Design and Implementation of a GSM Mobile Detector and Jammer

Albert Kofi Kwansah Ansah *Member, IAENG*

***Abstract*—The use of mobile telephones may be nuisance at certain areas and functional places where silence is imperative. This paper seeks to design a pocket sized Global System for Mobile Communications (GSM) jammer device that transmit signals on the same frequency at which GSM system operates to prevent cellular phones from receiving and transmitting signals to the base station. The artistry used is designing systematic combination of analogue components including, capacitors, inductors, transistors and resistors which helps to generate the frequency (Noise) needed and then amplified to increase the transmitted power. The generated frequency lies in the range of 860 MHz and 1900MHz in order to match the frequency of the main serving base station. The circuit detects the incoming and outgoing calls, SMS and video transmission even if the mobile phone is kept in the silent mode. Our GSM jamming system provides cost effective solution in any area where cellular communications ring tones frequently cause nuisance.**

***Index Terms*— Mobile Jammer, GSM, Mobile Detector, Radio Frequency, Signal Detection**

I. INTRODUCTION

A GSM jammer is a device that transmit signal on the same frequency at which the GSM system operates. GSM jamming devices were originally developed for law enforcement and the military to interrupt communications by criminals and terrorists [1]. The jamming process succeeds when the mobile phones in the designated area are disabled by the jammer. Organizations and some notable places suffer from the use of cell phones that tends to create excessive forms of noise and frustrate most people to grumble and occasionally go extreme to retaliate. Mobile phones may be an annoying device in working ambient, study area, prayer places, movie theatres, hospitals etc. Wireless mobile jammer can be placed in places such as schools, mosques, conference halls, meeting rooms, library and other places that desire serene and diplomatic environment. This jammer device is capable of adulterating and interrupting the transceiving of GSM signals. The jamming device broadcasts an RF signal in the frequency range reserved for cell phones and interferes with the cell phone signal resulting in *"no network available"*. The jamming effectively acts on mobile phones within the defined regulated frequency and zones where the jammer device is planted without causing any interference to other communications. Jamming devices overpower the cell phone by transmitting a signal on the same frequency as the cell phone and at a high power that the two signals collide and cancel out. It should be mentioned that cell phone jammers are illegal devices in most countries. The disadvantage of the mobile jammer is that, transmission of the jamming signal is prohibited by law in many countries and goes with fines. Use of RF jammers are constrained due to transmission of high power signals that may affect operation of critical devices [2].
The uniqueness of our system is that, it can be fully implemented with a minimal budget.

The rest of the paper is sectioned as follows; section two presents the review of related literature. Design of mobile detector and jamming device is captured in section three and section four discusses the implementation and testing. Section five draws out some conclusions.

II. RELATED LITERATURE

Communication jamming devices were first developed and used by the military in situations where tactical commanders used RF Communications to exercise control of their forces where an enemy has interest in those communications [3]. Lately jammer devices are becoming civilian security products rather than electronic warfare devices with the increasing number of mobile phone users to protect specific places where the ringing of mobile phone would be disruptive. According to Federal Communications Commission (FCC) manufacture, importation, sale or offer for sale of devices designed to jam wireless transmissions is prohibited [4].

A. GSM Operation

Cell phones are designed to add power if they experience low-level interference, therefore jammer must recognize and match the power increase from the phone. Some jammers block only one of the frequencies used by cell phones. Less complex devices block only one group of frequencies, while sophisticated jammers block several types of networks at once to head off dual-mode or tri-mode phones that automatically switch among different network types to find an open signal. Although different cellular systems process signals differently, all cell phone networks use radio signals that can be interrupted. Jammers can broadcast on any frequency and are effective against Code Division Multiple Access (CDMA), Time Division Multiple Access (TDMA), GSM, Personal Communication Service (PCS), and Distributed Controlled System (DCS). A cell phone works by communicating with its service network through a cell tower or base station which divides a city into small areas or cells [5]. A jamming device transmits on the same radio

Manuscript received February 19, 2018; revised April 1, 2018.
A. K. Kwansah Ansah is with the Computer Science and Engineering Department of University of Mines and Technology, Tarkwa-Ghana (phone: +233 5033 22554; fax: +233 3123 20306; email; afkansah@umat.edu.gh).

frequencies as the cell phone hence disrupting the communication between the cell phone and the base stations i.e. denial-of-service attack. The jammer denies service of the radio spectrum to the cell-phone users within range of the jamming device.

