AJCSE
ASIAN JOURNAL OF COMPUTER SCIENCE ENGINEERING

www.ajcse.info

Asian Journal of Computer Science Engineering 2017; 2(5):01-06

RESEARCH ARTICLE

Intelligent Mobile Signal Jammer

***Dr. Ibrahim Patel[3], Ashok Shigli[2], V Sripathi Raja[3], Dr. Raghavendra Kulkarni[4]**

[1]Assoc. Prof. Dept. of ECE.B. V. Raju Inst. of Tech. Narsapur Medak (Dist) T S
[2]HOD & Prof. Dept. of BME B. V. Raju Inst. of Tech. Narsapur Medak (Dist) T S
[3]Assoc. Prof. Dept. of BME B. V. Raju Inst. of Tech. Narsapur Medak (Dist) T S
[4]Principal K.M.C.E&T, Devarkonda, under JNT University, Hyderabad, T S.

Received on: 10/07/2017, Revised on: 30/08/2017, Accepted on: 15/09/2017

ABSTRACT

Now a days, privacy could be a crucial issue because of rise in mobile communication; most are having a mobile set, whether or not they square measure in private meeting, library, schools, or recreation centers that disturb the privacy. The Mobile detection device may be used as sort of a detector and it's capable of detection the cellular phone like device from the very of few centimeters to few feet relying upon the Cell phones transmission strength and alternative parameters. Furthermore there's high likelihood of secrets escaping of defense meeting and massive gangs use technological means that to focus on high worth item or for terrorist activities. This paper presents the propose of mobile sender that gives service denial for prime security zones and is additionally employed by the status person whereas move to avoid technological techniques of following employed by huge rowdy.

Keyword: - Mobile Communication, Metal Detector, Mobile Detection, Mobile Jammer, GSM, CDMA,

INTRODUCTION

A mobile phone jammer could be a device that blocks transmission or reception of signals, sometimes by making some style of interference at an equivalent frequency ranges that cell phones use. As a result, a mobile phone user can either lose the signal or experience a major loss of signal quality. Mobile phone jammers have each benign and malicious uses. Police and also the military usually use them to limit or disrupt communications throughout security things, bomb threats or once action is afoot. Moveable personal transmitter is additionally offered to modify their owner to prevent others in their immediate neck of the woods (up to 60-80 feet away) from cell phones. Similar instrumentality is factory-made to dam signals in environments wherever mobile phone activity might not be fascinating, like theaters, churches, mosque, Mandir (pooja), and operative rooms functioning on phones mistreatment solely analogue or older digital mobile principles.

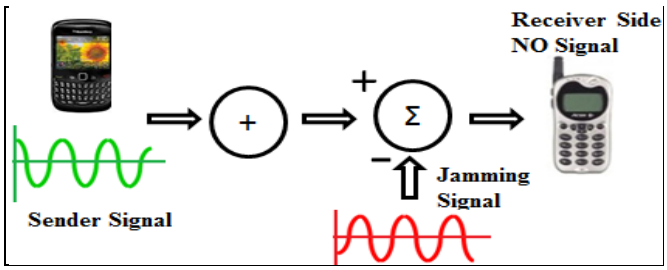

Fig 1: Block Diagram representing selective jamming

New models like the double and triple band jammers will block all wide used GSM Networks and area units, even terribly effective against new phones that hop to completely different frequencies and systems once interfered with because the dominant network technology and frequencies used for mobile phones vary worldwide, some work solely in specific regions like Asia, Australia, Europe, African nation and USA. This superb mobile signal jammer is meant to spice up 100 percent effectiveness, guarantee undisturbed conferences and better of all, to supply you massive 'shanti' for final peace of mind and cutout the discarded noise. Movable sender is employed to forestall cellular phones from receiving signals from base stations. This device may be employed in much any location; however area unit found primarily in places

***Corresponding Author:** Dr. Ibrahim Patel**, Email**: Ibrahim.patel@bvrit.ac.in

wherever a telephone would be notably riotous as a result of silence is predicted as shown in the fig. 1 & 2.

