An Analysis on Effective Outdoor Mobile Phone Jamming Using Radio Frequency Channels

RM Indika Nalin Bandara

Department Electrical, Electronic and Telecommunication Engineering Faculty of Engineering, General Sir John Kotelawala Defence University 1 Sri Lanka
nalin2316@gmail.com

Abstract - *This paper investigates the design and implementation of mobile phone jammers for GSM (900MHz AND 1800MHz) and 3G (2100MHz) for outdoor use in a high signal reception zone. A mobile phone jammer is a device that blocks reception of signals from a Base Transceiver Station (BTS) of a service provider to a Mobile Set (MS). Blocking is conventionally done by creating some form of interference at the same frequency ranges that MS use. As a result, a MS will either lose the signal, or indicate non availability of network coverage.*

Keyword: ARFCN,URFCN, Microcontroller

I. INTRODUCTION

Jamming technology generally does not discriminate between desirable and undesirable communications. A jammer can block all radio communications on any device that operates on radio frequencies within its range or within a certain radius of the jammer by emitting radio frequency waves that prevent the targeted device from establishing or maintaining a connection.

Cell phone jammer is a device which allows blocking or jamming all incoming and outgoing calls and SMS within a specified area. It does not have any direct connection with the cell phone. It works on the same frequency band of which the cell phones operate.

Communication jamming devices were first developed and used by military. Where tactical commanders use RF communications to exercise control of their forces, an enemy has interest in those communications. This interest comes from the fundamental area of denying the successful transport of the information from the sender to the receiver.

Nowadays, mobile jammer devices are becoming civilian products rather than electronic warfare devices, because with the increasing number of the mobile phone users, the need to disable mobile phones in specific places where the ringing of cell phone would be disruptive has increased. These places include worship places, university lecture rooms, libraries, concert halls, meeting rooms, and other places where silence is appreciated.

II. TYPES OF JAMMERS AND THEIR FUNCTIONALITIES

Jamming objective is to inject an interference signal into the communications frequency so that the actual signal is completely submerged by the interference. This can be achieved in several ways .They are as follows.

A. *Blind Jammers*

When this type of a jammer is active in a designated area, such devices will ,by means of RF interference, that prevent mobile phones located in that area from receiving and transmitting calls. This type of device transmits only a jamming signal and has very poor frequency selectivity, which leads to interference with a larger amount of communication spectrum than it was originally intended to target. This type is very uneconomical and very high in power consumption. [2]

B. Intelligent Cellular Disablers

This system achieved the blocking with the support of the service provider or the BTS. This Type of a device detects the presence of a mobile phone which blocks the communication between the BTS and MS (Mobile Station) and the filtering or the prevention of authorization of call establishment is done by the software at the base station. This process of detection and interruption of call establishment is done during the interval normally reserved for signaling and handshaking.

C. Direct Receive & Transmit Jammers

This jammer 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. The jam signal would only stay on as long as the mobile continues to make a link with the base station, otherwise there would be no jamming transmission the technique forces the link to break or unhook and then it retreats to a passive receive mode again.[2]

D. EMI Shield - Passive Jamming

This technique is using EMI suppression techniques to make a room into what is called a Faraday cage. The Faraday cage essentially blocks, or greatly attenuates; virtually all electromagnetic radiation either from entering or leaving the cage or in this case a target room.[2]

III EXISTING METHODS

A. 3G/GSM Link Architecture

Figure1: 3G/GSM Architecture

Two frequency links are used to establish communication and to handle traffic between BTS (Base Station Transceiver) and the MS (Mobile Station).One is for uplink and the other one is for down Link. The traffic and signaling are sent at burst of 0.577ms at interval of 4.615ms to data block of each 20ms. The Uplink /Downlink Frequencies usage in Sri Lanka is mentioned in the Table 1. [1]

Table 1: The Uplink , Downlink Frequencies uses in Sri Lanka

Frequency Band Name	Up Link	Down Link
E-GSM-900 Band	880.0 915.0	925.0 960.0
DCS-1800	1,710.2 1,784.8	1,805.2 1,879.8
3G Band	1930.1 1980.1	2120.1 2170.1

B. Existing Methods of Jamming - (Using a Ramp generator Circuits)

The most of available jammers are concentrating down link band. Because the effect jammer only affects the MS and affect the BTS minimum level. Most of the circuit functions jammers are depicted in the figure 2.

