Novel Design for Mobile Phone Jammer

By

Maj Ali Raza Khan

Maj Muhammad Qasim Latif

Maj Shahzad Maqbool

Capt Mohsin Malik

Supervised by:

Dr Farooq Ahmed Bhatti

Submitted to the faculty of Department of Electrical Engineering,
Military College of Signals, National University of Sciences and Technology, Islamabad,
in partial fulfillment for the requirements of B.E Degree in Electrical (Telecom) Engineering.

June 2023

In the name of ALLAH, the Most benevolent, the Most Courteous

CERTIFICATE OF CORRECTNESS AND APPROVAL

This is to officially state that the thesis work contained in this report

"Novel Design for Mobile Phone Jammer"

is carried out by

Maj Ali Raza Khan

Maj Muhammad Qasim Latif

Maj Shahzad Maqbool

Capt Mohsin Malik

under my supervision and that in my judgement, it is fully ample, in scope and excellence, for the degree of Bachelor of Electrical (Telecom.) Engineering in Military College of Signals, National University of Sciences and Technology (NUST), Islamabad.

Approved by

Supervisor
Dr Farooq Ahmed Bhatti
Department of EE, MCS

Date: **April 26,2023**

DECLARATION OF ORIGINALITY

We hereby declare that no portion of work presented in this thesis has been submitted in support of another award or qualification in either this institute or anywhere else.

ACKNOWLEDGEMENTS

Allah Subhan'Wa'Tala is the sole guidance in all domains.

Our parents, colleagues and most of all, Dr Farooq Ahmed Bhatti, without your guidance the completion of our project could not have been accomplished. Mr. Ahsan Javed, PhD student of our supervisor, also guided us through his vast experience in the field And The group members, who through all adversities worked steadfastly.

Plagiarism Certificate (Turnitin Report)

This thesis has 25% similarity index. Turnitin report endorsed by Supervisor is attached.

_____

Maj Ali Raza Khan

NUST Serial no: 00000325143

_____

Maj Muhammad Qasim Latif

NUST Serial no: 00000325203

_____

Maj Shahzad Maqbool

NUST Serial no: 00000325197

_____

Capt Mohsin Malik

NUST Serial no: 00000325179

_____

Signature of Supervisor

ABSTRACT

The goal of the project is to design a mobile phone jammer which is cheap and compact. Multiple utilities that the project offers, include, maintaining mobile phone silence in libraries, mosques, and offices. It can also help to avoid unfair means via use of mobile phones in exam halls. The project also offers prevention against IEDs in conflict zones.

The project makes use of a noise generator whose output is fed to several VCOs, operating on different frequencies being used by mobile phones. Using multiple antennas the noise signal modulated with GSM, DCS, CDMA and 3G frequencies, respectively, are transmitted to do the desired jamming.

To avoid overheating, a heat sink, along with cooling fans, is used for operating the jammer for longer durations. Its compact size and light weight help in its easy operation and quick mobility.

The project will be a great deal for several organizations including educational institutes, security organizations and especially law enforcement agencies.

Contents

Chapter 1: Introduction

1.1 Overview

The use of mobile phones has increased dramatically in recent years. This has made it necessary to utilize a more effective and manageable signal transmission in places like libraries, hospitals, and conference rooms where stillness is required. Additionally, there has been an upsurge in the detonation of radio-controlled IEDs, particularly mobile-triggered IEDs, which may be operated from miles away thanks to the ability of mobile signals to travel long distances. Mobile phone jammers are now more commonly used to counter such threats. Although there are jammers on the market, they are only compatible with the first two GSM bands because the public now has access to 3G and 4G mobile technologies. But they don't yet have a countermeasure. However, if they perform, they have very expensive countermeasures that are not yet available. Therefore, a jammer that can block all four mobile frequency bands is required. It also needs to be reasonably priced.

1.2 Problem Statement

Even though mobile phones have many benefits and are extremely useful, their fast spread has made them a problem in our daily lives as well as an annoyance. Here are some issues that using a mobile phone has brought about in our daily lives:

In locations requiring a significant degree of silence, such as meetings, libraries, places of worship, courtrooms, etc. The necessary silence in these settings can be disturbed by the sporadic ringing of people's phones. To completely deny service so that persons inside the area where phone use is restricted cannot access it, it is vitally important to appeal to the users' consciences to turn off their phones.

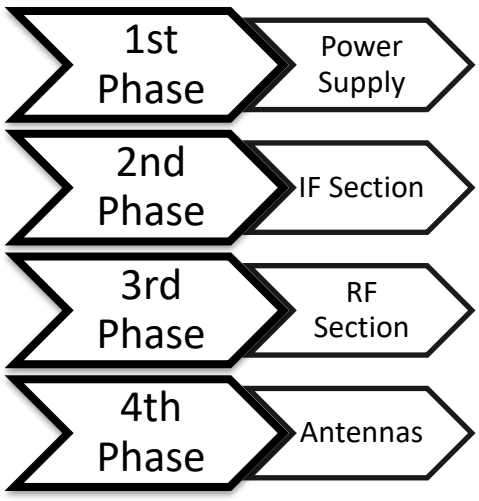
Students might use their mobile devices to look up information online or communicate information over SMS during exams. Jammers must be used in order to stop fraud in testing facilities.

As mobile technology advanced, terrorist groups began to use mobile-triggered IEDs more frequently since they could be operated from a distance. Jammers must be put in public spaces to eliminate this threat and protect the populace from the impacts of IEDs.

1.3 Approach

1. Design a power supply to give input to IF and RF section.
2. Design an IF (Intermediate Frequency) section to generate a tuning signal and to generate a noise signal which would create the jamming effect.
3. Design the RF (Radio Frequency) section and feed it the tuning and noise signal to generate the jamming transmissions.
4. Design monopole antennas for enhanced range

The illustration depicts the steps that will be taken over the time period in order



1.4 Objectives

1. To design a compact, low cost, and portable mobile phone jammer with enhanced range
2. To design and develop Radio Frequency, power amplifier, Intermediate Frequency, and Power Supply circuit for the said mobile phone jammer.
3. To block mobile phones transmission by using methodology of noise generation.
4. To effectively disable cellular communication in the regulated zone without interfering with other communications.

1.5 Scope

Designing a cheap, compact and portable jammer with relatively enhanced range which can be used as a prototype for commercial use.

1.6 Relevant Sustainable Development Goals

Build resilient infrastructure, promote inclusive and sustainable industrialization and foster innovation.

1.7 Structure of Thesis

The introductory section, which outlines the problem statement, strategy, and goals, comes after the abstract, which provides a summary of the project's major components (the "Novel Design for Mobile Phone Jammer"). The many internet resources that were read before the study started are included in the literature review section. It gives a succinct summary of the various mobile technology generations. likewise, a little overview of the GSM systems. Diagrams illustrating the detailed design of the jammer, its components, interfaces, and data required for the implementation

phase are shown in the design and development section. The specific comparison of the actual results to the predicted results is done in the analysis and assessment phase. The improvements that can be made to the application are described in the future work.

Chapter 2: Literature Review

Since the goal of this project is to successfully jam mobile phone communication systems, it was crucial to thoroughly study mobile communications in order to become familiar with all of the strategies used by these systems and identify any vulnerabilities that might make it difficult to successfully jam such effective networks. The collection of these studies could be categorized as follows:

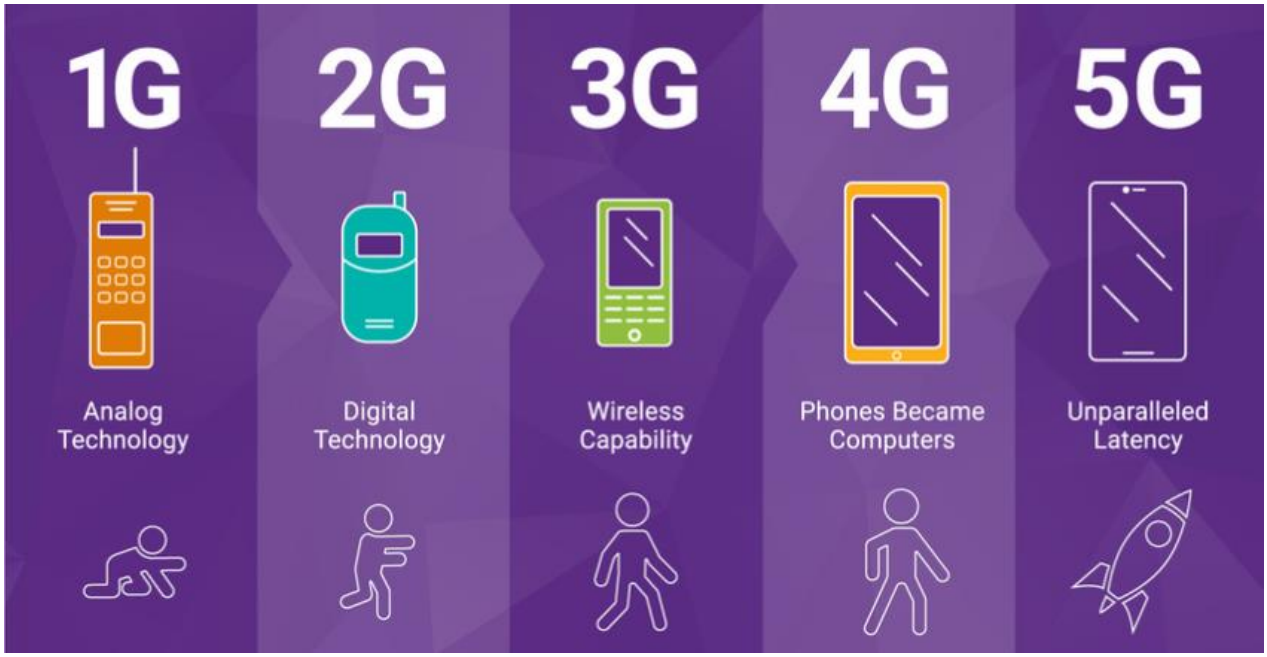
2.1 Brief Description of Technologies Used in Cellular Telephone Systems.

The effective utilization of the available frequencies is one of the essential components of any radio-based communications system. Cellular frequency reuse is one of the main technologies utilized in cellular mobile radio. The use of analogue technology was a defining feature of the first generation (1G) of systems. Different channels were assigned to different users within the same cell. FDMA, or frequency division multiple access, is the name of this method. The analogue systems (1G) were created for voice applications, and these include systems like the Advanced Mobile Phone System (AMPS), Nordic Mobile Telephone (NMT), Total Access Communication System (TACS), etc. Although all of these systems had changeover and roaming capabilities, cellular networks could not communicate across international borders. This was one of the unavoidable drawbacks of first-generation mobile networks. Additionally, as demand increased, the available spectrum gradually became increasingly crowded. It became immediately clear that a less 18 spectrum-hungry approach would be needed as a result.

The second generation of systems (or 2G) was born as a result. Digital technology was used by 2G systems to achieve the necessary levels of efficiency. All of the early 2G systems, including GSM,

US-TDMA, and its descendant PDC (Pacific Digital Cellular), combined FDMA with another method in which various users were given distinct time slots on the same channel. This system became known as Time Division Multiple Access (TDMA). Because these systems (2G) provided few data facilities, temporary solutions were sought. Higher data speeds than those made feasible by 2G systems were offered by 2.5G systems. An improvement in data rate was made possible by the introduction of the General Packet Radio Service (GPRS) system with GSM. Here, the main modification was the substitution of packet radio systems for the earlier systems' circuit switches. Up to 115 kbps of data rate was possible. Another technology called Enhanced Data rate for GSM Evolution (EDGE), which has a higher data rate, was introduced. Although the systems mentioned above employ a time division method, another system employed a different method. It was based on spread spectrum technology and employed code division multiple access (CDMA), which used various codes to grant access to various users. Originally, CDMA One, a system that utilized the full 2G standard, used this technology. Third generation systems (3G systems) use its concept.

