IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Secured Wireless Communication System Using Standard Symmetric Encryption Algorithm

[1]Ogbuokebe S. K., [2]Amibor I. Patricia, [3]Linda O. Adesina, [4]Alao O. J.

[1,2,3] Center for Satellite Technology Development (CSTD), National Space Research & Development Agency (NASRDA), Airport Road, Abuja, Nigeria.

ABSTRACT

As security is the most important aspect of day to day life, this paper presents a secured data transmission technology by using a half-duplex HC-12 transceiver module. This technology was used to generate and transmit text message. The advantage of this proposed technology is its long distance communication range. Also, unlike the mobile network which requires "pay as you go", this technology can be used for personal communication system in which information can be sent without any cost. More so, the message (data) is secured as it is encrypted at the transmitter side. In order to decrypt the message at the receiving side, standard algorithm such as Advanced Encryption Standard (AES) was employed. AES is a symmetric algorithm that requires only one encryption and decryption key. The implemented technology is a two-way communication system in which the user can transmit and also receive text information. Based on the result obtained, it was observed that the text message (data) was transmitted securely within a short time. By comparing the transmitting and receiving time for 8-bit and 16-bit messages for different distances, the proposed AES algorithm took 2 seconds to transmit 8-bit and 16-bit messages for 100m and 200m distances while 5 seconds was taken to transmit 16-bit messages over a distance of 400m.

Keywords: HC-12 transceiver module, Wireless communication module, communication, AES, symmetric algorithm, encryption and decryption key, 8-bit and 16-bit, message.

1. INTRODUCTION

Exchange of information has become a very important part of human life as it has become inevitable in day to day activities. With the arrival of technology, exchange of information is becoming easier and very much effective. Therefore, with just a click of button on phones, laptops and other communication devices, information can be sent, processed and received within a short time at any destination situated at some distance where there is network coverage. With increasing usage of these telecommunication systems and growth in internet technologies, there is increase in criminal activities such as cyber thieves and hackers gaining access to vital data of their victims. They sometimes use the same data to steal from them, impersonate them or for terrorism purposes. This is possible when the data transmitted are unsecured, and since the wireless network channel is the most widely used today, it is more exposed to cybercrimes. When the sender transmits the message (data) via a wireless network without securing them, there is possibility of hackers intercepting the transmitted data and use them for illegitimate purposes, and the receiver gets an adulterated message. Hence, there is need for securing sensitive data [1] in such a way that they will appear meaningless or senseless to unauthorized users they are not intended for. In order to ensure that the

transmitted data is secured, data is encrypted into formats that are seemingly corrupted or unreadable to unauthorized persons; this process is called cryptography [2]. Several encryption key managements have been developed but up till now, final solution has not been provided [3].

2. SYSTEM COMPONENTS

2.1. HC-12 Transceiver Module

The HC-12 is a half-duplex wireless serial communication module with frequency bands ranging from 433.4 MHz to 473.0 MHz. Its dimension is 27.8mm × 14.4mm × 4mm (including antenna cap, excluding spring antenna). It has a total of 100 channels with a step of 400 KHz between each channel. Transmitting power is from -1dBm (0.79mW) to 20dBm (100mW) and receiving sensitivity is from -117dBm (0.019pW) to -100dBm (10pW) at baud rate of 5,000bps in the air. HC-12 transceiver module is capable of transmitting up to 1 km in open space [6]. As shown in Figure 1, the HC-12 module has a microcontroller which actually doesn't have to be programmed by the user.

Figure 1: HC-12 Transceiver Module

In order to configure the HC-12 module, we simply use AT commands, which can be sent from an Arduino, a PC, or any other microcontroller using the serial port. The "Set" pin of the module is set to a low logic level so as to put the module in the AT command mode. The possible product applications of the HC-12 transceiver module are wireless sensor, community building security, robot wireless control, industrial remote control and telemetering, automatic data acquisition, container information management, POS system, wireless acquisition of gas meter data, vehicle keyless entry system, PC wireless networking, etc.

