ISSN 2278-3091

**International Journal of Advanced Trends in Computer Science and Engineering**, Vol.3 , No.4, Pages : 29-32 (2014)
*Special Issue of ICCEIT 2014 - Held on September 01, 2014 in The Solitaire Hotel, Bangalore, India*

# Cell Phone Detection and Jamming System for GSM - 900 MHz and 1800 MHz Frequency Bands

**Rehna V J [1], Kehkeshan Jalall S [2], Hasrsha K[3], Vinay V[4]**
[1]Research Scholar, India ,Rehna_vj@yahoo.co.in
[2]Asst Professor, India, Kehkeshaneng@yahoo.co.in
[3]Asst Professor, India, Harsha_karamchandani@yahoo.co.in

**Abstract *:*** This paper deals with the design & implementation of a low cost Cell Phone Detection System with a "Denial of Service" technique jamming. The cell phone detector is a RF based sensor which monitors the RF activity in the vicinity. The Jammer generates a RF signal on the same frequency as that used by the Communication carriers with modulated noise with a greater power than that of that of the original signal. This causes collision between the two RF signals, which cancels the incoming or outgoing signal from the cell phone with respect to the Base station.

**Key words :** Base Station (BS), Denial of Service (DoS), Radio Frequency (RF).

## INTRODUCTION

Cell phones are everywhere these days. It is great to be able to call anyone at any time. Unfortunately, they are also used as a means for misguided purposes. Cell phones these days are wrongly abused and taken advantage of in events such as Exam Halls by students for the purpose of malpractice. Cell phones are also widely used as one of the means for industrial sabotage by employees, spying by external entities, etc. to name a few of the problems created by Cell phones in the day to day life.Cell phones as a base are also often used by terrorists and anti-social elements to extreme means such as detonators to set off explosive devices in populated civilian localities and sensitive areas such as hospitals, temples, etc. Although on a much smaller scale, but in our daily life we see restaurants, movie theaters, concerts, shopping malls and churches all suffer from the spread of cell phones because not all cell-phone users know when to stop talking while most of us just grumble and move on, some people often go to extremes to retaliate.

A cell phone works by communicating with its service network through a cell tower or base station. Cell towers divide a city into small areas, or cells. As a cell-phone user drives down the street, the signal is handed from tower to tower. A jamming device transmits on the same radio frequencies as the cell phone, disrupting the communication between the phone and the cellphone base station in the tower. Jamming devices overpower the cell phone by transmitting a signal on the same frequency and at a high enough power that the two signals collide, and cancel each other out.

To jam a cell phone, we need a device that broadcasts on the correct frequencies. Although different cellular systems process signals differently, all cell-phone networks use radio signals that can be interrupted. GSM, used in digital cellular and PCS-based systems, Operates in the 900-MHz and 1800MHz bands in Europe and Asia and in the 1900-MHz (sometimes referred to as 1.9-GHz) band in the United States.. Jammers can broadcast on any frequency and are effective against CDMA, GSM and DCS. Old-fashioned analog cell phones and today's digital devices are equally susceptible to jamming.

The Cell Phone Detector is used to detect any use of Cell Phones by sending/receiving RF signals. It comprises of a RF sensor that continuously monitors the vicinity for any RF activity. Whenever there is any cell phone activity in the sensor's range, an output is produced indicating Cell Phone Mobile jammer is used to prevent mobile phones from usage, receiving or transmitting signals with the base stations. Mobile jammers effectively disable mobile phones within the defined regulated zones without causing any interference to other communication means. Mobile jammers can be used in practically any location, but are used in places where a phone call would be particularly disruptive like temples, libraries, hospitals, cinema halls, schools & colleges etc. As with other radio jamming, mobile jammers block mobile phone use by sending out radio waves along the same frequencies that mobile phones use. This causes enough interference with the communication between mobile phones and communicating towers to render the phones unusable. Upon activating mobile jammers, all mobile phones will indicate "NO NETWORK". 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.

