IJARST
International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

Secure Zigbee Wireless Communication Using AES Encryption

A L Siridhara[1], Robin Varghese[2],P Sahithi[3],S Naga Pavithra[4],S Jahnavi[5],B Surendra[6]
[1]Professor, Department of Electronics and Communication Engineering, Aditya Engineering College, Surampalem, India
[2-6] U G Students, Department of Electronics and Communication Engineering, Aditya Engineering College, Surampalem, India

Abstract

The present paper describes secure wireless communication utilizing Zigbee technology and AES encryption. By integrating these advanced technologies, the system ensures both the confidentiality and integrity of data exchanged between two systems. Employing 128-bit AES encryption, the communication channel is highly secure, permitting access solely to authorized parties. This communication enables seamless transmission and reception at both ends, facilitated by Atmega microcontrollers interfaced with XBee modules and LCD displays for message and key transmission through visual display. Additionally, USB keyboards, enhance user interaction. Upon system initialization, users can input messages of up to 32 characters, followed by a 16-character key prompt for encryption. The encrypted message is then transmitted to the recipient system, where the Zigbee receiver module decrypts it using the designated code, rendering it readable on the LCD display. This integration of Zigbee technology and AES encryption fortifies data security, offering a robust solution to safeguard wireless communication channels against potential threats.

Keywords — Zigbee, IEEE802.15.4, 128-bit AES, Xbee module, encryption, decryption, security.

Introduction:

In today's interconnected world, ensuring the security and integrity of transmitted data is crucial a cross various sectors, ranging from multinational corporations to military operations, and even for everyday individuals. The proliferation of wireless communication technologies has presented both opportunities and challenges in this regard[1]. Among these technologies, Zigbee stands out for its efficiency, reliability, and low-cost deployment. Zigbee with IEEE 802.15.4 standard, offers a compelling solution. However, with the increasing importance of data security, there arises a pressing need to implement strong encryption methods to safeguard sensitive information during transmission[2]. One such method is the Advanced Encryption Standard (AES) that is established by the U.S. National Institute of Standards and Technology (NIST) renowned for its strength and reliability. By integrating Zigbee with AES encryption, this paper proposes a innovative method to secure wireless communication. This integration aims to address the vulnerabilities inherent in traditional wireless communication technologies while leveraging the benefits of Zigbee's low- cost, low-power consumption. Through the implementation of AES encryption, data can be transmitted wirelessly in a secured manner, ensuring confidentiality, integrity, and authenticity[3]. This paper explores the principles behind Zigbee, AES encryption, and their integration. Additionally, it gives a simple practical implementation of Secure bi- directional wireless communication through Zigbee utilizing AES.

II. SYSTEM ARCHITECTURE

The system architecture block diagrams in Fig.1and Fig.2 illustrates the core components facilitating secure wireless communication[4]. At the earliest the Atmega microcontroller, serving as the central processing unit coordinating data encryption and decryption processes. The Xbee module is a good choice that specifically supports the Zigbee protocol. Integrated effortlessly into the architecture is the Xbee module, responsible for establishing and maintaining the wireless communication link. Complementing these components is the LCD display, providing real-time feedback and interaction with the system's operations. Additionally, manual input interfaces empower users with direct control and configuration capabilities[5,6]. This design architecture ensures robustness, efficiency, and security in Zigbee-based wireless communication, promising are liable frame work for encrypted data transmission.

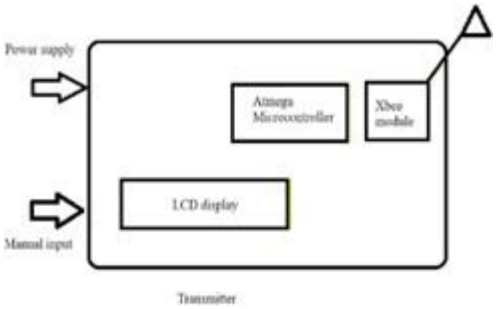

Fig.1. Transmitter side block diagram

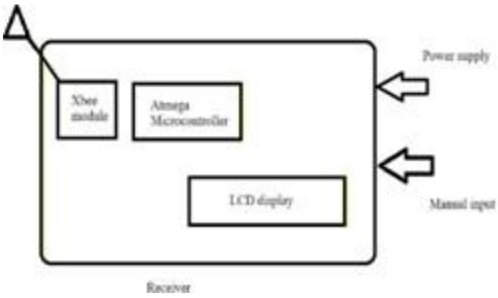

Fig.2. Receiver side block diagram

III. HARDWARE SYSTEM

A. Atmega microcontroller

Using Atmega microcontrollers is really important for making Zigbee-based secure wireless communication with AES encryption. Here the microcontroller can be an Arduino UNO. These microcontrollers are well-known for being flexible and dependable, and they're like the main part of the system, making everything work together smoothly and reliably. Because they're powerful and can connect to lots of other devices, Atmega microcontrollers handle the job of keeping · data safe by encrypting and decrypting it.

