International Journal of Scientific Research in Physics and Applied Sciences
Vol.11, Issue.2, pp.31-37, April 2023
E-ISSN: 2348-3423
Available online at: www.isroset.org

Research Paper

Designing and Implementing Phone Jammer with Safety Implications in Nigeria

N. Nwokocha[1]

[1]Physics Dept, Faculty of Natural Science, University of Jos, Jos, Nigeria

Author's Mail Id: nnwokochagabriel@gmail.com

Received: 15/Oct/2022; **Accepted**: 25/Feb/2023; **Published**: 30/Apr/2023

Abstract— This study was purported to design and develop a mobile phone jammer with the possibilities of creating safety implications for lives and property, as well as organizational communication systems, particularly on the need to handle business transactions/exchanging emergency alert messages. Parts, materials, and instruments were purchased and assembled which resulted in a useable mobile jammer. The testing was conducted with 2G, 3G, and 4G on Airtel, Globacom, MTN, and 9Mobile services within a jamming range of 20 meters. Results revealed that the 2G and 3G networks were successfully jammed within less than 20 meters range, while that of 4G failed. The safety needs to implement mobile jammers in places associated with dangers after securing full permission and approval from the government as specified by the Nigeria Communication Commission (NCC) in the case of Nigeria was established. As such, designing sophisticated jammers to block mobile phones with 4G networks in line with the safety implications of both hazards and an effective organizational communication system was recommended.

Keywords— Designing, Implementing, Phone Jammer, 2G/3G/4G, Safety Implications

1. Introduction

Phone jammers are wireless equipment that is capable of blocking the transmission of signals to cell phones. Jammers are generally categorized into "Radio Frequency (RF) and Global System for Mobile Communication (GSM)". Jammers are developed with the capacity to wedge any functional Frequency Modulation (FM) band of "87.5 MHz to 108 MHz", as well as the transmission indication of GSMs operating within the functional range of the jammer. Jammers introduce dirty signals (noise) to possibly wedge the frequencies of the active GSM [1]. As such, the RF system is famously utilized to detect cell phone signals between the range of 0.9GHz to 3GHz [2].

Basically, jammers can be of two sizes: the smaller ones which can block signals coming from cell phone towers within a 30-foot (9m) radius; and the much smaller ones which are capable of blocking transmission from the satellite to the cell phone towers [3]. Just as advancement in mobile phone technology continues from 1-Generation (1G for wireless analog network), 2G, 3G, 4G, and even 5G which is still undergoing development (all of the digital communications) and being differentiated by their individual speed and technology, mobile jammer redesign and reconfiguration is needed. Nevertheless, this study focuses its jammer design for 2G, 3G, and 4G networks which enhance communication at speeds of 64kbps, 144kbps-2mbps, and 100mbps-1gbps – as they operate on Long Term Evolution - LTE technology respectively, on functional frequencies. A successful jammer design entails all networks on the same frequency are to be cancelled [4].

The implementation of mobile jammers has been illegally proscribed by the International Telecommunication Union (ITU), which provides room for the enforcement of huge penalties by most countries of the world. Domesticating this in Nigeria, the government through the Nigeria Communication Commission (NCC) has imposed a ban on the use of mobile jammers in line with the Telegraphy Act of 2004, except with express permission and approval from the commission. Their reasons are premised on the fact that the effect of jammers may extend beyond targeted parameters to degrade the quality of network and technical standards for untargeted users. Despite these concerns, GSM phone signals have been taken advantage of by criminals to blow up explosives as well as carry out coordinated attacks in security formations, disruption of delicate medical instruments, and also caused dangerous risks in refineries and filling stations [5]. Furthermore, due to the importance of jammers against these dangerous activities, this study joins similar research that previously designed and tested this type of device but not on the latest technological advancement of mobile networks like 4G and above.

The importance of this study in terms of designing and implementing mobile jammer is to guarantee the prevention of harm to lives and property in danger-prone environments, and also ensures this does not degenerate into organizational communication breakdown within the confine of jammers' usage regulation.

