GENERACIÓN DE SPREAD SPECTRUM USANDO MICROCONTROLADOR

Generation of Spread Spectrum using Microcontroller

RESUMEN
En este documento se presenta una descripción de la modulación en Spread Spectrum, así como una de las principales técnicas para su obtención: DSSS (Direct Sequence Spread Spectrum). También se muestra el desarrollo de un módulo generador de código Barker para Spread Spectrum por la técnica de secuencia directa, basado en microcontrolador, el cual permite realizar un análisis real de está técnica de modulación, con el fin comparar su comportamiento con los resultados teóricos obtenidos y las simulaciones desarrolladas en la herramienta Simulink de Matlab®.

PALABRAS CLAVES: Ancho de Banda, Canal de Transmisión, Espectro, Modulación, Redes WLAN, Secuencias Pseudoaleatorias, Microcontrolador.

ABSTRACT
In this document presents a description of the modulation in Spread Spectrum, as well one of the principal techniques for its obtaining: DSSS (Direct Sequence Spread Spectrum). Also there appears the development of a generating module of Barker code for Spread Spectrum for the technique of direct sequence, based on microcontroller, which allows to realize a real analysis of this technical of modulation, with the purpose of compares its behavior with the theoretical obtained results and the simulations developed in the tool Simulink of Matlab®.

KEYWORDS: *Bandwidth, Microcontroller, Modulation, Pseudorandom Sequences, Spectrum, Transmission Channel, WLAN Networks.*

EDWIN ANDRÉS QUINTERO
Ingeniero Electrónico
Candidato a Magíster en Instrumentación Física
Profesor Auxiliar
Universidad Tecnológica de Pereira
equintero@utp.edu.co

HUGO ARMANDO GALLEGO
MSc. Física
Profesor Asistente
Universidad Tecnológica de Pereira
ugo@utp.edu.co

HOOVER OROZCO GALLEGO
MSc. Física
Profesor Asistente
Universidad Tecnológica de Pereira
hog1084@utp.edu.co

1. INTRODUCCIÓN

En las comunicaciones modernas se hace más notable la necesidad de ampliar el número de usuarios que utilizan el mismo canal de transmisión; así como disminuir la susceptibilidad al ruido de los medios de propagación de las señales. Es gracias a esta necesidad que la teoría del Spread Spectrum ha encontrado una gran aplicación en las técnicas de modulación digital que buscan maximizar el rendimiento de uno de los parámetros más importantes en una comunicación: la seguridad de los datos.

Inicialmente, esta técnica de modulación fue desarrollada para aplicaciones militares gracias a su capacidad de camuflar la información de manera que no sea interpretada por usuarios del canal ajenos a la comunicación [1], pero se encontró además que el costo a pagar por la seguridad de los datos es una ineficiente utilización del ancho de banda disponible y de la potencia del transmisor. Sin embargo, posteriormente se observa en el presente documento que esta ineficiencia es tolerable en las aplicaciones en las cuales Spread Spectrum es usada con gran versatilidad. Esta gran ventaja ha permitido que sea utilizada, por ejemplo, en sistemas de comunicaciones donde varios usuarios móviles desean crear un enlace con una estación central o radio base, es decir, en los sistemas de telefonía celular.

2. MODULACIÓN EN SPREAD SPECTRUM

El desarrollo de la telemática ha mostrado que los principales problemas de las comunicaciones digitales son la eficiente utilización del ancho de banda y de la potencia. La justificación de este problema estriba en que el ancho de banda y la potencia son los dos principales recursos en comunicaciones, siendo entonces esenciales en el diseño de la mayoría de estos sistemas. No obstante, existen situaciones en las cuales se hace necesario sacrificar la eficiencia de estos dos recursos, por otros más importantes para la aplicación. Por ejemplo, es importante introducir un nivel alto de seguridad al sistema para que otros usuarios del canal de transmisión ajenos a la comunicación no puedan obtener el mensaje enviado fácilmente.