2.2. Cryptography

In order to achieve the goal of this research, cryptographic protection of message information was chosen. Cryptography is a method of securing information and communications via the use of codes so that the information can reach an authorized person only. Hence, unauthorized person access to the transmitted information can be prevented. In cryptographic protection of data, the technique employed to protect data information was derived from algorithm, which encrypted the messages into formats that are seemingly unreadable or corrupted to unauthorized people and unable to decode it. This algorithm is usually employed for cryptographic key generation, to protect confidential transactions such as credit card and debit card transactions, verification to protect data privacy, web browsing on internet, and digital signing [7].

2.3 Arduino IDE Software

The Arduino Software (IDE) is a cross-platform application (for Windows, macOS, and Linux), which makes it easy to write code (in functions from C and C++) and upload it to board offline. It can be used with poor or no internet connection. This software can be used with any Arduino board. It is used to write and upload programs to Arduino compatible boards, but also, with the help of 3rd party cores, other vendor development boards. The Arduino IDE supports C and C++ languages with special rules of code structuring [9]. Arduino Software IDE connects to the Arduino boards to upload programs and communicate with them. Programs written using Arduino Software (IDE) are called sketches. These sketches are written in the text editor and are saved with the file extension '.ino.'

2.4 ATmega328 Microcontroller

The ATmega328 is a high-performance Microchip 8-bit AVR® RISC-based microcontroller, which combines 32 KB ISP Flash memory with read-while-write capabilities, 1 KB EEPROM, 2 KB SRAM, 23 general purpose I/O lines, 32 general purpose working registers, three flexible timer/counters with compare modes, internal and external interrupts, serial programmable USART, a byte-oriented Two-Wire serial interface, SPI serial port, 6-channel 10-bit A/D converter (8-channels in TQFP and QFN/MLF packages), 14 digital input/output pins, programmable watchdog timer with internal oscillator, and five software selectable power saving modes, 16 MHz ceramic resonator. The device operates between 1.8 - 5.5 volts. By executing powerful instructions in a single clock cycle, the device achieves throughputs approaching one MIPS per MHz, balancing power consumption and processing speed [5].

2.5 Arduino Uno Board

Arduino Uno board is a microcontroller board based on the ATmega328P (datasheet). It has 14 digital input/output pins, 6-analog inputs, a 16 MHz ceramic resonator (CSTCE16M0V53-R0), a USB connection, a power jack, an ICSP header and a reset button. It contains everything needed to support the microcontroller. The board can be powered by simply connecting it to a computer with a USB cable or power it with an AC-to-DC adapter or battery to get started [8].

3. METHODOLOGY

The aim of this research is to transmit data through a wireless communication system in a secured way. Unlike in the mobile network, this device does not require the user to pay for the transmitted message. The device could be use as personal communication system and information can be transmitted at free of cost. In addition, the data sending is secured as it is encrypted at the sender side. AES algorithm was employed for both encryption and decryption purposes [4]. This algorithm was derived from the mathematical concepts to protect the messages in such a way that it will appear senseless or meaningless to unauthorized to decode it. HC-12 transceiver module was implemented as a two-way communication system was for sending and receiving the data. This enables the data transmission over a long distance.

The transmitted information from the sender is encrypted with the algorithm to generate an encrypted key (known as cipher text). This cipher text is channeled to HC-12 wireless communication module, which was then transmitted wirelessly to the receiving HC-12 module. In order to visualize the transmitted and received data, the information being transmitted was composed on the Arduino serial monitor at the transmitting end and at the same time displayed on the Arduino serial monitor at the receiving side. The transmitted data will be like a 16-bit for the proposed AES algorithm. This technology could also be used for applications such as security gadget, library management, automated parking, IoT devices, etc.

Here, the transmission distance was limited to 400m. 8-bit and 16-bit messages were sent through HC-12 transceiver module by considering 100m, 200m, and 400m distances. High power transmitter like nRFL01+ transceiver module, LoRa transceiver modules can be used to achieve long distance communication with this technology.

3.1 Proposed Algorithm

There is need for more security as the universe is becoming increasingly digital. That's why cryptography and its applications to cybersecurity becomes important. Advanced Encryption Standard (AES) algorithm has become more popular and widely adopted symmetric encryption algorithm because it is faster. In addition, it requires only one encryption and decryption key, easier to implement, the software is implemented in C and Java languages, and also provides full specification and design details. The flowchart of the proposed AES algorithm is presented in Figure 2.

