International Journal of VLSI System Design and Communication Systems

ISSN 2322-0929
Vol.02, Issue.05,
August-2014,
Pages:0346-0350

ww.semargroup.org
www.ijvdcs.org

Design of Novel Mobile Jammer system using FPGA

D. SWATHI[1], P. PARVATI[2], B. NAGA PRASANNA[3]

[1]PG Scholar, GPCET, JNTU Ananthapur University, Andhrapradesh, India.
[2]GPCET, JNTU Ananthapur University, Andhrapradesh, India.
[3]GPCET, JNTU Ananthapur University, Andhrapradesh, India.

Abstract: Cell phones cannot be used in all the areas where it may result disturbing others or creating a serious disaster. Hence a Wireless jammer is designed which is used to avoid the usage of cell phones in such areas. The main significance of this model is that the system is flexible and does not interfere or collapse the signal received from the base station so that the calls or messages intended for the mobile is received but cannot be attended. That is, the system disables the microphone, loud speaker and keypad in the mobile. The jammer effectively disables cellular phones. When the ignition in the jammer unit goes ON, an RF signal is encoded and passed through RF transmitter to the RF receivers in the mobile unit and the message is decoded. As soon as Mobile unit receives the Signal it locks the Microphone, Speaker and the keypad of the smart phone. The user is still notified about the calls and the messages are received.

Keywords: Cooperative Jammer, FPGA, RFID, XILINX.

I. INTRODUCTION

Organizing a collection of nodes into a wireless network requires cooperative implementation of critical network functions such as neighbour discovery, channel access and assignment, routing, and time synchronization. These functions are coordinated by exchanging messages on a broadcast channel, known as the control channel. In most network architectures, including mobile ad hoc, vehicular, sensor, cellular, mesh, and cognitive radio networks (CRNs), the location1 of the control channel, determined by its frequency band, time slot, or spreading code, is known a priori to all nodes participating in the network. From a security standpoint, operating over a globally known control channel constitutes a single point of failure. Networks deployed in hostile environments are susceptible to Denial-of- Service (DoS) attacks by adversaries targeting the functionality of the control channel .If the adversary is successful, network service can be denied even if other available frequency bands remain operational. One of the most effective ways for denying access to the control channel is by jamming it. In this attack, the adversary interferes with the frequency band(s) used for control by transmitting a continuous jamming signal, or several short jamming pulses.

Typically, jamming attacks have been analyzed and addressed as physical layer vulnerability. Conventional anti-jamming techniques rely extensively on spread spectrum (SS). These techniques provide bit-level protection by spreading bits according to a secret PN code, known only to the communicating parties. An adversary unaware of this code has to transmit with a power which is several orders of magnitude higher compared to the SS transmission, in order to corrupt a SS signal. However, in packet radio networks, corrupting a few more bits than the correction capability of the error correcting code (ECC).In this work, we define the location of the control channel as a frequency band used to broadcast messages for coordinating network functions. Packet length for WLANs) is sufficient to force the dropping of a data packet. Hence, the adversary need only stay active for a fraction of the time required for a packet transmission. Moreover, targeting the control channel, which typically operates at a low transmission rate, significantly reduces the adversary's effort. In fact, it was shown that the power required performing a DoS attack in GSM networks is reduced by several orders of magnitude when the attack targets the control channel.

A. Need & History of Jammers

The speedy proliferation of cell phones at the start of the twenty first century to close present standing eventually raised issues, like their potential use to invade privacy or contribute to educational cheating. Additionally, public backlash was growing against the disruption cell phones introduced in lifestyle. Whereas older analog cell phones usually suffered from poor reception and will even be disconnected by straightforward interference like high frequency noise, more and {more} subtle digital phones have semiconductor diode to more elaborate counters. Cellular phone electronic jamming devices are an alternate to costlier measures against cell phones, like Michael Faraday cages, that are principally appropriate as inbuilt protection for structures. They were originally developed for enforcement and therefore the military to interrupt communications by criminals and terrorists. Some were additionally designed to foil the utilization of sure remotely

detonated explosives. The civilian applications were apparent, thus over time several corporations originally contractile to style jammers for state use changed to sell these devices to non-public entities. Since then, there has been a slow however steady increase in their purchase and use, particularly in major metropolitan areas.

