Indian Journals of Science and Technology, Vol 9(17), DOI: 10.17485/ijst/2016/v9i17/93110, May 2016
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Secured Data Transfer using ZigBee

A. S. R. Murty[1*], K. Phani Mounika[2], K. Anusha Reddy[2], K. Bhanu Karthik[2]

[1]Department of Mechanical Engineering, KL University, Vaddeswaram, Guntur - 522502, Andhra Pradesh, India; asrmurty42@gmail.com

[2]Department of Electronics and Computer Science Engineering, KL University, Vaddeswaram, Guntur - 522502, Andhra Pradesh, India; mouni3781@gmail.com, anushakarumuri55@gmail.com, kamarajukarthik@gmail.com

Abstract

Background/Objectives: The main objective is to provide security while transmitting any data through a wireless data communication. Here we will be having two sections transmitter section and receiver section. The data we are transmitting is encrypted and send from the transmitter and is decrypted at receiver end. **Methods/Statistical Analysis:** We will be converting the given data into its ASCII values. The transmitter encrypts it and sent it to the receiver; the receiver needs to decrypt the data in order to know what data actually being sent. **Findings:** This system has to provide the exact data and also it should see that security is maintained. **Applications:** It is used in places where security is given higher preference. It is good to be used in banks.

Keywords: Receiver, Security, Transmitter, Zigbee

1. Introduction

The data transmission technologies are not up to the expectations. Despite them the loss of security are noticed frequently. In this work we aim to provide a method for communicating between the transmitter and receiver in which security is provided. Basically there are two ways of communication one is wired other is wireless. Of the two we use wireless communication because it does not require any medium to transmit the data. In wireless communication there many technologies like WI-FI technology, IR technology, RFID technology and ZIGBEE technology. Here we are using ZIGBEE technology in order to transmit the data between the transmitter and receiver in a secured manner. Here in this project we will be having two sections one is the Transmitter Section other is Receiver Section.

2. Techniques Used

2.1 Transmitter

In this section the data that is to be transmitted is entered using a keypad and is sent to a microcontroller. After the data is received based on the program the microcontroller transmits the data to MAX-232. From Figure 1 we are having two modes one is normal mode other is the encrypted mode. In normal mode if the data is transmitted it is sent to everyone who has access to the normal mode but in encrypted mode if the data is sent it is visible to only those who have a decryption on the receiver side remaining all can receive it as an encrypted data they can't know what is actually being transmitted. Here in transmitter section we are having a keypad connected to microcontroller which is used to give the data that is to be transmitted. The

*Author for correspondence

microcontroller receives the data and passes it over the MAX-232 from there it is transmitted to ZIGBEE Module where the data is transmitted. This process continues for every new message we send to it[1].

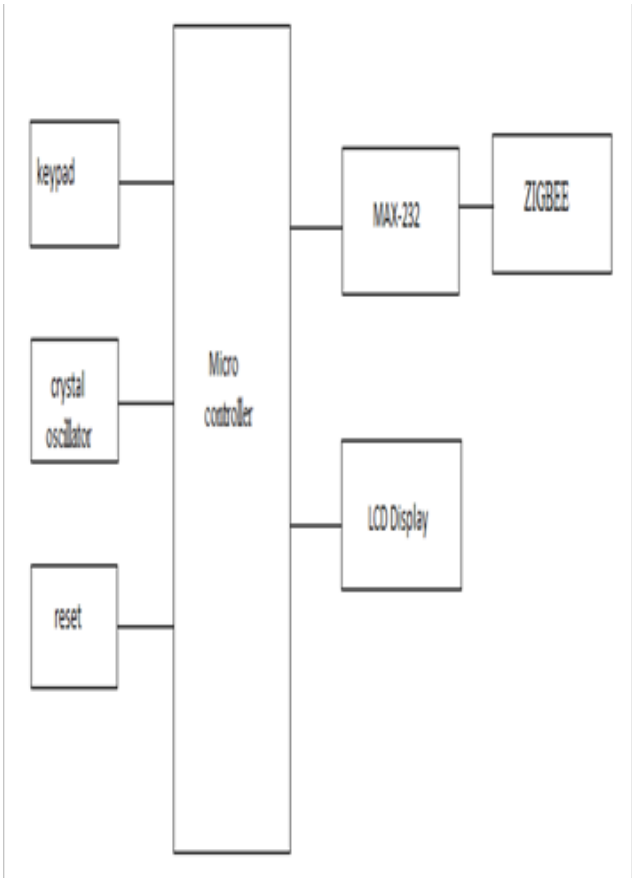

Figure 1. Block diagram of transmitter.

