

DUAL BAND GSM MOBILE JAMMER USING ACTIVE DENIAL OF SERVICE TECHNIQUE FOR NIGERIAN GSM NETWORK

By

Isizoh A. N.¹

Alagbu E.E.²

Dept. of Electronic and Computer Engineering,
Nnamdi Azikiwe University, Awka, Nigeria.

Dept. of Electronic and Computer Engineering,
Nnamdi Azikiwe University, Awka, Nigeria.

ABSTRACT

The ubiquity of cell phones has made communication easier and faster, integrating the world into a global village as people who are in different geographical locations are connected within seconds. There is great need to limit the use of cell phone at a particular place and at a particular time. Hence, the use of a GSM jammer is necessitated. This paper highlights the design of a low-cost dual band GSM mobile jammer and solves the problem of inappropriate use of cell phones in restricted areas. The design employs a technique known as Active Denial of Service, where a noisy interference signal is constantly radiated into space and the environment of interest, over a target frequency band and at a desired power to cover a defined area. The construction of the jammer involves the design of a frequency generator, which produces a set of signal frequencies (noise), and then the amplifier, which raises the frequencies, generated to a range of 900 MHz to 1.9 GHz in order to match the frequency of the mobile phone operator being transmitted by the base station. Thus, satisfactory jamming of the mobile signals was confirmed by the blocking of the signals of the mobile phones operated via MTN, Airtel, Globacom and 9 Mobile service providers in Nigeria. The phones indicated “no network” and as such allowed no call with no interference to other communication gadgets.

Keywords: Bearer Channel, Base Transceiver Station (BTS), Denial of Service, Digital Cellular System, Enhanced Data Rates for Global Evolution.

1. INTRODUCTION

Telecommunication industry over the past decades has witnessed an exponential growth in telephony,

especially mobile telephony. The dramatic rise in the use of wireless communication devices such as mobile phones, Personal Digital Assistants (PDA), and many others can be attributed to their portability and thus have become indispensable in people’s lives. The convenience and portability of mobile phones has made it possible for it to be carried everywhere; in Mosques, Churches, Libraries, Conference halls and Examination halls etc. The numerous advantages of mobile phones cannot be overemphasized; however, their convenience can create inconvenience in some public places where a considerable amount of silence is needed. Also in certain locations, the use of mobile phones is prohibited for security and safety reasons and their use in such places can be of serious detrimental effect [1].

The inconvenience is mostly due to the incessant noise generated from the ring tones of users; also certain jurisdictions do not permit the exchange of information using mobile phones as long as users are within the jurisdiction. A way of preventing users from getting access to their phone’s service is to install a device known as a mobile phone jammer.

Jamming is the radiation of electromagnetic energy in a communication channel which reduces the effective use of the electromagnetic spectrum for legitimate communications [2]. A GSM mobile jammer is a device which transmits (radiates) noise induced signals at the same frequency range as a mobile, thus rendering mobile phones in the specific location unusable. Global System for Mobile Communication (GSM) is a second generation cellular standard developed to offer voice, data and video services. The frequency band for GSM ranges from 380MHz to 1900MHz, with most mobile operators using the 900MHz to 1800MHz range.

The technology behind the mobile jammer is that the jamming device broadcasts a Radio Frequency (RF) signal in the frequency range reserved for cell phones; these signals interfere with the cell phone signal, which results in a “no network available” displayed on the cell phone screen. All phones within the effective radius of the jammer will lose the tendency to make or receive calls, as long as they are within that radius [3].

The aim of this research is to design and implement a dual band GSM mobile jammer using the technique known as Active Denial of Service.

The system is a dual band mobile jammer, which focuses on blocking the signal transmission of the GSM 900, which has a frequency range of 935 – 960MHz and the Digital Cellular System (DCS) 1800, which has a frequency range of 1805 – 1880MHz.

Significance of the Research

The increased, incessant and alarming rate at which mobile phones are used during lecture hours can easily be pointed out as one of the factors affecting the poor academic performance students of various institutions. The improvised smart technique which students use in various forms of exam malpractices by which mobile phones are employed need to be curtailed using the GSM mobile jammer.

Likewise, communication between mobile stations can serve as a means of detonating improvised explosive devices (IEDs), a technique that is applied by both veteran and amateur terrorists; this is a major threat to life and property and it is experienced worldwide. Since a mobile phone jammer proves to be effective way to jam the mobile-air interface, they are useful in the following places: university lecture rooms, libraries, concert halls, meeting rooms, police stations, VIP protection, checkpoints, perimeter borders, exam halls, board rooms etc.

Thus, the significance of a GSM mobile jammer can be summarized in three (3) categories: security, education and discipline.

Jamming Technology

The coming of the information age brought about a considerable reliance on wireless electronic

The main limitation of the work is that the device can only jam the four main service providers, which are MTN Nigeria, Globacom, Airtel and 9 mobile. This is because, these lines are only for Nigerian users and the frequency band range is between 900 – 1900MHz. These requirements fulfill the GSM900 and DCS 1800 specifications.

