International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Vol. 3, No. 2, May, 2014
© 2014 IJERST. All Rights Reserved

Research Paper

FPGA BASED WIRELESS JAMMING NETWORKS

G M S Vishnu Charan[1]* and S Hannah Pauline[2]

Corresponding Author: **G M S Vishnu Charan, ✉ vishnucharangms@gmail.com*

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. But the existing mobile phone jammers are having several defects so we are going to design a new mobile phone jammer using VLSI Technology which will be more efficient than existing jammers.

Keywords: Jammers, Mobile Jammer, FPGA, RF Transmitter, RF Receiver, LCD, Frequency Jamming

INTRODUCTION

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. Mobile Jammers were originally developed for law enforcement and the military to interrupt communications by criminals and terrorists to foil the use of certain remotely detonated explosives. The civilian applications were apparent with growing public resentment over usage of mobile phones in public areas on the rise & reckless invasion of privacy. Over time many companies originally contracted todesign mobile jammers for government switched over to sell these devices to private entities. 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. Mobile jammer’s effect can vary widely based on factors such as proximity to towers, indoor and outdoor settings, presence of buildings and landscape, even temperature and humidity play a role.

The choice of mobile jammers are based on the required range starting with the personal pocket mobile jammer that can be carried along with you to ensure undisrupted meeting with your client or a personal portable mobile jammer for your room or medium power mobile jammer or high power mobile jammer for your organisation to very high power military jammers to jam a large campuses.

[1] Department of Embedded Systems, SRM University, Chennai, India.

[2] Department of Electronics and Communication, SRM University, Chennai, India.

This article can be downloaded from http://www.ijerst.com/currentissue.php

NEED & HISTORY OF JAMMERS

The rapid proliferation of cell phones at the beginning of the 21st century to near ubiquitous status eventually raised problems, such as their potential use to invade privacy or contribute to academic cheating. In addition, public backlash was growing against the disruption cell phones introduced in daily life. While older analog cell phones often suffered from poor reception and could even be disconnected by simple interference such as high frequency noise, increasingly sophisticated digital phones have led to more elaborate counters. 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. They were originally developed for law enforcement and the military to interrupt communications by criminals and terrorists. Some were also designed to foil the use of certain remotely detonated explosives. 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.

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. The radius of cell phone jammers can range from a dozen feet for pocket models to kilometers for more dedicated units. The TRJ-89 jammer can block cellular communications for a 5-mile (8 km) radius.

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, iDEN, GSM, et al.) and are even very effective against newer phones which hop to different frequencies and systems when interfered with. As the dominant network technology and frequencies used for mobile phones vary worldwide, some work only in specific regions such as Europe or North America. Some Cell Phone Jammers have been introduced to some State Prisons in the United States. Cell phones that have been sneaked into prison pose a security risk for guards and property owners living nearby.

PROBLEMS IN EXISTING JAMMERS

Envisage a situation where you are essaying to dial 911 and cannot get through because someone has a cell phone jammer with him. Otherwise, you want to call the police to avoid a robbery in your building but the robber has a cell phone jammer with him. So, what could you do in such a dangerous situation? Jamming devices utilized with some thoughts may be much more useful than just a method of enjoyment. To remove these hazards a new efficient type of mobile jammer is proposed using FPGA. In this new design we are going to disable the keypad, MIC, speaker, will be only disabled by using the FPGA & we doing it using a 400MHz frequency which has an public license so there is no need of licensing. Some of the Common Problems are listed below:

- The person didn't even get the notification of a call or message when he is in the jammer coverage area.
- The person cannot be contacted for some urgent information also.
- Nearly the mobile phone will be in Switch Off state.
- There will not be any notification that the user mobile has been jammed.