2.2 Receiver

In this section the data that is transmitted by receiver is received by the ZIGBEE and is sent to the MAX-232 which is sent to microcontroller from the microcontroller to the LCD display. From Figure 2 when a data is received a buzzer will be produced in order to indicate us that some data is sent by the transmitter and the receiver has received it. In the receiver section one is normal mode other is the decryption mode. In normal mode only the data that is sent from the transmitter in normal is seen but in decryption mode both the normal data and the data that is encrypted both can be read. So by maintaining normal mode and decrypted mode separately we can maintain security. Only the authorized people who have access to decryption mode are able to know what is actually transmitted.

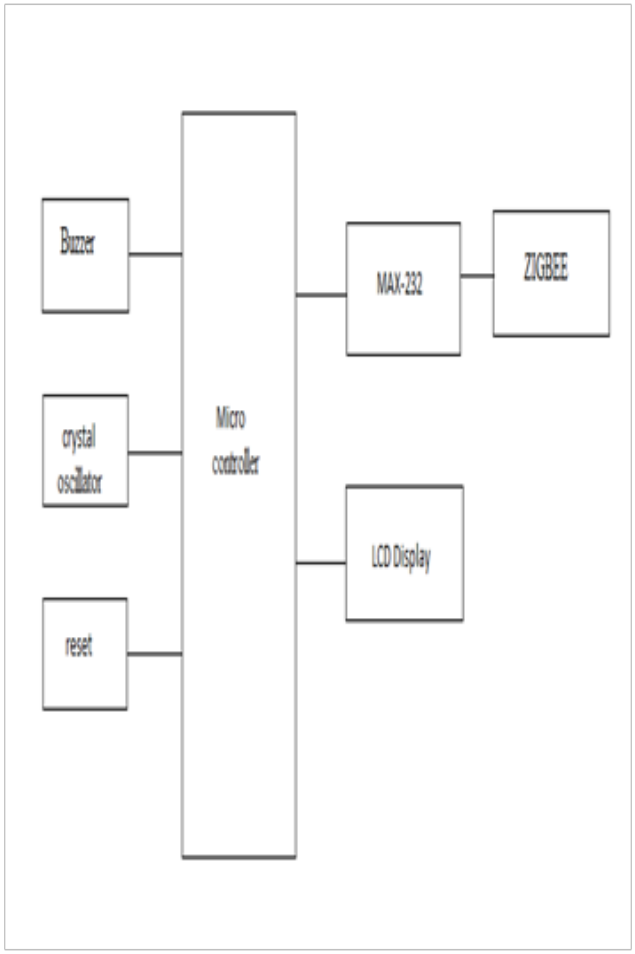

Figure 2. Block diagram of receiver.

2.3 ZigBee

It is a wireless technology which is designed to address the unique needs. ZigBee is easy to operate and it needs less power. ZigBee module as shown in Figure 3. It operates at a radio frequency of 2.4 GHz which is used to deliver data more reliably and these standards are easy to use in entire world. ZigBee devices are the combination of application, ZigBee logical, and ZigBee physical device types[2].

ZigBee is battery operated and its performance is very flexible. ZigBee operates in many ways such as industrial, scientific and medical fields 2.4 GHz and 868/915 MHz dual PHY modes[3] which is operated at a frequency of 868 MHz in Europe and 950 MHz in Australia and U.S.A. There are two types of ZigBee's one is low cost ZigBee and other is high cost ZigBee. Low cost ZigBee's frequency

is limited to very small area where as high cost ZigBee's frequency is extended to large area. These protocols are anticipated for embedded applications that require low power and low cost. ZigBee is used in various applications such as industrial, medical data control etc.

Figure 3. ZeeBe.

The ZigBee Security Services provided within the specification are:

- Key institution.
- Key transport.
- Frame protection.
- Device authorization.

ZigBee introduces the concept of the Trust Center,

- Stores the keys for the network.
- Uses the security services to configure a device with its key(s).
- Uses the security services to authorize a device onto the network.

There are three key types in ZigBee which are established in order to establish security

- Master key.
- Link key.
- Network key.

2.3.1 Link Key

Key which is uniquely shared between two devices for protecting frames at the APS layer. One of these devices is normally the trust center.

2.3.2 Network Layer

It is a global key which is used by all devices in the network. A set of network is held by the trust center. The current network key is identified by key sequence number which is transported by trust center.

2.4 MAX-232

The MAX232 could be a hardware layer protocol device IC factory-made by the Maxim Corporation. Usually called a RS-232 Transceiver, it consists of two driver and two receiver. At a really basic level, the motive force converts TTL and CMOS voltage levels to TIA/EIA-232-E levels, that square measure compatible for interface communications. The receiver performs the reverse conversion.

