# GHANA TELECOM UNIVERSITY COLLEGE (GTUC)

## FACULTY OF ENGINEERING

## DEPARTMENT OF TELECOMMUNICATION ENGINEERING

TITLE:

# DESIGN AND CONSTRUCT A DUAL BAND MOBILE JAMMER FOR GSM 900 & GSM 1800

A Project Work Submitted in Partial Fulfillment of the Requirements for

BSc. in Telecommunication Engineering

**BY:**

AFFO ALEX (B010908017)

EFFAH ONASIS (B010908073)

IBRAHIM I. FAREED (B010908092)

**SUPERVISOR:**

ING. ISAAC HANSON

**JUNE 2012**

## Declaration

This Project is presented as part of the requirements for BSc. in Telecommunication Engineering awarded by Ghana Telecom University College. I hereby declare that this project is entirely the result of hard work, research and enquiries. I am confident that this project work is not copied from any other person. All sources of information have been acknowledged with due respect.

AUTHOR: AFFO ALEX SIGNATURE…………………….

STUDENT ID: B010908017 DATE: ……………………………

AUTHOR: EFFAH ONASIS SIGNATURE…………………….

STUDENT ID: B010908073 DATE: …………………………....

AUTHOR: IBRAHIM I. FAREED SIGNATURE…………………….

STUDENT ID: B010908092 DATE: ……………………………

SUPERVISOR: ING ISAAC HANSON SIGNATURE……………………..

DATE: ……………………………

HOD: ING ISAAC HANSON SIGNATURE……………………..

DATE: …………………………….

## Abstract

Mobile jammer is an electronic device used to prevent mobile phones from receiving or transmitting signals with the base stations. Mobile jammers effectively disable mobile phones within the defined regulated zones without causing any interference to other communication means. Mobile jammers can be used in practically any location, but are used in places where a phone call would be particularly disruptive like Temples, Libraries, Hospitals, Cinema halls, schools & colleges etc. As with other radio jamming, mobile jammers block mobile phone use by sending out radio waves along the same frequencies that mobile phones use. This causes enough interference with the communication between mobile phones and communicating towers to render the phones unusable. Upon activating mobile jammers, all mobile phones will indicate "NO NETWORK". Incoming calls are blocked as if the mobile phone were off. When the mobile jammers are turned off, all mobile phones will automatically re-establish communications and provide full service. Mobile Jammers were originally developed for law enforcement and the military to interrupt communications by criminals and terrorists to foil the use of certain remotely detonated explosives. The civilian applications were apparent with growing public resentment over usage of mobile phones in public areas on the rise & reckless invasion of privacy. Over time many companies originally contracted to design mobile jammers for government switched over to sell these devices to private entities. This project aims at designing and constructing a GSM mobile jammer to address the problems caused by the mobile phones.

## Table of Contents

## List of Tables

**Lists of Figures**

## List of Abbreviations

| | |
|---|---|
| **2G** | 2nd Generation |
| **3G** | 3rd Generation |
| **4G** | 4th Generation |
| **A** | Ampere |
| **AMPS** | Advanced Mobile Phone Service |
| **AC** | Alternating Current |
| **AF** | Audio Amplifier |
| **B-channel** | Bearer Channel |
| **BS** | Base Station |
| **BTS** | Base Transceiver Station |
| **CDMA** | Code Division Multiple Access |
| **dB** | Decibels |
| **DoS** | Denial of Service |
| **DCS** | Digital Cellular System |
| **DC** | Direct Current |
| **EDGE** | Enhanced Data Rates for Global Evolution |
| **EMI** | Electromagnetic Interference |
| **ETSI** | European Telecommunication Standards Institute |
| **FDD** | Frequency Division Duplexing |
| **FDMA** | Frequency Division Multiple Access |
| **GHz** | Gigahertz |

| | |
|---|---|
| **GPRS** | General Packet Radio Service |
| **GSM** | Global system for mobile communications |
| HSPA | High Speed Packet Access |
| **IMSI** | International Mobile Subscriber Identity |
| **ITU** | International Telecommunications Union |
| **ISDN** | Integrated Services Digital Network |
| **ITU-T** | ITU Telecommunication Standardization Sector |
| **KHz** | Kilohertz |
| **LTE** | Long Term Evolution |
| **ME** | Mobile Equipment |
| **MHz** | Megahertz |
| **ms** | Millisecond |
| **MS** | Mobile Station |
| **MSC** | Mobile Switching Center |
| **NMT** | Nordic Mobile Telephone |
| **Op-amp** | Operational Amplifier |
| **PDA** | Personal Digital Assistant |
| **PDC** | Pacific Digital Cellular |
| **PSTN** | Public Switched Telephone Network |
| **RF** | Radio Frequency |
| **SIM** | Subscriber Identity Module |
| **SMS** | Short Message Service |

| | |
|---|---|
| **SNR** | Signal-to-noise ratio |
| **TACS** | Total Access Communication System |
| **TDMA** | Time Division Multiplexing Access |
| **TD-SCDMA** | Time Division Synchronous CDMA |
| **TRX** | Transmitter |
| **UMB** | Ultra-Mobile Broadband |
| **VCO** | Voltage Controlled Oscillator |
| **V** | Volts |
| **VSWR** | Voltage standing wave ratio |
| **W** | Watts |
| **WCDMA** | Wideband Code Division Multiple Access |

## Lists of Symbols and SI Units

| | |
|---|---|
| **A:** | Ampere |
| **dB:** | Decibel |
| **F:** | Farad |
| **G:** | Giga |
| **Hz**: | Hertz |
| **K:** | Kilo |
| **M:** | Mega |
| **V:** | Volts |
| **W:** | Watts |
| **µ:** | Micro |
| **Ω:** | Ohms |
| ***:** | Multiplication |

## Acknowledgement

We would like to express our profound gratitude first and foremost to the Almighty for keeping us alive and healthy during the duration of working on this project. Our thanks also go to our able supervisor ING Isaac Hanson for the guidance and advice he gave us in the completion of this project. Finally we would like to thank all those who in various ways contributed to the completion of the project.

# Chapter 1: - Introduction

## 1.1 Background to Study

The telecommunication industry over the past decades has witnessed an exponential growth in telephony especially mobile telephony; estimates by International telecommunications union (ITU) indicate that over 5.3billion people across the world had mobile subscriptions as at 2010.[1] The dramatic rise in the use of wireless communication devices such as mobile phones, personal digital assistant (PDA), and many others can be attributed to their portability, and thus have become indispensable in our lives.

The convenience and portability of mobile phones has made it possible to be carried everywhere, e.g. Mosque, Churches, libraries, conference halls and examination halls etc. The numerous advantages of mobile phones cannot be over emphasized; however their convenience can create inconvenience in some public places where a considerable amount of silence is needed, also in certain locations the use of mobile phones is prohibited for security and safety reasons and as well as examination centers where phones can aid in cheating. The inconvenience is mostly due to the incessant noise generated from the ringing tones of users; also certain jurisdictions do not permit the exchange of information using mobile phones, as long as users are within that jurisdiction. A way of preventing users from getting access to their phone’s network service is to install a device known as a mobile phone jammer.

Jamming is the radiation of electromagnetic energy in a communication channel which reduces the effective use of the electromagnetic spectrum for legitimate communications.[2]. A GSM mobile jammer is a device which transmits (radiates) noise induced signals at the same frequency range as a mobile phone, thus rendering mobile phones in the specific location unusable.

Global system for mobile communications (GSM) is a second generation cellular standard developed to offer voice, data and video services. The frequency band for GSM range from 380MHz to 1900 MHz, with most mobile operators using the 900MHz to 1800MHz. [3]

Jammer devices were first developed and used by the military with the main objective of denying the successful transfer of information by enemy forces. In recent times with the proliferation of mobile phones, mobile phone jamming devices are becoming products of civilian rather than military devices. The technology behind the mobile jammer is that, the jamming device broadcasts a Radio Frequency (RF) signal in the frequency range reserved for cell phones; these signals interfere with the cell phone signal, which results in a "no network available" displayed on the cell phone screen. All phones within the effective radius of the jammer are therefore silenced. This means that all phones within the effective radius of the jammer will lose the tendency to make or receive calls, as long as they are within that radius.

*Figure 1.0 Warning sign typically used in places where mobile phones are not allowed*

### 1.2 Problem Statement(s)

In spite of the numerous advantages and usefulness of mobile phones, their rapid proliferation has made mobile phones ubiquitous and a nuisances as well as problematic in our daily activities. Various problems mobile phone usage has caused in our daily lives are stated below;

I. In places where some considerable amount of silence is required such as meetings, libraries, lecture halls, worship centers, court rooms etc. The intermittent ringing of people’s phones can disrupt the silence needed in these places. Appealing to the conscience of users to turn off their phones is not enough and a complete denial of service (DoS) is very necessary such that people within the location where their use is prohibited cannot have access.

II. During examinations students could use their mobile phones to either exchange information through SMS or look up information from the internet.

III. Certain institutions that value security and safety such as military, banks, prisons laboratories fuel pumps etc. prohibit people from using their phones within their premises, as these phones could aid in criminal activities such as spying.

These and many other problems have caused a growing public backlash against the intrusive disruption of mobile phones introduced in our lives.

However these problems cannot prevent the ban or handling of phones in these public places. Our project therefore seeks to tackle the problems that arise from the use of mobile phones daily.

### 1.3 Objectives

The objectives of our project are;

I. To design a dual band GSM jammer

II. To simulate and test our designs

III. To construct a dual band GSM jammer

### 1.4 Significance

The significance of our project is to:

I. Reduce the incidence of noise generated from cell phones when ringing at places where a level of silence is required.

II. Prevent students from using their phones to facilitate cheating, during examinations.

III. Prevent people from spying with the aid of mobile phones, as well as reduce the hazards mobile phones can create at signal sensitive installations such as fuel pumps.

### 1.5 Methodology

In our quest to successfully design and construct a mobile jammer various processes were taken into consideration. These considerations are stated below.

**Study Various Projects**.

In order to achieve our aim the first stage of our project was to study various projects done in relation to our project. Studying the different jammer projects enabled us to make some decisions on the; type of jammer to implement, frequency range and coverage distance.

**Design Parameters**

Having studied related works, our jammer was designed based on certain parameters which include;

- Frequencies involved
- Power Requirements
- Effective jamming distance

**Design and Simulations**

With our designs completed the next stage was to have schematic drawings of the various parts of the jammer circuitry. After our schematic drawings are done simulations are carried out based on the schematic to ensure that the designs are working and meet our requirements. The simulations are a very important stage in arriving at our goal. We used the Multisim software version 11 for all our computer simulations.

**Construction of the Mobile Jammer**

With the completion of the simulations and getting the desired results, we proceed to construct the jammer circuits. The construction is done using various electronic devices needed to build the jammer.

**Testing and Packaging**

The device is tested to ascertain the characteristics of the jamming system such as; effective jamming, radiated power, etc. Packaging is important to prevent any damage to the jamming system. The packaging also prevents harm to humans such as electrocution and damage to property.

# Chapter 2: - Literature Review

## 2.1 Brief Overview of Mobile Telephone Systems Technologies (Generations)

One of the key requirements for any radio-based telecommunications system is the efficient use of the frequencies that are available. The key technologies used in cellular mobile radio include cellular frequency reuse. The first generation systems (1G) were characterized by the fact that they were based on analogue technology. Different users in the same cell were allocated different channels. This technique is known as Frequency Division Multiple Access (FDMA). These include systems such as the Advanced Mobile Phone System (AMPS), Nordic Mobile telephone (NMT), Total Access Communication System (TACS), etc. the analog systems (1G) were designed for voice applications. All these systems offered handover and roaming capabilities but the cellular networks were unable to interoperate between countries. This was one of the inevitable disadvantages of first generation mobile networks. Also as demand grew, the available spectrum became progressively more congested. As a result, it quickly became obvious that a less spectrum-hungry technique would be required. This led to the birth of the second generation systems (2G).

2G systems employed digital technology to provide the required levels of efficiency. The two early 2G systems namely GSM and US-TDMA as well as its derivative PDC (Pacific Digital Cellular), all used a combination of FDMA and another technique where by different users were allocated different time-slots on the same channel. This system is known as Time Division Multiple Access (TDMA). These systems (2G) offered limited data facilities, therefore interim solutions were sought. 2.5G systems provided higher data rates than were possible with the existing 2G systems. A system known as General Packet Radio Service (GPRS) used with GSM provided an increase in data rate. Here the chief change was the use of packet radio systems rather than using circuit switch as in the earlier systems. A data rate of up to 115kbps was attainable. A further data rate improvement was provided by another system known as Enhanced Data rate for GSM Evolution (EDGE).

Although the above systems use a time-division approach, another system used different approach. Based on a spread spectrum technology, it used different codes to provide access to different users, known as Code Division Multiple Access (CDMA); this technology was originally used in a system known as cdmaOne (a full 2G technology). Its concept is employed in third generation systems (3G systems). CDMA2000 1X provided an evolutionary path to 3G systems. The CDMA2000 1xEV-DO (EV-DO stands for Evolution Data Only) is designed for data only and provides a peak data rate capability of over 2.4Mbps on the forward channel (downlink). It was followed by CDMA2000 1xEV-DV another 3G system (EV-DV meaning Voice and Data only) is an evolution of CDMA2000 that can simultaneously transmit both voice and data. Its peak rate is limited to about 384kbps on the reverse channel (uplink) and about 3.1Mbps on the forward channel (downlink).The Universal Mobile Telecommunication System (UMTS) uses wideband CDMA (WCDMA) providing data rates of up to 2Mbps. Another 3G system is the Time Division Synchronous CDMA (TD-SCDMA), which uses the same time slot for base stations and mobiles to communicate. Unlike other 3G systems which uses time division duplexing (TDD) technique. [4]

Other solutions were sought as the need for more spectral efficient technologies and very high speed data rates arose. The High Speed Packet Access (HSPA) was developed; it’s referenced as a 3.5G system or technology. This gives a peak rate of about 14.4Mbps on the forwards using packet data. Finally, even though the above technologies/systems are not being fully utilized, attention is being drawn to the next generation of systems such as the Ultra-Mobile Broadband (UMB) which is a 3.99/4G evolution cellular technology for CDMA 2000, the Long Term Evolution (LTE) which is also a 3.99/4G technology. [16] These systems would be much more spectral efficient and also provide improved capabilities in terms of data rates, etc.

## 2.2 Brief Overview of GSM

Global system for mobile communication (GSM), originally Groupe Spécial Mobile is an open digital mobile telephony standard developed by the European Telecommunication Standards Institute (ETSI) to describe technologies for second generation cellular networks.[5]

The GSM system is a digital-only system and not designed to be backward-compatible with the established analog systems. The GSM radio band is shared temporarily with analog cellular systems in some European nations. GSM uses a variation of time division multiple access (TDMA) and is the most widely used of the three digital wireless telephony technologies (TDMA, GSM and CDMA). GSM digitizes and compresses data, then sends it down a channel with two other streams of user data each in its own time slot, operating either in the 900 or 1800 MHz frequency band. [6]

### 2.2.1 Architecture and Operation of GSM Network

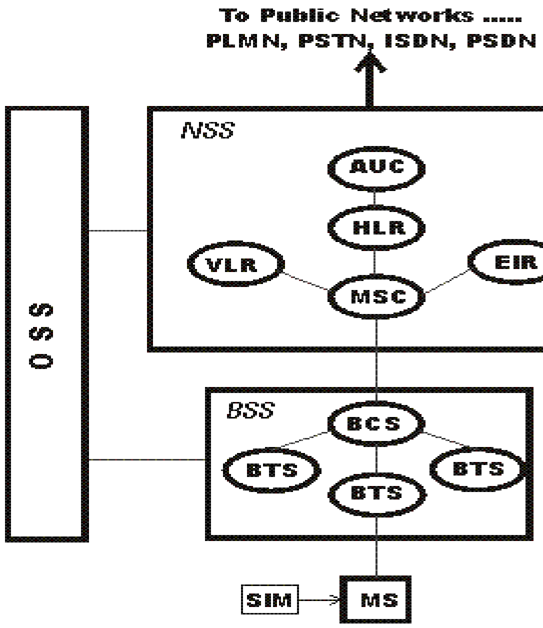


*Figure 2.0 Simplified GSM Network Architecture [20]*

The GSM mobile telephony service is based on a series of contiguous radio cells which provide complete coverage of the service area and allow the subscriber operation anywhere within it. Prior to this cellular concept, radio phones were used, however it was limited to just the one transmitter covering the whole area.

