ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Cell Phone Jamming for Safe Driving to Avoid Accidents

Rubiya Yasmin [*1], M.Jasmin [2], Kiran Kumar [3]
[*1] M.Tech (VLSI Design), [2] Assistant Professor, [3] Head of the Department,
Department of Electronics and Communication Engineering, Bharath University, India
rubiyayasmin@gmail.com

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: RF Transmitter, RF Receiver, FPGA, Jammers, Interference, Encoded Signal, Vehicle Unit, Mobile Unit, RAM, Switch.

Introduction

THE radio broadcast of the opposition is often jammed using jammers during wartime to avoid people from getting information about the broadcast from their country. The technology of jamming during these periods were simple and hence the radio broadcast station of the opposition alters the frequencies, transmission power is increased and additional frequency is added.

The Nazis, in occupied Europe, tried to block broadcasts to the continent from the BBC and other allied stations. Counteract was made to this jamming by increasing transmitter power, adding extra frequencies .

The Global Positioning Systems (GPS) used by the opposition to track the place were also jammed using jammers so that the troops lose their way.

The mobile jammers came into picture when there was fast growth of usage of cell phones at the beginning of the 21st century, eventually raised problems such as their potential use to invade privacy, contribute to academic cheating, or even in illegal industrial surveillance. In addition public criticism was growing against the disturbing interruption of cell phones in day to day life. The primitive analog cell phones often experienced persistent bad signal reception and calls could even get terminated by simple interference such as high frequency noise.

The hi-tech digital phones have led to more complicated 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.

Related work

The jammers currently available successfully jams the signal from base station by transmitting a RF signal that are stronger than the signal received by the mobile from the base station. Some of the jamming techniques currently used in different jammers are given below

Spoofing:

In this type of jamming, when a mobile phone enters the region of jammer, it is forced to switch off. No calls can be received or can be made. Some jammers

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

send a notification to user that the device is going to switch off or a request is sent to switch off the device.

This type of jammers can be used in examination hall, airplanes or places where disturbances cannot be tolerated. Places where usages of mobile phones depends upon the urgency or importance, cannot use this kind of jammers. Upgrade of this system is difficult. A new system has to be formulated and designed if upgrade is required.

Shielding attacks:
Shielding attacks is identified as TEMPEST or EMF shielding. In this type of jamming, an area is enclosed in a faradays cage and any device inside this cage cannot transmit or receive any RF signal.

Denial of service:
Denial of Service also referred to as DOS. This is the simplest technique in which a noise signal is sent to the mobile phone to reduce the signal to noise ratio. This automatically reduces the signal received and hence the service is denied.

The user still will be able to access the other applications of the mobile but cannot attend or make any calls. Also the user will not be notified of any calls or message since the service provided by the base station is completely denied.

As mentioned in the above techniques as the methods successfully achieves the goal but fails to notify the person about the calls or the messages received. Hence a car jammer is designed and developed in this project that successfully avoids the user from using the mobile when driving and also notifies the person about the call or messages received.

Depending upon the urgency of the call the person can pull over the car and attend the call. Another main aspect of the system developed is that the system can be modified or upgraded any point of time.

Instead of blocking the signal received by mobile, the system locks the mobile from using it when it enters the jamming region. Hence the complex algorithm and programming involved for jamming the signal from base station are avoided.

Hardware setup

The main concept of the system is that when the vehicle ignition is turned on then the mobile phones in the car is locked such that user cannot make or attend to any calls but still the notification of the calls are received. Thus the system does not jams the signal received from the base station but instead locks the mobile phone.

The system consists of two units. Vehicle unit and mobile unit. The communication between the vehicle unit and the mobile is established through a wireless medium to avoid fussy and complex wired transmission. Since the system here is specifically designed as a mobile phone jammers in the car, the communication range between the vehicle unit and mobile unit is less.

Considering the above points, a simple mode of wireless communication can be opted for this system that does not involve high programming and complex algorithms. Hence RF transmitter and receiver is used in this system for wireless communication.