As with alternative radio electronic jamming, cellular phone jammers block cellular phone use by causation out radio waves on constant 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 merely seem out of vary. Most cell phones use completely different bands to send and receive communications from towers (called frequency division duplexing, FDD). Jammers will work by either disrupting phone to tower frequencies or tower to phone frequencies. Smaller hand-held models block all bands from 800 Mc to 1900 Mc at intervals a 30-foot varies (9 meters). Little devices tend to use the previous methodology, whereas larger costlier models might interfere directly with the tower. The radius of cellular phone jammers will vary from a dozen feet for pocket models to kilometers for a lot of dedicated units. The TRJ-89 transmitter will block cellular communications for a 5-mile (8 km) radius.

Less energy is needed to disrupt signal from tower to itinerant than the signal from itinerant to the tower (also referred to as base station), as a result of the bottom station is found at larger distance from the transmitter than the itinerant which is why the signal from the tower isn't as robust. Older jammers typically were restricted to engaged on phones exploitation solely analog or older digital itinerant standards. Newer models like the double and triple band jammers will block all wide used systems (CDMA, iDEN, GSM, et al.) and ar even terribly effective against newer 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 Europe or North America. Some cellular phone Jammers are introduced to some State Prisons within the us. Cell phones that are sneaked into jail create a security risk for guards and property house owners living near.

B. Problems in Existing Jammers

Envisage a scenario wherever you're essaying to dial 911 and can't get through as a result of somebody encompasses a mobile phone sender with him. Otherwise, you wish to decision the police to avoid a theft in your building however the thief encompasses a mobile phone sender with him. So, what may you are doing in such a dangerous situation? Electronic countermeasures devices utilized with some thoughts are also way more helpful than simply a technique of enjoyment. To get rid of these hazards a brand new economical variety of mobile sender is planned victimization FPGA. During this new style we tend to are attending to disable the computer keyboard, MIC, speaker, are solely disabled by victimization the FPGA & we tend to doing it employing a 400MHz frequency that has A public license therefore there's no want of licensing.

Some of the Common issues are listed below:

- The person didn't even get the notification of a decision or message once he's within the sender coverage space.
- The person cannot be contacted for a few imperative data additionally.
- Nearly the portable are in turn out state.
- There won't be any notification that the user mobile has been jam-panicked.

II. PROPOSED SYSTEM DESIGN

In most countries, it's hot for personal voters to jam cell-phone transmission; however some countries are permitting businesses and government organizations to put in jammers in areas wherever cell-phone use is seen as a nuisance. In Dec 2004, France legalized cell-phone jammers in show theaters, concert halls and different places with performances. France is finalizing technology which will let calls to emergency services undergo. Republic of India has put in jammers in parliament and a few prisons. It's been rumored that universities in Italian Republic have adopted the technology to forestall cheating. Students were taking photos of tests with their camera phones and causation them to classmates. Alternatives to mobile phone electronic countermeasures while the law clearly prohibits employing a device to actively disrupt a cell-phone signal, there are not any rules against passive cell-phone interference. Which means victimization things like wallpaper or building materials embedded with metal fragments to forestall cell-phone signals from reaching within or outside the area? Some buildings have styles that block radio signals by chance as a result of thick concrete walls or a steel skeleton. Corporations are acting on devices that management a mobile phone however don't "jam the signal." One device sends incoming calls to voicemail and blocks outgoing calls.

