Design and Implementation of a Dual Band Mobile Phone Jammer

Nsikan Nkordeh, Iwu C. Lawson, Francis Idachaba, Ibinabo Bob-Manuel

***Abstract*- The incessant use of mobile phones can be attributed to its portability and thus have become one of the most widely used devices in mobile communication which makes it so essential in our lives.**
The convenience and portability of mobile phones has made it possible to be carried everywhere, e.g. Churches, lecture halls, medical centers etc. Its convenience can create inconvenience in some places when there is continuous beeping or ringtones of cell phones which becomes annoying when such noise is disruptive in areas where silence is required or the use or of mobile phone is restricted or prohibited like Libraries and Study rooms
.
This paper focuses on the design of a cell phone jammer to prevent the usage of mobile communication in restricted areas without interfering with the communication channels outside its range. Interference and jamming severely disrupt the ability to communicate by decreasing the effective signal-to-noise ratio and by making parameter estimation difficult at the receiver. Interference and jamming severely disrupt our ability to communicate by decreasing the effective signal-to-noise ratio and by making parameter estimation difficult at the receiver[5] Similarly with other radio jamming techniques, mobile phone jammer sends the signal (jamming signal) of the same frequency that mobile network use. This causes enough interference with the communication between mobile phones and communicating towers to render the phones unusable. Upon activating mobile jammers, all mobile phones will indicate "NO NETWORK"

***Index Terms*-- B**ase station, Cell phone, GSM signal, jamming,
.

I. INTRODUCTION

The telecommunication industry over the past decades has witnessed an increasingly rapid growth in mobile telephony. Due to the use of mobile phone which is on the increase and globally appreciated, it is sometimes inappropriately especially in public areas where silence is required or the use of cell phone is prohibited.
A mobile phone jammer is a device used to prevent mobile communication by causing interference between the cell phone and the base station. When used the jammer effectively disables mobile phones around the restricted area. These devices can be used practically in any location, but are found primarily in places such as lecture halls, banks, medical centers etc. where a phone call would be practically disruptive because silence is required.This jammer is designed to work at GSM 900MHz and DCS 1800MHz simultaneously and thus jams the four well-known network carriers in Nigeria (MTN, GLO, ETISALAT AND AIRTEL).

Cell phone jamming devices 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] Mobile jammers prevents the use of mobile communication by transmitting radio wave signals (jamming signal) along the same frequencies that mobile phones use. This causes enough interference with the communication between mobile phones and base station to render the phones inoperative. Incoming calls are blocked as if the mobile phone were off. When the mobile jammers are turned off, all mobile phones will automatically re-establish communications and provide full service. Mobile jammer's effect can vary widely based on factors such as proximity to towers, indoor and outdoor settings, presence of buildings and landscape.

The jamming success rate depends on multiple parameters of the communication system, namely [6, Dabcevic]:

- Received power of the jamming signal.
- Received power of the targeted transmitted signal.
- Type, modulation and bandwidth of the jamming signal.
- Modulation and bandwidth of the targeted transmitted signal.
- Error correction mechanisms implemented within the transmitted signal.
- Sensitivity of the receiver.
- Type of detector implemented at the receiver (coherent or non-coherent).

II. ` FUNDAMENTALS OF FREQUENCY JAMMING

The essence of frequency jamming is to interfere with a signal in order to stop or degrade the quality of service of a given mobile network. Given a communication system, the propagation loss on the transmitter-receiver can be expressed as:

At the transmitter

$$P_{RT} = \frac{P_T G_{RT} G_{TR}}{L_T L_{TR}} \qquad (1)$$

Manuscript received July 22, 2016; ; revised August 10, 2016.
N.S Nkordeh is a Lecturer with Department of Electrical and Information Engineering Covenant University Ota Nigeria, nsikan.nkordeh@covenantuniversity.edu.ng
Iwu Lawson is a student with Department of Electrical and Information Engineering Covenant University Ota Nigeria, Chidic04@gmail.com
F. E Idachaba a Associate Professor with Department of Electrical and Information Engineering Covenant University Ota Nigeria, francis.idachaba@covenantuniversity.edu.ng
Ibinabo Bob-Manuel is an IT consultant ibinabo.bobmanuel@gmail.com