Older jammers sometimes were limited to working on phones using only analogue or older digital mobile phone standards. Newer models such as the double and triple band jammers can block all widely used systems and are very effective against newer phones which hop on different frequencies and systems when interfered with. The power of the jammer's effect can vary widely based on factors such as proximity to towers, indoor and outdoor settings, presence of buildings and landscape, temperature and humidity. There are concerns that crudely designed jammers may disrupt the functioning of medical devices such as pacemakers [6]. Fig. 1 shows a typical operation of jammer between cell phone and base station. Cell towers 1 and 2 (Fig. 1) transmit signals which can be received by GSM or radio sets. The jamming device placed between towers 1 and 2 produces a signal with same frequency being transmitted by the tower. This produce a resultant sign of zero. Cell phones use one band to send signal to the base station (upward signal) and another band to receive signal from base station (download signal). Mobile phone can be disabled via interrupting any of these signals. Because the distance to the base station is larger than the distance to mobile phone that needs to be blocked, it needs less energy to block signal from base station to phone.

B. GSM MOBILE JAMMER AND DISABLERS TECHNIQUES

TYPE A Device: Jammers

Type A device overpowers cell phone's signal with a stronger signal and comes equipped with several independent oscillators transmitting jamming signals. By means of RF interference, it prevents all pagers and mobile phones located in the catchment area from receiving and transmitting calls. Type A transmits only a jamming signal with pretty poor frequency selectivity. [1].

TYPE B Device: Intelligent Cellular Disablers

Type B devices do not transmit an interfering signal on the control channels but functions as a detector. It has a unique identification number for communicating with cellular base station. When it detects the presence of a mobile phone, prevention of authorization of call establishment is done by software at the base station and no communication is established between the mobile phone and the base station. The system is capable of recognizing and allowing all emergency calls routed to 911 [1].

TYPE C Device: Intelligent Beacon Disablers

Type C devices when located in a designated *"quiet"* area, functions as a beacon and any compatible terminal is instructed to disable its ringer or operation. Only terminals which have a compatible receiver would respond and typically built on a separate technology from cellular/PCS. This technology does not cause interference and does not require any changes to existing PCS [1].

TYPE D Device: Direct Receive and Transmit Jammers It behaves like a small, independent and portable base station, which can directly interact intelligently or unintelligently with the operation of the local mobile phone. The jammer is predominantly in receiving mode and will intelligently choose to interact and block the cell phone directly if it is within close proximity of the jammer. This selective jamming technique uses a discriminating receiver to target the jamming transmitter. It also discriminates 911 calls and allow for breakthroughs during emergencies [1].

TYPE E Device: EMI Shield - Passive Jamming

This technique uses EMI suppression to make a room into what is called a Faraday cage. Although it is labour intensive to construct, the Faraday cage essentially blocks, or greatly attenuates, virtually all electromagnetic radiation from entering or leaving the cage or target room. With current advances in EMI shielding techniques and commercially available products one could conceivably implement this into architectures of newly designed buildings for quiet conference rooms. 911 calls are blocked unless there was a way to receive and decode their transmissions [1].