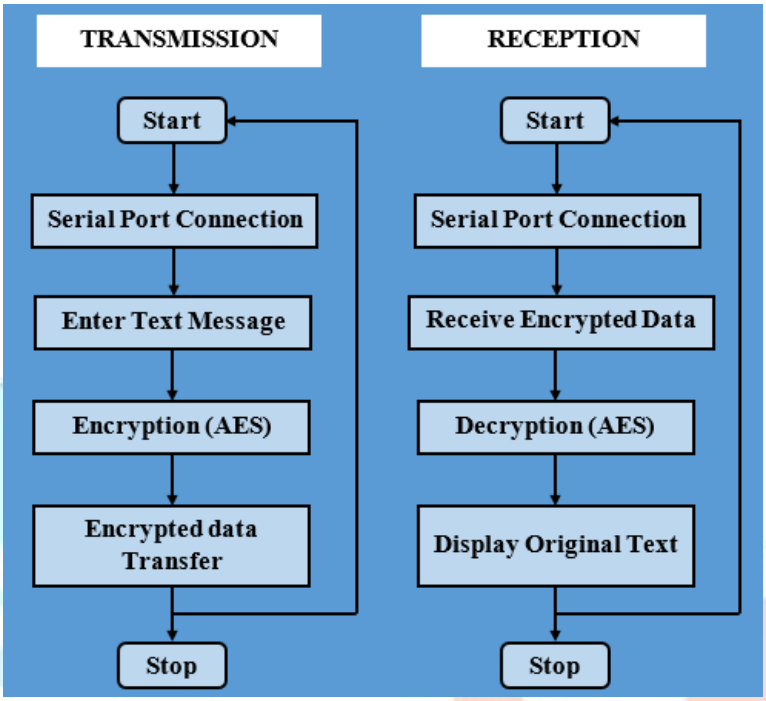

Figure 2: Flowchart of the Proposed AES Algorithm.

3.2 System Design and Implementation

As shown in the block diagram of Figure 3, the first HC-12 transceiver module was connected to an ATmega328 via an Arduino UNO board and the second HC-12 module was then connected to an another ATmega328 via an Arduino Uno. The setup of schematic diagram is presented in Figure 4. The supply voltage was 5V as the operating voltage of the HC-12 module is 3.2 V to 5.5 V. The same code was uploaded on both Arduino boards as the implemented system was a two-way communication. Arduino IDE was used to write the code and upload it on the ATmega328 on the Arduino board. Arduino serial monitor was used for visualizing the transmitting and receiving encrypted text messages.

