IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735,
PP 11-13
www.iosrjournals.org

Secure Wireless Communication based on Cryptography using Zigbee

Prof.A.R. Kaushik[1], Khan Shahebaz[2], Suryavanshi Nitin[3],Kajale Gaurav[4]
[1](Asst. Prof, Electronics and Telecommunication, Loknete Gopinathji Munde Institute of Engineering and Research, India)
[2,3](Student, Electronics and Telecommunication, Loknete Gopinathji Munde Institute of Engineering and Research, India)

Abstract: *The role of communication in day to day life is very important .Communication can be of two types which are wireless or wired. Basically wireless communication is mostly preferred over wired .But sometimes we need a secured wireless communication in case of industries, companies etc. This paper helps in enabling the user for transmitting data wirelessly through ZigBee with encrypting data to provide security. In the paper it consists of two sections they are transmitter and receiver .The data can be sent to microcontroller through pc by using software called hyper terminal, this software is used for serial communication. The microcontroller after receiving the data it forwards the data to the ZigBee transmitter which is connected to the microcontroller. The data is encrypted and then transmitted to receiver. ZigBee transceiver does data transmission. Encryption does conversion of plain text to cipher text. Original data is Plain text whereas the modified data by using operations so that only authorized person can decode is called as Cipher text. Decryption does conversion of Cipher text to Plain text. The received data is decrypted and is displayed on pc which requires some password to open the data. So by this the data cannot be hacked and is secured.*
Keywords*: Cryptography, security ,wireless Network, Zigbee S2.*

I. Introduction

Everyone in this world wants to be safe and secure. When it comes to the safety and security of Multinational companies , Military, Army, the situation becomes more complicated. Even a common man puts his maximum efforts to protect his data. One of the popular methods to protect the data in a more secure way is to encrypt the data while sending and when received, decrypt the data to retrieve the original message. Before transmitting the data, the data will be converted into an unreadable form and will be sent. At the receiving end, the reverse of encryption carries on to get back the original message. Thus the data will be protected in every way by following the encryption and decryption standard formats. Wireless makes this project more flexible. Standard algorithms require software to be installed into the system before actually using them and hardwired connections. The hardware connections and cabling can be completely eliminated in this project.

The most efficient and reliable wireless communication is Zigbee. The name ZigBee is said to come from the domestic honeybee which uses a zigzag type of dance to communicate important information to other hive members. This communication dance (the "ZigBee Principle") is what engineers are trying to emulate with this protocol, a bunch of separate and simple organisms that join together to tackle complex tasks. The goal IEEE had when they specified the IEEE 802.15.4 standard was to provide a standard for ultra-low complexity, ultralow cost, ultralow power consumption and low data rate wireless connectivity among inexpensive devices.

II. Problem Statement Of Project

Nowadays confidential data transfer is a crucial task in many multinational companies, military departments, intelligence and surveillance departments, and so on. In such departments and companies lots of efforts are put forth for securing confidential data. Therefore, they need Data encryption and decryption for their applications. An example, which is given below describes data encryption and decryption to secure data using Zigbee wireless communication technology for short and long distances. With help of many encryption and decryption techniques we can achieve the goal of secure communication. So we will implement the idea of cryptography for secure communication. For now we will use transposition or substitution cryptography technique for secure communication. And wireless data reception can be achieved by Zigbee module.

A popular way to protect data is to encrypt the data while sending and decrypt it while receiving to regain the original message. Before transmitting, the data is converted into unreadable format, and then the data is encrypted and decrypted in the receiver end to get the original message. Let us demonstrate the project in brief with the help of a block diagram given below.