1.1 Statement of Problem

Although, there are existing ban on the use of phone jammers in most climes due to the tendency of preventing everyone within the affected range from emergency calls, there are still less concerns on how to address this issue in business places and religious gathering. This work is a stepping stone to exploring the chances of designing and implementing jammers in restricted areas without affecting the internal communication systems in non-explosive environments.

1.2 The Objective of the Study

This study aims to create wireless frequencies for blocking amplitude-modulated and frequency-modulated signal transmissions:

i. To develop phone jamming devices for 2G/3G/4G networks, while other specific objectives include.
ii. To identify the safety implications of using mobile jammers in organizations.

To achieve these objectives, jammer parts are purchased and assembled, and organized in sections: 1 - introducing the study; 2 – discussing related issues; 3 - presenting materials and method; 4 – discussing the results; and 5 concluding and setting the direction for further study.

2. Related Work

The development of mobile jammers has gained experts' attention recently around the world. Most jammers developed were unsuccessful during the test while others were successful in jammers cell phone networks. For instance, jammers that were meant to block GSM signals of 900MHz, Code Division Multiple Access (CDMA), 3G networks and Bluetooth, had their power supply unable to amplify appropriate current to Voltage Controlled Oscillator (VCO), making it impossible to turn to desired frequencies. Another jammer successfully blocked the GSM signals but could not cover the expected range of 10 meters [6]. A frequency within 963-970MHz was successfully jammed in the works of [7];[8]. In another, a Yagi antenna of 900MHz was designed which successfully expand the range of jamming, distinguishing it from blocking the distance obtainable in helical antenna [9]. More so, 20 meters distance frequencies were successfully jammed in the works of [10].

Similarly, another designed jammer was able to restrict GSM 900MHz and GSM 1800MHz frequencies simultaneously of mobile cell phone carriers of MTN, GLO, Etisalat and Zain in Nigeria [12]. Phone jammer was also developed and tested successfully on 2G but failed to jam the 3G network of 2100MHz with Globacom, MTN and Etisalat [13],[14]. Another mobile phone jamming success was recorded in the work of [15]. Mobile phones were also jammed with prescheduled time duration in the work of [16]. The use 555 timer IC along with other components successfully disabled cell phone signal within the targeted range [17]

Furthermore, ATmega328 being associated with low-power density was installed as the centerpiece system to support top performance in the Advanced Virtual RISC (AVR) [5]. Based on organized commands in program writing, a Microcontroller Element is meant to process manifold activities (LCD, Messages, and jamming system) simultaneously.

In another study, a jammer system was built using VCO (PMB2110) processor which generated a signal in the frequency range of GSM900 and a Digital Cellular System (DCS1800MHz). Tests were carried out, and it successfully shut out mobile phone's services [18]. Again, a study in Kenya fairly jammed 2G and 3G networks using four service providers [19]. Most of these studies used the denial-of-service method to jam the mobile networks and most of them were tested on 2G but very few on 3G. Thus, this current study includes a 4G network for testing of the jammer.

3. Materials/Methods

Materials and methods explain the components and procedures adopted in carrying out this study to a conclusive end. In this case, the qualitative experimental design is used to construct and test the mobile jammer. This implies that the process of designing the jammer is based on literature review, enquiry from radio technicians, observation and the application of knowledge acquired during the course of study. Thus, these materials and methods are discussed further.

3.1 Materials

The materials are items assembled for the construction of the jammer as displayed in table 1.

Table 1: Jammer components

Name	Value	Usage
R1 resistor	100R	Emitter loading
"R2 resistor	30K	Base biasing"
"C1 capacitor	15pf	Frequency generating"
"C2 capacitor	4.7pf	Feedback"
"C3 capacitor	4.7pf	Feedback"
"C4 capacitor	102pf	Noise reduction"
"C5 capacitor	1MF	Coupling"
"C6 capacitor	2.2pf	Coupling"
"C7 capacitor	103pf	Decoupling"
"Q1 transistor	BF 494	Amplification"
"L inductors	22Nh	Frequency generating"

Source: [19]

The listed electronic components in table 1 are all direct current (DC) compliance. They are categorized into resistors, capacitors, transistors, and inductors which will be built into various units of the jammer. Thus, all these components are meant to operate in different functions as represented in the usage above and in different stages of the jammer circuit according to the values designated.