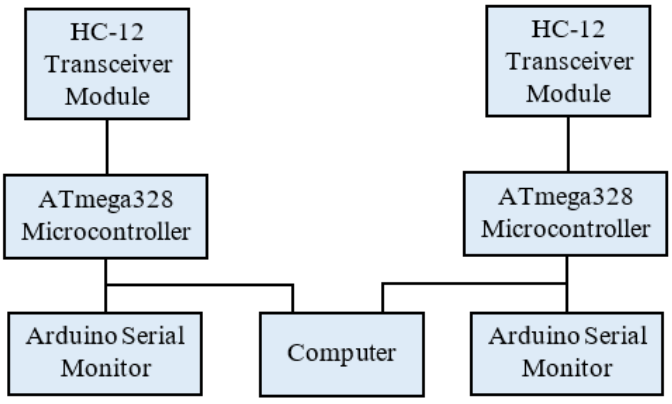

Figure 3: Block Diagram of the Proposed System

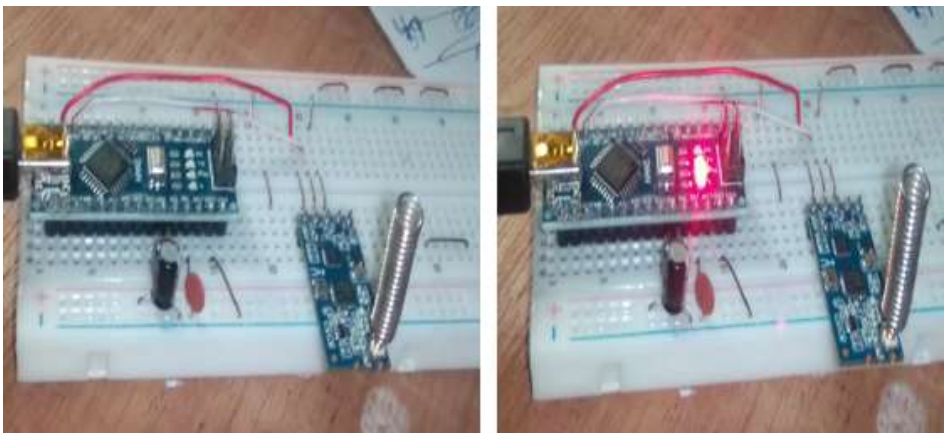

Figure 4: Bread boarding of the Proposed System

4. RESULTS

4.1 Transmitter Side

Here, 8-bit and 16-bit messages were used to characterize the performance of the proposed algorithm as well as the developed sender and receiver system. Each of the 8-bit and 16-bit message to be sent was entered on the Arduino IDE Serial monitor. The original message was entered at the transmitter end while the AES algorithm was used to encrypt the message into a format that the attackers will not be able to understand the original message. After the message was encrypted, the encrypted message was displayed on the serial monitor as shown in Figure 5 and then sent to receiver via HC-12 transceiver module.

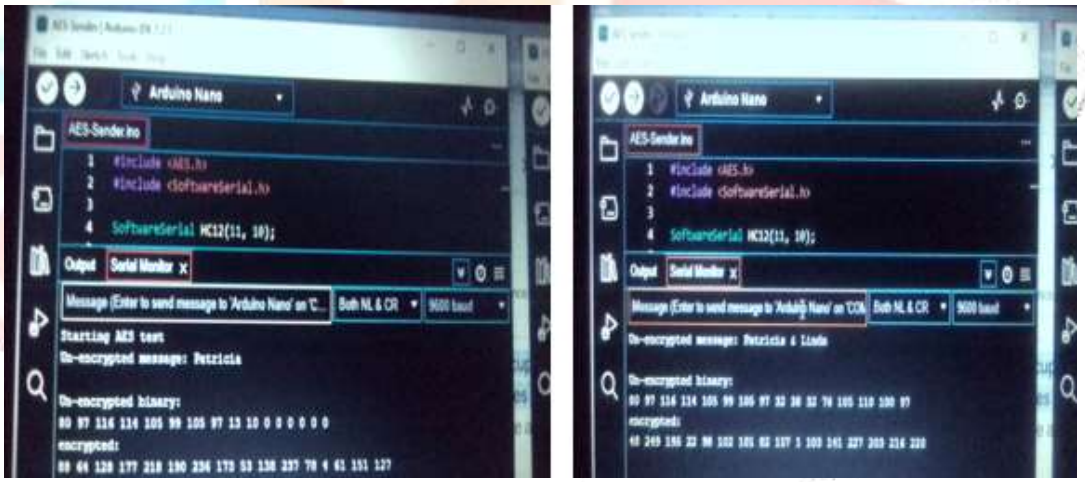

Figure 5: 8-bit and 16-bit Message Sent from Sender to Receiver

4.2 Receiver Side

As shown in the receiver side of Figure 6, the encrypted message sent by the transmitter was received, decrypted by using AES algorithm and the original 8-bit and 16-bit message was displayed on the Arduino serial monitor.

