DESIGN AND CONSTRUCTION OF A MOBILE PHONE SIGNAL JAMMER

BY

DADA ABIDEMI

2007/2/26402EE.

A Thesis submitted to the Department Of Electrical and Computer Engineering in Partial fulfillment for the requirement for the Award of B. Eng in Electrical and Computer Engineering of the Federal University of Technology, Minna, Niger State.

NOVEMBER, 2011.

DEDICATION

This project is dedicated to the glory of God, the Almighty and also to my mum Mrs. Alice Aduke Dada for her constant and silent prayers for me.

ACKNOWLEDGEMENT

My profound gratitude goes to God Almighty for his love, guidance, protection, provision, favours and blessings all through the period of my study.

My sincere appreciation to my mum Mrs. .Alice Aduke Dada, my uncle and his wife Mr. and Mrs. Tosinkoya Dada and my brother, boss and mentor Engr. Igunnu O. for always being there to offer their uncompromising support in every wise.

My appreciation is also greatly expressed to my supervisor, Mr. Ambafi J.G and Mallam Mohammed Doko for their time, assistance and quality advice leading to the successful completion of this work, and to the entire staff of the department.

Finally, a big thanks to my friends Olawepo peter, Biggyray, Yusuf, Femi Abiodun, Shola Awarun, Oke Oluwatoyosi, Ahmad Tajudeen, Shobayo, and others.

May the good Lord in his abundance, bless you and prosper your every Endeavour, Amen.

ABSTRACT

Signal jammer is an electronic device that jams the frequency of a transmitting device. Mobile phone signal jammer interferes with the communication frequency within a specified radius depending on the strength of the signal jammer. This is achieved by generating and transmitting radio signal of the same frequency as the base station (BS) of the mobile phone and at a higher power so as to collide and cancels out the mobile phone signal. The method employed in realizing this project is made up of discrete components, resistor, capacitor, inductor and transistor to generate the required frequency (noise) and then amplifies the frequency generated to range of 800 MHZ to 1.4 GHZ in order to match the frequency of the mobile phone being transmitted by the base station (BS). Jamming of a mobile signal is successful, when a mobile phone within the area where the jamming device is situated, is disable. This was confirmed by to be efficient in jamming MTN, GLO, AIRTEL, ETISALAT and frequencies. Thereby allowing no call to go through.

TABLE OF CONTENT

LIST OF FIGURES

LIST OF TABLES

CHAPTER ONE

INTRODUCTION

Mobile phone jammer is a device that transmits signal of the same frequency at which the GSM system operates, with the jamming achieved when the mobile phones in the area where the jammer is located are disabled [4].

The artificial intelligence device is to keep the GSM jammer off until it senses the presence of GSM mobile phone signals, then it switches on the artificial intelligent mobile phone jammer. It is a watch-dog that alarms the jammer for action [5].

The main purpose of a mobile phone jammer is to obstruct phone signal in a designated area. The mobile phone jammer is a radio frequency equipment which produces RF signal to beat the mobile phone frequency and effectively jam the signal which results in no service to any type of mobile phone such as CDMA and GSM in the range of 800MHz to 900MHz [9].

The jammer described here is for 800MHz to 1.4GHz range. Once the mobile phone jammer is in operation, all mobile phones present within the jamming coverage area are blocked and cellular activity in the immediate surroundings is jammed. Presently, mobile phones are regularly used by millions of people all over the world. Because we can use a mobile phone from just about anywhere in the world to communicate, it is one of the greatest inventions for social and business life today.

Even though mobile phones have many advantages, it eventually raise problems such as their potential use to invade privacy, contribute to academic cheating, and even aid in industrial espionage. It's great to call anyone at anytime. Unfortunately, places like restaurants, concerts and temples, all suffer from the spread of mobile phones because not all phone users know when to stop talking. Who has not seethed through one side of a conversation about an incredibly personal situation as someone shares intimate details with his friend as well as everyone else in the area? While most of us just grumble and move on, some people are actually going to extremes to retaliate. As mentioned above, these situations will cause nuisance, and to avoid these problems, the need to use jammers. Disrupting a phone communication is the same as jamming any other type of radio communication. A mobile phone works by communicating with its service network through a cell tower or base station [10].

A jamming device transmits on the same radio frequencies as the mobile phone, disrupting the communication between the phone and the mobile phone base station in the tower. This is called a denial of service attack. The jammer denies service of the radio spectrum to the mobile phone users within the range of the jamming device. As with other radio jamming, mobile phone 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 towers to render the phones unusable. On most retail phones, the network would simply appear out of range. Most mobile phones use different bands to send and receive communications from towers. Jammers can work by either disrupting phone to tower frequencies or tower to phone frequencies [7].

The jammer's effect can vary widely based on factors such as proximity to towers, indoor and outdoor settings, presence of buildings and landscape, even temperature and humidity play a role. It should be mentioned that mobile phone jammers are illegal devices in most countries. ("According to the Federal

Communications Commission (FCC) in the USA: "The manufacture, importation, sale, or offer for sale, of devices designed to block or jam wireless transmissions is prohibited") [11]. However, recently, there has been an increasing demand for portable mobile phone jammers. It should be clearly noted that this project, presented in this report, is solely done for educational purposes.

The possible application areas of jamming system are:

- Prevent industrial espionage where mobile units are used as bugging devices.
- Counter terrorism threats such as remotely detonated bombs in high risk areas.
- Eliminate public nuisance in places like movie theatres, restaurants and temples.

1.1 AIMS AND OBJECTIVES

The project involves the design and implementation of mobile phone jammers to block all the mobile phones within the designated area. This device will disrupt mobile communication with respect to the following:

- Operate in the 900MHz band.
- It has a five meter of radius effective blocking ability.

1.2 METHODOLOGY

This project is constructed using electronic component such as resistor, capacitor, inductor, and transistor. The transistor is used to regulate the amount of voltage and current going into the resistor.

The capacitor in conjuction with the inductor forms the tank circuit, which is the major oscillator or frequency generator subcircuit in the project circuit diagram. Some capacitors in the circuit act as a filter. Some transistors are used to respond to very high frequency.

Hardware used in the project:

- Power supply
- Sensor
- Mixer
- Noise generator
- Amplifier
- Antenna
- Jammer

1.3 SCOPE OF WORK

- Operate in the 800 - 950MHz band.
- It has a five meter effective blocking radius.

1.4 USES

The mobile phone jammer is highly advantageous, and some of its usefulness are:

- Can be used in educational institutions to reduce the rate of examination malpractice using GSM.
- Can be used in banking sector to reduce robbery operation by rendering the network useless, and as such, there would be no communication between the informant in the bank and robbers outside the bank.
- Can be used in worship places to reduce the rate at which people are distracted during worship.

