Las redes de área personal inalámbricas (WPAN) proporcionan muchas ventajas al permitir la transmisión de datos con la comodidad de conectarse en cualquier lugar. Por otro lado, las redes inalámbricas requieren nuevos conceptos de seguridad que se obvian en las redes cableadas. Un intruso que busque acceso a una LAN cableada se enfrenta irremediablemente con el problema del acceso físico a la misma. En una WPAN al intruso le basta permanecer en el área de cobertura para estar en contacto con la red local. De esta situación nace la necesidad de encriptar los datos con un protocolo eficiente.

Comunicación encriptada por radiofrecuencia usando un microcontrolador A 433,92 MHz

Pablo Corral González, Ricardo García Gutiérrez, Juan Navarro Muñoz
Área de Teoría de la Señal y Comunicaciones
Universidad Miguel Hernández

El vigente Cuadro Nacional de Atribución de Frecuencias (CNAF) fue aprobado por la Orden ITC/1998/2005 de 22 de junio de 2005 (BOE nº 153, de 28 de junio de 2005). En él se establecen 8 bandas de frecuencias susceptibles de ser usadas con fines Industrial, Científico o Médico (bandas ICM). La banda que se usa en este artículo es la ICM 4 que comprende el rango de 433,050 a 434,970 MHz. Las frecuencias designadas ICM son frecuencias denominadas de «uso común» y, por tanto, de uso regulado pero que no requiere de título habilitante, ni de solicitud expresa de uso de dominio público radioeléctrico.

Este proyecto pretende mostrar el diseño e implementación de una comunicación bidireccional de muy bajo consumo en la banda UHF con estas frecuencias de uso común y cumpliendo con los límites de potencia indicados en la Recomendación CEPT/ERC 70-03 (Anexo 1).

DIAGRAMA GLOBAL DEL SISTEMA

Se ha realizado un sistema de comunicación por radiofrecuencia, el cual se pueda conectar a un ordenador por el puerto USB y que, a su vez, realice una comunicación encriptada. Se realizará un dispositivo basado en microcontroladores, en concreto microcontroladores PIC de la empresa Microchip. Para realizar la comunicación USB se utiliza un PIC18F4550, el cual posee un módulo USB 2.0 embebido capaz de comunicarse a 12 Mb/s, que por su capacidad de cómputo éste será el encargado de

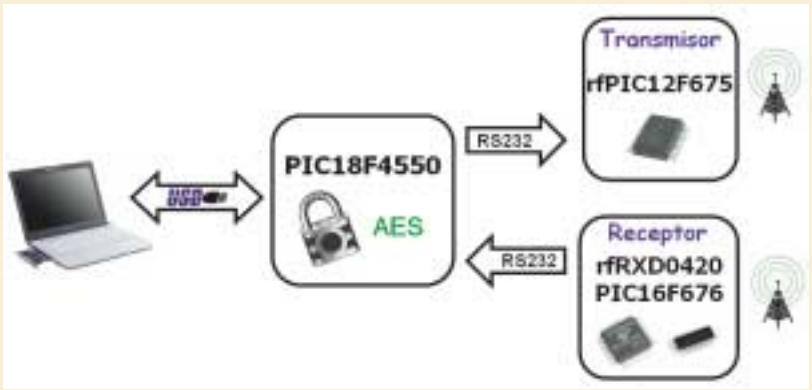

Figura 1

dominar el sistema (el módulo emisor y el módulo receptor), y además de realizar la encriptación mediante un algoritmo simétrico. Para la transmisión se utilizará un microcontrolador RFPIC12F675F, el cual posee embebido un transmisor UHF que puede emitir entre 380 y 450 MHz, y se comunicará con el PIC18F4550 mediante el protocolo RS-232, puesto que no posee módulo USART, ésta se implementará mediante software. Para la recepción se utiliza un RFRXD0420, que se trata de un receptor superheterodino en banda UHF, que será gestionado por un PIC16F676, para ver si la trama recibida es correcta, y éste se la comunicará mediante su módulo USART por RS232 al PIC18F4550. En la Figura 1, se puede ver el diagrama planteado.

DISEÑO Y PROGRAMACIÓN DEL SISTEMA

En principio, los PIC's fueron pensados para un uso unidireccional. La empresa Microchip actualmente, no ofrece ningún microcontrolador que tenga embebido un receptor para UHF, sino que lo ofrece como un módulo independiente. A este receptor se le une otro microcontrolador con la única finalidad de analizar lo que el receptor escucha y si se trata de información correcta en recepción, enviar ésta al PIC18F4550.