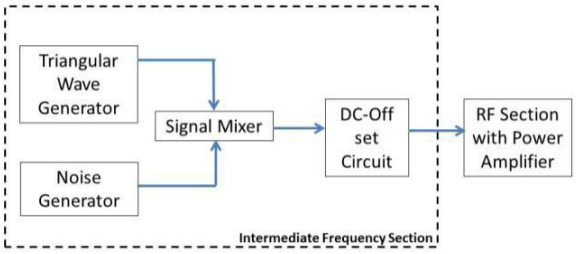


Figure 2: The functions of a Jammer

The function of the Intermediate Frequency section of the Mobile jammer is to generate the tuning signal for the VCO, which will 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 then offset by proper amount so as to sweep the VCO output from the minimum desired frequency to a maximum.[3]

To achieve jamming a noise signal is mixed with the triangle wave signal to produce the tuning voltage for the VCO. The noise will help in making the jamming transmission, making it look like random "noise" to an outside observer. Without the noise generator, the jamming signal is just a sweeping, unmodulated Continuous Wave RF carrier.

The Disadvantages of the RAMP generator jamming system is that the jamming signals covering the entire BTS to MS transmission band. As the bandwidth is high which results in a reduced power spectral density, this in turn dilutes the emission power. Further, in this method it is very difficult to demarcate the Uplink and Downlink band precisely. As a result, jamming signal may interfere with the Uplink frequencies. Then it may affect the BTS.

This method is not effective to the 3G mobile

communication, due to the spread spectrum technique uses. When a noise applied to the frequency range it also spreads throughout the band and the spectral density will be low. Then it will be cancelled out when it is going through a band pass filter.

IV PROPOSED OUTDOOR JAMMER

The design and effective deployment of outdoor mobile phone jammers is complicated when it is compared with the indoor application due to the following reasons:

- The Jamming Signal strength is weakening throughout the jamming area due to multipath reflections, absorption and attenuation. Thus, as a result, it is very difficult to narrow down or focus the jamming strength to a particular zone.[3][4][5]

- It is difficult to confine the jamming signal within the zone, which results in jamming the area outside the zone which is undesired. The signal strength of reception from BTS is greater outdoor in comparison to indoor. Moreover, in a outdoor scenario the MS will acquire reception from more than one BTS. Thus, if the reception of a particular BTS is low, the MS will automatically latch into another BTS (which has a higher reception). The power output required for jamming is low for indoor application, usually a low power such as 1 to 5 watts being sufficient for the purpose. However, in contrast, outdoor jammers require higher output in the region of 20 to several hundred watts (depending on the strength of receptions from BTS to MS) due to the complications involved in the jamming process.

- The high output power, entails serious considerations in heat dissipation of the system.

- More precautions to protect the system from high voltage surges and the lighting surges which is common in for any outdoor telecommunication device.

A. ARFCN & URFCN

ARFCN:-In GSM cellular networks, an absolute radio-frequency channel number (ARFCN) is a code that specifies a pair of physical radio carriers used for transmission and reception in a land mobile radio system, one for the uplink signal and one for the downlink signal.[1]

UARFCN:- The UMTS frequency bands are radio frequencies used by third generation (3G) wireless Universal Mobile Telecommunications System networks.[1]

Table1: ARFCN & UARFCN

Frequency Band Name	ARFCN / UARFCN
E-GSM-900 Band	0 TO 124 & 975 to 1023
DCS-1800	512 to 885
3G Band - 2100	9612 to 9888 & 10562 to 10838

B. Methodology used for E-GSM-900 and DCS-1800Bands.

This system is based on the ARFCN and URFCN selection method is based on microcontroller.