At the receiver, the antenna received power is given as:

$$P_{RJ} = \frac{P_J G_{RJ} G_{JR}}{L_J L_{JR}} \qquad (2)$$

The effects of jamming depend on the jamming-to-signal ratio (J/S), range between transmitter and receiver (mobile device), modulation scheme, channel coding and interleaving of the target system, bandwidth of transmitter and receiver. Generally Jamming-to-Signal ratio can be measured according to the following equation

$$\frac{J}{S} = \frac{P_J\ G_{JR}\ G_{RJ}\ R_{TR}^2\ L_R\ B_R}{P_T\ G_{TR}\ G_{RT}\ R_{JR}^2\ L_J\ B_J} \qquad (3)$$

For equations (1), (2) & (3) ,the parameters are defined as:
P_J = Jammer transmit power
P_T = transmitter power
G_{JR}= antenna gain from jammer to receiver
G_{RJ} = antenna gain from receiver to Jammer
G_{TR} = antenna gain from transmitter to receiver
G_{RT} = antenna gain from receiver to transmitter
B_R = communications receiver bandwidth
B_J = jamming transmitter bandwidth
$\boldsymbol{R_{TR}}$ = range between communications transmitter and receiver
$\boldsymbol{R_{JT}}$= range between jammer and communications receiver
L_J =transmission losses / communication signal loss
L_{JR}= Propagation loss in the Jammer-receiver path l (including polarization mismatch)

The performance of the jammer is a function of the Jammer-To-Signal Ratio (JSR) ζ , given by:

$$\zeta = \frac{P_{RJ}}{P_{RT}} \qquad (4)$$

The Signal-To-Jammer Ratio (SJR),γ is the reciprocal of the JSR

$$\gamma = \frac{1}{\zeta} \qquad (5)$$

In this session, we take a brief look at the fundamentals of jamming a QPSK-modulated signal.QPSK is achieved by transmitting two bits per symbol, i.e. two BPSK in quadrature, hence achieving $\pi/2$, and thereby improving spectral efficiency.

A transmitted QPSK-modulated signal $s(k)$ during the time interval k can be represented as :

$$s_k(t) = \sqrt{2R}\sin\left(2\pi f_0 t + d_k \frac{\pi}{4}\right) \qquad (6)$$

$$=\pm\sqrt{R}\cos(2\pi f_0 t) \pm \sqrt{2}\sin(2\pi f_0 t), \qquad (k-1)T \le t < kT \qquad (7)$$

Where $d_k \in \{1,3,5,7\}$

The received signal during the time interval k , is given as$r(t)$:

$$r_k(t) = s_k(t) + n(t) \qquad (8)$$

$n(t)$ = Additive White Gaussian Noise (AWGN) which may interfere with the signal

The probability density function (PDF) is computed

$$p(r|d_k) = \frac{1}{\sqrt{\pi N_0}} e^{-\frac{(r-d_k\sqrt{E_S})^2}{N}} \qquad (9)$$

$E_s = Average\ Signal\ Energy$, $N_0 = Noise\ Energy$

At the receiver the decoder differentiates between the signals by comparing the received signal with the threshold, γ

For instance, if

$$symbol = \begin{cases} s_0\ , r(t) < \gamma \\ s_1, r(t) > \gamma \end{cases} \qquad (10)$$

Then the probability of error given that s_1 is transmitted is expressed as

$$p(e|s_1) = \frac{1}{\sqrt{\pi N_0}} \int_{-\infty}^{0} e^{-\frac{(r-d_k\sqrt{E_S})^2}{N}} dr = \frac{1}{2} erfc\left(\sqrt{\frac{E_s}{N_0}}\right) \qquad (11)$$

Where $erfc(x)$ is the complementary error function of x given as:

$$erfc(x) = \frac{2}{\sqrt{\pi}} \int_{-0}^{\infty} e^{-x^2}\, dz \qquad (12)$$

If the jamming is done using Average White Gaussian Noise given by equation (8), the Symbol error of probability for the QPSK-modulated signal, assuming all four bits are transmitted is:

$$P_e = erfc\left(\sqrt{\frac{E_s}{2N_0}}\right) - \frac{1}{4} erfc^2\left(\sqrt{\frac{E_s}{2N_0}}\right) \qquad (13)$$