C. GSM – MOBILE JAMMING REQUIREMENTS

Jamming objective is to inject an interference signal into the communications frequency so that the actual signal is completely submerged by the interference to hinder reception at the other end. It is important to notice that transmission can never be totally jammed. Successful jamming denies the usability of the communications transmission and requires that jammer power is roughly equal to signal power at the receiver. In digital communications, usability is denied when error rate of transmission cannot be compensated by error correction. The effects of jamming depend on the jamming-to-signal (J/S) ratio (Eqn. 1), modulation scheme, channel coding and interleaving of the target system [2].

$$\frac{J}{S} = \frac{P_j G_{jr} G_{rj} R_{tr}^2 L_r B_r}{P_t G_{tr} G_{rt} R_{jr}^2 L_j B_j} \tag{1}$$

P_j = jammer power

G_{jr} = antenna gain from jammer to receiver

G_{rj} = antenna gain from receiver to jammer

R_{tr} = range between communication transmitter and receiver

B_r = communication receiver bandwidth

L_r = communication signal loss

P_t = transmitter power

G_{tr} = antenna gain from transmitter to receiver

G_{rt} = antenna gain from receiver to transmitter

R_{jr} = range between jammer and communication receiver

ISBN: 978-988-14048-1-7
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

B_j = jammer bandwidth

L_j = jamming signal loss

Eqn. 1 indicates that the jammer Effective Radiated Power (product of antenna gain and output power), should be high if jamming efficiency is required. On the other hand, to prevent jamming, antenna gain toward the communication partner must be as high as possible while the gain towards the jammer should be kept small. The antenna pattern; thus relation between the azimuth and the gain, is an important aspect in jamming [1]. The distance has a strong influence on the signal loss. If the distance between jammer and receiver is doubled, the jammer has to quadruple its output to achieve same effect. It must also be noted here that the jammer path loss is often different from the communications path loss hence it gives jammer an advantage over communication transmitters [3].

GSM Frequency Hopping does not provide real protection against jamming attacks. However, interleaving and forward error correction scheme of GSM Systems can protect GSM against pulsed jamming. A jammer requires 5 dB S/J in order to successfully jam a GSM channel of SNR 9 dB. The optimum GSM SNR is 12 dB, after which the system begins to degrade. To expurgate an existing connection, the jamming has to last at least until the call re-establishment timer at the MSC expires and connection is released, which means that an existing call can be cut after a few seconds of effective jamming [4]. In most cases, the efficiency of a cellular jamming is very difficult to determine, since it depends on many factors, which leaves the jammer confused [3].

III. DESIGN

The GSM jammer (Fig. 2) comprises the Power Supply, IF Section and RF Section. The Power Supply (Fig. 3) is used to supply needed voltages to the other sections. Its components consist of 220VAC transformer, rectifier to convert the AC voltage to DC, filter which is used to eliminate the fluctuations in the output of the full wave rectifier to produce constant DC voltage and a regulator to provide a desired DC-voltage. The function of the IF-section is to generate the tuning signal for the VCO in the RF-section to sweep the VCO through the desired range of frequencies. This tuning signal is generated by a triangular wave generator (110 KHz) along with noise generator, and offset by apt amount to sweep the VCO output from minimum desired frequency to maximum. Its components are timer IC (Triangular wave Generator), Zener diode (Noise Generator) to provides the output noise and mixer summer. In the design 555timer IC was used operating in the a-stable mode to generate the sweeping signal. The output frequency depended on the charging and discharging of the capacitor, resistors values and the power supply for the IC. Fig. 4 shows how 555timer was used in the general A-stable mode.

The charging (Eqn. 2) and discharging (Eqn. 3) times for the capacitor can be found as follows:

$$Tc = 0.693\left(R_a + R_b\right) * C \qquad (2)$$

$$TD = 0.693\ R_b * C \qquad (3)$$

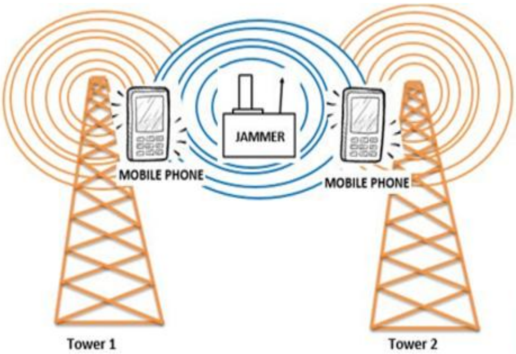

Fig. 1a - Jammed Towers

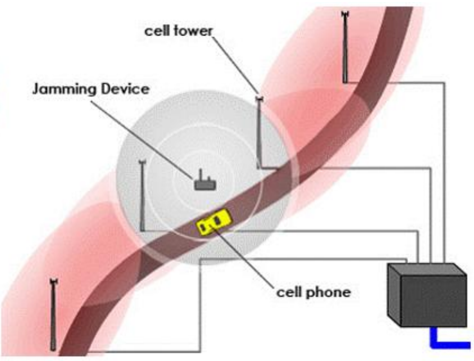

Fig. 1b - Jammed Towers

Table 1 – Comparison of Jammer/Disablers Techniques

Type	Emergency Call	Efficiency	Regularity Approval	Implementation
A	Blocked	Low	Not allowed	Very simple
B	Allowed	Medium	Required	Complex (Required Third Party Cellular/PCS Services)
C	Allowed	High	Required	Complex (Required Intelligent Handset)
D	Allowed	Medium	Required	Simple
E	Blocked	High (No- signal transmitted)	Allowed	Simple

The output frequency can be calculated with Eqn. 4.

$$f_{out} = \frac{1.44}{\left(R_a + 2R_b\right) * C} \quad (4)$$

This design required a duty cycle (D.C.) of 50% which means the capacitor charging and discharging times are equal. This can be done by making $R_a = R_b$ and placing a diode across Rb. The output frequency is given in Eqn.

$$f_{out} = \frac{1.44}{\left(R_a + R_b\right) * C} \quad (5)$$

The output of VCO is just an un-modulated sweeping FR carrier with noise. Therefore, the triangular signal was mixed with noise signal (FM modulating the RF carrier with noise) generated Zener diode operated in reverse mode. Reverse mode causes avalanche effect to create wide band noise which is then amplified and used in our system. Two amplification stages were used. Firstly, NPN transistor as comer emitter, and secondly LM386 IC as Audio amplifier. The most imperative part of the jammer is the RF-Section. It is the output of this section that interfaces with the cell phone. The RF-section consists of three parts; namely voltage controlled oscillator (VCO), power amplifier and antenna with the VCO being the heart and generates the RF signal which will interfere with the cell phone. The VCO has a frequency output proportional to the input voltage and therefore, could be controlled by altering the input voltage. The output is a specific frequency when the input voltage is DC, and spans a specific frequency range when input is a triangular waveform. In our design, we used a VCO for GSM 900 and GSM 1800. Three selection criteria were used in this design; VCO must cover the bands that we need, readily available at low cost, and run at low power consumption. CVCO55BE was selected for GSM 1800 with output frequency ranging between 1785 and 1900 MHz and output power up to 5 dBm and CVCO55CL for GSM 900 which, has an output frequency between 925 and 970 MHz and output power up to 8 dBm. The ICs chosen were based on; surface amount, large output power, same output supply power of 5V and having same noise properties. The Power Amplifier was added to increase the VCO output to the desired 34bBm since 5 dBm output power does not achieve the desired output power of the GSM jammer. PF08109B amplifier IC was used due to its suitability, cheap, easy to get and has a high gain of 35 dB. As datasheets illustrated that this IC is designed to work in dual band GSM and DCS by using two power amplifier ICs [4]. A proper antenna is necessary to transmit the jamming signal. Two 1/4 wavelength monopole antennas with 50Ω input impedance were used so that they are matched to the system. In order to have optimal power transfer, the antenna system must be matched to the transmission system. I used monopole antenna since the radiation pattern is Omni-directional.