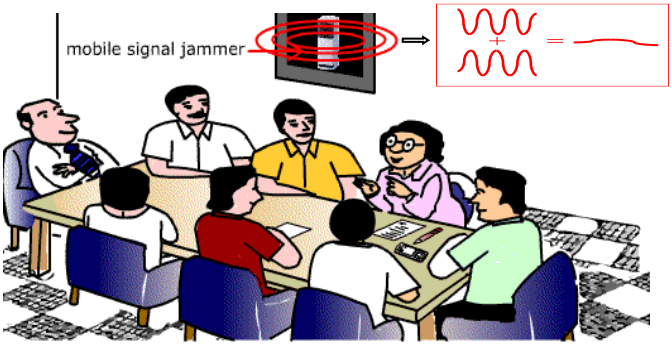

Figure 2: Mobile jammer blocking signals in a meeting

BACKGROUND OF RADIO FREQUENCY JAMMER

During World War II ground radio operators would commit to mislead pilots by false information in their own language, in what was a lot exactly a spoofing attack than blocking. Radar blocking is also vital to interrupt use of radar used to guide an enemy's missiles or aircraft. Modern secure communication techniques use such methods as spread spectrum modulation to resist the deadly effects of blocking.

Blocking of foreign radio broadcast stations has frequently been used in wartime (especially during periods of tense international relations) to prevent or deter citizens from listening to broadcasts from enemy countries. However such blocking is usually of limited effectiveness because the affected stations usually change frequencies, put on additional frequencies and increase transmission power.

Jamming has also infrequently been used by the Governments of Germany (during WW2), Israel, Cuba, Iraq, Iran (Iraq and Iran war, 1980-1988 and Iraq and USA alliance, Kuwait war, 1990), China, North and South Korea and several Latin American countries, as well as by Ireland against pirate radio stations such as Radio Nova. The United Kingdom government used two coordinated, separately located transmitters to jam the offshore radio ship, Radio North Sea International off the coast of Britain in 1970.

During the Cold War Soviet blocking of some Western broadcasters led to a "power race" in which broadcasters and jammers alike repeatedly increased their transmission power, utilized highly directional antennas and added extra frequencies to the already heavily jammed shortwave bands to such an extent that many broadcasters not directly targeted by the jammers (including pro-Sostations) suffered from the rising levels of noise and interference. For example, radio free Europe and its sister service radio liberty were the main target of Soviet jammers followed by Voice of America and the BBC World Service.

Mobile phone jammer devices were originally developed for law enforcement and the military to interrupt communications by criminals and terrorists.

During a hostage situation, police can control when and where a captor can make a phone call. Police can block phone calls during a drug raid so suspects can't communicate outside the area. Cell phone jammers can be used in areas where radio transmission are dangerous, (areas with potentially explosive atmosphere), such as chemical storage facilitates or grain elevators. The TRJ-89Jammer from Antenna system & supplies Inc. carries its own electrical generator and can block cellular communications in a 5mile (5km) radius. Corporations use jammers to stop corporate espionage by blocking voice transmissions and photo transmissions from camera phones. On the more questionable end of the legitimacy spectrum, there are rumors that hotel chains install jammers to block guests' cell phone usage and force to use in-room phones at high rates.

FREQUENCY JAMMER DESIGN PARAMETERS

If we want to jam the frequencies of the cell sets, we must have the knowledge of the frequencies at which cell phones operate in India. The frequency of the transferred signal of the jammer must cover the GSM frequency range. As the power received from the GSM Base Station is usually low, it is easier to jam the downlink than uplink as it requires less power.

Frequency Range	Uplink	Downlink
GSM 900	890-915 MHz	925-960 MHz
GSM 1800	1710-1785MHz	1805-1880MHz
CDMA	1920 -1980 MHz	2110 - 2170 MHz

This parameter is very vital in our design, since the amount of the output power of the jammer depends on the area that we need to jam. Our design is established upon D=10 meters for E-GSM band.

Jamming is successful when the mobile set stops communication with rest of the network. 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 end (mobile device). The general equation of the jamming-to-signal ratio is given as follows:

The GSM Air-interface uses two different multiplexing schemes: TDMA (Time Division Multiple Access) and FDMA (Frequency Division Multiple Access). The spectrum is divided into 200 kHz channels (FDMA) and each channel is divided into 8 timeslots (TDMA). Each 8 timeslot TDMA frame has duration of 4.6ms (577s/timeslot) [3]. The GSM transmission frequencies are presented in Table 1 movement of subscribers. The hopping sequence may use up to 64 different frequencies, which is a small number compared to military FH systems designed for avoiding jamming. Also, the speed of GSM hopping is approximately 200 hops / s; So GSM Frequency Hopping does not provide real protection against jamming attacks.