3.2 Method

Method of Constructing the Jamming Device

The Jammer-circuit. This has five fundamental parts to be assembled into one whole for it to function as a jammer. They include triangular wave generators, mixer circuits, RF-amplifier, noise generators, and voltage-controlled-oscillator/transmitters [19]. The flow chart of the phone jammer is displayed in Figure 2.

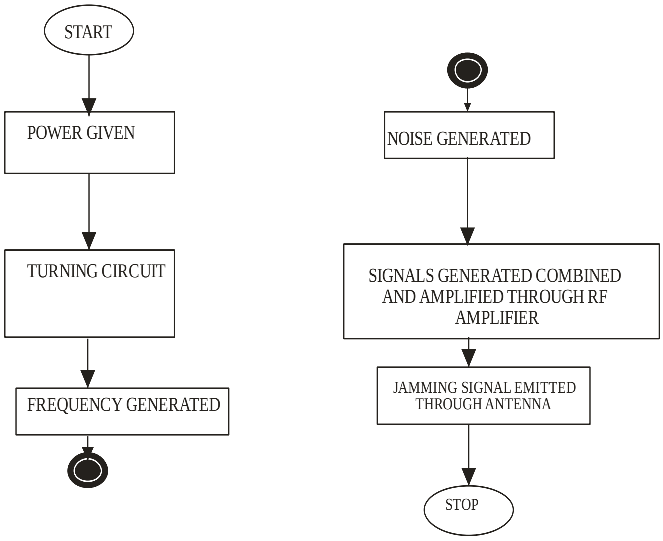


Figure 1: Jammer's Operational Mode

Figure 1 demonstrates the operational mode of the jammer. This means that as the jammer is connected to power, the functional mode gets ready, and turns the circuit to generate a frequency that spreads noise. Hence, the jamming signal gets amplified and emitted through the antenna. These sections and their component constituents are further discussed below.

The Power Supply**.** The power supply is the main source of voltage in the operational circuit and consists of the following main parts: Transformer (for transforming the 220v Alternating Current-AC to other levels of voltages); Rectifier (for converting the AC voltage to a DC one); Filter (for eliminating noise to pave way for the production of DC-voltage); and Regulator (for regulating voltage going into the circuit apparatuses). Furthermore, the power supply circuit has a power indicator known as a Light Emitting Diode (LED**)** of 0.0001A made of a transformer, rectifier diodes, filtering capacitor, limiting resistors**,** LM3905, and LM3912.

The Triangular Wave Generator. This wave generator enables frequency movement of VCO from the lowermost to uppermost level through a feedback system that uses the "phase-locked-loop (PLL)". It usually sweeps the tuning frequency to the VCO. The 555 timer Integrated Circuit (IC) also utilized is meant to operate in a steady manner for it to produce extensive indicators to VCO. In this case, an output frequency of 110KHz for a triangular wave generator was utilized.

The Noise Signal Generator**.** This helps in the production of arbitrary electronic waves in a definite rate gap to block phone signals. To create electronic beats (also called sound or noise), a circuit of two capacitors is linked together and spread on air to obstruct similar signals. Such obstructing beats enhance the jamming transmission, which without it, will make the jamming signal to be a mere broad un-modulated nonstop surge of RF mover.

All signals wedged by such noise are known as signal-to-noise rate which is defined as:

$$\frac{S(F)}{N(F)} = \frac{\text{Average signal P}}{\text{average noise P}}$$

P=power

The total noise power is $\int_{f1}^{f2} P = (f)df$

The overall output of noise (in bandwidth) is evaluated as the additions of the individual mean-squared contributions from each output sinusoid to equal mean-squared value [19].

Assuming the resistors are two in the sequence, the overall voltage is:

$$V_T(t) = V_1(t) + V_2(t)$$

This, therefore, results in:

$$V_T(t)^2 = [V_1(t) + V_2(t)\ ^2]^2$$

$$V_1(t)^2 + V_2(t)^2 + 2V_t(t)\ V_2(t)$$

If sound sources (V_1 & V_2) remain statistically independent emanating from two spate resistors should turn the average of V_1* V_2 becomes zero.