The argument is that the phone still works; therefore it's technically not being jam-panicked. It's a legal area that has not been dominated on by the Federal Communications Commission as of Apr 2005. Cell-phone alerter's is out there that indicate the presence of a cell-phone signal. These are employed in hospitals wherever cell-phone signals may interfere with sensitive medical instrumentation. Once a symptom is detected, users are asked to show off their phones. For a less technical resolution, Caudal Partners, a style firm in Chicago, has launched the SHHH, the Society for hand-held Hushing. At its computer, you'll transfer a note handy to individuals conducting annoying cell-phone conversations, expressing your lack of interest in what they are talking regarding.

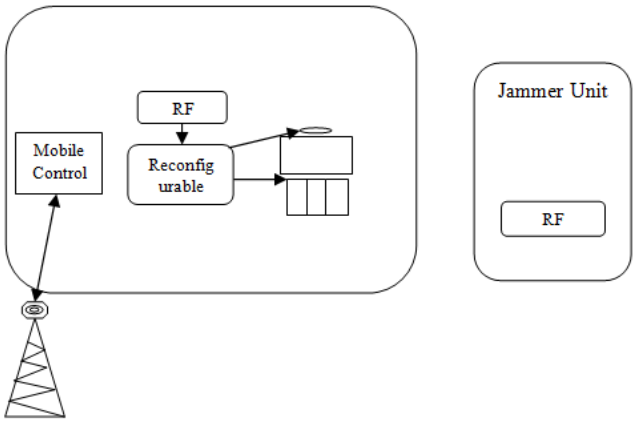

Figure1. Mobile Jammer General Block Diagram.

III. FPGA

A Field-programmable Gate Array (FPGA) is Associate in nursing computer circuit designed to be organized by the client or designer once manufacturing hence "field-programmable". The FPGA configuration is usually such as employing a hardware description language (HDL), the same as that used for Associate in Nursing application-specific computer circuit (ASIC) (circuit diagrams were antecedently accustomed specify the configuration, as they were for ASICs, however this is often progressively rare). FPGAs are often accustomed implement Associate in Nursing logical operate that an ASIC may perform. the power to update the practicality once shipping, partial re-configuration of the portion of the style[1] and also the low non-recurring engineering prices relative to Associate in Nursing ASIC design (notwithstanding the widely higher unit cost), provide blessings for several applications. FPGAs contain programmable logic elements referred to as "logic blocks", and a hierarchy of reconfigurable interconnects that permit the blocks to be "wired together"—somewhat like several (changeable) logic gates which will be inter-wired in (many) completely different configurations. Logic blocks are often organized to perform complicated combinatory functions, or just easy logic gates like AND and XOR. In most FPGAs, the logic blocks additionally embrace memory parts, which can be easy flip-flops or additional complete blocks of memory.

In addition to digital functions, some FPGAs have analog options. the foremost common analog feature is programmable slew rate and drive strength on every output pin, permitting the engineer to line slow rates on gently loaded pins that will otherwise ring intolerably, and to line stronger, quicker rates on heavily loaded pins on high-speed channels that will otherwise run too slow. Another comparatively common analog feature is differential comparators on input pins designed to be connected to differential sign channels. a number of "mixed signal FPGAs" have integrated peripheral Analog-to-Digital Converters (ADCs) and Digital-to-Analog Converters (DACs) with analog signal learning blocks permitting them to control as a system-on-a-chip. Such devices blur the road between Associate in Nursing FPGA that carries digital ones and zeros on its internal programmable interconnect material, and field-programmable analog array (FPAA), that carries analog values on its internal programmable interconnect material.