The advantage of the cellular over radiophone is its ability to handover a call from one cell to the next when a user moves his/her phone from one location to another whiles making a call. Cellular telephone is a totally automatic process and requires no special intervention by the user but it is a complex technical functioning requiring significant processing power to achieve a quick reaction.

The functional architecture of GSM system can be broadly divided into the Mobile Station (MS), the Base Station Subsystem (BSS) , the Network and Switching Subsystem (NSS) and finally, the Operations and Support Subsystem (OSS). Each subsystem is comprised of functional entities that communicate through the various interfaces using specified protocols.

The subscriber carries the mobile station. The mobile station represents the only equipment the GSM user ever sees from the whole system, it consists of two parts. The hardware popularly referred to as mobile phone. The mobile phone consists of devices such as radio transceivers, digital signal processing and a display screen. The other part is the subscriber identity module (SIM), implemented as a smart card. The SIM card contains the international mobile subscriber identity (IMSI), which identifies a subscriber, a secret key for authentication, and other user information. The mobile equipment or phone is operational only when a valid SIM provided by a network operator is placed in it.

The base station subsystem controls the radio link with the mobile station. The network and switching subsystem, which is the main part of which is the mobile-services switching center (MSC), performs the switching of calls between the mobile and other fixed or mobile network users, as well as management of mobile services such as authentication. [15]

### 2.2.2 Multiple Access and Channel Structure

Radio spectrum is a limited resource shared by all users a method must be devised to divide up the bandwidth among as many users as possible. The method GSM uses is a combination of both time and frequency division multiple access, (TDMA/FDMA). The FDMA part involves the division by frequency of the (maximum) 25MHz bandwidth into 124 carrier frequencies spaced 200 KHz apart. One or more carrier frequencies are assigned to each base station. Each of these carriers’ frequencies is then divided in time using a TDMA scheme. The fundamental unit of time in TDMA scheme is called a burst period and it last 15/26ms (approximately 0.577ms). Eight burst periods are grouped into a TDMA frame (120/26ms or approx. 4615ms) which forms the basic unit for the definition of logical channels. One physical channel is one burst period per TDMA frame. [15]

### 2.2.3 Multiplexing Techniques

One of the key elements of any radio communications system is the way in which radio communications are maintained in both directions. Terms including simplex, duplex, frequency division duplex (FDD), and time division duplex (TDD), are all methods that can be used.

The two multiplexing techniques or schemes widely used in cellular and cordless terminologies are;

I. Frequency Division Duplexing (FDD) – in FDD for the communication between the mobile and base stations two symmetric frequency bands are used, that is, the available frequency band is split in to two partial bands, to enable simultaneous sending and receiving. One partial band is assigned as uplink (from mobile to base station) and the other partial band is assigned as downlink (from base station to mobile station).

Uplink: transmission band of mobile station = receiving band of base station.

Downlink: receiving band of mobile station = transmission band of base station

II. Time Division Duplexing (TDD) – TDD systems uses only a single frequency and it shares the channel between transmission and reception, spacing them apart by multiplexing the two signals on a time basis. In other words, the uplink of the voice call is time multiplexed on the same frequency as the downlink of the voice call.

The system uses frequency division duplex, and as a result the channels are paired – one for the downlink from the BTS to the mobile and another for the reverse link back to the BTS. The frequency difference between the two channels varies according to the band in use. For 900MHz there is a difference of 45 MHz between transmit and receive, when the 1800MHz band is used the frequency difference is 95 MHz, and for the 1900MHz band the difference is 80 MHz [4]

*Table 2.0 Transmit and receive bands for the various GSM bands*. [4]

| Band/system | BTS transmit(mobile receive) | BTS receive(mobile transmit) |
|---|---|---|
| 900MHz | 935–960MHz | 890–915MHz |
| DCS1800 | 1805–1880MHz | 1710–1785MHz |
| PCS1900 | 1930–1990MHz | 1850–1910MHz |

### 2.2.4 Power levels

A variety of power levels is allowed by the GSM standard. The highest is 20 watts (43dBm) and the lowest is 800mW (29dBm). As mobiles may transmit for only one-eighth of the time (i.e. for their allocated slot, which is one of eight), the average power is one-eighth of the maximum. Additionally, to reduce the levels of transmitted power and hence the levels of interference, mobiles are able to step the power down in increments of 2dB from the maximum to a minimum of 13dBm (20mW). The mobile station measures the signal strength or signal quality (based on the bit error rate), and passes the information to the BTS and hence to the BSC, which ultimately decides if and when the power level should be changed.

A further power-saving and interference-reducing facility is the discontinuous transmission (DTx) capability that is incorporated within the specification. It is particularly useful because there are long pauses in speech; such as when the person using the mobile is listening, and during these periods there is no need to transmit a signal. [17]

Output Power

The maximum transmitting powers for GSM (900 & 1800MHz frequencies) for both the mobile station and base station is given below: [18]

*Table 2.1 Mobile station maximum output power and lowest power control level*

| Power Class | GSM 900<br>Maximum output power | DCS 1800<br>Maximum output power |
|---|---|---|
| 1 | ---------------- | 1W (30dBm) |
| 2 | 8W (39dBm) | 0.25W (24dBm) |
| 3 | 5W (37dBm) | 4W (36dBm) |
| 4 | 2W (33dBm) | |
| 5 | 0.8W (29dBm) | |

Note: The lowest power control level for all classes of GSM 900 MS is 19 (5dBm) and for all classes of DCS 1 800 MS is 15 (0dBm). [18]

*Table 2.2 Base station transmitter maximum output power [18]*

| TRX Power Class | GSM 900<br>Maximum output power | DCS 1800<br>Maximum  output power |
|---|---|---|
| 1 | 320 – (<640)W | 20 – (<40)W |
| 2 | 160 – (<320)W | 10 – (<20)W |
| 3 | 80 – (<160)W | 5 – (<10)W |
| 4 | 40 – (<80)W | 2.5 – (<5)W |
| 5 | 20 – (<40)W | |
| 6 | 10 – (<20)W | |
| 7 | 5 – (<10)W | |
| 8 | 2.5 – (<5)W | |

### 2.2.5 What GSM Offers

The originators of GSM wanted Integrated Services Digital Network (ISDN) compatibility in terms of the services and the control signalling used. However, radio transmission limitations, in terms of bandwidth and cost do not allow the standard ISDN B-channel (bearer channel) of bit rate 64 kbps to be practically achieved.

Telecommunication services can be divided into bearer services, teleservices and supplementary services. A basic teleservice supported by GSM is telephony. As with all other communications, speech is digitally encoded and transmitted through GSM network as with a digital stream. It also has an emergency service, where the nearest emergency service provider is notified by dialling three digits (similar to 911)

Other data services include group 3 facsimile, as describe by ITU-T recommendation T.30, which is supported by use of an appropriate fax adaptor. A unique feature of GSM, not found in older analogue systems, is the Short Message Service (SMS). SMS is a bidirectional service for short alphanumeric (up to 160 bytes) messages. Messages are transported in a store-and-forward fashion. For point-to-point SMS, a message can be sent to another subscriber to the service, and an acknowledgement of receipt is provided to the sender. SMS can also be used in a cell- broadcast mode, for sending messages such news or weather updates. Messages can also be stored in the Subscriber Identity Module (SIM) card for later retrieval.

Supplementary services are provided together with teleservices or bearer services, they include several forms of call forward (such as call forwarding when the mobile subscriber is unreachable by the network), and call barring of outgoing or incoming calls, for example when roaming in another country. Many additional supplementary services include caller identification, call waiting, Multimedia services and multi-party conversations. [7]

### 2.2.6 Frequency Bands

Frequency bands are groupings of radio frequencies that are used by mobile networks to communicate with mobile phones. [8] GSM frequency bands are cellular frequencies designated by the ITU for the operation of GSM mobile phones. The frequency bands that a phone supports determine to a large degree where and on which networks it can be used.

GSM was first developed to work in the 900MHz range. Later developments led to the first derivative of GSM, the Digital Cellular System 1800 (DCS 1800). This development translates GSM system into 1800MHz frequency range.

In the United States of America the Personal Communication System 1900 (PCS 1900) was developed and adapted after the introduction of the DCS 1900. In Africa, Europe, Middle East and Asia mobile service providers use both 900MHz and 1800MHz band. Fewer operators use DCS-1800 and GSM-1800. A dual band 900/ 1800 phone is required to be compatible with almost all operators. At least the GSM-900 band must be supported in order to be compatible with many operators. [9]

In Ghana there are six telecommunications service providers, out of that number, five operate on the GSM platform with the other employing CDMA technology. [13]

## 2.3 Basic Cellular System

The cellular system connects mobile radios (called mobile stations) via radio channels to base stations. Some of the radio channels (or portions of a digital radio channel) are used for control purposes (setup and disconnection of calls) and some are used to transfer voice or customer data signals. Each base station contains transmitters and receivers that convert the radio signals to electrical signals that can be sent to and from the mobile switching centre (MSC). The MSC contains communication controllers that adapt signals from base stations into a form that can be connected (switched) between other base stations or to lines that connect to the public telephone network. The switching system is connected to databases that contain active customers (customers active in its system). The switching system in the MSC is coordinated by call processing software that receives requests for service and processes the steps to setup and maintain connections through the MSC to destination communication devices such as to other mobile telephones or to telephones that are connected to the public telephone network. When linked together to cover an entire metro area, the radio coverage areas (called cells) form a cellular structure resembling that of a honeycomb. Cellular systems are designed to overlap each cell border with adjacent cell borders to enable a “hand-off” from one cell to the next. As a customer (called a subscriber) moves through a cellular system, the mobile switching centre (MSC) coordinates and transfers calls from one cell to another and maintains call continuity. [19]

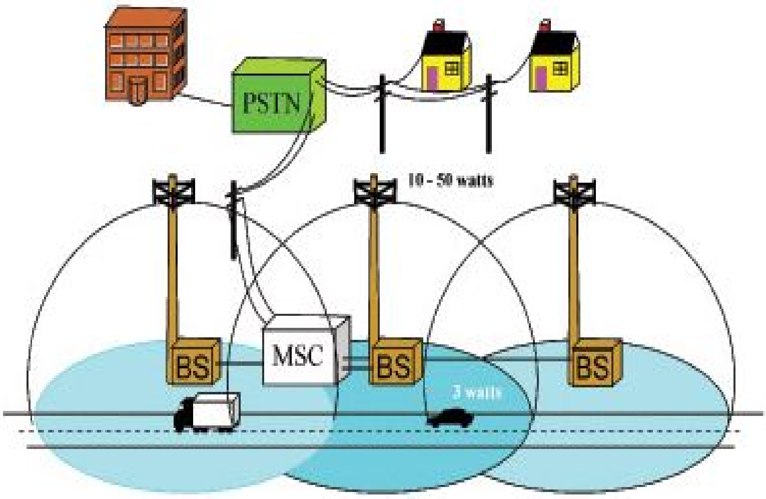


*Figure 2.0 cc Basic Cellular System [19]*

### 2.3.1 Basic Multiple Access Schemes In Cellular Systems

Every cellular system generally consists of a base station (BS) and a number of mobile stations (MS) that transmits and receives signals to and from the BS. Since there are many MSs within the cell of a BS (its coverage area), it’s necessary to have a method of allowing multiple subscribers to gain access to the system and use it simultaneously. This method or processes is known as multiple access schemes, and there are three main methods that are in use: Frequency Division Multiple Access (FDMA), Time Division Multiple Access (TDMA) and Code Division Multiple Access (CDMA). [14]

### Frequency Division Multiple Access (FDMA)

This scheme was used by all analogue systems and is the most straightforward of the multiple access schemes that have been used. As a subscriber comes onto the system, or swaps from one cell to the next, the network allocates a channel or frequency to each one. In this way the different subscribers are allocated a different slot and access to the network. As different frequencies are used, the system is naturally termed Frequency Division Multiple Access.

### Time Division Multiple Access (TDMA)

This system came about with the transition to digital schemes for cellular technology. Here digital data could be split up in time and sent as bursts when required. As speech was digitized it could be sent in short data bursts, any small delay caused by sending the data in bursts would be short and not noticed. In this way it became possible to organize the system so that a given number of slots were available on a given transmission. Each subscriber would then be allocated a different time slot in which they could transmit or receive data. As different time slots are used for each subscriber to gain access to the system, it is known as time division multiple access.

### Code Division Multiple Access (CDMA)

CDMA uses one of the aspects associated with the use of direct sequence spread spectrum. The scheme has been likened to being in a room filled with people all speaking different languages. Even though the noise level is very high, it is still possible to understand someone speaking in your own language. With CDMA, different spreading or chip codes are used. When generating a direct sequence spread spectrum, the data to be transmitted are multiplied with spreading or chip code. This widens the spectrum of the signal, but it can only be decoded in the receiver if it is again multiplied with the same spreading code. All signals that use different spreading codes are then not seen, and are discarded in the process. Thus, in the presence of a variety of signals it is possible to receive only the required one.

In this way the base station allocates different codes to different users, and when it receives the signal it will use one code to receive the signal from one mobile and another spreading code to receive the signal from a second mobile. In this way, the same frequency channel can be used to serve a number of different mobiles.

### Orthogonal Frequency Division Multiple Access (OFDMA)

As the name implies, OFDMA is based around OFDM. This is a technology that utilizes a large number of close spaced carriers. OFDM is a form of transmission that uses a large number of close spaced carriers that are modulated with low rate data. Normally these signals would be expected to interfere with each other, but by making the signals orthogonal to each another there is no mutual interference. This is achieved by having the carrier spacing equal to the reciprocal of the symbol period. This means that when the signals are demodulated they will have a whole number of cycles in the symbol period and their contribution will sum to zero - in other words there is no interference contribution. The data to be transmitted is split across all the carriers and this means that by using error correction techniques, if some of the carriers are lost due to multi-path effects, then the data can be reconstructed. Additionally having data carried at a low rate across all the carriers means that the effects of reflections and inter-symbol interference can be overcome. To utilize OFDM as a multiple access scheme for cellular technology, two different methods are used, one for the uplink and one for the downlink. In the downlink, the mobile receives the whole signal transmitted by the base station and extracts the data destined for the particular mobile. In the uplink, one or more carriers are allocated to each handset dependent upon the data to be transmitted, etc. In this way the cellular network is able to control how the data is to be sent and received.

## 2.4 History of Jamming

The coming of the information age brought about a considerable reliance on wireless electronic communication. Although cellular phone systems and personal communication systems have brought wireless radio frequency (RF) communications to the masses, nowhere is this reliance observable than in the military. For decades, the military has hinged on RF communications for the execution of command and tactical forces.

An adversary has interest in these communications, since tactical commanders use RF communication to exercise control of their forces. This interest lies in two primal areas;

(i) To intercept the information that transpires over them and

(ii) To deny the successful exchange of the information from the sender to the receiver.

Jamming of radio telegraph was first deployed by the military with records of its success dating back to the early 20th century. Germany and Russia were the first to engage in jamming back then. The jamming signal most frequently consisted of co-channel characters. It was until the early thirties, when the first cases of jamming of radio broadcasting were first recorded. In the late 20's Berlin started to jam the programs of Radio Kominterm. Jamming of foreign radio broadcast stations has often been used in wartime to prevent or deter citizens from listening to broadcasts from enemy countries. However such jamming is usually of limited effectiveness because the affected stations usually change frequencies, put on additional frequencies and/or increase transmission power.

During World War II ground radio operators would attempt to mislead pilots by false information in their own language, in what was more precisely a spoofing attack than jamming. Radar jamming is also important to disrupt use of radar used to guide an enemy's missiles or aircraft. Modern secure communication techniques use such methods as spread spectrum modulation to resist the deleterious effects of jamming.

Jamming has also occasionally been used by the Governments of Germany (during World War II), Israel, Cuba, Iraq, Iran (Iraq and Iran war, 1980-1988), China, North and South Korea and several Latin American countries, as well as by Ireland against pirate radio stations such as Radio Nova. The United Kingdom government used two coordinated, separately located transmitters to jam the offshore radio ship, Radio North Sea International off the coast of Britain in 1970. [10]

### 2.4.1 Difference between Jamming and Interference

These terms are used interchangeably, but in recent times most radio users use the term "Jamming" to describe the deliberate use of radio noise or noise induced signals in an attempt to disrupt communication (or prevent listening to broadcast) whereas, the term "interference" is used to describe unintended or unwanted forms of disruption. The latter is far more common than the former. [11]

### 2.5 Mobile Jamming and Disabler Techniques

There are several way to prevent mobile phone from being used i.e. ringing in specific area. Five type used and being developed by Mobile and Personal Communications Committee of the Radio Advisory Board of Canada meeting of 22nd June 1999 are explained below. [12]

#### 2.5.1 Type "A" Device (Jammers)

In type "A", the mobile phone's signal is overpowered with a stronger signal. This type of device comes equipped with several independent oscillators, transmitting jamming signals capable of blocking frequencies used by paging devices as well.