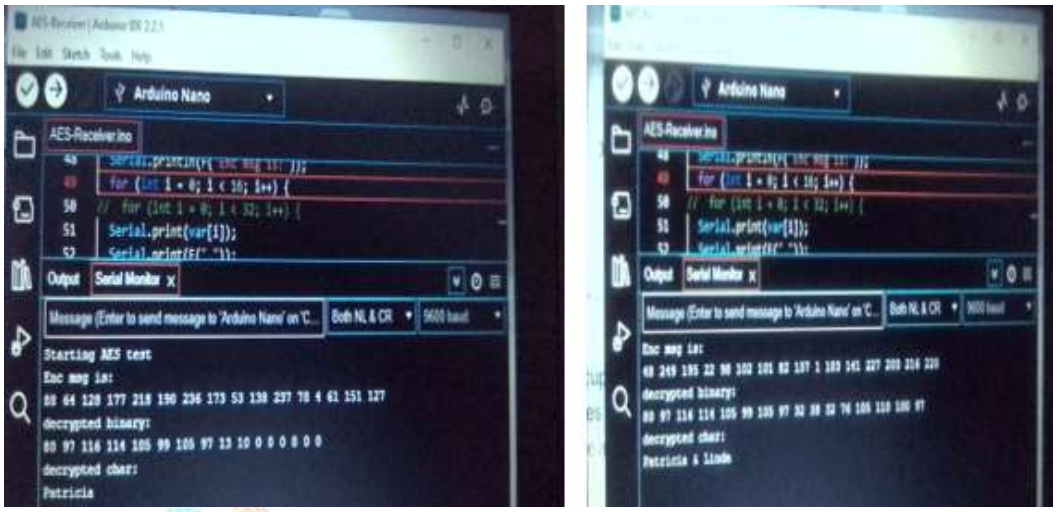

Figure 6: 8-bit and 16-bit Message Received from Sender

4.3 Performance Analysis of AES

In order to achieve the goal of this research, AES algorithm has been employed to ensure that secured data was transmitted within short time. Comparative analysis of various parameters (such as number of characters, distance and time taken to send message from the sender to the receiver) was carried out. The duration for sending the data between the transmitter and receiver when varying the distance for different number of the characters is presented in table 1.

Table 1: AES Algorithm Analysis

S/N	Distance (m)	Number of Characters in Bits	Message Sent	Duration (secs)
1	100	8	Patricia	2
2	200	8	Patricia	2
3	400	8	Patricia	2
4	100	16	Patricia & Linda	2
5	200	16	Patricia & Linda	2
6	400	16	Patricia & Linda	5

5. CONCLUSION

Cryptographic application using the proposed Advanced Encryption Algorithm (AES) has been developed with HC-12, a half-duplex wireless serial communication module. The method adopted ensured that the data was transmitted in a secured manner and in the least amount of time. Detailed comparative analysis with respect to various parameters (such as distance, number of characters, and time taken to send messages from the sender to the receiver) were considered. With respect to the computation time, it was observed that AES is fast by taking an average of 2 seconds to transmit 8-bit and 16-bit messages to the receiver over 100m and 200m distance while 5 seconds was taken for 16-bit message over a distance of 400m. The developed system operation was quite simple and was designed to be user friendly. Based on the performance of the proposed AES algorithm, an authorized user can able to send and receive the message without security issue. The implemented two-way communication system will restrict unauthorized access to the messages that is

sending between two nodes. Therefore, government and security sectors can adopt this system to communicate between their employees. Agricultural sectors can as well make use of this research to keep relationship with their buyers.

REFERENCES

[1] Nian Liu, Jinshan Chen, Lin Zhu, Jianhua Zhang, Yanling He, A Key Management Scheme for Secure Communications of Advanced Metering Infrastructure in Smart Grid, J. IEEE Trans. on Industrial Electronics, vol. 60, no. 10 (Oct. 2013) pp. 4746-4756.
[2] Liddell HG, Scott R, Jones H, McKenzie R (1984) A Greek-English Lexicon. Oxford University Press.
[3] S. Fuloria, R. Anderson, F. Alvarez, K. McGrath, Key management for substations: Symmetric keys, public keys or no keys?, J. IEEE/PES Power Systems Conference and Exposition (PSCE) (20-23 March 2011) pp. 1-6.
[4] Hierarchical Key Management for Smart Grids.
[5] https://www.microchip.com/en-us/product/atmega328
[6] https://howtomechatronics.com/tutorials/arduino/arduino-and-hc-12-long-range-wireless-communication-module/
[7] https://www.kaspersky.com/resource-center/definitions/what-is-cryptography
[8] https://www.arduino.cc/en/software
[9] https://docs.arduino.cc/learn/starting-guide/the-arduino-software-ide/