DESIGN AND CONSTRUCTION OF A SIMPLE GSM SIGNAL JAMMER

BY

SHOBAYO OLAMILEKAN SAHEED

(2007/2/26407EE)

A Project submitted to the Department of Electrical and Electronics Engineering in partial fulfillment of the requirement for the award of Bachelor of Engineering degree (B.Eng) in Electrical/Electronics Engineering, Federal University of Technology, Minna, Niger State, Nigeria.

November, 2011.

DECLARATION

I,SHOBAYO OLAMILEKAN SAHEED, declare that this work was done by me and has never been presented elsewhere for the award of a degree. I also hereby relinquish the copyright to Federal University of Technology, Minna.

Shobayo Olamilekan Saheed
(Student)

Saheed 09/11/2011
....
Signature and Date

CERTIFICATION

This is to certify that this project titled "Design and Construction of a Simple GSM Signal Jammer" was carried out by Shobayo Olamilekan Saheed, with matriculation number 2007/2/26407EE, and submitted to the Department of Electrical and Electronics Engineering, Federal university of Technology, Minna. in partial fulfillment of the requirement for the award of Bachelor degree in Engineering (B.Eng).

Mr. Agbachi Eugene Okenna
(Project Supervisor)

....
Signature and Date

Engr. A.G. Raji
(Head of Department)

....
Signature and Date

(External Examiner)

....
Signature and Date

DEDICATION

This project is dedicated to the memory of a dear friend, late Mr Olotu Benson Ochuko, who also had the intention of taking up this project but never lived to complete it.

ACKNOWLEDGEMENT

Iam grateful to God Almighty for his grace and protection.My sincere gratitude goes to the H.O.D of my department Engr. Raji and all my lecturers for their support in my academic pursuit.My gratitude to my supervisor and co-supervisor Mr. Agbachi Eugene Okenna and Mallam. Abdulahhi Umar for their guidance and constructive criticism through the period of this project.

This project would not have been possible, without the confidence, endurance and support from my mother Mrs.Ramota Omoladun Shobayo, Also to all my friends and colleagues for their wonderful contributions.

ABSTRACT

The GSM mobile phone jammer is a device that is used to block or interfere with frequency of a transmitting device. Mobile phone signal jammer is used to interfere with the communicationfrequency withina specific radius depending on the strength of the signal jammer. This is achieved by generating and transmitting radio signal on the same frequency as the base station of the mobile phone network provider and at high power so as to collide and cancel each other out. The artistry used in designing this project is a systematic combination of analog components which includesresistors, capacitors, transistors and inductors to generate the frequency (Noise) needed and then amplified to increase the transmitted power. The generated frequency will be about 860MHz to 1.9GHz in order to match the frequency of the serving base station. The jamming process is successful if a mobile phone within the perimeter of the jammer has its network disable. This is confirmed by the inability to make and receive calls or to send or receive SMS. The mobile phone jammer helps within some specific area where the distraction caused by mobile phone is highly undesirable.

TABLE OF CONTENT

Pages

Chapter One: Introduction

Chapter Two: Literature Review

Chapter Three: Design and Implementation

Chapter Four: Test, Result and Discussion

LIST OF FIGURES

CHAPTER ONE

1.1INTRODUCTION

A Global System of Mobile communications (GSM) jammer also known as phone breaker is designed to block communication between mobile phones and cellular base station, without interfering with other communication systems. It is a device that transmit signal on the same frequency at which the GSM system operates, the jamming is said to be a success when the GSM phones in the area where the jammer is located are disabled. [1]

Communication jamming device was first developed and used by the military, whereby tactical commanders use Radio Frequency device (RF) communications to exercise control over their forces. [1].An enemy can abrupt this conversation if he has in his custody a mobile phone jammer. This interest comes from fundamental area of successful transport of information from sender to receiver.

Nowadays the mobile jammer are becoming civilian products rather than military warfare device, since with the increasing number of mobile phone users the need to disable phones in some places where the ringing of GSM phones would be disruptive has increased. This place include worship places, lecture rooms of higher institutions, libraries, concert halls, meeting rooms and other places where silence is appreciated.The jammer transmits a signal that radiates electromagnetic waves in all direction (for an omnidirectional antenna which is usually installed in them). This small signal reaches all receivers within the area of its effective range which is about 6meters in radius and swamp the receiver in that area.It is also worth noting that the transmitters from the GSM base station transmit the signal frequency at a very high power up to several kilowatts (Kw) to the GSM towers which then also transmits to the receiver of the mobile phone in that particular area but because the distance to be covered by the travelling signal is large, before it gets to the receiver the power would have been reduced which gives an advantage to our relatively low power signal jammer to be able to at least jam the signal to cover more appreciable range.[1]

1.2 OBJECTIVES

- It is aimed at disenabling the initiation of calls or SMS messages.
- It is also aimed at disenabling the receiving of calls or SMS messages.
- To disenable the communication between mobile phone and base station.
- It is also aimed at disconnecting all calls upon entering a covered area.
- To also serve as a device against bugging.

1.3STATEMENT OF PROBLEM / JUSTIFICATION

The GSM signal jammer is justified in the sense that it is targeted at different applications such as:

- Preventing acoustic noise caused by mobile phone ring or conversations. Acoustics in this regard means any sound that comes out from discussion on mobile phones. The area of applications of this device i.e. the signal jammer or GSM breaker to silence GSM phones includes: Theaters, Cinemas, Schools, Libraries, Concert halls, Studios, Meeting rooms, Restaurants, Religious places, Universities and finally Courts.
- Minimizing hazards of interference to sensitive equipment through handset or mobile phone or GSM transmission. Transmission in this case refers to electromagnetic waves being transmitted by the device. The device can then be employed for safety purposes in

places where safety to the transmission of electromagnetic waves is of paramount importance. The safety markets for the mobile phone jammer includes: Hospitals and Medical clinics, Airports and Vehicle Computer Rooms, Laboratories and finally petrol stations.

- Enforcing policy due to security concerns. This regards to proffering some form of security policies in some particular places and establishments. These strategic places or establishments include:Police forces, Bomb squads, Banks, Embassies, Prisons, Anti-terrorist units, Gaming Facilities.

1.4 METHODOLOGY

Jamming devices overpower the GSM phone signal by transmitting a signal on the same frequency as the cell phone and at a high enough power that the two signal collides and cancels each other out. GSM phones are designed to add power if they experience low level interference, so the jammer must recognize and match the power increase from the phone. GSM phone are full duplex devices i.e. they communicate in two ways simultaneously from the sender to the receiver which implies that they use two different frequencies, one for talking and one for listening simultaneously. Some jammers block only one of the frequencies used by the cell phones, which has the effect of blocking both. The phone is tricked into thinking there is no service because it can receive only one of the frequencies. Less complex devices block only one group of frequencies, while sophisticated jammers can block several type of at once to head off dual-mode or tri-mode phones that automatically switch among different network type to find an open signal. Some of the high end-devices block all frequencies at once and others can be tuned to specific frequencies. To jam a GSM signal, all that is needed is a device that will broadcast on the correct frequencies. Although different cellular systems process signals differently, all GSM phone network uses radio signals that can be interrupted. GSM, used in digital cellular and PCS-based system, operates in the 900-MHz and 1800-MHz bands in Europe and Asia and in the 1900-MHz(sometimes referred to as 1.9-GHz) band in the United States. Jammers can broadcast on any frequency and is effective against CDMA, FDMA, GSM, PCS and Nextel systems. Old-fashioned analogue cell phones and today's digital devices are susceptible to jamming.