Type "A" device operates by broadcasting radio frequency (RF) interferences preventing mobile phones and even pagers located within its area of broadcast the ability to transmit and receive calls. It broadcasts 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. There are two types; the brute force jamming, which jams everything. The other puts out a small amount of interference, and you could potentially confine it within a single cell block.

#### 2.5.2 Type "B" Device (Intelligent Cellular Disablers)

This device is also known as "Intelligent Cellular Disablers". It does not transmit an interfering signal on the control channels. The device basically works as a detector. This device works by communicating with the nearest cellular base station. When the device detects the presence of a mobile phone in the room it operates ("silent room"), a prevention of authorization of call establishment is done by the software, at the base station.

The device signals the base station that the user is in a "quite room", and hence do not establish the target communication. This process of detection and interruption of call establishment is done during the interval normally reserved for signaling and handshaking.

This intelligent device as its name implies can recognize emergency calls and also allow specific pre-registered users to use their mobile phones for a specified duration. Though this device sounds like a good solution, a provision is needed by the cellular/pcs service providers, allowing the detector device to be an integral part of the cellular/pcs systems.

### 2.5.3 Type “C” Device (Intelligent Beacon Disablers)

This device like type “B” does not transmit any interfering signal on the control channels. This device when located in a specific “silent” room, functions as a ‘beacon’ and any compatible terminal is ordered to disable its ringer or operation. Within the coverage area of the beacon, only terminals which have a compatible receiver would respond and this should be built on a separate technology from cellular/PCS, e.g. Bluetooth technology. In addition, the handset must re-enable its normal functions as it leaves the coverage of the beacon.

The need for intelligent handsets with a separate receiver for the beacon receiver from the cellular/PCS receiver makes effective use for type “C” problematic for years.

### 2.5.4 Type “D” Device (Direct Receive and Transmit Jammer)

This jammer works similar to type “A”, but with a receiver, so that the jammer is predominantly in receive mode, and when it detects the presence of a mobile phone in the “silence” area, it will intelligently choose to interact and block the cell phone by transmitting a jamming signal. This jamming signal would only remain on, so long as the mobile continues to establish contact with the base station, otherwise there would be no jamming transmission.

The advantage of type “D” against “A” is that “D” emits less electromagnetic pollution in terms of raw power transmitted and frequency spectrum from the type “A” jammer, and therefore much less disruptive to passing traffic. This technique could be implemented without cooperation from pcs/cellular providers. Again this technique has an added advantage over type “B” in that no added overhead or effort is spent negotiating with the cellular network.

### 2.5.5 Type “E” Devices (EMI Shield – Passive Jamming)

This technique uses electromagnetic interference to make a room into what is known as a faraday cage. Faraday’s cage essentially blocks, or greatly attenuates virtually all electromagnetic radiations from entering or leaving the cage. The cage ranges from as small as a room to a whole building. 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.

## 2.6 GSM Jammer Requirements

The idea behind jamming is to introduce noise induced signals (interference) into the communications channel so that the actual signal is completely overwhelmed by the interference. However, it should be noted that a signal can never be totally jammed, rather the jammer only impedes the reception at the other end.

Jamming is successful only when the signal induced in the communications channel is able to limit the usability of the communications channel. In digital communication, the effectiveness of the channel is impeded only when the error rate of transmission cannot be compensated by error correction.

For a jamming attack to be successful, the power of the jammer should be roughly equal to the signal power at the receiver. The effectiveness of jamming depends on the jamming-to-signal ratio (J/S), modulation scheme, and channel coding and interleaving codes of the target system.

Generally, jamming-to-signal ratio can be measured by the equation:

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

Where:

Pj = jammer power

Pt = transmitter power

Gjr = antenna gain (jammer to receiver)

Grj = antenna gain (receiver to Jammer)

Gtr = antenna gain (transmitter to receiver)

Grt = antenna gain (receiver to transmitter)

Br = communications receiver bandwidth

Bj = jamming transmitter bandwidth

Rtr = range between communications transmitter and receiver

Rjt = range between jammer and communications receiver

Lj = jammer signal loss (including polarization mismatch)

Lr = communication signal loss

The above Equation indicates that the jammer's Effective Radiated Power, which is the product of antenna gain and output power, should be high if jamming efficiency is required. As the equation shows, the antenna pattern, the relation between the azimuth and the gain, is a very important aspect in jamming.

To successfully jam a particular region, we need to consider a very important parameter 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 up to 9dB.

### 2.6.1 Related Works

In this section we review four previous works in relation to this project. Jammer designs, results and recommendations of these projects are what we will be reviewing. To start with, it is important to note that all the four projects we are reviewing implemented the type "A" jammer technique known as Denial of Service. (DoS)

1. Ahmed Jisrawi, an undergraduate student at Jordan University of Science & Technology undertook his project on jammers titled "GSM-900 Mobile Jammer". The project was carried out in 2006. The following are the specifications of his work.

**Frequency:** His jammer was intended to jam GSM 900MHz band only

**Power Supply:** He designed and constructed a power supply to provide the needed electrical energy to the jammer. A 220V AC transformer was used. This is because components of the jammer use different voltage levels which are lower than the supply voltage (220VAC). A full wave rectifier was employed, the advantage of using full wave rectification is that it allows unidirectional current to the load during the entire cycle of the input voltage and the result of a full wave is an output voltage with a frequency twice the pulse every half-cycle of the input. The rectifier was made of four diodes connected as a bridge.

In order to filter out possible fluctuations coming out from the output of the full wave rectifier, capacitors were used. The value of capacitance was as larger as possible to minimize the ripples in the dc voltage and filter out any high frequency noise. In order to maintain a constant voltage a single chip regulator was used to provide voltages of +5, + 9 and -9 volts.

**Intermediate Frequency:** The IF function is used to generate the tuning signal for the voltage controlled oscillator (VCO) in the RF part. It is made up of the following parts; triangular wave generator, noise generator, signal mixer and a diode-clamper. The triangular wave generated is used as relaxation oscillator to produce square wave, before another op-Amp as an integrator to produce the desired waveform. 555-Timer IC operating in astable mode was used to generate the triangular waves. (All four projects we reviewed used the triangular wave generator).

In order to generate noise, zener diode which operates in reverse mode therefore creating an Avalanche effect which causes wide band noise was used .The triangular wave generated is mixed with the noise signals. This is done using operational amplifier configured as a summer. Then a DC voltage is added to the resulted signal to obtain the required tuning voltage using diode-clamper circuit. To obtain the required tuning voltage a diode-clamper circuit is used. He added a potentiometer in order to control the biasing voltage so as to get the desired tuning voltage.

**Radio Frequency:** In this section components are selected according to the desired specification of the jammer such as frequency range and coverage.

For the VCO; the MAXIM 2623 was used for a frequency range of 935-960MHz.The output power was -3dBm. A tank circuit is used to generate or oscillate the desired frequency. In the RF power amplification, to achieve the desired output power, a gain stage is needed. Ahmed used a cheap power amplifier from an old mobile phone. The PFO8103B Hitachi power amplifier from a Nokia mobile phone was sufficient to amplifier an input signal in the range of 800MHz to 1GHz by 34dB. It is recommended in the data sheet that the power input should be 1dBm. To meet this requirement he used another power amplifier stage after the VCO and before the Hitachi power amplifier module. At that stage he used the MAR-4SM power amplifier; it has a typical gain of 8dB for frequency range from dc to 1GHz, so the output after this stage should be around 5dBm. Finally a ¼ wavelength monopole antenna with 50Ω impedance and a gain of 2dBi, VSWR less than 1.7, bandwidth of 150MHz with 916MHz center frequency with a sweeping range of 625-960 MHz was selected and used.

**Results:** The designed jammer was successful in jamming the two GSM-900 networks in Jordan (Fastlink and mobilecom at that time).He faced a problem with the power supply which was not able to deliver the right amount of load current to the VCO, which in turn could not tune the VCO to the desired frequency range. In view of this the jammer could jam a distance of 10meters instead of the intended 20meters.

2. Syed Absar Ahmed Shah, Sohaib Zafar and Syed Ali Wajahat Jafri undergraduate students at National University of Science and technology Pakistan undertook their project titled “GSM Jammer”. The project was also carried out in 2006.

**Frequency:** Their jammer was intended to jam GSM 900MHz band only

**Power Supply:** Their power supply used a transformer to convert 220V AC to 12V AC with a 2A rating. This is then fed to a full wave rectifier with the rectifier made of four diodes connected as a bridge. Their rectifier converts the 50Hz AC signal to a 100 Hz pulsating DC signal. In order to minimize power fluctuations capacitors were used to filter out the undesired voltage levels. The capacitors used were as larger as possible, to minimize the ripples in the dc voltage and filter out any high frequency noise. To maintain a constant voltage single chip regulators were used to provide voltages of +5, +9 and -9 volts, the ICs used were LM7805 (+5V), LM7809 (+9V) and LM7909 (-9V).

**Intermediate Frequency:** To provide a triangular wave 555- Timer IC operating in astable mode was used zener diode that allows currents in the forward direction as well as in the reverse direction were also integrated. It was connected in a reverse bias mode. Noise generator consisted of a 6.4V zener diode with small reverse current, a transistor buffer, LM386 audio amplifier acting as a natural band pass filter and small signal amplifier. Avalanche noise is similar to short noise but more intense and has a flat frequency spectrum (white noise).

**Radio Frequency:** The MAXIM 2623 Voltage controlled oscillator was used for a frequency range of 935-960MHz.The output power was -3dBm, with an input tuning voltage of around 120 KHz. A tank circuit is used to generate or oscillate the desired frequency. In the RF power amplification, to achieve the desired output power a gain stage is needed. Ahmed used a cheap power amplifier from an old mobile phone. The PFO8103B Hitachi power amplifier from a Nokia mobile phone was sufficient to amplifier an input signal in the range of 800MHz to 1GHz by 34dB. It is recommended in the data sheet that the power input should be 1dBm. To meet this requirement he used another power amplifier stage after the VCO and before the Hitachi power amplifier module. At that stage he used the MAR-4SM power amplifier; it has a typical gain of 8dB for frequency range from dc to 1GHz, so the output after this stage should be around 5dBm. Finally a helical antenna, with a reflection coefficient of -17dB was selected and used as an antenna.

**Results:** The jamming device was successful. As it was able to jam all the existing networks at the time namely; Mobilink GSM, Telenor, Warid, Paktel and Ulone. Among the constraints faced was that the power amplifier they used PF08103B was locally acquired and all the purchased ICs had internal inter-pin short circuits making them unfit for use. To bypass this, they used a HITTITE GSM power amplifier with gain of 20dB instead of the 33dB power gain of the intended power amplifier. The jamming radius was below the maximum theoretical value, this was due to atmospheric losses the range varied from 5m to 10m depending on these atmospheric conditions. They also experienced voltage dips due to problems with the power supply as they were unable to have good voltage regulations.

3. Balal Ansar, Faisal Mehmood Ahmed and Bilal Tariq undergraduate students of Comsats Institute of Information technology Pakistan undertook their project titled “Mobile Service Denial” in 2009.

**Frequency:** Their jammer was designed to work in the GSM 900MHz &1800MHz

**Power Supply:** They used an external power source, and therefore had no writings on their power supply as they did not do any designs on the power supply.

**Intermediate Frequency:** In order to generate noise they used zener diode and applied reverse bias voltage to establish avalanche breakdown region. When this happens it generates pink noise. Pink noise is random noise where the power is spread uniformly over a specific spectrum of frequencies such as 20-20,000Hz for audio.

**Radio Frequency:** They implemented a tank circuit design. A tank circuit is used to generate or oscillate the desired frequency. A tank circuit is typically a combination of capacitive and inductive circuits that exchanges energy back and forth. An inductor stores energy as a magnetic field, whereas a capacitor stores energy as a charge across plates. The tank circuit used a DC 12V.In choosing an antenna they used a ¼ wavelength monopole antennas, with50Ω input impedance, frequency 850-1GHz, length 234/fr and VSWR<2.

**Results:** The jamming device was a success; it was able to jam all the networks. The effective jamming distance was around 10m.

4. Adeyemi Bayode Victor, Tebe Ifede Parfait and Filson Kwadwo Banful undergraduate students of Ghana Telecom University College Ghana also undertook their project titled “Design and Construct a Frequency Jamming Device for Mobile Networks”. It was done in 2011.

**Frequency:** They intended jamming GSM 900&1800MHz, CDMA, 3G networks and Bluetooth.

**Power Supply:** Used a transformer with 220/240VAC primary windings and 15VAC secondary windings, their transformer had a centre- tapped secondary windings. They employed full wave rectification. The advantage of using full wave rectification is that it allows unidirectional current to the load during the entire cycle of the input voltage and the result of a full wave is an output voltage with a frequency twice the pulse every half-cycle of the input. In filtering they used a 35volts, 1000µF. the reason is that the values should be higher than their supply voltage of 30V between positive and negative terminals.

**Radio Frequency:** In order to jam the various frequency bands they used three different VCOs as they had to deal with three different frequency ranges. The following are the various VCOs used:

i. CVCO 55BE-0800-0980, for CDMA and GSM 900.
ii. CVCO 55BE-1200-2300 for GSM 1800 and 3G
iii. CVCO55BE-2400-2670 for Bluetooth/Wi-Fi.

Two penta-bands with frequency between 800-2200MHz, linear polarization input power 20W, input impedance 50Ω and gain 0dBi due to its small size.

**Results:** The jammer was unable to deny service to any of the networks intended, therefore, their set objective was not achieved due to the following reasons;

Two AH312 power amplifiers and one TQP777002 matched power amplifies were unable to amplify signals from the VCOs to the required power levels. This was due to the tiny nature of the two power amplifiers and the matched power amplifier.

They also indicated that the base station on their campus caused a higher uplink power to the mobile phone that meant that the signal the jammer generated had to be greater in order to jam the BTS's transmit signal.

# Chapter 3: - Design and Implementation

### 3.1.0 Design Parameters

After studying the various technique of jamming, our device is of the type "A" also known as denial of service (DOS). It involves transmitting noise induced signals on the same frequency as the frequency band used. The block diagram for this type is shown in figure 3.1.0, it shows the main parts which are: RF-section, IF-section, and the power supply.

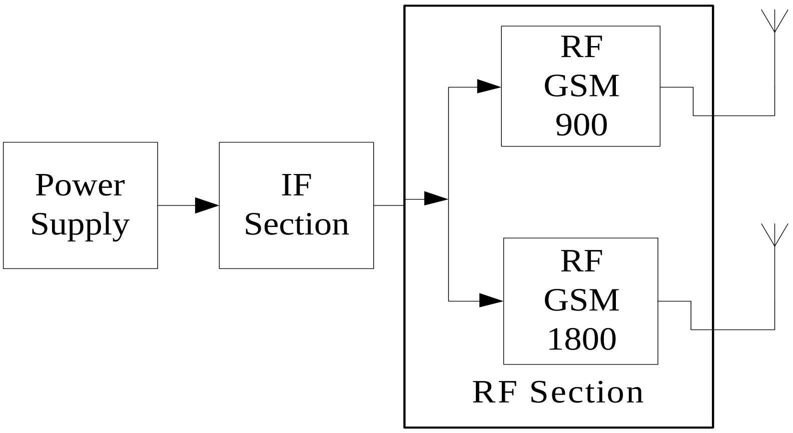


*Figure 3.1.0 Block diagram of type "A"*

*Table 3.0 Transmit and receive bands for the GSM frequencies of interest*

| Band/system | BTS transmit (mobile receive/downlink) | BTS receive (mobile transmit/uplink) |
|---|---|---|
| 900MHz | 935–960MHz | 890–915MHz |
| DCS1800 | 1805–1880MHz | 1710–1785MHz |

Now we consider the approach to jamming, that is, whether to jam the BTS transmit (mobile receive) or the BTS receive (mobile transmit). Jamming the mobile transmit would mean disrupting communication over the entire cell and therefore would require a high power transmitter. Jamming the mobile receive only jams the required area and therefore requires a transmitter of sufficient power. Our goal therefore is to disrupt communication over the mobile receive (forward link) only. So our frequency design will be as follows:

GSM 900 $\longrightarrow$ 935 – 960 MHz

GSM 1800 $\longrightarrow$ 1805 – 1880 MHz

We focused on some design parameters to establish the design specifications. These parameters are as follows:

**The distance to be jammed (D): -** this parameter is of relevance to our design, since the amount of output power to the jammer depends on the area that we need to jam. Our design is established upon D of 25 meters for either frequency band or systems.