Another limitation of the research is that the jammer struggles to jam the mobile signal frequency when it is being transmitted in the 3G, 3.5G and 4G LTE. This is probably because these technologies operate at a relatively higher frequency than the stipulated frequency range for the GSM 900 and DCS 1800.

The system will prevent cellular phone from transmitting and receiving mobile signals to and from the base station.

communication. Although cellular phone systems and personal communication systems have brought wireless radio frequency (RF) communications to the masses, nowhere is this reliance observable than in the military. For decades, the military had hinged on RF communications for the execution of command and tactical forces. An adversary has interest in these communications, since tactical commanders use RF communication to exercise control of their forces. This interest lies in two primal areas;

- (i) To intercept the information that transpires over them and
- (ii) To deny the successful exchange of the information from the sender to the receiver.

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

affected stations usually change frequencies, put on additional frequencies and/or increase transmission power. During World War II ground radio operators would attempt to mislead pilots by false information in their own language, in what was more precisely a spoofing attack than jamming [4].

Radar jamming is also important to disrupt use of radar used to guide an enemy's missiles or aircraft. Modern secure communication techniques use such methods as spread spectrum modulation to resist the deleterious effects of jamming. Jamming has also occasionally been used by the Governments of Germany (during World War II), Israel, Cuba, Iraq, Iran (Iraq and Iran war, 1980-1988), China, North and South Korea and several Latin American countries, as well as by Ireland against pirate radio stations such as Radio Nova. The United Kingdom government used two coordinated, separately located transmitters to jam the offshore radio ship, Radio North Sea International off the coast of Britain in 1970 [5].

Difference between Jamming and Interference

These terms are used interchangeably, but in recent times most radio users use the term “Jamming” to describe the deliberate use of radio noise or noise induced signals in an attempt to disrupt communication (or prevent listening to broadcast) whereas, the term “interference” is used to describe unintended or unwanted forms of disruption. The latter is far more common than the former [6].

Mobile Jamming and Disabling Techniques

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

Type “A” Device (Jammers)

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

Radio Frequency (RF) interferences preventing mobile phones and even pagers located within its area of broadcast the ability to transmit and receive calls. There are two types; the brute force jamming, which jams everything. The other puts out a small amount of interference, and you could potentially confine it within a single cell block.

Type “B” Device (Intelligent Cellular Disablers)

This device is also known as “Intelligent Cellular Disablers”. It does not transmit an interfering signal on the control channels. The device basically works as a detector. This device works by communicating with the nearest cellular base station. When the device detects the presence of a mobile phone in the room it operates (“silent room”), a prevention of authorization of call establishment is done by the software, at the base station. The device signals the base station that the user is in a “quite room”, and hence does not establish the target communication. This process of detection and interruption of call establishment is done during the interval normally reserved for signaling and handshaking. This intelligent device as its name implies can recognize emergency calls and also allow specific pre-registered users to use their mobile phones for a specified duration. Though this device sounds like a good solution, a provision is needed by the cellular/pcs service providers, allowing the detector device to be an integral part of the cellular/pcs systems.

Type “C” Device (Intelligent Beacon Disablers)

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

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

This jammer works similar to type “A”, but with a receiver, so that the jammer is predominantly in receive mode, and when it detects the presence of a mobile phone in the “silence” area, it will intelligently choose to interact and block the cell phone by transmitting a jamming signal. This jamming signal would only remain on, so long as the mobile continues to establish contact with the base station, otherwise there would be no jamming transmission. The advantage of type “D” against “A” is that “D” emits less electromagnetic pollution in terms of raw power transmitted and frequency spectrum from the type “A” jammer, and therefore much less disruptive to passing traffic. This technique could be implemented without cooperation from Cellular/PCS providers. Again, this technique has an added advantage over type “B” in that no added overhead or effort is spent negotiating with the cellular network [7].

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

This technique uses electromagnetic interference to make a room into what is known as a faraday cage. Faraday’s cage essentially blocks, or greatly attenuates virtually all electromagnetic radiations from entering or leaving the cage. The cage ranges from as small as a room to a whole building. With current advances in EMI shielding techniques and commercially available products, one could conceivably implement this into the architecture of newly designed buildings for so-called “quiet” conference rooms.

GSM Jamming Requirements

The idea behind jamming is to introduce noise induced signals (interference) into the communications channel so that the actual signal is completely overwhelmed by the interference. However, it should be noted that a signal can never be totally jammed, rather the jammer only impedes the reception at the other end. Jamming is successful only when the signal induced in the communications channel is able to limit the usability of the communications channel. In digital communication, the effectiveness of the

channel is impeded only when the error rate of transmission cannot be compensated by error correction. For a jamming attack to be successful, the power of the jammer should be roughly equal to the signal power at the receiver. The effectiveness of jamming depends on the Jamming-to-Signal ratio (J/S), modulation scheme, and channel coding and interleaving codes of the target system [8].