El PIC18F4550 es un microcontrolador que puede ser programado tanto en lenguaje ensamblador como en C. La programación en ensamblador resulta costosa, ya que sólo para la comunicación USB se han

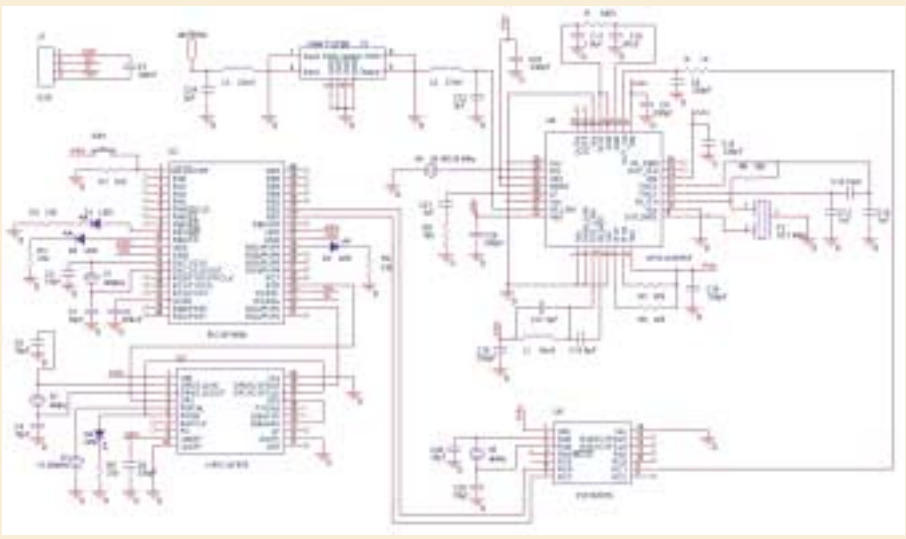

Figura 2

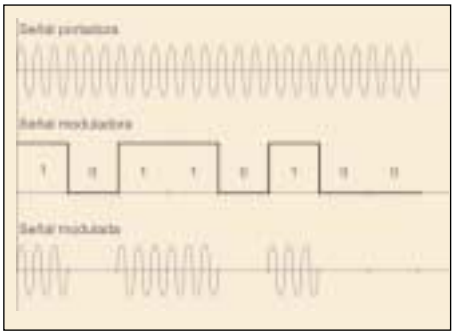

Figura 3

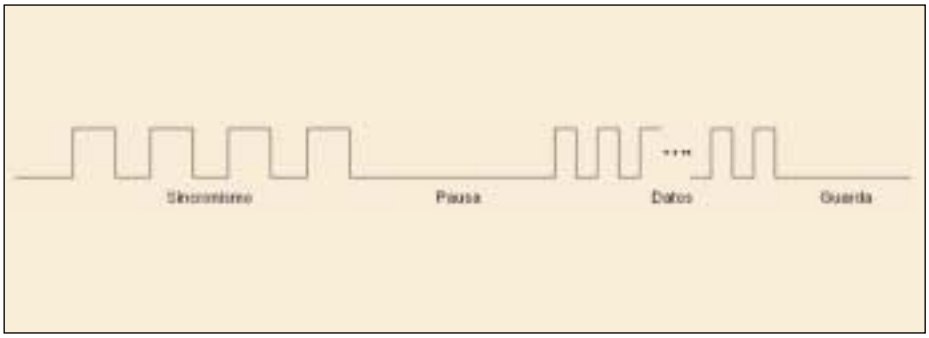

Figura 4

de utilizar una gran cantidad de registros. La programación en C para PIC resulta mucho más sencilla, con el inconveniente de que el código compilado ocupa mayor cantidad de memoria dentro del microcontrolador. Para el microcontrolador RFPIC12F675 se utiliza programación en ensamblador, puesto que permite una mayor precisión al tratarse de un lenguaje de bajo nivel donde se conoce de antemano el tiempo que tarda cada instrucción.

En un primer momento se realiza un diseño electrónico por ordenador del sistema, utilizando el programa Capture CIS del paquete Orcad, desarrollado por la empresa Cadence Design Systems, donde a su vez se obtiene un esquema electrónico del sistema. En la Figura 2 se puede ver el esquema.

Para garantizar una comunicación segura en entornos abiertos y asegurar así la confidencialidad de los datos transmitidos, se hace necesaria la encriptación o enmascaramiento de la información a transmitir. Desde el punto de vista de la criptografía moderna, existen dos tipos de tecnología de claves a utilizar: los llamados algoritmos y protocolos asimétricos, también llamados de clave pública (*public key*) y los algoritmos y protocolos simétricos o de clave privada (*private key*). Las principales características de cada uno de ellos, son las siguientes:

Algoritmos y protocolos asimétricos: son aquellos que hacen uso de un par de claves para el intercambio de información entre entidades. Una de ellas es pública y por tanto conocida por todas y otra es privada y únicamente conocida de forma confidencial por cada entidad. En estos protocolos, el remitente hace uso de la clave pública del destinatario para encriptar la información a transmitir y únicamente se podrá desencriptar dicha información mediante la clave privada del destinatario o receptor.