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

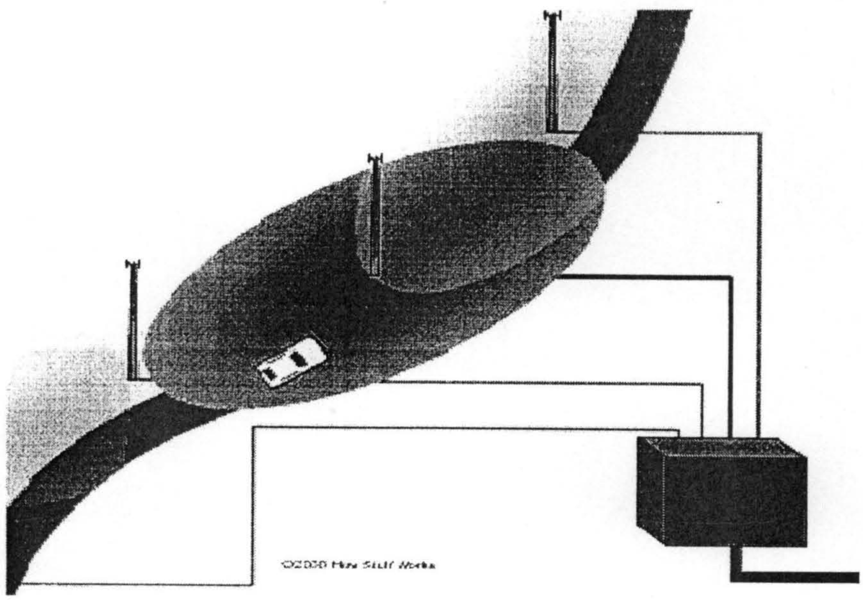


Fig 1.1 Illustration of GSM Signal Reception

A jamming device transmits at the same frequency as the cell phone, disrupting communication between the GSM phone and the base station in the town. This is illustrated in the picture below.

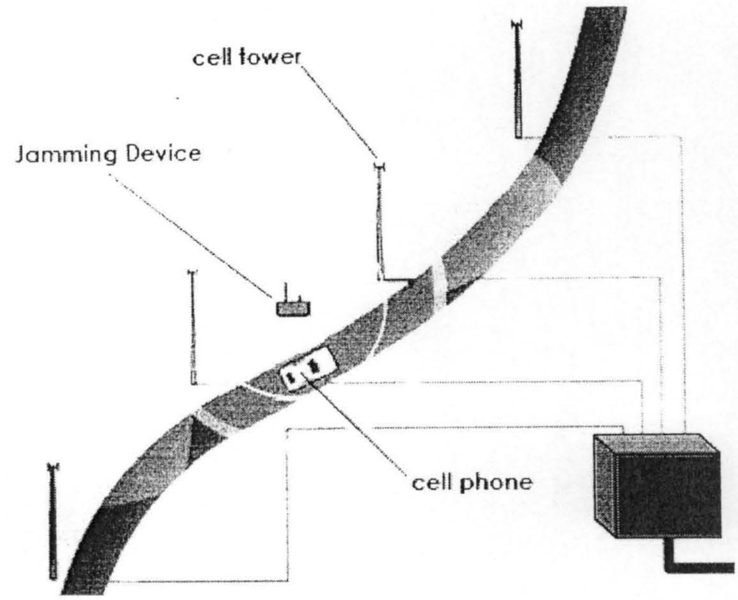


Fig 1.2Jamming Process Illustration

The jamming process is called a **denial-of-serviceattack.** The jammer denies the service of the radio spectrum to the GSM phone users within the range of the jamming device. Older jammers sometimes were limited to working on phones using only analogue or digital mobile phone standards. Newer models such as the double and triple band jammers can block all widely used systems and even very effective against newer phones which hops to different frequencies and systems when interfered with. As dominant network technology and frequencies used for mobile phones worldwide varies, some work only in specific regions such as Europe or North America.

The power of the jammer's effect can vary widely based on factors such as proximity to towers, indoor and outdoor settings, presence of building and landscape, even temperature and humidity play a role. There are concerns that crudely designed jammers can disrupt the functioning of medical devices such as peacemakers. However, like GSM phones, most of the devices in common use operates at low enough power output (<1W) to avoid causing any problems. [1]

This project is achieved through the intelligent combinations of simple electronic components such as resistors, transistors, capacitors and inductors. The resistor is used to regulate the amount of voltage and current going into the transistor. The capacitor in conjunction with the inductor forms the tank circuit which is the major oscillator or frequency generator sub circuit in the project circuit diagram. Some capacitor in the circuit diagram acts as a filter.

CHAPTER TWO

2.1LITERATURE REVIEW

Mobile phone jammer is an instrument used to prevent Mobile phone or cellular phones from receiving signals from a Base station. When used, the jammer effectively disables cellular phones. These devices can be used in practically any location, but are found primarily in places where a phone call would be particularly disruptive because silence is expected. Older jammers, i.e. electronic devices that are used to interfere with Radio Frequencies (RF) are mainly targeted at Radio and TV signals. Nowadays due to the advent of GSM mobile phones that also uses Electromagnetic waves, GSM mobile phone jammers has also been developed. In the past GSM jammers produced are relatively expensive based on the sophistication in its production with the use of several sophisticated electronics components such as the programmed Microcontroller, Oscillators, high quality Mixers and a very complex Transmitters all coming at a very exuberant prices. However this system was reviewed and a GSM signal jammer that is made from the simple combination of both active and passive components like transistors, inductors, capacitors and the resistors alike, giving rise to an effective GSM signal jammer and that also come at a cheaper price with a less complex circuitry was feasible, and hence adopted.

2.2HISTORICALBACKGROUND

The rapid proliferation of cell phones at the beginning of the 21st century to near ubiquitous status eventually raised problems such as their potential use to invade privacy or contribute to rampant and egregious academic cheating. In addition public backlash was growing against the intrusive disruption cell phones introduced in daily life. While older analog cell phones often suffered from chronically poor reception and could even be disconnected by simple interference such as high frequency noise, increasingly sophisticated digital phones have led to more elaborate counters. Cell phone jamming devices are an alternative to more expensive measures against cell phones, such as Faraday cages which are mostly suitable as built in protection for structures. They were originally developed for law enforcement and the military to interrupt communications by criminals and terrorists. Some were also designed to foil the use of certain remotely detonated explosives. The civilian applications were apparent, so over time many companies originally contracted to design jammers for government use switched over to sell these devices to private entities. Since then, there has been a slow but steady increase in their purchase and use, especially in major metropolitan areas expected .cell phone jammers block cell phone use by sending out radio waves along the same frequencies that cellular phones use. This causes enough interference with the communication between cell phones and towers to render the phones unusable. [2]

On most retail phones, the network would simply appear out of range. Most cell phones use different bands to send and receive communications from towers (called frequency division duplexing FDD). Jammers can work by either disrupting phone to tower frequencies or tower to phone frequencies. Smaller handheld models block all bands from 800MHz to 1900MHz within a 30-foot range (9 meters). Small devices tend to use the former method, while larger more expensive models may interfere directly with the tower. The radius of cell phone jammers can range from a dozen feet for pocket models to kilometers for more dedicated units. The TRJ-89 jammer can block cellular communications for a 5-mile (160km) radius. Interestingly enough, less energy is required to disrupt signal from tower to mobile phone, than the signal from mobile phone to the tower (also called base station), because the base station is located at larger distance from the jammer than the mobile phone and that is why the signal from the tower is not as strong. [1]

2.3 THEORETICAL BACKGROUND

The mobile phone signal jammer is a device that blocks the reception of mobile phone network transmitting from the base station. This is possible through the skillful combination of some passive and active electronic component which includes Resistors, Capacitors, Transistors, and Inductors.This stages which includes the combination of these components is described thus:

2.3.1 FREQUENCY AMPLIFIERS

In this project, the amplifier used to boost the frequency is the transistor. A transistor is a three-terminal semiconductor device that can perform two functions that are fundamental to the design of electronic circuits: **amplification** and**switching.** Put simply, amplification consists of magnifying a signal by transferringenergy to it from an external source; whereas a transistor switch is a devicefor controlling a relatively large current between or voltage across two terminalsby means of a small control current or voltage applied at a third terminal. The two families of the transistors are the field effect transistors (FET) and the bipolar junction transistors (BJT). The BJT acts essentially as acurrent-controlled device, while the FET behaves as a voltage-controlled device. A BJT is formed by joining three sections of semiconductor material, eachwith a different doping concentration. The three sections can be either a thin *n*region sandwiched between p+ and players, or a pregion between nand n+layers, where the superscript "+" indicates more heavily doped material. Theresulting BJTs are called pnpand npntransistors, respectively. The operation of the npnBJT may be explained by considering the transistor as consisting of two back-to-back pnjunctions. The **base-emitter (BE) junction**acts very much like a diode when it is forward-biased; thus, one can picture thecorresponding flow of hole and electron currents from base to emitter when thecollector is open and the BEjunction is forward-biased. The electron current has been shown larger than the hole current, becauseof the heavier doping of the *n* side of the junction. Some of the electron-hole pairsin the base will recombine; the remaining charge carriers will give rise to a netflow of current from base to emitter. It is also important to observe that the baseis much narrower than the emitter section of the transistor.The BEjunction acts very much asan ordinary diode when thecollector is open. In this case,I_b=I_eCurrent flow inan npnBJT. [3],[4]