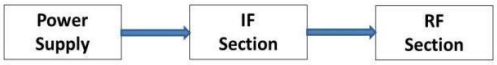


Figure 3: The Main Parts of a Jammer

1) Power Supply

This section consists of 13V switch mode power supply with a High Amperage current output. This mainly uses for providing power supply to high output power amplifiers (20W- 100W) and regulated voltage output is drawn to circuits in the system.

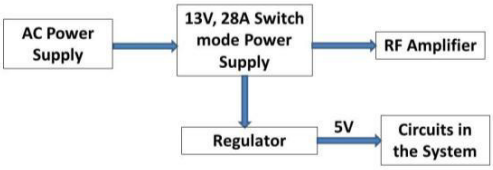


Figure 4: The Power Supply

2) IF Section

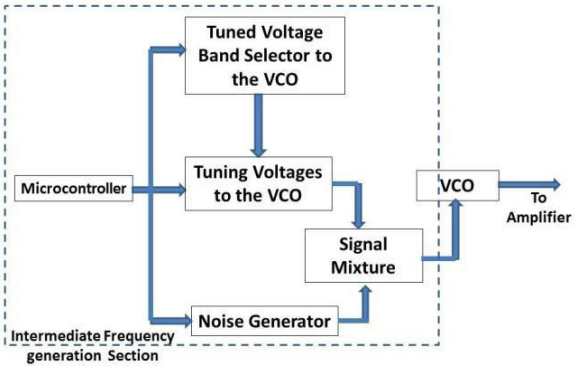


Figure 5: The Components of IF section (E-GSM-900 and DCS-1800Bands)

The main function of the IF section of the mobile phone jammer is to generate the tuning signal to the VCO. The intermediate frequency section consists of a Microcontroller, Tuned Voltage Band selector to the VCO, Tuning voltages to the VCO, Noise Generator and a Signal Mixture.

3) Microcontroller

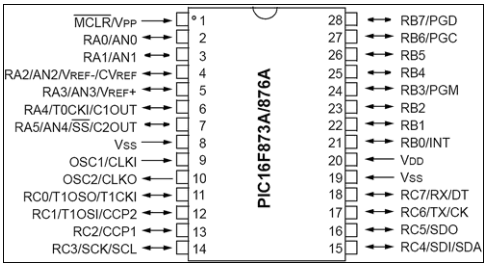


Figure 6: The Pin layout of the PIC16F876A

16F876A used as the main controller part of this circuit. Two ports of this PIC used as output pins (Port B and Port C) to select the Tuned Voltage Band selector to the VCO and Tuning voltages to the VCO appropriately. Further, to generate a noise frequency PWM Signal generation is used as a noise generator.

4) Tuned Voltage Band selector to the VCO

The E-GSM-900 Band and DCS-1800Band downlink frequencies were divided into 5 and 7 sub bands respectively. (Table 1)

Table2: Frequency Bands uses

Service Provider	E-GSM-900 Band - MHz	DCS-1800 Band - MHz
Air Tel	925 - 930	1835-1842.4
Mobitel	930 -937.4	1805-1812 & 1812-1820
Hutchson	937.6 - 945	1820-1827.4
Etisalat	945 -952.4	1827.6 - 1835
Dialog	952.6 - 960	1842.6-1850 & 1850 -1858

Port C pins are configured as output pins and select the mobile frequency bands appropriately by this section.