IV. RF ENCODER AND DECODER

A. General Encoder and Decoder Operations

The Holtek HT-12E IC encodes 12-bits of {data of knowledge} and serially transmits this data on receipt of a Transmit change, or an occasional signal on pin-14 /TE. Pin-17 the D_OUT pin of the HT-12E serially transmits no matter knowledge is offered on pins ten, 11, 12 and 13, or D0, D1, D2 and D3. Knowledge is transmitted at a frequency selected by the external generator resistance. By mistreatment the switches hooked up to the information pins on the HT-12E, as shown within the schematic, we will choose the data in binary format to send to the receiver. The receiver section consists of the Ming dynasty RE-99 and also the HT-12D decoder IC. The DATA_IN pin-14 of the HT-12D reads the 12-bit binary data sent by the HT-12E and so places this knowledge on its output pins. Pins 10, 11, 12 and thirteen square measure the information out pins of the HT-12D, D0, D1, D2 and D3. The HT-12D receives the 12-bit word and interprets the primary 8-bits as address and also the last 4-bits as knowledge. Pins 1-8 of the HT-12E square measure the address pins. Mistreatment the address pins of the HT-12E, we will choose completely different addresses for up to 256 receivers.

The address is set by setting pins 1-8 on the HT-12E to ground, or simply exploits them open. The address selected on the HT-12E circuit should match the address selected on the HT-12D circuit (exactly), or the data are unnoticed by the receiving circuit. When the received addresses from the encoder matches the decoders, the Valid Transmission pin-17 of the HT-12D can go HIGH to point that a sound transmission has been received and also the 4-bits of knowledge square measure secured to the information output pins, 10-13. The semiconductor circuit shown within the schematic can use the VT, or valid transmission pin to lightweight the LED. Once the VT pin goes HIGH it activates the 2N2222 semiconductor that successively delivers power to the LED providing a visible indication of a sound transmission reception.

B. Controlling the Project with a FPGA

Using these RF transmitter & receiver circuits with a FPGA would be easy. We will merely replace the switches used for choosing knowledge on the HT-12E with the output pins of the FPGA. Additionally we will use another output pin to pick TE, or transmit change on the HT-12E. By taking pin-14 LOW we have a tendency to cause the transmitter section to transmit the information on pins 10-13. To receive data merely attach the HT-12D output pins to the FPGA. The VT or valid transmission pin of the HT-12D may signal the FPGA to grab the 4-bits of knowledge from

the information output pins. If you're employing a FPGA with interrupt capabilities, use the VT pin to cause a jump to Associate in Nursing interrupt vector and method the received knowledge. The HT-12D knowledge output pins can LATCH and stay during this state till another valid transmission is received. NOTE: you may notice that in each schematic every of the Holtek chips have resistors hooked up to pins fifteen and sixteen. These resistors should be the precise values shown within the schematic. These resistors set the inner oscillators of the HT-12E/HT-12D. It's suggested that you simply select a tenth resistance for every of those resistors to make sure the right circuit oscillation.

C. Range of Operation

The normal operative varies mistreatment (only) the LOOP TRACE ANTENNA on the transmitter board is concerning fifty feet. By connecting 1/4 wave antenna mistreatment nine.36 inches of twenty-two gauge wire to each circuits, you'll be able to extend this vary to many hundred feet. Your actual vary could vary owing to your finished circuit style and environmental conditions. The transistors and diodes are often substituted with any common equivalent kind. These can usually depend upon the categories and capacities of the actual hundreds you wish to manage and may be selected consequently for your supposed application.

D. RF Details

The TWS-434 and RWS-434 square measure extraordinarily little, and square measure glorious for applications requiring short-range RF remote controls. The transmitter module is simply 1/3 the scale of a regular postage, and might simply be placed within a little plastic enclosure. TWS-434: The transmitter output is up to 8mW at 433.92MHz with a variety of roughly four hundred foot (open area) outdoors. Indoors, the variation is or so two hundred foot and can undergo most walls.

Figure2. RF 434 Mhz Transmitter. Modulation: ASK

The TWS-434 transmitter accepts each linear and digital inputs, will operate from one.5 to twelve Volts-DC, and makes building a miniature hand-held RF transmitter terribly straightforward. The TWS-434 is close to the dimensions of a customary item.