2.3.2 FREQUENCY OSCILLATOR

An oscillator is an electronic device that generates oscillations (Signals). Simply put an oscillator receives DCenergy and converts it into AC energy of desired frequency. The frequency of oscillations depends up on the time constants of thedevice which is derived by multiplying its value of Resistance and Capacitance. Oscillators are extensively used in electronic equipment.Oscillators can produce sinusoidal or non-sinusoidal signals. [3]

However for this design, the use of sinusoidal oscillation signal is used since electromagnetic wave is propagated sinusoidally in its natural state.

2.3.2.1Sinusoidal Oscillators.

An electronic device that generates sinusoidal oscillations of desired frequency is known as a sinusoidal oscillator.[3]

2.3.2.2 Basic Principles of Sinusoidal Oscillator.

A feedback amplifier is one that produces a feedback voltage which is in phase with the input signal. A phase shift of180 degrees is produced by the amplifier and a further phase shift of 180 degrees is introduced by the feedback network. Thus the signal isshifted by 360 degrees and fed to the input. That is feedback voltage is in phase with the input signal. But, oscillator is a circuit whichproduces oscillations without any external signal source .An input voltage signal is first supplied to the network and removed .Then a feedback signal is still applied to the input signal. The oscillator will respond to this signal and the feedback signal will be amplified and send to the output. The feedback portion will send a portion of the output again back to the input. Hence the amplifier receives another input cycleand another o/p cycle is produced. This process continues and amplifier will produce oscillations without any external input.

2.3.2.3 Barkhausen Criterion:

The frequency for which a sinusoidal oscillator will operate is the frequency for which the total phase shift is introduced, the signal that proceeds from the input terminals through the amplifier and feedback network, and back to the input, is precisely zero i.e. the frequency of a sinusoidal oscillator is determined by the condition thatthe loop gain phase shift is zero. [4]

2.3.3 TRANSMITTER

The current ratings of the transmitter used in the construction of the jammer has a range of values of about 4-20 mA. [4]. Over the years the 4-20 mA transmitter has become an accepted standard technique for transmitting information between field input/output and the control area. Meanwhile there are thousands of input/output points and associated control components that will continue to use the analog current loop method for transmitting data.

Almostall process control systems are distributed throughout a plant site and information flow may be over long distances. Transmitting data over considerable distances often causes major problems in distributed process control systems. Transmitting data reliably has prompted many different communication schemes and associated products, some of which employ smart electronics in the I/O sensors and control elements.[4]

Long before the electronic age, process control was dominated by pneumatics. Ratio controllers, PID controllers, actuators, and recorders were all pneumatic. The standard was a 3 to 15 psi pneumatic signal, where 3 psi was the live zero. As computer process control began to evolve in the early 1950.s, the signal transmission technique shifted from 3-15 psi to 4-20 mA signals, where 4 mA was the "live" zero. A "real" dead zero has always been an alarm condition. It should be noted that multiple loads can be series connected in a transmitter loop, providing considerable control and display opportunities. Loads today typically have full scale input requirements of 1 volt, 5 volts, and 10 volts. Typical 4-20mA transmitters require a voltage across their output terminals to maintain the device within its operational specifications. This voltage is often referred to as compliance voltage and has a rather wide range. Depending on transmitter specifications, a larger supply voltage may be required or perhaps a 5 volt (250 Ω) controller. It is noteworthy to observe that selecting a supply needs to be consistent with the number and type of series loads and the required 4-20 mA transmitter compliance voltage. Multiple series loads, wide variation in supply voltage, and some inherent noise immunity are advantages of current loop transmitters.[4]

2.3.4 MIXERS

A frequency mixer is a 3-port electronic circuit—two of the ports are input ports and the other port is an output port. The ideal mixer mixes the two input signals such that the outputsignal frequency is either the sum (or difference) frequency of the inputsas shown in the equation below. In other words

$F_{out} = F_{in1} \pm F_{in2}$..................................equation 2.1

The nomenclature for the 3 mixer ports are the Local Oscillator (LO) port, the Radio Frequency (RF) port and the Intermediate Frequency (IF) port. The LO port is typically driven with either a sinusoidal continuous wave (CW) signal or a square wave signal. The choice to apply a CW or square wave signal depends on the application and the mixer in this case a continuous wave was chosen. Conceptually, the LO signal acts as the gate of the mixer in the sense that the mixer can be considered "ON" when the LO is a large voltage and "OFF" when the LO is a small voltage. The LO port is exclusively used as an input port. [5]

In principle, any nonlinear device can be used to make a mixer circuit. As it happens, only a few nonlinear devices make "good" mixers. The devices of choice for modern mixer designers are Schottky diodes, GaAs FETs and CMOS transistors. The choice depends on the application. FET and CMOS mixers are typically used in higher volume applications where cost is the main driver and performance is less important.There are many ways to build a mixer. The simplest mixer consists of a single diode. [5] [6]

2.3.5 MOBILE JAMMING TECHNIQUES

2.3.5.1 Type "A" Device: JAMMERS

In this device we overpower cell phone's signal with a stronger signal, This type ofdevice comes equipped with several independent oscillators transmitting jamming signals capable of blocking frequencies used by paging devices as well as those used by cellular/PCS systems control channels for call establishment. When active in a designated area, such deviceswill (by means of RF interference) prevent all pagers and mobile phones located in that areafrom receiving and transmitting calls. This type of device transmits only a jamming signal and has very poor frequency selectivity, which leads to interference with a larger amount ofcommunication spectrum than it was originally intended to target. [1]

2.3.5.2 Type "B" Device: INTELLIGENT CELLULAR DISABLERS

Unlike jammers, Type "B" devices do not transmit an interfering signal on the control channels. The device, when located in a designated 'quiet' area, functions as a detector. It has aunique identification number for communicating with the cellular base station. When a Type "B"device detects the presence of a mobile phone in the quiet room; the 'filtering' (i.e. theprevention of authorization of call establishment) is done by the software at the base station.When the base station sends the signaling transmission to a target user, the device after detecting simultaneously the presence of that signal and the presence of the target user, signalsthe base station that the target user is in a 'quiet' room; therefore, do not establish thecommunication. Messages can be routed to the user's voice- mail box, if the user subscribes to avoice-mail service. This process of detection and interruption of call establishment is doneduring the interval normally reserved for signaling and handshaking. For 'emergency users', theintelligent detector device makes provisions for designated users who have emergency status.These users must pre-register their phone numbers with the service providers. When an incomingcall arrives, the detector recognizes that number and the call are established for a specifiedmaximum duration, say two minutes. The emergency users are also allowed to make outgoingcalls. Similarly, the system is capable of recognizing and allowing all emergency calls.

