International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 3 Issue 6, October 2019 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

FPGA Based Wireless Jamming Networks

G. Sugumar[1], Mrs. T. Sathiyabama[2]

[1]MCA Student, [2]Assistant Professor,
[1,2]Department of Computer Applications (PG),
[1,2]Dr. SNS Rajalakshmi College of Arts and Science, Coimbatore, Tamil Nadu, India

ABSTRACT

A mobile jammeris a device which is used to jam signals of cell phone from receiving signals from base stations. Mobile jammer is used majorly where the disturbances that are occurred with the cell phones. So, in this paper we are designing a new Mobile Jammer unit which is capable of blocking the cell phone working not the signal receiving from Base Station, which make effective use of the situation where jammers actually used. This was implemented using FPGA by interfacing Mobile Device, RF Transmitter and RF Receiver and LCD Unit.

KEYWORDS: *Jammers, Mobile Jammer, FPGA, RF Transmitter, RF Receiver, LCD*

How to cite this paper: G. Sugumar | Mrs. T. Sathiyabama "FPGA Based Wireless Jamming Networks" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-3 | Issue-6, October 2019, pp.1215-1217, URL: https://www.ijtsrd.com/papers/ijtsrd29343.pdf

IJTSRD29343

INTRODUCTION

Cell phones are everywhere these days. According to the Cellular Telecommunications and Internet Association, almost 195 million people in the United States had cell-phone service in October 2005. And cell phones are even more ubiquitous in Europe. The mobile phone or mobile, also called a wireless, cellular phone, cell phone, cell or hand phone (HP), is a long-range, portable electronic device used for mobile communication that uses a network of specialized base stations known as cell sites. In addition to the standard voice function of a telephone, current mobile phones may support many additional services, and accessories, such as SMS for text messaging, email, packet switching for access to the Internet, and MMS for sending and receiving photos and video. Most current mobile phones connect to a cellular network of base stations (cell sites), which is in turn interconnected to the public switched telephone network (PSTN) (the exception is satellite phones). Cell phones are basically handheld two-way radios. And like any radio, the signal can be disrupted, or jammed.

INSIDE A DIGITAL CELL PHONE

If you take a basic digital cell phone apart, you find that it An amazing circuit board containing the brains of •contains just a few individual parts: A keyboard (not unlike the one you find in a TV• A liquid crystal display (LCD) • An antenna •the phone A battery• A speaker • A microphone •remote control)

JAMMING BASICS

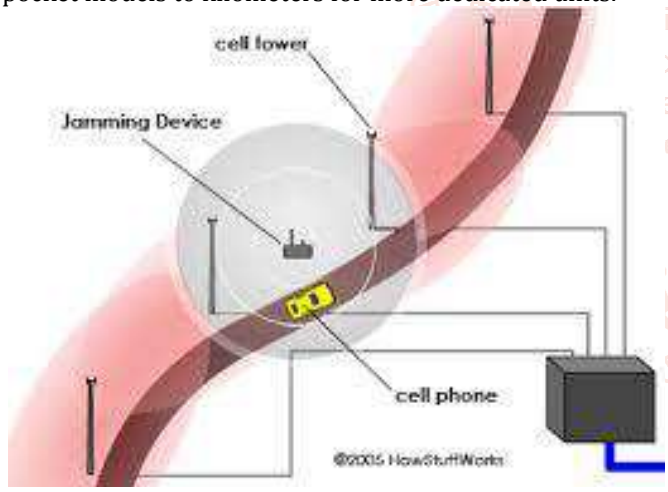
Disrupting a cell phone is the same as jamming any other type of radio communication. A cell phone works by communicating with its service network through a cell tower or base station. Cell towers divide a city into small areas, or cells. As a cell-phone user drives down the street, the signal is handed 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 cell-phone base station in the tower. Cell Phone Jammer is an instrument to prevent cellular phone from receiving and transmitting the mobile signals to the base station.