Voltage VP and Vn are the voltages at the respective positive and negative inputs to the amplifier referenced to the ground.

The output voltage for an ideal Operational Amplifier (OP-Amp) is

$$Vo = \left(\frac{R_4}{R_3+R_4}\right)\frac{R_1+R_2}{R_3+R_4}\ Vin_2 - Vin_1\left(\frac{R_2}{R_1}\right)$$

Where:

$V_{THR1}, V_{THR2}, V_{THR3}$, = Thermal Noise from R1, R2, R3; R_n= Inverting "input Effective Series Resistance"; Rp = Non-inverting "Input Effective Resistance; en = Input Voltage-Noise Density at the Frequency of Interest; in = Input Current-Noise Density at the Frequency of interest; T =Ambient Temperature in Kelvin"; K = 1.38 X 10-23 KJ/OK (Boltzmann's constant).

The Mixer Circuit. The mixer is just an amplifier that operates as a summer whereby the triangular signal and noise add together in the mixer before entering the VCO. To achieve the desired target, LM741 was used. There is also a two-channel op-amp mixer circuit with its gain equal to R_5/R_1

and/or R_5/R_2 for channels 1 and 2, respectively. Typically, R1 and R2 are 2.2 to 22kΩ and R5 is 10 to 100Ω, and the top amp is any suitable type, such as a 741 or its numerous variations [20].

The Clamper Circuit. Clamper is a circuit where a capacitor is connected in series with a resistor and diode. The input of VCO is bounded from 0 to 3.5V as a reason for using the clamper to achieve the desired voltage needed for VCO.

The RF – Amplifier. RF-Amplifier helps to expand the jammer's covered area together with its signal-blocking power [19]. In other words, the more power the signal blocker has, the bigger radius it can jam. The RF amplifier circuit will amplify the signal generated by the tuned circuit. Therefore, an ideal differential amplifier occurs when the coefficients of Vin 1 and Vin 2 have identical magnitudes and opposite signs.

$R_1R_4 = R_2R_3$ and the output becomes
$V0 = [R_2/R_1(\text{Vin } 2 - \text{Vin } 1)]$

For the Jammer, a transistor with a high frequency is required, and dealing with the pair associated with the base, R_1 and R_2, they form a voltage divider network with the ratio.
$[R_2/(R_1 + R_2)(\text{Vin } 2 - \text{Vin } 1)] \times 12V = \text{Base voltage}$

$R_1 = 82k\Omega = 82 \times 10^3\Omega = 82{,}000\Omega$
$R_2 = 39k\Omega = 39 \times 10^3 = 39{,}000\Omega$

$$= [39k/(82k + 39k)] \times \frac{12=(39 x 10^3)}{(82 x 10^3 + 39 x 10^3)} = 3.87v(d.c)$$

For current flowing through the base transistor, it is calculated as:

$$Ib = 12/(R_1 + R_2) = \frac{12}{82 x 10^3 x 39 x 10^3} = 0.1MA \quad \therefore Ib = 0.1MA$$

The Voltage Controlled Oscillator (VCO). This helps to generate the RF signal which blocks the mobile signal transmission. The output of the VCO has a frequency that is proportional to the input voltage. In this case, it is possible to change the output frequency by changing the input voltage. More so, CVCO55CL is a more suitable component for blocking the frequency range of 935 to 960 Mhz.

The Antenna. Generally, a transmitting antenna is a necessary part of any transmitter which is usually matched to the transmission system for power transfer optimization. The main characteristic of an antenna is to facilitate the Voltage Standing Wave ratio (VSWR). In this study, therefore, the λ/ 4 upsurge monopole antenna with 50- ohm resistance is utilized to enable it to suit the system of transmission. Additionally, it is branded by a low VSWR of 1.7, a bandwidth of 150 MHz, and about 916 MHz core-frequencies to provide jamming-frequency coverage for the mobile range.