It should be noted that the Type "B" detector device being an integral part of thecellular/PCS systems, would need to be provisioned by the cellular/PCS service providers or provisioned by a third-party working cooperatively with full support of the cellular/PCS serviceproviders. [1]

2.3.5.3 Type "C" Device: INTELLIGENT BEACON DISABLERS

Unlike jammers, Type "C" devices do not transmit an interfering signal on the controlchannels. The device, when located in a designated 'quiet' area, functions as a 'beacon' and anycompatible terminal is instructed to disable its ringer or disable its operation, while within thecoverage area of the beacon. On leaving the coverage area of the beacon, the handset mustre-enable its normal function.This technology does not cause interference and does not require any changes to existing PCS/cellular operators. The technology does require intelligent handsets with a separatereceiver for the beacon system from the cellular/PCS receiver. It will not prevent normaloperation for incompatible legacy terminals within a "quiet" coverage area, thus effectivedeployment will be problematic for many years.While general uninformed users would lose functionality, pre-designated"emergency" users could be informed of a "bypass terminal key sequence" to inhibit response tothe beacon. Assuming the beacon system uses a technology with its own license (or in the licenseexempt band), no change to the regulations are needed to deploy such a system. With thissystem, it would be extremely difficult to police misuse of the "bypass key-sequence" by users. [1]

2.3.5.4 Type "D" Device: DIRECT RECEIVE & TRANSMIT JAMMERS

This jammer behaves like a small, independent and portable base station, which candirectly interact intelligently or unintelligently with the operation of the local mobile phone. Thejammer is predominantly in receiving mode and will intelligently choose to interact and block the phone directly if it is within the proximity of the jammer. This selective jamming technique uses a discriminating receiver to target the jamming transmitter. The benefit of such targeting selectivity is much less electromagneticpollution in terms of raw power transmitted and frequency spectrum from the jammer, andtherefore much less disruptive to passing traffic. The jam signal would only stay on as long asthe mobile continues to make a link with the base station, otherwise there would be no jammingtransmission – the technique forces the link to break or unhook and then it retreats to a passivereceive mode again.This technique could be implemented without cooperation from PCS/cellular providers, but could negatively impact PCS/cellular system operation. This technique has an added advantageover Type B in that no added overhead time or effort is spent negotiating with the cellular network. As well as Type B, this device could emergency calls and allow forbreakthroughs during emergencies. [1]

2.3.5.5 Type "E" Device: EMI SHIELD - PASSIVE JAMMING

This technique is using EMI suppression techniques to make a room into what iscalled a Faraday cage. Although labour intensive to construct, the Faraday cage essentially blocks, or greatly attenuates, virtually all electromagnetic radiation from entering or leaving the cage –or in this case a target room. With current advances in EMI shielding techniques and commercially available productsone could conceivably implement this into the architecture of newly designed buildings for socalled"quiet-conference" rooms. Emergency calls would be blocked unless there was a way to receive and decode the emergency transmissions, pass by coax outside the room and re-transmitted. [1]

CHAPTER THREE

3.1 DESIGN AND CONSTRUCTION

The G S M signaljammer consist of three (3) major sub circuits which are stated below

- **Noise Generator Module**

This module of the circuit generates the noise signal that will interfere the G.S.M signal.

- **Carrier/ RF Oscillator/ Mixer Module**

This is the module of the design circuitry that generates the modulating carrier frequency to be transmitted to the antenna. The frequency generated here is the intermediate frequency (I.F). It also mixes with the noise frequency.

- **Amplifiers Module**

This is the module of the design circuitry that amplifies the weak signal noise generated by the noise generator which is mixed with the intermediate frequency before it is being transmitted to the antenna.

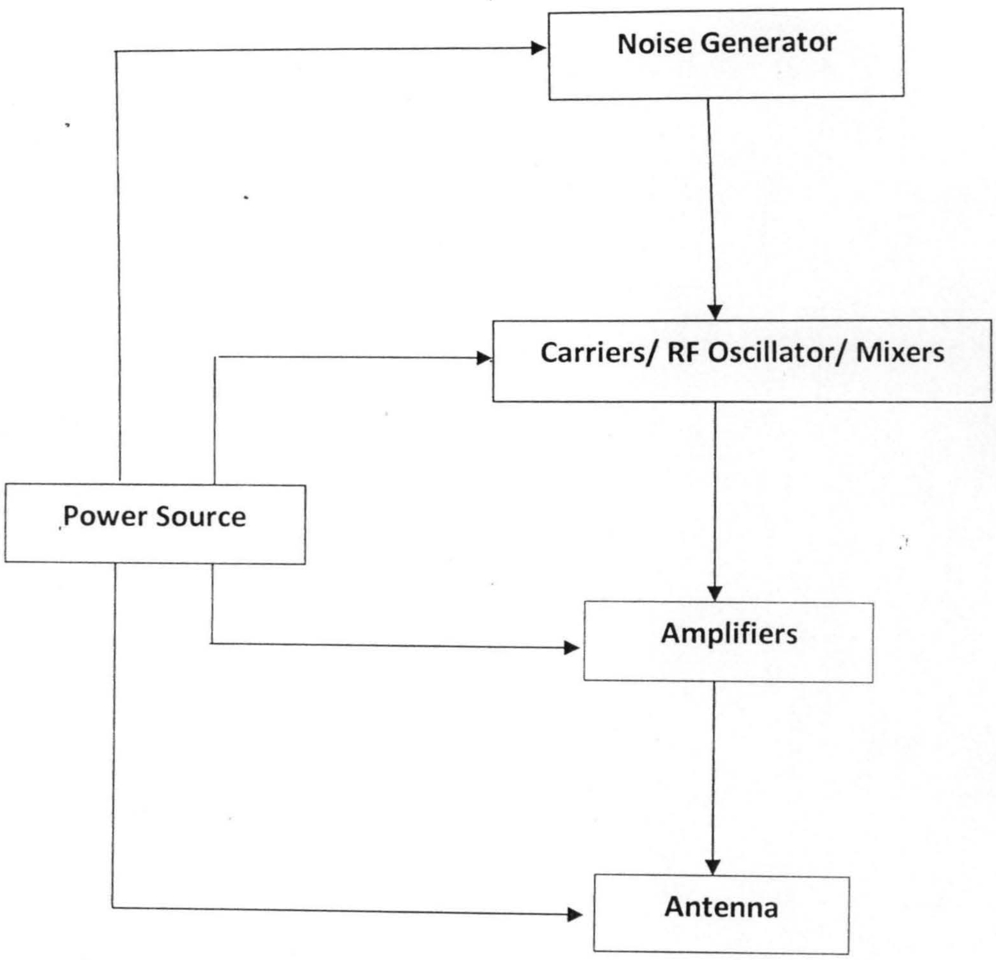


Fig3.1 design block diagram

3.2 THE POWER SUPPLY CIRCUIT

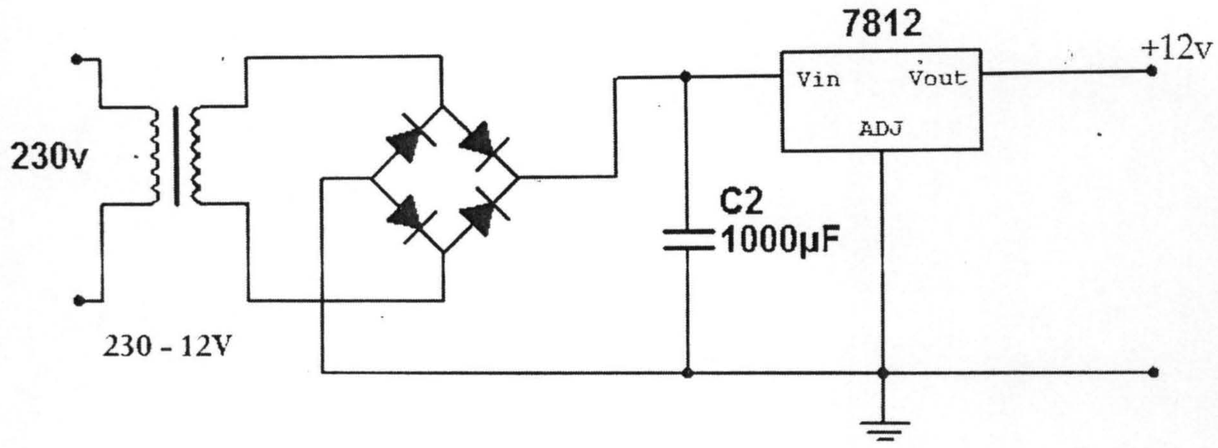


Fig.3.2Power supply circuit

The power supply comprises basically about four (4) components:

- Transformer
- Rectifier
- Filter
- Regulator

3.2.1 Selection of transformer

Since that AC power supply rating of Nigeria is 220-240V,50Hz, a step down transformer of 230V primary voltage and 12V secondary voltage with secondary current rating of 300mA AC to DC rectified voltage, 12V rating is used. The transformer is assumed to have a unity power factor (i.e. ideal situation).