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

Where

P_j= power jammer,

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 & communication receiver,

B_j= Jammer bandwidth,

L_j= Jammer signal loss,

To successfully jam a particular region, we need to consider a very important parameter the signal to noise ratio, referred to as the SNR. Every device working on radio communication principles can only tolerate noise in a signal up to a particular level. This is called the SNR handling capability of the device. Most cellular devices have a SNR handling capability of around 12dB. A very good device might have a value of 9dB, although it is highly unlike. To ensure jamming of these devices, we need to reduce the SNR up to 9dB. Free Space Loss By using the following equation we can get the free path loses.

$$Path\,loss\,(db) = 32.44 + 2.\log d\,(km) + 20\log f\,(Mhz) \qquad (2)$$

Where 'f' is the frequency in MHz, and 'd' is the distance in kilometers. Using the GSM downlink with resonant frequency (947.5MHz) and a jamming radius of 10m, we get the value of path 58dBm. This path loss is for free space only, and the path losses in air will be much greater. This means that the jamming radius will be less than the 10m used to calculate this value.

$$F\,(db) = 32.44 + 20\log 0.01 + 2\log 1800$$
$$F = 58\,db \qquad (3)$$

Energy calculation is the energy transmitted to jam any cell phone within a distance of around 10 meters for GSM. 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= -15 dBm,

$$SNR = S / N$$
$$We\,know that\, S = -15 \;\; and \;\; SNR = 9$$
$$J = N = -15/9 \qquad (4)$$
$$J = -24\,dbm.$$

So we need to have jamming signal strength of -24dBm at the mobile device's reception to effectively jam it. However, our transmitted signal will undergo some attenuation while transmitting through antenna of the jammer and in open air. This path loss can be calculated using the simple free space path loss approximation. To have resultant output power we will add the value of 'J' with the value of free path loss. *Output power=-24dBm+58dB = 34dBm.*

OPERATION OF MOBILE JAMMER SIGNAL

Jamming devices overpower the cell phone by transmitting a signal of the same frequency as the cell phone and at a high enough power that the two signals collide and cancel each other. 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. Cell phones are full-duplex devices, which mean they use two separate frequencies, one for talking and one for listening simultaneously. Some jammers block only one of the frequencies used by cell phones, which has the effort of blocking both. The phone is tricked into thinking there is no service because it can receive only one of the frequencies. Less complex devices block only one group of frequencies, while the sophisticated jammers can block several types of networks at once to head off dual –mode or tri-mode phones that automatically switch among the

different network types to find an open signal. Some of the high-end services block all frequencies at once and others can be tuned to specific frequencies.

There are several ways to jam an RF device. The three most common techniques can be categorized as follows:

1. Spoofing: In this kind of jamming the device forces the mobile to turn off itself. this type is very difficult to be implemented since the jamming device first detects any mobile phone in a specific areas then the device sends the signal to disable the mobile phone. Some types of this technique can detect if a nearby mobile phone is there and sends a message to tell the user to switch the phone to the silent mode (Intelligent beacon disablers)
2. Shielding Attacks: this is known as "TEMPEST" or EMF shielding. This kind requires closing an area in a faraday cage so that any device inside this cage cannot transmit or receive RF signal from outside of the cage. This area can be as large as buildings, for example.
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 SNR of the mobile under the minimum value. This kind of jamming technique is the simplest one since the device is always on.

Less energy is required to disrupt signal from tower to mobile phone, than the signal from mobile phone to the tower or base station, because the base station is located at larger distance from the jammer than the mobile phone and that is why the signal from the tower is not as strong. Older jammers sometimes were limited to working on phones using only analog or digital mobile phone standards. Newer models such as the double and triple band jammers can block all widely used systems such as …CDMA, PCS,CDS, AMPS, NEXTEL SYSTEM, IDEN ,GSM et al. and are even very effective against newer phones which hop to different frequencies and systems when inferred with . Old-fashioned analog cell phones and today's digital devices are equally susceptible to jamming. As shown in the fig. 3.

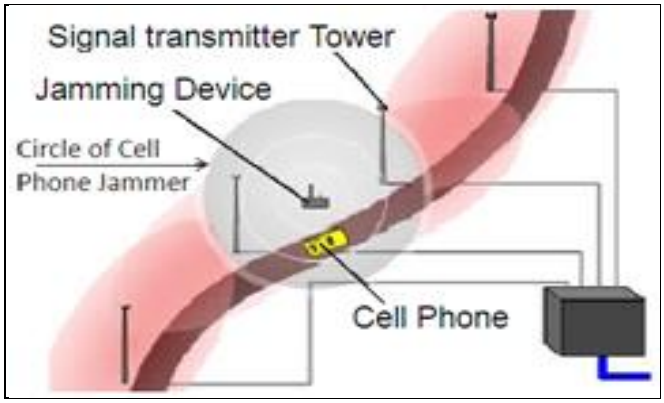

Fig. 3: base station of the signal transmitter and mobile jammer.