- Can be used in conference room to deactivate network and as such confidential information will be secured.
- Can help to counter explosive device

CHAPTER TWO

LITERATURE REVIEW

The RF oscillator forms the heart of the system. The frequency of the oscillator is 900 MHz, and this is the carrier frequency of the jammer. This frequency is modulated by the modulating signal given to the base of the transistor and the modulated output is obtained across the collector terminal. This modulated output is connected to the antenna, which converts the electric signal into electromagnetic signal and transmits it into the space.

The receiver, which is the mobile phone in this case, receives the transmitted signal and tries to demodulate it. Since this signal is not within the bandwidth of the cell it displays "Network Busy" on the LCD panel. Also, since the power of the transmitter is greater than the original signal transmitted from the mobile phone tower, the mobile phone will not respond to the original signal. This project effectively jams the cell signals.

The heart of the circuit is formed by the MCU, which is used to generate a square wave. This signal is fed to the integrator and it is mixed with noise which is generated by the noise generator in the active mixer. This low level signal is feed to VCO circuit module, which generates the equal frequency of RF spectrum to be jammed. The RF signal is then feed into a critical tuned BPF and is feed to amplifier; then the amplified signal is fed to high power RF module for further amplification and terminated to antenna [8].

Electronically speaking, mobile phone jammers are very basic devices. The simplest just have an on/off switch and a light that indicates when it is on. More complex devices have switches to activate jamming at different frequencies.

2.1 HISTORICAL BACKGROUND

Communication jamming devices were first developed and used by military. This interest comes from the fundamental objective of denying the successful transport of information from the sender (tactical commanders) to the receiver (the army personnel), and vice-versa. Jammers were also used to disable or sabotage the enemy's use of remote controls. Nowadays, mobile phones are becoming essential tools in our daily life. Here in Nigeria, for example, with a rather high population (around 150 million), four main mobile phone carriers are available; namely; Airtel, Glo, Etisalat, and Mtn. The first three use the GSM 900 system, while the fourth uses the GSM 1800 system [11].

The rapid proliferation of mobile 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 mobile phones introduced in daily life. While older analogue 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.

Mobile phone jamming devices are an alternative to more expensive measures against mobile 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.

2.2 THEORETICAL BACKGROUND

As with other radio jamming, mobile phone 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 towers to render the phones unusable. On most retail phones, the network would simply appear out of range. Most mobile 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 mobile phone jammers can range from a dozen feet for pocket models to a few kilometres for more dedicated units. The TRJ-89 jammer can block cellular communications for a 5-mile (8 km) radius.

Every jamming device has an antenna to send the signal. Some are contained within an electrical cabinet. On stronger devices, antennas are external to provide longer range and may be tuned for individual frequencies.

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.

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

Smaller jamming devices are battery operated. Some look like mobile phones and use phone batteries. Stronger devices can be plugged into a standard outlet or wired into a vehicle's electrical system.

The jammer's effect can vary widely based on factors such as proximity to towers, indoor & outdoor settings, presence of buildings and landscape, even temperature and humidity play a role.

There are concerns that crudely designed jammers may disrupt the functioning of medical devices such as pacemakers. However, like mobile phones, most of the devices in common use operate at low enough power output (<1W) to avoid causing any problems. Since these jammers actively broadcast radio signals, they may or may not be legal to possess or operate based on the specific laws of the area one is in.

2.3 MOBILE JAMMING AND DISABLERS TECHNIQUES

There are several approaches to prevent mobile phones from ringing in specific areas.The main five approaches used or being developed is described below [2].

1. Type 'A' Device

In this device, we overpower mobile phone signal 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 as those used by cellular / PCS systems' control channels for call establishment.

When active in a designated area, such devices will (by means of RF interference) prevent all pagers and mobile phones located in that area from receiving and transmiting calls. This type of device transmits only a jamming signal and has very poor frequency selectivity, which leads to interference with a larger amount of communication spectrum than originally intended to target. A technologist called Jim Mahan said "There are two types. One is called brute force jamming, which just blocks everything. The problem is, it's like power-washing the airwaves and it bleeds over into the public broadcast area. The other puts out a small amount of interference, and you could potentially confine it within a single cell block. Lots of little pockets of small jamming could be used to keep the facility under control. "

2. Type 'B' Device

This device also called "Intelligent Cellular Disabler devices", and it does not transmit an interfering signal on the control channels. The device basically works as a detector, and is capable of communicating with the cellular base station. When the device detects the presence of a mobile phone in a "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 target user is in a 'quiet' room; therefore, do not establish the communication. Messages can be routed to the user's voice-mail box, if the user subscribes to a voice-mail service.

This process of detection and interruption of call establishment is done during the interval normally reserved for signalling and hand-shaking.

The intelligent device as its name imply can recognise emergency calls and also can allow specific pre-registered users to use their mobile phones for a specified duration. Although this device sounds the best solution for disabling mobile phone, a provision is needed by the cellular / PCS service providers or provision by a third party working cooperative with full support of the cellular / PCS service providers, allowing the detector device to be integral part of the cellular / PCS systems.

3. Type 'C' Device

This device also called "Intelligent Beacon Disablers", as in the Type B device, does not transmit an interfering signal on the control channels.

The device, when located in a specific 'silent' room, functions as a 'beacon' and any compatible terminal is ordered to disable its ringer or disable its operation. In the coverage area of the beacon, only terminals with a compatible receiver would respond, and this should be built on a separate technology from cellular / PCS, for example, bluetooth technology. Also, the handset must re-enable its normal function as it leaves the beacon's coverage area.

The need for intelligent handsets with a separate receiver for the beacon receiver from the cellular/PCS receiver, make effective deployment for the Type C device will be problematic for many years.

4. Type 'D' Device

This jammer is similar to Type A, but with a receiver, so that jammer is predominantly in receive mode and when the device detects the presence of a mobile phone in the 'silent' room; it will intelligently choose to interact and block the mobile phone by transmitting jamming signal. This jam signal would only stay on as long as the mobile continues to make a link with the base station; otherwise there would be no jamming transmission.

Thus this device much 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. Also this technique has an added advantage over Type B in that no added overhead time or effort is spent negotiating with the cellular network.

5. Type 'E' Device

This technique is using EMI suppression techniques to make a room into what is called 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 products one could conceivably implement this into the architecture of newly designed building for so-called "quiet-conference" rooms.

Emergency calls would be blocked unless there was a way to perceive and decode the emergency call transmission, pass by coax outside the room and re-transmitted. This passive configuration is currently legal in most worlds' countries for any commercial or residential location; however some building may not allow this type of construction.

TYPE	EMERGENCY CALL	EFFICIENCY	REGULARITY APPROVAL	IMPLEMENTATION
A	Blocked	Low	Not allowed	Very simple
B	Allowed	Medium	Required	Complex (required third party cellular/PCS services)
C	Allowed	High	Required	Complex (required intelligent handset)
D	Allowed	Medium	Required	Simple
E	Blocked	High (no signal transmitted)	Allowed	Simple

Table 1: Comparison between Jammer/Disabler Techniques

2.4 GSM-MOBILE JAMMING REQUIREMENTS

As discussed earlier, jamming objective is to inject an interference signal into the communications frequency so that the actual signal is completely submerged by the interference. It is important to note that transmission can never be totally jammed. Jamming hinders the reception at the other end. The problem here for the jammer is that only transmitters can be found using direction find and the location of the target must be a specific location; usually where the jammer is located and this is because the jamming power is never infinite.

