International Journal of Advance Research in Science and Engineering
Vol. No.4, Issue 07, July 2015
www.ijarse.com
IJARSE
ISSN 2319 - 8354

AUTHORIZATION DATA TRANSMISSION BASED ON WIRELESS TECHNOLOGY

A. Haimavathi[1], B. Santhosh Kumar[2]

[1] *Pursuing M.Tech, ES, Visvesvaraya College of Engineering and Technology (VCET), M.P.Patelguda, Ibrahimpatnam, RangaReddy, Telangana, (India)*

[2]*Working as Assistant Professor & HOD, ECE Department, Visvesvaraya College of Engineering and Technology (VCET), M.P.Patelguda, Ibrahimpatnam, RangaReddy, Telangana, (India)*

ABSTRACT

In this paper consists of Secure Message Transmission over Wireless Communication technology using ZigBee based wireless data transmission from one person to another person with data security. Here in this system we are using two section ,both section consists of ZigBee module also it works as receiver and transmitter section ,one section of ZigBee module is interfacing to the Personal Computer(PC)/mirocontoller and another section of ZigBee module is interfacing to the ARM LPC2148 micro controller and LCD.A person can communicate with other person securely that is whatever the information sends by person to other location that should not be hacked .So, for security purpose we are using wireless ZigBee communication technology which is data transmission done with securely in a short range of communication

Keywords: Microcontroller, Zig Bee Transceivers

I. INTRODUCTION

Wireless communication systems don't appear to be new, but they have been regularly progressing for several years, especially in the space of mobile communications. First generation mobile systems began to arise within the late 1970s and within the early Eighties. In the early Nineteen Nineties migration to the second generation system started momentum and inside 2 years all of the major European operators had began to operate commercial GSM networks. Throughout the mid-1990s, ground work preparations that will eventually cause the development of third generation systems started and the first business network was launched within the early 2000.

Comparing the evolution ways of the assorted mobile systems it may be found that the trend was migration from ADC, and also process speeds for initial generation systems through to the bit/s rates for third generation systems, with migration to fourth generation evolution ways. For Wi-Fi, the trend was migration from low Mbit/s rates to low 100s of Mbit/s. However, the advances that are created in each mobile and Wi-Fi systems mostly mirrored technological advances that enabled more and more advanced basic wireless communication. Consequently, these improvements area unit, in theory, typically applicable to be used in

any kind of wireless technology. In this paper we planned the system design based on ZigBee technology instead of WIFI.

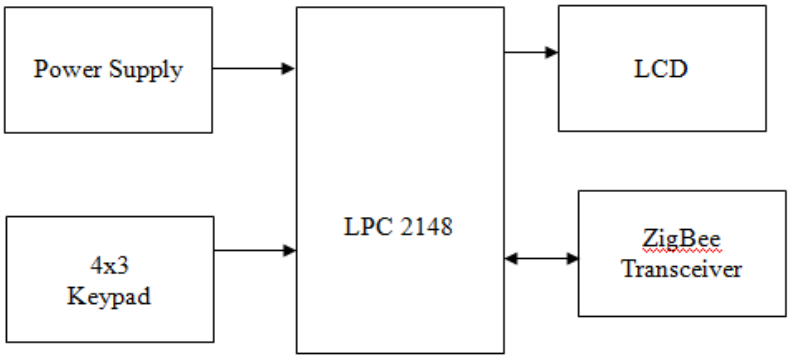
II. PROPOSED SYSTEM

The proposed system of secure message transmission using ZigBee wireless communication an alternative solution for data encryption secured transmission. This system is designed to be used in short range communication applications. The system comprises of a ZigBee transceiver module interfaced with a LPC2148 microcontroller at one end of the communication and it also contains an alphanumeric keypad for giving the text input. The other end of the system will have another ZigBee transceiver and LCD display for displaying the received text information from the source. At the destination side, there will be an alphanumeric keypad for providing the password security for received data.

