# Design of A Cooperative Jammer Providing Notifications To The User

S. Rajalingam[1], S. Duraichamy[2]

*Assistant Professor(Senior Scale)[1], Assistant Professor[2]*

*Department of Electronics and Communication Engineering, Rajalakshmi Institute of Technology, Kuthambakkam, Chennai*

***Abstract - Cell phones today have become a necessity in human being life. It is treated as a vital instrument carried by individual to be informed and connected with the world. Cell phones cannot be used in all the areas where it may result in 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 existing jammer does not provide any information about the incoming calls and messages even at the time of urgency. Hence, a new mobile jamming system is proposed using VLSI technology. 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.***

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

## I. INTRODUCTION

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 the mobile jammer devices are becoming civilian products rather than electronic warfare devices, since 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.

Mobile jammer is used to prevent mobile phones from receiving or transmitting signals with the base stations. Mobile jammer effectively disable mobile phones within the defined regulated zones without causing any interference to other communication means Mobile jammer can be used in practically any location, but are used in places where a phone call would be particularly disruptive like Temples, Libraries, Hospitals etc.[2]

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 to design mobile jammer for government switched over to sell these devices to private entities.

As with other radio jamming, mobile jammer 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 jammer, 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 high power mobile jammer for your organization to very high power military jammers to jam a large campuses.

## II. JAMMING BASICS

Disrupting a cell phone is the same as jamming any other type of radio communication. A cell phoneworks 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.It's a called a **denial-of-service attack**. The jammer denies service of the radio spectrum to the cell-phone users within range of the jamming device.Jamming devices overpower the cell phone by transmitting a signal on the same frequency and at a high enough power that the two signals collide and cancel each other out. Cell phones are designed to add power if they experience low-level interference, so the jammer must recognize and match the power increase from the phone.[4]

Cell phones are full-duplex devices, which means they use two separate frequencies, one for talking and one for listening simultaneously. Some jammers block only one of the frequencies used by cell phones, which has the effect of blocking both. The phone is tricked into thinking there is no service because it can receive only one of the frequencies.Less complex devices block only one group of frequencies, while sophisticated jammers can block several types of networks at once to head off dual-mode or tri-mode phones that automatically switch among different network types to find an open signal. Some of the high-end devices block all frequencies at once, and others can be tuned to specific frequencies.To jam a cell phone, all you need is a device that broadcasts on the correct frequencies. Although different cellular systems process signals differently, all cell-phone networks use radio signals that can be interrupted. 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. 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. Low-powered jammers block calls in a range of about 30 feet (9 m). Higher-powered units create a cell-free zone as large as a football field. Units used by law enforcement can shut down service up to 1 mile (1.6 km) from the device.

## III. PROBLEM STATEMENT

Envisage a situation where you are trying to dial 100 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.

The use of an ordinary jammer in libraries, there is a chance of playing audio file, through which readers are disturbed. Also there is a chance of misuse of mobiles in examination halls. To remove all these hazards, a new efficient type of mobile jammer is proposed using FPGA.

## IV. PROPOSED 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.

### a) 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.

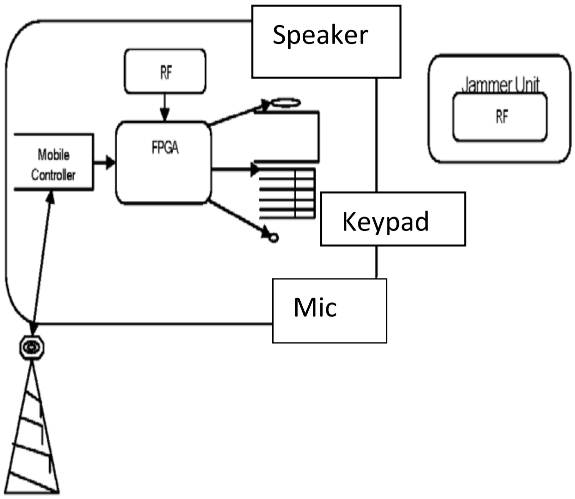

Fig 4.1 Schematic Diagram Of The Proposed Jammer

**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.When a signal is detected, users are asked to turn off their phones.For a less technical solution, Caudal Partners, a design firm in Chicago, has launched the SHHH, the **Society for Handheld Hushing**. At its Web site, you can download a note to hand to people conducting annoying cell-phone conversations, expressing your lack of interest in what they're talking about.

