ISSN: 2278 – 7798
International Journal of Science, Engineering and Technology Research (IJSETR)
Volume 2, Issue 9, September 2013

Mobile Phone Signal Jammer for GSM, CDMA with Pre-scheduled Time Duration using ARM7

P.Naresh[1], P. Raveendra Babu [2], K.Satyaswathi [3]

***Abstract*— This Paper is designed and implemented for Mobile phone signal jammer for GSM, CDMA with prescheduled time duration using Mobile jammer and ARM7. The jamming device broadcasts an RF signal in the frequency range reserved for cell phones that interferes with the cell phone signal, which results in a "no network available" display on the cell phone screen. All phones within the effective radius of the jammer are silenced. The activation and deactivation time schedules can be programmed with microcontroller. Real time clock chip DS1307 is used to set the schedule.**

***Index Terms*— ARM7, keypad, Mobile jammer, RTC**

I. INTRODUCTION

Communication jamming devices were first developed and used by military. This interest comes from the fundamental objective of denying the successful transport of information from the sender (tactical commanders) to the receiver (the army personnel), and vice-versa. Nowadays, mobile (or cell) phones are becoming essential tools in our daily life. Here in Jordan, for example, with a rather low population (around 5 million), three main cell phone carriers are available; namely; Zain, Orange, and Umniah The first two use the GSM 900 system, while the third uses the GSM 1800 system. Needless to say, the wide use of mobile phones could create some problems as the sound of ringing becomes annoying or disrupting. This could happen in some places like conference rooms, law courts, libraries, lecture rooms and mosques. One way to stop these disrupting ringing is to install a device in such places which will inhibit the use of mobiles, i.e., make them obsolete. Such a device is known as cell phone jammer or "GSM jammer", which is basically some kind of electronic countermeasure device [1].

The technology behind cell phone jamming is very simple. The jamming device broadcasts an RF signal in the frequency range reserved for cell phones that interferes with the cell phone signal, which results in a "no network available" display on the cell phone screen. All phones within the effective radius of the jammer are silenced. It should be mentioned that cell phone jammers are illegal devices in most countries. According to the Federal communications commission (FCC) in the USA: "The manufacture, importation, sale, or offer for sale of devices designed to block or jam wireless transmission is prohibited". However, recently, there has been an increasing demand for portable cell phone jammers. We should mention that this paper, presented in this report, is solely done for educational purposes [1].

II. RELATED WORK

A. *Mobile jammer*

A mobile phone jammer is an instrument used to prevent cellular phones from receiving signals from base stations. When used, the jammer effectively disables cellular phones. These devices can be used in practically any location, but are found primarily in places where a phone call would be particularly disruptive because silence is expected. As with other radio jamming, cell phone jammers block cell phone use by sending out radio waves along the same frequencies that cellular phones use. This causes enough interference with the communication between cell phones and towers to render the phones unusable. On most retail phones, the network would simply appear out of range. Most cell phones use different bands to send and receive communications from towers (called frequency division duplexing, FDD). Jammers can work by either disrupting phone to tower frequencies or tower to phone frequencies. Smaller handheld models block all bands from 800 MHz to 1900 MHz within a 30-foot range (9 meters). Small devices tend to use the former method, while larger more expensive models may interfere directly with the tower [2] [3].

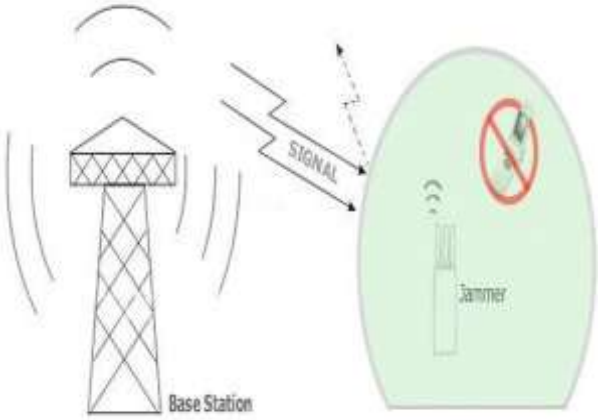

Figure1. Basic principle of Mobile jammer

The radius of cell phone jammers can range from a dozen feet for pocket models to kilometers for more dedicated units. The actual range of the jammer depends on its power and the local environment, which may include hills or walls of a building that block the jamming signal.