As discussed in the above sections, the ZigBee is one to multi node communication, while sending the data from the source, any other ZigBee devices operating within in the range and within the frequency band will able to receive the data. The PIN security feature will make it an authentic data exchange.They can be used for both transmission and reception. Then our implemented system will be two way communication method, that both ends of devices can send and receive the data.The two way transmission will make it full duplex communication technique in short range data transfer applications.

2.1 Block Diagram

2.1.1 Transmission Unit



2.1.2 Receiving Unit

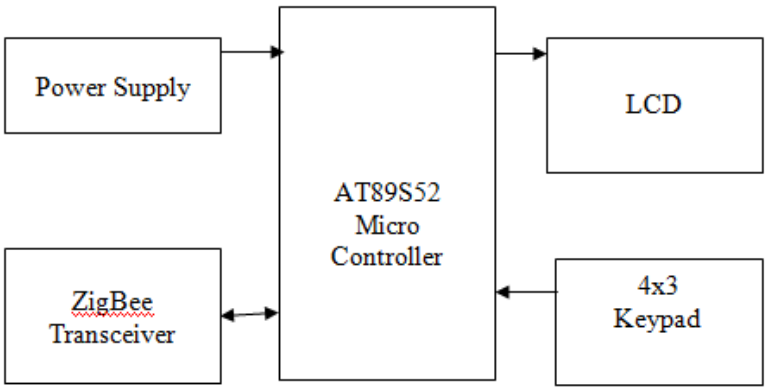


Fig 1 : Block Diagram of Proposed Method

The above figure shows the block diagram of the proposed system. Both the units will consists of a microcontroller each side, ZigBee transceiver and Keypad. Together the elements at dissimilar nodes can transfer the information to controller. While one unit sending the data to the other, it can be displayed on the unit LCD in encrypted form and after entering the correct password by the user at the other end, the original data will be displayed.

In the same way, the other section can also transmit the data to another node. In this, we are using 4x3 keypad to get the alphanumeric data input to the microcontroller.

III. WORKING

The aim of this project is to implement a wireless communication network which would useful for less distance range of data transfer from one node to another node. The communication technology must be always cheaper as this is intended to use in less range of communication and also the data rate is enough faster. The reason behind choosing the ZigBee as communication technology in our system is its unique features such as the ZigBee works on 2.4GHz operating frequency band which is unlicensed and free to use. And there is also flexibility to use the frequency as per the hardware compatibility. The data rates varies from 20Kbps to 250Kbps based on 868MHz and 2.4GHz respectively. ZigBee is a low cost and low power communication technology and the ZigBee devices can communicate in a propagation manner.