**Jamming-to-signal ratio (J/S): -** the J/S is the ratio of the jamming signal strength (within the receivers' bandwidth) to the strength of the desired signal. Jamming becomes effective when the interfering signal in the receiver is strong enough to prevent or deny the usability of the communication transmission or channel.

To successfully jam a particular region, we need to consider a very important parameter 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 up to 9dB.

**Free space loss (F): -** for us to able to effectively jam the mobile device's reception, we need to have jamming signal strength of -24dBm. Our radiated signal however, will undergo some attenuation in transmission from the jammers antenna to the antenna of the mobile device. This attenuation is due to path loss (which is the reduction in the power density of an electromagnetic wave as it propagates through space). This path loss can be calculated using the simple *free space path loss* (Lp) approximation given by:

$$Lp\ (dB) = 32.44 + 20\log (f\ .D) \qquad (1)$$

Where f is the frequency in MHz and D, the distance travelled in kilometres.

The worst case of path loss happens when the maximum frequency is used in equation (1).

For GSM 900:

Lp (dB) = 32.44 + 20log (0.025*960); which gives 60.04 dB, Lp ≅ 60 dB

For GSM 1800:

Lp (dB) = 32.44 + 20log (0.025*1880); which gives 65.88dB, Lp ≅ 66 dB

### 3.2.0. System Design

### 3.2.1. Power Calculations

We need to find the power that needs to be transmitted to jam any cell phone within a distance of around 25 meters for both systems. Here, we take into account the ideal signal-to-noise ratio (SNR) and also the maximum power signal for mobile receiver. A very good device has an SNR of about 9dB, which will be used as our worst case scenario for the jammer.

Our goal here is to find the output power from the device, so when we add the path loss to the jammer power we get our target:

For GSM 900:

The minimum signal to noise ratio SNR = 9dB

The maximum signal power at receiver S = -15dBm

The jammer power Jr is calculated as follows:$\frac{S}{Jr} = 9\ dB$

Then Jr = S – 9 = -15 -9 = -24dBm

Output jammer power = -24dBm + 60.04 = 36dBm ≅ 4.0 W

For GSM 1800:

The minimum SNR = 9dB and the maximum S = -23dBm

Then, Jr = -23 – 9 = -32dBm

Output jammer power = -32dBm + 65.88 = 33.88dBm ≅ 2.5 W

### 3.3.0. Parts of the jammer Device

Figure 3.1.0 above shows the block diagram of the jammer to be designed

### 3.3.1. Power Supply

The power supply is an important part of the jammer. The power supply provides the required electrical energy to the whole circuitry. Figure 3.1.1 shows the main parts of a basic power supply unit.

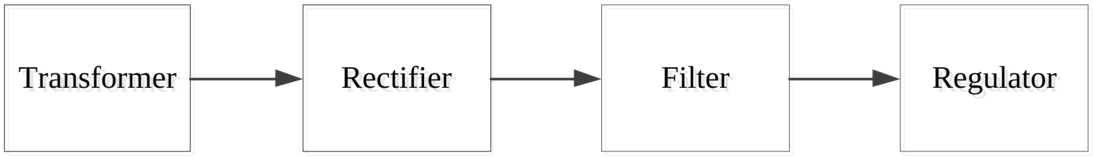


*Figure 3.1.1 Block Diagram of Power Supply*

**Transformer: -** a transformer is an electrical apparatus designed to convert alternating current from one voltage level to another. It can be designed to “step up” or “step down” voltages and works on the magnetic induction principles.

**Rectifier: -** The rectifier converts alternating current (AC) input to direct current (DC) output, and can be a full wave or half wave rectifier (rectification).

A full wave rectifier has an advantage over half wave rectifiers. The average (DC) output voltage from a full wave rectifier  is higher than that of half wave (twice that of half wave); also its output has fewer ripples which in effect produce(s) a smoother or a smooth output.

**Filter: -** a filter is used to eliminate fluctuations from the DC output of the full wave rectifier in order to produce a constant DC voltage.

**Regulator: -** a regulator is used to provide the desired constant DC output independent of the input voltages.

The choice of the power supply unit was influenced, the cost and size, the input voltage range (AC), and lastly the voltages needed by the various parts of our system.

In finding an appropriate supply for the project, we used an ST VIPer series DVD power supply, due to the following qualities of the power unit;

VIPer22A has a wide operating voltage range from 8V to 42V, respectively minimum and maximum values for under-voltage and over-voltage protections. This function is very useful for achieving low stand-by total power consumption.

ST VIPer series of off-line switch mode power supply regulators combines an optimized, high voltage, avalanche rugged Vertical Power MOSFET with current mode control PWM circuitry. The AC to DC conversion that is simpler and quicker.

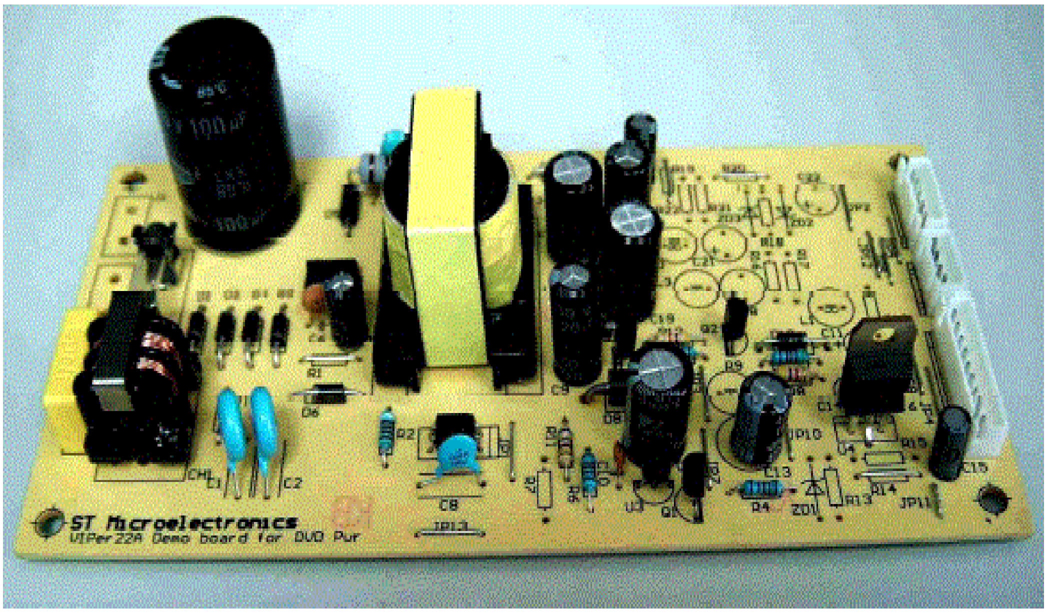


*Figure 3.1.2 Picture of the VIPer Power Supply (AN1897)*

*Table 3.1 Full Load Regulation*

| **Output** | **85Vac** | **230Vac** | **260Vac** |
|---|---|---|---|
| 5V/1.5A | 5.02V | 5.09V | 5.08V |
| 12V/30mA | 12.03V | 12.06V | 12.05V |
| -12V/30mA | -12.01V | -12.05V | -12.05V |
| 3.3V/0.15A | 3.77V | 3.80V | 3.78V |

### 3.3.2. Intermediate Frequency (IF) Section

The IF sections role is to generate a/the tuning voltage(signal) for the VCO in the radio frequency(RF) section, so that the output of the VCO is swept through the desired range of frequencies (from minimum to the desired maximum frequency). The output of this section is basically a triangular wave to which noise is added. This is then offset at a proper amount of DC value to obtain the desired tuning voltage or signal. The IF section (control section) is composed of the following:

1. Triangular wave generator
2. Noise generator
3. Signal mixer
4. Offset circuit

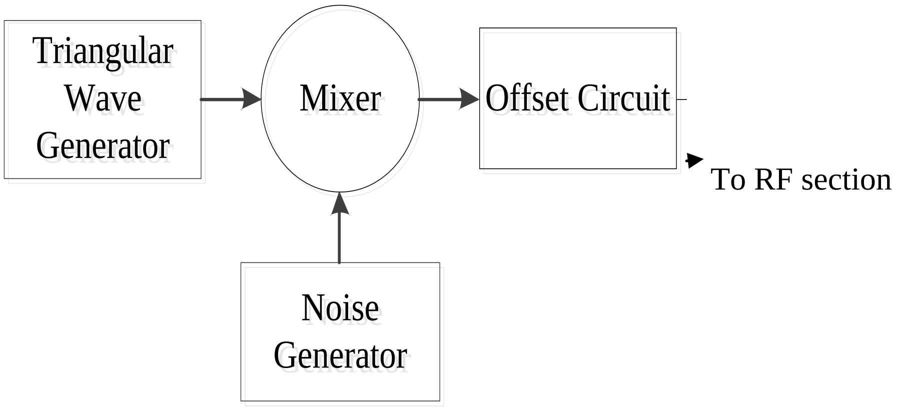


*Figure 3.1.3 Block Diagram of IF Section*

### Triangular Wave Generator

The triangular wave is used to sweep the VCO through the desired range of frequencies. In our design a 555-timer IC operating in the astable mode is used to generate the triangular wave. In the astable mode the 555-timer has no stable states, that is, it oscillates when operated in this mode and puts out a continuous stream of rectangular pulse.

In order to get a 555-timer to operate in the/an astable mode, it’s necessary to continuously re-trigger the 555-timer IC after every time cycle. This can be done by connecting the trigger input (pin 2) and the threshold input ((pin 6) to a common node, the device therefore acts as an astable oscillator.

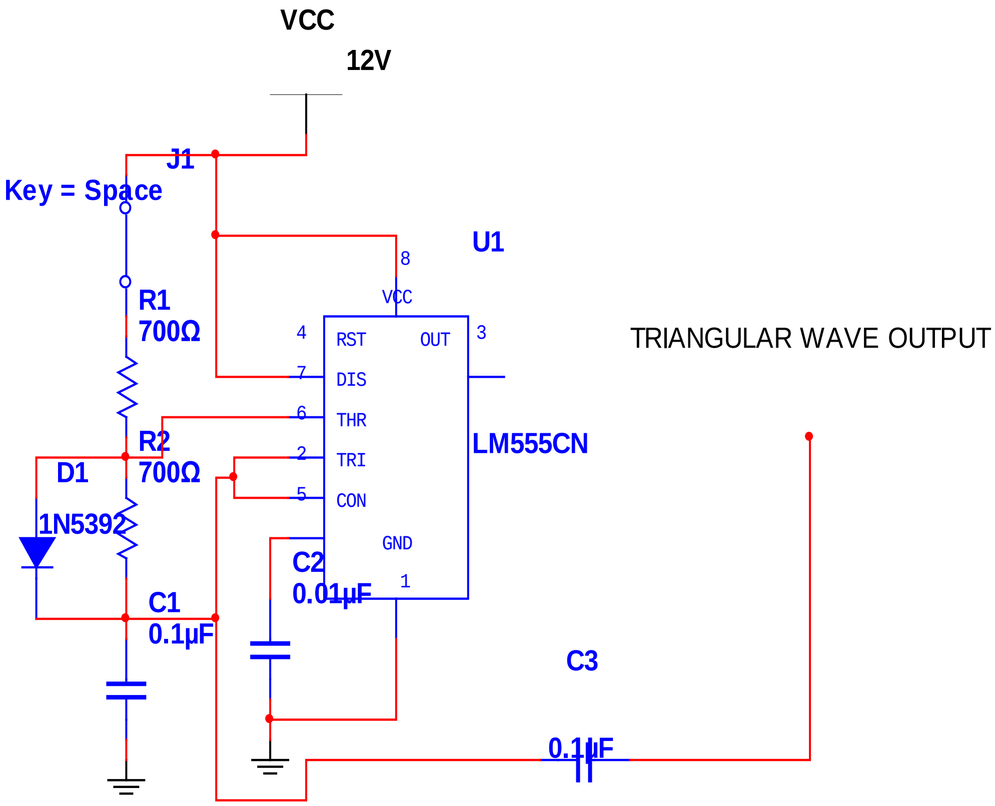


*Figure 3.1.4 Circuit Diagram of Triangular Wave Generator*

*Table 3.2 Showing the pin numbers of a 555-timer with their functions*

| **Pin Number** | **Function** |
|---|---|
| 1 | Ground |
| 2 | Trigger |
| 3 | Output |
| 4 | Reset |
| 5 | Control voltage |
| 6 | Threshold |
| 7 | Discharge |
| 8 | Vcc |

From figure 3.1.4, pin 2 and pin 6 are connected together allowing the circuit to re-trigger itself on each cycle allowing it to operate as a free running oscillator. The resistor R2 is connected between Vcc of 12VDC and pin7, the resistor R1 is also connected between pin 7. The resistor R1 and R2 together with the capacitor C1 form the timing circuit that sets the frequency of oscillation. During each circle the capacitor C1 charges up through the timing resistor R1 and R2, but discharges itself only through R2 as the other side of R2 is connected to pin 7 which has low impedance to ground for low output intervals of the cycle.

The capacitor C2 connected to pin 5 is for decoupling and has no significant effect on the operation of the circuit. It is used to eliminate electrical noise, therefore can be disconnected if noise is not a problem The frequency of the pulse stream in the astable mode is dependent on the values of the timing circuits formed by R1, R2 and C. the frequency of oscillation is expressed in the formula:

$$f = \frac{1.44}{C(R1 + 2R2)}$$

$$f = \frac{1.44}{\big(700 + 2(700)\big)0.1 \times 10^{-06}}$$

$$= 6857.143 \cong 6857Hz$$

The high (“ON”) and low (“OFF”) times of each pulse can be calculated from;

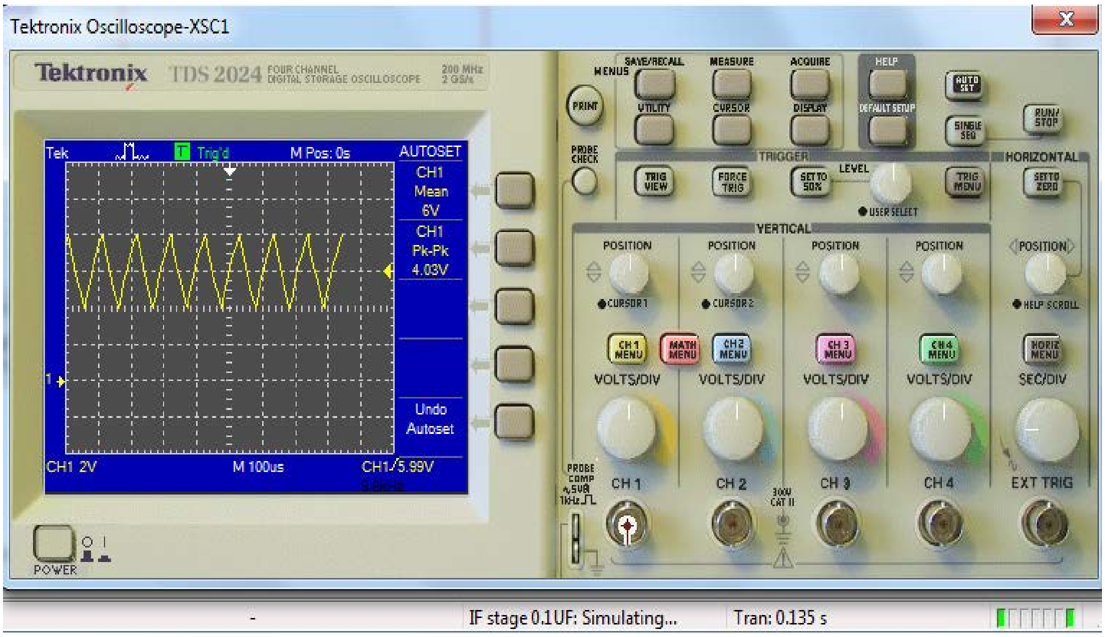
High time = 0.693(R1 +R2)*C     Low time = 0.693(R2*C)

As we require a 50% duty cycle (charging and discharge times to be equal) for this project, a diode is connected between the trigger and discharge input pins and making R1=R2. The timing capacitor will now charge up through R1 directly, this is because R1 is effectively shorted out by the diode but still discharges itself through R1. The duty cycle, D is expressed in this formula:

$$D = \frac{R1}{R1 + R2}$$

$$D = \frac{700}{700 + 700} = 0.5$$

In our project; we used resistor R1 = R2 = 700Ω with capacitor C = 0.1μF which gives an oscillating frequency of 6857Hz, with a duty cycle of 0.5 (50%). The output signal would be bounded from 4V (1/3Vcc) to 8V (2/3Vcc), the reason being that a +12V (Vcc) was applied. The output was then taking from the voltage on an external capacitor. The figure 3.1.5 below shows the simulation of the output.