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

The effects of jamming depend on the jamming-to-signal ratio (J/S), modulation scheme, channel coding and interleaving of the target system.

Generally, jamming-to-signal ratio can be measured according to the following 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,

Gjr= antenna gain from jammer to receiver, Grj=antenna gain from receiver to jammer,

Rtr=range between communication transmitter and receiver,

Br=communication receiver bandwidth,

Lr =communication signal loss,

Pt=transmitter power,

Gtr= antenna gain from transmitter to receiver,

Grt=antenna gain from receiver to transmitter,

Rjr=range between jammer and communication receiver,

Bj=jammer bandwidth, and

Lj=jamming signal loss.

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

The above equation indicates that the jammer effective radiated power, which is the product of antenna gain and output power, should be high if jamming efficiency is required. On the other hand, in other to prevent jamming, the antenna gain toward the communication partner should be as high as possible while the gain towards the jammer should be as small as possible. As the equation shows, the antenna pattern, the relation between the azimuth and the gain, is very important aspect in jamming.

Also as we know from microwave and shown in the equation distance has a strong influence on the signal loss. If the distance between jammer and receiver is doubled, the jammer has to quadruple its output in order for the jamming to have the same effect. It must also be noted, that jammer path loss is often different from the communications path loss; hence gives jammer an advantage over communication transmitters.

In GSM network, the Base Station Subsystem (BSS) takes care of the radio resources. In addition to Base Transceiver Station (BTS), the actual RF transceiver, BSS consists of three parts. These are the Base Station Controller (BSC), which is in charge of mobility management and signalling on the Air-interference between Mobile Station (MS), the BTS, and the Air-interference between BSS and Mobile Services Switching Centre (MSC). The GSM Air- interference uses two different multiplexing schemes: TDMA (Time Domain Multiple Access) and FDMA (Frequency Domain Multiple Access). The spectrum is divided into 200kHz channels (FDMA) and each channel is divided into 8 timeslots (TDMA). Each 8 timeslot TDMA frame has duration of 4.6 ms (577s/timeslot). The GSM transmission frequencies are presented in Table 2.

GSM Type	Uplink (handset transmit)	Downlink (handset receive)	Used in Nigeria by
GSM 900	890-915 MHz	935-960 MHz	Airtel, Glo & Etisalat
GSM 1800	1710-1785 MHz	1805-1880 MHz	Mtn

Table 2: GSM Operating Frequency Bands.

Frequency hopping in GSM is intended for the reduction of fast fading caused by movement of subscribers. The hopping sequence may use up to 64 different frequencies, which is a small number compared to military FH systems designed for avoiding jamming. Also, the speed of GSM hopping is approximately 200 hops/s; so GSM frequency Hopping does not provide real protection against jamming attacks. Although FH doesn't help in protection against jamming, interleaving and forward error correction scheme. GSM systems can protect GSM against pulse jamming. For GSM it was shown that as the specified system SNR_{min} is 9dB, a jammer requires a 5dB S/J in order to successfully jam a GSM channel. The optimum GSM SNR is 12dB, after this point the system starts to degrade.

GSM system is capable to withstand abrupt cuts in Traffic Channel (TCH) connections. These cuts are normally caused by propagation losses due to obstacles such as bridges. Usually another cell could be used to hold communication when the original BTS has disconnected. The GSM architecture provides two solutions for this; First handover when the connection is still available, second call re- establishment when the original connection is totally lost. Handover decisions are made based on transmission quality and reception level measurements carried out by the MS and the BTS. In jamming situations call re-establishment is probably the procedures the network will take in order to re- connect the jammed TCH.

It is obvious that downlink jamming (i.e. jamming the mobile station 'handset' receiver) is easier than uplink, as the base station antenna is usually located far away from the MS on a tower or a high building. This makes it efficient for the jammer to overpower the signal from BS. But the Random Access Channel (RACH) control channels of all BTSs in the area need to be jammed in order to cut off transmission. To cut an existing connections, the jamming has to last at least until the call re-establishment timer at the MSC expires and the connection is released, which means that an existing call can be cut after a few seconds of effective jamming.

The GSM RACH Random Access Scheme is very simple: when a request is not answered, the mobile station will repeat it after a random interval. The maximum number of repetitions and the time between them is broadcast regularly. After a MS has tried to request service on RACH and has been rejected, it may try to request service from another cell. Therefore, the cells in the area should be jammed. In most cases, the efficiency of a cellular jamming is very difficult to determine, since it depends on many factors, which leaves the jammer confused [4].

