Wireless Data Security using Encryption and Frequency Hopping

Prof. Pravin A. Dhulekar[1] Chirag Prajapat[2] Nakul Korde[3] Vivek Verma[4] Vikas Khare[5]
[1]Assistant Professor [2,3,4,5]Student
[1,2,3,4,5]Department of Electronics & Telecommunication Engineering
[1,2,3,4,5]SITRC, Nashik, Maharashtra

Abstract— Data Security is very important aspect for every communication system. One of the very popular techniques to assure the data security is encryption, where the transferred data is converted into cipher text. Also, protection against undesired interception while transmission process takes place is the key priority for secure reception of data. This feature is supported by spread spectrum techniques such as FHSS [1]. For FHSS, a bandwidth is divided into number of different distinct channels. The transmitter as well as receiver has to be synchronized on a particular channel and seed value to get a faithful output at the receiver. The transmitting section then transmits the message, broadcasting only for a few hundred milliseconds on any given channel. The transmitter then starts jumping (hopping) between different channels according to a pseudo-random algorithm (which is predefined by user); since the receiver knows the start channel and has exactly same seed, it can use the same algorithm to follow the hops and receive the signal. To any unauthenticated user who does not know the hopping sequence, the message is nearly indecipherable.

Key words: FHSS, Spectrum, Encryption

I. Introduction

The project aims to establish one-way wireless communication between two nodes. The issue with security of communication is addressed by encryption and frequency hopping. Herein, we use a traditional keyboard to give in the text input which is shown on the LCD display, this input message is digitized and then encrypted in the microcontroller and transmitted through the wireless media with the help of RF synthesizer. Communication through wireless media applications like radios and Wi-Fi is widely used communication service in the today's scenario. Being wireless communication no doubt that the transmitted data is highly prone to threats and illegal hacks. The risks are increased even more if the data is confidential. So in essence, encryption is the process of transforming the information in such a form that it is undetectable to all the unauthorized parties except the actual recipient, forming the basis of data privacy which is necessary for wireless communication. What this means is that the main reason for encrypting a document is that the intended recipient is the only one who receives in intelligible form the information which has been encrypted [2].

Avoiding any interferences and multi-path fading improves the channel quality which results in improved quality of the wireless communication. FHSS is a technique of data transmission where carrier signal hops from one specified frequency to another frequency. Mathematical modeling is generally used to simulate and analyze the performance improvement of spread spectrum with any modulation technique. A spread-spectrum transmission provides three main advantages:

- Avoids narrow band interference
- Difficult to intercept spread spectrum signals.
- Provides minimum interference when sharing the frequency band with other Conventional transmissions.

Two of the most used spread spectrum transmission techniques are frequency hopping (FHSS) and direct sequence (DSSS).

Definitions of FHSS: A system is defined to be a spread-spectrum system if it fulfills the following requirements

- The modulated signal occupies a more bandwidth than required minimum bandwidth necessary to send data.
- It must generate a spreading sequence by using wideband signal which is independent from the input data

At the reception, the data carried out by dispreading of spread sequence. It is necessary that receiver must be in synchronism with transmitter [2].

II. Overview of Literature Survey

In literature survey we literate many papers and IEEE documents which provide much help about theory belong to design, existing designs and techniques and new ideas which are related to my project. Before building the system below papers are taken into account for developing the proposed system.

A. Wireless Data Encryption and decryption technique for secured communication using RF module

The RF module used by them was STT-433 MHz Transmitter, STR-433 MHz Receiver, HT12E RF Encoder and a HT12D RF Decoder. RF Transmitter is connected to different sensors through RF Encoder. Their encoder used to converts the 8-bit binary data into a single bit data and then it sends to the transmitter to transmit. The data in physical medium has analog value. At the destination end, the receiver receives this analog value on a single data line and passes this data to the decoder. The function of a decoder is opposite of what an encoder does i.e. it converting a single bit digital data into eight bit data and pass it on to the microcontroller which does the further processing.

B. Enhancement of security by FHSS transmission system using hopping sequence and its compliment

They were worked on, a latest technique known as CHS-FHSS (Complemented Hopping Sequence - FHSS) is described to enhance the security of their trans-mission system by application of spreading sequence and also its compliment to change the carrier frequency and spread the narrow band information signal over larger bandwidth. Employing the proposed technique can provide a much stronger security system than the already existing system.