PROPOSED SYSTEM DESIGN

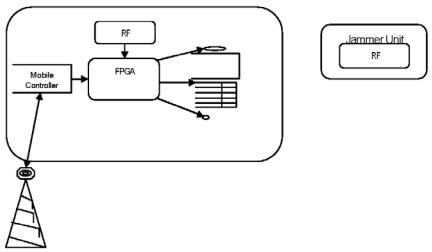
In most countries, it is illegal for private citizens to jam cell-phone transmission, but some countries are allowing businesses and government organizations to install jammers in areas where cell-phone use is seen as a public nuisance. In December 2004, France legalized cell-phone jammers in movie theaters, concert halls and other places with performances. France is finalizing technology that will let calls to emergency services go through. India has installed jammers in parliament and some prisons. It has been reported that universities in Italy have adopted the technology to prevent cheating. Students were taking photos of tests with their camera phones and sending them to classmates.

ALTERNATIVES TO CELL PHONE JAMMING

While the law clearly prohibits using a device to actively disrupt a cell-phone signal, there are no rules against passive cell-phone blocking. That means using things like wallpaper or building materials embedded with metal fragments to prevent cell-phone signals from reaching inside or outside the room. Some buildings have designs that block radio signals by accident due to thick concrete walls or a steel skeleton. Companies are working on devices that control a cell phone but do not "jam the signal." One device sends incoming calls to voicemail and blocks outgoing calls. The argument is that the phone still works, so it is technically not being jammed. It is a legal gray area that has not been ruled on by the FCC as of April 2005.

Cell-phone alerters are available that indicate the presence of a cell-phone signal. These have been used in hospitals where cell-phone signals could interfere with sensitive medical equipment.

Figure 1: Mobile Jammer General Block Diagram



EPGA

A Field-programmable Gate Array (FPGA) is an integrated circuit designed to be configured by the customer or designer after manufacturing-hence "field-programmable". The FPGA configuration is generally specified using a hardware description language (HDL), similar to that used for an application-specific integrated circuit (ASIC) (circuit diagrams were previously used to specify the configuration, as they were for ASICs, but this is increasingly rare). FPGAs can be used to implement any logical function that an ASIC could perform. The ability to update the functionality after shipping, partial re-configuration of the portion of the design[1] and the low non-recurring engineering costs relative to an ASIC design (notwithstanding the generally higher unit cost), offer advantages for many applications.

FPGA's contain programmable logic components called "logic blocks", and a hierarchy of reconfigurable interconnects that allow the blocks to be "wired together"-somewhat like many (changeable) logic gates that can be inter-wired in (many) different configurations. Logic blocks can be configured to perform complex combinational functions, or merely simple logic gates like AND and XOR. In most FPGAs, the logic blocks also include memory elements, which may be simple flip-flops or more complete blocks of memory.

In addition to digital functions, some FPGAs have analog features. The most common analog feature is programmable slew rate and drive

strength on each output pin, allowing the engineer to set slow rates on lightly loaded pins that would otherwise ring unacceptably, and to set stronger, faster rates on heavily loaded pins on high-speed channels that would otherwise run too slow. Another relatively common analog feature is differential comparators on input pins designed to be connected to differential signaling channels. A few "mixed signal FPGAs" have integrated peripheral Analog-to-Digital Converters (ADCs) and Digital-to-Analog Converters (DACs) with analog signal conditioning blocks allowing them to operate as a system-on-a-chip. Such devices blur the line between an FPGA, which carries digital ones and zeros on its internal programmable interconnect fabric, and field-programmable analog array (FPAA), which carries analog values on its internal programmable interconnect fabric.

RF ENCODER AND DECODER GENERAL ENCODER AND DECODER OPERATIONS

The Holtek HT-12E IC encodes 12-bits of information and serially transmits this data on receipt of a Transmit Enable, or a LOW signal on pin-14 /TE. Pin-17 the D_OUT pin of the HT-12E serially transmits whatever data is available on pins 10,11,12 and 13, or D0,D1,D2 and D3. Data is transmitted at a frequency selected by the external oscillator resistor. By using the switches attached to the data pins on the HT-12E, as shown in the schematic, we can select the information in binary format to send to the receiver. The receiver section consists of the Ming RE-99 and the HT-12D decoder IC. The DATA_IN pin-14 of the HT-12D reads the 12-bit binary information sent by the HT-12E and then places this data on its output pins. Pins 10,11,12 and 13 are the data out pins of the HT-12D, D0,D1,D2 and D3. The HT-12D receives the 12-bit word and interprets the first 8-bits as address and the last 4-bits as data. Pins 1-8 of the HT-12E are the address pins. Using the address pins of the HT-12E, we can select different addresses for up to 256 receivers. The address is determined by setting pins 1-8 on the HT-12E to ground, or just leaving them open. The address selected on the HT-12E circuit must match the address selected on the HT-12D circuit (exactly), or the information will be ignored by the receiving circuit.