IV. IMPLEMENTATION AND OUTCOME

A. IMPLEMENTATION

The circuit was designed to detect calling process and issues a warning signal to the control system to shift the jamming into power on mode. The circuit (Fig. 6) can sense the presence of an activated mobile phone from a distance of one and half (1.5) meter. It can detect incoming and outgoing calls, Short Message Service (SMS) and multimedia data. The bug detects RF signal from an activated mobile phone, alarm beeps and Light Emitting Diode (LED) blinks. The alarm continues until the signal transmission ceases. The design (Fig. 5) consists of four stages; sensor stage (SS), power stage (PS), operational amplifier (OM) and response stage (RS). The RF antenna receives wireless signal when circuit is powered by 9 Volts DC battery. OM amplifies the received signal which in turn triggers the buzzer and makes the LED to flicker. Buzzer alarm continues until the signal transmission ceases.

The construction was first done on a bread board and transferred on to a PCB (Fig. 7). The OM IC chip (U1) was placed on board straddling the channel. Orientation of the chip was noted after which the variable resistor was placed with pins on separate rows. Centre pin of the variable resistor (R5) is connected to Pin 6 of the IC while Pin 4 of the IC is connected to the bottom left row. Several other locations will use this connection for ground. A 6.8 MΩ resistor (R2) and a capacitor (C1) are connected between Pin 3 and Pin 4 of the IC. It should be noted that Pin 4 is connected to ground. A capacitor (C2) is then connected between Pin3 and Pin 2 of the IC. A 6.8 MΩ resistor (R1) is connected between Pin 3 of the IC and bottom pin of the variable resistor. A wire is needed to make this connection. It should be noted that the bottom Pin1 of the variable resistor will be connected to the battery positive terminal. A 6.8 MΩ (R3) is also connected between Pin 1 and Pin 2 of the IC. One leg of the 1KΩ (R4) is connected to Pin 7 of the IC. Other leg of the LED is connected to Pin 8, and the short leg to the row above Pin 8. A wire is connected to the bottom right row to the long leg of the LED (Pin 8). One end of a long wire (antenna) is connected to Pin 2 of the IC.

B. TESTING AND RESULTS

When an activated phone is in detection range, voltage across each component increases or drops. There is a fluctuating voltage drop across C1, C2, C3 and OP LM358AN as the signal is received by the antenna. The fluctuation is due to the irregularity of the signal (sine wave). The voltage across the LED also increases and fluctuates as the signal comes and goes at a voltage of 1V and above. Bug detects RF transmission signal from an activated mobile phone and starts sounding beeping the alarm and blinks LED (Fig. 8). The alarm continues until the signal transmission ceases. Fig. 9 shows device not detecting cell phone signal.

