Wireless Secured Based Communication System

Ayan Pal[1], Ch. Laxman[2], G.Pavan Kumar[3], V.Ratna Kumar[4] , Prasanth Varma[5]
[1234]*UG Student, Hyderabad Institute of Technology and Management*
[5]*Assistant Professor, Hyderabad Institute of Technology and Management*

***Abstract*- The main problem for every communication system is data security. There are numerous methods for communicating security data. But what if security is guaranteed regardless of how far away the hackers are from the noise? One of the most widely used techniques is to encrypt data before sending it and then decode it once it has been received to restore the original contents. A password code is set and sent prior to the data transmission. The reverse of encryption is continued at the receiving end to recover the original communication. Zigbee offers the most effective and trustworthy wireless communication. In this method, data entry is possible by keyboard or computer. The microcontroller at the Zigbee transmitter receives this data next. The data is encrypted by the transmitter before being sent across the air. The Zigbee receiver module at the receiving side receives the data, and by entering the right code, the receiver decrypts the data, converting it into a format that users can read. This data is displayed on the LCD. This way the is secured between the two different paths.**

***Index Terms*—Encryption, Zigbee, Microcontroller, Communication**

I. INTRODUCTION

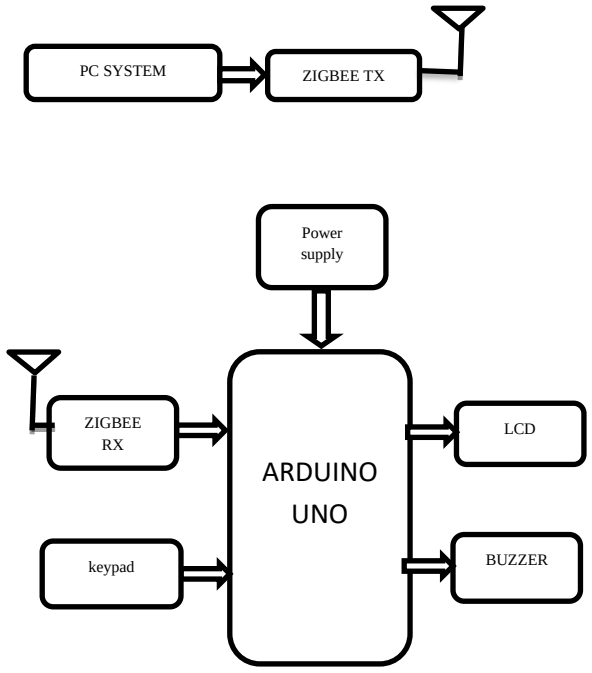
This project's major goal is to generate and transport data in a secure and wireless manner. The problem becomes more complicated when it comes to the safety and security of tasks in many international corporations, the military, and the army. The importance of data security extends to the average person as well. Encrypting data while it is being sent and decrypting it once it has been received are two common techniques for protecting data in a more secure fashion. Using a password code, the data is first transformed into an unreadable format before being transferred. At the receiver end, the data is then retrieved by entering the right password codes in order to make it user-friendly. The most reliable and effective wireless communication in Zigbee.

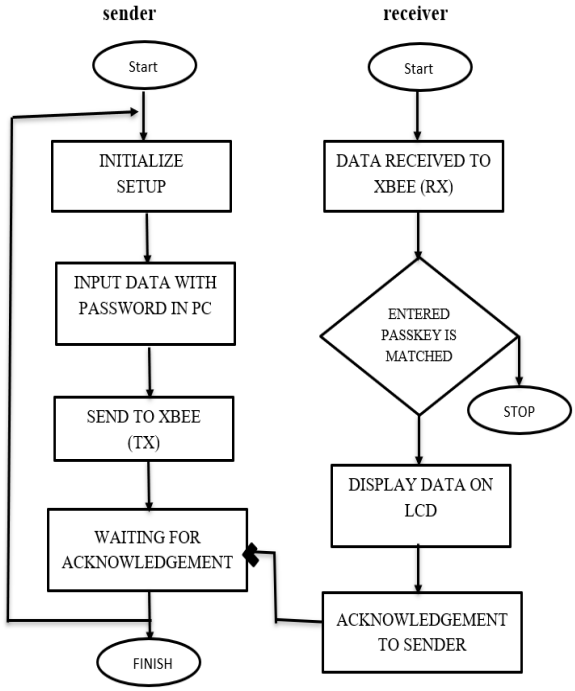
II. LITERATURE REVIEW

An IEEE 802.15.4 standard for data transmission between industrial and consumer electronics is ZigBee. Because of its minimal power requirements, batteries can practically last a lifetime. The IEEE 802.15.4 Medium Access Control (MAC) and Physical Layer (PHY) wireless standard is supported by the network, security, and application support services offered by the ZigBee standard. It makes use of a number of technologies to make networks scalable, self-healing, and capable of managing different data traffic patterns. A low-cost, low-power wireless mesh networking protocol is called ZigBee. The technology can be widely used in wireless control and monitoring applications due to its inexpensive cost, low power consumption, longer battery life with smaller batteries, and mesh networking's great range and reliability. To answer the rising demand for effective wireless networking amongst various low power devices, ZigBee was developed. With tiny transmitters embedded in every piece of equipment on the floor, ZigBee is being utilized in industry for next-generation automated manufacturing to connect gadgets to a central computer. Fine-tuned remote monitoring and manipulation are possible because to this new degree of connectivity.