CHAPTER THREE

DESIGN AND IMPLEMENTATION

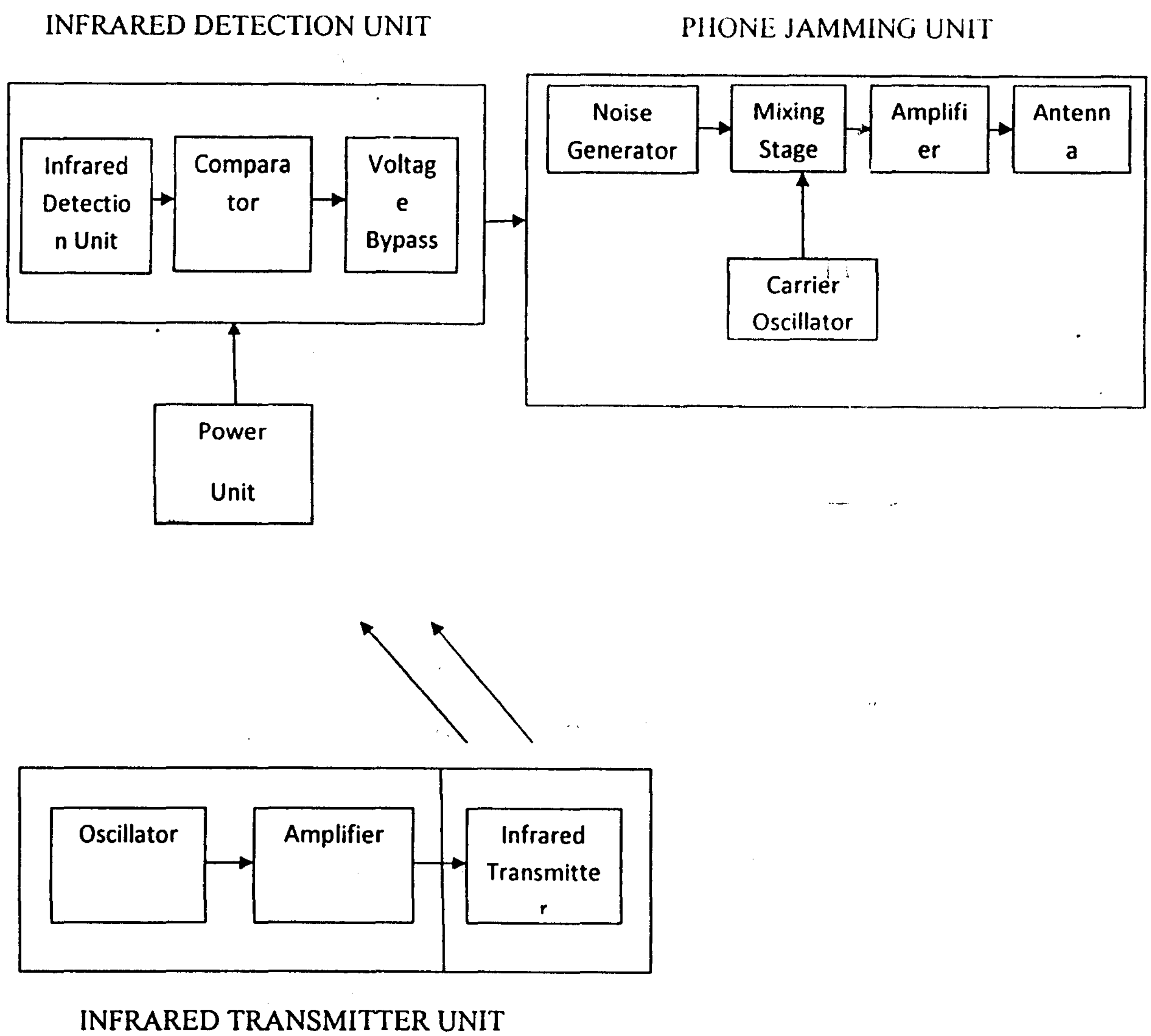


Fig: 3.0 Block Diagram of a Mobile Phone Signal Jammer

3.1 POWER SUPPLY UNIT:

The input to the circuit is applied from the regulated power supply. The a.c. input i.e.

230V from the mains supply is step down by the transformer to 12V and is fed to a rectifier. The output obtained from the rectifier is a pulsating d.c voltage. So in order to get a pure d.c voltage, the output voltage from the rectifier is fed to a filter to remove any a.c components present even after rectification. Now, this voltage is given to a voltage regulator to obtain a pure constant d.c voltage.

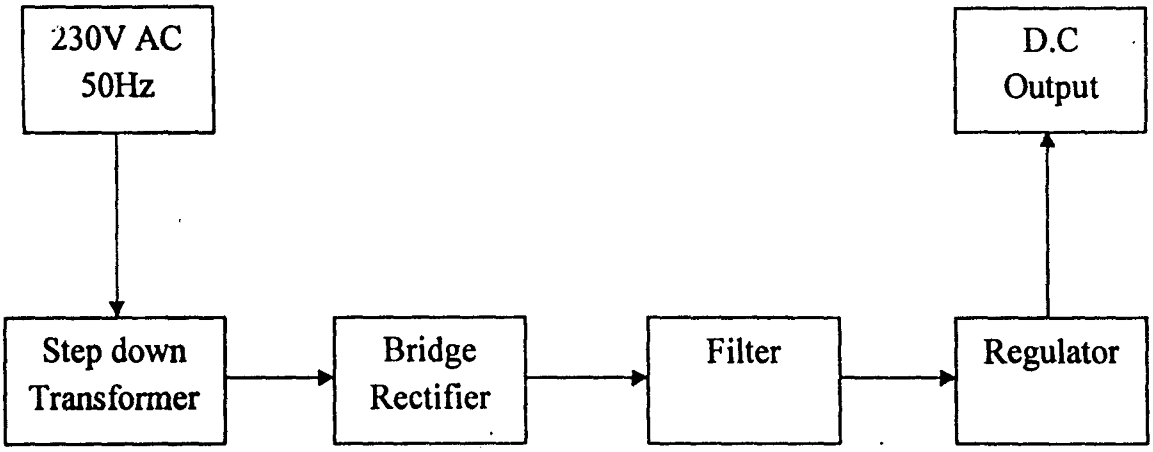


Fig 3.1: Power Supply

3.1.1 TRANSFORMER:

Usually, DC voltages are required to operate various electronic equipment and these voltages are 5V, 9V or 12V. But these voltages cannot be obtained directly. Thus the a.c input available at the mains supply i.e., 230V is to be stepped down to the required voltage level. This is done by a transformer. Thus, a step down transformer is employed to decrease the voltage to a required level.

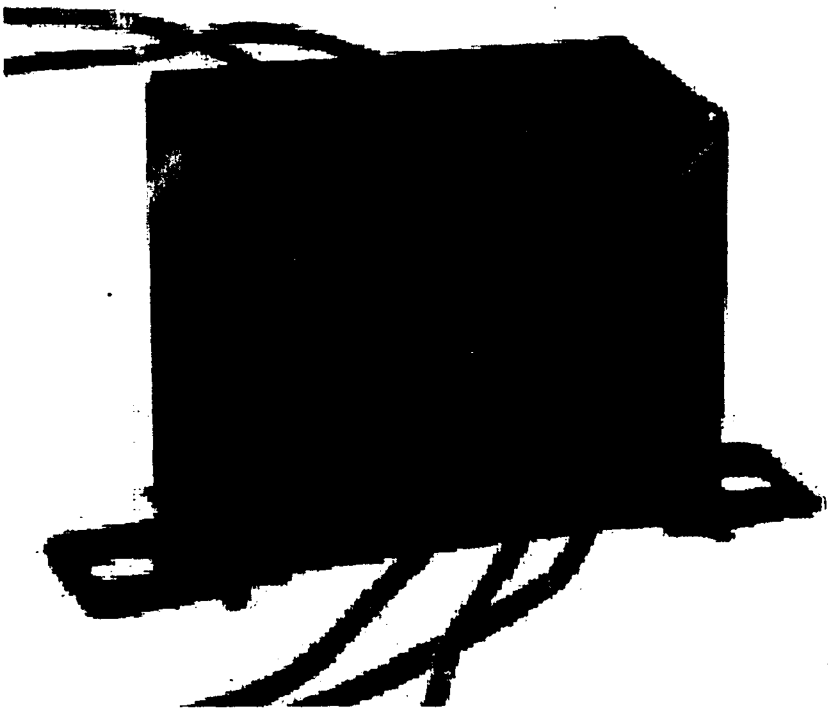


Fig 3.2: Transformer

3.1.2 RECTIFIER:

The output from the transformer is fed to the rectifier. It converts A.C. into pulsating D.C. The rectifier may be a half wave or a full wave rectifier. In this project, a bridge rectifier is used because of its merits like good stability and full wave rectification.