3.3 THE NOISE GENERATOR:

The noise generator, are a high frequency, stable oscillator with high phase noise (jitters). The oscillator generates a noise frequency up to approximately 1GHz as will be seen in the design calculations below.

The noise generation module is being subdivided into six (6) different modules namely;

- Timing Part
- Voltage Divider
- Tank Circuit
- Negative Feedback
- Amplifier Gain
- Decouplers/Filters

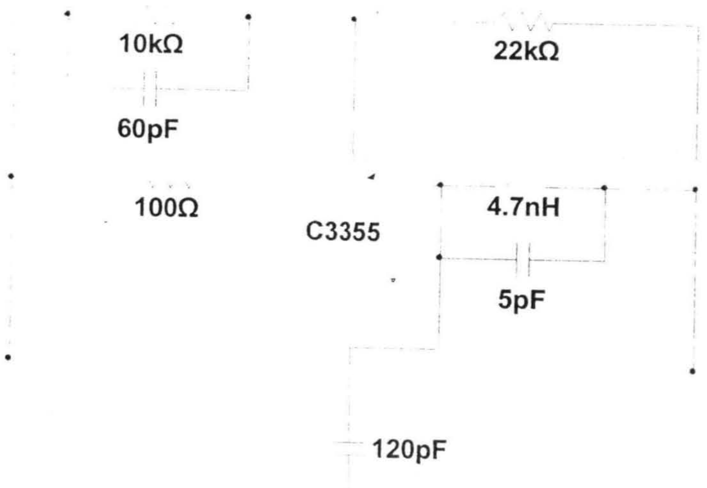


Fig 3.3 Noise generator circuit

3.3.1 Timing Part

This provides the required timing for the on and off of the oscillation generated in the main module, which is done by the assistance of the R.C circuit shown below

Fig 3.4TimeConstant.

Hence the time constant I.e.λ of the oscillating frequency that would be generated is given by

$$\lambda = RC$$

Where$R = 22 \times 10^3\Omega, C = 60.8 \times 10^{-12}F$,

Hence $\lambda = 22 \times 10^3 \times 60.8 \times 10^{-12} = 1.32\mu S$

3.3.2 Voltage Divider Part

Fig 3.5 Voltage Divider

The voltage divider part consists of two (2) resistors connected in series so that the input voltage i.e. 12V is shared between the two resistors. Hence the initial voltage entering the base of the transistor i.e. (C3355) is calculated below;

Initial voltage (V_0) is given by

$$\frac{V_{CC} \times R_1}{R_1 + R_2}$$

Where$V_{CC} = 12V, R_1 = 10K\Omega\,, R_2 = 22K\Omega$

hence $V_0 = \frac{12\times10\times10^3}{10\times10+22\times10^3} = 3.73V$

Base current I_b entering the base of the transistor is given by

$$I_b = \frac{V_{cc\times}V_{be}}{R_1 + \beta R_2}$$

Where$V_{CC} = 12V, V_{be} = 0.7V\ (from\ manufacturer), R_{1=}10K\Omega, \beta =$

$300\ (from\ manufacturer), R_2 = 22K\Omega$

Hence base current $I_b = \frac{12\times0.7}{10\times10^3+(300\times22\times10^3)} = 1.27\mu A$

Therefore, $V_R = 1.27 \times 10^{-6} \times 22 \times 10^3 = 0.02794V$

Hence voltage entering the base is given by;

$$V_b = V_0 - V_R$$

$$V_b = 3.75 - 0.02794 = 3.722V$$

Therefore the voltage entering the base of the frequency oscillation i.e. the transistor is approximately $3.72V$

3.3.3 Tank Circuit

The tank circuit comprises of an inductor and a capacitor coupled to generate a radio frequency of approximately 1GHz. At resonant frequency, when the reactance of the inductor or coil equals to the reactance of the capacitor, the current in the coil will be equal and opposite to the current in the capacitor and the net current flow in the external circuit will be zero (0) i.e. from the voltage source. At this resonant frequency, the impedance of the circuit is greatest. The diagram below shows the tank circuit part.

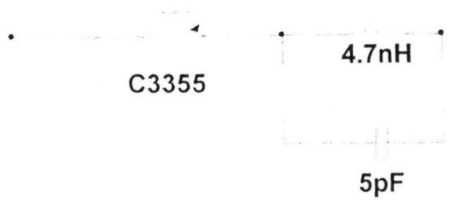


Fig 3.6 Tank Circuit

Hence the frequency of operation of the circuit i.e. the noise generator is calculated below;

$$F_0 = \frac{1}{2\pi\sqrt{LC}}$$

Where F_0= resonant frequency (frequency of operation)

$$L = 4.7nH, C = 5pF;$$

Hence $F_0 = \frac{1}{2\times3.142\times\sqrt{4.7\times10^{-9}\times5\times10^{-12}}} = 1.03GHz$

Therefore, the frequency generated by the tank circuit is approximately1GHz.

3.3.4 Feedback

Feedback is the method of supplying external energy to the LC circuit. Some oscillators work at frequency over 100 million cycles per second and it is quite obvious that no mechanized switch could work at that speed. By connecting the LC circuit to the base of the transistor (C3355), the oscillating voltage can be amplified, if a small portion of this amplified voltage can be feedback in the proper phase, enough electrical energy will be put back in the LC tank circuit. The transistor in the oscillator does not itself do any oscillating, it is the LC circuit that oscillates and it is the value that gives the push. The two types of feedback that this gives to the transistor are namelyPositive Feedback and negative feedback. [5],[9]

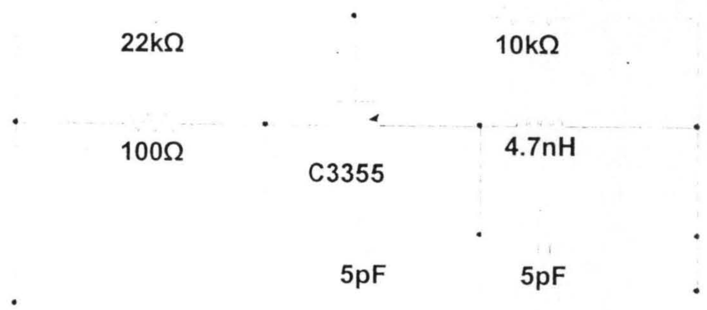


Fig 3.7 Feedback circuit

The voltage input at resonant frequency is calculated below;

Reactance of the capacitor at a frequency of 1.03GHz is given by

$$X_C = \frac{1}{2\pi FC}$$

Where $F = 1.03GHz, C = 60.8pF$

Hence $X_C = \frac{1}{2\times3.142\times1.03\times10^{9}\times60.8\times10^{-12}}$

Therefore $X_C = 2{,}54\Omega\ at\ 1.03GHz$

The voltage at this impedance during oscillation using voltage divider principle is given by

$$\frac{2.54 \times 12}{2.54+22 \times 10^3} = \quad 0.001385\text{V}$$

Also the current entering the base at this impedance during oscillation is given

$$I_b = \frac{V_{cc} \times V_{be}}{R_1 + \beta R_2}$$

$$I_b = \frac{12 \times 0.7}{2.54+(300 \times 22 \times 10^3)} = 1.27 \times 10^{-6} A$$

But$V_R = VI_b$, hence $V_R$is given by

$$V_R = 1.27 \times 10^{-6} \times 22 \times 10^3 = 0.027V$$

Therefore the voltage entering the base of the transistor is given by

$$V_b = 0.001385 - 0.022 = -0.027V$$

The base voltage having a value of $V_b = -0.027$ implies a negative feedback at the resonating frequency which turns on the transistor.

The output voltage to the external circuit is gotten from the collector terminal of the transistor to the tank circuit.