When the received addresses from the encoder matches the decoders, the Valid Transmission pin-17 of the HT-12D will go HIGH to indicate that a valid transmission has been received and the 4-bits of data are latched to the data output pins, 10-13. The transistor circuit shown in the schematic will use the VT, or valid transmission pin to light the LED. When the VT pin goes HIGH it turns on the 2N2222 transistor which in turn delivers power to the LED providing a visual indication of a valid transmission reception.

CONTROLLING THE PROJECT WITH A FPGA

Using these RF transmitter & receiver circuits with a FPGA would be simple. We can simply replace the switches used for selecting data on the HT-12E with the output pins of the FPGA. Also we can use another output pin to select TE, or transmit enable on the HT-12E. By taking pin-14 LOW we cause the transmitter section to transmit the data on pins 10-13. To receive information simply hook up the HT-12D output pins to the FPGA. The VT, or valid transmission pin of the HT12D could signal the FPGA to grab the 4-bits of data from the data output pins. If you are using a FPGA with interrupt capabilities, use the VT pin to cause a jump to an interrupt vector and process the received data.

The HT-12D data output pins will LATCH and remain in this state until another valid transmission is received. NOTE: You will notice that in both schematics each of the Holtek chips have resistors attached to pins 15 and 16. These resistors must be the exact values shown in the schematic. These resistors set the internal oscillators of the HT-12E/HT-12D. It is recommended that you choose a 1% resistor for each of these resistors to ensure the correct circuit oscillation.

RANGE OF OPERATION

The normal operating range using (only) the LOOP TRACE ANTENNA on the transmitter board is about 50 feet. By connecting a quarter wave antenna using 9.36 inches of 22 gauge wire to both circuits, you can extend this range to several hundred feet. Your actual range may vary due to your finished circuit design and environmental conditions. The transistors and diodes can be substituted with any common equivalent type. These will normally depend on the types and capacities of the particular loads you want to control and should be selected accordingly for your intended application.

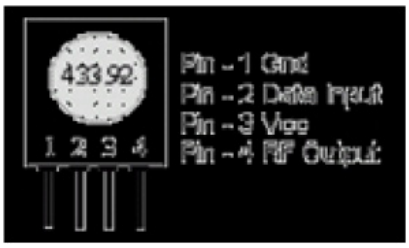
RF DETAILS

The TWS-434 and RWS-434 are extremely small, and are excellent for applications requiring short-range RF remote controls. The transmitter module is only 1/3 the size of a standard postage stamp, and can easily be placed inside a small plastic enclosure. TWS-434: The transmitter output is up to 8mW at 433.92MHz with a range of approximately 400 foot (open area) outdoors. Indoors, the range is approximately 200 foot, and will go through most walls.

Figure 2: RF 434 Mhz Transmitter Modulation: ASK

The TWS-434 transmitter accepts both linear and digital inputs, can operate from 1.5 to 12 Volts-DC, and makes building a miniature hand-held RF transmitter very easy. The TWS-434 is approximately the size of a standard postage stamp.

Figure 3: RF-434 Pin Diagram



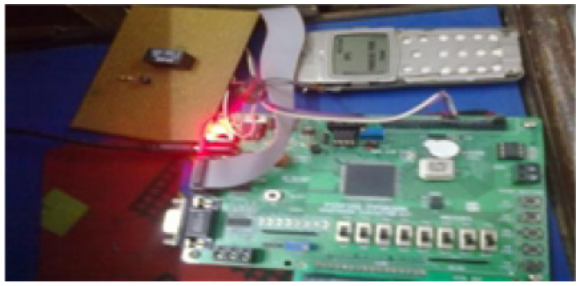
LCD DISPLAY

More FPGA devices are using 'smart LCD' displays to output visual information. The following discussion covers the connection of a 16x2 LCD display to a PIC FPGA. LCD displays designed around Hitachi's. LCD HD44780 module, are inexpensive, easy to use, and it is even possible to produce a readout using the 8x80 pixels of the display. Hitachi LCD display have a standard ASCII set of a characters plus Japanies, Greek and Mathematical symbols.