Este requerimiento es proveído por una clase de técnicas de señalización conocidas como modulación Spread Spectrum. La principal ventaja de un sistema de comunicación que utiliza Spread Spectrum es la habilidad de rechazar la interferencia involuntaria producida por un usuario que intente transmitir por el canal simultáneamente, así como repeler la interferencia producida por un usuario que intenta sabotear la transmisión [1].

Fecha de Recepción: 26 de enero de 2009
Fecha de Aceptación: 20 de marzo de 2009

Spread Spectrum es una técnica de modulación en la cual, la señal de interés ocupa un ancho de banda mucho mayor que el ancho de banda mínimo necesario para que la información sea transmitida. Este ensanchamiento del espectro produce que la señal tenga la apariencia del ruido, siendo difícil de leer por usuarios indeseados y presentando una protección contra interferencias intencionales o "jamming", el cual consiste en señales de alta potencia con un ancho de banda limitado que son dirigidos directamente al receptor para sabotear la comunicación [2].

Este ensanchamiento de la señal es logrado al utilizar la secuencia de datos a transmitir para modular el ancho de banda de un código aleatorio definido (figura 1). Después de este proceso la señal toma el ancho de banda del código ruidoso, llamado comúnmente código o secuencia PN. El código pseudo aleatorio consiste en una cadena de 1's y 0's con un periodo de repetición conocido y con un espectro ancho y de baja potencia muy similar al del ruido [3]. En el receptor debe existir un generador de código PN con iguales características al del transmisor y sincronizado con este para que la información pueda ser recuperada.

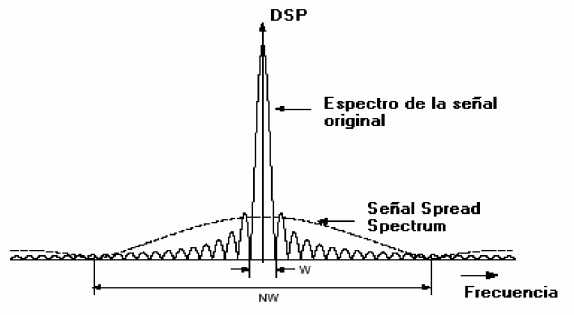

Figura 1. Densidad espectral de potencia de una señal modulada en Spread Spectrum.

Puede pensarse inicialmente que la aplicación de Spread Spectrum limita el uso del canal ya que aumenta el ancho de banda de la señal original y por consiguiente el número de usuarios permitidos disminuye. Sin embargo, este problema es resuelto al utilizar códigos PN diferentes para cada transmisión independiente en el mismo canal de comunicación. De esta forma, cada receptor aplicará a la señal recibida el código PN correspondiente obteniendo solo la señal deseada sin sufrir la interferencia de los demás usuarios que están usando el medio al mismo tiempo. Se observa entonces la gran utilidad de la técnica de modulación de Spread Spectrum, al permitir que un gran número de usuarios utilicen la misma banda de frecuencias sin sufrir los riesgos de las interferencias involuntarias (causadas por los demás usuarios del canal cuando desean transmitir), y de las interferencias tipo "jamming" que tienen como objeto sabotear la comunicación. Las limitaciones de esta técnica de modulación consisten en que a medida que los códigos PN se hacen más largos para dar cabida a más usuarios en el canal, es más difícil realizar la sincronización entre el transmisor y el receptor, así como el gran número de códigos PN hace que estos no se diferencien lo suficiente, provocando de esta forma que las señales en el receptor no sean tan claras, por la dificultad de diferenciar el espectro de dos códigos PN similares.

2.1 DIRECT SEQUENCE SPREAD SPECTRUM

Una de las técnicas de Spread Spectrum usada en las redes LAN inalámbricas es conocida como Direct Sequence Spread Spectrum (DSSS). En este método, el ancho de banda de la señal a transmitir es ampliado mediante la multiplicación de los datos de información con el código PN. Esta operación se muestra en la figura 2.