## LITERATURE SURVEY

In our technique voltage controlled oscillator (VCO) plays a major role in generating the jamming frequency. In our research we found that the above technique is complex one as compared to our technique because our idea of jamming through spectrum distortion proves to be simpler, easier to fabricate and cost effective [1]. Cell phone jamming devices are an alternative to more expensive measures against cell phones, such as Faraday cages, which are mostly suitable as built in protection for structures. 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].

Reference [3-5] gives information regarding 8051 Microcontroller. The assembly level language and 'C' Programming is clearly explained [6]. Information regarding OP-Amps is present in [7] Assembly Language and Programming. Gives the required information for serial port

communication basics and serial port programming between 8051 and the GSM module in the communication part of the circuitry. Signal conversion from RS232 to TTL logic level is explained in chapter 10 of [6]. The required working configurations of operational amplifier used in stages I and 3 of the RF Detector are explained in chapter 4 of reference [7]. The working principle of the capacitor coupled inverting amplifier is implemented in the audio amplification stage.
The signal jammer concepts which require the decrease in Signal to Noise ratio is explained in chapter 6 of reference [7]. The RF detection part of the Mobile detector which monitors the RF level in the vicinity implements Voltage level detector explained in chapter 8 of reference [7]. The Jammer uses a Voltage Controlled Oscillator whose concepts and basic IC implementation is explained in chapter 10 of reference [6] as are the triangular wave generation basics which are used for jamming of RF signals. The circuit uses an on board voltage regulator which is used to provide a regulated DC supply, which uses basic regulator concepts which are explained with an IC LM340 configuration as an example in chapter 13 of reference [7-12].

## OVERVIEW

### Block Diagram

The Mobile Detector and the Mobile Jammer shown in Fig.1 forms the primary blocks of the system. The Detector is a simple RF signal detector with amplification stages. The Jammer is a RF signal generator which generates signals on a higher power level & on the frequency as that of the Mobile carriers with superimposed noise. A Micro-controller is used to interface and control the same various blocks. A GSM module is used in tandem with the RF Detector, to provide a functionality of alerting the authorities of the breach in security protocol. Relay is used to drive the Jammer circuit as the output of the Micro-controller does not have a sufficient current drive to control the Jammer directly. A Regulated power Supply is used to provide DC power to the system docks. An Inverter (later shown) is used to provide AC lower to the Jammer circuit.

### Working Principle

The Cell Phone Detector monitors the area for any Cell one activity. When a cell phone is in use, the Cell Phone detector generates a signal using the Ring Detector and the amplification stages. This signal is sent to the Microcontroller as an input. The Microcontroller immediately sends a message to monitoring authorities through the GSM module alerting them of the breach in security. The mobile number of the authorized personnel is programmed into the Micro-controller using the Embedded Coding. Once the message has been sent the next step is progressed to.

The Micro-controller at this point drives the transistor driver circuit, which in turn controls the Relay. The output current drive of the Micro-controller is about I-2mA, while the input drive of the Relay has to be about 10mA, for its coils to be energized. Hence we use an intermediate transistor drive circuit to run the Relay, which is basically a power transistor switch acting as a current driver or the relay. The Relay which is an electronically operated switch used to drive high load circuitry, turns on the Jammer. The Jammer generates two RF signals on the same frequency (downlink) of the Cell Phone carriers using its Voltage Controlled Oscillators. These signals collide with the RF carriers that the Cell Phones use to communicate with the Base Station.

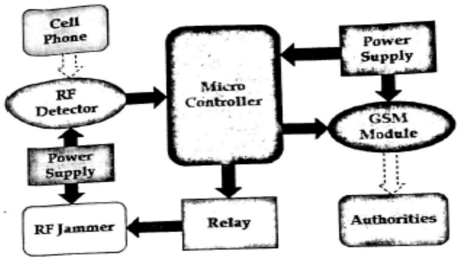

**Fig 1:** Cell Phone Detector with 'Denial of Service" Jamming

A regulated DC supply, which uses basic regulator concepts are explained with an IC LM340 configuration as an example in chapter 13 of reference [7].