III. Proposed Methodology

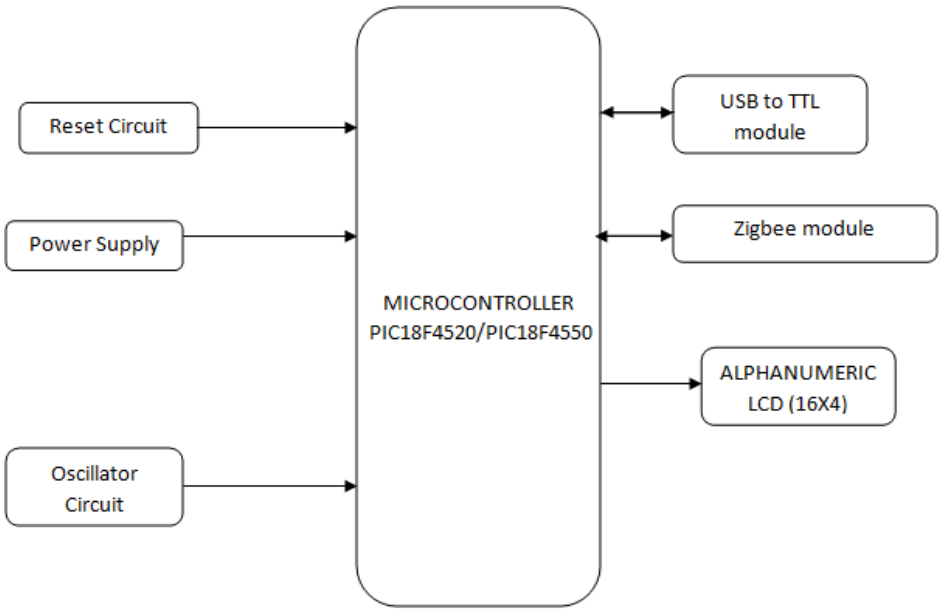

Fig.: *Block diagram of transmitter section*

In a transmitter section, the data to be transferred to a remote location is entered using a keypad, and the data is sent to a microcontroller PI16F877A. The Microcontroller encrypts the data according to the logic implemented in the microcontroller PIC16F877A. Also displays the data on 16x4 LCD display. It displays both encrypted and original message. So the logic of transposition or substitution cryptography does the work of encryption inside microcontroller PIC16F877A. The Crystal circuit plays a key role in the microcontroller operation. This Crystal circuit generates clock pulses so that the internal operation gets synchronized .When the reset pin is high, the microcontroller returns to a power on state, by leaving the currently executing program. RESET operation is performed by holding the RST pin high for at least two machine cycles.

At the receiver end, the Zigbee receiver module receives the data through air and the microcontroller decrypts the encrypted data with the opposite logic to that of the encryption algorithm. Finally the data is converted into the original data so that a user can read it and the decrypted data makes its way to the LCD display to get displayed there. Thus data can be protected at both the ends while transmitting and receiving. LCD display shows both received and decrypted message. Thus we can have the secure communication for many of the private and government firms as only dedicated receiver able to decipher the encrypted message.