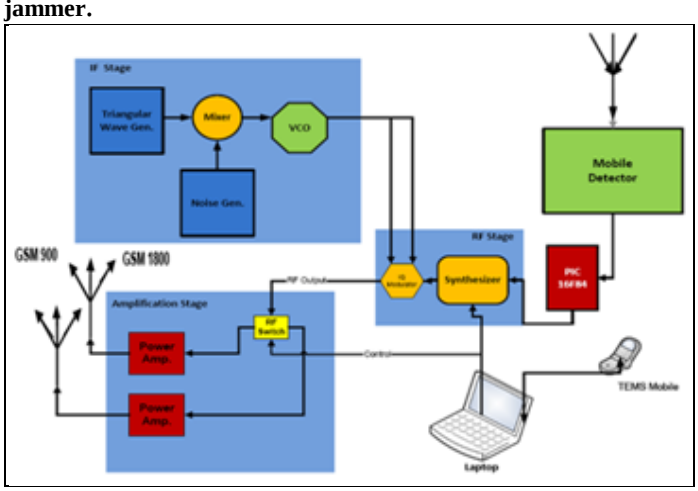

Fig.4: Block diagram of the jamming signal transmitter

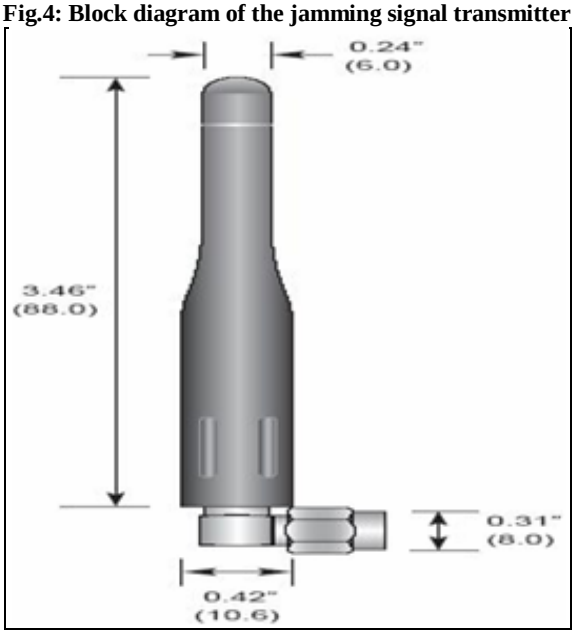

Fig. 5: the patterns for the antenna.

The RF-section is the most important part of the mobile jammer it consist of the Voltage Controlled Oscillator (VCO), RF Power amplifiers, and the antenna. These components were selected according to the desired specification of the jammer such as the frequency range and the coverage range. It's important to note that all the components used has 50 ohm input/output impedance, so 50 ohm micro strip was needed for matching between the

components. The width of the micro strip is calculated using the following Equations for w/h >1

$$Zo = \frac{120\pi}{\sqrt{\varepsilon_{eff}}} \frac{1}{\left(\frac{w}{h} + 1.393 + 0.667 \ln\left(\frac{w}{h} + 1.44\right)\right)} \quad (5)$$

$$\varepsilon_{eff} = \left[\frac{\varepsilon_r + 1}{2} + \frac{\varepsilon_r - 1}{2}\left[\frac{1}{\sqrt{1 + \frac{12h}{w}}}\right]\right] \quad (6)$$

The most important part of any transmitter is the antenna, so a suitable antenna should be selected. The antenna used in this project is 1/4 wave monopole antenna, and it has 50 Ohm impedance so that the antenna is matched to the transmission system. Also this antenna has low VSWR less than 1.7, and a bandwidth of 150 MHz around 916 MHz center frequency which cover the mobile jammer frequency range. The antenna gain is 2dBi. The patterns for the antenna are shown in the fig. 5 and fig. 6(a) and (b).

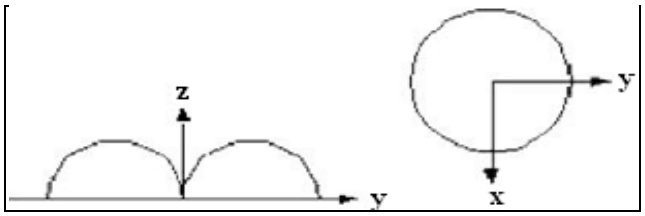

Fig.6 (a) Fig.6 (b)

Fig. 6: (a) Monopole Principal E-plane Pattern
(b) Monopole Principal H-plane Pattern

RESULTS AND DISCUSSION

Fig. 6 shows the clarified techniques observed on spectrum analyzer. The misleading frequency spectra obtained through the techniques show very evidently that how the new spectrum misrepresentation technique is superior to the noise attack blocking technique because there is no possibility that a mobile signal at a discrete frequency will be available in the vicinity of jammer at any instant.