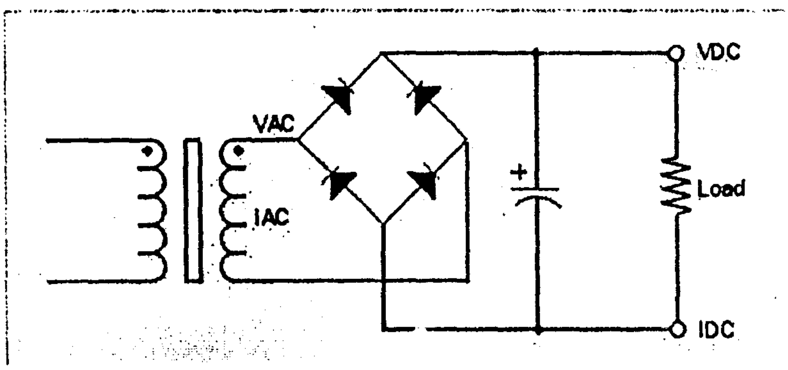
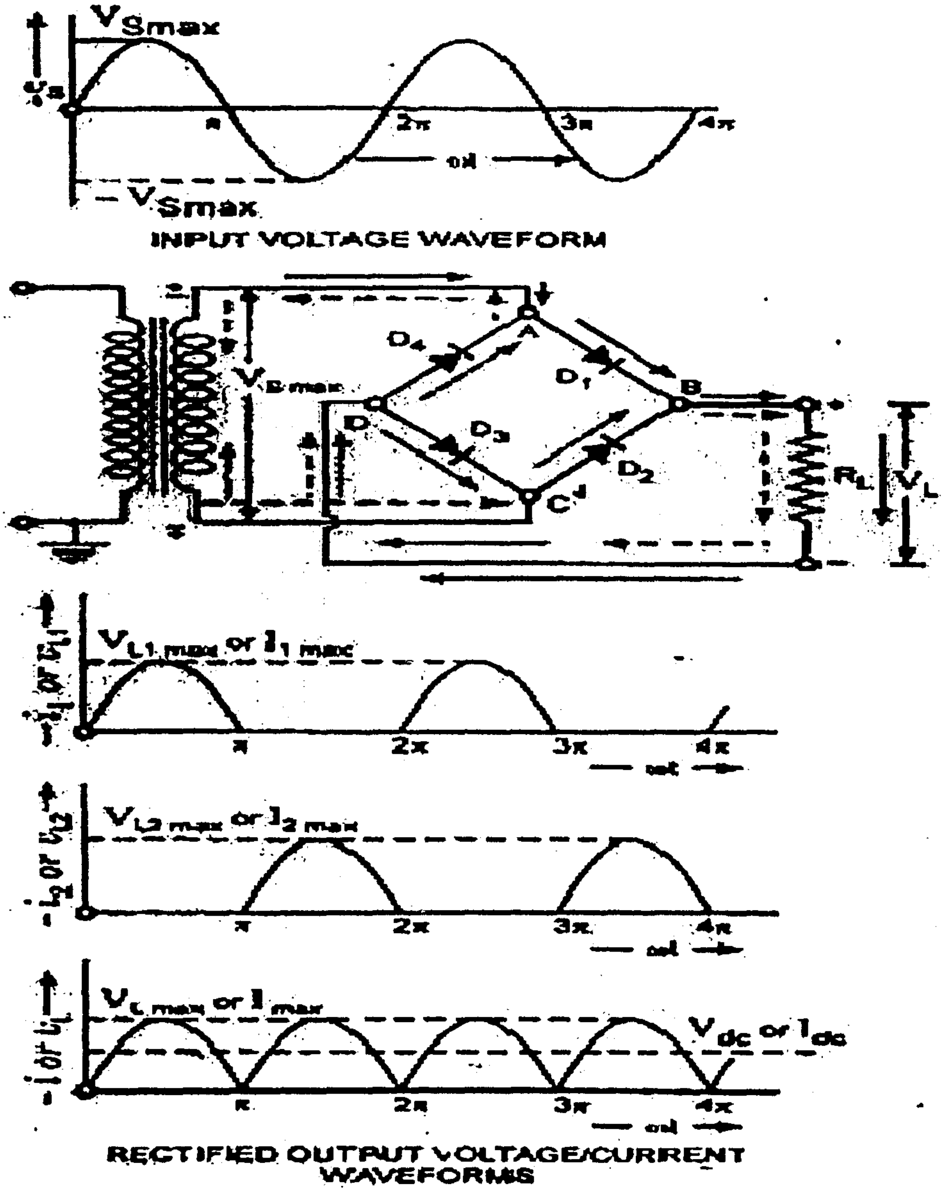


Fig 3.3: Bridge Rectifier

The bridge rectifier is a circuit, which converts an ac voltage to dc voltage using both half cycles of the input ac voltage. The Bridge rectifier circuit is shown in the figure above. The circuit has four diodes connected to form a bridge. The ac input voltage is applied to the diagonally opposite ends of the bridge. The load resistance is connected between the other two ends of the bridge.

For the positive half cycle of the input ac voltage, diodes D1 and D3 conduct, whereas diodes D2 and D4 remain in the OFF state. The conducting diodes will be in series with the load resistance RL and hence the load current flows through RL.

For the negative half cycle of the input ac voltage, diodes D2 and D4 conduct whereas, D1 and D3 remain OFF. The conducting diodes D2 and D4 will be in series with the load resistance RL and hence the current flows through RL in the same direction as in the previous half cycle. Thus a bi-directional wave is converted into a unidirectional wave.



Bridge Rectifier

Fig: 3.4(a)

3.1.3 FILTER:

Capacitive filter is used in this project. It removes the ripples from the output of the rectifier and smoothens the D.C. Output received from this filter is constant until the mains voltage and the load is maintained constant. However, if either of the two is varied, D.C. voltage received at this point changes. Therefore a regulator is applied at the output stage.

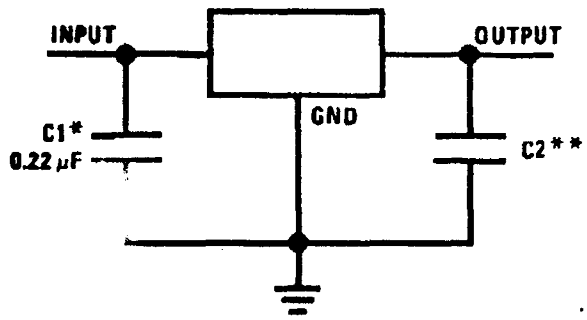


Fig: 3.5 Capacitive Filter

3.1.4 VOLTAGE REGULATOR:

As the name itself implies, it regulates the input applied to it. A voltage regulator is an electrical regulator designed to automatically maintain a constant voltage level. In this project, power supply of 5V and 12V are required. In order to obtain these voltage levels, 7805 and 7812 voltage regulators are to be used. The first number 78 represents positive supply and the numbers 05, 12 represent the required output voltage levels. The L78xx series of three terminal positive regulators is available in TO-220, TO-220FP, TO-3, D2PAK and DPAK packages and several fixed output voltages, making it useful in a wide range of applications.

These regulators can provide local on-card regulation, eliminating the distribution problems associated with single point regulation.

