International Journal of Engineering Research & Management Technology ISSN: 2348-4039

March- 2015 Volume 2, Issue-2

Email: editor@ijermt.org www.ijermt.org

VIWA- Vibrating Watch Anti Theft System for Mobile Phones Using Zigbee Modules

Aayush Tandon, Bhavya Awasthi
B.Tech Students
Department of ECE
SRM University, NCR Campus
Modinagar, Ghaziabad

Arun Kumar
Assistant Professor
Department of ECE
SRM University, NCR Campus
Modinagar, Ghaziabad

ABSTRACT:
In present world, costly items such as mobile phones, Tablets, Laptops are prone to theft are required to be monitored to ensure safety. This report presents a way of monitoring the phones within a short distance by the use of wireless security system. It is implemented using modules which are capable of communicating with each other. The LED and buzzer attached to the modules sounds instantly when the phone moves approximately eight meters away from the owner to the fixed location. The modules are designed with two ATmega8 microcontrollers and CC2500 ZigBee modules. A wrist band on which a receiver is mounted with a vibrator, vibrates when phone cross the eight meter margin. Hence, through our project implementation we can secure it at the same time when it is stolen or lost by electronic mobile cover.

Keywords: CC2500 ZigBee, ATmega8, IC 7805

I. INTRODUCTION

The thefts of valuable phones or valuable goods are increasing every day. There is a tremendous increase of theft in public places in the previous years. In the current situation how to protect the phones such as mobile phones, laptops and tablets has become a tough task. These phones are easy for thieves to steal and resale. According to statistics, for every fifty three seconds a phone is stolen. Checking the physical presence and location of these devices is an important task needed at all times. There can be number of ideas to protect the phones from being stolen. We can reduce the amount of theft by using an anti theft alarm system. A buzzer is present at the transmitting end or cover of the phone in which LED is attached; it is having a wrist band or receiving portion which vibrates when phone is out of range. The owner of the phone is alerted by an alarm if the phone is moved eight meters away. In wireless communication, data is broadcasted by radio frequencies. As a result, data may be captured when it is broadcasted. There are many wireless communication technologies such Zig Bee, WIFI, RF, Bluetooth, etc. Various wireless technologies have different communication range from centimetres to several hundred meters. In this project a range approximately eight meters is used because it is easy to protect the phone from being stolen. Eight meters range is an accessible range and can be more effective than others.

II. EVOLUTION OF ANTI THEFT SYSTEMS FOR MOBILE PHONES

The design of anti-theft alarm systems is an important safety measure to keep a mobile phone safe. The main idea of this design is to give information or any kind of alarm or warning to the owner of the phone when the phone is moved from its original position. A personal phone alarm device is designed which works on a position sensing principle and gives out an audible alarm ,starts blinking of LED and vibration on wrist band in case of theft. The device is housed in a sealed box with an opening for the sound signal to come out and is comprised of an alarm,

sensing switch and a battery source. It also has a receiving section on the owner wrist which vibrates when the phone is out of range. The device has two position sensitive switches which are employed in the design to overcome any faulty errors that may occur with the use of the single switch. ZigBee modules have high accuracy than normal RF modules as number of other RF devices can be working the region which can interrupt the signal but ZigBee has high frequency than RF which makes it more efficient and accurate. Previous models of anti theft system consist of position sensing of mobile phones using timers .It was consisting a pulse generator at transmitter end and a timer at receiver end when there is any delay in the receiving of the signal the buzzer starts beeping and the theft is indicated. After this, a frequency receiving anti theft device was made in which frequencies are compared simultaneously and if there is any weak signal found then it triggers alarm.

III. WHAT IS ZIGBEE

ZigBee is an IEEE 802.15.4 standard for data communications with business and consumer devices. It is designed around low-power consumption allowing batteries to essentially last forever. The ZigBee standard provides network, security, and application support services operating on top of the IEEE 802.15.4 Medium Access Control (MAC) and Physical Layer (PHY) wireless standard. It employs a suite of technologies to enable scalable, self-organizing, self-healing networks that can manage various data traffic patterns. ZigBee is a low-cost, low-power, wireless mesh networking standard. The low cost allows the technology to be widely deployed in wireless control and monitoring applications, the low power-usage allows longer life with smaller batteries, and the mesh networking provides high reliability and larger range. ZigBee has been developed to meet the growing demand for capable wireless networking between numerous low power devices. In industry ZigBee is being used for next generation automated manufacturing, with small Transmitters in every device on the floor, allowing for communication between devices to a central computer. This new level of communication permits finely-tuned remote monitoring and manipulation.