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

$$\frac{J}{S} = \frac{P_j G_{jr} G_r R_{tr}^2 L_r B_r}{P_t G_{tr} G_{rt} R_{jt}^2 L_j B_j} \dots\dots\dots (1)$$

Where:

- P_j = Jammer Power
- P_t = Transmitter Power
- G_{jr} = Antenna Gain (Jammer to Receiver)
- G_{rj} = Antenna Gain (Receiver to Jammer)
- G_{tr} = Antenna Gain (Transmitter to Receiver)
- G_{rt} = Antenna Gain (Receiver to Transmitter)
- B_r = Communications Receiver Bandwidth
- B_j = Jamming Transmitter Bandwidth
- R_{tr} = Range between communications transmitter and receiver
- R_{jt} = Range between jammer and communications receiver
- L_j = Jammer signal loss (including polarization mismatch)
- L_r = Communication signal loss

The above equation indicates that the jammer’s effective radiated power, which is the product of antenna gain and output power, should be high if jamming efficiency is required [9]. As the equation shows, the antenna pattern, the relation between the azimuth and the gain, is a very important aspect in jamming. To successfully jam a particular region, we need to consider a very important parameter, the Signal-to-Noise Ratio, referred to as the SNR. Every device working on radio communication principles can only tolerate noise in a signal up to a particular level. This is called the SNR handling capability of the device. Most

cellular devices have a SNR handling capability of around 12dB. A very good device might have a value of 9dB, although it is highly unlikely. To ensure jamming of these devices, we need to reduce the SNR up to 9dB.

II. METHODOLOGY

To every functional device or system, there must be a process or series of processes to undergo in designing it; to every process, there are procedures or steps to it as well. This research does not involve the construction of individual components (such as the VCO, Antenna, RF Amplifier etc.) of the system from scratch for certain reasons explained. Nevertheless, the design methodology of this research draws feed from the actual systematic approach for engineering design and implementation (i.e. computer simulations and hardware designs).

After an extensive study of the various techniques of jamming and consequent review of previous works by past authors and scholars, the choice of the type “A” device also known as Denial of Service (DOS) was settled on. It involves transmitting noise induced signals on the same frequency as the frequency band used.

Design Specification

The beginning of every system design process is based on the design specification of each main part of the system i.e. the choice of each part chosen because it serves as a guide during the course of design.

Though it serves as a guide, it can still be changed (modified) especially when difficulty is encountered at the long run of the entire design process. Design specification as it concerns this research will be discussed based on the following headings: functional, power and physical structure specification.

1. Functional specification:

Discrete components like inductors, capacitors, transistors etc. were used in the construction of the project. The major components like the Voltage Controlled Oscillator (VCO), The Radio Frequency Amplifiers and the Antennas were used together with the inductors, capacitors, transistors etc. to generate a frequency high enough to jam the intended frequencies of the mobile subscribers.

2. Power specification:

Having considered the voltage and current consumption of the individual main components, a conclusion was reached that the power source of this system will be an AC supply. Since all the major parts of this system requires a maximum of 5V D.C supply, AC mains is therefore appropriate. The major components of the system, such the Radio Frequency Amplifier, consume a lot of power and as such would easily drain a DC power supply. The system uses an AC Adapter that works on the Switch Mode Power Supply Principle (SMPS).

3. Physical structure design:

With respect to the significance of this research, starting with the internal structure, the circuit board is of the Vero board format, because of its convenience in miniaturizing the circuit size. The discrete components are mounted on the board during construction.

Block Diagram of a GSM Jammer

The block diagram of a GSM Jammer is shown in figure 1.