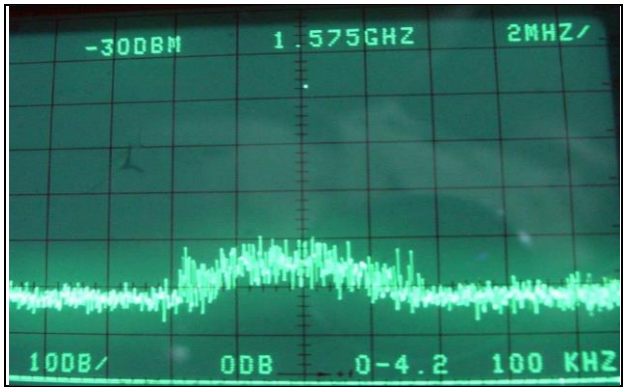

Fig.7 jamming through white noise attack

CELL PHONE JAMMING LEGAL ISSUES:

In USA, UK, OZ and many other countries, blocking cell-phone services (as well as electronic transmissions) is against the law. Jamming is seen as PROPERTY THEFT, because a private company has purchased the rights to the radio spectrum, and jamming the spectrum is akin to stealing the property the company has purchased. It also represents a SAFETY HAZARD because jamming blocks all calls in the Areas, not just the annoying ones. Jamming a signal could block the call of a babysitter frantically trying to contact a parent or someone trying to call for an ambulance. Since these jammers actively broadcast radio signals, they may or may not be legal to possess or operate based on the specific laws of the area one is in.

The main disadvantage of the mobile jammer is that the transmission of the jamming signal which is prohibited by law in many countries, for instance the fines for this offense can range as high as 11,000 $. Despite the legal issues the transmission of high power signal may affect the operation of some critical devices, such as hearing impairment hardware solution. These disadvantages will constrain the use of mobile jammer.

CONCLUSION

In this paper the proposed techniques turned out to be a full success, a device that stops phone ringing. This device could be used in places where ringing is not desired at specific times, as this ringing may disturb people in such places. The effective jamming range was not as expected, due to the shortage in the current supplied to the power amplifier also a more stable power supply needed for robust operation. That means using things like wall paper or building materials embedded with metal fragments to prevent cell phone signals from reaching inside or outside the room.

AJCSE, Sep-Oct, 2017, Vol. 2, Issue 5

REFERENCES

1. Mobile & Personal Communications Committee of the Radio Advisory Board of Canada, "Use of jammer and disabler Devices for blocking PCS, Cellular & Related Services" http://www.rabc.ottawa.on.ca/e/Files/01pub3.pdf
2. Braun, T.; Carle, G.; Koucheryavy, Y.; Tsaoussidis, V., Wired/Wireless Internet Communications, Third International Conference, WWIC 2005, Xanthi, Greece, May 11-13, 2005, Proceedings, p188.
3. John Scourias, Overview of the Global System for Mobile Communications,
4. http://ccnga.uwaterloo.ca/~jscouria/GSM/gsmreport.html#1 [4] Rick Hartley, RF / Microwave PC Board Design and Layout, ww.jlab.org/accel/eecad/pdf/050rfdesign.pdf
5. Siwiak, K., Radiowave Propagation and Antennas for Personal Communications, Artech House, 2nd.ed, p138.
6. Pozar, D. M., Microwave Engineering, John Wiley and Sons, 2nd.Ed, p198.
7. Gopalan, K. Gopal, Introduction to Digital Microelectronic Circuits, Irwin, New York, 1996. pp. 496-500.
8. Floyd, Electronic Devices, Prentice Hall, 5th. Ed, pp.60-85
9. Horowitz, P.; Hill, W., the Art of Electronics, 2nd. Ed, Cambridge University Press.
10. http://en.wikipedia.org/wiki/Spoofing_attack
11. http://en.wikipedia.org/wiki/Denial-of-service_attack
12. Prof. Nihad Dib. " Dual Band Mobile Jammer for GSM 900 & GSM 1800"
13. Antenna theory book.
14. Ahmed Jisrawi, "GSM 900 Mobile Jammer", undergrad project, JUST, 2006.
15. Floyd, Electronic Devices, Prentice Hall, 5th. Ed