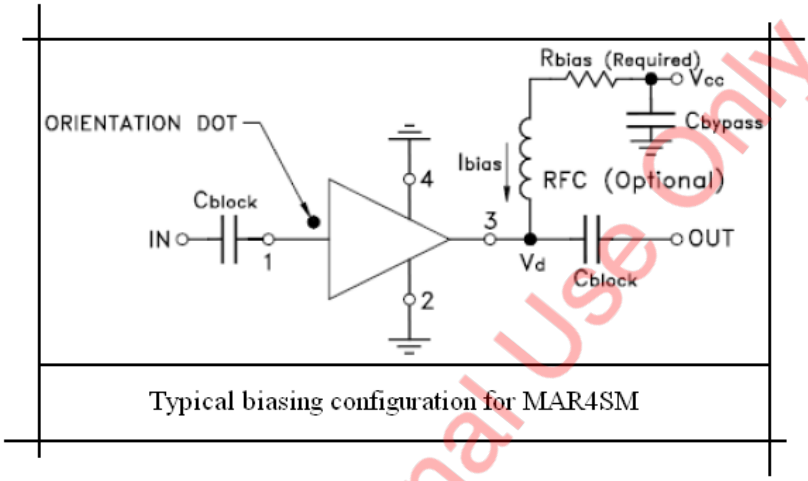


Pin Configuration

3.4.3 RF POWER AMPLIFIERS:

For the desired output to be achieved, gain stages were needed. The Hitachi PF08103B power amplifier module used in Nokia mobile phones sufficiently amplifies signals between 800 MHz and 1 GHz by 34 dB. But the recommended input in the datasheet is 1dBm.

Due to this, another power amplifier was used between the VCO and PF08103B, the MAR4SM amplifier from Mini-Circuits. It has a gain of 8dB for frequencies from dc to 1 GHZ. This made the output 5 dBm. A typical biasing configuration for the MAR4SM is shown.

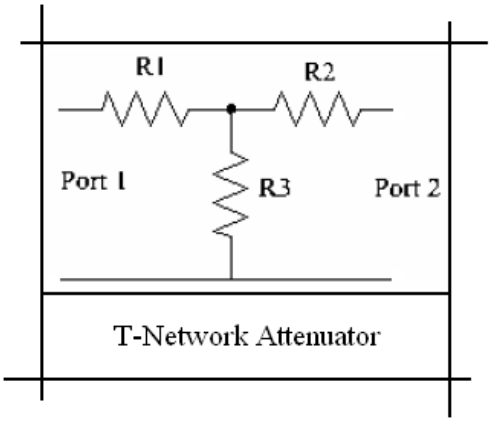


Typical biasing configuration for MAR4SM

The bias current is delivered from a 9 V power supply through the resistor R_{bias} and the RF choke. The effect of the resistor is to reduce the effect of device voltage on the bias current by simulating a current source. Blocking capacitors are required at the input and output ports. A bypass capacitor is used at the connection to dc supply to prevent stray coupling to other signal processing components. The biasing current is given by the following equation:

$$I_{bias} = \frac{V_{cc} - V_d}{R_{bias}}$$

Since the power required for the Hitachi PF08103B power amplifier is 1 dBm and the output of MAR4SM is 5dBm, a 4 dB T-Network Attenuator is used as shown.



For 4 dB attenuation and a symmetrical network, $S_{12} = S_{21} = 0.631$. This implies:

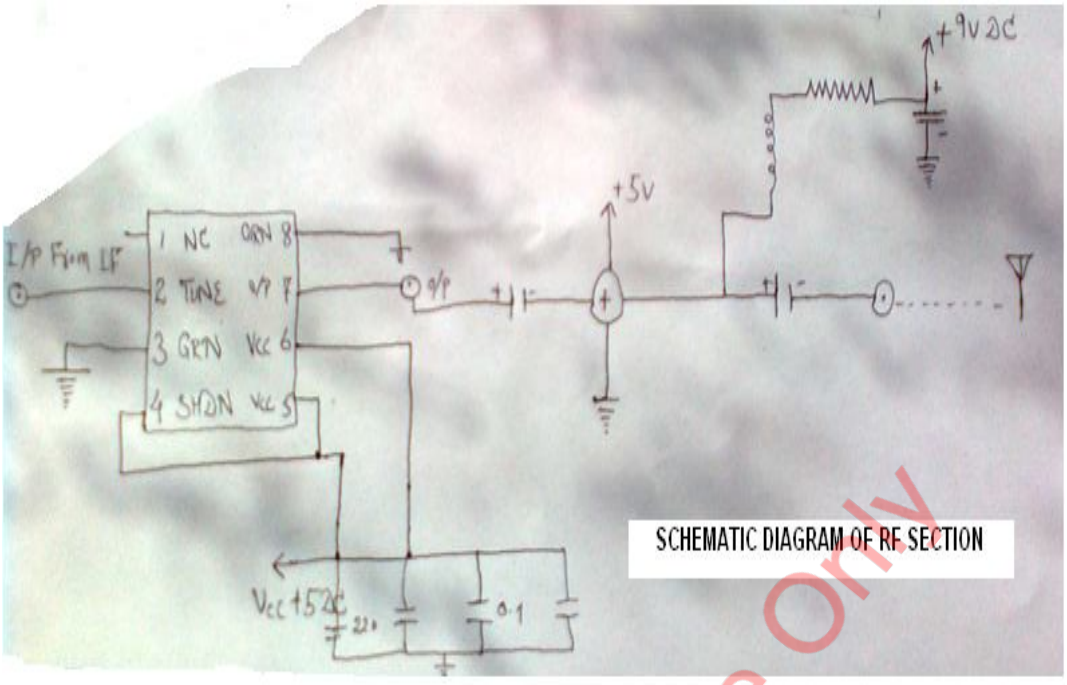
$$V_2 = 0.631 V_1$$

And for 50 ohm characteristic impedance, the values of the resistors were found using the following equations:

$$50 = \frac{R2 + 50}{R3} + R1$$

$$0.631 = \left(\frac{X}{X + R1}\right) \times \left(\frac{50}{50 + R1}\right)$$

Where, $X = \frac{R2 \cdot 50}{R3}$.



The schematic diagram of the Radio Frequency section is shown.

3.4.4 ANTENNA:

At this point, we have a transmissible signal ready. Now we need to radiate it into our intended area to produce the desired jamming effect.

Antenna designs are pattern and frequency specific. This means we needed to select the right antenna that matched:

- The correct frequency range (935-960MHz)
- An Omni directional radiation pattern

From among the various antennas available in the market, we tested a few that matched our criteria using a network analyzer. The antenna used in the project was a helical antenna, with a reflection coefficient of -17dB. It should be noted that the smaller the reflection coefficient, the better. And this value of -17dB is a very good value.

HELICAL ANTENNA

3.5 TESTING

The equipment was tested on oscilloscope and its output was found to 5dBm at the RF section. However, due to unavailability of the Power Amplifier PF 08103b the output power remained limited. If a better amplifier is used like the one stated above then the output and effective distance may be increased which relates directly to the power of the amplifier.

CHAPTER 4
USER GUIDE

4.1 INTRODUCTION

The Jammer has been made in order to be used only for the sake of research purpose. Its out put may be seen as a continuous noise signal of random nature. The important facts that needs to be considered have been evaluated through this chapter to make a user able to join all the connections and put the jammer into operation. The salient features include the connection between all of the parts i.e. Power section, IF Section and RF Section. Once integrated, the jammer starts working with a 110~220V AC source.

4.2 POWER

Once all the components i.e. the power section, the intermediate frequency section and the radio frequency section have been connected to each other. A current source will be provided by means of a centrally taped transformer. The regulators in the Power section will regulate the threshold to a pre set level and will maintain a continuous supply.

4.3 OSCILLOSCOPE OUTPUT

Once the device is successfully put into operation. The next step is to check its output on oscilloscope. The probe of oscilloscope will be connected to the output wire of the 555 timer IC. It will show a signal in the form of a sawtooth. This is our required carrier.

The noise signal will appear as a random signal with varying amplitude at some instants. We may also check the amplitude and DC component of the signal if there is any.

In the Mixer, the two signals i.e. the noise signal and the carrier are to be mixed with the help of a mixer IC. The noise will appear as riding onto the carrier signal i.e. the sawtooth wave. This is our required noise signal with a constant amplitude. The signal may be DC blocked if required and the output may also be checked on oscilloscope by putting the probe on the output of DC Blocker.