RF Transmitter
RF transmitter TWS-434 is implemented in the system which is extremely small and suitable for shorter RF communication. The transmitter output is up to 8mW at 433.92 MHz with a range of approximately 400 foot outdoors and 200 foot indoors. The TWS-434 transmitter operates from 1.5 to 12 V DC and accepts both digital and linear inputs.

Fig - 1 TWS-434

RF Receiver
RWS-434 is deployed as RF receiver in this system. As the transmitter, the receiver also operates at 433.92 MHz, to match the communication with that of the transmitter and has a sensitivity of 3µV. The RWS-434 receiver has both linear and digital outputs and operates from 4.5 to 5.5 V DC.

Fig – 2 RWS-434

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

Encoder

The wireless module does not incorporates inbuilt encoder and decoder. Hence a separate encoder and decoder is used. HT-12E is used as encoder which is a Holtek made encoder. The 212 encoders are a series of CMOS LSIs for remote control system applications. They are capable of encoding 12_N data bits and N address bits information.

Each address/ data input can be set to one of the two logic states. Upon receipt of a trigger signal, the encoder sends an encoded signal of data or addresses via RF transmitter. The HT12E enhances the application flexibility of the 212 series of encoders by providing an option for selecting transmit enable - TE trigger.

Decoder

To pair the HT12E series encoder used, HT12D series is implemented. To match the communication between the vehicle and mobile unit proper encoder and decoder must be selected. Hence a same series encoder and decoder is used which decodes the same number of bits of data or addresses it receives via RF receiver.

FPGA

The main advantage of this system is the implementation of Field Programmable Gate Array commonly known as FPGA. Spartan 3A series FPGA is used in this project. The FPGA design flow involves design entry, synthesis, simulation, implementation and programming. The main advantage of using FPGA is that the program can be modified and updated or altered at any point of time.

Some of the important features of Xilinx Spartan-3A are it is high-performance logic solution, very low cost for high-volume, cost-sensible applications. It simplifies 3.3V-only design by providing dual-range VCC AUX supply. Effective use of system power is done as suspend and hibernate modes are available.

When system is idle it will enter into any one of the above said mode according to the program. Multi-standard select IO interface pins and Multi-voltage are provided in this series. Abundant, flexible logic resources, up to eight Digital Clock Managers (DCMs) makes this suitable to our system.

Hierarchical Select RAM memory architecture, eight low-skew global clock networks, eight additional clocks per half device, plus abundant low-skew routing and configurable interface to industry-standard PROM are the added features of this series.

Test setup

The system is designed such that when the engine of the vehicle is turned on, the system locks the microphone, loud speaker and the keypad of the mobile phone. The vehicle unit has switch, encoder and RF transmitter.

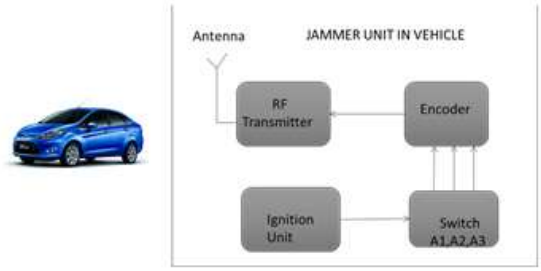

Fig - 3 Block Diagram of Vehicle Unit.