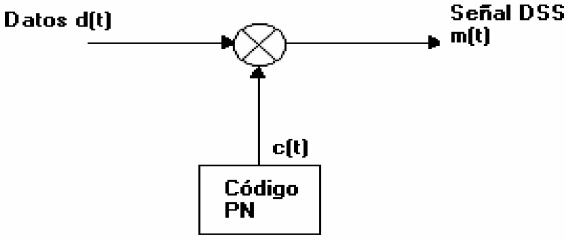

Figura 2. Transmisión de DSSS en banda base

Los conceptos de la transformada de Fourier afirman que la multiplicación en el tiempo de dos señales independientes, corresponde a su convolución en frecuencia [4]. Así, si el ancho de banda de la secuencia de datos *d(t)* es pequeño y el espectro del código PN, *c(t)* es ancho, la señal *m(t)* obtenida tendrá necesariamente el ancho de banda del código PN. Dado lo anterior es posible afirmar que la secuencia PN actúa como un código ensanchador. En este caso, el periodo de la secuencia pseudo aleatoria debe ser igual al tiempo de cada bit de información T_b, de manera que todo el código sea multiplicado por el bit correspondiente. Para realizar esta operación, cada bit de información es dividido en una serie de pequeños incrementos de tiempo denominados chips. El tiempo de duración de cada chip es igual al tiempo de cada símbolo del código PN y es conocido como tiempo de chip Tc. La figura 3 muestra los diagramas de tiempo para cada señal.

Para transmisión en banda base, la señal *m(t)* representa la señal transmitida. Esta señal puede ser expresada como:

$$m(t) = c(t) * d(t) \qquad (1)$$

La señal recibida *r(t)* consistirá en la señal transmitida *m(t)* y una interferencia aditiva introducida en el canal de transmisión denotada por *i(t)*. Entonces, en el receptor:

$$r(t) = m(t) + i(t) \qquad (2)$$

$$r(t) = [c(t) * d(t)] + i(t) \qquad (3)$$

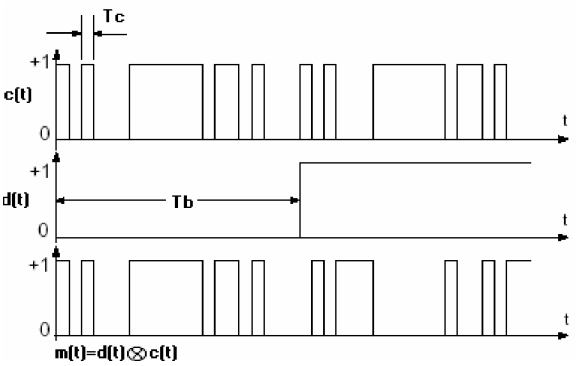

Figura 3. Diagrama de tiempo de la secuencia de datos *d(t)*, el código PN *c(t)*, y la señal resultante *m(t)*.

Para recobrar la secuencia de datos original, la señal recibida *r(t)* debe ser multiplicada por el código PN *c(t)* generado en el receptor, el cual, es la réplica exacta del código PN del transmisor. El resultado de esta operación será:

$$z(t) = r(t) * c(t) \qquad (4)$$

$$z(t) = [c^2(t) * d(t)] + [c(t) * i(t)] \qquad (5)$$

La ecuación 5 muestra que la señal deseada *d(t)* se encuentra multiplicada dos veces por *c(t)*, mientras que la interferencia *i(t)* se encuentra multiplicada solo una vez. Ahora, si el código PN alterna entre los niveles -1 y +1, es posible afirmar que:

$$c^2(t) = 1 \quad \text{para todo } t \qquad (6)$$

Por lo tanto, la ecuación (5) queda:

$$z(t) = d(t) + c(t) * i(t) \qquad (7)$$

De la ecuación anterior se observa que la secuencia de datos *d(t)* es reproducida después del multiplicador en el receptor, excepto por los efectos de la interferencia representada por el término aditivo *c(t)*i(t)*. La multiplicación de la interferencia *i(t)* por el código PN *c(t)* hace que el código ensanchador la afecte de igual forma como lo hizo con la señal original en el transmisor. Así, la señal *d(t)* en el receptor será de banda estrecha y el término *c(t)*i(t)* tendrá un espectro muy ancho, por lo que al pasar la señal *z(t)* por un filtro pasa-banda con un ancho igual al de la señal *d(t)* se obtendrá la señal original con una potencia mucho mayor que la del término *c(t)*i(t)*, por lo que los efectos de este ruido son despreciables [3].