At resonance frequency $X_L = X_c = \frac{R_L}{Q}$

Where Q = quality factor is defined by $\sqrt{\frac{X_C}{X_L} - 1}$

But X_C for feedback is given by $\frac{1}{2\pi FC}$

$$X_C = \frac{1}{2 \times 3.142 \times 1.03 \times 10^9 \times 5^{-12}} = 30.9\Omega$$

Also $X_L = 2\pi FL = 2 \times 3.142 \times 1.03 \times 10^9 \times 4.7 \times 10^{-9} = 30.4\Omega$

Hence $Q = \sqrt{\frac{30.9}{30.4} - 1} = 0.13$

R_L is the load resistance which is gotten when the noise generator stage is loaded, therefore it is equal to the reactance of capacitor of the load next stage i.e. the $30pF$ capacitor

Hence $R_L = R_C$

But $X_C = \frac{1}{2\pi FC} = \frac{1}{2 \times 3.142 \times 1.03 \times 10^9 \times 30 \times 10^{-12}} = 5.15\Omega$

Therefore, $\frac{R_L}{Q} = \frac{5.15}{0.13} = 39.6\Omega$

If $I_C = I_b \times \beta$

$I_C = 1.27 \times 10^{-6} \times 300 = 0.4mA$

Hence $V_{out} = I_C \times R_C$

$V_{out} = 3.81 \times 0.4 \times 10^{-3} \times 39.6 = 0.01508V$

This voltage implies that there is no conduction at signal output.

3.3.5 Amplifier Gain

The common emitter gain of the amplifier is given by the relation $\frac{R_{CN}}{\gamma_{e}+R_{E}}$

Where R_{CN} = Resistance between the common and the collector,

γ_e =Dynamic resistance, R_E =Emitter resistance

But $R_{CN} = R_L // R_{CE} // R_C$

Where $R_{CE} = 100K\Omega$(from the manufacturer), $R_L = 5.15\Omega, R_C = 39.6\Omega$

Hence $R_{CN} = 5.15 // 100 \times 10^3 // 39.6 = 4.55\Omega$

Also γ_e is given by the relation

$$\gamma_e = \frac{2.6 \times 10^{-3}}{I_E}$$

Where = $I_E = I_C = 0.4mA$ (computed before)

$$\gamma_e = \frac{2.6 \times 10^{-3}}{0.4 \times 10^{-3}} = 6.84\Omega$$

$R_E = 100\Omega$(From the circuit i.e. Fig 3.2)

$$\text{Hence Gain} = \frac{4.55}{6.84 \times 100} = -0.042$$

$$V_{out} = V_{in} \times Gain$$

$$V_{out} = -0.027 \times -0.042 = 0.0011V$$

The output voltage shows that the transistor is not conducting i.e. it is in the off state. When the tank circuit is oscillating i.e. there is frequency in the noise generating circuit, the gain becomes;

$$-\frac{R_{CN}}{\gamma_e + R_E}$$

$$R_{CN} = R_L // R_{CE} // R_L,$$

$R_{CN} = 100K //100K //39.6$, $R_{CN} = 50K//39.6, R_{CN} = 50 \times 10^3 //39.6$, $R_{CN} = 39.56\Omega$

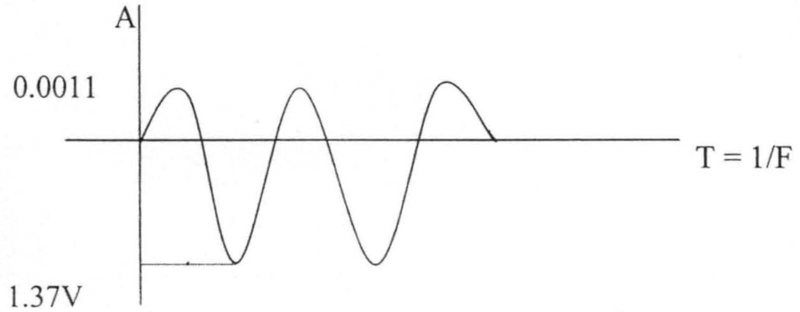
$\gamma_e = 6.84\Omega$ (Computed before)

Hence, Gain $= -\frac{39.56}{6.84+100} = -0.37$

$$V_{out} = -0.37 \times 3.72 = -1.37V$$

Hence the negative sign shows that the transistor is on.

Therefore the generated frequency wave form is shown below.



The total power emitted at this stage is given by the relation;

$$P = I^2 R \ (watts)$$

$$P = (0.4 \times 10^{-4})^2 \times 39.6 = 4\mu W$$

It is therefore noted that the power at which this frequency is generated is low hence there's need for this signal to be amplified.

3.3.6 Decoupler / Filters

If an amplifier contains several stages of amplification all those stages will be supplied with the signal source of DC power supply. The anode current of the entire amplifier transistor must flow through the power supply. Therefore the internal resistance of the power supply will act as common impedance for all the amplifier circuit.

Therefore when a signal is supplied to the circuit, the collector current of all the transistor will vary in accordance with the signal in addition to the DC flowing through the common power supply. Therefore the AC component flowing through the common impedance, some of this current will be in phase with each other and some will be 180^0(degrees) out of phase. It is the resultant of these several difference which causes the trouble.

This resultant alternating current produces voltage variation across the common impedance which feedback the variation into the powerline, the overall effect is the sound in the loudspeaker which resemble the powering of an outboard motion.

The purpose of the decoupler / filter is to provide a path to earth of low reactance for the AC current and path of high resistance to their passage through the power supply. The decoupler / filter used in coupling the noise generator stage to the next stage is a capacitor of $120pF$ shown in the Fig 3.3

3.4 CARRIER / RF OSCILLATION / MIXER MODULE

This is the module of the circuit design where a very high frequency known as the intermediate frequency (I.F) is produced using the LC tank circuit in this module. The frequency response of the C3355 transistor used in this stage is capable of withstanding the high frequency generated at thisstage. The frequency generated at this stage is up to 1.9GH□.

This module also acts as the mixer that mixes the frequency from the noise generator and the frequency (IF). This two frequencies mixes in the form shown below;

$F_M = F_0 + F_1$, And $F_M = F_0 - F_1$

WhereF_M = Modulating frequency

F_0 = Fundamental frequency($1.03GHz$)

F_1 = Intermediate frequency($1.9GHz$)

Therefore; $F_{M1} = F_0 + F_1 = (1.9 + 1.03)GHz = 2.93GHz$

Also; $F_{M2} = F_0 + F_1 = (1.9 - 1.03)GHz = 870MHz$

Hence the modulated signal being transmitted to the antenna has a frequency band of $870MHz$ up to $2.93GHz$ because neither of its sides bands are filtered off which means that the jammer covers the whole bandwidth of the GSM signal which is about $890MHz$ to

$960MHz$ for both forward and reverse link. [4] Therefore the GSM signal transmitting in the area where this jammer is located will have its signal effectively jammed by the jammer.

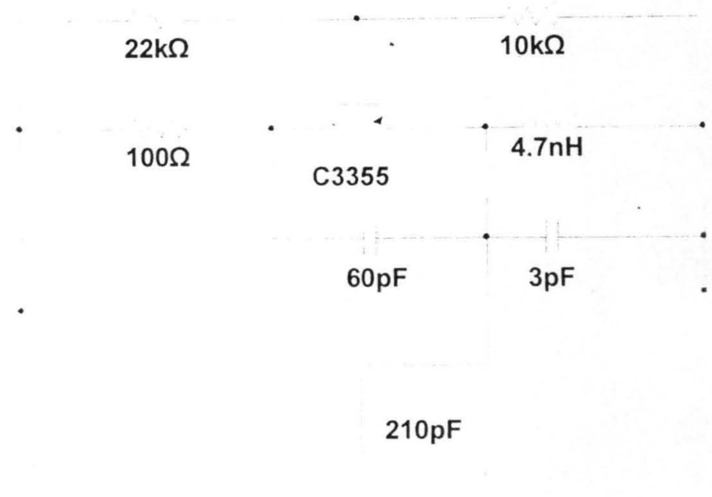


Fig 3.8 Carrier Circuit

3.5 AMPLIFIER MODULE

The relative low output power of the signal being produced is subject to amplification so that its signal strength will have enough power to interpose the GSM signal which is beamingfrom the base station at a high power.