$$\approx\ erfc\left(\sqrt{\frac{E_s}{2N_0}}\right) \qquad (14)$$

If the noise used in jamming the QPSK-modulated signal is narrow-band, P_e is approximated to

$$P_e \approx erfc\left(\sqrt{\frac{E_s}{2(J+N_0)}}\right) \qquad (15)$$

III. JAMMING A QPSK-MODULATED SIGNAL WITH A TONE AWGN JAMMER

In order to properly jam the signal, the tone jammer should either jam the quadrature or in-phase components of the QPSK-modulated signal [6]. At the receiver, the jamming Probability of causing a signal error to each of the orthogonal components is

$$P_e^I = Q(\sqrt{\frac{R}{N_0}}(1 - \sqrt{\frac{2J}{R}} sin\theta^J))) \qquad (16)$$

ISBN: 978-988-14047-1-8
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

$$P_e^Q = Q(\sqrt{\frac{R}{N_0}}(1 - \sqrt{\frac{2J}{R}} cos\theta^J))) \quad (17)$$

The average symbol error probability for the QPSK signal conditioned on the phase θ^J of the jamming signal may be computed as [6]

$$P_e = P_e^I + P_e^Q - P_e^Q P_e^I \quad (18)$$

If we assume that the phase of the jamming signal is evenly distributed over $[0, 2\pi]$, the unconditioned average symbol error probability can be computed as

$$P_e^{uncond} = \frac{2}{\sqrt{\pi}} \int_0^{2\pi} P_e \ d\theta^J \quad (19)$$

According to [6, Dabcevic], in order for the jammer to successfully jam the signal, the phase between the jamming and the targeted signal must not coincide

IV. JAMMING TECHNIQUE

There are several ways to jam a radio frequency device. The three most common techniques can be categorized as follows:

1. Spoofing

This type is very difficult to implement since the jamming device first detects any mobile phone in a specific area, then the device sends the signal to disable the mobile phone.

2. Shielding Attacks

This is known as TEMPEST or EMF shielding. This type requires closing an area in a faraday cage of conductive mesh so that any device inside this cage cannot transmit or receive RF signal from outside of the cage.

3. Denial of Service

This technique is referred to DOS. In this technique, the device transmits a noise signal at the same operating frequency of the mobile phone in order to decrease the signal-to-noise ratio (SNR) of the mobile under its minimum value. [3]

The technique implemented in this paper is **denial of service (DOS)** and it is achieved when the jamming device transmits a high power signal of frequency range used by mobile phone thereby degrading the Signal to Noise (S/N) of the mobile device. The transmitted signal of the jammer is seen as noise by the mobile device, hence increasing the noise threshold of the system.

V. JAMMER TECHNOLOGY

After studying different jamming techniques such as spoofing, shielding attacks and denial of service, the DOS technique was used in implementation for this paper because it keeps the jamming device ON permanently. This type of technique is achieved when the jamming device transmits the noise induced signal (jamming signal) which is of the same frequency band as the communication system (mobile phone) transmits. The operating frequency bands to be considered are listed below:

Table 1 – Operating uplink and downlink frequency range with duplex spacing

Operating Band	UPLINK (Mobile State to Base station(MHz)	DOWNLINK (Base Station To Mobile Station)	DUPLEX Spacing (MHz)
GSM900	890-910	935-960	45
DCS1800	1710-1785	1805-1880	95

To achieve the required frequency of the downlink signal to be jammed emphasis on the following design parameters were considered to establish the device specifications and they are:distance to be jammed, the frequency bands, jamming to signal ratio and free space path loss**.** The jammer consists of power supply section, detector section, intermediate frequency section and the Radio Frequency section**.**

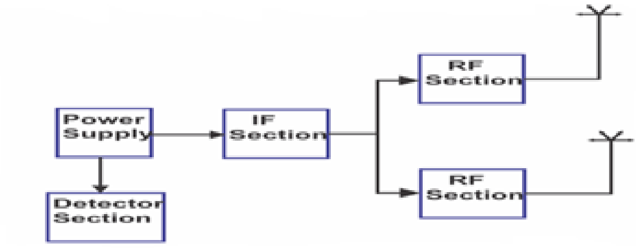

Fig 1: block diagram of a jammer device

The power supply section provides power supply to the remaining sections (detector, IF and RF) of the jammer device. The power supply section consists of a 24V transformer, a rectifier which consists of two diodes for rectification, a filter and a 12V voltage regulator. The power section supplies 9volts to the detector section and 12volts to the IF and RF section. The Jammer is designed such that it would have a 12V battery which would act as backup in case of power loss. The detector section uses an operational amplifier (Op-Amp) to sense the presence of an activated cell phone from a distance of several meters. The detector circuit can detect any activity of a mobile phone such as incoming or outgoing voice, voicemail, texting, and data. The detector circuit emits light through an LED and there would also be a sound buzzer to show the detection of a cell phone signal.