Less energy is required to disrupt signal from tower to mobile phone than the signal from mobile phone to the tower (also called 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 older digital mobile phone standards. Newer models such as the double and triple band jammers can block all widely used systems (CDMA, GSM) and are even very effective against newer phones which hop to different frequencies and systems when interfered with [4][7].

1) Jamming Techniques:

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

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 area, 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).

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 can't transmit or receive RF signal from outside of the cage.

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 signal-to-noise ratio (SNR) of the mobile under its minimum value. This kind of jamming technique is the simplest one since the device is always on [5]. Our device is of this type. Mobile jammer circuit includes IF section, RF section, Antenna and Power supply.

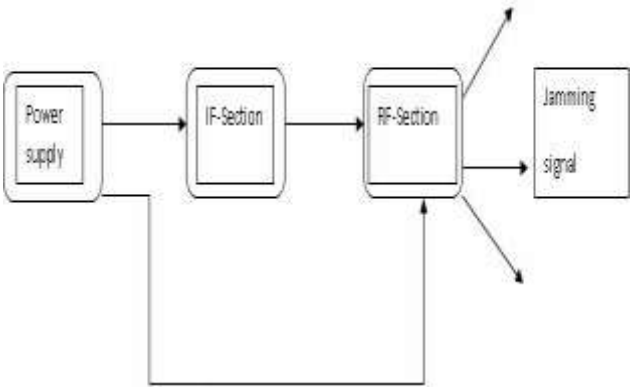

Figure2. Block diagram of jammer device

GSM, used in digital cellular and PCS-based systems, operates in the 900-MHz and 1800-MHz 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 AMPS, CDMA, TDMA, GSM, PCS, DCS systems [6][8].

Table I: Operating frequency bands

	UPLINK (Handset transmit)	**DOWN LINK** (Handset receive)	**USED IN JORDAN BY:**
GSM 900	890-915 MHz	935-960 MHz	Zain + Orange
DCS 1800	1710-1785 MHz	1805-1880 MHz	Umniah

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 900 ----→ 935-960 MHZ

GSM 1800---→ 1805-1880 MHZ

The CDMA frequency range will be 860-894 MHZ (Asia & Europe) and 850-894 MHZ (United States).

B. ARM 7(LPC2148)

The ARM7TDMI-S is a general purpose 32-bit microprocessor, which offers high performance and very low power consumption. The ARM architecture is based on Reduced Instruction Set Computer (RISC) principles, and the instruction set and related decode mechanism are much simpler than those of micro programmed Complex Instruction Set Computers. This simplicity results in a high instruction throughput and impressive real-time interrupt response from a small and cost-effective processor core. Pipeline techniques are employed so that all parts of the processing and memory systems can operate continuously. Typically, while one instruction is being executed, its successor is being decoded, and a third instruction is being fetched from memory. The ARM7TDMI-S processor also employs a unique architectural strategy known as THUMB, which makes it ideally suited to high-volume applications with memory restrictions, or applications where code density is an issue. The key idea behind THUMB is that of a super-reduced instruction set. Essentially the ARM7TDMI-S processor has two instruction sets:

- The standard 32-bit ARM instruction set.
- A 16-bit THUMB instruction set.

The THUMB set's 16-bit instruction length allows it to approach twice the density of standard ARM code while retaining most of the ARM's performance advantage over a traditional 16-bit processor using 16-bit registers. This is possible because THUMB code operates on the same 32-bit register set as ARM code. THUMB code is able to provide up to 65% of the code size of ARM, and 160% of the performance of an equivalent ARM processor connected to a 16-bit memory system.