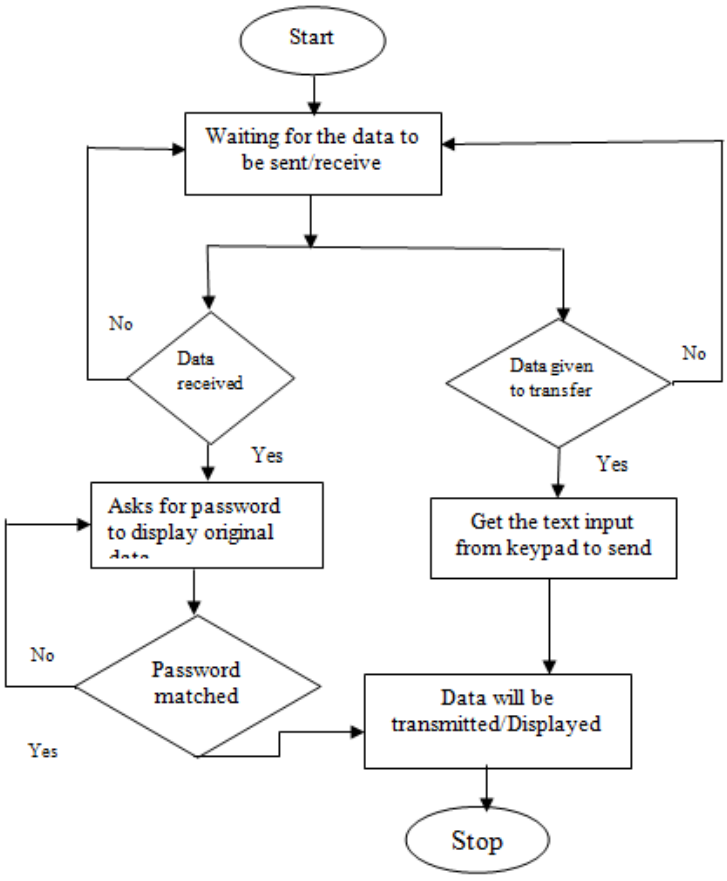


Fig 2 : Flowchart of System Design Model

The project is also aimed to provide a secure data transfer through ZigBee by using a secured password access to view the message. The PINentrance is a straight method but efficient as well as faster to access compared to other security methods. The implemented system is an alternative solution for short range data transfer and which is no cost methodology. The GSM technology ruling the communication world with its powerful short messaging service (SMS) service. But in case of short range data exchange or in case of communication is needed within a building or office, the SMS service will be a wastage of money in the form of call cost to the service providers. Targeting the communication needs of a corporate office, educational institutes, etc. we are implementing the secure message transmission system by using ZigBee, which is no cost communication method

IV. SOFTWARE IMPLEMENTATION

In order to communicate with the hardware we require a predefined software. An embedded system we require both hardware and software, it is mandatory to perform a precise application. The hardware elementsdeterminationpathway according to the instruction given to the program. The software tools should be selected based on micro-controller using in this application. The following some of software tools are used in this project.

1) MDK Keil µVision

2) Flash Magic

4.1 Keil µVision

The Keil µVision is an IDE which will consist of complete programming environment for various micro-controllers. Keil is having a C editor, ANSI C cross compiler. It supports programming for various 8-bit, 16-bit and 32-bit micro-controllers.

4.2 Flash Magic

It is simply a programming dumping software. Micro-controllers can only understand machine language. Whatever we are writing in the program, that we convert into machine level language. That machine level language format of the program, we call it as Hex file. By generating hex file the programmer desires to write the hex file into micro-controller.

V. RESULTS

The output of each and every stage of the fingerprint detection algorithm which has been implemented is shown in Fig 3. LPC2148 through serial communication. Programming the ARM controller is done by FLASH MAGIC. Proteus Professional 8 is also used as simulator on Windows 8. The hex file is also generated using the KEIL MICRO VISION 4 compiler is dumped into the ARM microcontroller by using Flash Magic software and it is then executed. The executed result of the fingerprint match is displayed on the LCD screen all the time. The output of the ARM controller should be connected to the ignition control unit of the vehicle. Fig 3 and Fig 4 shows two possible outputs of the fingerprint matching algorithm implemented using the ARM controller.