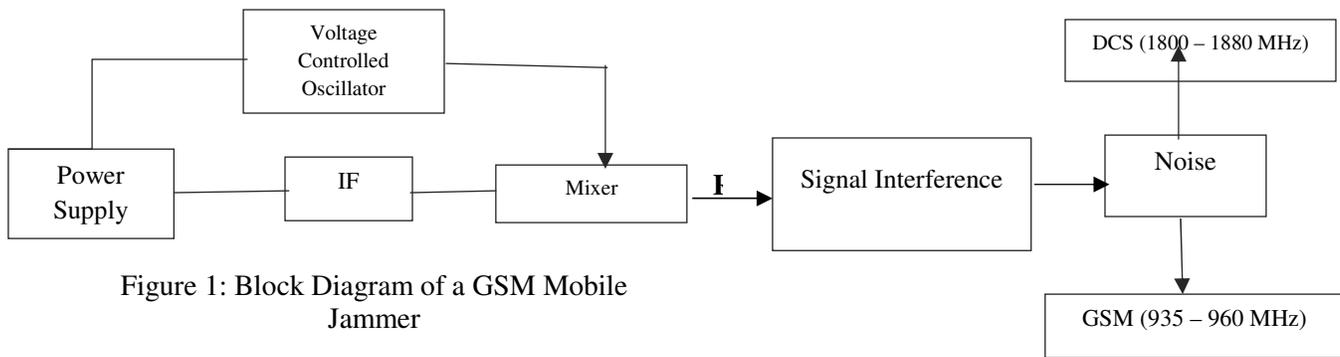


Figure 1: Block Diagram of a GSM Mobile Jammer

The block diagram helps to analyze each block or main part of the circuit so that one can effectively select other minor circuit components suitable to drive each of the main components according to their individual data sheet. The electrical interconnection of the entire system components and their physical layout were done using Proteus 8 professional (ISIS schematic capture).

Design Simulation

This is where the developed circuit diagram is being simulated using a schematic capture tool known as Proteus Virtual System Modeling. The essence of this simulation is to ascertain with fact the real-life work-ability of the developed circuit diagram, shown in figure 2.

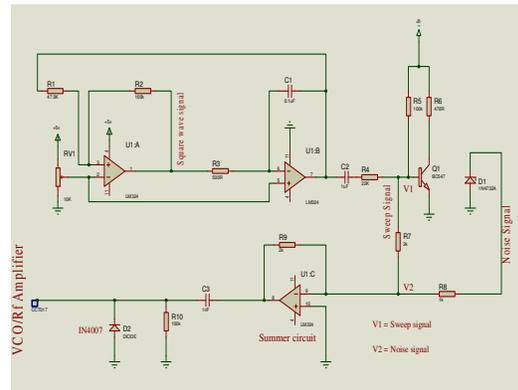


Figure 2: The Circuit Diagram of the System

Circuit Board Design

Having certified that the built prototype is working as the simulated design with respect to the aim and objectives of the system, the design of the circuit board is the next step. The aim of designing circuit board is to achieve portability of the system and to make the system easier to troubleshoot in case of any system error. The block diagram of Type ‘A’ is shown in figure 3.

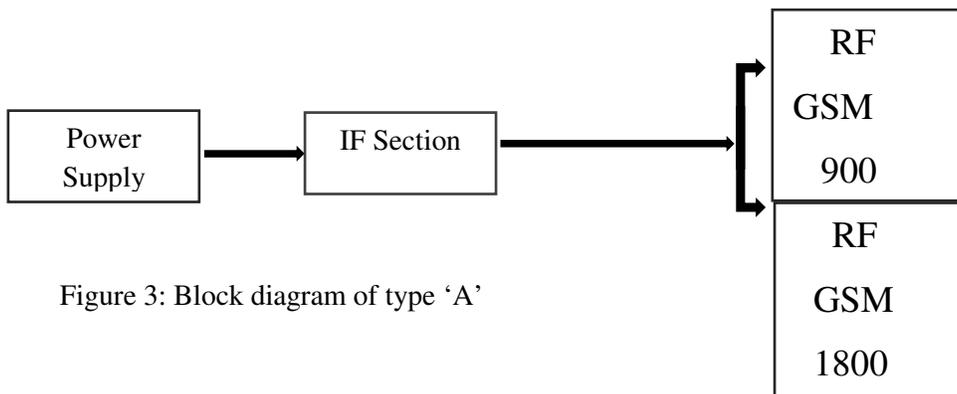


Figure 3: Block diagram of type ‘A’

Power Supply

The power supply is an important part of the jammer. The power supply provides the required electrical energy to the whole circuitry.

For this project, an AC adapter of 240V AC, 8.0A/4.5V was used. The choice for this power supply was made in consideration to cost, size and compatibility.

The AC/ adapter used is a simple mode power supply that contains a small ferrite core transformer which operates at a very high frequency. The high frequency is more easily filtered than the mains frequency and allows the transformer to be very small and also reduce losses. With the help of the switching component, the high frequency/voltage can be reduced to the desired output voltage and current respectively.

Intermediate Frequency (IF) Section

The role of the IF section is to generate a/the tuning voltage(signal) for the VCO in the radio frequency(RF) section, so that the output of the VCO is swept through the desired range of frequencies (from minimum to the desired maximum frequency). The output of this section is basically a triangular wave to which noise is added. This is then offset at a proper amount of DC value to obtain the desired tuning voltage or signal. The block diagram of IF section (control section) is shown in figure 4, and it consists of the following:

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

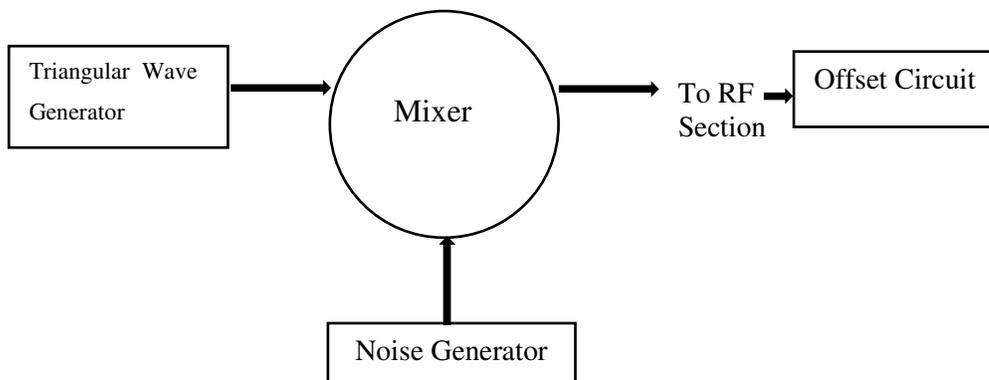


Figure 4: Block Diagram of IF Section

Triangular Wave Generator

The triangular wave is used to sweep the VCO through the desired range of frequencies. In this design, an operational amplifier was used to generate the sweeping signal (triangular waveform) as in figure 5.

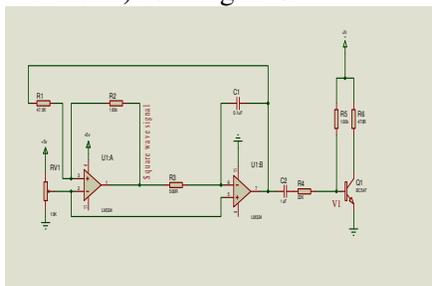


Figure 5: Design Circuit of the triangular waveform

As shown in the figure 5, the circuit uses two operational amplifiers (OPAMP) in such a way that the first Op-amp was generating a square wave which was fed into the integrator which in turn integrates the square wave into the triangular wave at a required frequency.

When power is given to the circuitry, the Op-amp drives its output HIGH. The signal is driven to the integrator through the resistor (R3). The capacitor C2 then starts to charge gradually with RC time constant. While the capacitor is charging, the output of the integrator is also taken to its low state with the same rate. When the positive input

of the Op-amp (through the voltage divider that the 47k and 100k resistors perform) is low enough, then it changes state and the integrator starts operating and so on.

Since the frequency of operation will only have to do with the RC standard, a half cycle period will be exactly the result of the RC. Therefore, a full cycle will then be twice the amount i.e.

$$F_{osc} = \frac{1}{2RC} \dots\dots\dots(2)$$

The frequency generated is thus calculated as:

$$F_{osc} = \frac{1}{2R3C1} \dots\dots\dots(3)$$

Where R3 = 500Ω and C1 = 0.1μf

$$F_{osc} \text{ (Frequency of oscillation)} = \frac{1}{2 \times 500 \times 0.1 \times 10^{-6}}$$

$$= \frac{1}{1000 \times 10^{-7}} = \frac{1}{10^{-4}} = 10^{-4}$$

= 10000Hz

Hence the frequency of operation is $F_{osc} = 10 \text{ kHz}$

Noise Generator

Noise is any random unwanted signal (electrical or electromagnetic) of different frequencies that degrades or corrupts the desired signal by changing

its amplitude, phase or frequency. In order to achieve jamming, the jamming system needs some amount of noise or a certain type to noise to cover portions of the communications spectrum. The noise is mixed with the triangular wave signal to achieve this.

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

The noise generator uses a Zener diode which is later amplified and used in the system designed. The noise in this case must be thermally generated, and that is the reason for the Zener diode because it has different characteristics from regular diodes. A Zener diode operating in the reverse mode was used to produce this noise. In the reverse mode of operation, the diode causes what is termed avalanche effect, which in turn causes wide band noise.

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

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

Signal Mixer

The mixer here is an operational amplifier (Op-amp) configured as a summer, so the noise and triangular wave are mixed to form a new “noisy” triangular waveform. When applied to the VCO, the resulting radio frequency (RF) signal will “sweep” across the cellular downlink frequencies, and will be frequency modulated (FM) with the noise signal before entering the VCO and therefore the circuit in figure 5 is updated as shown in figure 6.

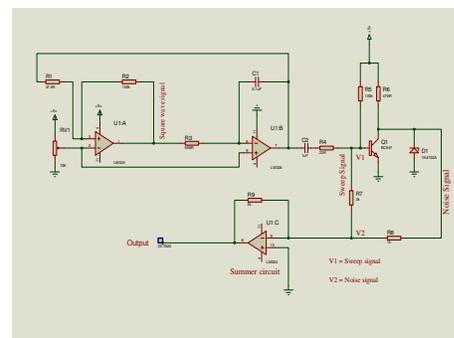


Figure 6: Circuit diagram of the square wave generator, triangular wave generator and summer circuit.