Tektronix Oscilloscope-XSC1

Tek Trig'd M Pos: 0s

AUTOSET

CH1 Mean 6V

CH1 Pk-Pk 4.03V

Undo Autoset

CH1 2V M 100us CH1 ∕ 5.99V

IF stage 0.1UF: Simulating... Tran: 0.135 s

*Figure 3.1.5 Simulation Results of a Triangular Wave by a 555-timer*

**Noise Generator**

Noise is any random unwanted signal (electrical or electromagnetic) of different frequencies that degrades or corrupts our desired signal by changing its amplitude, phase or frequency. In order to achieve jamming, the jamming system needs some amount of noise or a certain type to noise to cover portions of the communications spectrum. The noise is mixed with the triangular wave signal to achieve this.

Without the noise generator, the jamming signal is just a sweeping un-modulated continuous radio frequency (RF) carrier wave or RF wave carrier. This noise helps in cloaking (masking) the jamming transmission, making it look like random noise.

The noise generator basically consists of three (3) parts: a zener diode, and two amplification stages. The noise in this case must be thermally generated, and that’s the reason for the zener diode because it has different characteristics from regular diodes. We used a/the zener diode operating in the reverse mode to produce this noise. In the reverse mode of operation, the diode causes what is termed avalanche effect, which causes wide band noise.

The avalanche effect (breakdown region or impact ionization) begins when the diode is applied with a high reverse voltage or current. Thermally generated minority carriers that acquire enough energy (kinetic energy) create an electron-hole pair through the collision with crystal atoms (other stable atomic structures). The free carriers created through this collision contribute to the reverse current and may also possess enough to participate in the collision creating further electron-hole pairs, these subsequent collisions leads to the avalanche effect (avalanche) or breakdown region.

The noise generated through the zener breakdown phenomenon (avalanche noise) is very similar to pink noise but much more intense and has a flat frequency spectrum (white), that is, it carries equal energy per frequency or spreads its power uniformly over specific spectrum (frequencies). The noise output power cannot be determined since it dependent on the diode's breakdown voltage and materials used.

In our designs we used a standard 6.8volts zener diode (1N5342B) with a 12volts power supply.

The noise output from the diode has a very low amplitude which would be  of no worth if mixed directly with the carrier signal, therefore to make it effective (the noise level) we amplify it to a level where the noise would be significant.

The noise amplification was done in two stages. In the first (1st) stage we used a common silicon NPN transistor(2N222) designed for use in the driver stage of audio frequency (AF) amplifier, small general purpose and low speed switching applications. The transistor is self-biased. Self-biasing refers to how the Q-point of the transistor is set. It refers, to the fact that negative-feedback is employed via a resistor connected between the collector and base of the transistor to set a stable DC operating point.

In the second stage we used an operational amplifier (op-amps) because they are perfect when you need to take a signal and have it go much higher than the original. Op-amps have high input impedance, very high voltage gain with low output impedance.

The LM386 audio amplifier is used at this stage. It's a versatile, small power amplifier designed for or requiring a low level power supply (low voltage applications). The internal gain is set to 20. Two pins (pin 1 and 8) are provided for gain control. Its gain however, can be set to any value from 20 to 200 with the addition of external capacitors and resistors between pins 1-8. The inputs are ground referenced and the output automatically biases to one half the supply voltage. The LM386 amplifier is acting as a natural band pass filter and small signal amplifier, thus, it does low pass filtering for the noise signal. The figure below (figure 3.1.6 & 3.1.7) shows the noise generator schematic and the output of the simulation.

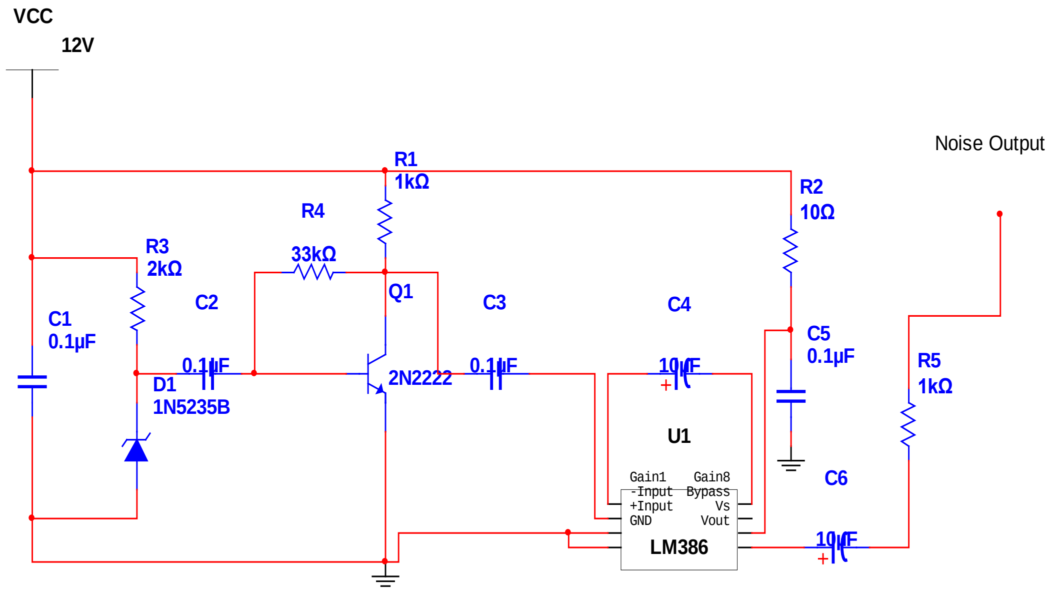
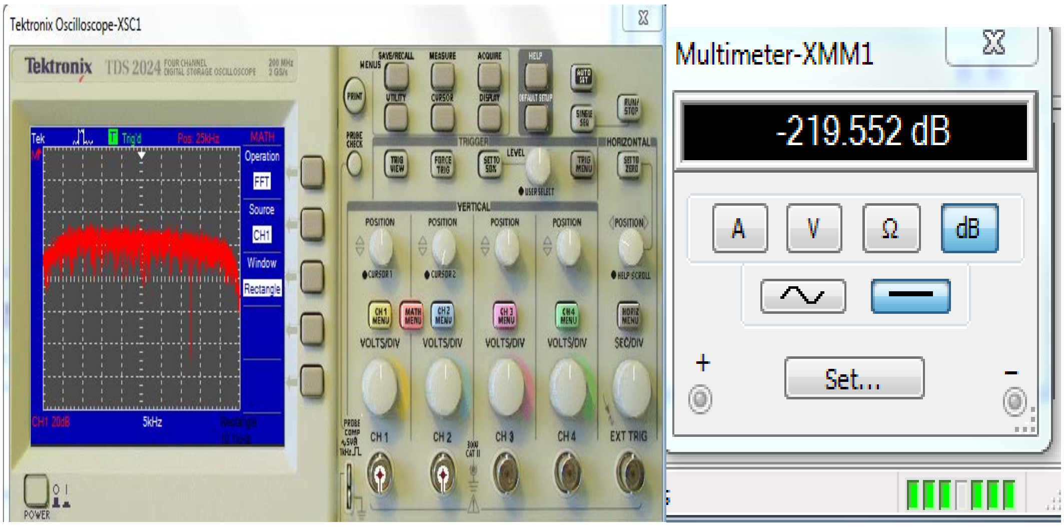


*Figure 3.1.6 Noise Generator Schematic (circuit diagram)*

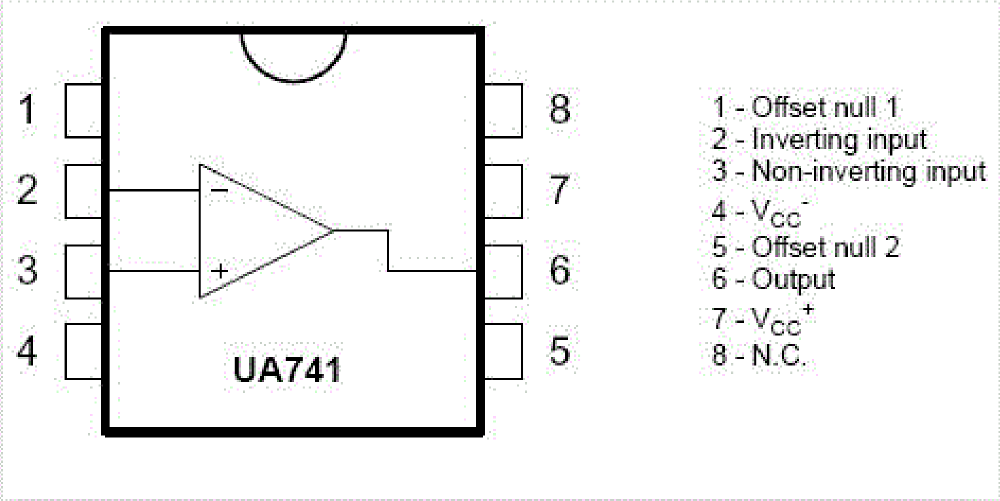


-219.552 dB

*Figure 3.1.7 Simulation of Noise Generator*

### Signal Mixer and Offset Circuit

The mixer here is an operational amplifier (op-amp) configured as a summer, so the noise and triangular wave are mixed to form a new “noisy” triangular wave form. When applied to the VCO, the resulting radio frequency (RF) signal will “sweep” across the cellular downlink frequencies, and will be frequency modulated (FM) with the noise signal. The UA741 which is an op-amp with; high gain, short-circuit protection, large input voltage range, no frequency compensation required, used with a spilt supply ( +/-), used with a feedback with gain determined by feedback network, is used at this stage for the mixing. +12V is given to the V+ (pin 7) and -12V to V- (pin 4). The non-inverting input (pin 3) is grounded and the output from the noise and triangular wave generators is/are connected to the inverting input (pin 2). The figure below shows the UA741 op-amp with its pin configuration



.

*Figure 3.1.8 UA741 Pin configurations (pin assignment)*

Another thing is to provide a DC offset (tuning voltage) for the VCO’s voltage tune pin. A clamper circuit (diode-clamper) is used to achieve this. The clamper consists of a capacitor connected in series with a resistor and a diode and it’s used at this stage to bind the input voltage to the VCO to a value between 0.3 to 4.5V. What this does is to give the triangular wave a positive DC voltage offset to help “centre” the wave within the required frequency range.