Fig 4.1 shows the system schematic diagram where connections between different hardware components are provided. As shown in the fig, a receiver module is connected with FPGA which controls the mobile controller unit receiving signal from the signal tower. Transmitter section acts as a jammer section, since it is used to provide the signal to disable the features of mobile phone.

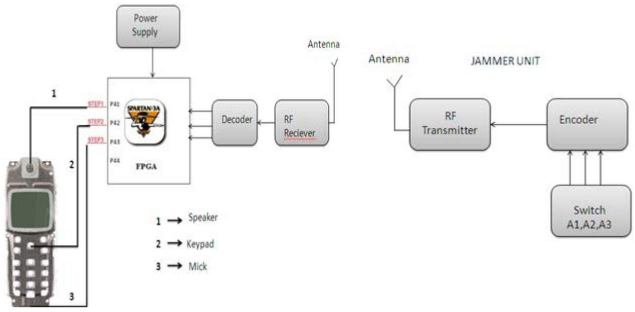

Fig 4. 2 System Block Diagram

Fig 4.2 shows the block diagram of the proposed project. Jammer unit consists of a RF transmitter, an encoder to convert parallel data into serial data along with the operating switches. The mobile section consists of the RF receiver, a decoder to convert serial data into parallel data, an FPGA kit to control the relay circuit and a mobile phone.

## V. FPGA

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 and the low non-recurring engineering costs relative to an ASIC design (notwithstanding the generally higher unit cost), offer advantages for many applications.

FPGAs 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 ANDandXOR. 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 signalling channels. A few "mixed signalFPGAs" 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.[5] 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.

## VI. RF MODULE

This **RF module** comprises of an **RF Transmitter** and an **RF Receiver**. The transmitter/receiver (TX/Rx) pair operates at a frequency of **434 MHz.**An RF transmitter receives serial data and transmits it wirelessly through RF through its antenna connected at pin4. The transmission occurs at the rate of 1Kbps - 10Kbps.The transmitted data is received by an RF receiver operating at the same frequency as that of the transmitter.

The RF module is often used along with a pair of encoder/decoder. The encoder is used for encoding parallel data for transmission feed while reception is decoded by a decoder HT12E-HT12D, HT640-HT648, etc. are some commonly used encoder/decoder pair ICs.

### a) RF TRANSMITTER

This simple RF transmitter, consisting of a 434MHz license-exempt Transmitter module and an encoder IC, was designed to remotely switch simple appliances on and off. The RF part consists of a standard 434MHz transmitter module, which works at a frequency of 433.92 MHz and has a range of about 400m according to the manufacture. The transmitter module has four pins. Apart from “Data” and the “Vcc” pin, there is a commonground (GND) for data and supply. Last is the RF output (ANT) pin.

Note that, for the transmission of a unique signal, an encoder is crucial. For this, I have used the renowned encoder IC HT12E from Holtek. HT12E is capable of encoding information which consists of N address bits and 12N data bits. Each address/ data input can be set to one of the two logic states. The programmed addresses/data are transmitted together with the header bits via an RF transmission medium upon receipt of a trigger signal.

Solder bridges TJ1 and TJ2 are used to set the address and data bits.

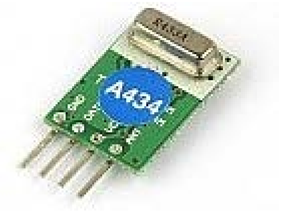

Fig 5.1 RF Transmitter

The current consumption with a supply voltage of near 5.4V is about 10 mA. Since the current consumption is very little, the power can also be provided by standard button cells. Recommended antenna length is 17 cm for 433.92 MHz, and a stiff wire can be used as the antenna. Remember to mount the antenna (aerial) as close as possible to pin 4 (ANT) of the transmitter module.

b) RF RECEIVER

This circuit complements the RF transmitter built around the small 434MHz transmitter module. The receiver picks up the transmitted signals using the 434 MHz receiver module. This integrated RF receiver module has been tuned to a frequency of 433.92MHz, exactly same as for the RF transmitter.