As shown in figure 5 above, the output voltage can be calculated using the formula below:

$$V_{out} = \left(\frac{-R_f}{R_7}\right)V_1 + \left(\frac{-R_f}{R_8}\right)V_2 = -(V_1 + V_2) \dots\dots\dots (4)$$

Using $R_{noise} (R_8) = 1k$, the noise signal is amplified by 2 and thus the ratio of the noise to the sweep signal is 2:1.

Offset Circuit

The input of the VCO must be bounded from 0 to 3.5v in order to get the required frequency range. So, a clamper circuit is added (offset circuit) to get the required frequency range.

Therefore, the clamper circuit comprises of a capacitor connected in series with a resistor and an IN4007 diode as shown in figure 7.

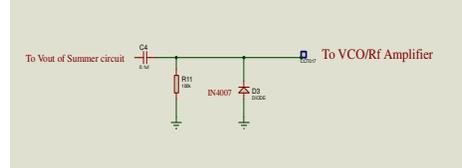


Figure 7: Circuit Diagram of the Clamper Circuit

Radio Frequency (RF) Section

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

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

Voltage Controlled Oscillator (VCO)

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

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

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

1. CVO55CL – 0925 – 0970 for GSM 900 and CDMA
2. CVO55BE – 1785 – 1900 for GSM 1800 and 3G

The VCO performance specifications:

- CVCO55CL – 0925 – 0970

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

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

Its output power is 3.0dBm minimum, with 9.0dBm maximum but typically gives out 6.0dBm. Figure 8 shows the top and bottom view of the CVCO55CL VCO;

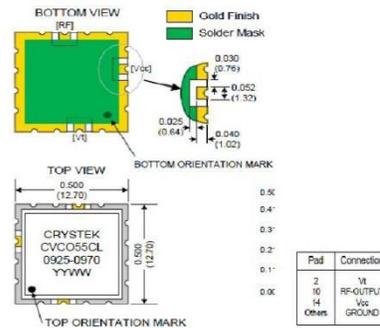


Figure 8: The Top and Bottom View of the CVCO55CL VCO

- CVO55BE – 1785 – 1900

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

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

Typical output power is 2.5dBm, with its maximum output (power) being 5.0dBm
 Figure 9 shows the top and bottom view of the CVCO55BE VCO;

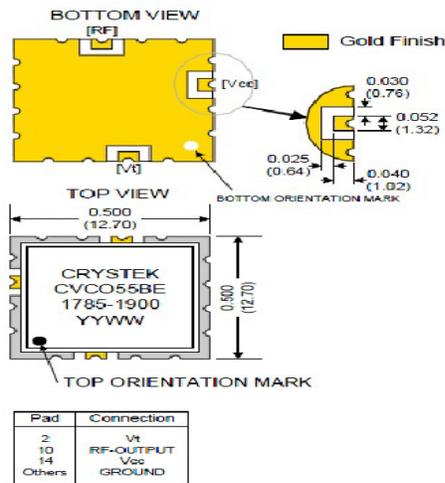


Figure 9: The Top and Bottom View of the CVCO55BE VCO

RF Power Amplifier

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

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

Two (2) Renesas PF08109B power amplifiers were used at each output of the VCO in the design. The PF08109B can be used as a dual band Amplifier for E-GSM (880MHz to 915 MHz) and DCS1800 (1710 MHz to 1785 MHz). It's a 2in/2out

dual band amplifier with high gain and efficiency. It has an output power 5W (approximately 37.0dBm) for GSM 900MHz and 3W (approximately 35.0dBm) for GSM 1800MHz.

Antenna

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

With reference to this project, several antennas were employed to transmit the RF signals coming from the VCO through the power amps to free space. The choice or selection of an antenna is important to achieving the desired goal of signal jamming. Parameters such as the Reflection Coefficient, Voltage Standing Wave Ratio (VSWR), Gain and Directivity are factors one should consider in deciding on any antenna to deploy for a device.

This jammer uses five (5) antennas operating simultaneously in the 900 and 1800MHz frequency range. The specifications of the antennas are length; ¼ wavelength monopole, gain of 2dBi, Omni-directional, VSWR less than 2 and an input impedance of 50Ω.

The five antennas include the 3G (2100MHz), 3G (2000MHz), GSM (900MHz), DCS/PHC (1800/1900 MHz) and the CDMA (800MHz).

This section has explained the methods and the functionality of all the components that were used in the construction of this research work. The device operates when the power supply gives ± 12V to IF and RF section. The triangular wave regulator will regulate the triangular waveform as an input to RF section. The triangular wave and the noise signal will be mixed in the mixer for the RF so that it will transmit the desired noise frequency. The mixture of the signal then will be transferred to clamper so that the clamper will give the desired voltage range between 0 to 3.5V for Voltage Controlled Oscillator. Then the signal will be amplified at power amplifier at the RF section and then transmitted as a high noise frequency between the range of 935 – 960MHz for GSM and 1805 – 1880MHz for DCS. This criterion is being chosen because the antenna must transmit at the same frequency as the mobile signal frequency. When the ratio between the antenna frequency and the mobile signal frequency is 1:1, the mobile signal frequency will

be blocked. Figure 10 summarizes the system of operation of the GSM mobile jammer.