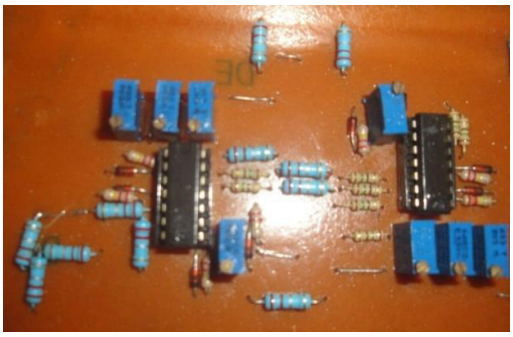


Figure 6: Tuned Voltage Band selector to the VCO

5) Tuning Voltage to the VCO

The frequencies mentioned in table 1 are divided into 1MHz frequency band calculate the required voltage supply to VCO for that respective frequency. The ARFCN in the respective area (Which required to Jammed) also can be selected to these required frequencies. Using 5 KΩ variable resistors (Preset) which acts as a voltage divider that is used to generate required voltage.

6) Noise Generator

PWM signal generation is used as the noise generator. The micro c Pro coding is as follows

PWM1_Init(50000); - Initialize PWM1 module at 5KHz

PORTC = 0XFB;

PWM1_Start();

PWM1_Set_Duty(125);- Set current duty for PWM1

7) Signal Mixture

The input to this mixer is a sine wave and a random "noise" signal. These signals are mixed to form a new, "noisy" waveform. When it is applied to the

VCO, the resulting RF signal will "sweep" across the cellular downlink frequencies, and will be Frequency Modulated (FM) with the noise signal. This noise modulation helps to increase the effectiveness of the jammers.

Figure 7: The RF Mixture Circuit

C. Methodology used for 3GBand

3G uses WCDMA and the wider band makes it possible to divide and combine reception signals propagated through multipath-fading channels into more multipath components, which helps to improve the reception quality through RAKE time diversity. WCDMA uses Direct Sequence spreading, where spreading process is done by directly combining the baseband information to high chip rate binary code.[11][12]

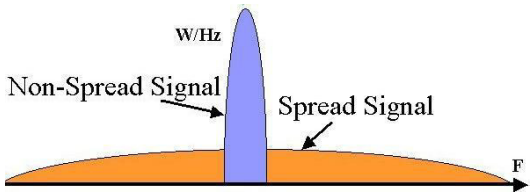


Figure 8: Signal Spreading in WCDMA

Implementing a noise to WCDMA is not much effect on the communication. Because noise signal also spreads throughout the bandwidth and will cancel out in band pass filter. A special method implemented to overcome this problem and figure 8 shows the block diagram of it.

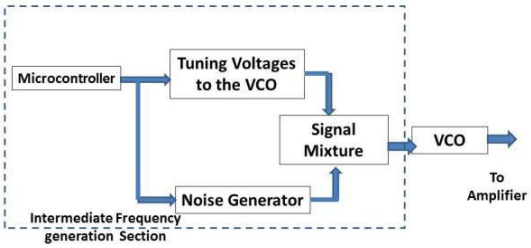


Figure 9: The Components of IF section (3G Bands)

If we consider a one service provider, they use 2 frequencies for downlink throughout the island. For an example Hutch uses DL UAFCN 10713 (2142.6MHz) and 10738 (2147.6MHz) uses to for their Coverage.

Tuning voltages section can generate the respective voltages which is required for the VCO to generate respective UARFCN frequency. PWM signal generation is used as the noise generator. Signal mixture uses to combine two of the outputs and applied to the VCO.

D. RF Section

This section consists of a VCO uses to generate respective frequencies, a Power amplifier and an antenna.

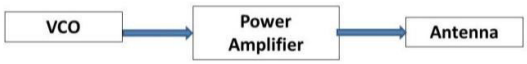


Figure 10: The Components of RF section

1) VCO

A voltage-controlled oscillator or VCO is an electronic oscillator whose oscillation frequency is controlled by a voltage input. The applied input voltage determines the instantaneous oscillation frequency. Consequently, modulating signals applied to control input may cause frequency modulation (FM).