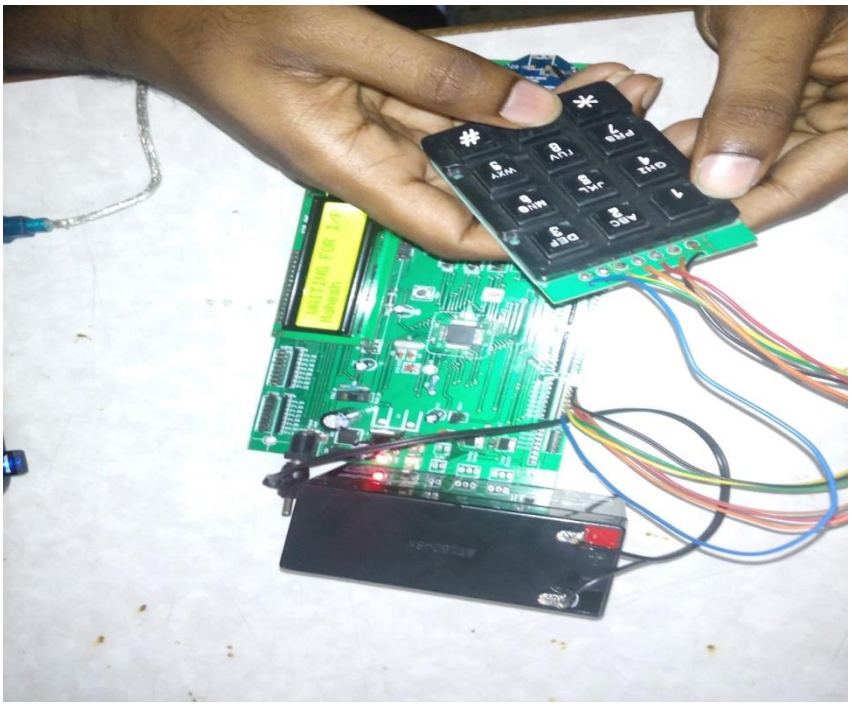


Fig 3: Board step of Design Overview

VI. CONCLUSION

The secure message transmission system through ZigBee is an advanced and solution for short range communication which is a simple alternative for the encryption and decryption techniques. The ZigBee procedure in this method makes it simpler and cheaper for short range data transfer. The security through keypad will provide a simple and secured feature for data security that can make it useful for all types of people .The system can be improved to create it even smarter by using it a touchscreen instead of a keypad for data input and password entering. With the touchscreen, the QWERTY keyboard will be simple to use compared to using a 4x3 keypad for alphanumeric input.

REFERENCES

[1]. ZigBee Alliance, ZigBee Specification. Version 1.0 ZigBee Document 053474r06, December 14th, 2004.

[2]. William Stalling, ―Wireless Communication and Networks‖, Fourth Edition, Pearson Publication Limited, 2004, Pp 39 - 118.

[3]. 802.15.4, Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LRWPANs).

[4]. Sheng-Fu Su, The Design and Implementation of the ZigBee Protocol Driver in Linux, White Paper dated 26 July 2005. Jacob Munk-Stander,Implementing a ZigBee Protocol Stack and Light Sensor in TinyOS,White Paper dated October 2005.

[5]. Freescale Semiconductor, ZigBee Implementer's Guide; Document Number: F8W-2004-0007, May23, 2005

[6]. Weiser, M. (1991). The Computer for the 21st Century. Scientific America, September 1991, 94-104. Journal of Theoretical and Applied Information Technology © 2005 -2009 JATIT

[7]. Pister K. S. J., Kahn J. M., and Boser B. E.(1999). Smart dust: Wireless networks of millimeter-scale sensor nodes. In 1999 UCB Electronics Research Laboratory Research Summary

[8]. 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.

[9]. ZigBee Specification v1.0, ZigBee Alliance, December 14th, 2004. [15] Tanenbaum, A. S., Gamage, C., & Crispo, B.(2006). Taking sensor networks from the lab to the jungle.Computer, 39(8), 98-100.

[10]. Kohvakka, M., Kuorilehto, M., Hännikäinen, M., & Hännikäinen, T. D. (2006). Performance analysis of IEEE 802.15.4 and ZigBee for large-scale wireless sensor network applications.

AUTHOR DETAILS

	**A. HAIMAVATHI**, Pursuing Mtech (ES) from Visvesvaraya College of Engineering and Technology (VCET), M.P.Patelguda, Ibrahimpatnam, RangaReddy, Telangana, INDIA. Her area of interest includes embedded systems interrelated with different types of microcontrollers.
	**B.SANTHOSH KUMAR**,working as Assistant Professor & HOD (ECE Department) from Visvesvaraya College of Engineering and Technology (VCET), M.P.Patelguda,Ibrahimpatna m, RangaReddy. He is pursuing Ph.D in Wireless Communications .He has morethan nine years of Experience in Teaching Field.