En resumen, el uso de un código ensanchador (con propiedades pseudo aleatorias) en el transmisor, produce una señal con un ancho de banda muy grande considerada como ruido por un receptor que no conozca el código PN. En la figura 4 se presenta el diagrama de bloques de un sistema de comunicación completo que utiliza DSSS.

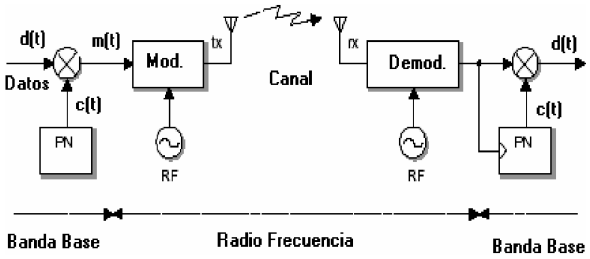

Figura 4. Diagrama de bloques de un sistema de comunicación con DSSS.

3. SECUENCIAS PSEUDO ALEATORIAS (CÓDIGOS PN)

Una señal pseudo aleatoria es una función en el dominio del tiempo generada siguiendo un patrón determinado, cumpliendo con unas propiedades matemáticas dentro de las cuales se destaca la auto correlación. Como estas señales son consideradas como ruidosas, su auto correlación deberá corresponder en teoría con la función de auto correlación del ruido blanco gaussiano, la cual se observa en la figura 6 [3].

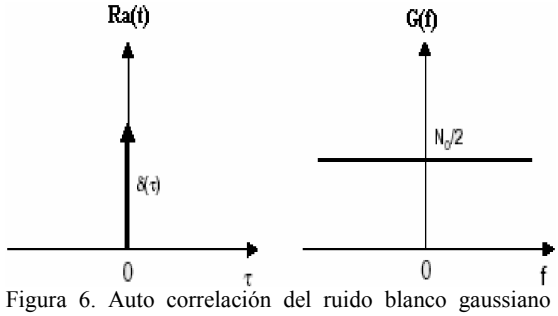

Figura 6. Auto correlación del ruido blanco gaussiano y su espectro.

Si se analiza la gráfica anterior, es posible observar que todos los elementos de la secuencia pseudo aleatoria tienen la misma probabilidad de aparición en un tiempo cualquiera, representada por la función delta de Dirac en el origen. En el caso de los códigos pseudo aleatorios de 11 bits usados en redes WLAN (conocidos como códigos Barker), la función de auto correlación no presenta un delta de Dirac en el origen, sino que muestra unos valores alrededor del mismo. Este inconveniente es causante de que al elevar el número de secuencias diferentes en el mismo canal de transmisión, exista un momento en el cual las señales comiencen a interferirse pues los códigos no serán distinguibles en los receptores. Entre mayor sea el número de símbolos o chips del código, más aproximada será su función de auto correlación a la ideal, pero el ancho de banda de la transmisión aumentará significativamente.

3.1 PROPIEDADES DE LAS SECUENCIAS PSEUDO ALEATORIAS

Todas las secuencias pseudo aleatorias usadas en la transmisión para ensanchar el espectro, deberán cumplir las siguientes propiedades [3]:
1. En cada periodo del código, el número de 1's es siempre uno más que el número de 0's. Esta característica es llamada propiedad de balance.

2. Un *Run* está definido como una secuencia consecutiva de unos y ceros. En una secuencia pseudo aleatoria, la mitad de los *Runs* tiene longitud 1. El total de los *Runs* de una secuencia pseudo aleatoria es:

$$R = (N + 1)/2 \qquad (8)$$

Donde *R* es la cantidad total de *Runs* de la secuencia pseudo aleatoria y N es el número de bits. A esta propiedad se le conoce como propiedad Run.