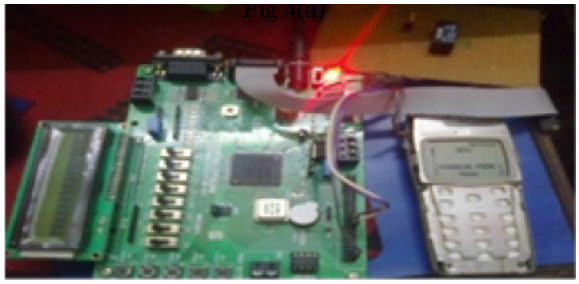
For a 8-bit data bus, the display requires a +5 supply plus 11 I/O lines. For a 4_bit data bus it only requires the supply lines plus seven extra lines. When the LCD display is not enabled, data lines are tri-state which means they are in a state of high impedence and this means they do not interfere with the operation of the display is not being addressed.

Reading data from the LCD is done in the same way, but control line R/W has to be high. When we send a high to the LCD, it will reset and wait for instructions. Typical instructions sent to LCD display after a reset are: turning on a display, turning on a cursor and writing characters from left to right. When the LCD is initialized, it is ready to continue receiving data or instructions. If it receives character, it will write it on the display and move the cursor one space to the right. The Cursor marks the next location where a character will be written. When we want to write a string of characters, first we need to set up the starting address, and then send one character at a time. Characters that can be shown on the display are stored in data display (DD) RAM. The size of DDRAM is 80 bytes.

Figure 4(a), 4(b): Pictures of our Proposed Mobile Jammer



4(a)



4(b)

CONCLUSION

Our Proposed Mobile Jammer is working perfectly without affecting the signals from the network. So that the user can able to get the notifications regarding Calls and messages (SMS, MMS). The notification about the calls will be given to the user. If there is any urgent call as we can get the notification we can go out from the coverage area and use our mobile as it is. No need of licensing. Implementation of our newly designed jammers is easy. As we are using a FPGA, our hardware can be modified whenever we want. Can be implemented where silence to be maintained. Future modifications are possible easily. Misuse of mobiles can be restricted. Thus our Mobile jammers can provide higher efficiency with lower misuses.

REFERENCES

1. A Chan, X Liu, G Noubir and B Thapa (2007), "Control Channel Jamming: Resilience and Identification of Traitors". *In Proceedings of ISIT*.
2. D Adamy (2001), "EW 101: A First Course in Electronic Warfare". *Artech House Publishers*.
3. I Akyildiz, W Lee, M Vuran and S Mohanty (2006), "Next Generation Dynamic Spectrum Access Cognitive Radio Wireless Networks: A Survey". *Computer Networks*, Vol. 50, No. 13, pp. 2127-2159.
4. J T Chiang and Y C Hu (2007), "Cross-layer Jamming Detection and Mitigation in Wireless Broadcast Networks". *In Proceedings of the MobiCom*, pp. 346-349.
5. L C Baird, W L Bahn, M D Collins, M C Carlisle and S C Butler (2007), "Keyless Jam Resistance". *In Proceedings of the 2007 IEEE Workshop on Information Assurance United States Military Academy*.
6. M Cagalj, S Capkun and J P Hubaux (2007), "Wormhole-based Anti-jamming Techniques in Sensor Networks". *IEEE Transactions on Mobile Computing*, Vol. 6, No.1, pp. 100-114.
7. T X Brown, J E James and A Sethi (2006), "Jamming and Sensing of Encrypted Wireless Ad-hoc networks". *In Proceedings of the ACM MobiHoc*, pp. 120-130.

International Journal of Engineering Research and Science & Technology
Hyderabad, INDIA. Ph: +91-09441351700, 09059645577
E-mail: editorijlerst@gmail.com or editor@ijerst.com
Website: www.ijerst.com