Jamming Techniques

The general techniques of blocking a wireless frequency include "Denial of Service, Shielding Attacks, and Spoofing" [19]. In the denial of service, confusing sounds are spread at par with the mobile's frequency to drop its signal-to-noise-level (SNR), thereby obstructing the flow of messages between the base- station and the mobile [18]. Similarly, the Shielding Attack technique is equally regarded as TEMPEST or EMF- shielding (Electromagnetic). It has to do with concealing a zone in the Faraday- pen to inhibit the spread of useful RF- signals around the pen. Furthermore, in spoofing, functional mobiles are compelled to shut down automatically. This is however often hard to enforce since it would require the jammer to first locate any close-by mobile, before conveying a signal that can deactivate it. Other techniques can descry the signal of a closed mobile and send switch-off or silent mode alerts to the user(s). Above all, this study adopts the Denial- of- Service method.

The Jamming Distance (D). The jamming distance refers to the parameter area in which the jamming device output power would be able to block transmission of the mobile. In designing this jammer; D = 20 meters for DCS1800 – band, GSM 900- band, UMTS 2100, and LTE900/ 1800.

The frequency bands. In Nigeria, mobile networks operate on "900 MHz, 1800 MHz (2G)", 2 GHz/ UMTS 2100 (3G), and LTE700-2300 (4G) bands like most European- carriers. GSM 900 "(Uplink 890- 915 MHz Downlink 935- 960 MHz); DCS 1800 (Uplink 1710- 1785MHz- 1785 MHz; Downlink 1805-1880 MHz)" [18]. Thus, this jammer design is anchored on the downlink, since it provides lower power than the uplink, to carry out jamming without affecting the base station. Therefore, a successful jamming attack is possible based on the following jammer equation of "jamming- to-signal rate (JSR)" [21].

JSR = (jPGjrGrjRtrLrBr)/(tGtrGrtRjrLjBj)

These symbols are interpreted as:

jP = "jammer power; Gjr = antenna gain from jammer to receiver; Grj = antenna gain from receiver to jammer; Gtr = antenna gain from transmitter to receiver; Grt = antenna gain from receiver to transmitter; Br = jamming transmitter bandwidth; Bj = jamming transmitter bandwidth; Rtr = range between message transmitter and receiver; Rjt = range between jammer and message receiver; Lj = jammer signal loss (including polarization mismatch); Lr = communication signal loss" [21].
Moreover, the GSM-UMTS-LTE system SNR ranges from a minimum of 9 dB to maximum power of Pr 15 dBm, in addition to a free-space (FSPL or path loss) as indicated in the formulae given below.

$$FSPL\ (dB) = 10\log_{10}\left[\frac{(4\pi df)^2}{c}\right]$$

Where:
F = the signal frequency/hertz; $\boldsymbol{\lambda}$ = the signal "wavelength/meters; c = the speed of light in a

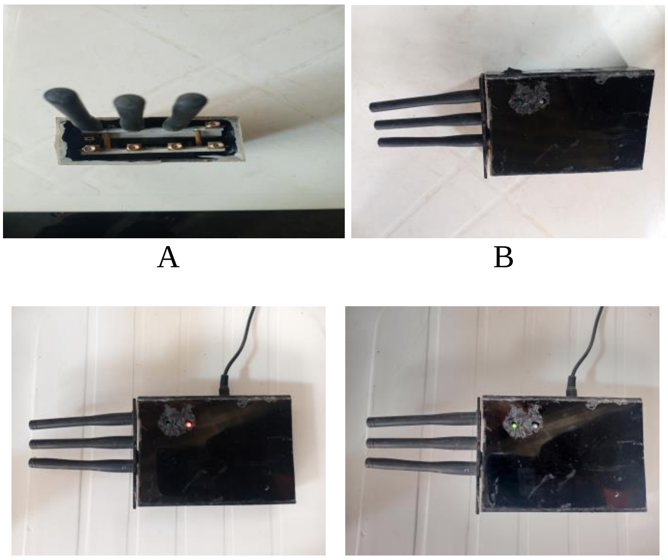
vacuum,2.99792458 x 10 meters per second; d = the distance from the transmitter/meters" [19]. Moreover, the outside -free- loss (that is, F's worst- case) is bound to occur when the highest rate is applied to the FSPL equation. Therefore, 1880 MHz results in "F (dB) = 32.44 20 LOG0.01 20 log 1880 which gives F = 58 dB".