To reach 3G systems, CDMA 2000 1X offered an evolutionary path. The CDMA20001x EV-DO (EV-DO stands for Evolution Data Only) is a data-only device with a peak downlink data rate capability of over 2.4Mbps. Following it, CDMA2000 1xEV-DV The CDMA2000-based EV-DV system, which stands for "Voice and Data Only," is another 3G technology that supports simultaneous voice and data transmission. Its max rate is capped at approximately 3.1 Mbps on the forward channel (downlink) and 384 kbps on the reverse 19 channel (uplink). Wideband CDMA (WCDMA), used by the Universal Mobile Telecommunication System (UMTS), offers data rates of up to 2Mbps. Time Division Synchronous CDMA (TD-SCDMA), another 3G system, uses the same time slot for communication between base stations and mobile devices. As opposed to other 3G systems, which employ the time division duplexing (TDD) method. As the demand for more



spectrally efficient technologies and extremely high data rates increased, more solutions were sought. The 3.5G system or technology known as High-Speed Packet Access (HSPA) was created. With packet data, this results in a peak rate of roughly 14.4Mbps on the forwards.

The next generation of systems, including the Ultra-Mobile Broadband (UMB) which is a 3.99/4G evolution cellular technology for CDMA 2000 and the Long-Term Evolution (LTE). The fourth generation of cellular networks is known as 4G. 4G networks, which were first made available to the general public in 2009, provided noticeably faster data speeds, lower latency, and more effective use of the radio frequency spectrum. Today, 4G networks handle more than 50% of all mobile connections. Users were given access to a wider bandwidth of 100 to 300 Mbps. Nevertheless, the telecoms sector sought more ways than ever before to innovate and lower latency.

With speeds of 10 Gbps, the next generation of wireless technology, or 5G, opens up a plethora of opportunities. The performance of 5G, a software-based network that employs cloud computing, is 20 times quicker than that of 4G. It takes advantage of technological innovations like full duplex, millimeter wave, smarter cells, massive multiple in multiple out (MIMO), and beamforming.

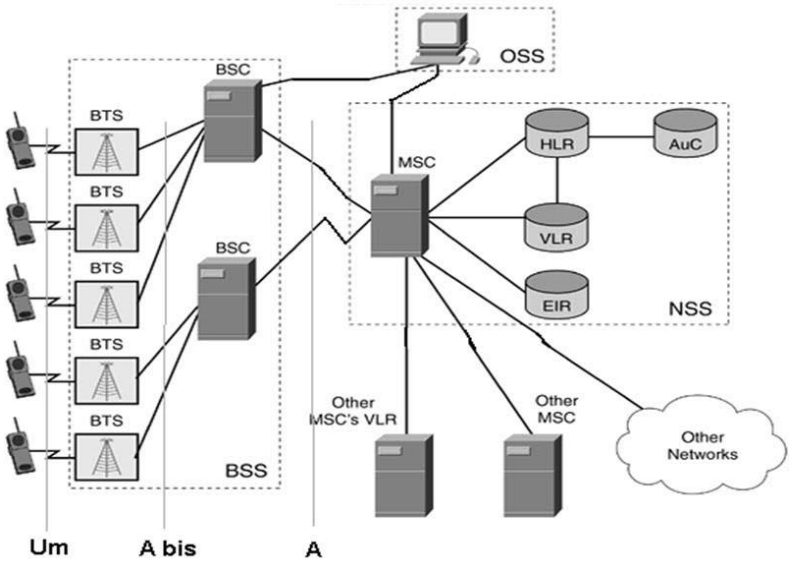
2.2 Brief Overview of GSM

The European Telecommunication Standards Institute (ETSI) created the Global System for Mobile Communication (GSM), formerly known as Groupe Spécial Mobile, as an open digital mobile telephony standard to describe technologies for second-generation cellular networks. The GSM system was not created to be backwards compatible with the existing analogue systems; it is a digital-only system. In various European countries, analogue cellular systems temporarily share the GSM radio frequency. The most popular of the three digital wireless telephony technologies (TDMA, GSM, and CDMA) employs a form of time division multiple access (TDMA). GSM operates in the 900 or 1800 MHz frequency band, digitizes, and compresses data before sending it down a channel with two other streams of user data, each in its own time slot.

2.3 Architecture and Operation of GSM Network

The foundation of the GSM mobile telecommunications service is a network of interconnected radio cells that completely enclose the service area and enable subscriber operation wherever inside it. Radio phones were in use prior to the development of the cellular concept, but they were only capable of reaching a large region with a single transmitter. When a user moves their phone from one location to another while on a call, the cellular phone has an advantage over a radio phone in that it can transfer the call from one cell to the next. Although using a cellular phone is entirely automatic and doesn't require any additional user activity, it is a sophisticated technical procedure that needs a lot of computing power to respond quickly. The Mobile Station (MS), Base Station Subsystem (BSS), Network Switching Subsystem (NSS), and Operations and Maintenance Subsystem (OMC) are the four major components that make up the GSM system's functional architecture.

GSM SYSTEM ARCHITECTURE

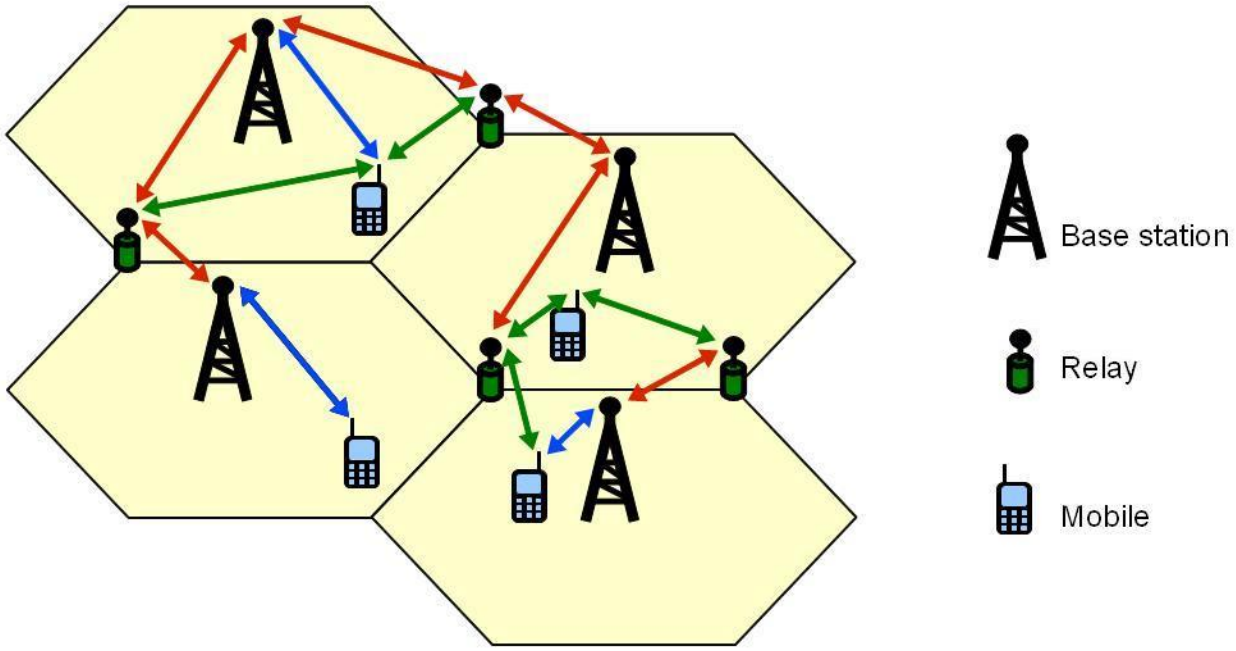


- **Mobile Station (MS)**
  - Mobile Equipment (ME)
  - Subscriber Identity Module (SIM)
- **Base Station Subsystem (BSS)**
  - Base Transceiver Station (BTS)
  - Base Station Controller (BSC)
- **Network Switching Subsystem(NSS)**
  - Mobile Switching Center (MSC)
  - Home Location Register (HLR)
  - Visitor Location Register (VLR)
  - Authentication Center (AUC)
  - Equipment Identity Register (EIR)

Each subsystem is made up of functional units that connect with one another using predetermined protocols through the various interfaces. Carrying the mobile station is the subscriber. The mobile station, which consists of two components, is the only system-wide equipment that a GSM user ever sees. The technological component is known as a mobile phone. The mobile phone is made up of components like radio transceivers, digital signal processors, and displays. The SIM, which is implemented as a smart card, is the additional component. A subscriber's international mobile subscriber identification (IMSI), a secret key for authentication, and other user data are all stored on the SIM card. Only when a working SIM card given by a network operator is inserted into the mobile device or phone does it become functional. The radio link with the mobile station is managed by the base station subsystem. The mobile services switching center (MSC), which is the primary component of the network and switching subsystem, manages mobile services including authentication in addition to switching calls between mobile and other fixed or mobile network users.

2.4 A Network of Cells

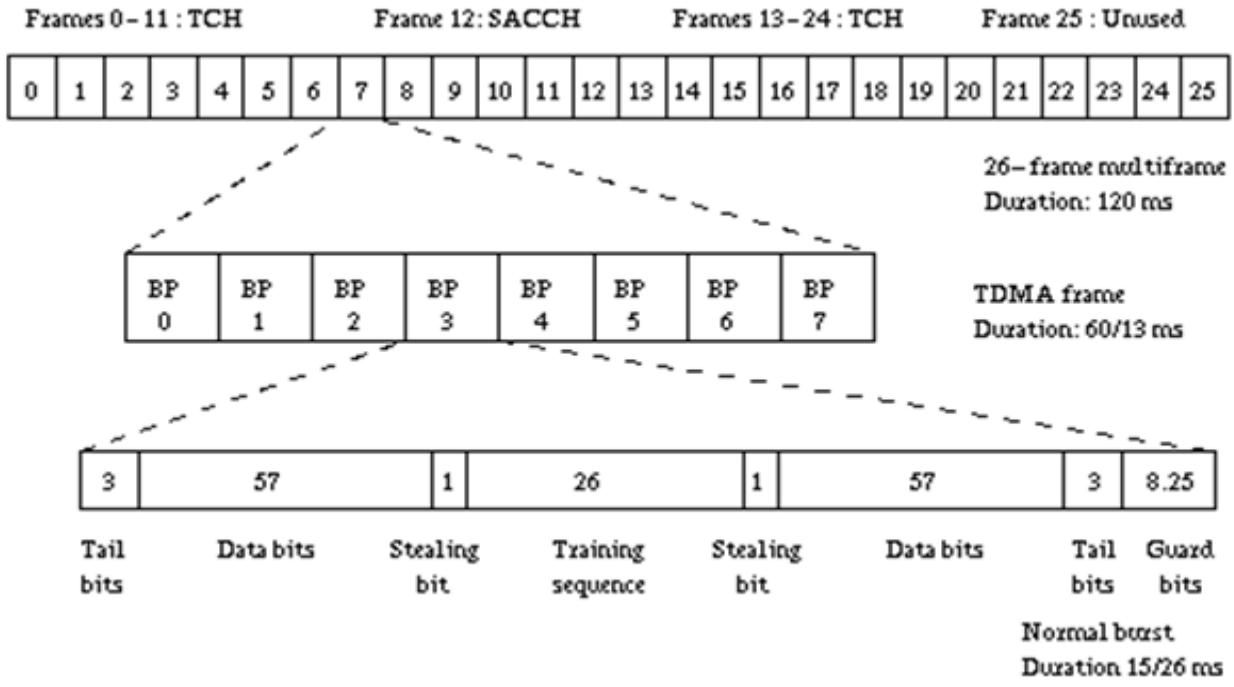
GSM Network in a country is divided into Location Areas (LA). LA can be identified by the system using the Location Area Identity (LAI). Location Area is divided into many cells. Cell is an identity that one BTS serves. The Base Station Identification Code (BSIC), which is transmitted by the cell, is used by the MS to distinguish between cells. At the cell boundary, the received power should lead to an acceptable bit error rate (BER).