In the RF section, the IC MAR4SM will simply swing the input signal into a sine wave pattern. This is our required signal which is propagated through a helical antenna being used in the project. The output may be checked by putting the probe shortly after the DC Blocker component which is in parallel to the MAR4SM IC.

4.4 NOTICES

Before linking all the sections and antenna, power supply shall not be switched on at first. Do non take off any component when the jammer is in the working condition.

The jammer shall be installed in the position with good ventilation. And large scale things shall be avoided to ensure to the shielding effect.

When use the jammer outdoors, preventing water shall be taken into consideration.

Antenna shall be used vertical to the ground.

4.5 FAQS

Q. Will jammer interference the other electronic equipment to be in good working condition?

A. No. Because the electromagnetic signal sent by jammer are totally used in the band that regulated by government and just have interception effect to cell phone communication.

Q. Will jammer have bad effect to human body and cell phone?

A. You should not worry about it. The intensity of electromagnetic signal sent by jammer is in compliance with the national standard of environmental electromagnetic wave health, the signal sent by jammer is relatively small and no damage will appear on human body according to the testing files. Mean while, this device is just damage the receiving condition to cell phone and makes the normal connection between cell phone and base station impossible. Therefore, no damage will occur on cell phone itself.

Q. Is there any difference of distance between using jammer indoor and outdoor?

A. Yes. Generally speaking, outdoor signal is bigger than the indoor signal. Thereby, the shielding effect is worse outdoor. Strictly speaking, whether using indoor or outdoor, the effective distance of interception is related to the surrounding environment as the distance between different base stations, positions of installation, etc.

Q. The visible body of jammer will become hot after working for some times. Does the long time keeping in working condition will damage the machine it self?

A. It is very normal. While designing, we are thinking of taking use of the conductivity of metal shell to help the heat sinking during our designation, by this way, the machine can be kept in good working condition for long time.

CHAPTER 5
CONCLUSION

5. CONCLUSION

The jamming device was successfully designed and subsequently constructed with similar success. It was tested in the presence of our supervisor with an output power of approximately 5db. Amplification greater than 12dbm is required to successfully jam a cellular signal. The required IC PF08103B was unavailable in the markets of Pakistan as it is a rare one and only manufactured abroad. The same IC of HITTITE may be used to amplify the signal but the problem with this IC is that it has an internal Gain of 20dB which may not be suitable for this operation as it adversely affects the jamming radius below the maximum theoretical value calculated, because of atmospheric losses. The range varied from 5m to up to 10m depending upon atmospheric conditions (such as the time of the day), and the coverage intensity at the testing site.

The device may be tested against all cellular carriers currently operating on the GSM band in Pakistan, including:

- Mobilink GSM
- Telenor
- Warid
- Zong
- Ufone

The power section of the device was, despite the complete success of the rest of the project, a bit troublesome near the end. Because of the lack of current regulation, the subsequent sections experienced voltage dips, which made the device less dependable.

To overcome this issue, a better power supply with current regulation can be designed, or a separate power supply can be used altogether.

CHAPTER 6
REFERENCES AND BIBLIOGRAPHY

6. REFERENCES & BIBLIOGRAPHY

• The International Engineering Consortium, http://www.iec.com/

• Cellular Communication Networks by Gerald Williams

• http://www-students.doc.ic.ac.uk/

• Performance Issues of Cellular Networks by Rajkumar Periannan & Fadi Joseph Fahham

• http://www.maxim-ic.com/appnotes

• http://www.mini-circuits.com/application.shtml

• http://gbppr.dyndns.org/PROJ/mil/celljam/pf08103b.pdf

• http://www-dse.doc.ic.ac.uk/~nd/surprise_96/journal/vol2/fjf/article2.html

• http://ccnga.uwaterloo.ca/~jscouria/GSM/gsmreport.html

• http://www.rabc.ottawa.on.ca/e/Files/01pub3.pdf

• www.jlab.org/accel/eecad/pdf/050rfdesign.pdf

• www.mumor.org/public/publications/ISCAS_2004_MuMo_Receiver.pdf

• Floyd, Electronic Devices, Prentice Hall, 5th Edition

• Horowitz, P.; Hill, W., The Art of Electronics, 2nd Edition, Cambridge University Press