C. Design and develop Wireless system using frequency hopping Spread spectrum

This paper discusses different methods for implementation of FH-SS and an overview of some wireless technologies. Here, by using a spectrum analyzer power levels emitted by transceiver were measured. To measure frequency of transmitted signal as well as output power, the instrument will scan ISM frequency band. When successive frequency sweeps are performed then traced elements on the spectrum analyzers display is updated with the maximum signal level detected.

D. Secure Wireless Transmission of Data via Encryption and Frequency Hopping

In this system we observed the application of wireless communication as well as we learn about the XOR-encryption technique which a type of symmetric encryption. In here, the transceiver used was CYWUSB6935 from Cypress Semiconductors and used the ATmega16 microcontroller for interfacing and encryption of input and decryption of the same. However, the implementation of frequency hopping wasn't successful. Synchronization was the most important hurdle for frequency hopping. Since this could not be achieved by simple transmission of known bytes, frequency hopping could not be implemented.

III. SYSTEM DESIGN AND IMPLEMENT

A. Input Signal

The input given to the system is a text signal. This message will converted to desired string of 0s and 1s with the help of an ADC (analog to digital converter) to be processed by controller or micro controller unit.

B. Analog to Digital Converter

Given analog input signal will be converted to its equivalent digital form by the ADCs. The output is a sequence of binary values that have been converted from a CT and CA analog signal to its DT and DA digital signal.

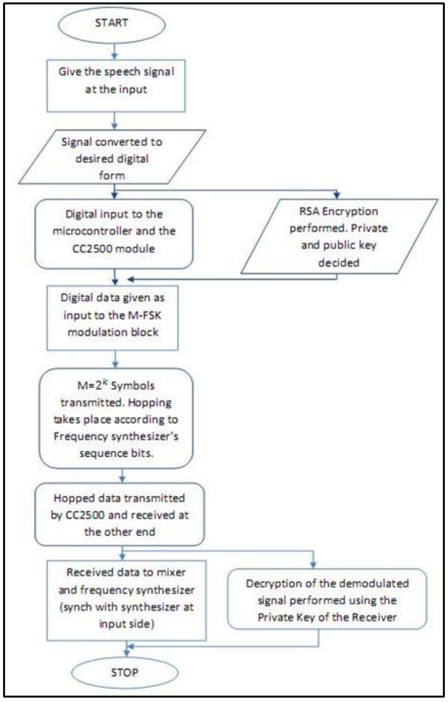
START
Give the speech signal at the input
Signal converted to desired digital form
Digital input to the microcontroller and the CC2500 module
RSA Encryption performed. Private and public key decided
Digital data given as input to the M-FSK modulation block
M=2^k Symbols transmitted. Hopping takes place according to Frequency synthesizer's sequence bits.
Hopped data transmitted by CC2500 and received at the other end
Received data to mixer and frequency synthesizer (synch with synthesizer at input side)
Decryption of the demodulated signal performed using the Private Key of the Receiver
STOP

Fig. 1: Flow Chart of System

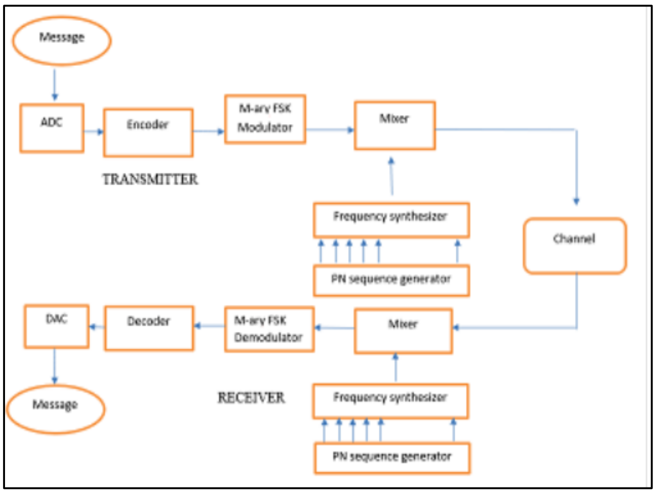

Fig. 2: Block diagram of system

C. CC2500 (Encoder)

SPI interface: CC2500 is configured via a simple 4-wire SPI compatible interface (SI, SO, SCLK and CSn) where CC2500 is the slave and micro-controller (here ATmega16) is used as master. Register access and commands are given by serial communication to the CC2500 by atmega16 with SPI interface. In SPI, master controller generate clock and chip select signal. SPI communication involves two shift registers. One in master and other is in slave. Data is shifted from master controller to the slave and vice -versa in circular manner in synchronous with clock generated by master and at the end of shift operation, data in master register and slave register is exchanged.