2.5 Multiple Access and Channel Structure

Since radio spectrum is a finite resource that all users share, a strategy must be developed to distribute the bandwidth among the greatest number of users. Time and frequency division multiple access (TDMA/FDMA) is a combination used by GSM. The (maximum) 25 MHz bandwidth is divided into 124 carrier frequencies, or "carrier spacing," that are spaced 200 KHz apart in the

FDMA portion. Each base station has one or more carrier frequencies assigned to it. The frequency of each of these carriers is then divided into time using a TDMA technique. In the TDMA method, a burst period, which lasts 15/26ms (about 0.577ms), is the basic unit of time. A TDMA frame (120/26 ms, or around 4.615 ms), which serves as the fundamental building block for the construction of logical channels, is made up of eight burst periods. Per TDMA frame, there is one burst period, or physical channel.



2.6 Multiplexing Techniques

The method by which radio communications are maintained in both directions is one of the crucial components of any radio communications system. Methods that can be employed include simplex, duplex, frequency division duplex (FDD), and time division duplex (TDD). The two multiplexing methods or systems that are frequently used in cellular and cordless telephones are:

2.6.1 Frequency Division Duplexing (FDD)

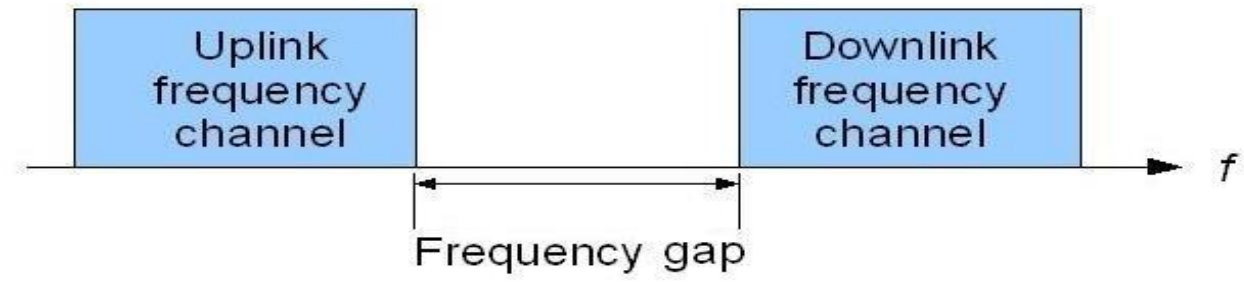
In FDD, two symmetric frequency bands are used for communication between mobile and base stations. To enable simultaneous transmission and receiving, the available frequency band is divided into two partial bands. The other partial band is designated as downlink (from base station to mobile station), with one partial band designated as uplink (from mobile to base station). Uplink: Mobile station transmission band equals base station reception band. Downlink: Mobile station receiving band equals base station transmission band.

2.6.2 Time Division Duplexing (TDD)

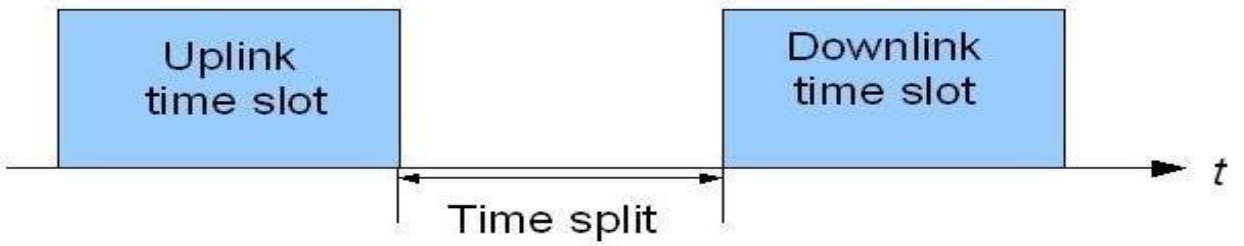
TDD systems only employ one frequency, sharing the channel between transmission and reception while spacing them apart by time-division multiplexing of the two signals. To put it another way, the voice call's uplink and downlink are time multiplexed on the same frequency. Since the system employs frequency division duplex, the channels are paired, with one used for the BTS's downlink to the mobile and the other for its linkback. The reference of the band in use affects how much frequency is different between the two channels.

2.7 What GSM Offers

The designers of GSM sought interoperability with the Integrated Services Digital Network (ISDN) in terms of the services and control signaling employed. However, the conventional ISDN B-channel (carrier channel) data rate of 64 kbps cannot be attained in practice due to radio transmission limits in terms of bandwidth and cost. Bearer services, teleservices, and supplemental services are three categories of telecommunications services. Telephony is a basic teleservice that GSM supports. Speech is digitally encoded and delivered across the GSM network as a digital stream, just like all other forms of communication. Additionally, it offers an emergency service that works similarly to 911 in that it allows users to call the nearest emergency service provider. Other data services include group 3 facsimile, which is supported by using a suitable fax adaptor and is described by ITU-T recommendation T.30. The Short Message Service (SMS) is a distinguishing feature of GSM that is absent from more ancient analogue systems. SMS is a two-way service for



(a) FDD



(b) TDD

sending and receiving brief alphanumeric messages (up to 160 bytes). A 26 store-and-forward method is used to transmit messages. With point-to-point SMS, the sender receives a confirmation of delivery after sending a message to another service user.

SMS can also be used to broadcast messages to a cell, such as news or weather updates. Additionally, messages can be kept on the Subscriber Identity Module (SIM) card and retrieved at another time.

2.8 Frequency Bands

Mobile networks use frequency bands, which are collections of radio frequencies, to communicate with mobile phones. Cellular frequencies called GSM frequency bands are set aside by the ITU for the use of GSM mobile phones. Where and on which networks a phone can be used depend greatly on the frequency bands that it supports. GSM was initially created to operate in the 900MHz band. The Digital Cellular System 1800 (DCS 1800), the first GSM derivative, was created through subsequent improvements. This innovation converts the GSM system to the 1800MHz frequency band.

Chapter 3: Development and Design

3.1 Design Factors

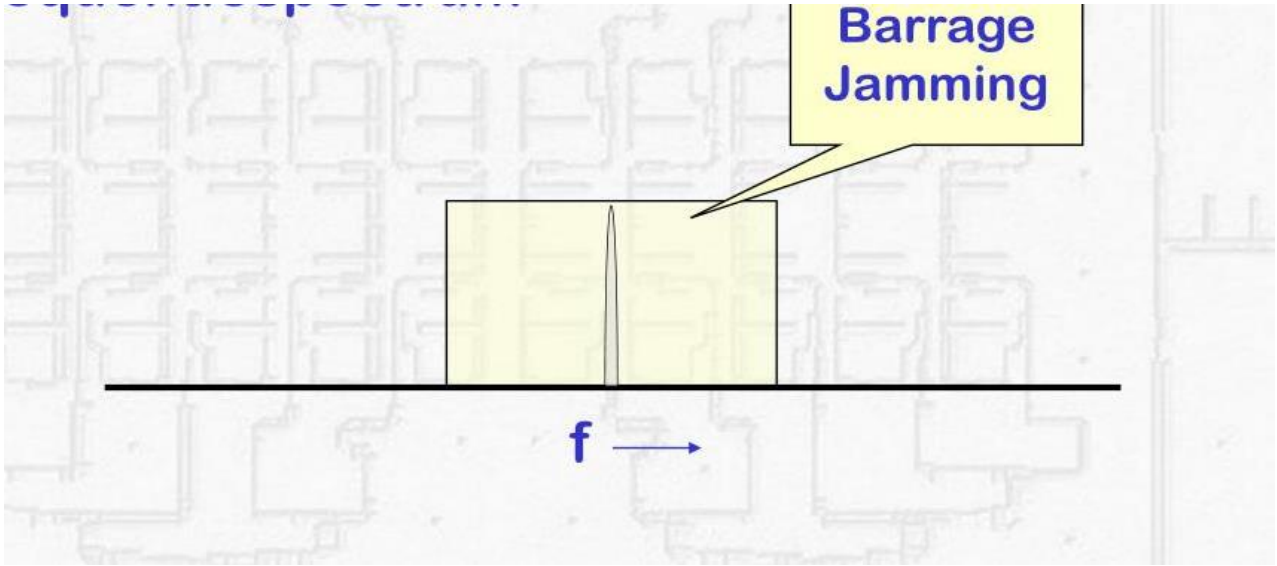
Before we move towards the design of the jammer, we would like to highlight the jamming techniques because design methodology for each of the jamming techniques is entirely different.

3.1.1 Jamming Techniques

Noise and repetition approaches are the two primary jamming methods. The three most frequent forms of noise jamming are spot jamming, sweep jamming, and barrage jamming; the most frequent kind of repeater jamming is Digital Frequency Radio Memory (DRFM) jamming.

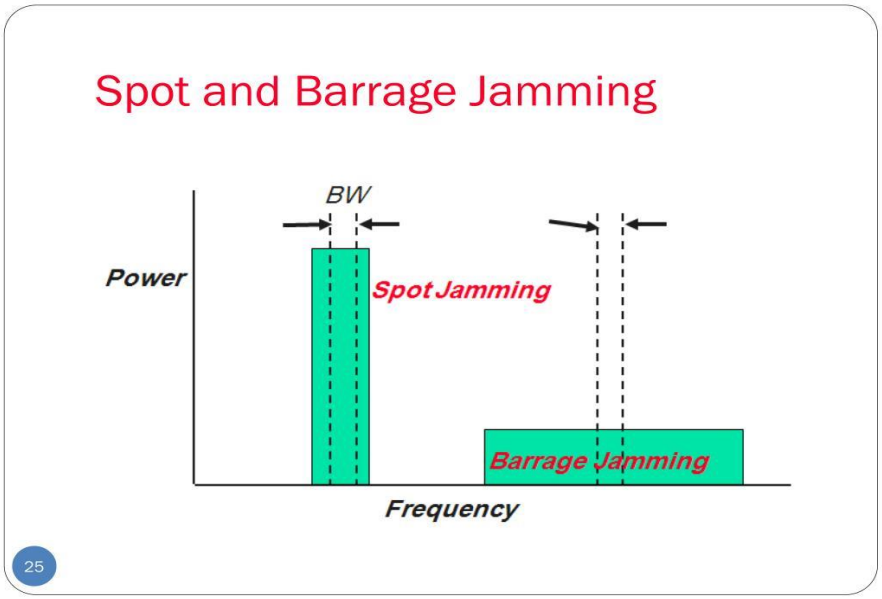
3.1.1.1 Barrage Jamming

Barrage jamming is the simultaneous jamming of several frequencies by one jammer. This method's fundamental flaw is that the jammer disperses its strength over a number of frequencies, making it relatively less potent at a single frequency.



3.1.1.2 Spot Jamming

Spot jamming is a type of noise jamming in which a jammer concentrates all of its strength on a single frequency, making the tactic useless against a radar that can change its frequency as needed.



3.1.1.3 Sweep Jamming

The act of switching a jammer's full power from one frequency to another is known as sweep jamming. Multiple frequencies are jammed by this "sweeping" motion quickly, though not simultaneously.

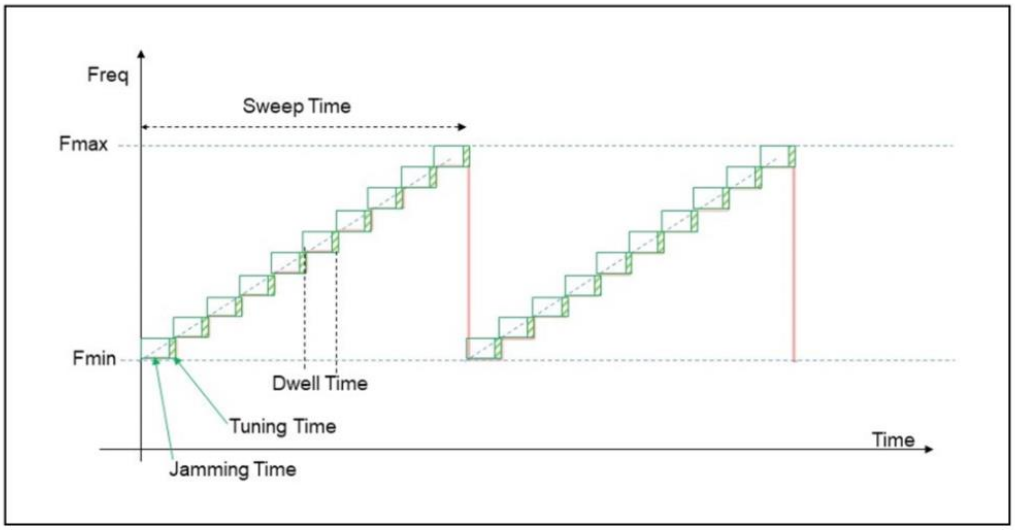


Figure 1: Sweep jamming timing

3.1.1.4 Digital Frequency Radio Memory (DRFM) jamming

A repeater technique known as digital frequency radio memory, or DRFM, confuses a radar by modifying and retransmitting received radar energy. The jammer, for instance, can vary the range that the radar detects and produces false targets by altering the latency in pulse transmission. These kinds of methods are employed by several jamming antennas.