IV. Simulation Results

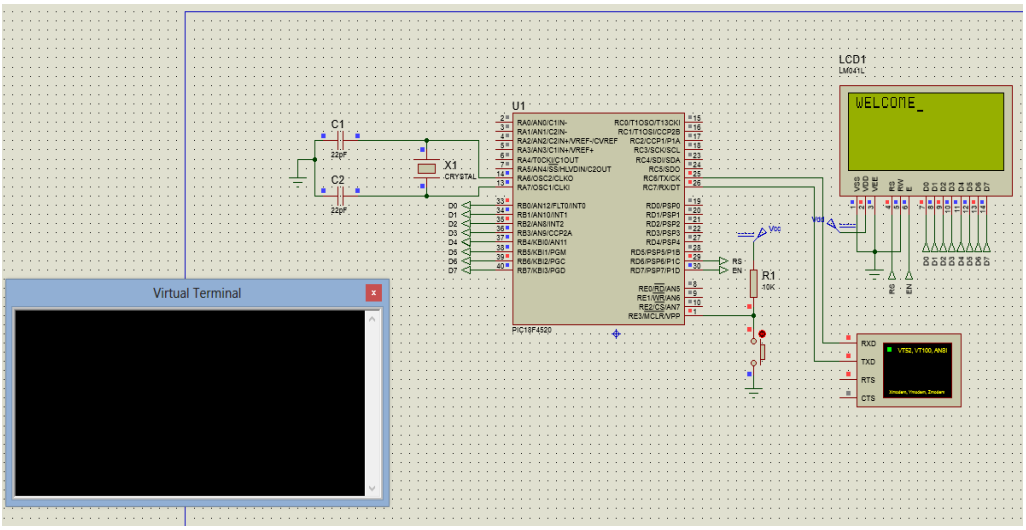

Fig.: *Displaying input string on LCD*

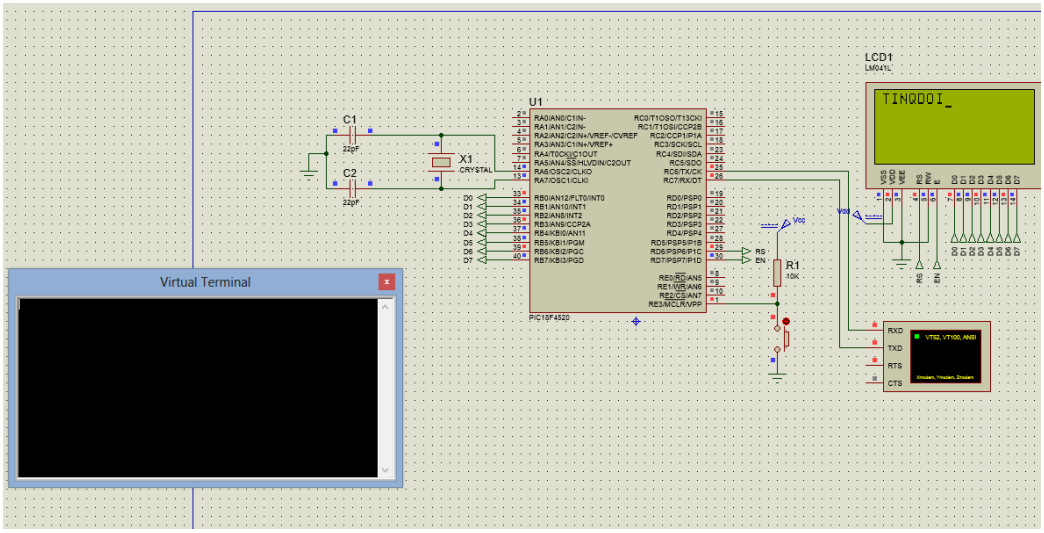

Fig.: *Displaying encrypted string on LCD*

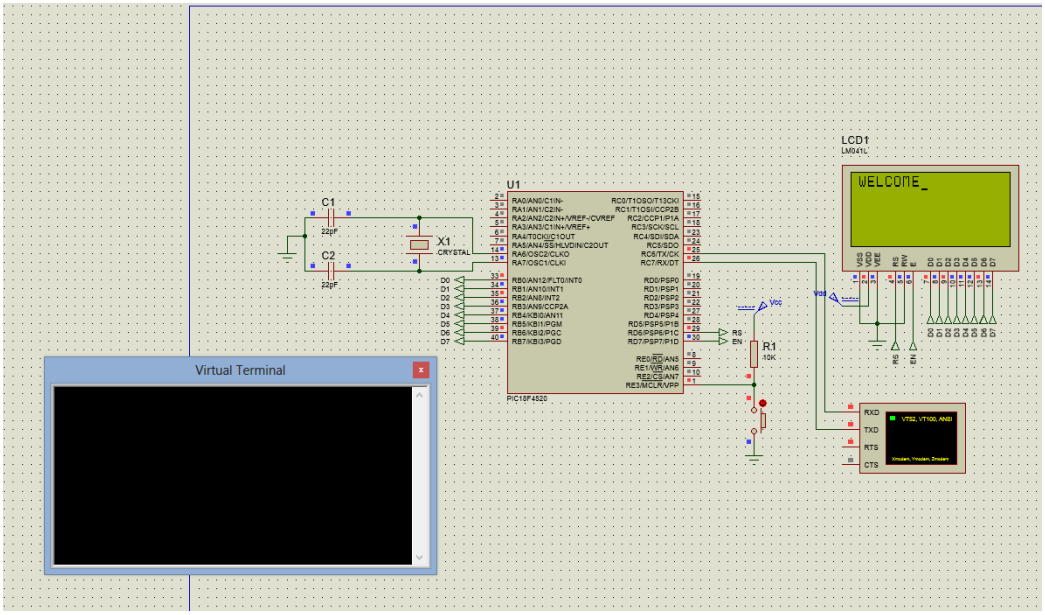

Fig.: *Displaying original string on LCD*

V. Conclusion

Cryptography is powerful and effective for communication of secret data. For the text cryptography various methods have been proposed. In this project, we propose a method that encrypts the secret messages in the text using cryptographic techniques. Cryptography is not only an encryption and decryption technique, but also used for security environment as well. It is provide more security for secret communications over a long and short distance. Thus the capacity of the hiding process to hide secret messages is also high in the proposed theme.

References

[1]. Anupama Mishra, "ENHANCING SECURITY OF CAESAR CIPHER USING DIFFERENT METHODS", International Journal of Research in Engineering and Technology, eISSN: 2319-1163 | pISSN: 2321-7308

[2]. International Journal of Advanced Research in Computer Science and Software Engineering. Volume 2, Issue 10, October 2012 ISSN: 2277 128X "Enhancing Security of Caesar Cipher by Double Columnar Transposition Method", Mr. Vinod Saroha ,Suman Mor, Anurag Dagar

[3]. International Journal of Advanced Research in Computer Science and Software Engineering. Volume 3, Issue 6, June 2013 ISSN: 2277 128X "Enhancing the Security of DES Algorithm Using Transposition Cryptography Techniques", Sombir Singh, Sunil K. Maakar, Dr.Sudesh Kumar.