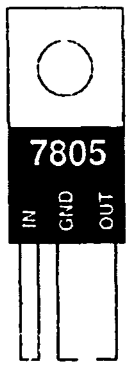


Fig: 3.6 Voltage Regulator

Each type employs internal current limiting, thermal shut-down and safe area protection, making it essentially indestructible. If adequate heat sinking is provided, they can deliver over 1A output current. Although designed primarily as fixed voltage regulators, these devices can be used with external components to obtain adjustable voltage and currents.

3.2 NOISE GENERATOR

It generates a noise signal and it is mixed with the triangle wave signal. This noise will help in masking the jamming transmission, making it look like random "noise" to an outside observer. Without the noise generator, the jamming signal is just a sweeping, unmodulated continuous wave RF carrier.

3.3 MIXER

The input to this mixer is a triangle wave and a random "noise" signal. These signals are mixed to form a new, "noisy" triangle waveform. When applied to the VCO, the resulting RF signal will "sweep" across the cellular downlink frequencies, and will be Frequency Modulated (FM) with the noise signal. This noise modulation helps to increase the jammers effectiveness.

Another thing op-amp performs is to provide a DC offset for the VCO's voltage tune pin. What this does is give the triangle wave a positive DC voltage offset to help "center" the triangle wave within the required frequency range.

3.4 VOLTAGE CONTROLLED OSCILLATOR

The voltage controlled oscillator is the most important component in a cellular jamming system. It is an electronic oscillator designed to control oscillation frequency by a voltage input. It is little four-terminal device (Power, Ground, RF Output, and

Voltage Tune) which generates the required, low-level RF output signal. The output from VCO is fed to RF amplifier for further amplification.

3.5 RF AMPLIFIER

It is a device which may take a small RF signal and amplify it. The cheap & easiest source of these amplifiers is from old cellular phones themselves. Some cellular phones will use broadband RF power "hybrid" modules which help to make their construction easier and smaller. These RF module devices tend to be very wide banded, and will easily amplify RF signals outside of their intended range. Increasing the module's bias, power control, or V_{dd} voltage can also milk a little more gain out of them. The modules will need to be connected to a large, smooth heat sink and may also require a cooling fan.

3.6 ANTENNA

Antenna, also referred to as an aerial, is a device used to radiate and receive radio wave through the air or through space. Antennas are used to send radio waves to distant site and to receive radio waves from distant sources.

Many wireless communication devices, such as radio broadcast television sets, radar and cellular telephones use antenna. The antennas used here are generated by electrical signals inside this device and convert them to waves that travel in an open space to distort the specified signals in transmission. It is a piece of tube into which alternating current can be passed and whose function is to radiate electromagnetic radiator into space.

An antenna serves two major functions, first it acts as an impedance matching device to match the impedance of the transmission medium to that of free space and direction or suppresses the radiation unto other directions where it is not desired. Antenna radiates most effectively when their length is directly related to the wavelength of the transmitted signal. It can be noted that the effective area of transmitter antenna is given by

$$A_{eff} = \lambda^2 G_T / 4\pi$$

where G_T is the antenna gain

λ Is the wavelength.

CALCULATIONS

Infra Red Diode

$irradiant = {}^{W}/_{A}$

Power transmitted per unit area = ${}^{7mW}/_{4\pi r^2}$

$= 7x10^{-3}/4\pi \times 400^2 = 3.48nW/cm^2$

If the active area of the photo receiver = 2×10^{-3}cm,

Therefore, power received = A × H

$= 2 \times 10^{-3}cm \times 3.48 \times 10^{-9}W/cm$

$= 6.96 \times 10^{-12}W$

Therefore, photocurrent in Amps = Power x Responsitivity

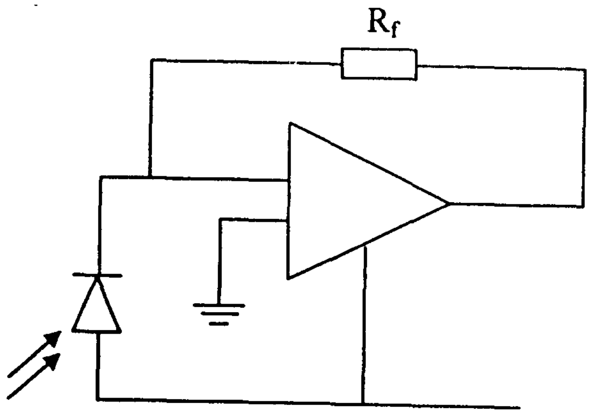
$I_p = P \times R_{\phi}$.

where responsitivity = 0.5μA/μW

$I_p = 6.96 \times 10^{-12} \times 0.5 = 3.48 \times 10^{-12}A$

For The First Operational Amplifier,

Output voltage = $I_p \times R_f$



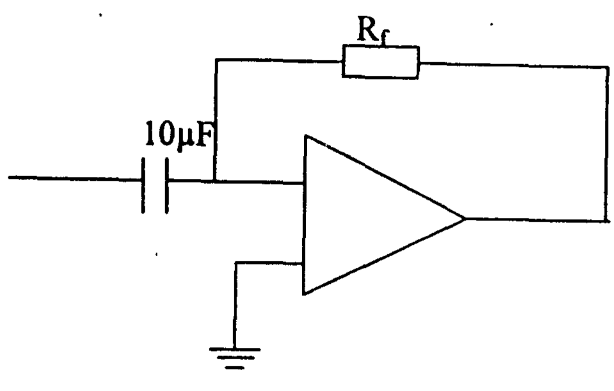
$V_0 = 3.48 \times 10^{-12} \times 1 \times 10^{6}$

$= 3.48 \times 10^{-6}$V.

Therefore the output voltage, V_o at the first op-amp is 3.48×10^{-6}V.

For The Second Operational Amplifier,

The transmitter operates at 30KHz frequency.



Reactance of 10µF = 1 / 2πfc

$= 1 / 2 \times 3.142 \times 30 \times 10^{3} \times 10 \times 10^{-6}$

= 1.9Ω.

$Gain = R_f / R_i = 1 \times 10^6 / 1.9 = 526.3 \times 10^3$

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

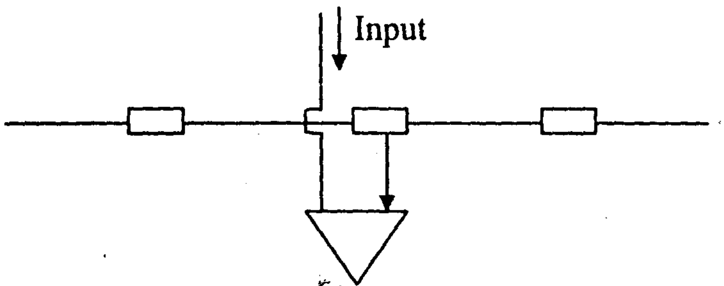
$V_{out} = V_{in} \times 526.3 \times 10^3$

$Vout = 3 \times 10^{-9} \times 526.3 \times 10^3$

$= 0.0$[illegible] V

Comparator

At the comparator, the voltage was compare between the input voltage and the real voltage

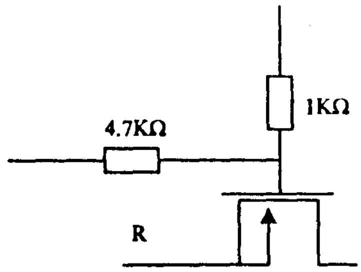


The gain of the comparator [illegible]0,000

If gain is 10,000; $V_{out} = V_R \times gain$

$V_{out} = 0.0015 \times 10,000 = 15V$

Therefore the real voltage is just 12V; it will rise and amplify the voltage to 12V of the real. The 12V was delivered to the field effect transistor, which was acting as a by-pass transistor.