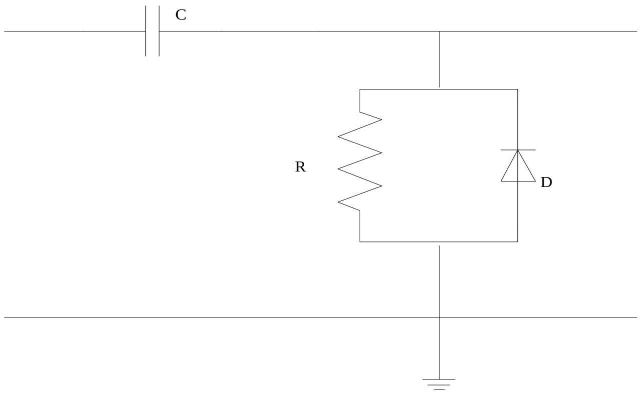


*Figure 3.1.9 Diode Clamper Circuit*

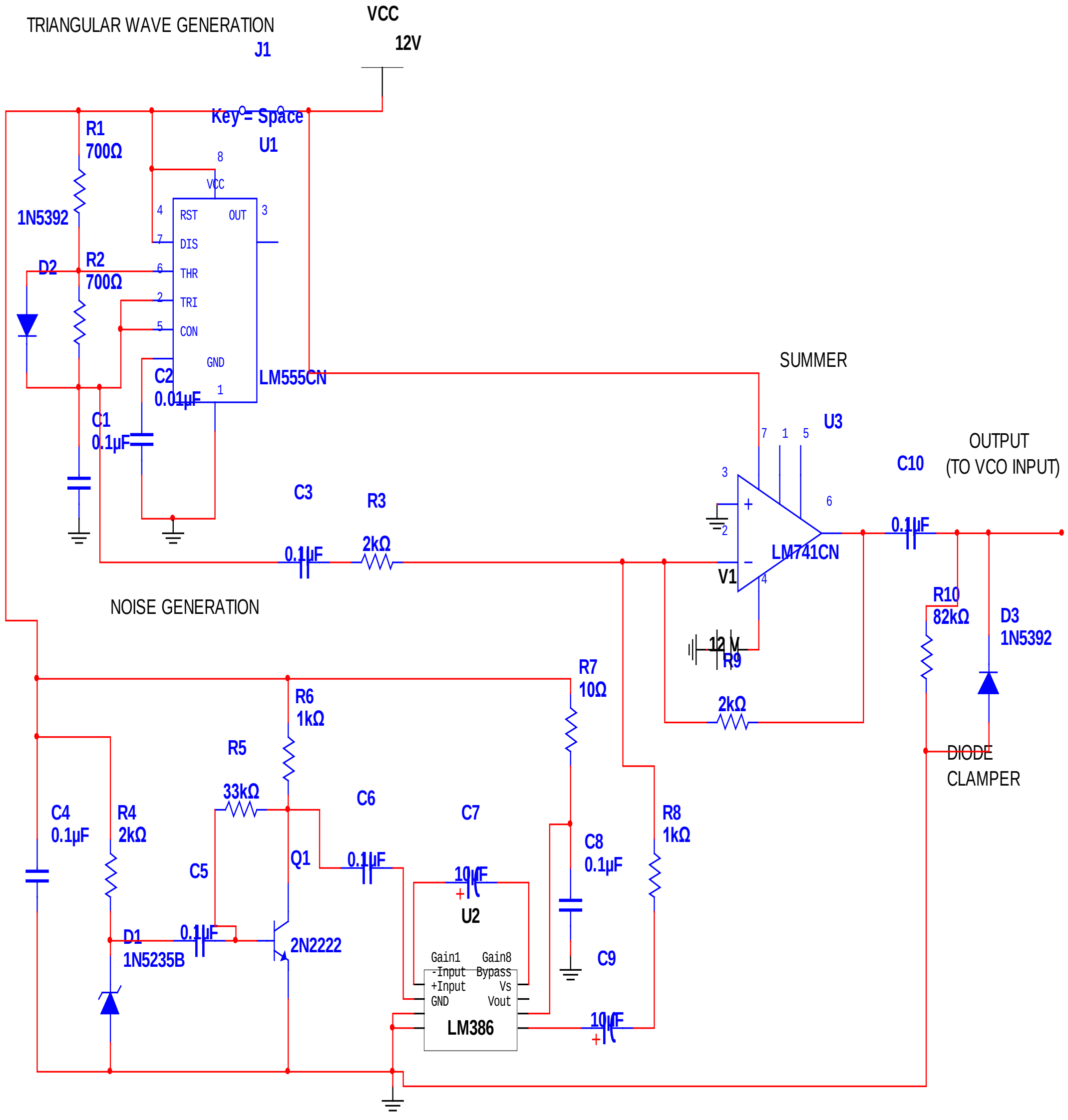


*Figure 3.2.0 Complete Schematic of the IF Section*

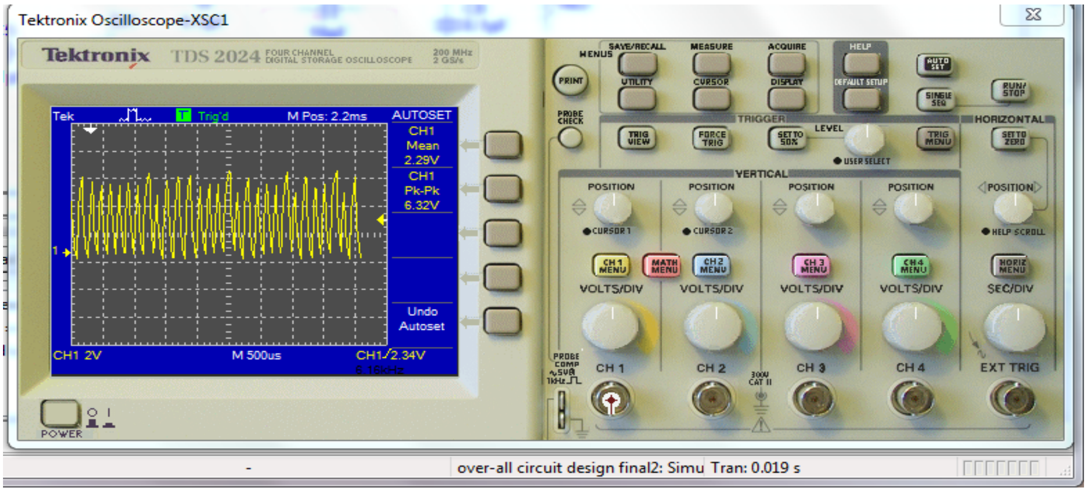


*Figure 3.2.1 Simulated Output for the Intermediate Frequency (IF) Section*

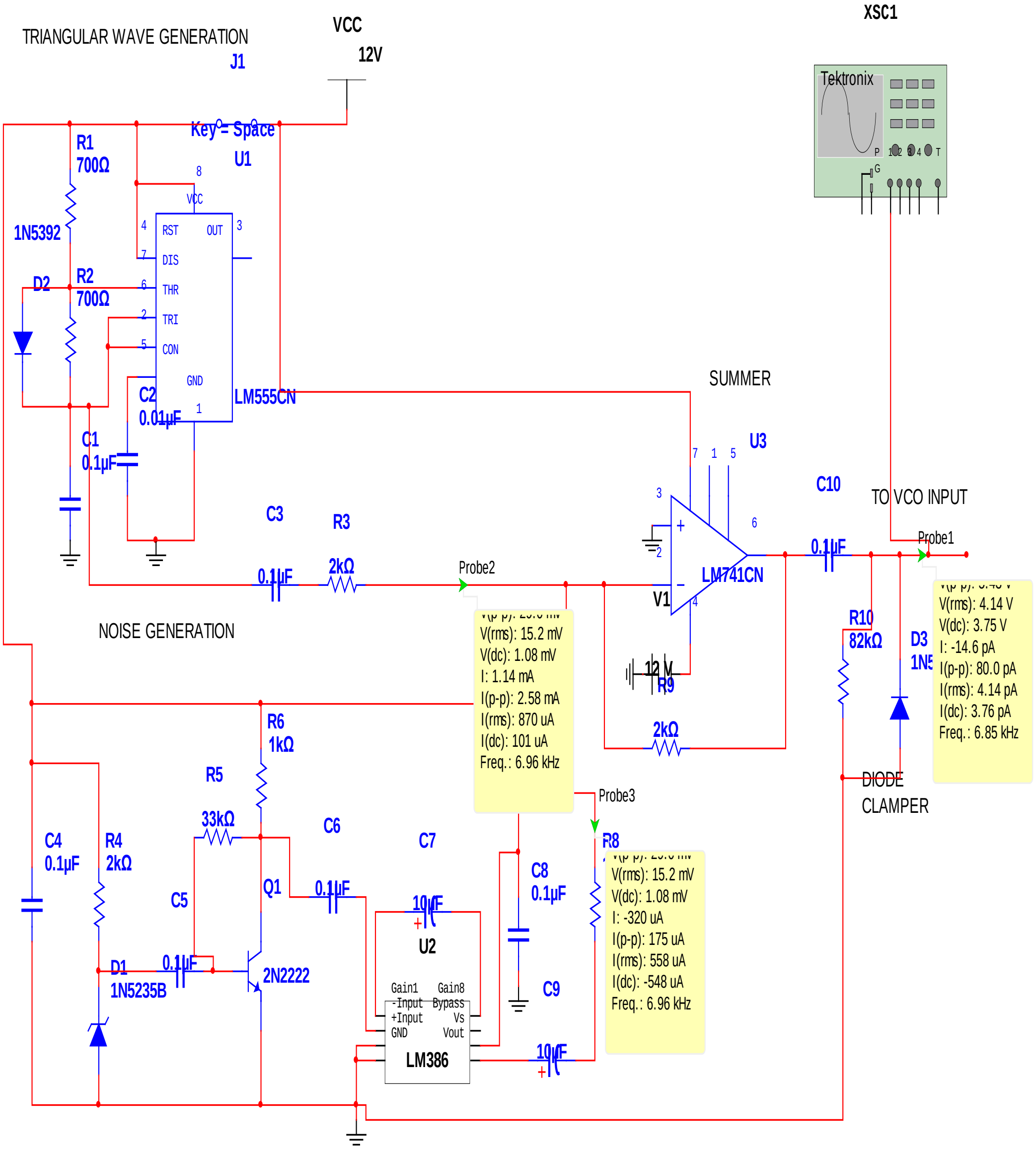


*Figure 3.2.2 Outputs from the various parts of the IF section*

### 3.3.3 Radio Frequency (RF) Section

The Radio Frequency (RF) section is the most important part of the jammer, since its output is what would interfere with the downlink frequency (mobile receive). It basically consists of;

1. Voltage Controlled Oscillator (VCO)
2. Radio Frequency (RF) Power Amplifier
3. Antenna(s)

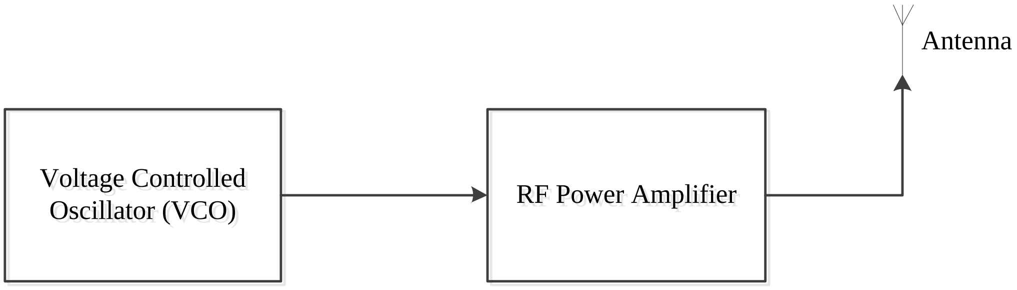


*Figure 3.2.3 Block Diagram of RF Section*

**Voltage Controlled Oscillator (VCO)**

The voltage controlled oscillator is the important component in the cellular jamming system. A VCO is an oscillating circuit or device whose output frequency changes in direct proportion to its voltage input or input voltage.

Every wireless device in use today has some sort of voltage controlled oscillator inside it, for example, there is at least one VCO inside every cell phone that generates RF waves that is used to communicate by-directionally to the cell tower (base station). The VCO here is responsible for generating an RF wave (signal) that will over power the mobile receive (downlink) signal.

The criteria for selection of the VCO for this project is influenced by; the frequency of the GSM system(s) to be jammed, its availability, cost and size, and lastly its control voltage and power consumption. The following VCOs were purchased and implemented in our circuit

CVCO55CL – 0925-0970 for GSM 900

CVCO55BE- 1785-1900 for GSM 1800

The VCO performance specifications:

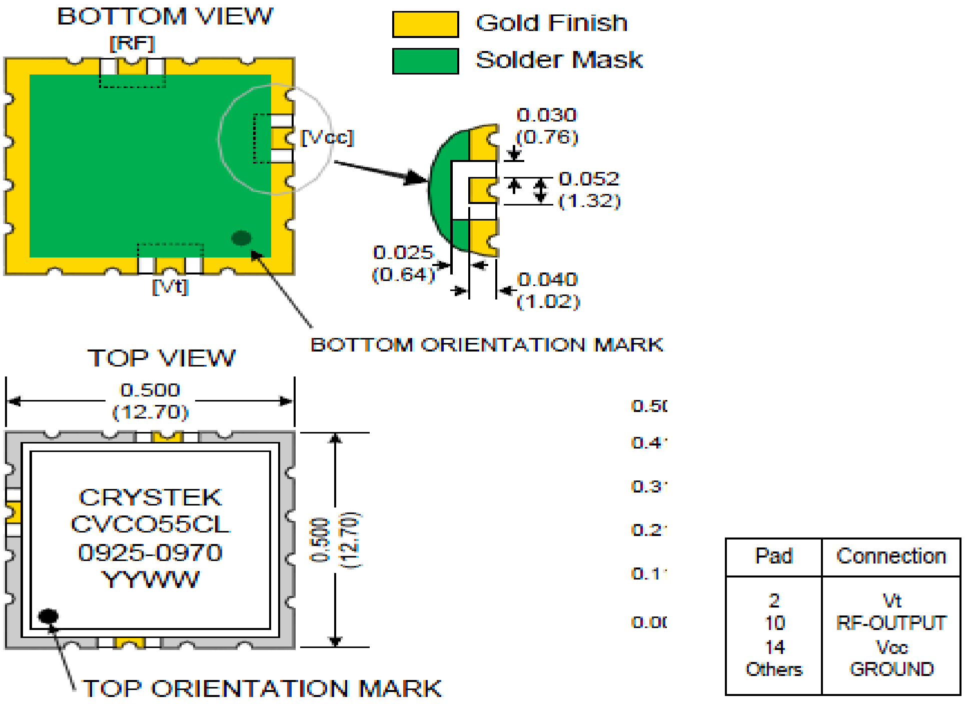
- CVCO55CL – 0925-0970

This VCO is used for GSM 900 with a mobile receive (downlink) frequency of 935-960MHz. According to its data sheet it has some of the following performance specifications.

| | |
|---|---|
| Frequency range | 925 – 970MHz |
| Tuning voltage | 0.5 – 4.5VDC |
| Supply voltage | 4.75 – 5.25VDC |
| Load impedance | 50Ω |

Its output power is 3.0dBm minimum, with 9.0dBm maximum but typically gives out 6.0dBm.

Below is the the top and bottom view of the CVCO55CL VCO;



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

*Figure 3.2.4 The top and bottom view of the CVCO55CL VCO*

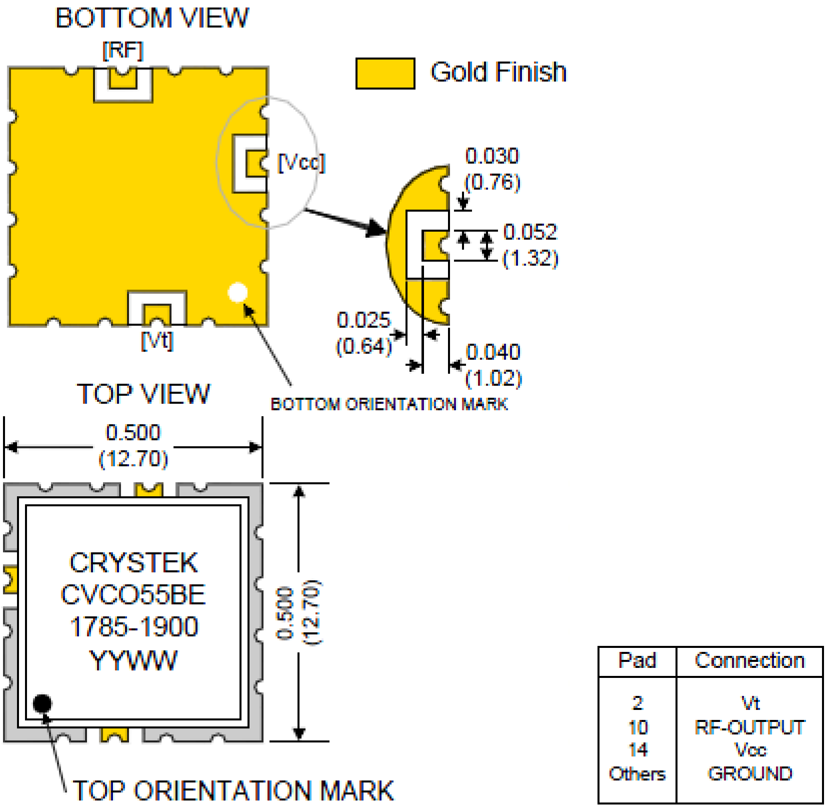
- CVCO55BE- 1785-1900

This VCO is used for GSM 1800 with a mobile receive (downlink) frequency of 1805-1880MHz. some of its performance specifications are;

| | |
|---|---|
| Frequency range | 1785 – 1900MHz |
| Tuning voltage | 0.3 – 4.7VDC |
| Supply Voltage | 4.75 – 5.25VDC |
| Load impedance | 50Ω |

Typical output power is 2.5dBm, with its maximum output (power) being 5.0dBm

Below is the the top and bottom view of the CVCO55BE VCO;



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

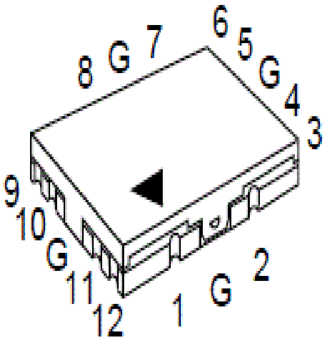
*Figure 3.2.5 The top and bottom view of the CVCO55BE VCO*

### RF Power Amplifier

An RF power amplifier is a type of electronic amplifier that is usually the final amplification stage in a device and it’s designed to give the desired (required) power output, that is, it converts a low-power radio frequency signal into a signal of significant power.

Since the output from the various VCOs does not achieve the desired output power of the GSM jammer, an RF power amplifier with a suitable gain is added at the output of each VCO to increase its output to that required Jamming power.

We used two (2) Renesas PF08109B power amplifiers at each output of the VCO in our design. The PF08109B can be used as a dual band Amplifier for E-GSM (880 MHz to 915 MHz) and DCS1800 (1710 MHz to 1785 MHz). It’s a 2in/2out dual band amplifier with high gain and efficiency. It has an output power 5W (approximately 37.0dBm) for GSM 900MHz and 3W (approximately 35.0dBm) for GSM 1800MHz. It comes at a low and can be found in most phones. Below is the pin arrangement for the PF08109B.



| Pin | Function |
|---|---|
| 1 | N/C |
| 2 | N/C |
| 3 | Pout DCS |
| 4 | Vdd DCS |
| 5 | Vdd GSM |
| 6 | Pout GSM |
| 7 | N/C |
| 8 | Vtxlo |
| 9 | Pin GSM |
| 10 | Vapc GSM |
| 11 | Vapc DCS |
| 12 | Pin DCS |
| G | GND |

*Figure 3.2.6 Pin arrangement of PF08109B Power Amplifier*

### Antenna

An antenna is a key component for wireless communications systems. It can be defined as a device that allows the coupling of a signal, i.e. RF from a guided medium into free space (transmitting) or from free space to a guided medium (receiving).

With reference to our project we employed an antenna to transmit the RF signals coming from the VCO through the power amps to free space. The choice or selection of an antenna is important to achieving our desired goal. Parameters such as the reflection coefficient, Voltage Standing Wave Ratio (VSWR), gain and directivity are factors one should consider in deciding an antenna to deploy for your device.

Our jammer requires two antennas operating simultaneously in the 900 and 1800 MHz frequency range. The specifications of both antennas are length; ¼ wavelength monopole, gain of 2dBi, Omni-directional, VSWR less than 2 and an input impedance of 50Ω.