3.1.2 Distance to be Jammed

This factor is crucial to our design because the size of the jammer's output strength depends on the area that needs to be blocked off. We shall later see how the output power and the distance D are related. Our design operates on a distance limit of 45–50 ft (which, under ideal circumstances and in accordance with the requirements of the module being used, might be increased to 70-75 ft).

3.1.3 Frequency Bands

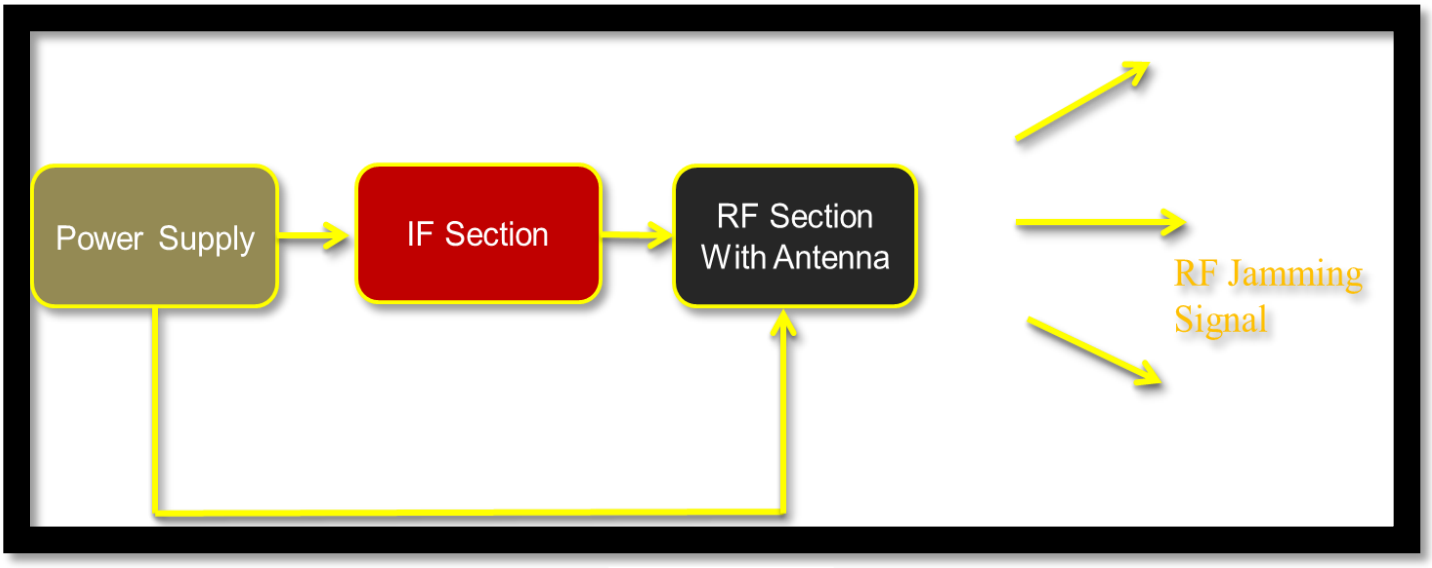
For jamming, only the downlink of all the four bands will be targeted. Bands to be jammed are as following:

FREQ BAND	DOWNLINK FREQ
GSM 900	925-960 MHz
DCS/GSM 1800	1805-1880 MHz
3G	2110-2140 MHz
4G	1840-1860 MHz
CDMA	824-894 MHz

Downlink Freq Used by Different Operators

3.2 Design

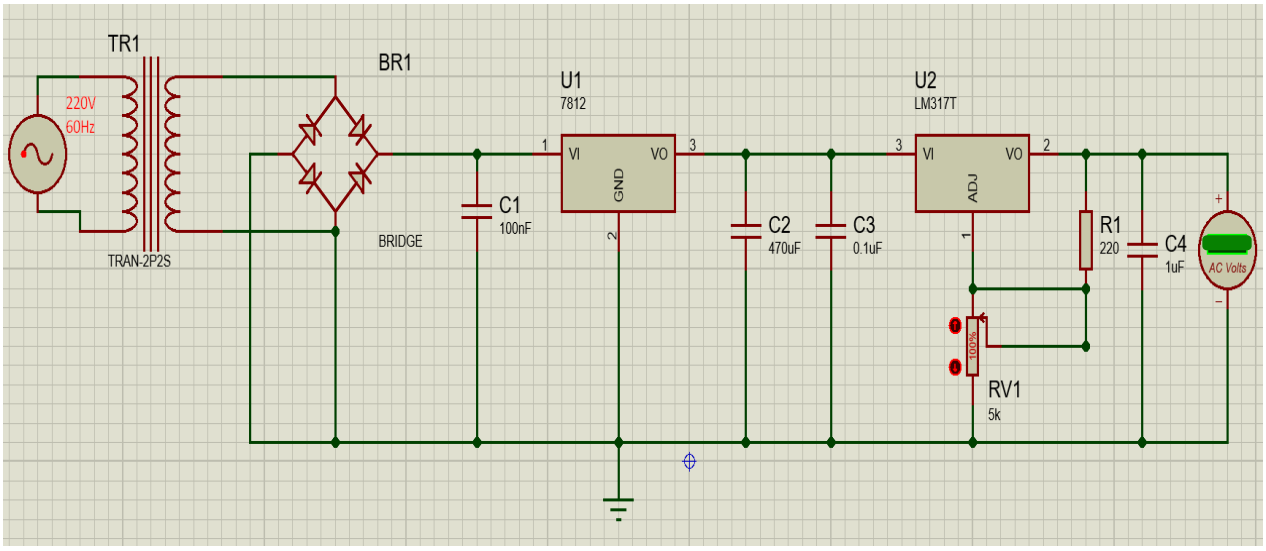
Following approach will be followed;



Block Diagram

3.2.0 Power Supply

In the first stage a power supply is designed to provide the desired input to IF and RF sections.



3.2.1 IF-Section

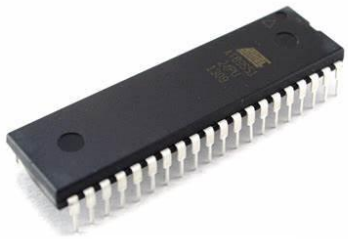
In this stage of the project, creating noise, creating square and triangular waves, combining them with noise, and feeding this sweep signal to the RF-Section are the primary stages. The following is a list of the steps that were taken for this design component.

The noise generator LM 386 and the 555 timer ICs are both activated by the microcontroller 89s51.

1. Two 555 timer ICs are employed as square and triangular wave generators in the IF section.
2. The LM 386 Audio Amplifier IC and NPN transistor are used to create the noise signal.
3. There are two summer ICs used. One involves combining triangular and square waves, and the other combines wave output with noise signal.
4. The output of the ICs is fed to the RF-Section's VCOs.

3.2.1.1 The 89S51 Microcontroller

A CMOS 8-bit microcontroller with low power consumption and high performance, the AT89S51 has 4K bytes of in-system programmable flash memory. The device is made utilizing high-density nonvolatile memory technology from Atmel and is pin-compatible with the 80C51 instruction set, which is widely used in electronics. The on-chip Flash enables, in-system or external nonvolatile memory programmer, reprogramming of the program memory. utilizing a monolithic device with an adaptable 8-bit CPU and in-system programmable flash. Powerful microcontrollers like the



AT89S51

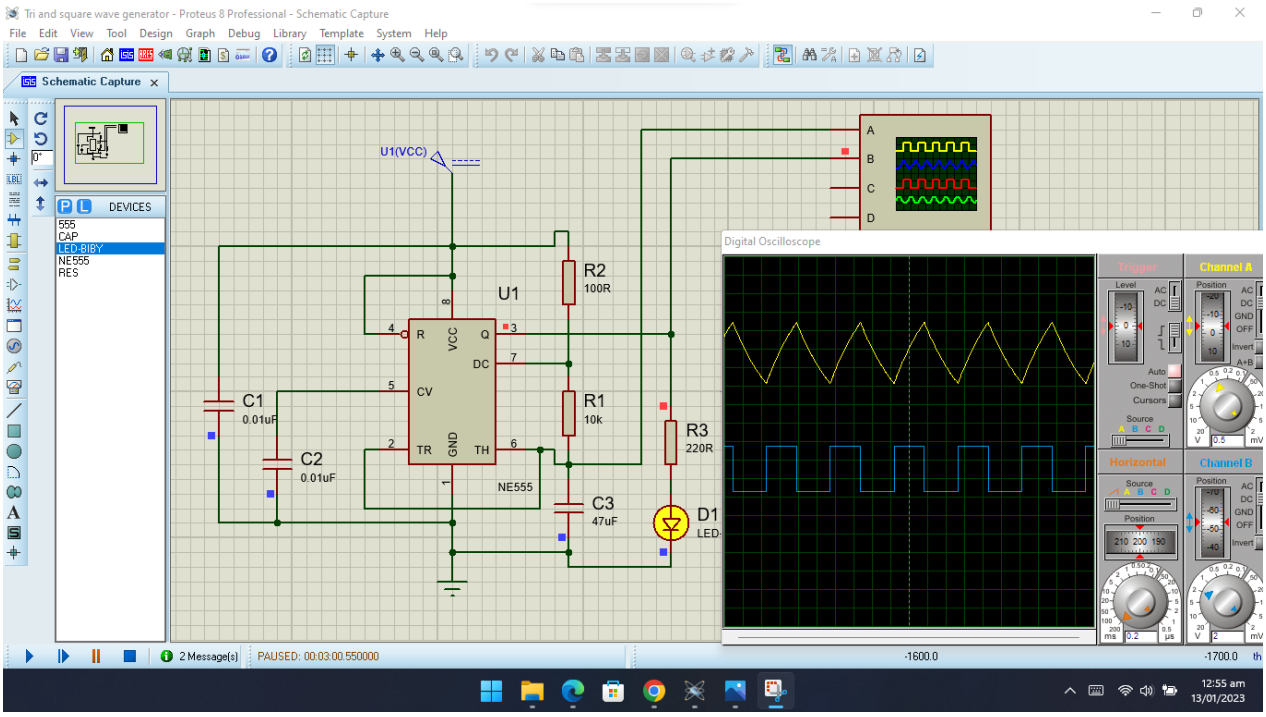
Atmel AT89S51 provide many embedded control applications, a highly adaptable and economical option.

The Microcontroller is being used to trigger the 555 timer ICs and LM 386 to generate their respective signals.

3.2.1.2 Triangular and Square Wave Generators (555 IC)

By employing this IC in the a-stable mode, the 555 timer IC has been used to generate a triangular wave and a square wave in the IF frequency section of the mobile phone jammer. The charging and discharging of the capacitor, the resistance values, and the power source utilized for the IC, together affect the wave's output frequency.

The Proteus circuit and its output is mentioned below:



3.2.1.3 Noise Generator

In order to trigger the pulse that is fed to the LM 386 IC using the correct configuration, we have employed an 89s51 microcontroller for the noise creation stage. Two levels of amplification are applied to the noise signal created. An NPN transistor operating in the common emitter mode is employed in the first stage of amplification. The LM386 audio amplifier IC is utilized at the second stage. The resulting noise signal is sent to the jammer's mixer in the IF section to be combined with the sweep signal we made using the 555 timer ICs. The noise signal swings between 100 Hz and 4.7 kHz.

