SECURE COMMUNICATION SYSTEM

VIRAJ SHINDE
Department of E & TC Engineering, Marathwada Mitra Mandal's College of Engineering, Pune, India
virajshinde.etc@mmcoe.edu.in

SAVITRI KULKARNI
Department of E & TC Engineering, Marathwada Mitra Mandal's College of Engineering, Pune, India
savitrikulkarni.etc@mmcoe.edu.in

MRS. RAJESHWARI R. MALEKAR
Department of E & TC Engineering, Marathwada Mitra Mandal's College of Engineering, Pune, India
rajeshwarimalekar@mmcoe.edu.in

ABSTRACT
The principal objective of this project is to develop a medium range stand-alone (ad-hoc) portable wireless communication system. The availability of portable wireless communication system will enable devices such as personal computers, smart phones to communicate with each other without the need for sophisticated base stations like mobile towers. Various people like travellers, military, students, corporate, etc. will make wide use of this system for communicating among themselves and others. Our project overcomes all the above drawbacks being portable, stand-alone, fast and end-to-end secure (encrypted). It uses cutting-edge Advanced Encryption Standard for securing the data being exchanged.

INTRODUCTION
In today's world there are various communication systems available, but almost all of them needs some sort of larger infrastructure to work. For example GSM needs cellular networks and servers. There is need for medium range stand-alone (ad hoc) network which should be capable to securely communicate and fast enough to meet today's communication needs. Thus our system should be able to provide highest level of security along with fast data transfer speeds. In addition to this it should be portable. Setting up the system should be very quick and easy. Our project tries to meet all the above specified needs at a very low cost. The system should be very mobile and robust, so that it can be used in various places like personal, corporate, government, transport, and defence. The role of computers and networks in our everyday lives has made a necessity to protect data and adding security an important issue. Data transmitted over a network is sent in clear text making it easy for unauthorised persons to capture and read sensitive information. Encryption algorithms protect data from intruders and make sure that only the intended recipient can decode and read the information. Encryption is simply the translation of data into a secret code, and it is considered the most effective way to ensure data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Modern encryption is achieved using algorithms with a "key" to encrypt text or other data into digital random data and then decrypting it by restoring it to its original form.

LITERATURE SURVEY
ENCRYPTION: A key allows the encrypted secret code to be decrypted or allows plaintext (data that can be read by anyone) to be encrypted. There are typically two types used with data encryption--secret keys and public keys [1].
COMMON TYPES OF ENCRYPTION: 1. Secret Key (Symmetric) Encryption: In symmetric-key cryptography, the same key is used by both parties. The sender uses this key and an encryption algorithm to encrypt data; the receiver uses the same key and the corresponding decryption algorithm to decrypt the data [1].
2. PUBLIC KEY (Asymmetric) Encryption: In asymmetric or public-key cryptography, there are two keys: a private key and a public key. The private key is kept by the receiver. The public key is announced to the public. Messages are encrypted using the intended recipient's public key and can only be decrypted using the private key [1].
NRF24L01+: The nRF24L01+ is a single chip 2.4GHz transceiver with an embedded baseband protocol engine suitable for ultra-low power wireless applications. The nRF24L01+ is designed for operation in the world wide ISM frequency band at 2.400 - 2.4835 GHz [2].

ALGORITHM
TRANSMITTER
1) Get data (text or file).
2) Get Encryption Key
3) Divide data in chunks.
4) Encrypt each chunk with AES using the Key.
5) Transmit the data.
6) Wait for acknowledgement from receiver.
7) Display "Data Transfer Completed" on the terminal.

RECEIVER
1) Stay continuously in the receive mode.
2) Receive incoming cypher text blocks/chunks.

3) Get decryption key from the user.
4) After receiving is complete decrypt each chunk with the given key.
5) Combine all chunks in a single block/file.
6) Display message and send acknowledgement to transmitter.

MATERIALS AND METHODS

HARDWARE

1. Raspberry Pi 3 Model B
2. Nordic nRF24L01+
3. Laptop / PC

SOFTWARE

1. Raspbian OS
2. GNU C Compiler
3. BCM2835 C library

WORKING

The system consists of two Raspberry Pi 3 Model B devices, each connected to an nRF24L01+ transceiver via SPI. The source code of the system is in C. After initialization of the devices both the devices enter receive mode. When a user wants to transmit text or file, the user needs to enter transmit mode. In transmit mode text or file is to be selected. Text or file name is to be entered to send. At the other end the receiver receives the data and displays it on the screen. If file is received, a new file is created having the same name as the transmitted file from transmitter.