3. La función de auto correlación de una secuencia debe ser periódica y de valor binario. Esta propiedad es llamada propiedad de correlación.

Con base en las propiedades anteriores, se ha escogido como secuencia para generar Spread Spectrum con el microcontrolador, el siguiente código de 11 bits:

$$10110111000 \qquad (9)$$

4. MÓDULO GENERADOR DE DSSS

Elegido el código a generar, es posible pasar a la etapa de diseño del módulo. El chip a utilizar es el AT89C51 de la marca Atmel. Este integrado es un microcomputador de 8 bits, CMOS, de baja potencia, y con una memoria flash programable de 4KB. Posee un reloj interno que puede trabajar desde 100Hz hasta 24MHz y 32 líneas programables de entrada y salida [5].
La figura 7 muestra el diagrama de flujo de programa desarrollado en lenguaje ensamblador con el fin de convertir al microcontrolador en una modulador de DSSS en banda base. La figura 8 muestra el prototipo desarrollado.

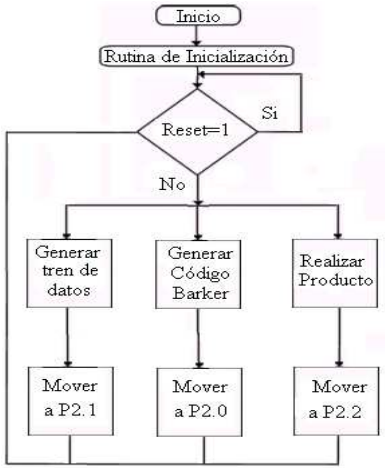

Figura 7. Diagrama de flujo del programa en ensamblador.

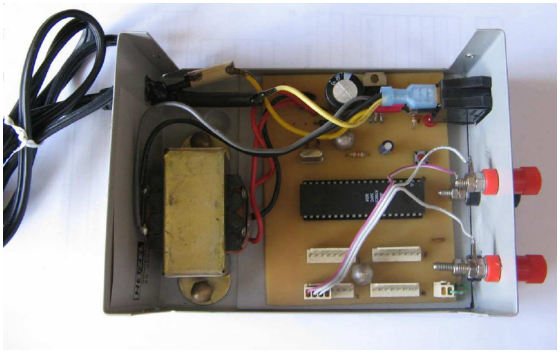

Figura 8. Prototipo construido.

5. RESULTADOS[1]

A continuación se presentan los resultados obtenidos al realizar las mediciones correspondientes en los respectivos puertos del microcontrolador, después de ensamblar completamente el módulo. Estas señales fueron visualizadas con un escopómetro marca Fluke, y posteriormente se calcularon los espectros de cada señal gracias al software Fluke View®. Para una completa comprensión e interpretación de las gráficas obtenidas es recomendable acudir primero a los manuales del escopómetro y del software anteriormente mencionado.

Para comprobar los resultados teóricos con los experimentales, también se muestran las simulaciones del módulo generador de DSSS, en forma de diagrama de bloques realizadas en la utilidad Simulink de MatLab®.

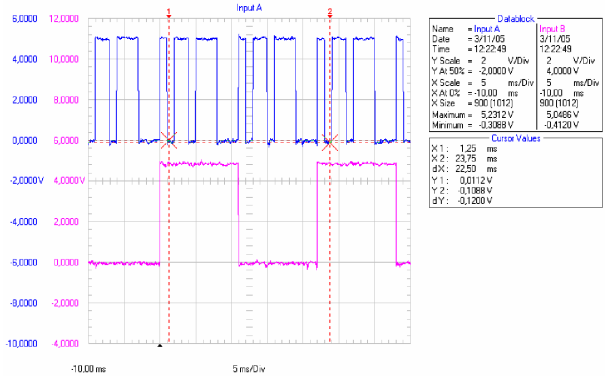

Figura 9. Imagen del código Barker (canal A en color azul) y la señal cuadrada utilizada como datos (canal B en color rosa). Obsérvese que todo el código Barker (10110111000) se repite durante cada bit de datos.