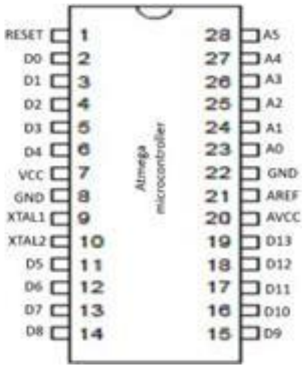

Fig.3.Schematic Diagram of Atmega microcontroller

By using Atmega microcontrollers, this paper suggests a complete plan for setting up safe wireless communication over Zigbee networks, all protected by AES encryption. This use of Atmega microcontrollers makes sure that important information stays private and secure, making the whole communication system strong and trustworthy against any possible risks.

B. Xbee module

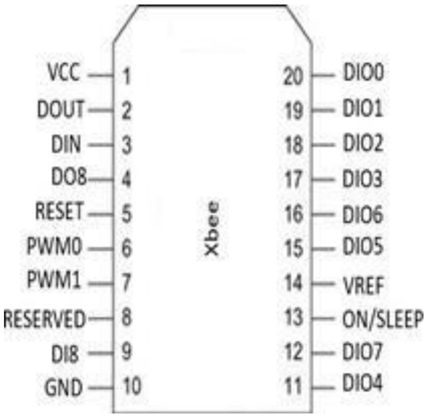

Fig.4. Xbee module schematic

Using XBee modules is really important for making Zigbee-based secure wireless communication with AES encryption. These modules are well-known for being easy to use and working well. They're like essential parts in setting up reliable wireless connections in Zigbee networks. Because they're small and easy to connect, XBee modules fit smoothly into the communication setup, making it quick to get everything up and running. Because they're designed to work with Zigbee and have strong encryption features, Xbee modules make it easy to use AES encryption in Zigbee networks, keeping data safe and secure.

The collaboration of Atmega microcontrollers, XBee modules, and AES encryption is super important. Atmega microcontrollers are like the brain, controlling how everything works. They make sure data is kept safe by encrypting and decrypting it. Meanwhile, XBee modules act like bridges between devices, making it easy for them to connect in the Zigbee network. They're simple to use and work well with Zigbee, making setup quick and easy. XBee modules also help send encrypted data securely using AES encryption. Together, these parts make a strong system for safe wireless communication over Zigbee networks. Here, the manual input can be given using a keyboard.

IV. Software Design

The communication process begins with the manual input of an AES encryption key, which is used to encrypt the message using the AES algorithm during the transmission phase. The encrypted data is then transmitted via the Xbee module, ensuring secure wireless communication. Upon reception, the system checks if the decryption key matches the encryption key. If the keys match, indicating a successful decryption, the received data is decrypted using the AES algorithm, revealing the exact message. This decrypted message is then displayed on an LCD screen. However, if the keys do not match, indicating an unauthorized attempt to access the message, the received data remains as garbage value, ensuring data security and integrity throughout the communication process. This robust encryption and decryption mechanism, coupled with secure transmission and stringent key verification, ensures confidentiality and reliability in data exchange.

The implementation of AES (Advanced Encryption Standard) as a fundamental component with insecure communication systems, particularly those reliant on Zigbee-based wireless networks. Operating on fixed-size data blocks, typically 128bits,AES utilizes asymmetric encryption approach, employing a cipher key for both encryption and decryption operations. The software architecture includes algorithms for AES encryption and decryption, incorporating a series of substitution, permutation and linear transformations known as rounds to achieve cryptographic objectives. The AES implementation provides flexibility in key length, with options including128, 192 and 256 bits, each offering different levels of security. Here we use 128 bits. During encryption, the software executes a sequence of substitution and permutation operations on input data, iteratively blending it with the cipher key over multiple rounds. This complex process ensures that the original data is effectively concealed, yielding cipher text that appears randomized and indecipherable without the corresponding decryption key. Subsequently, AES decryption with in the software reverses the encryption sequence, utilizing the same cipher key to rest ore the cipher text to its initial plain text form. By integrating AES encryption into the software design, Zigbee networks can uphold data confidentiality and integrity, thus safeguarding sensitive information against unauthorized access or tampering during transmission.

The proposed communication system utilizing AES encryption offers an effective and reliable solution for transmitting sensitive data securely. By leveraging Zigbee's low-power, long-life characteristics and AES encryption's robust security features, the system ensures that only authorized parties can access and interpret transmitted data. This paper contributes to enhancing data security in wireless communication systems, ensuring confidentiality and integrity during data transmission.

V. Software Design

The communication process begins with the manual input of an AES encryption key, which is used to encrypt the message using the AES algorithm during the transmission phase. The encrypted data is then transmitted via the Xbee module, ensuring secure wireless communication. Upon reception, the system checks if the decryption key matches the encryption key. If the keys match, indicating a successful decryption, the received data is decrypted using the AES algorithm, revealing the exact message. This decrypted message is then displayed on an LCD screen. However, if the keys do not match, indicating an unauthorized attempt to access the message, the received data remains as garbage value, ensuring data security and integrity throughout the communication process. This robust encryption and decryption mechanism, coupled with secure transmission and stringent key verification, ensures confidentiality and reliability in data exchange.