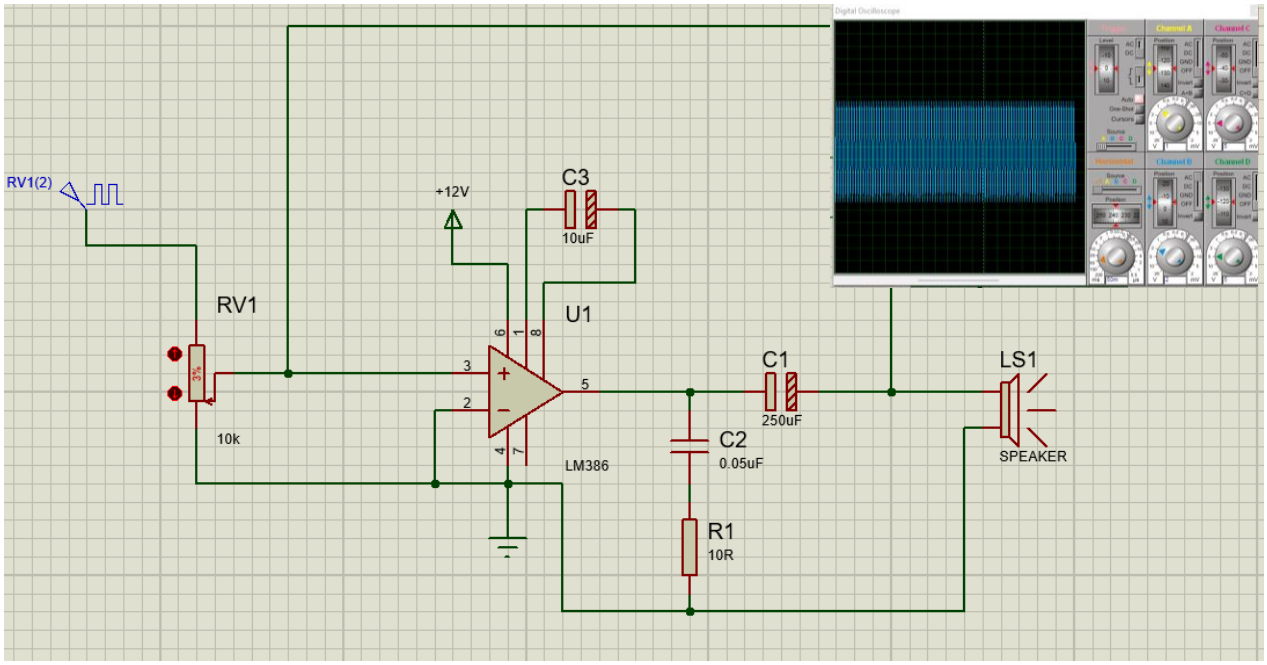
LM-386

NE-555

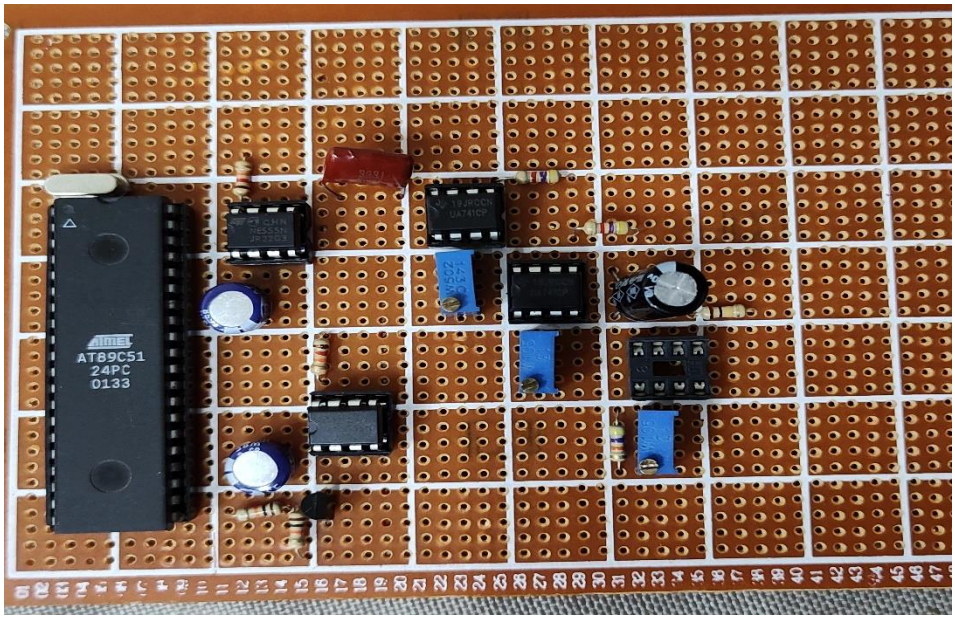
3.2.1.4 Summer IC (LM 324)

The mixer is merely an amplifier that serves as a summer. Here, the produced noise signal, triangular wave, and square wave from the 555 timer IC are combined before being sent to the VCO in the RF section of the mobile phone jammer. The summer IC used here is LM 324. It requires two inputs and one output (we are using non-inverting input pins). This IC adds the noise signal, the sum of the square and triangle waves.

LM-324



Noise Circuit



Hardware implemented IF Section

3.2.2 RF Section

The output of this segment interferes with the mobile, making it the most crucial component of the jammer. Four different VCOs two for GSM, one for 3G, and one for 4G LTE are fed the sweep signal from the IF-Section. The signal is swept through four VCOs' complete frequency bands. The RF-Section for jammer mainly consists of three major parts that are VCO, Power Amplifiers and Antennas. The sections that follow address these components.

3.2.2.1 The Voltage Controlled Oscillator (VCO)

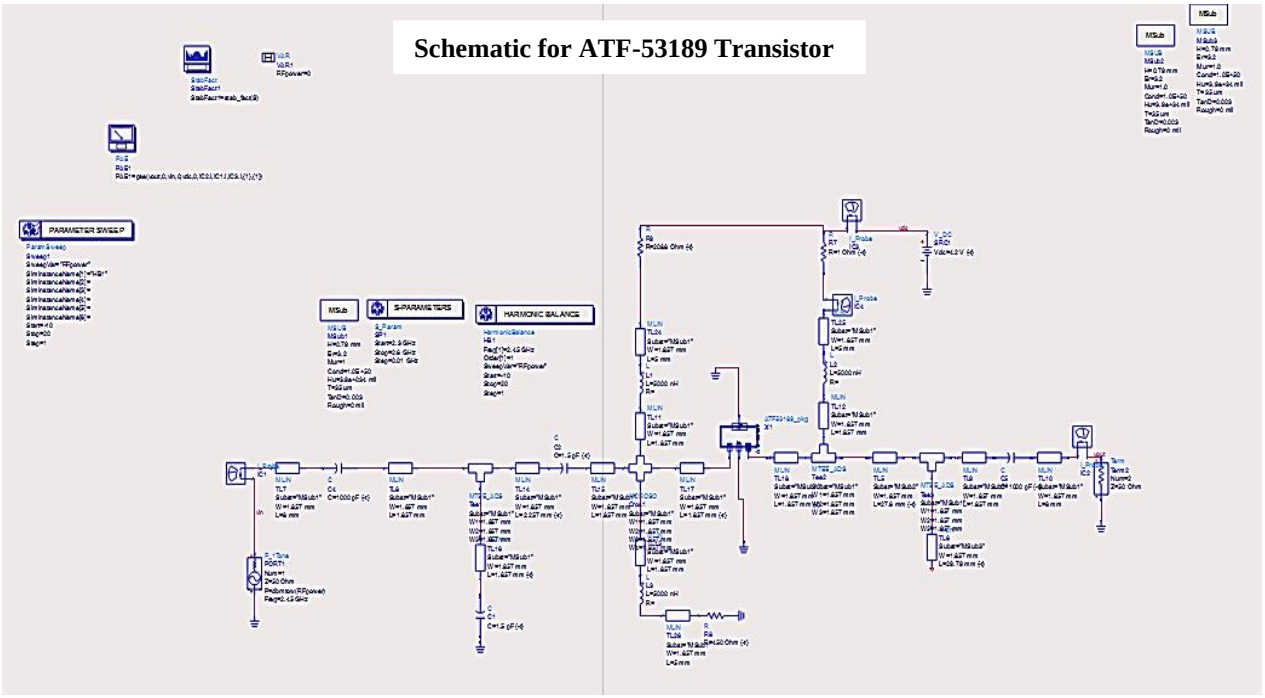
The voltage-controlled oscillator (VCO) serves as the RF-section's brains. The cell phone's ability to communicate will be hampered by the source of the RF signal. The input voltage determines the frequency of the VCO's output, which means that the input voltage can be modified to alter the output frequency. The output has a particular frequency when the input voltage is DC, but the output has a specific frequency range when the input is a triangle waveform. The module features four built-in VCOs: CVCO33CL, CVCO55BE, CVCO55CW, and CVCO55CM, as required by the design for the four different mobile bands. All these VCOs requires sweeping voltage of 0.7V to 4.2V to successfully to generate the desired signal of pertinent frequency.

3.2.2.2 Power Amplifier

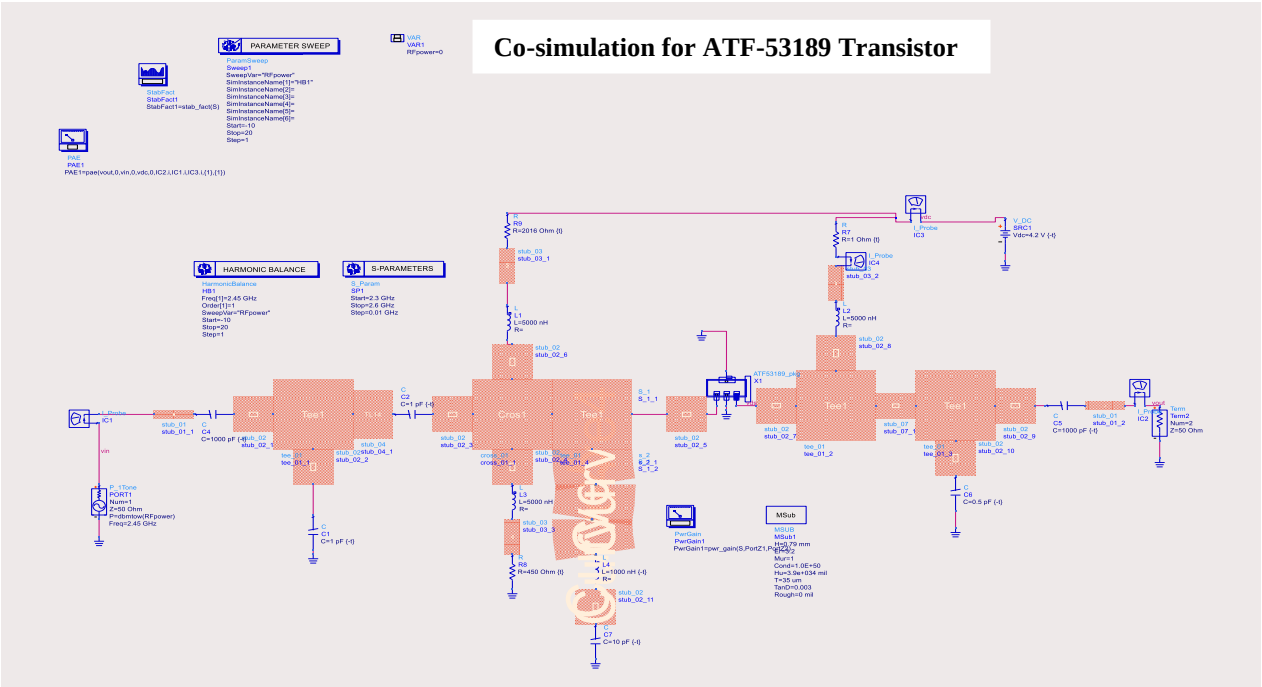
The Mobile jammer needs an amplifier with a suitable gain to boost the VCO output in order to provide the requisite output power. A power amplifier is a sort of electronic amplifier that is used