FIELD-PROGRAMMABLE GATE ARRAY (FPGA)

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 Mobile Cell Phone Jammer can block all kinds of mobile phones ringing sound at all places such as church, mosque, library, Movie Theater and meeting room. You just buy it and just attach it at some place. And you will never hear the bell sound of mobile phone any more.

NEED & HISTORY OF JAMMERS

International Journal of Science Engineering and Advance Technology, IJSEAT, Vol 2, Issue 9, September-2014 ISSN 2321-6905 www.ijseat.com Page 391 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 The radius of cell phone jammers can range from a dozen feet for pocket models to kilometers for more dedicated units.



RF ENCODER AND DECODER

A. 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.

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..... Fig3: RF 434MhzTransmitter. 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 4: RF-434 Pin Diagram TWS-434RF Receiver operates at 433.92MHzFrequency and at Voltage: 4.5V~5.5V and Bit-rate: 0.2kbps-4kbps Fig5: Receiver Pin configuration

LCD DISPLAY

International Journal of Science Engineering and Advance Technology, IJSEAT, Vol 2, Issue 9, September-2014 ISSN 2321-6905 www.ijseat.com Page 394 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 a 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.. For a 8-bit data bus, the display requires a +5V 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 impendance (as though they are disconnected) and this means they do not interfere with the operation of the FPGA when the display is not being addressed. Fig 6: Pictures of our Proposed Mobile jammer X.

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."

CONCLUSIONS

Our projected Mobile jammer is functioning utterly while not moving the signals from the network. In order that the user will able to get the notifications relating to Calls and messages (SMS, MMS). The notifications regarding the calls are given to the user. If there's any imperative decision as we will get the notification we will leave from the coverage

space and use our mobile because it is. No would like of licensing. Implementation of our freshly designed jammers is straightforward. As we tend to square measure employing a FPGA, our hardware will be changed whenever we would like. Will be enforced wherever silence to be maintained. Future modifications square measure attainable simply. Misuse of mobiles will be restricted. So our Mobile jammers will offer higher potency with lower misuses.

References:

[1] SeongahJeong, Keonkook Lee, Heon Huh, and Joonhyuk Kang, "Secure Transmission in Downlink Cellular Network with a Cooperative Jammer," IEEE WIRELESSCOMMUNICATIONS LETTERS, ACCEPTED FOR PUBLICATION, 2162-2337/13$31.00 _c 2013 IEEE.

[2] Y. Yang, W.-K. Ma, J. Ge, and P. C. Ching, "Cooperative secure beam forming for AF relay networks with multiple eavesdroppers," IEEE Signal Process. Lett., vol. 20, no. 1, pp. 35–38, Jan. 2013.

[3] M. Vzquez, A. Prez-Neira, and M. Lagunas, "Confidential communication in downlink beam forming," in Proc. 2012 IEEE Workshop on Sign. Proc. Adv. in Wireless Comm., pp. 349–353.

[4] S. Jeong, K. Lee, J. Kang, Y. Baek, and B. Koo, "Cooperative jammer design in cellular network with internal eavesdroppers," in Proc. 2012IEEE Mil. Comm. Conf., pp. 1–5.

[5] Q. Li and W. K. Ma, "Optimal and robust transmit designs for MISO channel secrecy by semi definite programming," IEEE Trans. Signal Process., vol. 59, no. 8, pp. 3799–3812, Aug. 2011.

[6] H. D. Ly, T. Liu, and Y. Liang, "Multiple-input multiple-output Gaussian broadcast channels with common and confidential messages," IEEE Trans. Inf. Theory, vol. 56, no. 11, pp. 5477–5487, Nov. 2010.

[7] R. Mochaourab and E. A. Jorswieck, "Optimal beam forming in interference networks with perfect local channel information," submitted to IEEE Trans. Signal Process. Preprint available on arXiv: 1004.4492, Oct. 2010.

[8] R. Liu, T. Liu, H. V. Poor, and S. Shamai (Shitz), "MIMO Gaussian broadcast channels with confidential and common