Computation of Power Rate. It is necessary to ascertain the amount of power transmission for the device to jam any mobile within 20 meters distance. In doing this, it is apt to consider the highest power signal and the SNR for the mobile receiver. Nevertheless, a good jammer should possess an SNR equivalent of 9dB as its most terrible benchmark. The idea is to determine output power such that with the addition of path loss, the desired mark of jammer power is gotten.

Aiming at GSM 900/ LTE 700- 900;
Lowest SNR = 9dB
Highest receiver's power S = -15 Bm
Therefore, jammer power Jr is s/jr = 9dB
Hence, Jr = S- 9 = - 15-9 = -24 dBm
Jammer power output = -24 dBm60.04 = 36dBm ≅4.0 W

Aiming at GSM 1800/ UMTS/ LTE 1800- 2300;
Lowest SNR = 9dB
Highest S = -23 dBm
Then, Jr = -23-9 = -32 dBm
Jammer power output = -32 dBm65.88 = 33.88 dBm ≅2.5 W8

4. Results and Discussion



A B C D

Figure 2: The Jammer

Table 2: Reading of Voltages and Frequency Obtained

"Voltage Tune (+Volts DC)"	"Frequency Output (MHz)"
0.0	790
0.1	810
0.2	830
0.3	850
0.4	870
0.5	890
0.6	910
1.2	1820

The mobile jammer as seen in figure 2 is portable and has three antennas, two light indicators, as well as an off-and-on switch by the side. Figure 2A displays the top internal part, 2B (not connected to power) captures the front and side views, while 2C demonstrates the off-light indicator and 2D shows the on-light indicator when connected to power. This means that when the jammer is connected to power, one indicator light is shown, but once it is turned on the two indicator lights are demonstrated which is the operational mode, as seen in figure 2D.

On the other hand, table 2 displays the turning voltage in DCs and the frequency outcome in MHz. in this regard, every unity changes results in additional 20MHz, from a starting point of 790 MHz. In the testing proper, there were disruptions of mobile signals which affected communication flow from the base- station. As mentioned earlier, the sounds produced by the jammer help to generate frequencies equivalent to those of the mobiles as recorded in table 2. This testing was repeated more than once to overcome the tendencies of chance occurrence.

More so, the cell- phone signals jammed were only successful on 2G and 3G systems by means of MTN, Airtel, Glo, and Etisalat (9mobile) package providers. The mobile phones were found indicating "out of service", and at that point, the calls could not connect through. This feat was not robust with a distance of 20-meter parameter, as the effectiveness of the jammer was found to reduce while the mobile phones were shifted towards the benchmark testing limit (20-meters). Conversely, this test did not successfully jam the 4G network which may be due to configuration issues, though it therefore calls for further investigations. Additionally, turning off the jammer did not restore mobile phones' service until they were reset. This means the mobile phones were restarted or put off and then on before use.

Furthermore, paying little attention to issues of jamming distance range is seemingly crucial to the success of this study. As realized in the testing phase, the jamming capacity of this device is very effective when mobile phones are found less than 20 meters distance. In line with similar findings, contributory factors to this outcome may include the location and settings of buildings, distance to towers, and temperature among others. As part of suggestions to improve on this development, an advanced powered- RF- amp is conceivably needed for the jammer range [19]. Jamming range is an important part of this study because it either determines the safety purpose of restricting mobile communication within prohibited parameters, or whether other legitimate mobile phone users outside of the targeted parameters are cut off.

Although, in Nigeria like many other countries of the world, there is a general consensus of ensuring the safety of lives and property in a hazardous environment, public places, organizations, restricted areas, or heavy security base when mobile jammer is used there; the implications of jamming cell-phones in these zones can have similar effects on every cell-phone user within the affected parameters. This means that both visitors or customers and residents or staff become parallel victims of no communication.