The voltage input = $V_{in} \times R1 / R2 + R1$

$= (12V \times 4.7K\Omega) / (4.7K\Omega + 1\ K\Omega)$

$= 9.8V$

Therefore, 9.8V was used to switch ON the MOSFET, which in return by-pass 12V to the cell phone jamming circuit.

Jamming Circuit

The noise generator produces 45MHZ which was fed to the high frequency oscillator which is operating at 1.5GHZ; therefore the signal will be modulated.

If noise generator = modulation with high frequency

$V_c = V_c \cos 2\pi f_c t = V_c \cos\omega_c t$

where V_c = sinusoidal voltage signal

and fc = frequency.

Therefore, let the modulating signal of amplitude V_m and frequency F_m to be represented by

$V_m = V_m \cos 2\pi f_m t = V_m \cos\omega_m t$

Therefore from the definition of amplitude modulation, the amplitude of the amplified modulation AM wave,

$V_{AM} = V_c t + KV_M(t)$

$= Vc + KV_M \cos w_m t$

where K is a proportionality constant and circuit parameter.

Therefore, the instantaneous voltage of Am signal is

$V_{Am}(t) = V_{Am} \cos w_c t$

$= (V_c t\ KV_m \cos w_m t).\ \mathrm{Cos}\ w_c t$

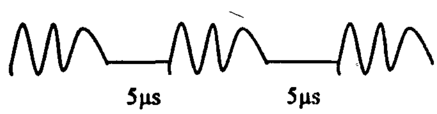
Time for noise tank circuit to regenerate is equal to RC

That is $T = R \times C$

Therefore $T = 100 \times 10^3 \quad \times 50 \times 10^{-12} = 5 \times 10^{-6}$

$= 5\mu s.$

It takes 5μs for the frequency of the tank circuit to regenerate.



V_{out} of the carrier oscillator at ON time

$12 \times 10M\Omega / 10M\Omega + 100K\Omega = 12 \times 10 \times 10^6 / 10 \times 10^6 + 100 \times 10^3$

Input voltage $= V_b = 11.8V$

If $I_b = Vcc - 0.67v / R_1 + \beta \times R_2$

$12 - 0.67 / 100K\Omega + 300 \times 100$

Therefore $I_b = 12 - 0.67 / 130{,}000 = 87 \times 10^{-6}A$

$V_R = 87 \times 10^{-6} \times 100 \times 10^3 = 8.7V$

Therefore, $V_b = 11.8 - 8.7 = 3.08V$

3.08v was used to switch ON the transistor of the carrier frequency.

Gain

Since it is a common emitter amplifier,

Gain $= -R_{CN} / (r_e + R_E)$

where R_{CN} = total resistance between collector and ground

r_e = dynamic resistance

R_E = emitter resistance

$R_{CN} = R_C // r_{ce} // R_L$

$R_C = X_L = 2\pi ft = 2\pi \text{ x } 105 \text{ x } 10^9 \text{ x } 83 \text{ x } 10^{-9} = 54.7K\Omega$

$r_{ce} = 100\ K\Omega$

$R_L = 47K\Omega$

$R_C // r_{ce} = 54.7 // 100 = 35.4K\Omega$

$35.4K\Omega\ // R_L = 35.4K\Omega // 47K\Omega = 20.2K\Omega$

$R_{CN} = 20.2K\Omega$

Dynamic resistance, $r_e = 2.6 \times 10^{-3} v/I_E$

$I_b = V_{CC} X 0.7 / (100 + \beta + 100) = 12 \times 0.7 / (100 + 300 + 100) = 87 \times 10^{-6} A$

$I_C = I_b \times \beta = 87 \times 10^{-6} \times 300 = 0.0261 = 26.1mA$

$I_C = I_E$

$r_e = 2.6 \times 10^{-3} / 26.1 \times 10^{-3} = 0.099 = 0.1\Omega$

$R_E = 100\Omega$

$Gain = -R_{CN}/(r_e+R)_E = -20.2 \times 10^3 / (0.1 + 100) = -201.8$

Second Amplifier Stage

$I_b = 12V / (220 \times 10^3) = 54 \times 10^{-6} A$

$I_C = I_b \times \beta = 54 \times 10^{-6} \times 300 = 0.016 = 16mA$

Since $V_O = 12V$,

$Power = 12 \times 16 \times 10^{-3} = 0.192W$

i.e. a signal of 0.192Watt was transmitted.