[1] Los resultados no incluyen tablas ya que el documento se extendería más allá de los límites establecidos por el formato. Estos son presentados gráficamente, ya que es una buena alternativa para mostrar las características de las señales en el dominio de la frecuencia.

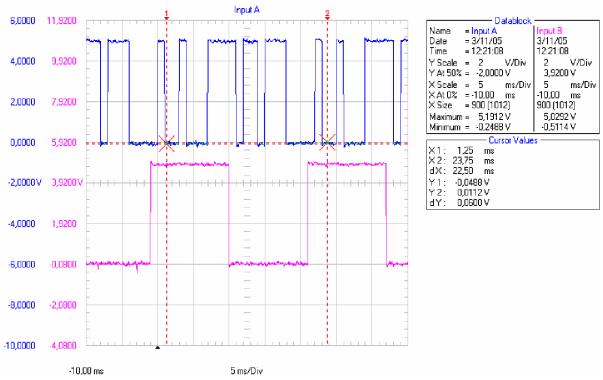

Figura 10. Imagen de la señal Spread Spectrum (canal A en color azul) obtenida realizando la función lógica XOR entre cada bit del código Barker y cada bit de la señal cuadrada utilizada como datos (canal B en color rosa). Se observa que cuando el dato es 0, la señal Spread Spectrum coincide con el código Barker; cuando es 1, obtenemos la negación del código.

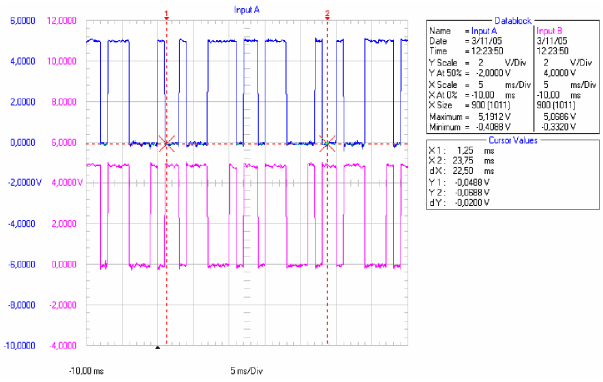

Figura 11. Imagen de la señal en Spread Spectrum obtenida (canal A en color azul) y el código Barker utilizado (canal B en color rosa).

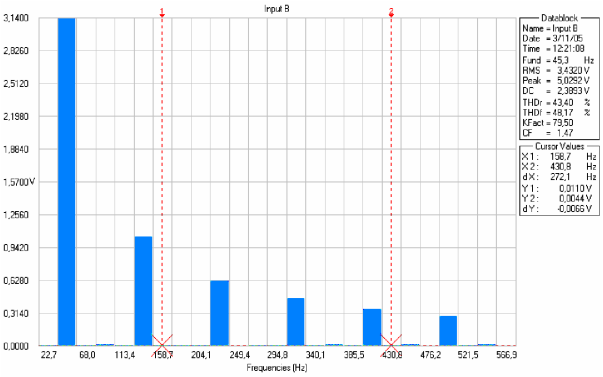

Figura 12. Espectro de la señal cuadrada utilizada como datos. Posee una componente fundamental de gran potencia acompañada de armónicos relativamente menos potentes.

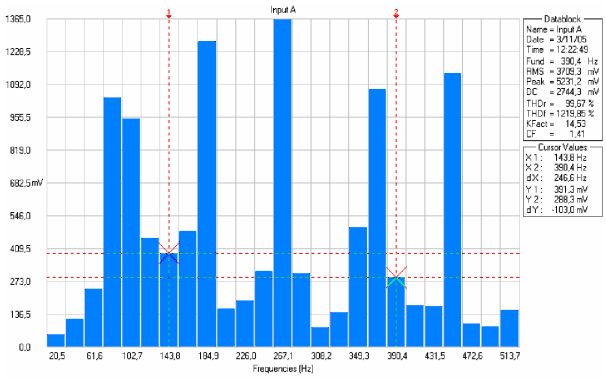

Figura 13. Espectro del código Barker. La gráfica muestra un espectro mucho más amplio con una potencia más distribuida entre los diferentes armónicos, característica propia de las secuencias pseudo aleatorias.