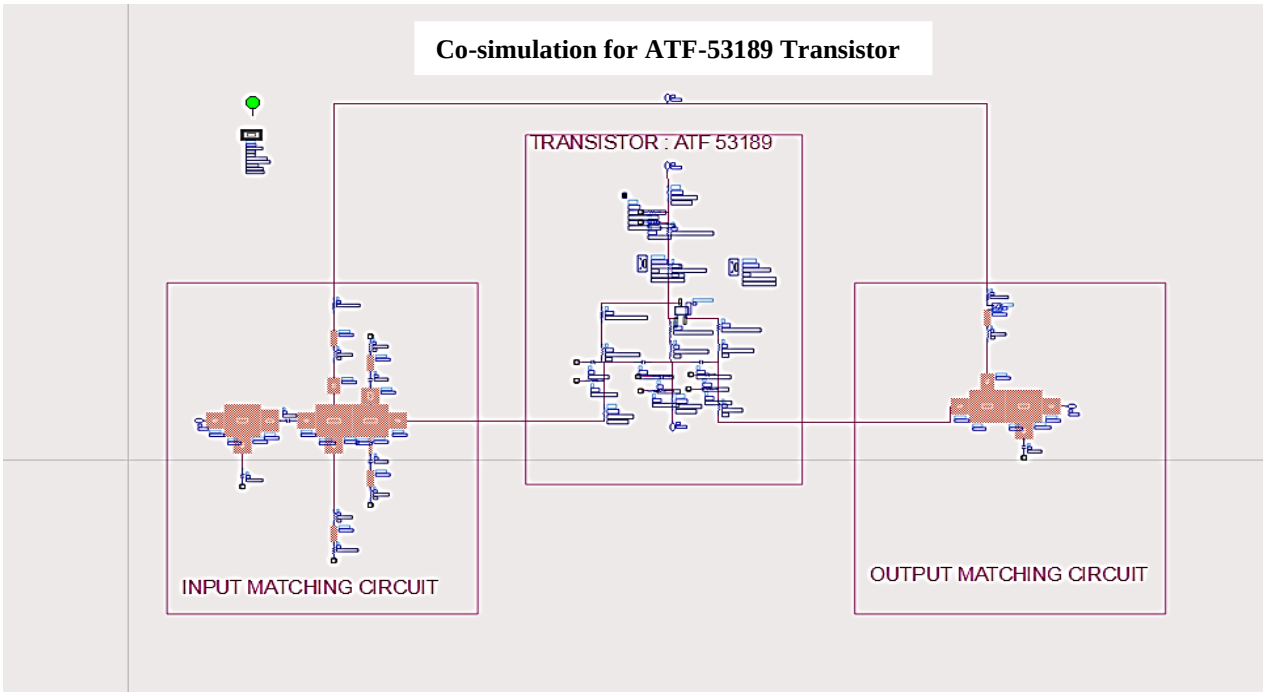
to increase the power of radio frequency signals, often to drive a transmitter's antenna. It is often optimized for high output power compression, high efficiency, minimal return loss at the input and output, strong gain, and efficient heat dissipation. For four different frequencies, four amplifiers have been employed.

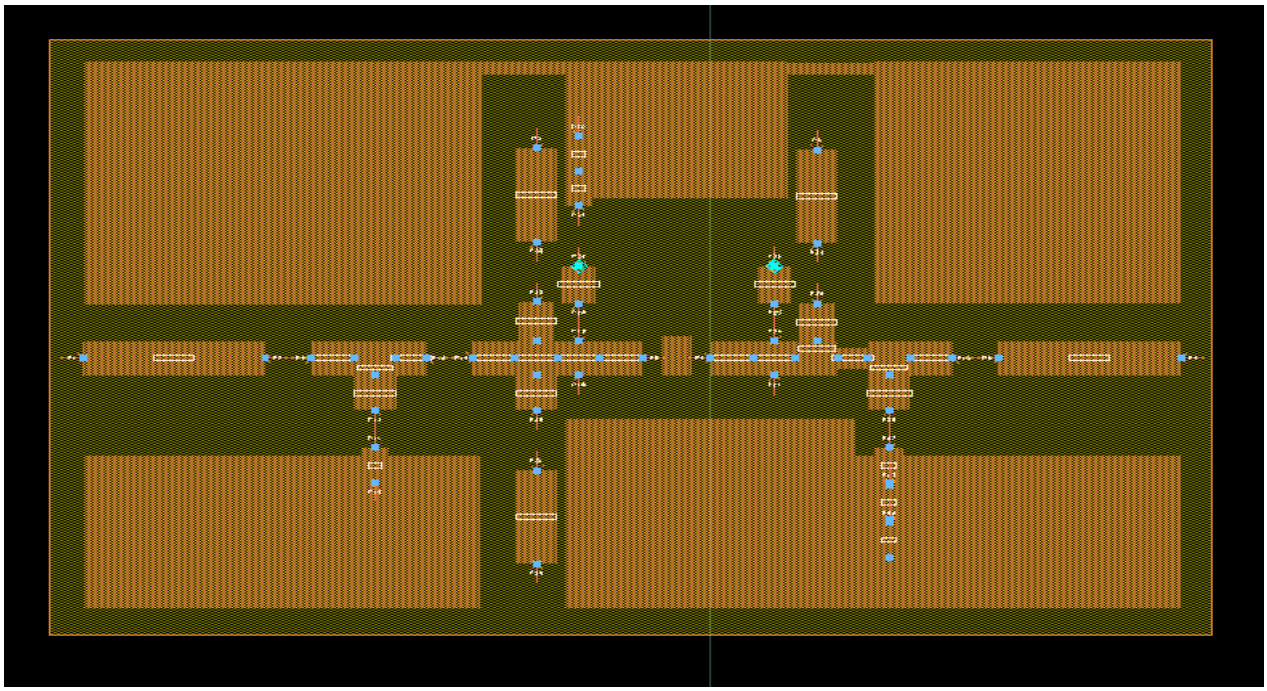
Schematic for ATF-53189 Transistor



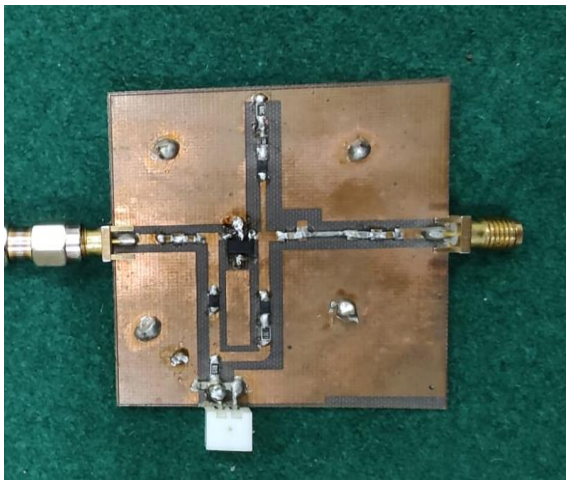
Co-simulation for ATF-53189 Transistor





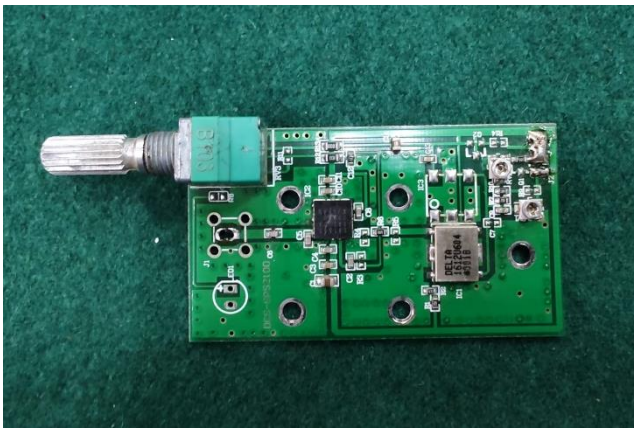


Layout for ATF-53189 Transistor



Prototype Development of Power Amplifier

To achieve better results, the schematics, co-simulation, and layout, shown above were sent to JLCPCB, China for fabrication.



Fabricated Module of RF Section

3.2.2.3 Antennas

An electrical device known as an antenna transforms electrical power into radio waves and the other way around. The jamming signal must be transmitted using the correct antenna. The antenna system and transmission system must be compatible for maximum power transfer. The antennas are matched to the system using four quarter wavelength monopole antennas with 50 input impedance.

Antennas

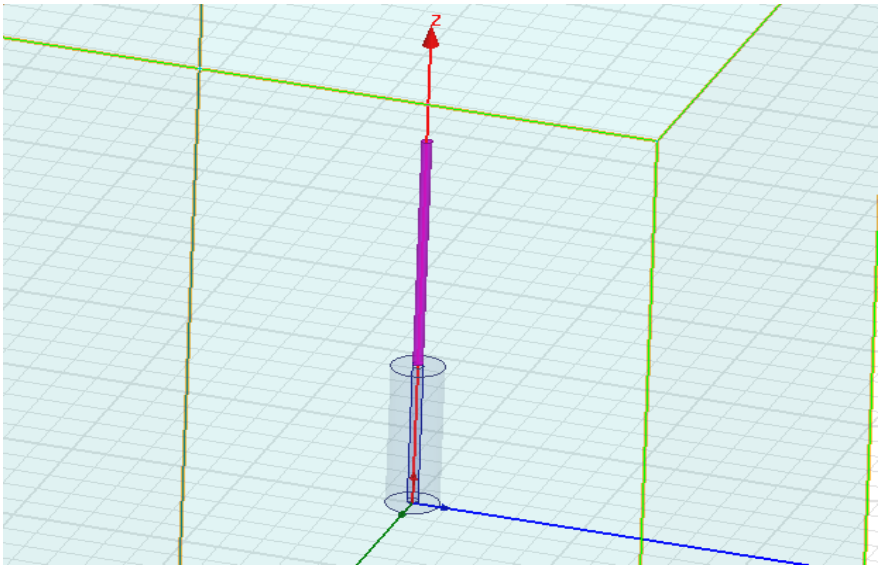
Chapter 4: Analysis and Evaluation

The modules were successfully designed and then developed by China were analyzed using designed IF circuit for noise generation.

Monopole antenna designed at four different frequency ranges were mounted on the modules to evaluate and analyze the functionality of the jammer.

Jammer with Monopole Antennas

4.1 RF Section

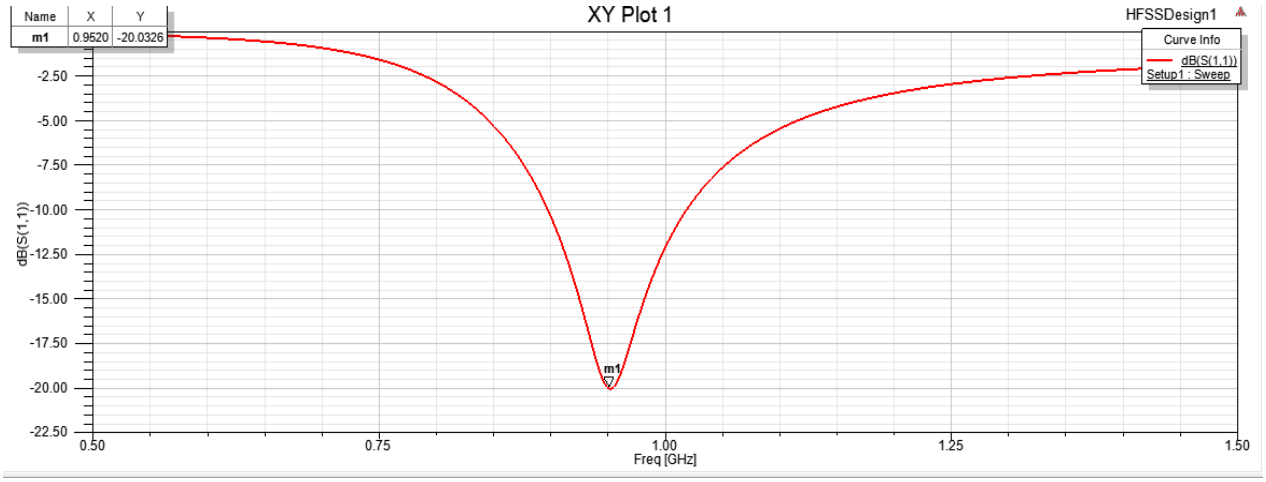


Antenna Design in Proteus

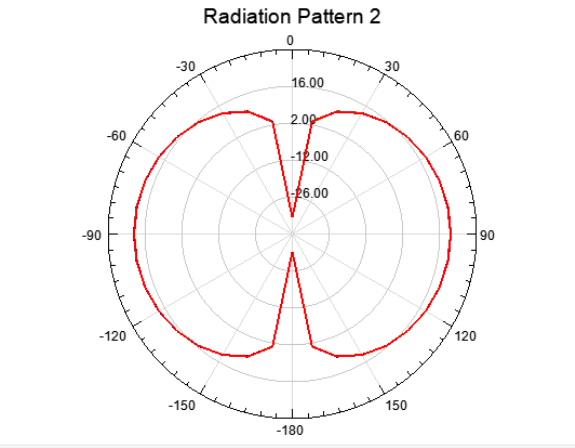
4.2.1 GSM Antenna

GSM antenna is designed to cater for the downlink frequency of the GSM Band i.e., 915-970 MHz.