Algoritmos y protocolos simétricos: son aquellos que utilizan una misma clave para producir el cifrado y el descifrado de los datos a transmitir en una red. Previa a la comunicación, las dos partes han de ponerse de acuerdo sobre la clave que van a utilizar. Una vez definida ésta, el remitente procede a encriptar la información a transmitir con dicha clave y el receptor desencriptará dicha información con la misma clave que usó el remitente.

Al no ser necesario un protocolo excesivamente complejo entre el transmisor y el receptor, se decidió utilizar, entre los algoritmos de cifrado, uno de tipo simétrico; concretamente el AES (*Advanced Encryption Standard*), adoptado en el año 2002 por el NIST (*National Institute of Standard and Technology*). Para realizar la implementación de esta parte del sistema, se decidió utilizar un hardware compuesto de un PIC de la familia 18, sobre el cual se incorpora la programación necesaria para realizar la encriptación descrita en el estándar AES.

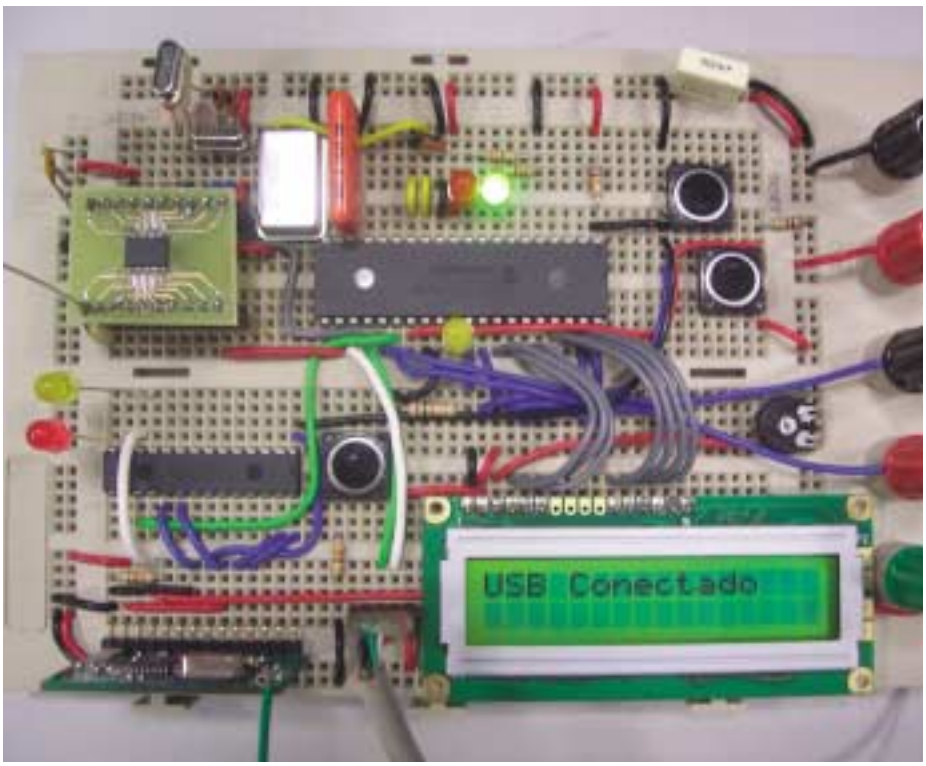

Figura 5

FRECUENCIA DE TRANSMISIÓN

Como ya se ha comentado, la frecuencia de transmisión utilizada es de 433,92 MHz. Esta frecuencia viene dada por el PIC del transmisor utilizado. Este, posee un oscilador Colpitts el cual alimenta con una frecuencia de referencia al PLL y es independiente del oscilador del microcontrolador. Para conseguir la frecuencia deseada, se conecta un cristal de cuarzo externo, que se multiplica por un

Tabla 1.
Márgenes de potencia de transmisión

Resistencia	Potencia de Salida (dBm)
Abierto	9
100 kΩ	2
47 kΩ	– 4
22 kΩ	– 12
Corto	– 70

valor de 32 que viene del lazo de realimentación del PLL, consiguiendo una frecuencia de transmisión que viene dada por la expresión:

$$F_{TRANSMISOR} = F_{CRISTAL} \cdot 32$$

Los datos se envían mediante ASK (*Amplitude-Shift Keying*, modulación por desplazamiento de amplitud) binario. El funcionamiento de esta modulación se basa en representar la información digital como variaciones de la amplitud de la onda portadora. La forma más sencilla y utilizada de este tipo de modulación, es imitar el funcionamiento de un interruptor: en ciertos intervalos de tiempo tenemos portadora (información a transmitir) y en otros no; donde la presencia de portadora indica un 1 binario y una ausencia de portadora indica un 0.