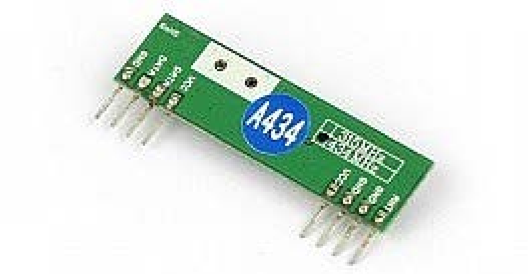

Fig 5.2 RF Receiver

The miniature 434MHz RF receiver module receives On-Off Keyed (OOK) modulation signal and demodulates it to digital signal for the next decoder stage. Local oscillator is made of Phase Locked Loop (PLL) structure. Technically, this is an Amplitude Shift Keying (ASK) receiver module based on a single-conversion, super-heterodyne receiver architecture and incorporates an entire Phase-Locked Loop (PLL) for precise local oscillator (LO) generation. It can use in OOK / HCS / PWM modulation signal and demodulate to digital signal.

The receiver module has eight (4+4) pins. Apart from three "ground (GND) " and two "Vcc" pins, there are two pins (one for Digital Data & other for Linear Data) for data output. Last is the RF input (ANT) pin.

The "coded" signal transmitted by the transmitter is processed at the receiver side by the decoder IC HT12F from Holtek. VR1 and R1 are used to tweak the oscillator frequency of the decoder to that of the transmitter. Any possible variations due to component tolerances and/or a different supply voltage can be compensated by this arrangement. HT12F is capable of decoding information that consists of N bits of address and 12N bits of data. HT12F decoder IC receives serial addresses and data from the HT12E encoder that are transmitted by the RF transmitter module. HT12D compare the serial input data three times continuously with the local addresses.

For proper operation, a pair of HT12E/HT12F ICs with the same number of addresses and data format should be chosen. The data bits are set up using solder bridges RJ1 and RJ2. Output of the decoder is brought out on a pinheaded K1, making the logical signal available to circuits that need it. This output is also fed to the relay driver transistor T1. The RF Receiver circuit can be powered from a standard 5VDC supply. Just as for the RF Transmitter, the aerial (17 cm for 433.92 MHz) has to be mounted as close as possible to the RF IN (ANT) pin of the 434MHz RF receiver module.

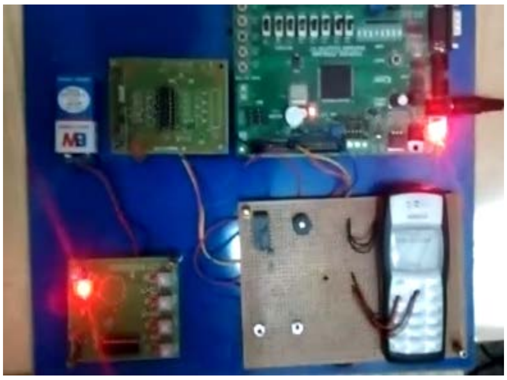

Fig 6.1 Proposed Mobile Jammer

## VII. CONCLUSION

Thus this project is of great use in areas where silence is to be preserved at the same time the user gets notifications about the incoming signals , it may be a message or a phone call. The use of existing mobile jammers has become illegal as it can be misused easily at the time of robbery. And also mobile phone jammer will end up being a hurdle within the public .Thus the output of this project is more advantageous than the existing model. The system performs well under different circumstances and in practical situations and its results are tested and verified.

## VIII. REFERENCES

[1] SeongahJeong, Keonkook Lee, Heon Huh, and Joonhyuk Kang, "Secure Transmission in Downlink Cellular Network with a Cooperative Jammer,"*IEEE WIRELESS COMMUNICATIONS*

*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 beamforming for AF relay networks with multiple eavesdroppers,”*IEEESignalProcess.Lett.*, vol. 20, no. 1, pp. 35–38, Jan. 2013.

[3] M. Vzquez, A. Prez-Neira, and M. Lagunas, “Confidential communication in downlink beamforming,” 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 semidefinite programming,”*IEEE Trans. SignalProcess.*, 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 messages,” in *Proc.IEEE Int. Symp. Inf. Theory*, Austin, TX, Jun. 2010.

[9] E. Ekrem and S. Ulukus, “Gaussian MIMO broadcast channels with common and confidential messages,” in *Proc. IEEE Int. Symp.Inf.Theory*, Austin, TX, Jun. 2010. [10] T. Liu and S. Shamai (Shitz), “A note on the secrecy capacity of the multiple-antenna wiretap channel,”*IEEE Trans. Inf. Theory*, vol. 55, no. 6, pp. 2547–2553, Jun. 2009.

[11] A. S. Motahari and A. K. Khandni, “Capacity bounds for the Gaussian interference channel,”*IEEE Trans. Inf. Theory*, vol. 55, no. 2, pp. 620–643, Feb. 2009.