C. *REAL TIME CLOCK (RTC)*

The real time clock (RTC) is a widely used device that provides accurate time and date for many applications. The RTC chip present in the PC provides time components of hour, minute and second in addition to the date/calendar components of year, month and day. The RTC chip uses an internal battery that keeps the time and date even when the power is off. One of the most widely used RTC chips is the DS1307 from Dallas semiconductor. The clock operates in either the 24-hour or 12-hour format with AM/PM indicator. The DS1307 has a built-in power-sense circuit that detects power failures and automatically switches to the backup supply. Time keeping operation continues while the part operates from the backup supply

D. Keypad

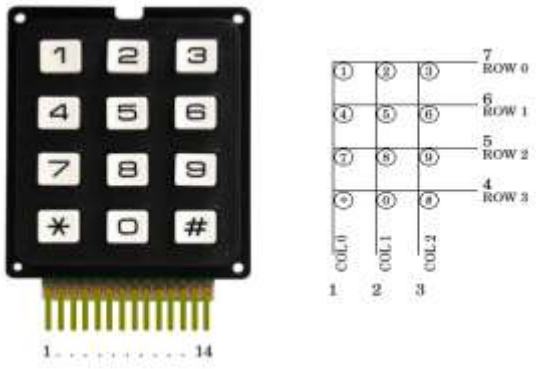

Figure3. 4x3 keypad structure

A basic 12 button keypad for user input. The buttons are setup in a matrix format. This allows a microcontroller to scan the 7 output pins to see which of the 12 buttons is being pressed. The jammer ON time and OFF time will be given with the help of keypad.

III. HARDWARE IMPLEMENTAION

The below Fig. 4 is the block diagram of the system that is to set the scheduled time duration for Mobile jammer. The activation and deactivation time schedules can be programmed with microcontroller. Real time clock chip DS1307 is used to set the schedule. In order to run the RTC(Real time clock) One Crystal oscillator is externally interfaced. The battery backup is interfaced for the purpose of update the time when the absence of power. Another crystal oscillator is interfaced in order to run the microcontroller. 4x3 Keypad is interfaced for the purpose of giving time schedule. In keypad Rows are interfaced to P0.16-P0.19 and Columns are interfaced to P0.20-P0.22. Switch is used for the updating time intervals. The switch is interfaced at P1.31. Reset circuit is used for adjusting the time schedule again. Mobile jammer will be interfaced to the controller at P1.30.

First we have to set the ON time and OFF time using DS1307 for signal jamming. Whenever it reaches ON time the signal jammer will be activated and it blocks all the mobiles (GSM, CDMA) within the jamming range.

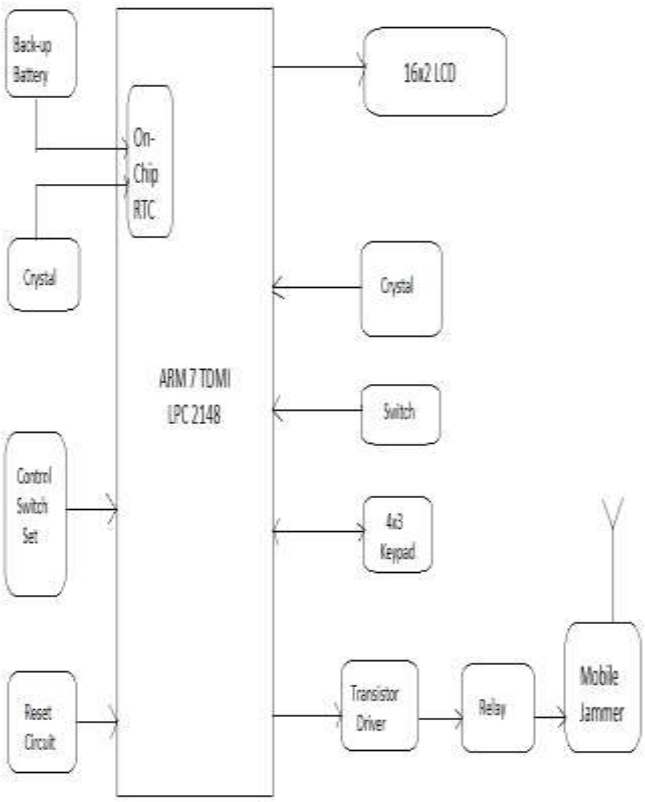

Figure4. Block diagram of the system

Whenever it reaches the OFF time the signal jammer will be deactivated. By using keypad we will set the ON time and OFF time. Before scheduling the time using keypad we have to press a switch for entering into schedule of time. ON time and OFF time will be display in LCD module. When ON time reaches in LCD the relay will be ON and automatically the mobile jammer will be activated with the help of relay. The relay consists of a coil and a switch. When the coil is energized, the switch closes, connecting the two contacts together. As we tested our jamming device in different places, the result was a full success. The effective jamming range was around 5-7 meters. When Incoming Signal has low power it completely jams mobile but when incoming Signal is coming with high power then jamming range reduces.