The implementation of AES (Advanced Encryption Standard) as a fundamental component with insecure communication systems, particularly those reliant on Zigbee- based wireless networks. Operating on fixed-size data blocks, typically 128bits,AES utilizes asymmetric encryption approach, employing a cipher key for both encryption and decryption operations. The software architecture includes algorithms for AES encryption and decryption, incorporating a series of substitution, permutation and linear transformations[7-9] known as rounds to achieve cryptographic objectives. The AES implementation provides flexibility in key length, with options including128, 192 and 256 bits, each offering different levels of security. Here we use 128 bits. During encryption, the software executes a sequence of substitution and permutation operations on input data, iteratively blending it with the cipher key over multiple rounds. This complex process ensures that the original data is effectively concealed, yielding cipher text that appears randomized and indecipherable without the corresponding decryption key.

Subsequently, AES decryption with in the software reverses the encryption sequence, utilizing the same cipher key to rest ore the cipher text to its initial plain text form. By integrating AES encryption into the software design, Zigbee networks can uphold data confidentiality and integrity, thus safeguarding sensitive information against unauthorized access or tampering during transmission.

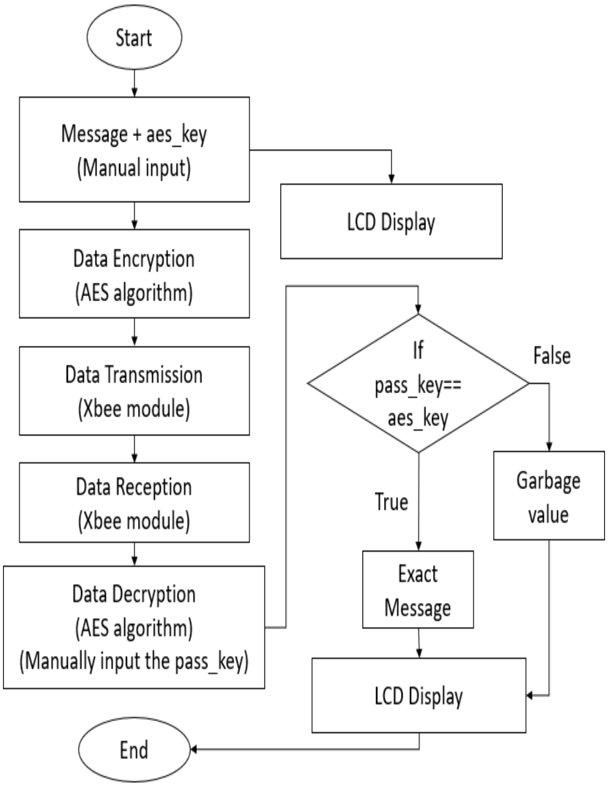

Fig.5.Flow chart of designed system

V. Conclusion

The proposed communication system utilizing AES encryption offers an effective and reliable solution for transmitting sensitive data securely. By leveraging Zigbee's low-power, long-life characteristics and AES encryption's robust security features, the system ensures that only authorized parties can access and interpret transmitted data. This paper contributes to enhancing data security in wireless communication systems, ensuring confidentiality and integrity during data transmission.

VI. References

[1] ZigBee Alliance , ZigBee Specifications (ZigBee Document053474r17). ZigBee Alliance, January 2008.

[2] J. Vinoth Kumar, N. Gowtham, G. Sonika, K. Ramya Sri, “ZIGBEE Based Secured Data Transmission and Reception”, Vol (2), Issue(3),2021.

[3]V Romashchenko, M Brutscheck, I Chmielewski ,“Investigation and Implementation of Robust Wireless Zigbee”, 29th Irish Signals and Systems Conference (ISSC), 2018.

[4]C Li, D Nina, “The Home Security System Based on ZigBee Technology”, 6th International Conference on WirelessCommunications,2010.

[5]A.U. Schmidt et al. (Eds.), “AES Data Encryption in a ZigBee Network: Software or Hardware”, MobiSec 2010, LNICST 47, pp.163–173,2010.

[6]B Yang, “Study on Security of Wireless Sensor Network Based on ZigBee Standard”, International conference on computationalintelligence,2009.

[7] Siridhara, A.L., Ratnam, D.V. Mitigation of Multipath Effects Based on a Robust Fractional Order Bidirectional Least Mean Square (FOBLMS) Beamforming Algorithm for GPS Receivers (2020) Wireless Personal Communications,112 (2), pp. 743-761. 2-s2.0-85078944515

[8] Siridhara, A.L., Ratnam, D.V. Multipath mitigation in GPS receiver using Taylor integrated bidirectional least mean square algorithm (2019) Transactions on Emerging Telecommunications Technologies, 30 (12), art. no. e3760,

[9] Siridhara, A.L., Reddy, M.S. Study of typical signal in a Global Positioning System's receiver (2018) Journal of Engineering and Applied Sciences, 13 (6), pp. 1523-1525.