In CC2500 module, all the transfers on the SPI serial communication are done MSB RST. All communication on the SPI interface initialize with header byte containing a Read/Write bit, a burst access bit (B) and 6-bit addresses (A5 A0). The CSn pin disabled during transfers on SPI bus. If CSn enables during the transfer of a header byte or during R/Wor from/to a register, the transfer will not be successful or cancelled.

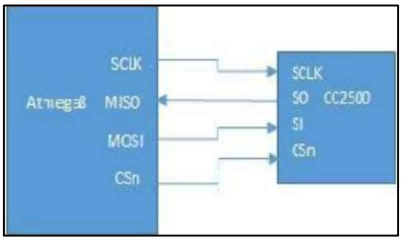

Fig. 3: Interfacing CC2500 module with Atmega16

D. Initialize/configure CC2500

The RF synthesizer CC2500 containing 47 configurable registers which has to be programmed with SPI interface after each time the chip is reset. CC2500 can enter into TX or RX mode or to decide data transmission rate and modulation scheme by programming these registers.

The configuration registers addressed from 0x00 and end at 0x2F. For writing data in configuration registers AVR Atmega16a will send two bytes to CC2500 through SPI interface. These two bytes are then sent one after the other. The last bits (A5 to A0) of the first byte (byte 1) gives CC2500 module the address of register, whereas the next byte gives data which is to be written into the registers. As SPI interface basically means exchange of data between master and slave, when Atmega16 (master) sends these two bytes, it will receive two bytes in exchange which will give the status of the CC2500 module. By this algorithm CC2500 program its configuration registers. Now CC2500 is ready to transmit or receive data wirelessly.[6]

E. Transmit Data:

There are TX and RX FIFO registers same as configuration registers. For transmission of data in wireless media, data has to be write in TX FIFO as same as that in configuration register. Address byte and data byte is send to CC that will be written into its TX FIFO. Then STX command is for sending data from TX FIFO to wireless media. The address for TX FIFO is 0x3F. So A5 to A0 bits are at high level. We are sending 3 bytes of data, so 6th bit of address byte will be 1 in burst mode. Hence address byte now becomes 01111111= 0x7F.[4]

F. M-ary FSK Modulation

The binary sequence is applied to M-ary modulator the output of which goes to the mixer. The other input is obtained from a digital frequency synthesizer. At the multiplier output we get two input frequencies, their sum and their difference frequency components. The BPF is designed to accept only the sum frequency components rejecting all other components.

G. Mixer

Frequency mixer is a non-linear electrical circuit which emits new frequencies from two signals frequencies applied to it. Two signals at frequencies f1 and f2 are applied to a mixer in its most of the applications. Here we can observe that output of M-ary Modulator (f1) and Frequency Synthesizer (f2) are both given as an input to the mixer block. The synthesizer output at a given instant of time is the frequency hop. Each frequency hop is mixed with the MFSK signal to produce the transmitted signal. The frequency hops at the output of the synthesizer are controlled by the successive bits at the output code of the PN code generator. The output bits of PN generator change randomly. Therefore the synthesizer output frequency will also change randomly. Hence the frequency hops produced will vary in random manner. IF the number of successive bits at the output bit of PN sequence is n, then the total no. of frequency hops will be 2n: The total bandwidth of transmitted FH signal is equal to the sum of all the frequency hops. Therefore the BW of the transmitted signal is very large of the order of few GHz.

H. Receiver Section

The received signal is applied to a mixer. The other input to the mixer comes from a digital frequency synthesizer. This digital synthesizer is driven by a PN code generator which is synchronized with the PN code generator at the transmitter and generates the same code sequence. Therefore the frequency hops produced at the synthesizers output will be identical to those at the synthesizers output at the transmitter.

At multiplier’s output, we get the input signals, their sum and difference. Out of these frequency components difference component is selected by the BPF that follows the multiplier. This difference signal is MFSK signal. Thus the mixer removes the frequency hop-ping. The MFSK signal at the mixer output is then applied to non-coherent MFSK demodulator. At the output of MFSK detector we obtain the digital modulating signal.

The non-coherent M-ary FSK detector can be implemented by using a bank of M, non-coherent matched filters. Each matched filter is matched to one of the tones of the MFSK signal. The largest output out of the M available outputs of filters is selected to obtain the digital modulating signal.

I. Encryption and Decryption

Encryption is the process of converting plain text into its complicated cipher text or it’s simply an encoding process. Encryption is done at transmitting side while decryption is done at the receiver.