ISBN: 978-988-14048-1-7
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

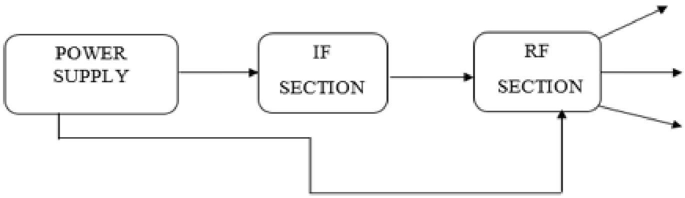

Fig. 2 - Block Diagram of the GSM Jammer

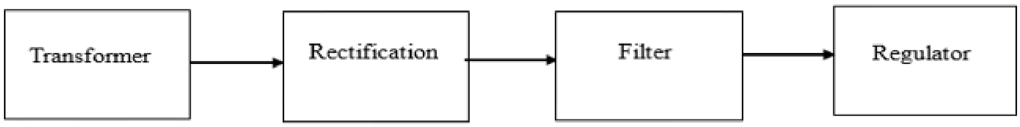

Fig. 3 - Parts of the Power Supply

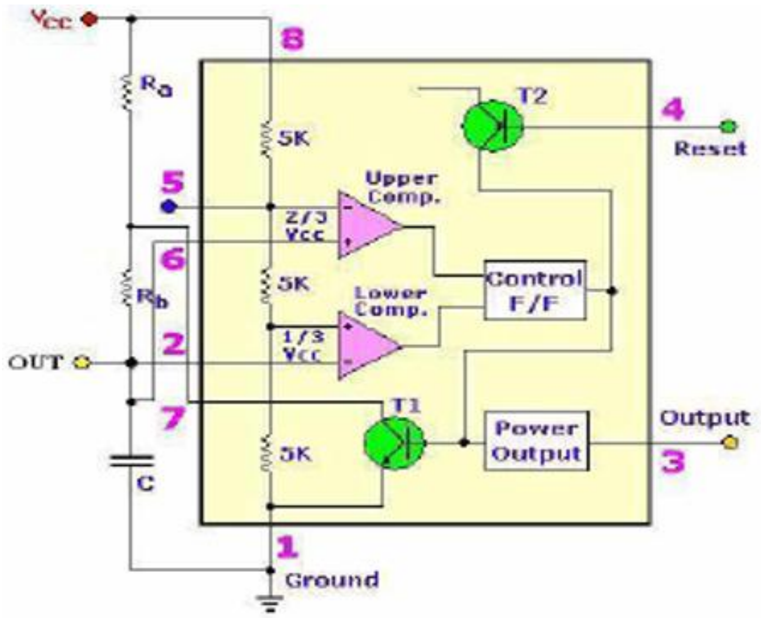

Fig. 4 - A-stable 555 timer

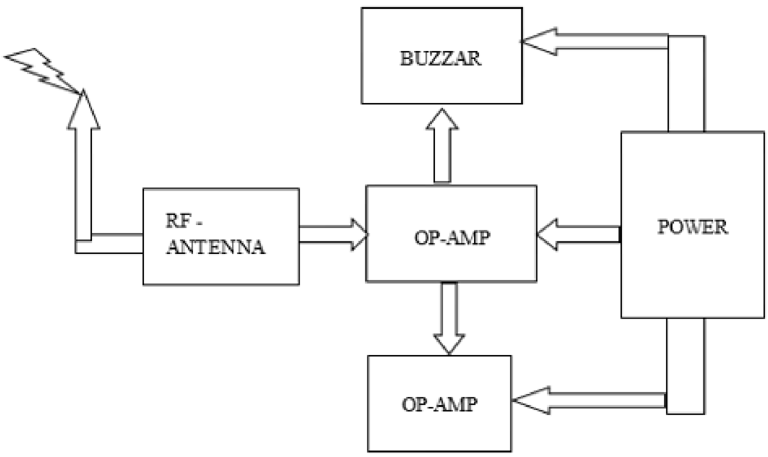

Fig. 5 - Block diagram of the Cell Phone Detector

ISBN: 978-988-14048-1-7
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

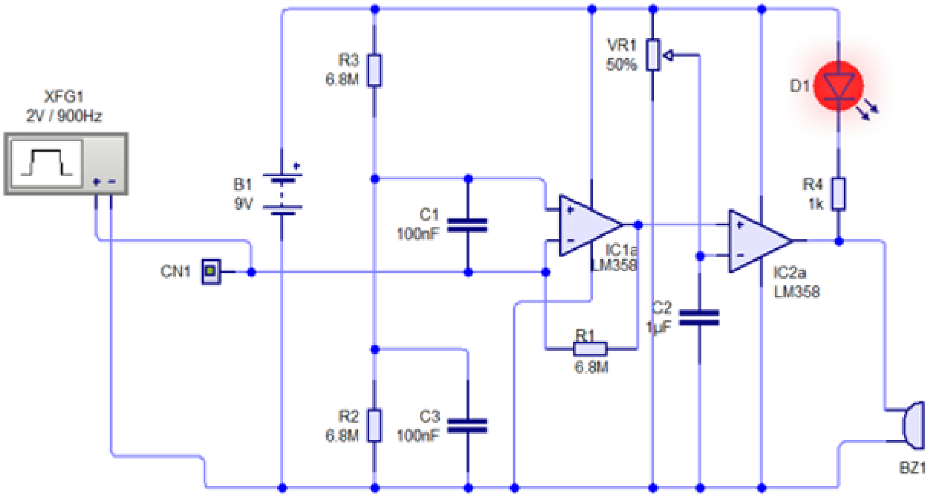

Fig. 6 - Schematic Diagram of the Cell Phone Detector using Circuit Wizard

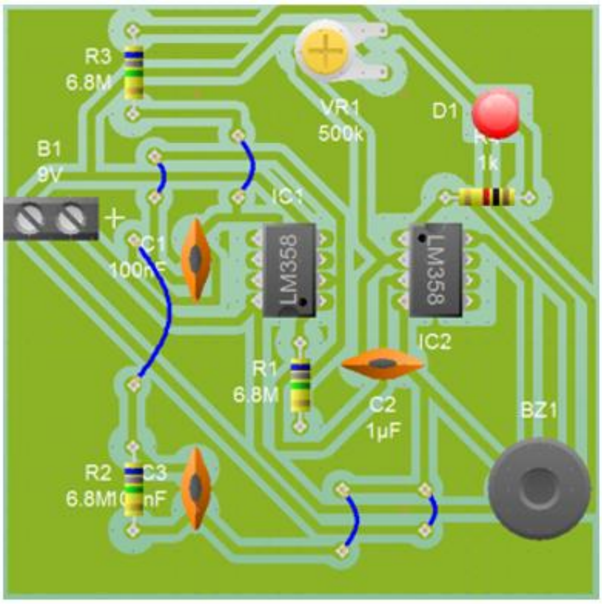

Fig. 7 - PCB Layout of the Detector

Fig. 8 - Device Detecting Phone Signal

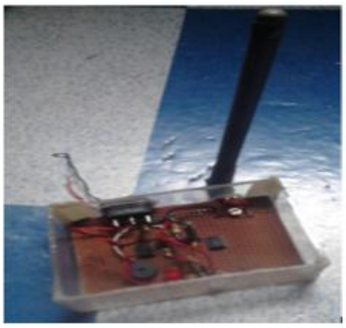

Fig. 9 - Device not detecting Phone Signal

ISBN: 978-988-14048-1-7
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

V. CONCLUSIONS

In this paper, a GSM mobile jammer was successfully designed and implemented. The implemented detector circuit could sense the presence of an activated mobile cell phone from a distance of 1.5m. The device could detect the presence of an active phone using both GSM 900 and GSM 1800 bands and prevents it from ringing. The desired frequency needed to make noise during the jamming process was achieved.