The antenna is designed in a way that it covers this complete frequency range.



S11 Return Loss of GSM Antenna

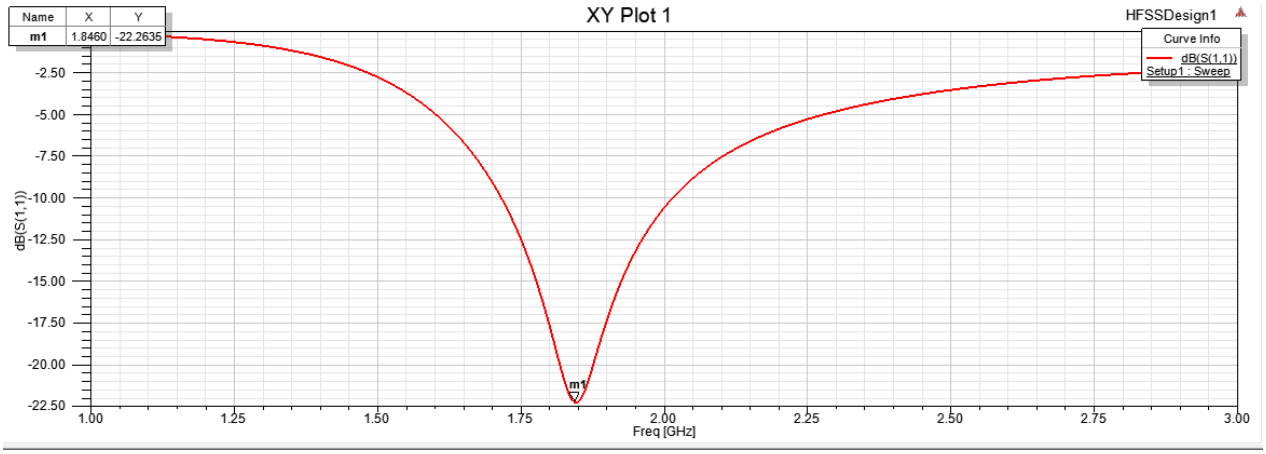


Radiation Pattern of GSM Antenna

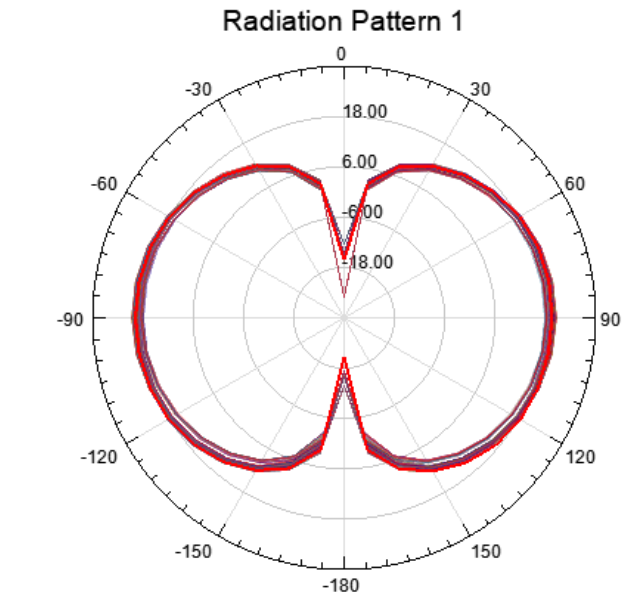
Gain of GSM Antenna

4.2.2 DCS Antenna

The antenna is designed to counter for DCS/GSM 1800 band i.e., 1796-1896 MHz.



S11 Return Loss of DCS Antenna

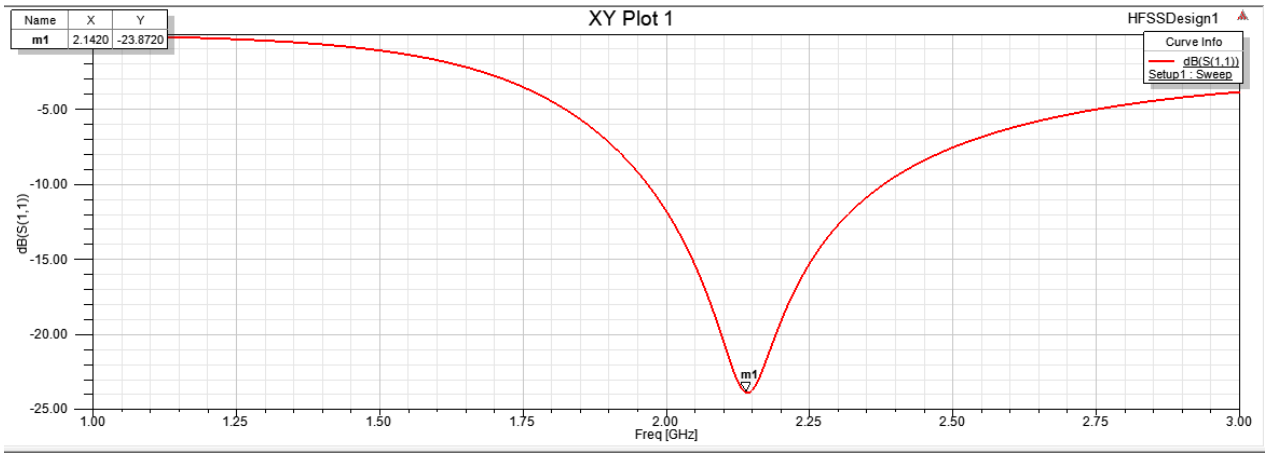


Radiation Pattern of DCS Antenna

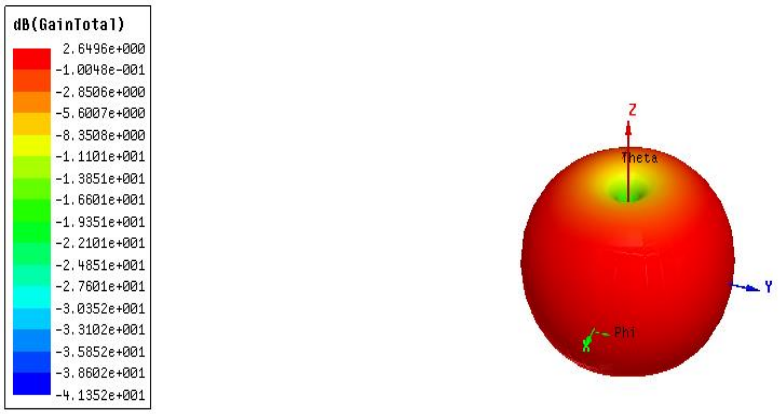
Gain of DCS Antenna

4.2.3 3G Antenna

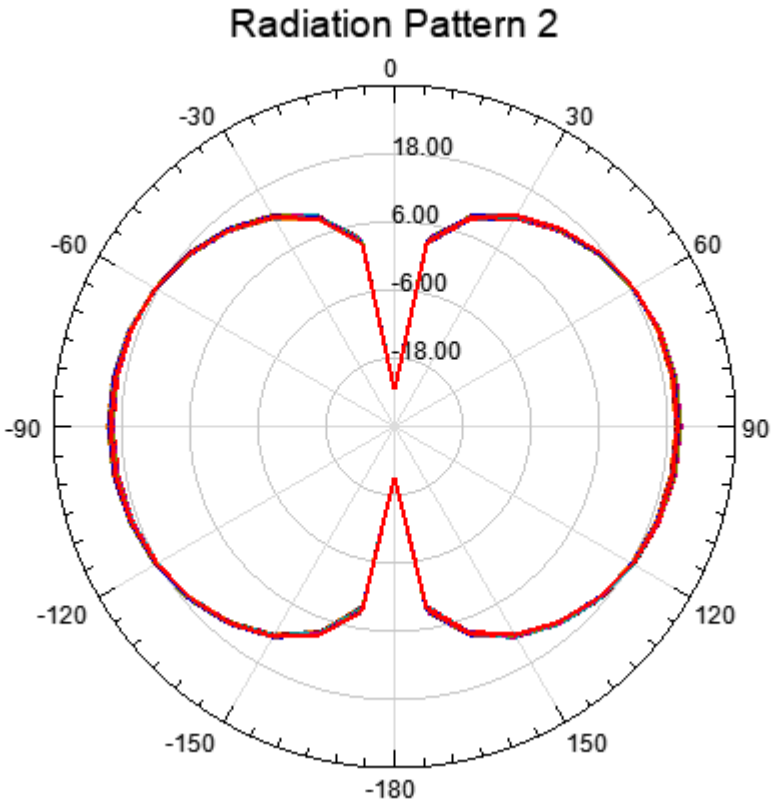
Frequency range of 2094-2184 MHz is covered by this antenna.