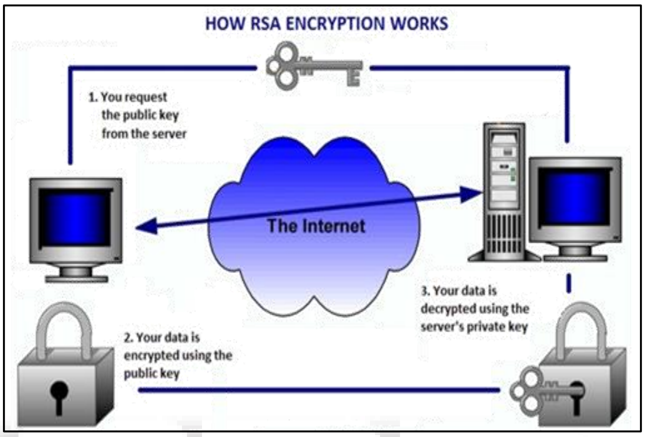
HOW RSA ENCRYPTION WORKS
1. You request the public key from the server
The Internet
3. Your data is decrypted using the server's private key
2. Your data is encrypted using the public key

Fig. 4: RSA algorithm technique

Here we use transposition cipher encryption technique to ensure the security of transmitting text. Transposition refers to rearranging the words and letters (change the sequence of letters) to achieve encryption.

IV. RESULTS

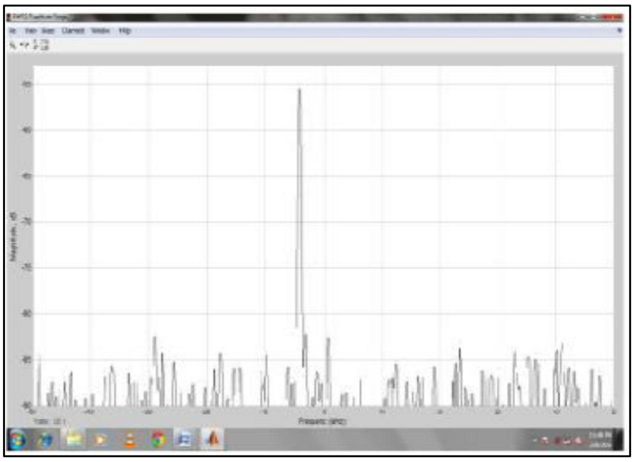

Fig. 5: Spectrum of FHSS in MATLAB

The spectrum of FHSS TX shows in Fig. 3. The data available at Spike in the each fig (3) which seems like noise, overall output of transmitter seems like a noise; FHSS output is very difficult to Hacked by any unauthorized person due to the hopping frequency in known to designer mean an authorized person. Fig. 4 shows the result of FHSS transmitter, the input data applied to the transmitter is obtained at the output of the transmitter as shown in the Fig.3, the low power technique that is clock gating is applied to the coding part hence it takes less power. [6]

V. Conclusion

The work done until now shows the working of the proposed "Secure data transmission using Encryption and frequency hopping". The encrypted data looks like garbage until it is decrypted. So, it is not possible for anyone to look over the data during the transmission.

Hence considering this we can say it is provided with an effective security for data communication by designing standard algorithm for encryption as well as decryption and this transmission will also include the password which provides additional security for the data.

This transmission including password so the users must and should remember this and keep it as secret and the password will be any of length we can use.

References

[1] P. OLSOVSKY, P. PODHORANSKY, \DESIGN AND SIMULATION OF FREQUENCY HOPPING", Institute of Electronics and Photonics, faculty of Electrical Engineering and Information Technology, Slovak university of Technology

[2] Shahid Latif, Muhammad Kamran, Wasim-ud-Din, RahatUllah and Abou Bakar Nouman,\Security Enhancement of Fhss Transmission System Using Hopping Sequence and its Compliment (CHS-FHSS), ISSN:1818-4952,IDOSI Publications, 2013

[3] Nentawe Y. Goshwe,\Data Encryption and Decryption Using RSA Algorithm in a Network Environment", IJCSNS International Journal of Computer Science and Network Security, VOL.13 No.7, July 2013

[4] Sandip Kamath, KartikMohta, Rohan Raj Desu, Anil Krishna N.,\Secure Transmission of Data via Encryption and Frequency Hopping", EE318 Electronic Design Lab Project Report,EEDept,IITBombay, April 2007.

[5] Proakis John G., Digital Communications, Third edition, New York, McGraw Hill, 1995.

[6] http:"Wireless Communication with 2.4 GHz RF Transceiver CC2500" //www.engineersgarage.com/contribution/wireless-communication-24-ghz-rf-transceiver-cc2500