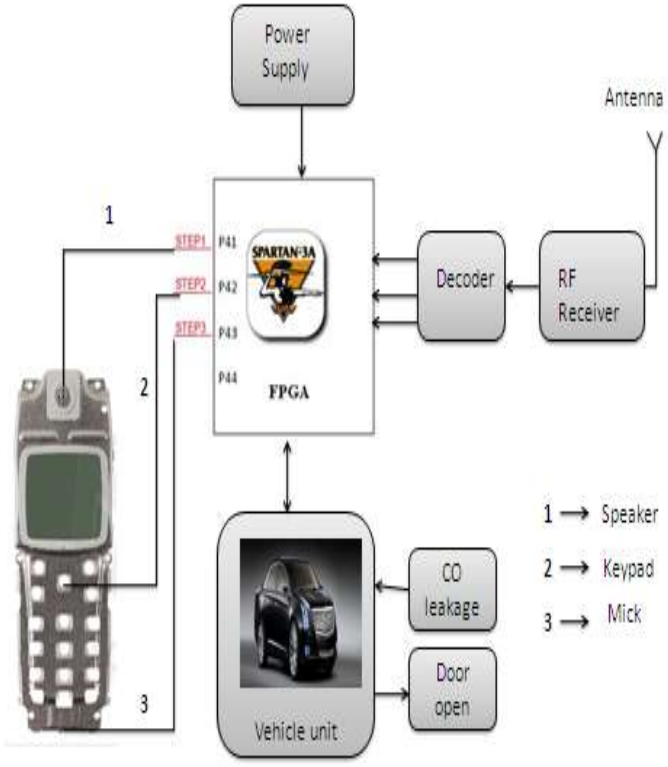

Fig - 4 Block Diagram of Mobile Unit

Switch A1, A2, A3 is connected to the ignition unit to immediately sense the system when it turns on. An encoder is implemented in the system which encodes the signal received from the switch. This encoded signal is transmitted to the mobile unit via RF transmitter

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 1.852

The mobile unit consists of RF receiver, decoder, FPGA connected to the mobile phone. The RF receiver receives the encoded signal from the RF transmitter and passes it on to the decoder. The decoder decodes the signal and feeds it to the FPGA. Pin 41, pin 42, pin 43 of FPGA is connected to the speaker, keypad and microphone respectively.

According to the signal received, the FPGA locks the microphone, loud speaker and keypad of the mobile phone. Hence the signal from the base station to the mobile is not corrupted or interrupted. The calls and text messages can still be received by the mobile phone but the user cannot access it.

Conclusion

The system designed above successfully locks the mobile when it enters the jamming region. The notification about the calls and messages were done effectively. The jammer designed here is specifically for cars. But the implementation of FPGA instead of a controller is an added advantage with which we can alter programs for other specific jamming or can be performance upgraded. The jammer is turned on as soon as the vehicle ignition turns on. Hence a person intended to attend a call or make a call he has to pull over and turn of the ignition to do or to get out of the car. By this way, the person cannot neglect or switch of the jammer as his desire to attend even if it is an urgent call. The system performs well under different circumstances and in practical situations and its results are tested and verified.

References

1. World Health Organisation, Fact Sheet: “The Top Ten Causes of Death, no.310, May 2010.
2. L. Aarts and I. van Schagen, “Driving speed and the risk of road crashes:A review”, Accident Analysis & Prevention, vol. 38, no. 2, pp. 215-224,2006.
3. Google Official Blog, “http://googleblog.blogspot.com/2012/05/new- research-shows-smartphone-growth-is.html”, accessed August 2012. [4] G. Rose, “Mobile Phones as Traffic Probes: Practices, Prospects and Issues”, Transport Reviews, vol. 26, no. 3, 2006.
4. P. Mohan, V.N. Padmanabhan, and R. Ramjee, “Nericell: rich monitoring of road and traffic conditions using mobile smartphones”, Proceedings of the 6th ACM conference on Embedded network sensor systems, pp. 323-336, 2008.
5. D.A. Johnson and M.M. Trivedi, “Driving Style Recognition using a Smartphone as a Sensor Platform”, Proceedings of the 14th International Conference on Intelligent Transport Systems, pp. 1609-1615, 2011.
6. C. Thompson, J. White, B. Dougherty, A. Albright and D.C. Schmidt, “Using Smartphones to Detect Car Accidents and Provide Situational Awareness to Emergency Responders”, Proceedings of the 3rd Mobile Wireless Middleware, Operating Systems, and Applications Conference, pp. 29-42, 2010.
7. J. Yoon, B. Noble and M. Liu, “Surface street traffic estimation”, Proceedings of The 5th International Conference on Mobile Systems, Applications, and Services, pp. 220-232, 2007.