In other words, jamming cell phone signals in filling stations, religious/public gatherings, security formations, and the like will equally shut down the communication system of the entire organization leaving even the staff to rely only on face-to-face communication. Hence, external mail and emergency information circulation will cease. This is as well, dangerous to contemporary organizational information sharing which enhances effective service delivery. Therefore, these issues call for flexible application of cell phone jammers in public spaces without causing communication barriers to management and staff and without preventing external correspondence. Above all, the safety implications of these findings are premised on the need to avoid hazardous and criminality outbreaks, and also to guarantee internal/external organizational communication and correspondence, especially in an emergency situation.

5. Conclusion and Future Scope

This study was an attempt to envisage the possibilities of developing mobile jammers for the safety implications of lives and property, as well as the organizational community system particularly to receive emergency alert messages. The jammer was constructed and tested on the four major mobile network providers in Nigeria: Airtel, Globacom, MTN, and 9Mobile within an effective jamming range of 20 meters. The 2G and 3G were successfully jammed within less than 20 meters range, while that of 4G was not successful. It is therefore safer to implement mobile jammers in places associated with dangers after securing full permission and approval from the government as specified by NCC in the case of Nigeria. In other words, more sophisticated jammers can be designed to jam mobile phones with 4G networks to suit the safety implications of both hazards and effective organizational communication systems. This should only be implemented in restricted parameters of areas within the confines of the law by seeking and securing legitimate approval. The jamming should also be carried out without degrading effects on the transmission systems of base stations and/or untargeted mobile phone users.

Data Availability
This study did not collect data for analysis because it is in the form of a technical note where literature was reviewed.

Conflict of Interest
There is no conflict of interest

Funding Source
None

Author's Contributions
Author 1 initiated the topic, gather materials, constructed the jammer, drafted the manuscript, and edited the article.

Acknowledgment
The contributions of the research panels of the Physics Department at the University of Jos, and radio and phone technicians who provided some practical insights are hereby appreciated for the outcome of this study

REFERENCES

[1] S. Zorn, M. Maser, A. Goetz, R. Rose, L. Weigel, "A power saving jamming system for e-GSM900 and DCS1800 cellular phone networks for search and rescue applications", *In the Proceedings of Wireless Sensors and Sensor Networks (WiSNet), IEEE Tropical Conference*, pp. 33-36, January 16-19, 2011.

[2] M. Al-Rawi, M. Al-Rawi, "System design of cell phone detector", *ACTA Technica Corviniensis – Bulletin of Engineering*, TOME XIII, 2020.

[3] S. Mahato, C. Vimala, "Cellular Signals Jamming System in 2G And 3G", *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering*, 2015.

[4] G. Miao, J. Zander, K.W. Sung, B. Slimane, "Fundamentals of Mobile Data Networks", *Cambridge University Press*, 2016.

[5] J.M. Mom, M.S. Adejoh, O.D. Agbo, "Implementation of GSM Detection System with Remote Jamming Capabilities," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 3, Issue 4, pp. 67-71, 2020.

[6] K.M. Shantanu, C. Vimala. C. "Cellular Signals Jamming System in 2G and 3G", *In the Proceedings of International Conference on Signal Processing, Embedded System and Communication Technologies and their applications for Sustainable and Renewable Energy*, Vol. 3, No. 14, pp. 2278 – 8875, 2014.

[7] J. Madhu, H. Keerthana, M. Priyatham, "Remote controlled mobile signal jammer", *International Journal of Engineering Research in Electronics and Communication Engineering*, Vol. 4, No. 11, pp. 245-248, 2017.

[8] V. Mupparaju, S. Yembadi, "Advanced Mobile Phone Signal Jammer for GSM, CDMA and 3G Networks with Prescheduled Time Duration using ARM 7", *International Journal of Professional Engineering Studies*, Vol. 1, No. 2, Dec., 2013.

[9] Y. Fitriyani, A.B. Mutiara, R. Refianti, "Yagi Antenna design for signal phone jammer", *Journal of Theoretical and Applied Information Technology*, Vol. 43, No. 1, pp. 39-44, 2012.