PROTOCOLO PARA RF

Para la correcta recepción de los datos, se ha diseñado un protocolo que hará que el receptor identifique los datos que envía el transmisor, ya que en una banda libre como ésta, podemos llegar a encontrar muchas fuentes de interferencias.

Se envía primero una trama de sincronismo (formada por una serie de pulsos) al receptor. Lo que se pretende con esta trama es sincronizar el receptor para que éste no se confunda con posibles señales interferentes. Tras esta trama, se realiza una pausa de un tiempo determinado, donde el receptor ya sabe que le va a llegar la trama de datos. Se envía toda la trama de datos, que el receptor almacena para posteriormente enviarla al PIC18F4550. Al terminar la trama de datos se deja otro tiempo de pausa, donde el receptor envía los datos recibidos al PIC18F4550 y el emisor se prepara para enviar de nuevo más datos. Se puede ver en la Figura 4 la trama con nivel más detalle.

La potencia de salida del transmisor según especificaciones del fabricante está en el rango de +9 dBm hasta –70 dBm. Esta potencia es variable, introduciendo una resistencia en el sistema, según la Tabla 1.

Las distancias previstas a alcanzar, según el fabricante, son de 100 m aunque tras pruebas realizadas con el sistema se comprueba como, en visión directa y espacio libre, se logra alcanzar los 150 m.

APLICACIONES Y USOS DEL SISTEMA

El sistema desarrollado es un dispositivo de corto alcance, que se puede adaptar a muchas aplicaciones. Un campo de aplicación importante sería la de telemetría y control. Se puede implementar una estación meteorológica con diferentes sensores de temperatura, humedad, viento, polen, polución, ruido... que sea autónoma, accionando sistemas de aire acondicionado, motores o lo que se necesite, pero a su vez, se puede acceder al sistema para cambiar parámetros para que de esta manera sus variables de acción cambien.

Otra aplicación sería la de puerta trasera en sistemas electrónicos, para poder acceder al sistema si por ejemplo le ocurre una avería y poder testearlo.

O incluso, gracias a su capacidad de encapsulamiento, se pueden desarrollar mandos a distancia accionables desde un ordenador o llaves electrónicas que a la vez que autentifiquen por USB también lo hagan por radiofrecuencia.

CONCLUSIONES Y LÍNEAS DE FUTURO

Este artículo muestra la implementación de un dispositivo de bajo consumo que permite una comunicación inalámbrica de área local en banda UHF con transmisión de información cifrada mediante el algoritmo AES. La implementación final del sistema se puede ver en la Figura 5, en ella se muestra cómo están interconectados los diferentes bloques de los que consta el sistema. Como se aprecia, la interconexión de los diferentes elementos se ha realizado en una placa de desarrollo facilitando así su manejo.

Una de las posibilidades que se plantean para el futuro es usar otra frecuencia ICM que permita un mayor ancho de banda como, por ejemplo, 2,4 GHz. Otra línea futura de trabajo sería crear una comunicación multipunto entre diferentes dispositivos, en vez de la comunicación punto a punto, tal y como se ha planteado en este proyecto.

BIBLIOGRAFÍA

(1) Orden ITC/1998/2005.
(2) Recomendación CEPT/ERC 70-03 (Anexo 1).
(3) Angulo Usategui, J. M. *Microcontroladores PIC. Segunda parte: PIC 16F87X diseño practico de aplicaciones.* Ed. Mc Graw-Hill, 2006. ISBN: 97884146271.
(4) Hernando Rábano, J. M. *Transmisión por radio.* Ed. Ramón Areces. 2006.
(5) Smith, J. *Modern Communications Circuits.* Ed. McGraw-Hill, 1986.
(6) Stallings, W. *Cryptography and Network Security. Principles and Practices.* Prentice Hall, 2003. Third Edition. ISBN: 0-13-111502-2.
(7) *Advanced Encryption Standard using the PIC 16XXX.* AN821, Microchip Technology Inc. 2002.
(8) *Designing Loop Antennas for the rfPIC12F675*, Microchip Technology Inc. 2003.
(9) Datasheet's PIC18F4550, RFPIC12F675F, RFRXD0420, PIC16F676.