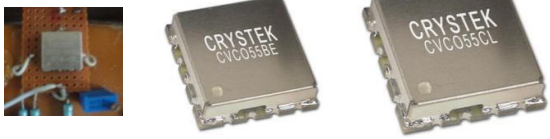
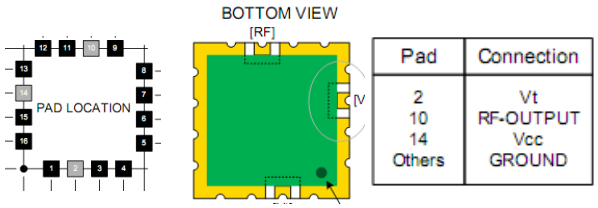


Figure 11: The Outlook of the VCO

Table2: Types of VCO used for the project

Description	E-GSM-900 Band	DCS-1800	3G Band - 2100
Part Number	CVCO55CL-0920-0980	CVCO55BE-1750-2150	CVCO55BE-2100-2200
Frequency (MHz)	920 to 980	1750 to 2150	2100 to 2200
Tuning Voltage (VDC)	1.0 to 5.0	0.3 to 4.7	0.5 to 4.5
2nd Harm (dBc)	-12	-15	-12
Output Power (dBm)	6.0±3.0	0.0±3.5	4.0±2.0
Vcc (VDC)	5.0±0.25	5.0±0.25	5.0±0.25
Icc Max (mA)	35	25	30



Pad	Connection
2	Vt
10	RF-OUTPUT
14	Vcc
Others	GROUND

Figure 12: VCO Pin Layout

Ophir RF Amplifier used to amplify the VCO output and fed in to the Antenna.