[10] S. Shahdadpuri, J. Patel, "GSM mobile phone jammer", *International Journal for Scientific Research and Development*, Vol. 2, No. 8, pp. 154-158, pp. 2014.

[12] U.E. Uno, P.F. Okoye, N.V. Charles, "On the Physics of GSM Jammer and its Application in Lecture Theaters", *Science Journal of Physics Publication* 2276-6367, 10pp, 2013.

[13] O.O. Olumide, O.O. Jimoh, L.A. Olaide, "Design and development of mobile phone jammer", *American Journal of Engineering Research*, Vol. 5, No. 2, pp. 71-76, 2016.

[14] O.A. Arowolo, A. Adekunle, "Development of frequency signal jammer", *FUOYE Journal of Engineering and Technology*, Vol. 3, No. 4, pp. 28-30, 2019.

[15] Y.P. Umratkar, H.B. Chalfe, S.K. Totade, "Design and Performance of Mobile Phone Jammer", *International Journal of Engineering Technologies and Management Research*, Vol. 6, No. 12, 1-5, 2019.

[16] K. Rameshbabu, M. Mangisthu, M.B. Wondosen, "Design and implementation of mobile phone jammer with prescheduled time duration", *International Journal of Advanced Research in Computer and Communication Engineering*, Vol. 7, No. 6, pp. 40-46, 2018.

[17] J.A. Ganiyu, O.A. Olamide, O. Olanrewaju, Y.N. Asafe, "Cell phone disable system", *ACTA Scientific Computer Sciences*, Vol. 4, No. 8, pp. 35-39, 2022.
[18] N. Nkordeh, L. Iwu, F. Idachaba, I. Bob-Manual, "Design and implementation of a dual band mobile phone jammer", *In the Proceedings of World Congress on Engineering and Computer Science*, Vol. 1, pp. 1-8, October 19-21, 2016.
[19] D.S. Madara, E. Ataro, S. Sitati, "Design and testing of a mobile-phone-jammer", *Innovative Systems Design and Engineering*, Vol. 7, No., 7, pp. 7-18, 2016.
[20] D.M. Pozar, "Electromagnetic Theory in Microwave Engineering: 3rd ed.", *John Wiley and Sons, Inc*., Hoboken, NJ, 2005.
[21] M. Tata, "Programming and customizing the PIC microcontroller: Third edition", *McGraw-Hill Education Pvt. Ltd*, 7 West Patel Nagar, New Delhi 11008, 2015.

AUTHORS PROFILE

Mr. N. Nwokocha pursued Bachelor of Science and Master of Science in Physics from the University of Jos, Nigeria from 2009 to 2016. He is currently a Ph.D. applicant and also pastoring in a Nigerian Church. His main research interest focuses electronics and communication technology, Network Security, and Computer Intelligence education. He has over 5 years of teaching experience in electronics and communication.


Int. J. of Scientific Research in Biological Sciences
www.isroset.org
Int. J. of Scientific Research in Chemical Sciences
www.isroset.org
Int. J. of Scientific Research in Computer Science and Engineering
www.isroset.org
World Academics Journal of Engineering Sciences
ISSN:2348-635X
www.isroset.org
Journal of Physics and Chemistry of Materials
ISSN:2348-6341
www.isroset.org
Int. J. of Scientific Research in Mathematical and Statistical Sciences
www.isroset.org
International Scientific Research Organization for Science, Engineering and Technology
ISROSET
Submit your manuscripts at
www.isroset.org
email: support@isroset.org
Make a Submission
ISSN: 2349-3178 (Print), ISSN: 2349-3186 (Online)
International Journal of Medical Science Research and Practice
Published by ISROSET
Int. J. of Scientific Research in Multidisciplinary Studies
www.isroset.org
Int. J. of Scientific Research in Network Security and Communication
e-ISSN: 2321-3256
World Academics Journal of Management
ISSN: 2321-905X
www.isroset.org
Int. J. of Scientific Research in Physics and Applied Sciences
www.isroset.org
Int. J. of Computer Sciences and Engineering
www.ijcseonline.org