REFERENCES

[1] Anon. (2006), "Mobile Jammer Wiki", http://www.seminarsonly.com/Labels/Mobile-Jammer-Wiki.php Accessed: March 29, 2015.

[2] Mahato, S. K., Vimala, C. (2014), "Cellular Signals Jamming System in 2G And 3G", *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering Vol. 3, Issue 3*, April 2014

[3] Jisrawi, J. (2006), "GSM-900 Mobile Jammer", undergraduate Project, Jordan University of Science and Technology (JUST), Jordan, pp 5-27.

[4] Ahmed S. and Ahmad N. (2006), " Dual Band Mobile Jammer for GSM 900 & GSM 1800", undergraduate Project, Jordan University of Science and Technology(JUST), Jordan, 5-23 pp.

[5] Schiller, J. H. (2003), "Mobile Communications" Addison Wesley-Pearson Education Ltd., England. pp. 29-35.

[6] Anon. (2015), "Cell Phone Jamming Device – HowStuffWork", http://www.electronics.howstuffworks.com/cell-phone-jammer2.htm

[7] Anon. (2013), "Construction of Radio Frequency GSM Signal Jammer" www.pubs.caritasuni.edu.ng/?dir=projects/2012-2013%20Projects/Electrical%20AND%20Electronics%20Engineering. Accessed: March 10, 2015.

ISBN: 978-988-14048-1-7
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)