Category	ZigBee	Bluetooth	Wi-Fi
Distance	5-15m	3m	50m
Extension	Automatic	None	Depends on network
Power Supply	Years	Days	Hours
Complicity	Simple	High	Complicated
Frequency Range	868MHz, 916MHz, 2.4GHz	2.4 GHz	2.4GHz
Linking Time	30ms	Up to 10 s	Up to 3s
Prime Cost	Low	Low	Normal
Ease of use	Easy	Normal	Hard

Table1: Comparison among various technologies

ZigBee Device Types:

1) ZigBee coordinator (ZC):

The most capable device, the coordinator forms the root of the network tree and might bridge to other networks. There is exactly one ZigBee coordinator in each network since it is the device that started the network originally. It stores information about the network, including acting as the Trust Centre & repository for security keys.

2) ZigBee Router (ZR):
As well as running an application function, a router can act as an intermediate router, passing on data from other devices.

3) ZigBee End Device (ZED):
Contains just enough functionality to talk to the parent node (either the coordinator or a router); it cannot relay data from other devices. This relationship allows the node to be asleep a significant amount of the time thereby giving long battery life. A ZED requires the least amount of memory, and therefore can be less expensive to manufacture than ZR or ZC.

IV. DESIGN OF SYSTEM

A RS232 communication protocol was used to interface Universal Asynchronous and Receiver and Transmitter in ATmega8 microcontroller and the ZigBee transceiver. The microcontroller-based embedded device along with CC2500 ZigBee transceiver in one module will maintain full duplex communication with another module. CC2500 ZigBee transceiver in both modules provides extensive hardware support for effective RF communication in eight meters of distance.

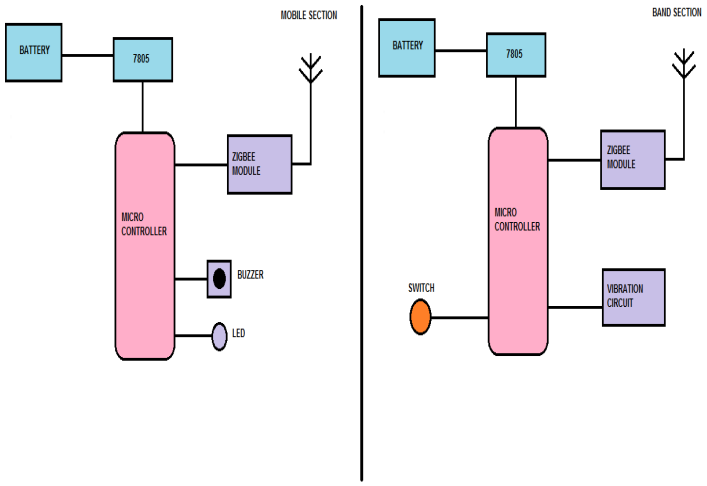

Fig 1: Block Diagram of Anti-theft system using ZigBee Technology

When any of the modules move eight meters away from the fixed location, the communication between two modules will be lost and it generates a buzzer sound and LED blinking at cover end and at band end the vibrations occurs. When the circuitry is in range then there is no functioning, the circuit is in idle state. The Oscillator is connected at XTAL1 and XTAL2. A reset switch RST is used to reset the circuitry. Power supply was made of 9V to 5V using a transformer and diodes. It was consisting of two diodes. Three capacitors of 1000µF, 10µF, 0.01µF respectively and IC 7805 are used as a voltage regulator to covert 9V to 5V.

V. BUILDING THE SYSTEM

In order to meet the project, the system is developed in various phases. In the initial phase, the required system criteria, such as inputs are identified, established and the Power supply was made. The next stage was simulation of circuit. In the next phase, all hardware components are configured for proper operation. The RS232 communication protocol is used to interface microcontroller and the ZigBee transceiver. The CC2500 ZigBee transceiver is configured for obtaining optimum register settings and to meet the design aspects of the

communication channel. CC2500 ZigBee transceiver is interfaced to an ATmega8 microcontroller and this controller is able to:

1. RD/WR buffered data to and from CC2500 ZigBee for lossless communication.
2. Program CC2500 ZigBee in different modes to meet the requirements of the communication channel.

In transmit mode, the circuit gets triggered when the band or the cover moves away from the distance of eight meters. In the final phase, the project of the wireless security system using ZigBee technology is evaluated by three factors in consideration, such as effective distance, time delay, and noise associated with the system. The distance between two modules can be varied depending on the application selected. CC2500 ZigBee transceiver is specifically used for short distance communications at lower power levels in a frequency range of 2.4GHz. By practically testing the system, the buzzer and LED blinking is observed in mobile cover section and vibration on band section when any of the modules is moved eight meters from the fixed location. Some minimum time delay is observed due to the interference of the communication channel between modules.