The network topology discovery algorithm and comprehensive implementation procedure are proposed in this paper. The paper presents a network topology discovery enhancement algorithm in addition to introducing various types of centralized network topology discovery technologies. The authors individually build a software development kit (containing encoding, decoding, network operation, etc.) and employ an asynchronous multi-threaded approach to implement the algorithm. The testing findings demonstrate that the method has clear advantages over commercial software SNMPs in terms of time and flow in the real campus network environment.

III. BLOCK DIAGRAM





IV. WORKING

Through the use of a computer keyboard and RF transmitters, users of our project can convey secret codes to one another. Through an RF receiver, this secret code is received. The remainder of the functionality is carried out at the receiving end, respecting the message's anonymity. The system is intended to be used for sensitive communications in the military, government, or other sectors that require secret code transmissions. The user can use the computer keyboard to type his message. An 8051 microcontroller processes this after which it is wirelessly transmitted to the receiver end. This technique encrypts the transmission with a secret code. An RF transmitter sends the user's message to the receiving end after it has been entered. The RF receiver is integrated with a code and display system at the receiving end. Only if the recipient user inputs the correct code will the message be seen. The sender then receives Acknowledgement.

V. FLOWCHART

VI. ADVANTAGES

1.Rapidity

2.Good Reproducibility

3.High Speed

4.Accuracy

5.Good Repeatability

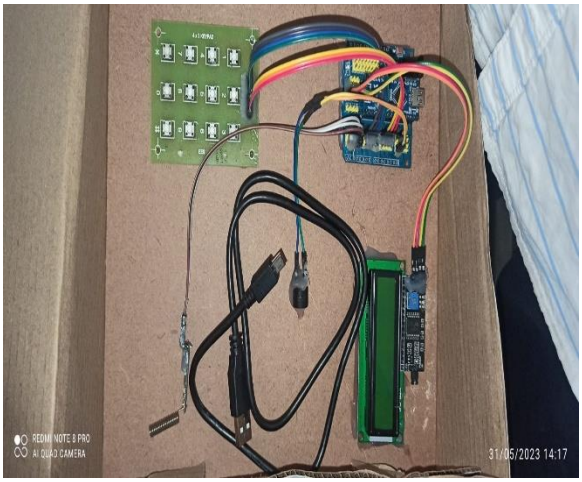
VII. CONCLUSION

Sending hidden data using the process of data encryption and decryption in a connection is very effective. Additionally, it offers a secure method of communicating covert messages across both long and short distances. The proposed work has a very high capability for disguising the material. Compared to Bluetooth and WIFI, ZigBee has a longer lifespan and uses less electricity. Additionally, we can extend the communication range by meshing ZigBee. The project's recommendation is to secure the data we are delivering. Here, data is being sent via encryption so that only those with the proper access can see it.

.

VIII.RESULTS

All the components are connected to each other and the power supply is turned ON.The components are centralised connected to the Arduino. The project is sending secured messages by using an encryption from a matrix keyboard connected to the transmitting unit via Zigbee technology. The message is retrieved at the receiver end only upon entering the secret code used by the transmitter. Thus, complete secrecy is maintained in this communication process. This system has a secret code attached to the transmission. The message typed in by the user is transmitted to the receiving end through Zigbee transmitter. At the receiving end the Zigbee receiver is integrated with a code and display system. User at receiving end can only view the message if he enters the right code and sender receive acknowledgement.



REFERENCES

[1] Hands on Xbee lab manual by Jon Titus.
[2] ZigBee Research Guide.
[3] Dr. S.S Raiz Ahamed, "The role of Zigbee technology in future data communication system", Journal of Theoretical and Applied Information Technology, 2005- 2009.
[4] ZigBee Wireless Networking by Drew Gislason.
[5] International Journal of Advance Engineering and Research Development Volume 5, Issue 04, April -2018
[6] (IJIRSE) International Journal of Innovative Research in Science & Engineering ISSN (Online) 2347-3207
[7] www.google.com
[8] Z.Wang, D.L.Huang, Research on Key Technology of Image Transmission Based on ZigBee, Computer Technology and Development, 2015.05, pp183-186.
[9] W. Z.S, Research on the Network Layer Topology Measurement Based on SNMP, AJETR 2013-02, pp123-126
[10] Xiao Shang Research of AS level Network Topology, AJETR-2015-02,pp 109-123
[11] Pei, Donghui, The Design and Implementation of Serial Monitoring Software Based on ZigBee, ICICEE2012.08, pp236-241
[12] Holman R,Stanley J, O zkan-Haller T. Applying video sensor networks to nearshore environment monitoring[J].IEEE Trans. on Pervasive Computing, 2003, 2(4); 14-21.