S11 Return Loss of 3G Antenna



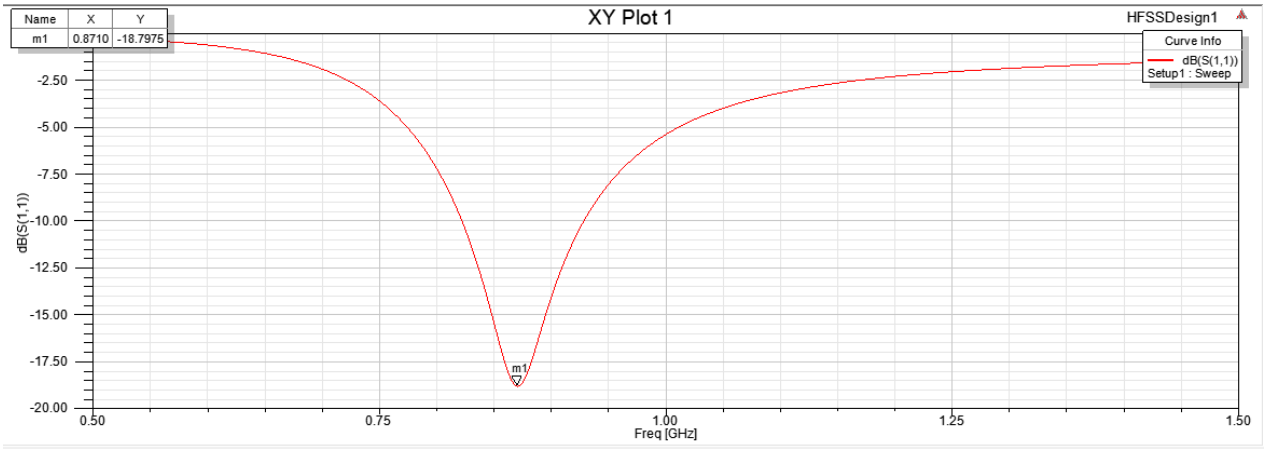
Gain of 3G Antenna



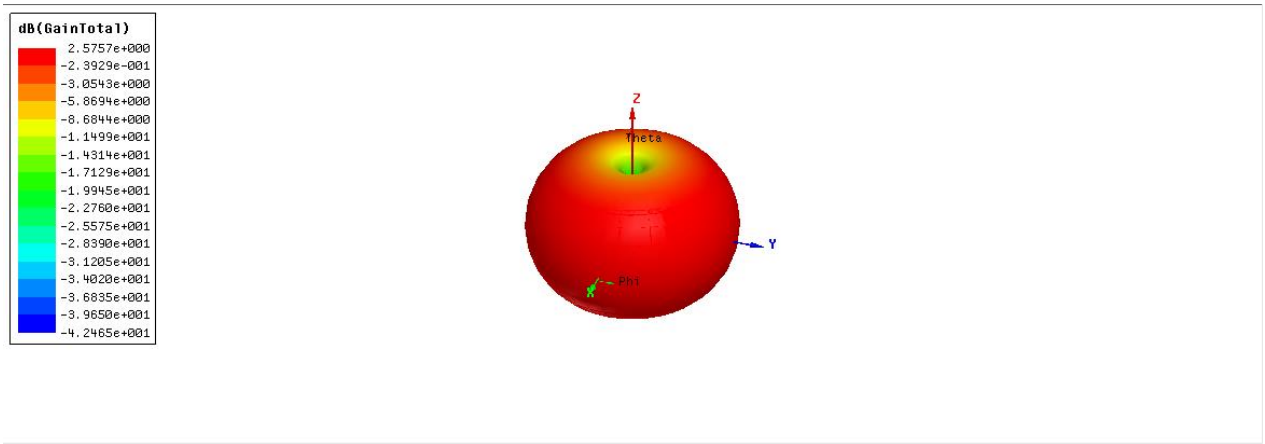
Radiation Pattern of 3G Antenna

4.2.4 CDMA Antenna

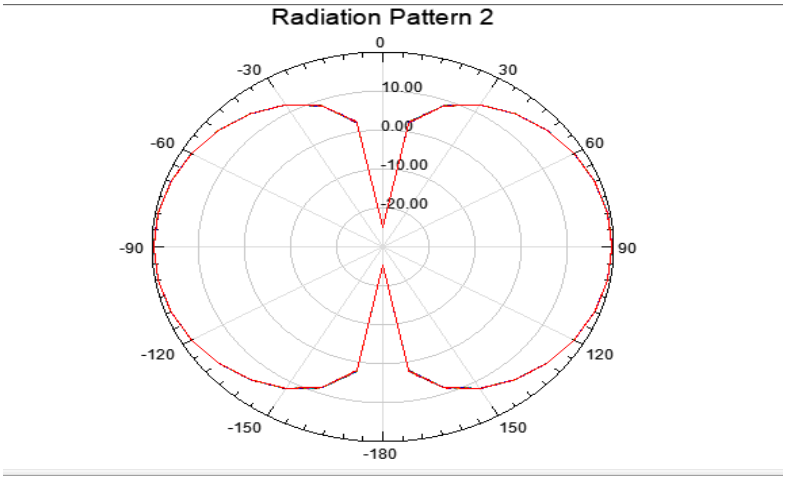
This antenna covers a frequency range from 841-902 MHz.



S11 Return Loss of CDMA Antenna



Gain of CDMA Antenna



Radiation Pattern of CDMA Antenna

4.3 Performance of System Developed

The system developed is found to be very successful at all the frequencies (GSM, DCS, 3G, CDMA, 4G) within the range of 50 ft. In the testing area all mobile service networks i.e., Zong, Telenor, Ufone and Mobilink were jammed within the jamming radius.

Chapter 5: Conclusion

5.1 Overview

1. A compact and portable mobile phone jammer operating at frequencies (GSM, DCS, 3G, CDMA) has been successfully developed.
2. The range of the jammer was found to be 50 ft which can be enhanced to 70+ ft using two stage amplifier.
3. Jammer is equally successful for all above mentioned frequencies and carriers used in Pakistan.

5.2 Limitations

Since restrictions are an essential component of every new technology being used globally, this project likewise contains some restrictions. These restrictions could be listed as follows.

Sr no.	Limitations	
1	Law	Due of their usage in terrorist actions, RF components are tightly prohibited by the government.
2	Law	Since the operators are using a frequency that was legally granted to them by PTA & FAB, the gadget is illegal in Pakistan
3	Distance	When there is more electromagnetic interference from nearby electrical devices, the jamming distance decreases

Chapter 6: Future Work

- The range is found to be limited to 50 ft because of single stage amplifier. The range can be enhanced using a two-stage amplifier.
- More frequency bands like Wi-Fi, VHF, UHF etc. can be included in future work.
- As research and development of 5G Network is in progress so there will soon be a need to overcome the network using MIMO antennas.
- The size can further be reduced, and light weight material can be used.

APPENDICES

Appendix A

Microcontroller Code

```
APPENDIX A
MICROCONTROLLER CODE
#include <AT89X51.H>
#include <string.h>
#define out P1_0
unsigned char p_width;
bit p_flag = 0;
void p_setup(){
 TMOD = 0;
 p_width = 160;
 EA = 1;
 ET0 = 1;
 TR0 = 1;
}
void timer0() interrupt 1 {
 if(!p_flag) {
 p_flag = 1;
 out = 1;
 TH0 = p_width;
 TF0 = 0;
 return;
 }
 else {
 p_flag = 0;
 out = 0;
 TH0 = 255 - p_width;
 TF0 = 0;
55
 return;
 }
}
void main(void)
{
TMOD = 0x22;
TH0 = -3;
TR0 = 1;
EA = 1;
while(1)
{
p_setup();
}
}
```

Appendix B-Data Sheets

LM555 Timer

Check for Samples: LM555

FEATURES

- Direct Replacement for SE555/NE555
- Timing from Microseconds through Hours
- Operates in Both Astable and Monostable Modes
- Adjustable Duty Cycle
- Output Can Source or Sink 200 mA
- Output and Supply TTL Compatible
- Temperature Stability Better than 0.005% per °C
- Normally On and Normally Off Output
- Available in 8-pin VSSOP Package

APPLICATIONS

- Precision Timing
- Pulse Generation
- Sequential Timing
- Time Delay Generation
- Pulse Width Modulation
- Pulse Position Modulation
- Linear Ramp Generator

Schematic Diagram

DESCRIPTION

The LM555 is a highly stable device for generating accurate time delays or oscillation. Additional terminals are provided for triggering or resetting if desired. In the time delay mode of operation, the time is precisely controlled by one external resistor and capacitor. For astable operation as an oscillator, the free running frequency and duty cycle are accurately controlled with two external resistors and one capacitor. The circuit may be triggered and reset on falling waveforms, and the output circuit can source or sink up to 200mA or drive TTL circuits.

LM386
Low Voltage Audio Power Amplifier

General Description

The LM386 is a power amplifier designed for use in low volt-age consumer applications. The gain is internally set to 20 to keep external part count low, but the addition of an external resistor and capacitor between pins 1 and 8 will increase the gain to any value from 20 to 200.

The inputs are ground referenced while the output automatically biases to one-half the supply voltage. The quiescent power drain is only 24 milliwatts when operating from a 6 volt supply, making the LM386 ideal for battery operation.

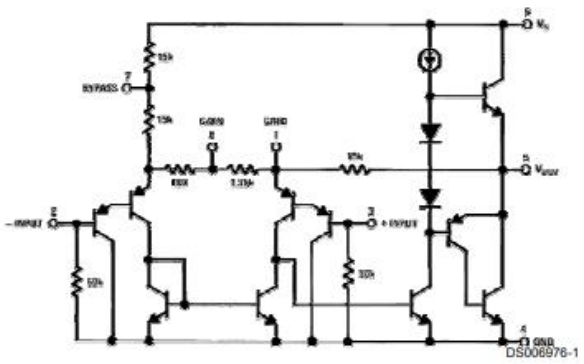
Features

- Battery operation
- Minimum external parts
- Wide supply voltage range: 4V±12V or 5V±18V
- Low quiescent current drain: 4mA
- Voltage gains from 20 to 200
- Ground referenced input
- Self-centering output quiescent voltage
- Low distortion: 0.2% (A_V = 20, V_S = 6V, R_L = 8Ω, P_O = 125mW, f = 1kHz)
- Available in 8 pin MSOP package

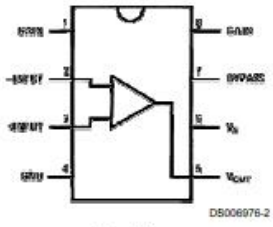
Applications

n AM-FM radio amplifiers
n Portable tape player amplifiers
n Intercoms
n TV sound systems
n Line drivers
n Ultrasonic drivers n
Small servo drivers n
Power converters

Equivalent Schematic and Connection Diagrams



Small Outline, Molded Mini Small Outline, and Dual-In-Line Packages



Top View
Order Number LM386M-1, LM386MM-1, LM386N-1, LM386N-3 or LM386N-4
See NS Package Number M08A, MUA08A or N08E

LM124/LM224/LM324/LM2902
Low Power Quad Operational Amplifiers

General Description

The LM124 series consists of four independent, high gain, internally frequency compensated operational amplifiers which were designed specifically to operate from a single power supply over a wide range of voltages. Operation from split power supplies is also possible and the low power supply current drain is independent of the magnitude of the power supply voltage.

Application areas include transducer amplifiers, DC gain blocks and all the conventional op amp circuits which now can be more easily implemented in single power supply systems. For example, the LM124 series can be directly operated off of the standard +5V power supply voltage which is used in digital systems and will easily provide the required interface electronics without requiring the additional ±15V power supplies.

Unique Characteristics

- In the linear mode the input common-mode voltage range includes ground and the output voltage can also swing to ground, even though operated from only a single power supply voltage
- The unity gain cross frequency is temperature compensated
- The input bias current is also temperature compensated

Advantages

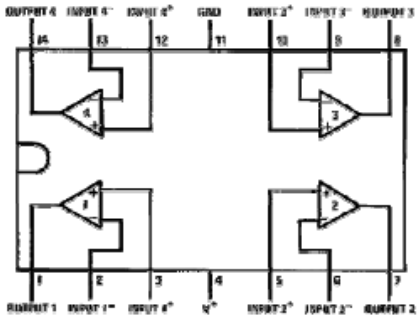
- n Eliminates need for dual supplies
- n Four internally compensated op amps in a single package
- n Allows directly sensing near GND and V_{OUT} also goes to GND
- n Compatible with all forms of logic
- n Power drain suitable for battery operation

Features

- n Internally frequency compensated for unity gain
- n Large DC voltage gain 100 dB
- n Wide bandwidth (unity gain) 1 MHz (temperature compensated)
- n Wide power supply range:
  Single supply 3V to 32V
  or dual supplies ±1.5V to ±16V
- n Very low supply current drain (700 µA) — essentially independent of supply voltage
- n Low input biasing current 45 nA (temperature compensated)
- n Low input offset voltage 2 mV and offset current: 5 nA
- n Input common-mode voltage range includes ground
- n Differential input voltage range equal to the power supply voltage
- n Large output voltage swing 0V to V^+ − 1.5V

Connection Diagrams

Dual-In-Line Package



APPENDIX-C: BIBLIOGRAPHY

REFERENCES

[1]. Mobile Communication by Dr. Mir Yasir

[2]. Miriam Joseph, "GSM jamming device", Arusha technical college., Dept of EE., Undergraduate project report, Tanzania 2008.

[3]. U. E Okoye and Charles, N. V, "ON THE PHYSICS OF GSM JAMMER AND ITS APPLICATION IN LECTURE THEATERS," Science Journal Publication., doi: 10.7237/sjp/144, January 2013.

[4]. Mohd zaidi bin husin, "GSM-900 MOBILE JAMMER," UNIVERSTI TEKNIKAL MALAYSIA MELAKA., Dept of EE., Undergraduate project report, Malaysia 2010.

[5]. Ahlin, L. (2012). Principles of Wireless Communications, (4th Ed.). Spain: McGraw-Hill Education.

[6]. Isaac Hanson, "design and construct a dual band mobile jammer for GSM 900&1800", Ghana telecom university college (GTUC)., Dept of EE., undergraduate project report, Ghana 2009.

[7]. Ahlin, L. (2012). Principles of Wireless Communications, (4th Ed.). Spain: McGraw-Hill Education.

[8]. Nigerian Communication Commission. [Internet] © (2005-2013). Retrieved on 2013-06-02. From: http://www.ncc.org.ng/

[9]. Jammers for Mobile Cellular Systems applied to unauthorized UAVs [Internet]. By Karla Valentina de Freitas Lara

[10]. Mobile phone signal jammer with prescheduled time duration [Internet] by S. Hema Latha