## CELL PHONE DETECTOR

### Block Diagram

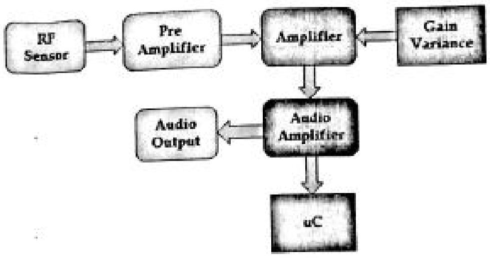

**Fig 2:** Block diagram of a RF Sensor based Cell Phone Detector

Fig 2 shows the block diagram of the RF sensor based Cell Phone Detector. The primary part of the circuit is an RF sensor built around the diode 1N3494. It consists of two stages of amplification, a gain variance stage made of a 1Mohm pot, which is used to vary the range of operation. It is to be noted that increasing the range abruptly causes false triggering. The circuit can sense both incoming and outgoing calls, SMS's, and also the usage of GPRS by any phone in the area of operation of the Detector circuit by detecting the RF transmission of the Cell Phone to the Radio Base Station. The Cell Phone Detector detects the usage of a Cell Phone even when it is in silent mode.

The Cell Phone Detector continuously monitors the vicinity for any RF activity. When there isn't any Cell Phone activity, the output of the Ring Detector is about 0.6mV. But when a Cell Phone is in use, i.e. during an incoming or outgoing call SMS, and the usage of GPRS, the output of the Ring Detector rises to about 60mV due to the RF activity in the area. This signal is then pre-amplified by the transistor BFR96 which is a low power, high frequency transistor with a large Current gain and bandwidth. The signal is then sent to the Microcontroller as an input.

## JAMMER

Jamming devices overpower the cell phone by transmitting a signal on the same frequency as the cell phone and at a high enough power that the two signals collide and cancel each other out. Cell phones are designed to add power if they experience low-level interference, so the jammer must recognize and match the power increase from the phone. To jam a cell phone, all you need is a device that broadcasts on the correct frequencies. A general block of a jammer is shown in Fig. 3. Although different cellular systems process signals differently, all cell-phone networks use radio signals that can be interrupted. GSM, used in digital cellular and PCS-based systems, operates in the 900-MHz and 1800-MHz bands in Europe and Asia.

Depending on the complexity, legal regulations& efficiency there are basically five types of jamming which an discussed in the next section. In our project we use the Type 'A' Device for "Denial o Service" jamming.

### Jamming Techniques

Type 'A' Devices: Jammers In this device we overpower cell phone's signal with a stronger signal. This type of device comes equipped with several independent oscillators transmitting jamming signal capable of blocking frequencies used by paging devices as well as those used by cellular/PCS systems control channels for call establishment.

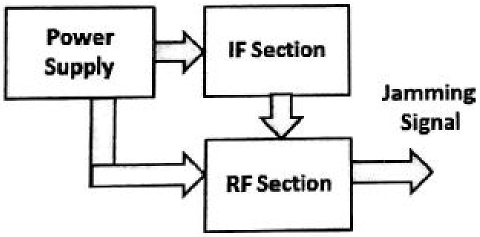

**Fig 3:** General Block of a Jammer

In this device we overpower cell phone's signal with a stronger signal. This type of device comes equipped with several independent oscillators transmitting jamming signals capable of blocking frequencies used by paging devices as well as those used by cellular/PCS systems control channels for call establishment. When active in a designated area, such devices will (by means of RF interference) prevent all pagers and mobile phones located in that area from receiving and transmitting calls.

We generate a signal on the same frequency as that used by the communication carrier using independent oscillators. Noise signals are added to these frequency signals and then transmitted after amplifying to a level greater than the received power at the Mobile Station from the Base Station. The generated jammer signals overpower the communication carriers and cancel each other out due to collision between the two.