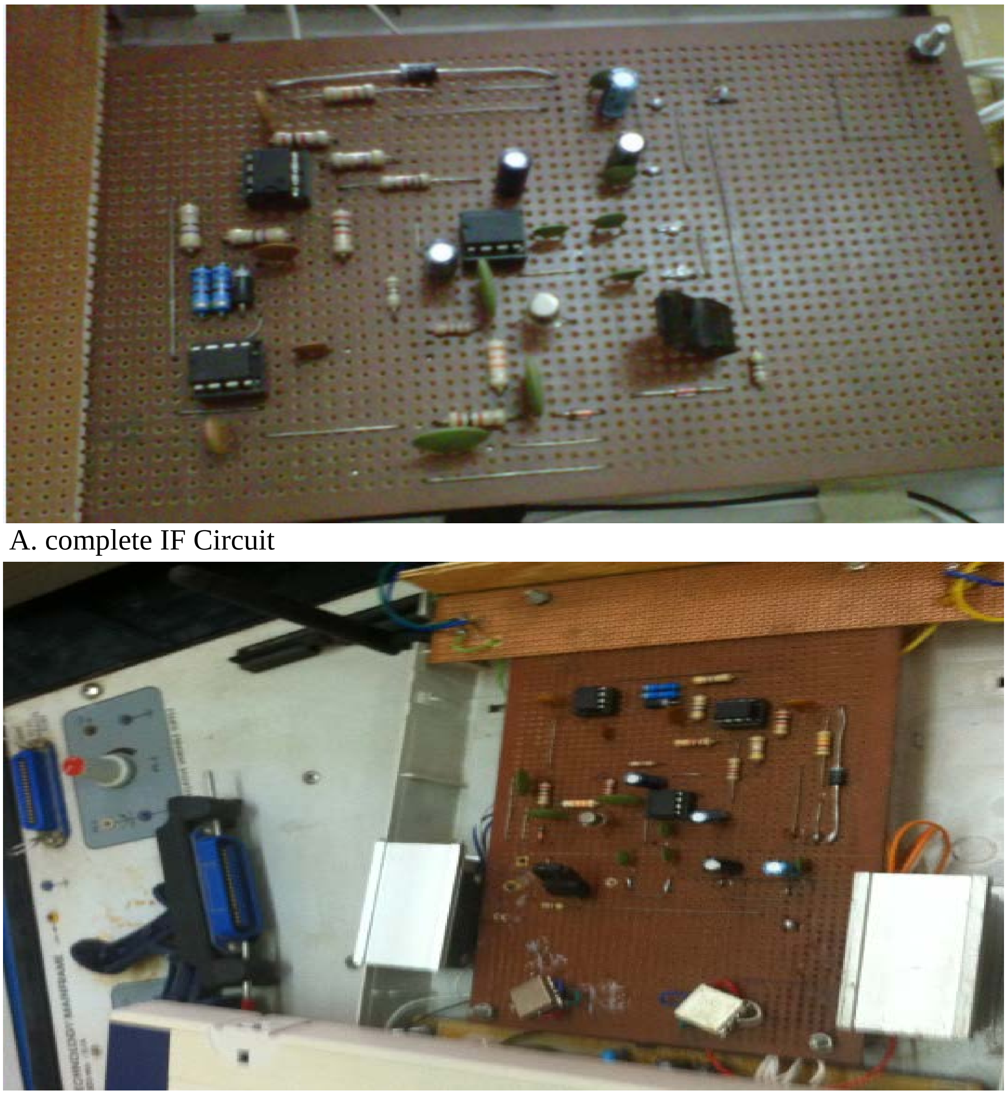
*Figure 3.2.6 A picture of the antenna*

# Chapter 4: - Results and Analysis

In this chapter we state the results of our work and also analyse the data and circuits we used in achieving our results.

## 4.1 Results

After the design and simulation of the schematics of our system, the schematics were transferred onto a breadboard for the various components to be fixed. The resultant circuit board and system is/are shown below



A. complete IF Circuit

B. Mobile Jammer System

*Figure 4.1 Pictures of Resultant Circuit Boards*

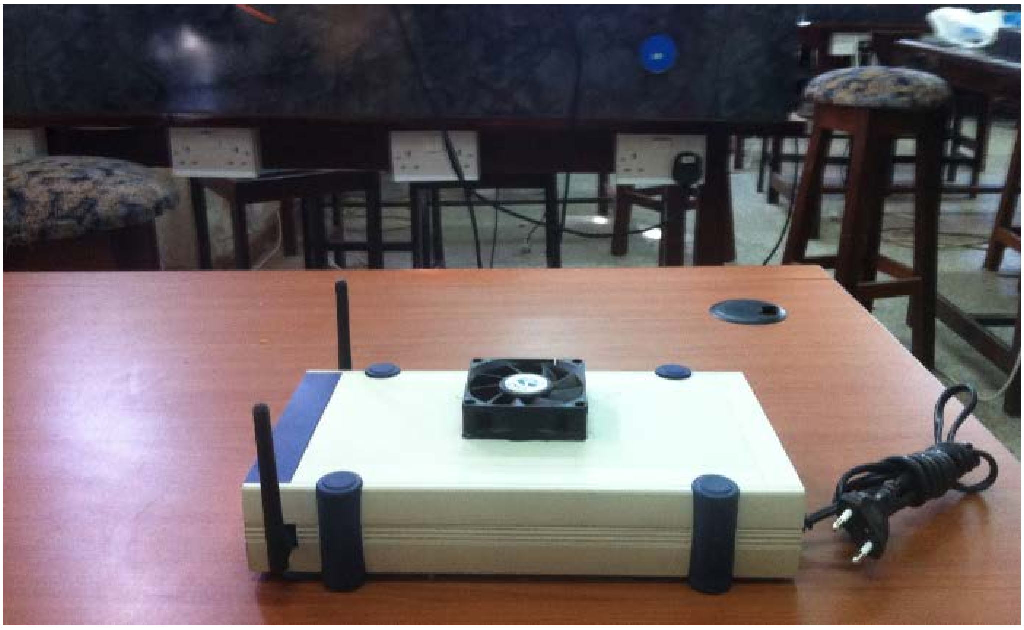


*Figure 4.2 Picture of our Mobile Jammer*

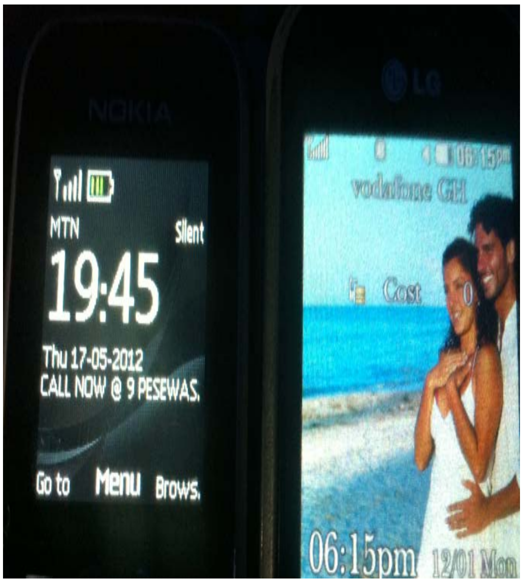
### 4.2 Results from Testing

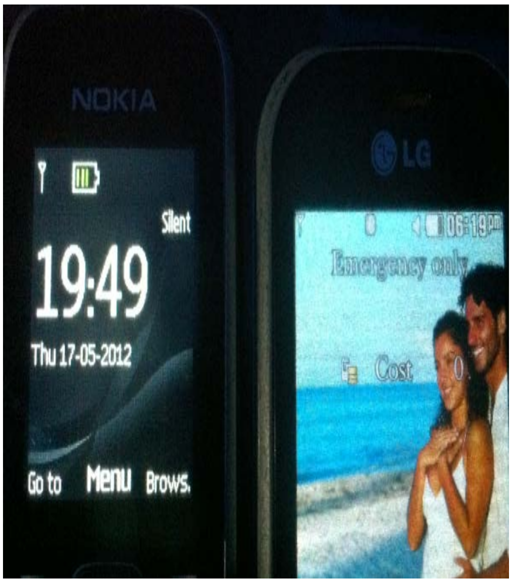
As we tested our jamming device, the result was a success. The device was able to jam all the mobile operators operating on the GSM 900 and 1800MHz systems/bands (Vodafone, MTN, Zain, Glo and Tigo). The figure below shows the results.

[1] MTN and Vodafone GH

Jammer “OFF”

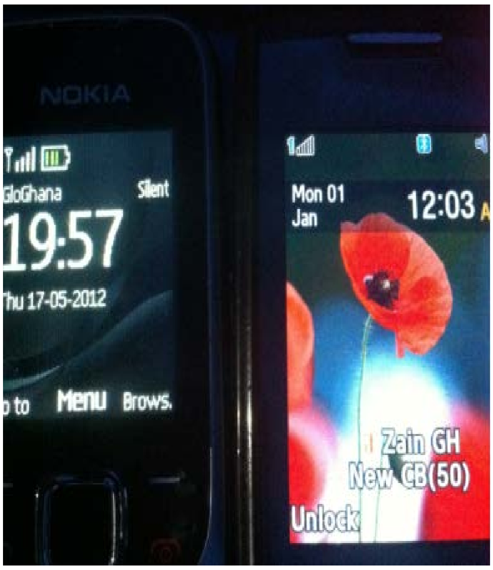
Jammer “ON”

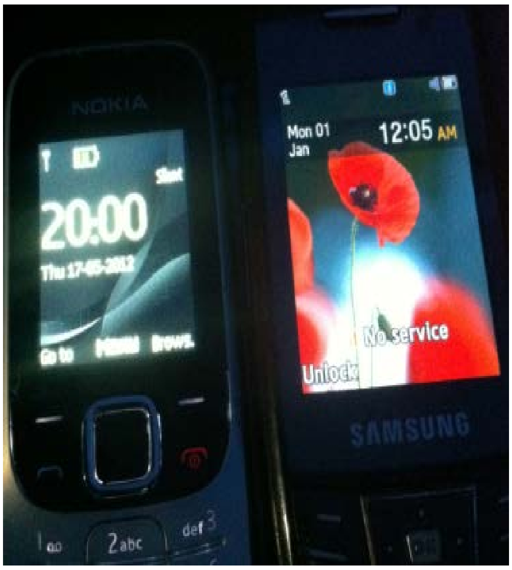




[2] Glo GH and Zain GH

Jammer “OFF” Jammer “ON”





[3] Tigo

Jammer “ON”

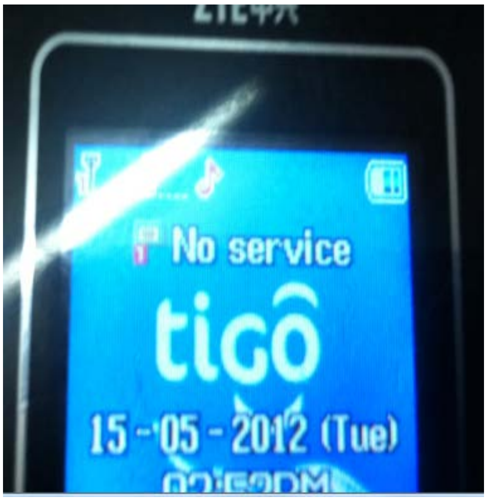


*Figure 4.3 Pictures (Results) from Testing of Jammer*

It can be seen clearly that the signal is “ON” when the jammer is “OFF”, whiles the signal disappears or the mobile phone displays “Emergency only”, “No Service” or “Limited service” when the jammer is “ON”.

### 4.3 Distance Jammed

*Table 4.0 Distance jammed*

| **Operator** | **System/Band (MHz)** | **Distance (m)** |
|---|---|---|
| MTN | 900/1800 | 11 |
| Vodafone GH | 900/1800 | 14 |
| Glo GH | 900/1800 | 13 |
| Zain (Airtel) GH | 900/1800 | 16 |
| Tigo | 900/1800 | 10 |

From the table, the average distance of jamming was 12.8m

During testing, we observed that the effective jammer distance varied. When tested close to a base station, we observed that the effective jamming distance was less and as we moved farther away from the base station (to a place where the base station is not too close) the effective area (jamming distance) increased. This is due to the fact that as we moved farther away base station, the amount of power reaching the cell phone from the base station decreases. Mobile 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.

We also noticed that with quad band and smart phones, the jammer could only work on them when the cellular area they are located in serves 900/1800MHz bands or when the Edge, 3G, etc. features are turned off. We observed that these phones tend to hop (frequency hopping). Frequency hopping is desirous for the following reasons:

1. If the level of transmitting power from the base station is low it searches for another with maximum power.

2. If there is interference on a frequency band or system, the mobile device searches for one without interference.

## 4.4 Simulated Results of Jammer (Output Waveform)

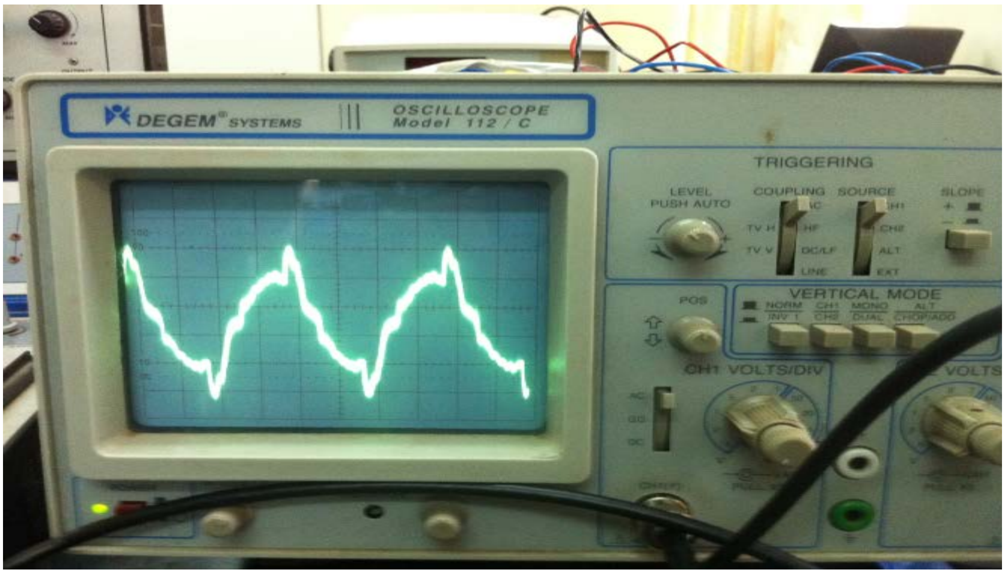
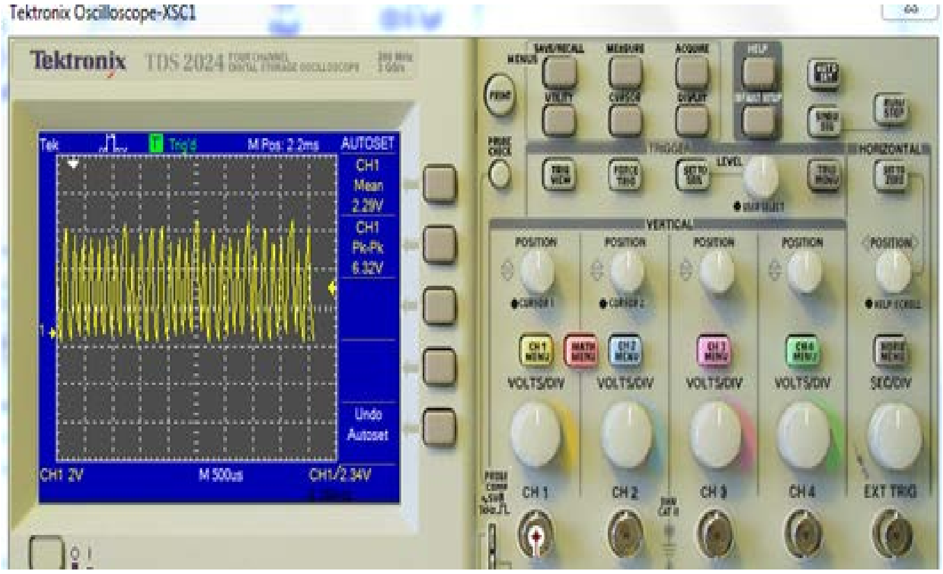


*Figure 4.4 Simulated Results of Jammer (Output waveform)*

The output waveform after the device was built can be compared to the simulation from the IF section (the noise mixed with the triangular wave). Here you can observe that the noise in the output is much more intense since it has gone through further amplification. Below is the simulated results from the IF section (chapter 3)


Tektronix Oscilloscope-XSC1

Tek Trig'd M Pos: 2.2ms

CH1 Mean 2.29V

CH1 Pk-Pk 6.32V

CH1 2V M 500us CH1 ∕ 2.34V

Figure 4.5 *Simulated Output for the Intermediate Frequency (IF) Section*

The choice of a power supply was very important to the success of our project. A power supply should deliver the right amount of steady current to the system. Also taking into consideration that voltages are not too stable, and fluctuate periodically in this country. It was important our power supply should be able to withstand these power fluctuations.

Our power supply was therefore taken from a DVD device and ranges from 85Vac to 260Vac. What we observed was that when the voltage levels dropped, it could still support the system

The power amplifiers we used caused some challenges. We found out that they heat minutes after turning on the device. This caused malfunctions of the device in general, as the power amplifier desolders from the circuit board. To resolve this, we added a heat sink to dissipate the heat, and provided a fan to help cool the amplifiers as well as the entire circuitry. It was realized after the introduction of the heat sink and fan that the device was performing better than previously.

# Chapter 5: - Conclusion and Recommendation

## 5.1 Conclusion

The decision to undertake this project was informed by the fact that with the growing use of mobile devices, there will be the need to regulate their use at some public places, hence the need for a way of preventing their use.