The IF Section consists of a triangle wave generator, noise generator, mixer and a clamper. The function of the IF section is to generate a tuning voltage for the voltage controlled oscillator.

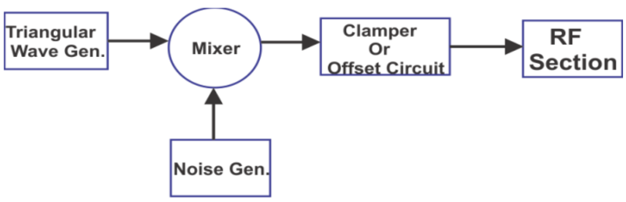

Fig 2: block diagram of IF Section

ISBN: 978-988-14047-1-8
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

This is done so that the output of the VCO is swept through the desired range of frequencies i.e. from minimum to the desired maximum frequency. The output signal of the IF section is the combination of the triangular wave signal from the triangle wave generator and noise signal from the noise generator. The mixer is responsible for the summation of both signals. The output signal of the mixer is then offset at a proper amount of DC value to obtain the desired tuning by the clamper. The RF Section is the most important part of the jammer device since the output signal of this section will be interfacing with the mobile frequency signal. The RF section consist of a voltage controlled oscillator, power amplifier and an antenna. The VCO (PMB2110) used in this jammer device is responsible for generating the RF signal that will overpower or jam the mobile signal thereby disrupting communication between the mobile device and the base station.

PMB 2110 Performance Specification [3]
According to the (PMB 2110) data sheet it has some of the following performance specifications.

- Frequency range: GSM 900 (880 – 915) MHz
- DCS 1800 (1710 – 1785) MHz
- Voltage supply (Vcc): 2.7 to 2.95V
- Control Voltage (VTUNE): GSM 900 (1.1 – 1.9V) DCS 1800 (0.5 – 1.9V)
- Output Power: For GSM 900 its output power is 4dBm minimum, with 9dBm maximum but typically gives out 6dBm.For DCS 1800 its output power is 3dBm minimum, with 8dBm maximum but typically gives out 6dBm.
- Two single ended RF power outputs to drive the power amplifier

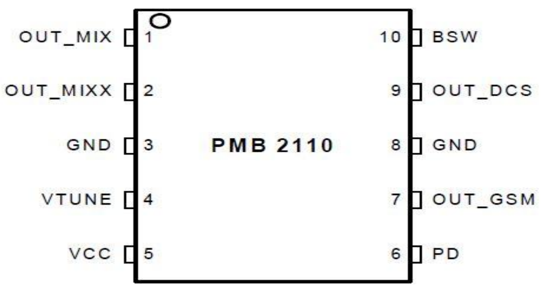

Fig 3: PIN Configuration of the PMB 2110 VCO

Table 2: PMB 2110 pin definitions and functions

PIN NO	SYMBOL	FUNCTION
1	OUT_MIX	Downconvert output
2	OUT_MIX X	Downconvert output inverted
3	GND	Ground
4	VTUNE	Frequency Control Voltage output
5	VCC	Supply Voltage
6	PD	Powerdown,PD==Low;VCO off PD=High VCO on
7	OUT_GSM	RF Output GSM900
8	OUT_MX	RF Output DCS1800
9	GND	Ground
10	BSW	Band Select:BSW=lowGSM900 VCO on BSW=High DCS1800 VCO on

The output signal of this section operates on the same frequency range as the mobile device but with a higher power level. The power level of the jamming signal from the VCO is amplified from a value of 5dBm to 35dBm using a power amplifier (PF08109B). For transmitting the RF Signal we need an Antenna. Two 1/4 wavelength monopole antennas, with 50 Ω input impedance are used in this paper so that the antennas are matched to the system.
This paper discusses the design and development of GSM Mobile jammer and aims to present a solution for the problems that are caused by mobile phones. The main concept of jamming is the transmission of the same frequency which is used by a mobile service provider with noise to cause interference with a user’s mobile device and the base station.