Here keil cross compiler will be used for building the application. LPC2148 development board will be used to test the built application. Flash magic software is used to dump the hex file into the microcontroller.

IV. RESULT ANALYSIS

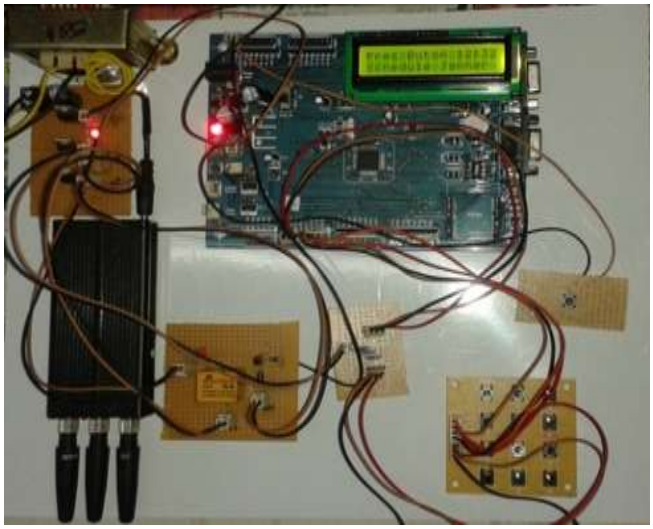

Figure5. Hardware design of the system

Figure6. Activation of mobile jammer

Fig5 shows the hardware design of the mobile jammer with pre-scheduled time duration. It includes the Jammer, ARM 7, keypad and relay. When the time schedule arrives in RTC the jammer will be activated with the help of relay and disrupt the communication system. This will be shown in fig6. We are able to block communication coming into and going out from a GSM phone operating on the 890MHz to 960MHz frequency band. This paper was tested against the networks and has proven success with average range of 5m. Testing in different locations shows the dependent of the jamming range on the signal strength, for instance in low network coverage area of the base station the jamming range exceed 7m.

V. CONCLUSION

This paper is successfully completed using Mobile jammer and ARM7. By this system we can deactivate all the mobile signals at any location. we designed a device that stops phone ringing in a particular time period. This device could be used in places where ringing is not desired at specific times, as these ringing may disturb people in such places. The designed device works in dual band. It jams both the GSM 900 and GSM 1800 bands. The device was able to jam the three main cell phone carriers in Jordan.

REFERENCES

[1] www.HowStuffWork.com

[2] En.wikipedia.org/wiki/Mobile_phone_jammer

[3] Multitopic conference2008.INMIC 2008.*IEEE* International

[4] "Zone of silence [cell phone jammer]," *Spectrum, IEEE, vol.42, no.5, 18*, May 2005

[5] Sami Azzam, Ahmad Hijazi, Ali Mahmoudy. "Smart Jammer for mobile phone systems"

[6] Mobile & Personal Communications Committee of the Radio Advisory Board of Canada, "Use of jammer and disabler Devices for blocking PCS, Cellular & Related Services"

[7]Ahmed Jisrawi, "GSM 900 Mobile Jammer", undergrad project, JUST, 2006.

[8]John Scourias Overview of the global system for Mobile communications,http://ccnga.uwaterloo.ca/~jscouria/GSM/gsmreport.html#1

***P.Naresh*[1]**, *M.Tech, Dept of ECE, CMR College of Engineering & Technology, Hyderabad, AP India*

***P. Raveendra Babu*[2]**, *Assoc Prof, Dept of ECE, CMR College of Engineering &Technology, Hyderabad, AP-India.*

***K.Satyaswathi*[3]**, *Asst Prof, Dept of ECE, CMR College of Engineering&Technology, Hyderabad, AP-India.*