The objectives we set out to achieve were; to design, simulate, test and construct a mobile jammer and these have been met. The successful implementation of this project was largely due to certain precautions we took when understudying related works done. One major precaution we took was with finding an appropriate power supply for the device, since it was a challenge faced by the projects we understudied.

To conclude, we will like to state that we are delighted to have carried out this project and most importantly to have successfully completed it. This project has been of great academic experience for us.

## 5.2 Recommendation

The acceptance of mobile jammers worldwide is still up to date a controversial issue regarding its legality. Western countries are yet to make legal the use of jammers in public places. However it is allowed to be owned and used privately. The reason behind this debate is whether one has the right to prevent a user from having services from his/her phone in public. In Ghana however there is no clear cut policy about the use of jammers as they are not common. This project however is intended purely for academic purposes.

With the successfully completion of the project we would recommend that implementation of this project could be carried out in the places where they will be needed.

We also recommend that further works be carried on this project, since much improvements can be made to this current work. The following steps are some improvements that can be made to our jammer.

1. Constructing an intelligent jammer: intelligent jammers are jammers that come with a microprocessor that is capable of being programmed. An area of interest here is where the jammer could be made to first detect the presence of a mobile

phone before radiating the noise induced signals, as compared to ours that will keep transmitting whether there is a phone or not.

2. With the advances in technology, mobile systems are constantly evolving. The introduction of quad band phones as well as the introduction of 2.5G, 3G, 3.5G and 3.75G systems means that future construction of jammers will have to be operating in the frequencies assigned to these new systems. Consideration should also be given to CDMA systems.
3. As stated in chapter 2 of this project there are 6 different techniques to jamming and we have used one of them. We therefore recommend that the other techniques could also be carried out.

## References / Bibliography

[1] International Telecommunications Union, ITU-R (Radio communication Sector of ITU) Report ITU-R M.2243 (00/2011) “Assessment of the global mobile broadband deployments and forecasts for International Mobile Telecommunications”, pp. 4

[2] S.M.K .Chaitanya, P. Naga Raju, Y.N.V.L. Ayyappa, Vundavalli Ravindra “International Journal of Computer Science and Telecommunications” [Volume 2, Issue 5, September 2011].

[3] GSM Frequencies and Frequency Bands [online], Available: http://www.radio-electronics.com/info/cellulartelecomms/gsm_technical/gsm-frequency-frequencies-bands-allocations.php [Accessed: 22nd October 2011].

[4] Ian Poole, “Cellular Communications Explained From Basics to 3G”, 2006, pp. 5-12

[5] Siegmund M. Redl, Matthias K. Weber, Malcolm W. Oliphant, “GSM and Personal Communications Handbook”, pp. 67

[6] The GSM system [online], Available: http://flylib.com/books/en/1.151.1.10/1/ [Accessed: 22nd October 2011].

[7] Services Provided by GSM [online], Available: http://www.privateline.com/mt_gsmhistory/ [Accessed: 23rd November, 2011]

[8] Definition of Frequency Band [online], Available: http://www.mobileburn.com/definition.jsp?term=frequency+band [Accessed: 23rd November, 2011].

[9] Gunnar Heine, “GSM Networks: Protocols, Terminology and Implementation”, pp. 2-3

[10] Rimantas Pleikys, “Radio Jamming in the Soviet Union, Poland and other East European Countries”, 2006.

[11] Abhinav Gaur, “Radio Jamming: Feeling the Interference”, September 2010.

[12] Mobile & Personal Communications Committee of the Radio Advisory Board of Canada, "Use of jammer and disabler Devices for blocking PCS, Cellular & Related Services" [online], Available: http://www.rabc.ottawa.on.ca/e/Files/01pub3.pdf [Accessed: 16/11/2011]

[13] National Communications Authority, "Broadband Wireless Access (BWA) Licenses in the 2500MHz – 2690MHz Band", March 2010, pp. 3

[14] Basic Multiple Access Schemes In Cellular Systems [online], Available: http://www.radio-electronics.com/info/cellulartelecomms/cellular_concepts/multiple_access_schemes.php [Accessed: 22nd October 2011]

[15] Varun Taliyan, "CDMA VS GSM", 2006 – 2009, pp.27-34

[16] Mobile Phone Systems Overview [online], Available: http://www.radio-electronics.com/info/cellulartelecomms/systems/mobile-overview.php [Accessed: 9th May, 2012]

[17] Ian Poole, "Cellular Communications Explained From Basics to 3G", 2006, pp. 83

[18] Technical Specification GSM 05.05 version 5.0.0. ETSI, March 1996, pp.9-11

[19] Lawrence Harte and David Bowler, "Introduction to Mobile Telephone Systems: 1G, 2G, 2.5G, and 3G Wireless Technologies and Services", Althos Publishing, ISBN: 0-9746943-2-0

[20] Simplified GSM Network Architecture [online], Available: http://www.radio-electronics.com/info/cellulartelecomms/gsm_technical/gsm_architecture.php [Accessed: 17th May, 2012]

Ahmed Jisrawi, "GSM-900 Mobile Jammer", 2006.

Adeyemi Bayode Victor, Filson Kwadwo Banful and Tebe Ifede Parfait, "Design and Construct a Frequency Jamming Device for Mobile Networks", 2011.

Balal Ansar, Bilal Tariq and Faisal Mehmood Ahmed, "Mobile Service Denial", 2009.

Syed Absar Ahmed Shah, Syed Ali Wajahat Jafri and Sohaib Zafar, “GSM Jammer”, 2006.

# Appendix

## Data Sheets

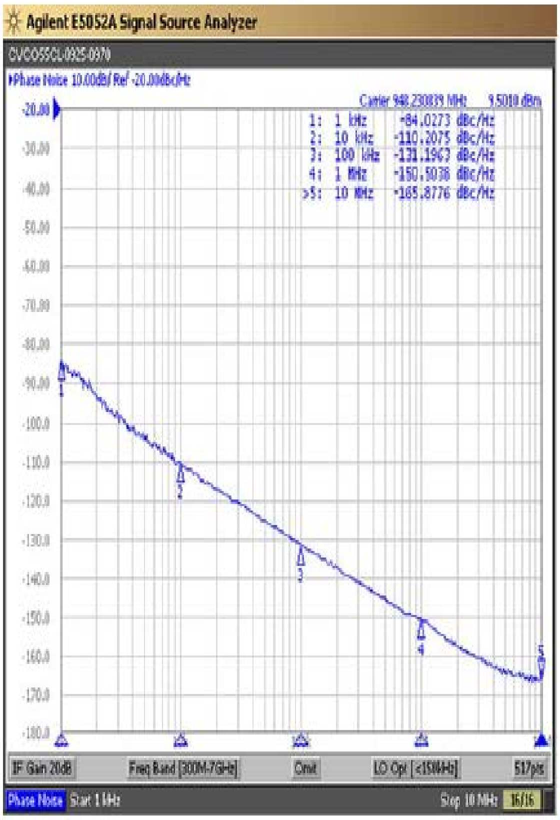
CRYSTEK MICROWAVE
A DIVISION OF CRYSTEK CORPORATION

Voltage Controlled Oscillator-VCO
CVCO55CL-0925-0970

| PERFORMANCE SPECIFICATION | MIN | TYP | MAX | UNITS |
|---|---|---|---|---|
| Lower Frequency: | | | 925 | MHz |
| Upper Frequency: | 970 | | | MHz |
| Tuning Voltage: | 0.5 | | 4.5 | VDC |
| Supply Voltage: | 4.75 | 5.0 | 5.25 | VDC |
| Output Power: | +3.0 | +6.0 | +9.0 | dBm |
| Supply Current: | | | 30 | mA |
| Harmonic Suppression (2nd Harmonic): | | -15 | -10 | dBc |
| Pushing: | | | 1.7 | MHz/V |
| Pulling, all Phases: | | | 4.4 | MHz pk-pk |
| Tuning Sensitivity: | | 13 | | MHz/V |
| Phase Noise @ 10kHz offset: | | -108 | | dBc/Hz |
| Phase Noise @ 100kHz offset: | | -128 | | dBc/Hz |
| Load Impedance: | | 50 | | Ω |
| Input Capacitance: | | | 50 | pF |
| Operating Temperature Range: | -40 | | +85 | °C |
| Storage Temperature Range: | -45 | | +90 | °C |

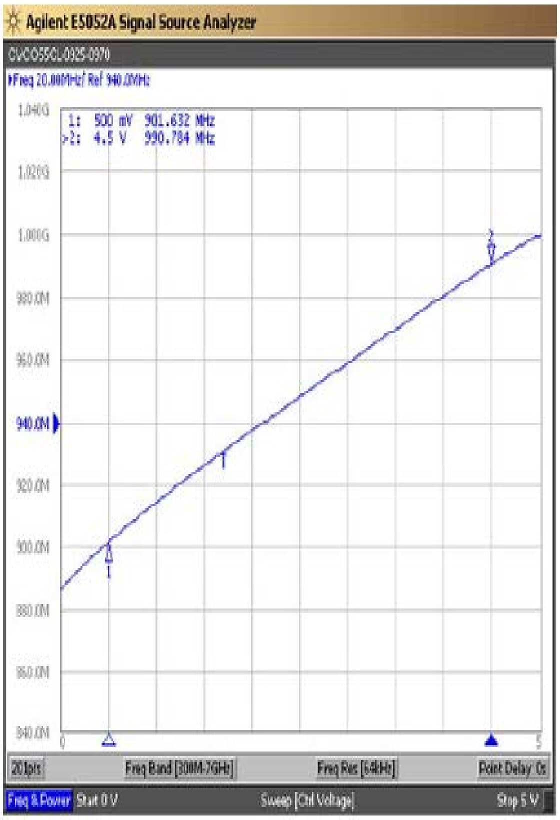
RoHS Compliant

### Phase Noise (1 Hz BW, Typical)



```
Carrier 948.230839 MHz     9.5010 dBm
  1:  1 kHz     -84.0273 dBc/Hz
  2:  10 kHz   -110.2075 dBc/Hz
  3:  100 kHz  -131.1963 dBc/Hz
  4:  1 MHz    -150.5036 dBc/Hz
 >5:  10 MHz   -165.8776 dBc/Hz
```

### Tuning Curve (Typical)



```
 1:  500 mV  901.632 MHz
>2:  4.5 V   990.784 MHz
```

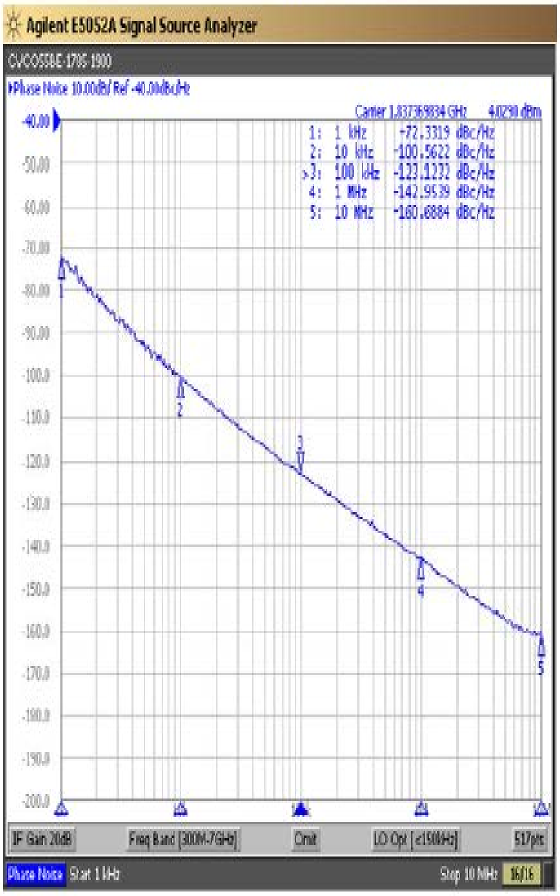
CRYSTEK MICROWAVE
A DIVISION OF CRYSTEK CORPORATION

# Voltage Controlled Oscillator-VCO
# CVCO55BE-1785-1900

RoHS Compliant

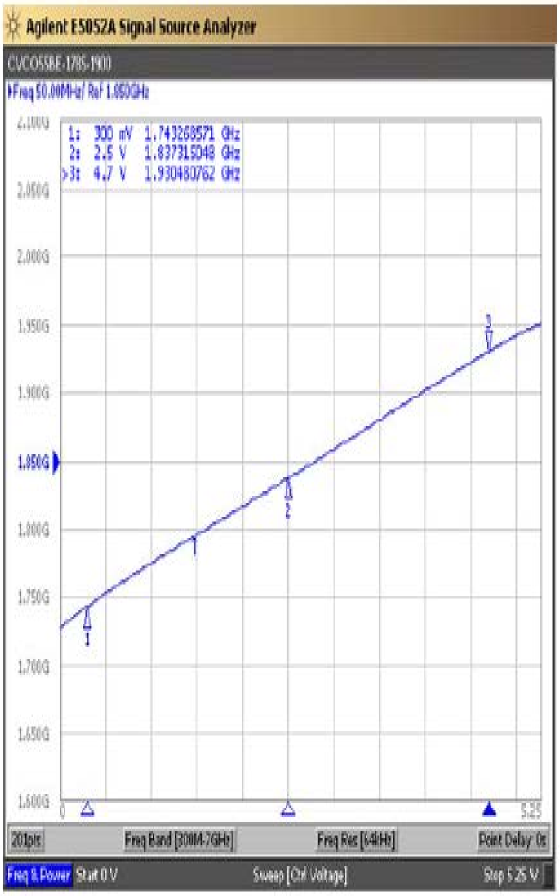
| PERFORMANCE SPECIFICATION | MIN | TYP | MAX | UNITS |
|---|---|---|---|---|
| Lower Frequency: | | | 1785 | MHz |
| Upper Frequency: | 1900 | | | MHz |
| Tuning Voltage: | 0.3 | | 4.7 | VDC |
| Supply Voltage: | 4.75 | 5.0 | 5.25 | VDC |
| Output Power: | 0 | +2.5 | +5.0 | dBm |
| Supply Current: | | | 35 | mA |
| Harmonic Suppression (2nd Harmonic): | | -15 | | dBc |
| Pushing: | | | 2.0 | MHz/V |
| Pulling, all Phases: | | | 3.0 | MHz pk-pk |
| Tuning Sensitivity: | | 45 | | MHz/V |
| Phase Noise @ 10kHz offset: | | -100 | | dBc/Hz |
| Phase Noise @ 100kHz offset: | | -122 | | dBc/Hz |
| Load Impedance: | | 50 | | Ω |
| Input Capacitance: | | | 50 | pF |
| Operating Temperature Range: | -40 | | +85 | °C |
| Storage Temperature Range: | -45 | | +90 | °C |

## Phase Noise (1 Hz BW, Typical)



```
  1:  1 kHz     -72.3319 dBc/Hz
  2:  10 kHz   -100.5622 dBc/Hz
>3:  100 kHz  -123.1232 dBc/Hz
  4:  1 MHz    -142.9539 dBc/Hz
  5:  10 MHz   -160.6884 dBc/Hz
```

## Tuning Curve (Typical)



```
 1:  300 mV  1.743268571 GHz
 2:  2.5 V   1.837315048 GHz
>3:  4.7 V   1.930480762 GHz
```

## Bill of Materials

| **Reference** | **Description** | **Quantity** | **Price (GH¢)** |
|---|---|---|---|
| AN1897 (VIPer22A) | Power Supply | 1 | 28.90 |
| LM555CN | 555-timer | 1 | 1.50 |
| LM741CN | Operational Amplifier | 1 | 1.00 |
| LM386 | Audio Amplifier | 1 | 1.00 |
| 2N222 | Transistor | 1 | 0.70 |
| CVCO55CL(0925-0970) | RF Power Amplifier | 1 | 43.01 |
| CVCO55BE(1785-1900) | RF Power Amplifier | 1 | 44.132 |
| D1 | Zener Diode | 1 | 1.00 |
| C7, C9 | Electrolytic Capacitor | 2 | 0.20 |
| D2, D3 | Diode | 2 | 0.20 |
| PF08109B | RF Power Amplifier | 2 | 7.684 |
| C1, C2, C3, C4, C5, C6, C8, C10 | Ceramic Capacitor | 8 | 1.60 |
| R1 to R9 | Resistor | 9 | 0.90 |
|  |  |  | **Total:**<br>135.668 |

**certain components were shipped due to their unavailability on the local market. The cost of shipment and money transfer (for payment) totalled approximately Gh¢512.858*