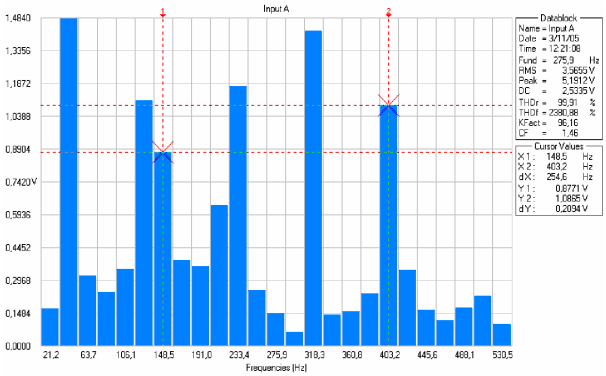

Figura 14. Espectro de la señal en Spread Spectrum obtenida. Los datos han dejado su espectro reducido y potente, a cambio del espectro del código Barker.

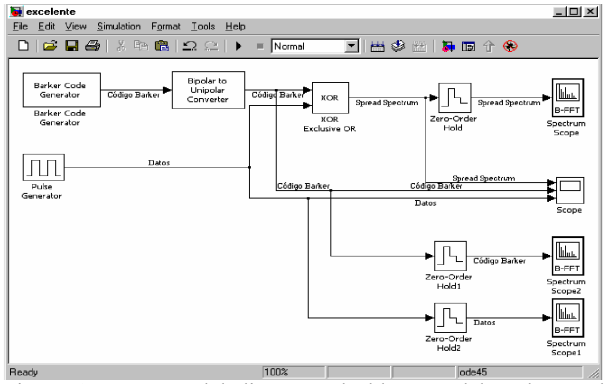

Figura 15. Imagen del diagrama de bloques elaborado en el Simulink de MatLab®, para simular el comportamiento del módulo.

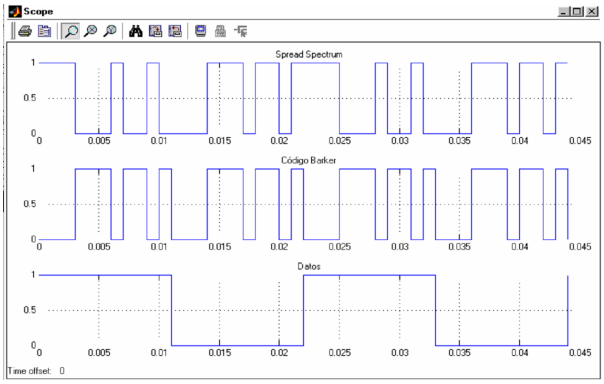

Figura 16. Resultado mostrado por el Scope del Simulink de MatLab®, de la señal en Spread Spectrum, el código Barker y la señal cuadrada utilizada como datos, respectivamente. Compárese con las imágenes 9, 10 y 11, obtenidas en el escopómetro.

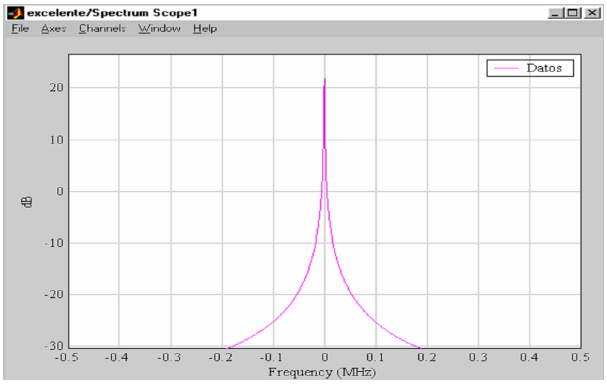

Figura 17. Espectro de la señal cuadrada utilizada como datos, mostrado por el Spectrum Scope del Simulink de MatLab®. Al igual que la imagen obtenida en el Fluke View (ver figura 12), se observa un espectro reducido de alta potencia.