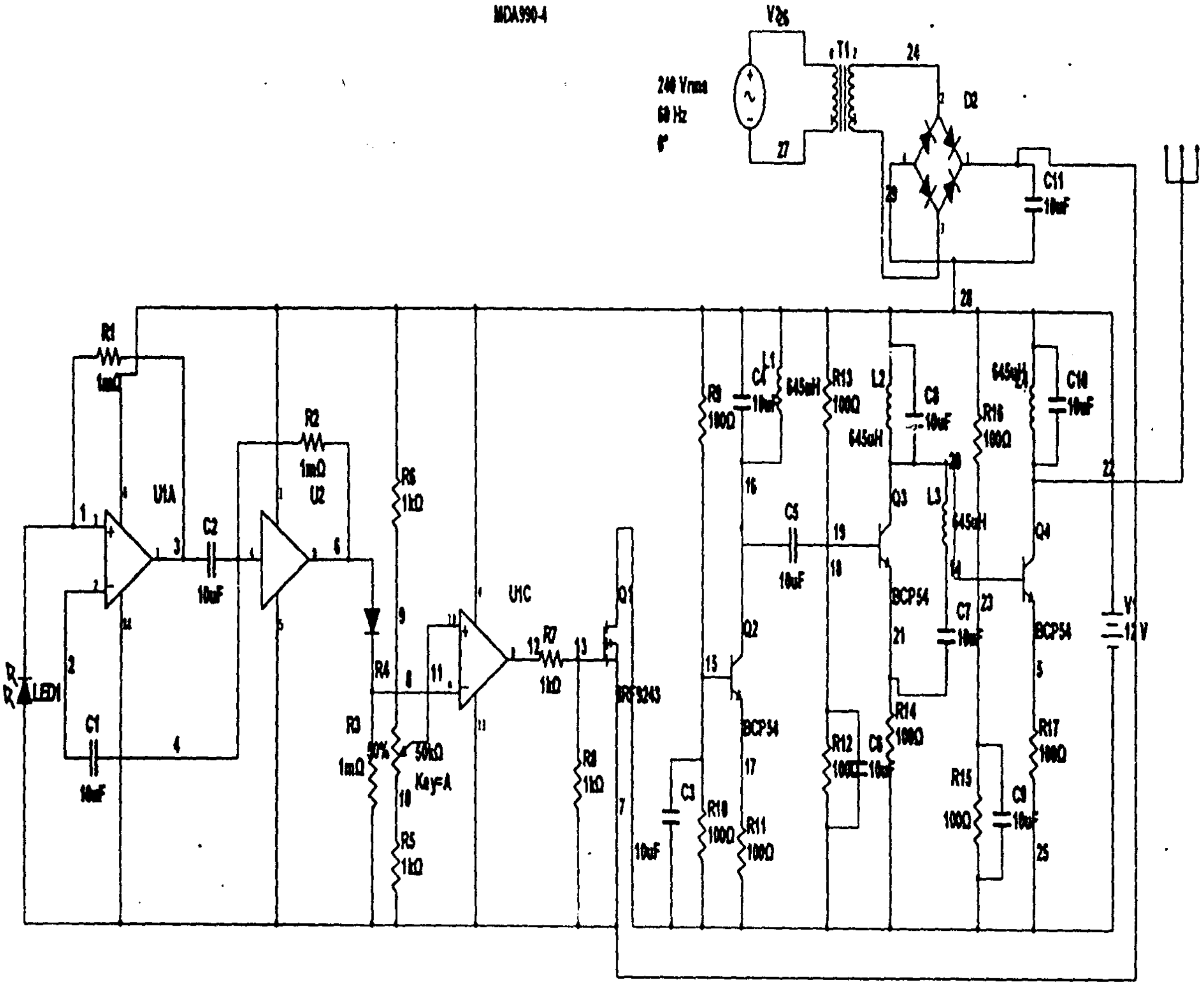


Fig: 3.7 Complete Circuit Diagram of a Mobile Phone Signal Jammer

CHAPTER 4

4.1 RESULT

- The circuit is carefully and correctly connected as shown in the circuit diagram fig. x above with its power source switched off.
- A mobile phone (GSM) is brought close to the area where the jamming circuit is to be tested.
- The network service in the handset (GSM) is confirmed by physically observing the network service in the handset through the screen of the handset.
- The network service in the GSM is also confirmed by dialling a number from the GSM phone A or by receiving a call from another GSM phone B which could either be within or outside the area where the GSM phone A is.
- A call made or received from the GSM phone A, confirmed the presence of network service in the phone.
- Switch ON the jamming device: When the jamming device is switched on, it will be observed that the network service which was on the GSM disappears with an inscription "emergency call only" on the GSM phone screen. This, therefore, shows that the signal or service in the GSM phone has been blocked or interfered with.

4.2 TEST.

While the jamming device is still on, try to make a call with the GSM phone A from the area where the jamming device is, it will be observed that call making within the jamming area will be impossible.

With the jamming device still on, if a second GSM phone B outside the jamming area tries to reach or call the other GSM phone A that is in the jamming area, it will be observed that the GSM phone A will not respond to the incoming call from GSM phone B, hence GSM phone A signal has been jammed.

4.3 OBSERVATIONS

In the cause of testing the mobile phone signal jamming device, it was observed that the jamming device, jammed/interfered with the TV transmitting signal (frequency) and some frequency bandwidth in a radio receiver was also observed to be blocked by the jamming device.

4.3.1 OBSERVATION PROCEDURE

- Switch on a TV.
- Bring the jamming device close to where the TV is and ensure that the device is off
- While a TV show (program) is in progress, switch on the jamming device.
- The ongoing TV show will be observed to stop transmitting.
- The TV show will start transmitting again when the jamming device is switched off.

- The jamming effect of the jammer was observed to reduce with distance i.e. the strength of the jamming device is inversely proportional to the distance between it and the jammed device (GSM). The longer the distance between jamming and the jammed devices, the less effective the jamming will be, while the lesser the distance between the jamming device (mobile phone jammer) and the jammed device (GSM phone) the more effective the jamming will be.

4.4 LIMITATIONS

The mobile phone signal jammer was primarily aimed at blocking mobile phone frequency. The blocking of TV, radio and other receivers whose frequencies fall within the jamming operating frequency was not intended.

Therefore, with the above drawback, the use of mobile phone jammer is limited to places where TV, radio, and other devices that operate within the frequency of the jammer device are not allowed.

The mobile phone jamming device could also be used as a parental control device, used by parents to control the type of TV programmes their children watch.

CHAPTER 5

5.1 CONCLUSION

A mobile phone signal jammer is a device that is used to interfere with a mobile phone frequency or used to restrict the use of mobile phone in some quiet required area e.g. churches, mosques, meeting rooms, lecture halls etc

Jamming of mobile phone frequency is achieved by sending a noise signal with frequency equal to or a bit greater than the transmitting frequency of the network service which is been used by the mobile phone. The strength of the jamming device, increase with decrease in the distance between the jamming device and the phone, and also decrease with increase in the distance between the jamming device and the phone to be jammed.

The mobile phone jamming device can interfere with the TV, radio, etc frequency which was not intent; this can therefore be seen as a disadvantage in the use of mobile phone signal jammer because this limits the areas where the device can be use. This jamming device can also jam TV frequency and hence could be use as a parental control device.

5.2 RECOMMENDATION

The following are recommended for further works

- A printed circuit board should be used instead of the Vero board.
- For effective jamming, higher frequency components should be used.

- Long distance jamming IC could be used to generate higher frequency for a wider bandwidth and greater range of jamming.

REFERENCE

1. Telecommunication Principle and System by Y.A Adediran, Federal University of Technology, Minna. ISBN 978-33101-3-5

2. Mobile and Personal Communication 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/files01

3. Pozar D.M, Microwave Engineering. John Wiley and Sons 2005

4. Dr Nihad Dib and Ahmed Jisrawi, "GSM 900 Mobile Jammer" 2006.

5. "Frequency Planning and Frequency Coordination for the GSM 900, GSM 1800, E- GSM and GSM-R Land Mobile Systems (Except Direct Mode Operation) (DMO) channels)" by Working Group Frequency Management. (WGFM).

6. John Scourias, Overview of the Global System for Mobile Communications

   http://ccnga.uwaterloo.ca/-jscouria/GSM/gms report.html

7. Design and Construction of Mobile Signal Jammer by Okezie David Chekwe; Undergraduate Project, FUT Minna, Nov 2010.

8. en.wikipedia.org/Mobile Phone Signal Jammer.

9. Telecommunication Switching, Traffic and Networks by J.E Flood

10. Electronics Communication Systems by George Kennedy.

11. Ahmad N. R. M. and Ahmad S. H. A. 'Dual Band Mobile Jammer for GSM 900 and 1800'.