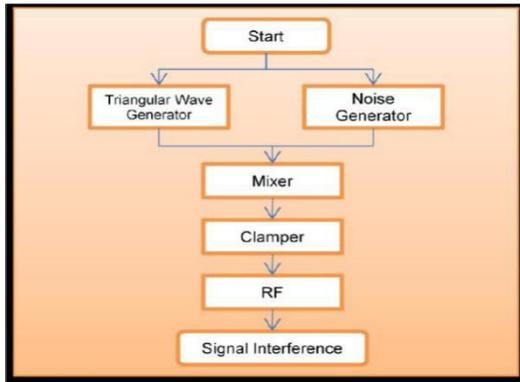


Figure 10: System Operational Chart

Design Parameters

The approach to jamming is of paramount importance. That is, whether to jam the BTS transmit (mobile receive) or the BTS receive (mobile transmit). However, jamming the mobile transmit would mean disrupting communication over the entire cell and therefore would require a high power transmitter. Jamming the mobile receive only jams the required area and therefore requires a transmitter of sufficient power. The goal of this research therefore, is to disrupt communications over the mobile receive (forward link) only. The frequency design is as follows:

GSM 900	—————>	935 – 960 MHz
DCS 1800	—————>	1805 – 1880 MHz

The focus was on some design parameters to establish the design specifications. These parameters are as follows:

The Distance to be jammed (D): - This parameter is of relevance to the design, since the amount of output power to the jammer depends on the area that needs to be jammed. The jammer is designed and established upon a D = 10m for the Digital Cellular System (DCS 1800) and D = 20m for the GSM 900 band (for Nigeria)

Jamming-to-Signal Ratio (J/S): - The J/S is the ratio of the jamming signal strength (within the

receivers’ bandwidth) to the strength of the desired signal. Jamming becomes effective when the interfering signal in the receiver is strong enough to prevent or deny the usability of the communication transmission or channel. To successfully jam a particular region, a very important parameter needs to be considered i.e. the Signal to Noise Ratio, referred to as the SNR. Every device working on radio communication principles can only tolerate noise in a signal up to a particular level. This is called the SNR handling capability of the device. Most cellular devices have a SNR handling capability of around 12dB. A very good device might have a value of 9dB, although it is highly unlikely. To ensure jamming of these devices, the SNR needs to be reduced up to 9dB.

Power Calculations

The aim is to find the power that needs to be transmitted to jam any cell phone within a distance of around 15 meters for both systems. Here, the ideal Signal-to-Noise Ratio (SNR) and also the maximum power signal for the mobile receiver were taken into account. A very good device has an SNR of about 9dB, which will be used as the worst-case scenario for the jammer. The goal here is to find the output power from the device, so when the path loss is added to the jammer power, the target will be acquired:
For GSM 900:

The minimum signal to noise ratio SNR = 9dB
The maximum signal power at signal at receiver S = -15dBm
Then Jammer power, $J_r = S - 9 = -15 - 9 = -24dBm$
Output jammer power = $-24dBm + 55.61 = 31.61dBm \cong 1.45 W$

For GSM 1800:
The minimum SNR = 9dB and the maximum S = -23dBm
Then, $J_r = -23 - 9 = -32dBm$
Output jammer power = $-32dBm + 61.44 = 29.44dBm \cong 0.9W$

III. SYSTEM IMPLEMENTATION Analysis

The GSM Mobile Phone jammer was successfully used to jam four mobile operators which are MTN Nigeria, Globacom, and Airtel (9 mobile). When the jammer was put ON, there was a complete loss of signal for the service providers in the 2G range. However, the jammer was not completely effective in jamming the signal for the 3G mobile reception probably because the 3G frequencies were too high (2100MHz and above) for the antenna used for this research to pick up.

The results showed that the jammer functioned as intended. Testing was done to see the duration of time taken by the jammer to jam the GSM mobile phones between the different service operators. The testing was also done in consideration of the

four main service operators in Nigeria; MTN Nigeria, Globacom, Airtel and 9 mobile.

Based on the result and testing of the Mobile Jammer, the objective of the research has been relatively achieved. The Mobile Jammer successfully jammed all the four main service operators but the coverage distance varied for the different operators.

When the GSM mobile jammer was switched “ON”, the mobile phone transmission signal displayed “NO NETWORK”. Figure 11 shows the results when the Jammer is “OFF” and when it is “ON”.