Also the C3355 amplifier is also used for the amplification purpose due to its high frequency response. The circuit diagram for this module is shown next page.

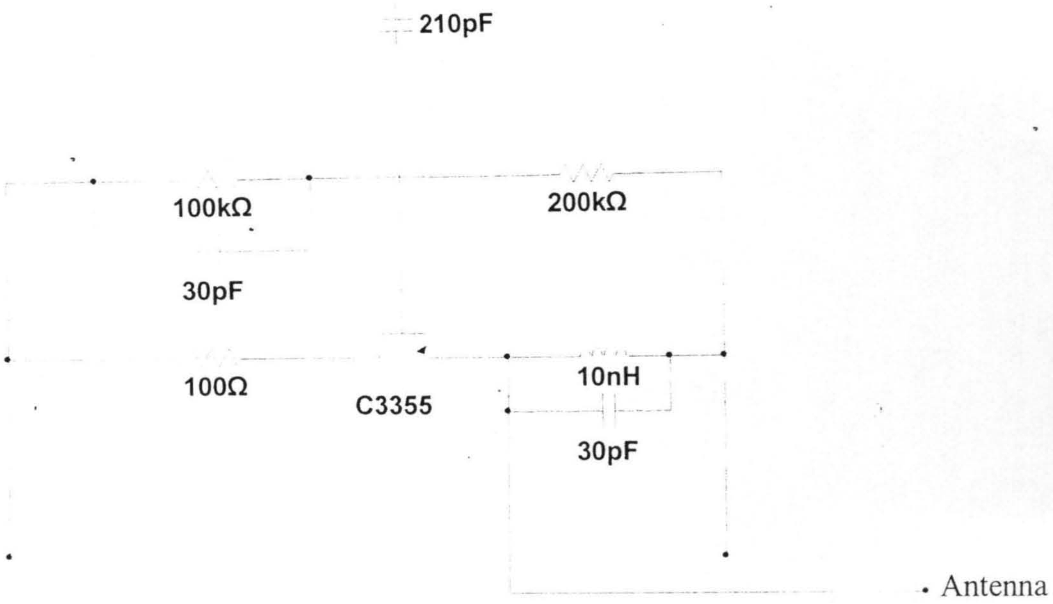


Fig 3.9 Amplifier Circuit

3.5.1SIGNAL STRENGTH

The signal strength or power density $(P.d)$ of the jammer is given by the formula

$$P.d = \frac{P_E}{4\pi r^2}$$

Where; P_E =Trarısmitting Power of the antenna, r = Radius Covered.

From the formula above it is seen that the transmitted power density (either from the jammer or the base station) to the receiver (mobile station) is directly proportional to the transmitting power and inversely proportional to the square of its distance.

Also, the transmitted power can be calculated using the power equation

$$P_E = \frac{V^2}{R_E}$$

Where R_E = Total collector reactance, $R_E = X_L + X_C$

Where X_L = inductive reactance (Amplification stage), and

X_C = capacitive reactance (Amplification stage)

Hence;$X_L = 2\pi FL$; assuming frequency =$870MHz$

$$X_L = 2 \times 3.142 \times 870 \times 10^6 \times 10 \times 10^{-9} = 54.6\Omega$$

$$X_C = \frac{1}{2 \times 3.142 \times 870 \times 10^6 \times 30 \times 10^{-12}} = 6.097\Omega$$

Hence $R_E = X_L + X_C = 54.7 + 6.097 = 60.8\Omega$ (collector resistance)

Base voltage of the transistor is given by

$$V_b = V - V_R$$

Where $V = \frac{V_{CC} \times R_1}{R_1 + R_2} = \frac{12 \times 100 \times 10^3}{100 \times 10^3 + 220 \times 10^3} = 3.75V$

$$V_R = I_b \times R_2$$

$$I_b = \frac{V_{CC \times V_{BE}}}{R_{1+\beta R_2}} = \frac{12 \times 0.7}{100 \times 10^3 + 220 \times 10^3} = 0.13\mu A$$

$$V_R = 0.13 \times 10^{-6} \times 220 \times 10^3 = 0.03V$$

Therefore $V_b = 3.75 - 0.03 = 3.72$

But $I_b = \frac{V_b}{R_b}$

Where R_b is base resistance gotten using parallel resistance rule shown below

$$R_B = \frac{100 \times 10^3 \times 200 \times 10^3}{100 \times 10^3 + 200 \times 10^3} = 68750\Omega$$

$$I_b = \frac{3.72}{68750} = 54.1\mu A$$

$$I_C = I_b \times \beta = 5.41 \times 10^{-6} \times 300 = 0.0162A$$

Collector voltage $= I_C \times R_C = 0.0162 \times 60.8 = 0.98V$

Transmission power $P_t = \frac{V^2}{R_C} = \frac{0.98^2}{60.8} = 0.016W$

If the radius is taken to be 6m, therefore the power density will be;