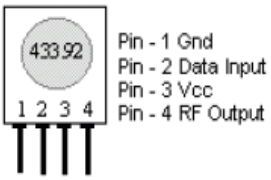

Figure3. RF-434 Pin Diagram

E. LCD Display

More FPGA devices are victimization 'smart LCD' displays to output visual data. The subsequent discussion covers the affiliation of a 16x2 liquid crystal {display|LCD| digital display alphanumeric display} display to a PIC FPGA. Digital display displays designed around Hitachi's digital display HD44780 module, are cheap, simple to use, and it's even doable to provide readout victimization the eight x eighty pixels of the show. Hitachi digital display displays have a customary code set of characters and Japanese, Greek and mathematical symbols. For an 8-bit information bus, the show needs a +5V offer and eleven I/O lines. For a 4-bit information bus it solely needs the provision lines and seven additional lines. Once the liquid crystal {display|LCD|digital display alphanumeric display} display isn't enabled, information lines are tri-state which suggests they're in a very state of high impendence (as the' they're disconnected) and this implies they are doing not interfere with the operation of the FPGA once the show isn't being addressed. Reading information from the digital display is completed within the same method, however management line R/W should be high. After we send a high to the digital display, it'll reset and anticipate directions. Typical directions sent to liquid crystal {display|LCD|digital show alphanumeric display} display when a reset is: turning on a display, turning on a pointer and writing characters from left to right. Once the digital display is initialized, it's able to continue receiving information or directions. If it receives a personality, it'll write it on the show and move the pointer one area to the proper. The pointer marks future location wherever a personality is going to be written. After we wish to jot down a string of characters, initial we want to line up the beginning address, so send one character at a time. Characters that may be shown on the show are hold on in information show (DD) RAM. The dimensions of DDRAM are eighty bytes.

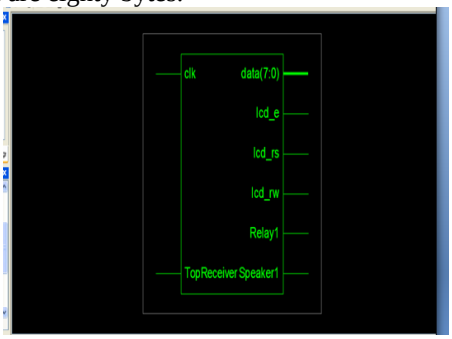

Figure4. RTL view of VHDL coding.

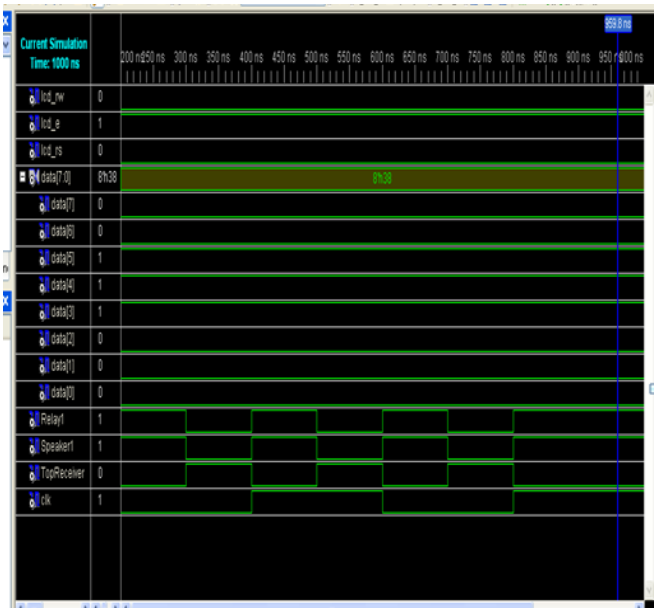

Figure5. Output Waveforms of our Proposed Mobile jammer.