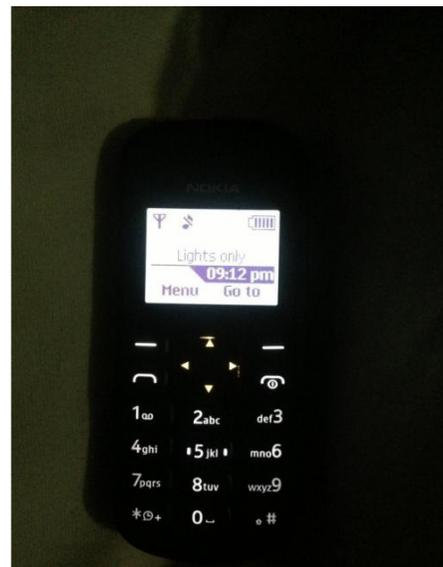


Figure 11: Snapshot showing mobile phone when Jammer is “OFF” and “ON”

Test Plan and Data Test

This section entails an overall system testing of the integrated design of the voltage measurement device. The testing and integration is done to ensure that the design is functioning properly as expected thereby enabling one or even intended users for which the research was targeted for to appreciate its implementation and the approaches used in the construction and integration of the various modules of the research work. This involves checks made to ensure that all the

various units and subsystems functioned adequately. Also there has to be a good interface existing between the input/output unit subsystems. When the totality of the modules was integrated together, the system was created and all modules and sections responded to as specified in the design through the power supply delivering into the system designed.

Component Test

Similar components like resistors were packed together. Other components include capacitor, preset switches, diodes, LED, transistor, voltage regulator etc.

Reference was made to resistor color code data sheet to ascertain the expected values of resistors used. Each resistor was tested and the value read and recorded. The transistor test is shown in Table 1.

Table 1: Test for Transistor

	Black probe	Red probe
1 st test on pins	Collector	Base
2 nd test on pins	Emitter	Base

System Testing

After the construction and implementation phase, the system was tested for durability, efficiency, and effectiveness and also to ascertain if there is need to modify the construction. The system was first assembled using a breadboard. All components were properly inserted into the breadboard from whence some tests were carried out at various stages. To ensure proper functioning of the components and expected data, the components were tested using a digital multi meter (DMM). Resistors were tested to ensure that they were within the tolerance value. Faulty resistors were discarded. The LEDs were tested to ensure that they were all working properly.

Testing was also done with a varying input supply voltage. This was to done to determine the system’s ability to provide protection to the equipment connected to it. The system was powered and operated upon using several possibilities. They include plugging and unplugging the mains and noting the output responses of the system hardware.

The actual testing is not just to block the transmission signal but to check the duration of the time taken by the device to block the transmission between these three operators. From the testing, the time taken for the device to block the transmission between these four operators was totally different. The duration of the time taken for the device to block the transmission is shown in Table 2.

Table 2: Duration of Time Taken to Block the Transmission

Operators	MTN Nigeria	Globacom	Airtel	9 Mobile
Duration (s)	32	37	55	67

The power of the operator at the mobile phone is different which makes the duration of time taken to block the transmission also different.

tested on this device. Although the device can operate as expected, but the radius of the antenna did not completely meet the required expectation.

System Performance

Based on the analysis and result, the device can successfully block the signal transmission of mobile phone. The device can block the four main operators in Nigeria which are MTN, Globacom, Airtel and 9 Mobile. The duration of time taken to jam each of the mobile operators has also been

IV. CONCLUSION

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

The successful implementation of this research was largely due to certain precautions taken when understudying related works done. One major precaution taken was finding an appropriate power supply for the device, since it was a challenge faced by the researches understudied.

REFERENCES

- [1] International Telecommunications Union, ITU-R (Radio communication Sector of ITU) Report ITU-R M.2243 (00/2011) “Assessment of the global mobile broadband deployments and forecasts for International Mobile Telecommunications”, pp. 4
- [2] S.M.K. Chaitanya, P. Naga Raju, Y.N.V.L. Ayyappa, Vundavalli Ravindra “International Journal of Computer Science and Telecommunications” [Volume 2, Issue 5, September 2011].
- [3] GSM Frequencies and Frequency Bands [online], Available:http://www.radio-electronics.com/info/cellulartelecomms/gsm_tech_nical/gsm-frequency-frequencies-bands-allocations.php [Accessed: 22nd October 2011].
- [5] Siegmund M. Redl, Matthias K. Weber, Malcolm W. Oliphant, “GSM and Personal Communications Handbook”, pp. 67
- [6] Rimantas Pleikys, “Radio Jamming in the Soviet Union, Poland and other East European Countries”, 2006.
- [7] Mobile & Personal Communications Committee of the Radio Advisory Board of Canada, “Use of jammer and disabler Devices for blocking PCS, Cellular & Related Services” [online], Available:<http://www.rabc.ottawa.on.ca/e/Files/01pub3.pdf> [Accessed: 16/11/2011].
- [8] “Frequency Jamming”, www.google.com, On-line accessed on 10/08/2021.
- [9] National Communications Authority, “Broadband Wireless Access (BWA) Licenses in the 2500MHz – 2690MHz Band”, March 2010, pp. 3