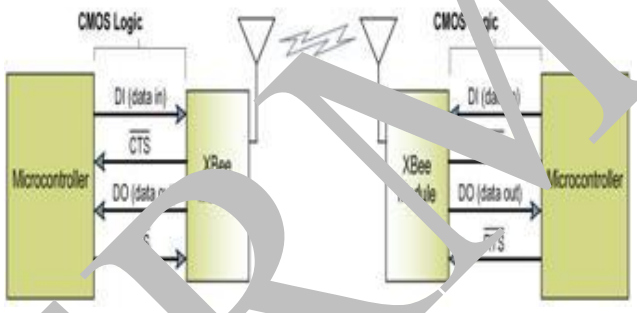

Fig 2: Project Methodology

The initial processing of the system with getting started and initialization of the registers of CC2500 ZigBee requires some time. Noise is tested by placing the modules in a vacuum environment and when the modules are in the external environment. There was more noise effect when modules are tested in external environment.

VI. I MPLEMENTATION OF THE SYSTEM

A ZigBee enabled wireless security system is built around CC2500 ZigBee RF transceiver and an ATmega8 microcontroller. A CC2500 ZigBee transceiver is interfaced to microcontroller using PD0 AND PD1. A RS232 communication protocol is used to interface ATmega8 microcontroller and the CC2500 ZigBee transceiver. In CC2500 ZigBee transceiver, first it is set in TX mode which is initiated in one module and data is transferred completely. After completing data transfer, it is automatically changed to RX. These modules are set to default settings from the factory and can communicate to one another without any configuration. The CC2500 ZigBee transceiver supports up to 250 kilobytes per seconds of data variable packet length mode. Here the channel number is selected as 0 which is a default number in both modules of CC2500 ZigBee transceiver. The CC2500 ZigBee transceiver supports amplitude, frequency and phase shift modulation formats. Frequency shift keying (FSK) modulation is used in both modules with symbol encoding as 0 for negative deviation and 1 for positive deviation. The PD0 and PD1 in ATmega8 microcontroller has a transmitter and receiver which communicate with CC2500 ZigBee transceiver using RS 232 communication protocol by the use of START and STOP pulses. When the power is turned ON, microcontroller initializes the code in flash memory and resets all the registers. The instructed program in ATmega8 microcontroller executes the required function (transmitting and receiving of an ASCII value to ensure communication between the modules) through RS 232 with a baud rate of 250kbps and make communication establishment with CC2500 ZigBee transceiver. The PD0 and PD1 receive the acknowledgement

from CC2500 ZigBee transceiver and update the test flag, which is used to monitor the continuous communication process ensuring security. When there is continuous communication between two modules of CC2500 ZigBee transceiver, the buzzer, LED, Vibrator is in off condition. And when two modules move away eight meters, the communication is lost and this results in a buzzer sound LED Blinking and Vibration at wrist band.

VII. CONCLUSION

An Anti theft security system attached with the phone in consideration was proved to be an efficient way to alert the user in case of theft. The wireless communication between two ZigBee modules is achieved through CC2500 Zig Bee Module and microcontroller ATmega8. The size of the system can be reduced or minimized by decreasing the battery sizes, making it more accessible, secure and compact to install on many portable devices. Hence, it can also be used for protecting other portable devices.

REFERRENCES

1. Su, G., Tan, L., "A Trade off Scheme in Multi-User System with Block Diagonal Geometric Mean Decomposition", The Computing Science and Technology International Journal, Vol. 1, No. 1, pp. 5-14, August, 2011.
2. Li, F., "Opportunistic Relaying in Cooperative OFDM Networks with Limit Feedback", the Computing Science and Technology International Journal, Vol. 1, No. 1, pp. 15-19, December, 2011.
3. ZigBee Alliance, ZigBee Specification. Version 1.0 ZigBee Document 053474r06, December 14th, 2004.
4. William Stalling, ―Wireless Communication and Networks‖, Fourth Edition, Pearson Publication Limited, 2004, Pp 39-118.
5. IEEE 802 Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks, IEEE Computer Society, 2003.
6. Yao, H., "Dynamic Restoration for Survivable Traffic Grooming in WDM Networks", the Computing Science and Technology International Journal, Vol. 1, No. 1, August, 2011.
7. A.M.F. Garcia, A.P. Esteban, "Re using Educational Contents in M-Learning", IEEE International Conference on Advanced Learning Technologies (ICALT), Page(s) 448-449, Year 2011.
8. Ran, P., Sun, M., Zou, Y. (2006). ZigBee routing selection strategy based on data services and energy-balanced ZigBee routing. APSCC '06, December 2006, 400-404.
9. Chen, B., Wu, M., Yao, S., & Binbin, N. (2006). ZigBee technology and its application on wireless meter reading system. Industrial Informatics, 2006 IEEE International Conference on, August 2006, 1257-1260.