V. CONCLUSION

Our projected Mobile sender is functioning dead while not touching the signals from the network. So the user will ready to get the notifications relating to Calls and messages (SMS, MMS). The notification regarding the calls is given to the user. If there's any imperative decision as we will get the notification we will depart from the coverage space and use our mobile because it is. No would like of licensing. Implementation of our recently designed jammers is straightforward. As we have a tendency to square measure employing a FPGA, our hardware is changed whenever we wish. Is enforced wherever silence to be maintained. Future modifications square measure potential simply. Misuse of mobiles is restricted. So our Mobile jammers will offer higher potency with lower misuses.

VI. REFERENCES

[1] D. Adamy. EW 101: A first course in electronic warfare. Artech House Publishers, 2001.
[2] I. Akyildiz, W. Lee, M. Vuran, and S. Mohanty. Next generation dynamic spectrum access cognitive radio wireless networks: A survey. Computer Networks, 50(13):2127–2159, 2006.
[3] L. C. Baird, W. L. Bahn, M. D. Collins, M. C. Carlisle, and S. C. Butler. Keyless jam resistance. In Proceedings of the 2007 IEEE Workshop on Information Assurance United States Military Academy, 2007.
[4] T. X. Brown, J. E. James, and A. Sethi. Jamming and sensing of encrypted wireless ad hoc networks. In Proceedings of the ACM MobiHoc, pages 120–130, 2006.
[5] M. Cagalj, S. Capkun, and J.-P. Hubaux. Wormhole-based anti-jamming techniques in sensor networks. IEEE Transactions on Mobile Computing, 6(1):100–114, 2007.
[6] A. Chan, X. Liu, G. Noubir, and B. Thapa. Control channel jamming: resilience and identification of traitors. In Proceedings of ISIT, 2007.
[7] www.wikipedia.org
[8] www.xilinx.com
[9] www.mobilejammers.com
[10] J. T. Chiang and Y.-C. Hu. Cross-layer jamming detection and mitigation in wireless broadcast networks. In Proceedings of the MobiCom, pages 346–349, 2007.
[11] Y. W. Law, L. V. Hoesel, J. Doumen, P. Hartel, and P. Havinga. Energy efficient link-layer jamming attacks against wireless sensor network MAC protocols. In Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN), 2005.
[12] L. Lazos, S. Liu, and M. Krunz. Mitigating control-channel jamming attacks in multi-channel ad hoc networks. In Proceedings of the 2nd ACM Conference on Wireless Network Security (WiSec), pages 169–180, 2009.
[13] L. Lazos, S. Liu, and M. Krunz. Spectrum opportunity-based control channel assignment in cognitive radio networks. In Proceedings of SECON, pages 135–143, 2009.
[14] M. Li, I. Koutsopoulos, and R. Poovendran. Optimal jamming attacks and network defense policies in wireless sensor networks. In Proceedings of the INFOCOM, 2007.
[15] G. Lin and G. Noubir. On link-layer denial of service in data wireless LANs. Journal on Wireless Communications and Mobile Computing, 2004.
[16] X. Liu, G. Noubir, R. Sundaram, and S. Tan. SPREAD: Foiling smart jammers using multi-layer agility. In Proceedings of the INFOCOM Mini Symposium, 2007.

Author's Profile:

D.Swathi
M.Tech student of GPCET, JNTU, Ananthapur University, AP, India.

Mrs.P.Parvati received her B.Tech degree from Vijayanagara Engineering College, Bellary, Karnataka, India. In ECE in 2007.Master's Degree from vishveshwara Institute of Technology, Bangalore, Karnataka, In VLSI Design and Embedded Systems in 2009.She is presently working as faculty in G.P.C.E.T, AP, India.

Mrs. B. Naga Prasanna received her Master's degree from KLU University in Communications and Radar Engineering and she is working as an Assistant Professor of GPCET, AP, India.