## DESIGN PARAMETERS

This parameter is very important in our design, since amount of the output power of the jammer depends on the area that we need to jam. Later on we will see the relationship between the output power and the distance D. Our design is established upon D=10m for DCS 1800 band and D=20m for GSM 900 band.

### Jamming Range

This parameter is very important in our design, since amount of the output power of the jammer depends on the area that we need to jam. Later on we will see the relationship between the output power and the distance D. Our design is established upon D=10m for DCS 1800 band and D=20m for GSM 900 band.

### Frequency Bands

In our design, the jamming frequency must be the same as the downlink, because it needs lower power to do jamming than the uplink range and there is no need to jam the base station itself. So, our frequency design will be as follows:
GSM 935-960 MHz
DCS 1805-1880 MHz

### Jamming to signal Ratio

Jamming is successful when the jamming signal denies the usability of the communication or transmission. In digital communications, the usability is denied when the error rate of the transmission cannot be compensated by error correction. Usually, a successful jamming attack requires that the jammer power is roughly equal to signal power at the receiver (mobile device).The general equation of the jamming-to-signal ratio is given as follows

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

$P_t$= Transmitter power.
$P_j$ = Jammer 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.
$R_{tr}$= 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.
For GSM, the specified system $SNR_{min}$ a,is 9dBm which will 131 used as the worst case scenario for the jammer. The maximum power at the mobile device Pr is -15 dBm

### Free Space Loss

The free-space loss (or path loss) is given by: PL(dBm) = 32.44 + 20logd (km) + 20log f (MHz) The maximum free space loss (worst case F) happens when the maximum frequency is used in the above equation. Using 1880 MHz gives

**F(dB)=32.44+20 log 0.01 + 20 log 1880 =58dBm.**

### Power Calculations

Here, we need to find the power that is needed be transmitted to jam any cell phone within a distance of wound 10 meters for DCS. From the above considerations, we can find the required output power from the device, as follows. Using SNR=9 dB and the maximum power signal for mobile receiver = -I5 dBm, gives J=-24 dBm. But, our goal is to find the output power from the device, so when we add the free space loss to the amount of power at the mobile receiver we get our target

**Output power=-24dBm+58dBm = 34 dBm**

## CONCLUSION

This paper illustrates the design of a Cell phone Security System that detects and stops Cell Phone usage. This device could be used in places where could be misused or cell phones are not allowed. The system works as a security system with the capability of cell phone detection range up to 8m with single stage amplification. The designed jammer device works in dual band and jams both GSM 900 and GSM 1800 bands.

## REFERENCES

[1] J.E. Flood, "*Telecommunication Switching Traffic and Network*",1st ed. Pearson Education ltd, 1999.

[2] K.Feher,"*Wireless Digital Communication*", PHI,

[3] Mike Predko, "*Programming and customizing the PIC microcontroller*", 3rd ed . Tata McGraw-Hill Education Pvt. Ltd, 2007.

[4] David E. Simon, "*An Embedded Software Primer* ", Pearson, 1999.

[5] Muhammad Ali Mazidi, Janice Gillispie Mazidi, Rolin D McKinley, "*8051 Micro-cocontroller and Embedded Systems using Assembly and C* " 2nd ed, Pearson Education Inc, 2008

[6] David A Bell, "*Operational Amplifiers and Linear ICs*" Oxford University Press India 3rd Ed, 2011.

[7] http://dmohankumar.wordpress.com/2010/12/15/mobile-phone-tracer

[8] http://www.datasheetarchive.com/1N3491+equivalent-datasheet.html

[9] http://www.electroschematic s.com/5650/1a-4440-stereo-amplifier/

[10] http://www.bucek.name/pdf/la4440.pdf

[11] http://www.001 product.com/theory_of cellphone_J ammer.htm

[12] http://blog.jammer-store.com/2011/06/how-to-make-your-cell-phone-ja mmer-diy-guide/