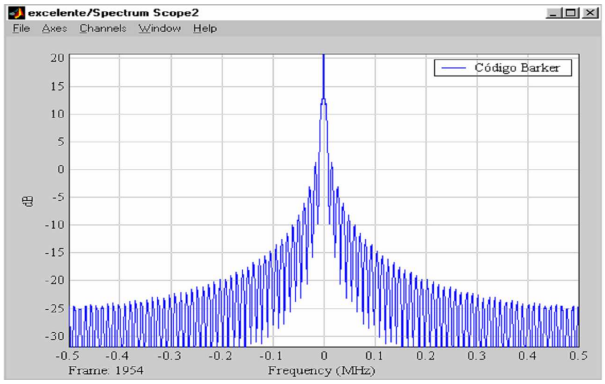

Figura 18. Espectro del código Barker generado, mostrado por el Spectrum Scope del Simulink de MatLab®. Al igual que la imagen obtenida en el software Fluke View (ver figura 13), se observa un espectro más amplio con la potencia distribuida en todos sus armónicos.

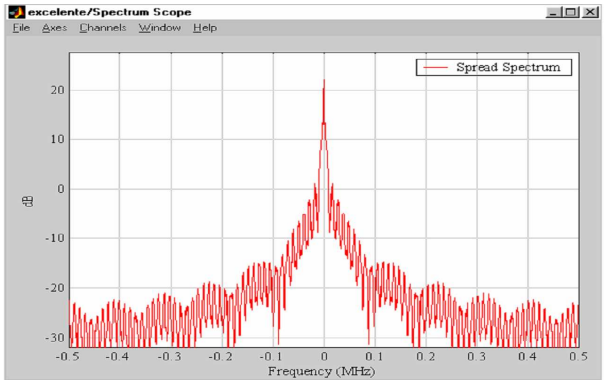

Figura 19. Espectro de la señal en Spread Spectrum obtenida, mostrado por el Spectrum Scope del Simulink de MatLab®. Al igual que la imagen obtenida en el Fluke View (ver figura 14), la señal de datos ha tomado el ancho de banda del código Barker.

6. CONCLUSIONES Y RECOMENDACIONES

El espectro mostrado en la figura 19, permite concluir que los sistemas de comunicación que utilizan Spread Spectrum mejoran significativamente la seguridad en el transporte de los datos, gracias a que estos se "camuflan" con el ruido. Esto es logrado gracias a que el receptor debe conocer a la perfección el código PN del transmisor para poder descifrar el mensaje. Sin embargo, el precio que se debe pagar por esta cualidad es el incremento del ancho de banda de la transmisión, el aumento de la complejidad del sistema debido a la necesidad de un sincronismo perfecto, y el retardo en el procesamiento ocasionado por las diferentes etapas que debe superar la secuencia de datos. Naturalmente, existen aplicaciones como las comunicación militares, donde es necesario pagar este costo a cambio de un transporte seguro de la información. Además, los medios de transmisión que poseen un gran ancho de banda, tales como el aire, permiten que la ineficiente utilización del ancho de banda no sea un problema cuando se trata de transmisiones a baja potencia en un radio limitado. Es por esto que Spread Spectrum es utilizado en accesos de último kilómetro.

7. BIBLIOGRAFÍA

[1] Guoliang Li, *Physical Layer Design for a Spread Spectrum Wireless LAN*, Virginia Polytechnic Institute, USA, 1996.

[2] Ir. J. Meel, *Spread Spectrum Introduction*, Hogeschool Voor Wetenschap & Knust de Nayer Instituuut, Bélgica, 1997.

[3] Simon Haykin, *Digital Communications*, 1◦ Edición, John Wiley & Sons, USA, 1988.

[4] Hwei P. Hsu, *Análisis de Fourier*, Addison-Wesley Iberoamericana, USA, 1973.

[5] *Atmel AT89C51 8 bit Microcontroller data sheet,* Atmel Corporation, 2000.