Figure 13: Complete Circuit System

V. OBSERVATIONS

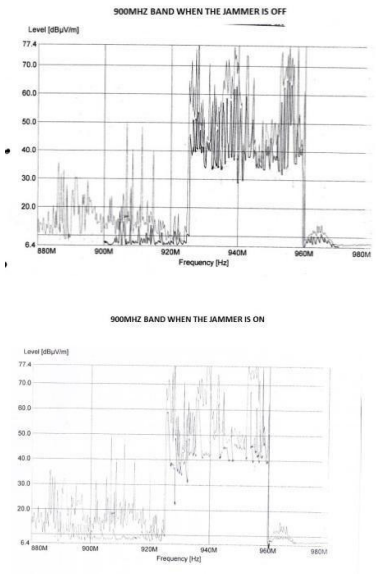


Figure 14: E-GSM-900 Band Jammer On & Off

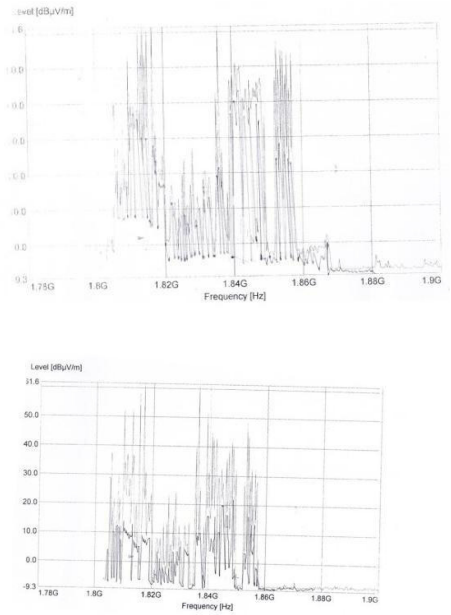


Figure 15 : DCS-1800 Band Jammer On & Off

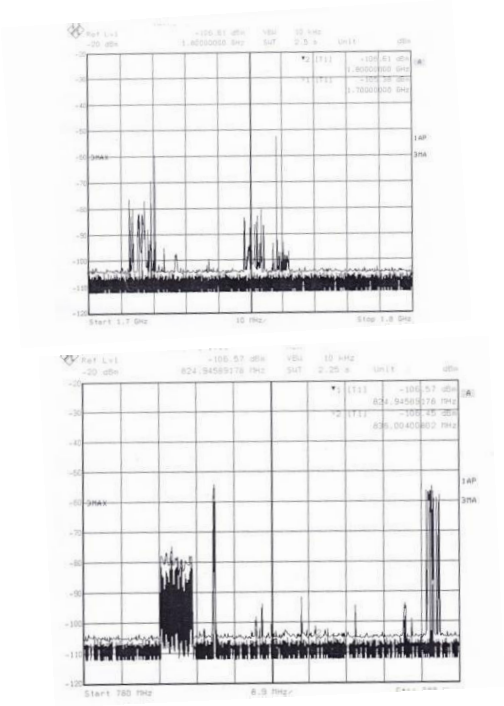


Figure 16: 2100 Bands (3G) Jammer On & Off

VI. CONCLUSION

A mobile phone from the time it is switched on communicates with its service network via the BTS using a frequency allotted for this purpose. The novel concept analyzed by this paper is the

development of a system to dentify these frequencies and jam them instead of the entire spectrum. This in turn effectively utilizes the jamming signal power through a greater power spectral density due to reduced bandwidth.

This system was successfully completed and deployed in outdoor location. Performance of the system is excellent. With the arrival of 4G mobile communication, jamming concept has to be revised again.

REFERENCES

http://en.wikipedia.org/wiki/Absolute_radio frequency_channel_number

Cell phone jammer Shah, S.W. ; Dept. of Electr. Eng., NWFP Univ. of Eng. & Technol Multitopic Conference, 2008. INMIC 2008. IEEE International

"Design of user specific intelligent cell phone jammer" Divya, E. ; Aswin, R. Recent Advances in Information Technology (RAIT), 2012 1st International Conference onDigital Object Identifie 2012

"Development of GSM — 900 Mobile Jammer: An approach to overcome existing limitation of jammer" Mishra, N.K. Wireless Communication and Sensor Networks (WCSN), 2009 Fifth IEEE Conference on Digital Object Identifier

"Intelligent FM signal jamming system" Patel, I. ; Kulkarni, R. ; Khan, J.A. Computing Communication & Networking Technologies (ICCCNT), 2012 Third International Conference on Digital Object Identifier

From GSM to LTE: An Introduction to Mobile Networks and Mobile Broadband by By Martin Sauter

GSM - Architecture, Protocols and Services By Jorg Eberspächer, Hans-Joerg Vögel, Christian Bettstetter, Christian Hartmann

GSM: switching, services, and protocols By Jorg Eberspacher, Hans-Jorg Vogel, Christian Bettstetter Wiley, May 15, 2001

Mobile Telecommunications Standards: GSM, UMTS, TETRA, and ERMES by By Rudi Bekkers
Introduction to 3G Mobile Communications By Juha Korhonen

3G Evolution: HSPA and LTE for Mobile Broadband By Erik Dahlman, Stefan Parkvall, Johan Skold, Per Beming

ACKNOWLEDGMENT

It is my sincere duty to thank all the personnel who were involved in the process of the project success. Then I like to thank to Maj Gen SAPP Samarasinghe who gave valuable ideas, taking all the necessary arrangements related to my project and who made necessary arrangements to utilize the CRD resources effectively.

I like to appreciate the support given by the lab assistants of the Electronic and Telecommunication Engineering department for their help rendered to me even in the busiest period of time. I extend my acknowledgement to all other staff members of the department for their friendly support and encouragement given by them during this project.

BIOGRAPHY OF AUTHORS

[1]Author is a Senior Lecturer (Grade II) in the Department of Electrical , Electronic and Telecommunication Engineering of General Sir John Kotalawala Defence University, Sri Lanka. His research interests include Robotic, Mobile communication, Microcontrollers and Embedded systems. He published four papers in international Journal. He completed MSc in Telecommunication Engineering in University of Moratuwa, Sri Lanka. Before joining with the KDU academic staff he served as a Research Engineer in Center for Research and Development under MOD Sri Lanka more than Four years.