$$P_d = \frac{P_E}{4\pi r^2} = \frac{0.016}{4 \times 3.142 \times 6^2} = 0.4mW$$

Hence Power density of the jammer is $0.4mW$

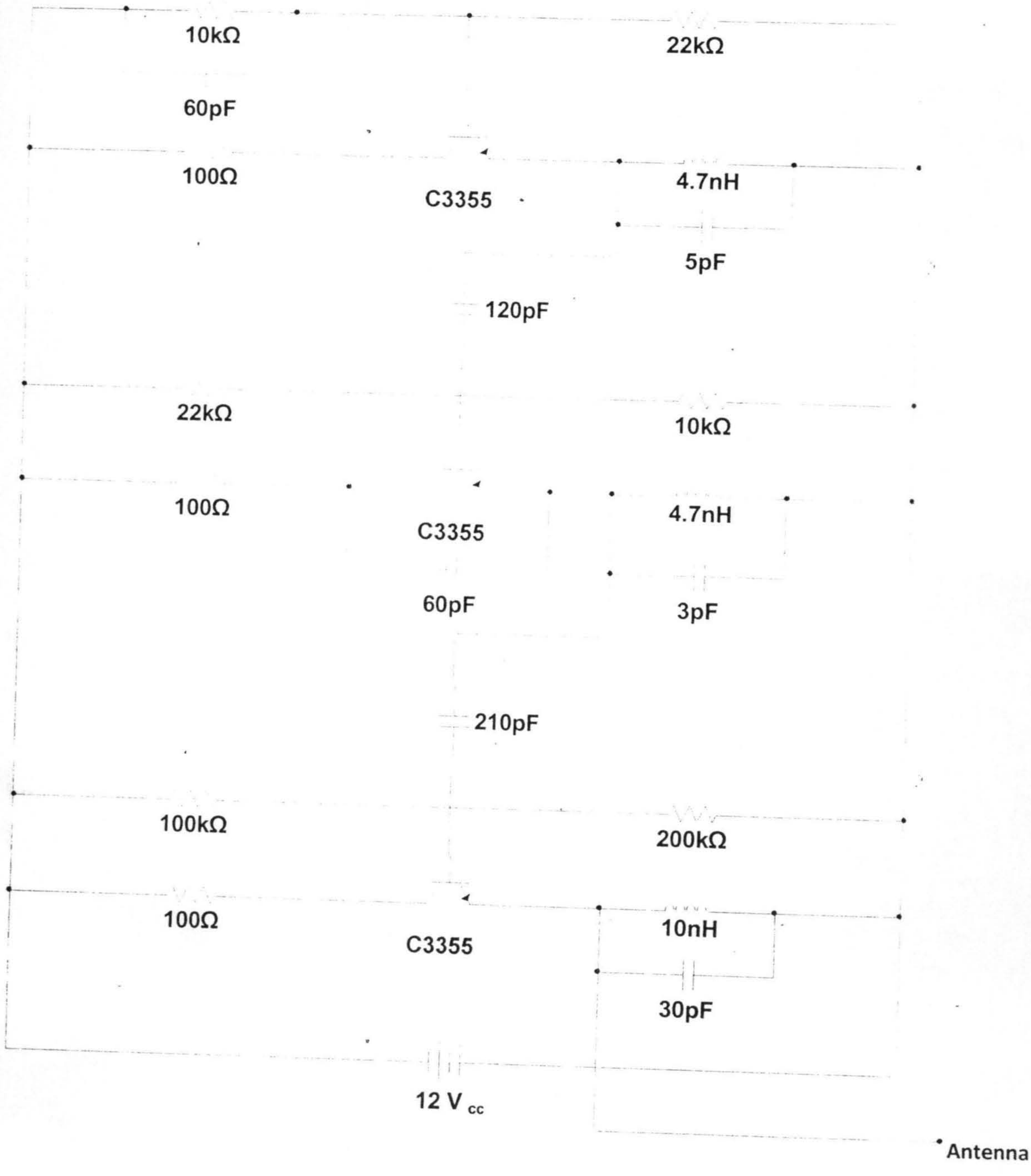


Fig 3.10 Circuit Diagram of the simple GSM Signal Jammer

CHAPTER FOUR

4.1 TESTING AND RESULT

- The circuit was carefully and stringently connected as shown in the circuit diagram of figure 3.10 with the circuit not energized.
- A mobile phone (GSM) was brought near the proximity of the jamming radius i.e. 6 meters, totaling a 12 meters omnidirectional radiation pattern of the jamming circuit.
- The network service bar on the cell phone (GSM) was confirmed by physically observing the network service in the mobile phone through the screen of the hand set.
- Communication between the mobile phone i.e. the mobile station and the base station (Network provider) was also confirmed by attempting a call to another GSM phone which might be within the perimeter of the mobile phone jammer or outside its radius, this can also be confirmed by trying to access the base station through some operational service code like that used in checking the account balance of a particular subscriber among others.
- A ring back tone received from the GSM phone to be tested confirmed the presence of full communication between the mobile phone (GSM) and the serving base station and also a text massage received in the mobile phone to be tested displaying the account balance of the particular subscriber also affirms the presence of a full communication between the mobile station and the base station.
- The circuit is then energized by connecting it to the ac power supply and pressing the button on the side of the outer casing. At this point, the jamming device is transmitting noise at the GSM frequency band covering a range of about 12meters, where the GSM

phone to be tested is brought near its perimeter, and the network bar on the mobile phone is disappeared having the mimicking antenna on its screen empty. When a second of generation phone, (2Gphone) having an inscription "E" on its screen indicating the presence of Packet Data Enabled Service is brought to the jamming proximity, the inscription "E" was crossed indicating no data service can be sent or received on the mobile phone (mobile station) via the base station. In this case both the uplink GSM frequency range i.e. from the mobile station to the base station, and the downlink frequency range from the serving base station has been effectively jammed or blocked by the GSM mobile phone jammer.

4.2 CONFIRMATORY TEST

During full operation of the mobile phone jamming device i.e. when the jammer is left transmitting signal through its antenna, trying to initiate a call through the mobile phone was impossible. Also trying to access the base station through the network operating codes also proved abortive with message of request not completed being displayed on the screen of the mobile phone.

While the mobile phone jammer is still being powered and the mobile phone to be tested is still in its radar, trying to establish a call between another cell phone outside the jamming radius and the specimen was also impossible and also text message sent to this specimen was not delivered.

4.3 DISCUSSION OF RESULT

The disappearance of the network bar from the mobile phone (specimen) screen and also the crossing of the "E" inscription of the 2^{nd} generation mobile phone (2G) indicate that it is within the vicinity of a microware frequency that is transmitting noise which is interfering with that it is receiving from the base station. This type of interference is known as destructive interference since the two frequencies from this transmitter are cancelling each other out. This means that the traffic channel (TCH) of the network provider has been blocked due to the effect of the jamming device on its network.

The network accessibility code returning a "Request not complete" message on the screen of the mobile phone indicating that the signaling channels which consists of the broadcast channels (BCH) for both uplink and downlink channels, common control channels (CCH) which is used for synchronizations and also the dedicate control channel which is used for paging has been effectively blocked by this jamming device.

The inadvertent unavailability of the specimen mobile phone indicate that downlink signaling channel from the base station has been blocked because the phone outside the jamming frequency radar can reach the mobile station but the mobile station cannot communicate with the specimen mobile station since it's signaling channel been blocked.

4.4 OBSERVATIONS

During the process of testing of the jamming device, few observations made include:

- Non jamming of the America mobile phone system in which it is an analog system that transmitted or performed communication with the use of the 800MHz frequency. Because this frequency falls below the jammers range which in between 870MHz –2.03GHz.
- There is effective jamming of the CDMA (code division multiple access) mobile phone system which uses a frequency band of 1800 MHz which falls within the range of the jammer.
- There is also effective jamming of the TDMA (Time Division Multiple access) mobile phone system which uses a frequency in the band of 1900MHz that also falls within the jamming range of the device.
- It was also observed that a partial jamming occur with the 3G (third generation) mobile phone system which use a frequency in the range of the jammer i.e. 2100MHz or 2.1GHz here it was discovered that there was breakage in the traffic channel (TCH) but no total blockage was observed.
- It was also observed that GSM mobile systems that uses the frequency hopping technique which is intended to avoid jamming and interception of the GSM signal by providing a hopping sequence f up to 64 different frequencies proved abortive when bought near the jammer because all of this 64 different spread frequency spectrum of the GSM network falls within the frequency range of the jammer. Hence it has defeated the inherent security of the frequency hopping technique.
- It was also observed that the further away the base station is to the mobile station the more effective the jamming power since there reduction in the signal to noise ratio i.e. reduced received signal strength increase the jamming capability

4.5 LIMITATIONS

The jamming device is not totally effective due to its relatively low transmitting power and it inability to cover a very wide area. Also because of it design constraint it cannot effectively jam or block some mobile phone device such as that use the analog (FDMA) American mobile phone system and the 3G (Third generation) mobile phones.However it has proven very effective in the particular system in which it is designed for.

CHAPTER FIVE

5.1 CONCLUSION

The G.S.M mobile phone signal jammer is a device that is used to jam or interfere/block the transmitting and receiving of information i.e. hindering communication between the GSM phone and the base station, Hence making it useful in area where this device are restricted such as workshop places, lecture rooms, libraries, concert halls, meeting rooms and other places where silence is appreciated.

The jamming technique is achieved by transmitting noise signal to interfere with the frequency of the mobile station (downlink) and the GSM transmitter (uplink) so as to interfere with each other a phenomenon known as destructive interference.

The jamming device also jams other mobile system effective and do not block some others like 3G mobile phone system. And also transmit at a small power level so jamming is more effective at a very low received signal level from the base station.

REFERENCES

[1]. Mobile and Personal Communications Committee of the Radio Advisory Board of Canada, "Use of jammer and disabler devices for blocking PCS, cellular and related services"http://www.rabc.ottawa.on.ca/e/files/01plus.pdf

[2]. http:// www.siganal.jammer.com/history/html

[3]. Siwiak, k., Radiowaves Propagation And Antennas For Personal Communication, *Artech House, 2nd edition, Pg138.*

[4]. Pozar, D.M., Microwave Engineering, *John Wiley and Sons, 2nd edition, Pg198.*

[5]. John Scourious, Overview Of The Global System For Mobile Communications, http://ccnga.uwater.ca/jscouria/GSM/gsmreport.html|1.

[6]. Marki, F.A., "Miniature Image Reject Mixers and Their Use in Low-noise Front-ends in Conjunction with Gaas FET Amplifiers," *Circuits, Systems and Computers, 1977. Conference Record. 1977 11th Asilomar Conference on* , vol., no., pp. 159-162, 7-9 Nov 1977. http://www.markimicrowave.com/menus/appnotes/noise.pdf.

[7]. "Mixer Evolution, the Balanced Mixer Family Circle." Application Note. http://www.markimicrowave.com/menus/appnotes/balanced.pdf.

[8].Henderson, B. C., "Predicting Intermodulation Suppression in Double-Balanced Mixers," Watkins-Johnson Company Technical Notes. Vol. 10, No. 4, July/August 1983

[9]. Micro Electronics Circuits,

Sedra/Smith, 4th Edition, Pg152-170

[10]. Principles of Electronics,

V.k, Metha, 5th Edition, Pg256-280