VI. RESULT

The simulation results of the various circuit components were observed and results are shown below using an oscilloscope. The first part of the Jammer is the Tuning circuit (IF Section) shown in the figure 4 and the second part of the jammer is the RF section which generates the jamming signal. The output waveform after the device was built can be compared to the simulation from the IF section (the noise signal mixed with the triangular wave signal). You can observe that the noise in the output is much more intense since it has gone through further amplification.

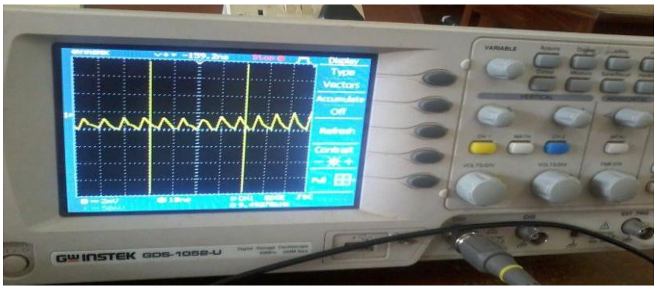

Figure 4: Simulation results of a triangular wave signal by a 555-timer

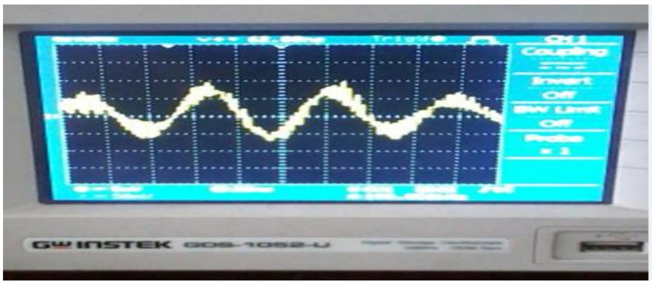

Fig 5: Simulated waveform of the output of the jammer device

VII. CONCLUSION

In this paper, a mathematical analysis of frequency jamming was done using a QPSK-modulated signal. In other to discourage student from using mobile phones during lectures and around the library areas, a jammer system was built using VCO (PMB2110) processor which generates signal in the frequency range of GSM900 and DCS1800.Tests were carried out in the lecture room areas

ISBN: 978-988-14047-1-8
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

and in the library, and it was found out that mobile phones were 'shut' out from service while the jammer was on.Oscilloscpe plots were taken, which shows that the noise level of the received mobile signals increased tremendously while the jammer was on.

The success of this project has in shutting down mobile services within the vicinity where it is not needed has open communication with some industry that may result in mass production of the device.

REFERENCES

[1] Radio communication sector of ITU (ITU-R), report ITU-R M.2243 "Assessment of the global mobile broadband deployments and forecasts for International Mobile Telecommunications , 2011".

[2] https://en.wikipedia.org/wiki/Talk%3AMobile_phone_jammer.

[3] Ahmed Sudqi Hussein Abdul-Rahman, Ahmad Nasr Raja Mohammad, "GSM 900 mobile jammer", Undergrad project, JUST, 2006.

[4] Infineon Technologies AG, "PMB 2110 GSM Dual band TX VCO", July 2001

[5] Affo Alex, Effah Onasis, Ibrahim I. Fareed, "design and construct a dual band mobile jammer for GSM 900 & GSM 1800", Ghana telecom university college (GTUC), 2012.

[6] Kresimir Dabcevic "Intelligent jamming and anti-jamming techniques using Cognitive Radios" PhD Programme in Computational Intelligence University of Genoa, April, 2015

[7] Galib Asadullah M.M. "Robustwireless Communications Under Co-Channel Interference And Jamming" PhD thesis to Department of Electrical and Computer Engineering, Georgia Institute of Technology, U.S.A 2008 821-826, 2013ISSN: 1549-3636©2013Science Publicationsdoi:10.3844/jcssp.2013.821.826 Published Online 9 (7) 2013 (http://www.thescipub.com/jcs.toc)

ISBN: 978-988-14047-1-8
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)