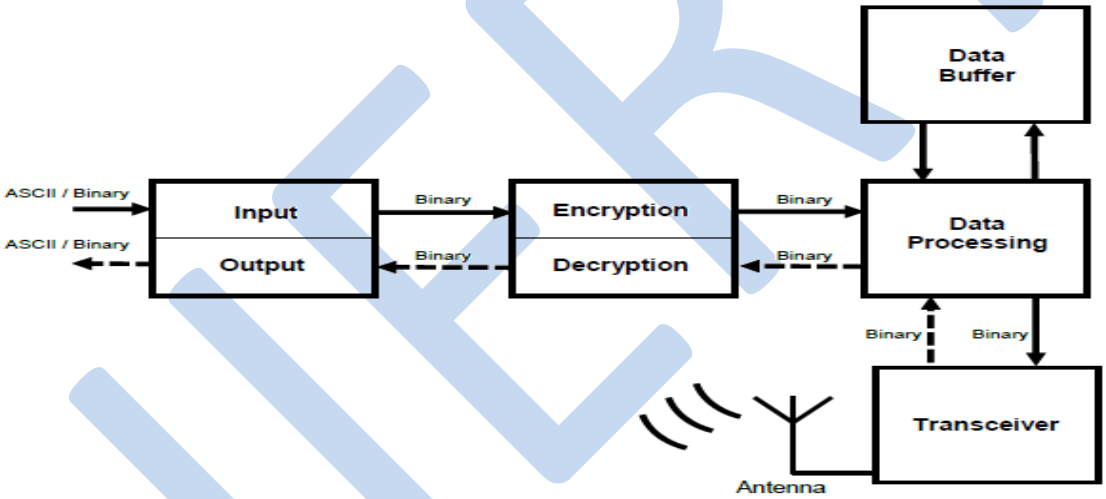


Figure 1: Block diagram of system

IMPLEMENTATION

Our system is implemented using two PCs as monitor.

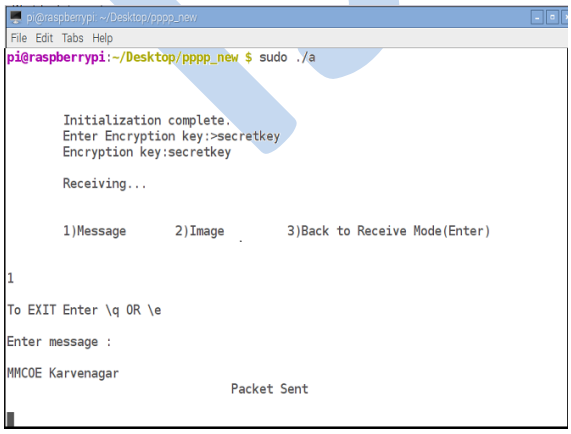


Figure 2: Transmitter Mode

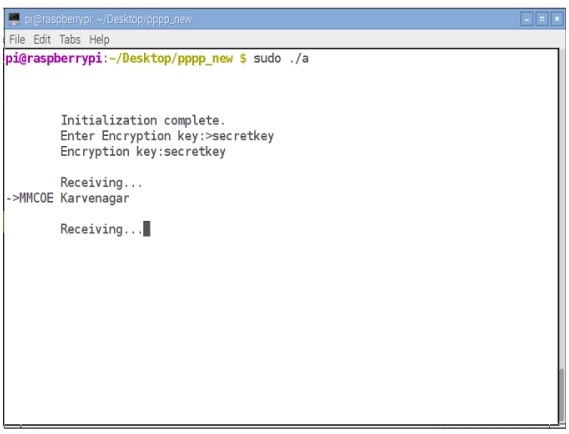
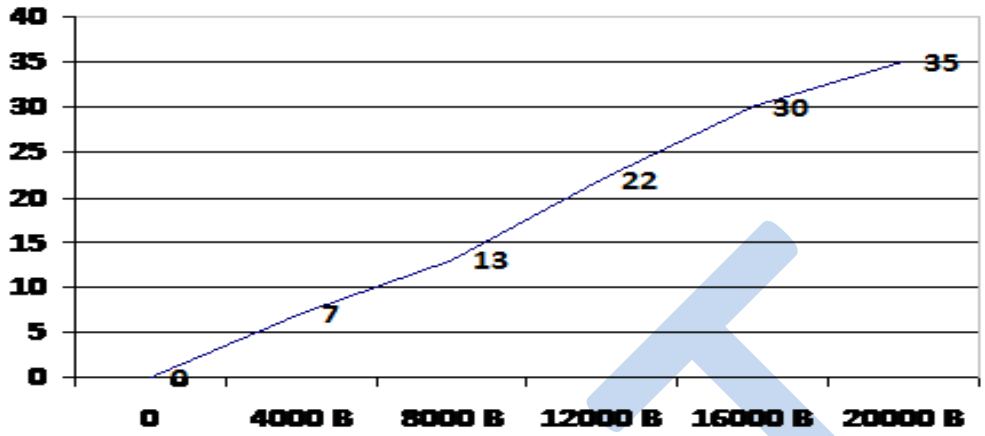


Figure 3: Receiver Mode

RESULTS

The time required to successfully transmit a packet is 164 us. The latency of the system with error control is less than 2.4 ms. The output of our system is as predicted. Text data is transmitted successfully with no errors. Large data such as computer files experience some error. The graph of Error density vs. data size is shown below.



Graph 1: Error Density vs. Bytes transferred

CONCLUSION

In this project, we demonstrated that it is possible for an optimized C implementation of AES encryption-decryption to achieve very high communication speed. We show very efficient communication using Raspberry Pi 3. Additionally, we show how each modules interact with each other. We provide a common, rigorous set of procedures and metrics for accurately measuring data transfer speed, and verifying encryption process. We also evaluate the hardware implementation on the nRF24l01+ radio module and find that it outperforms all software-based schemes. However, this comes at the cost of lack of flexibility, e.g., different sized data blocks and difficulty of evolving to patch future security vulnerabilities.

FUTURE SCOPE

The system can be expanded to accommodate very large number of devices to make a large Metropolitan Area Network. The system can be modified for increasing compromises and unauthorised access to critical business information. The system can be scaled down to use with various embedded devices, IOT applications, and Android Devices. The data transfer speed of the system can be increased by using other high speed RF modules.

REFERENCES

1) Behrouz A. Foruzan, "Data communication and Networking", Tata McGraw-Hill, 5th Edition.
2) nRF24L01+ Single Chip 2.4GHz Transceiver Product Specification v1.0.