Used in an embedded microcontroller systems, and computers, this IC has been one among the foremost standard parts in production for overrun 20 years. If you have got a microcontroller circuit that needs communication through a interface, then this is often the chip to use. This is often a flexible IC, that is one among those tremendous parts that solve such a large amount of signal conversion issues. The gate diagram as shown in Figure 4.

3. Existing System

In the present existing system it has only access to the desired one who can see the encrypted data. It does not have any intimation when data is received or after it is received[4]. All the others cannot receive even the normal information. If they need to know what the normal data is sent they need to have a separate device which has access to the normal data sent.

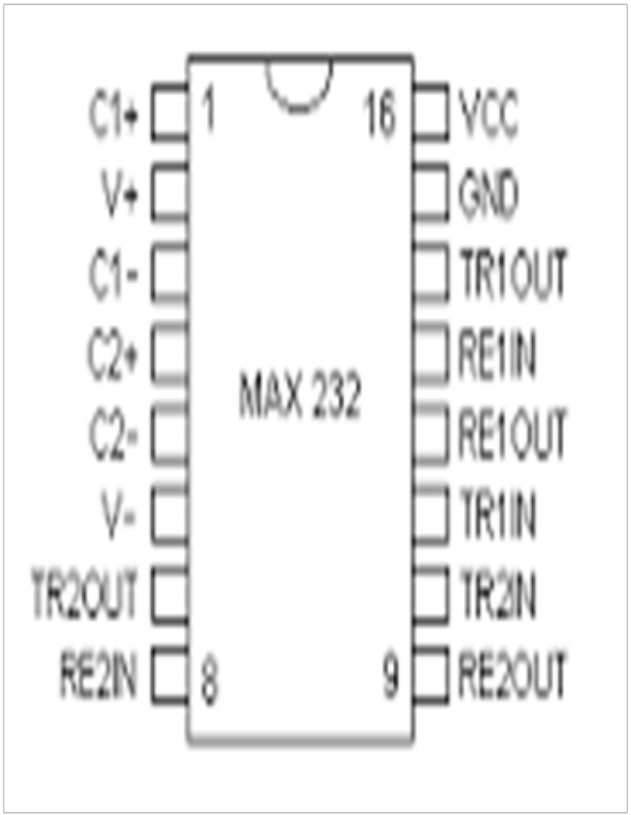

Figure 4. MAX-232.

4. Proposed System

The draw back in the previous system was recovered by our proposed system. The extension that we are doing is adding the alarm when data is received and in existing system only the authorized people are able to receive the data. But in our project all are able to receive the data which is sent in the normal form but only the encrypted data is received by the receiver who has the access to the decryption.

5. System Working

This paper aims in coming up with a portable computer to portable computer data transfer system that's improbably necessary for sharing files pattern ZigBee technology this may be very useful for transfer of data from one portable computer to a distinct portable computer pattern PIC microcontroller. There are two modes in the transmission of data one is normal mode and the other is encrypted mode[5]. When we enter the required data that is to be transmitted it first enters the microcontroller then it goes to the LCD where it is displayed and through MAX-232 it goes to ZigBee where it is encrypted from ZigBee it goes to the receiver ZigBee and then to microcontroller to LCD where the received data is displayed. In normal mode the data entered through the key board will be sent to the ZigBee to all the receivers and all are able to see the actual data that is sent because the normal data sent does not require any special decryption techniques or any passwords to access it. When the data is received we can get an alarm so that we can know that some data has been received by the receiver. In other mode which is encryption mode the data which we need to send is entered using keypad or key board the data is sent in encrypted mode is received by the receiver and it is seen only to the one who has access to the encryption means that it need to have decryption within it whenever the data is received an alarm is blown. All the receivers who does not have access to encrypted mode does not receive the message. Thus security is maintained by providing access only to the desired persons.

6. Output Analysis

The expected output is whenever the transmitter is in normal mode all the receivers receive the actual data we are sending. When the transmitter is in encrypted mode only the receivers who have access to decryption can receive it normal form.

7. Conclusion

The proposal of the project is to provide security to the data which we are sending. Here we are sending data with encryption so that none can see the data except the authorized ones.

8. References

1. Akkula SS, El Taeib T. Wireless data transmission between Pc's using ZigBee technology. JMEST. 2015 Apr; 2(4):1–2.
2. ZigBee alliance specification[z]. Version 1.0; Available from: http://www.ZigBee.org
3. Ahamed RSS. The role of Zigbee technology in future data communication system. Journal of Theoretical and Applied Information Technology. 2005-2009; 129–35.
4. ZigBee. Available from: http://en.wikipedia.org/wiki/ZigBee

5. Krithika N, Seethalakshmi R. Safety scheme for mining industry using zigbeemodule. Indian Journal of Science and Technology. 2014 Aug; 7(8):1222–7.