Análisis de un Esquema Novedoso de Comunicaciones Caóticas con OFDM y su Aplicación en Comunicaciones Seguras

David Luengo García
Departamento de Teoría de la Señal y Comunicaciones
Universidad Carlos III de Madrid
e-mail: luengod@ieee.org

Ignacio Santamaría Caballero
Departamento de Ingeniería de Comunicaciones
Universidad de Cantabria
e-mail: nacho@gtas.dicom.unican.es

***Abstract*— The broadband nature and noise-like appearance of chaotic signals makes them attractive for spread spectrum and secure communications. Although many chaotic communication systems have been proposed, they usually show a poor performance under realistic channel conditions. In this paper, we propose to combine a novel chaotic modulation technique with a conventional OFDM system to provide simultaneously protection against interception and inmunity against channel distortion. The chaotic modulator/demodulator is described, three different chaotic maps are studied, and the tradeoff between performance and security is explored. Computer simulations confirm the good performane of the proposed approach.**

I. Introducción

Las señales y sistemas caóticos han recibido una gran atención en los últimos años. Aunque las señales caóticas son puramente deterministas, presentan característica típicas de señales aleatorias: sensibilidad a las condiciones iniciales, espectro aproximadamente plano y de banda ancha, función de autocorrelación con rápida caída, e impredecibilidad práctica a medio/largo plazo. Además presentan otras propiedades de índole práctica, como su facilidad de generación o su posibilidad de implementación con sistemas de bajo consumo.

Estas características las convierten en atractivas en un amplio rango de aplicaciones en las áreas de procesado de señal y comunicaciones (véase por ejemplo [1]). En este artículo se consideran únicamente mapas lineales a tramos (PWL) unidimensionales. Aunque se trata posiblemente de la clase más sencilla de sistemas caóticos, muestran todas las propiedades fundamentales de los sistemas de mayor orden, y resultan de aplicación práctica en numerosos problemas: generación de secuencias aleatorias en criptografía [2], comunicaciones seguras y de espectro ensanchado [3], "watermarking" [4], etc.

En concreto, dentro del área de las comunicaciones caóticas se han propuesto múltiples técnicas diferentes (véase [3]), aunque todas ellas presentan en general un pobre rendimiento en condiciones realistas del canal. En primer lugar, en este artículo se propone un nuevo esquema de modulación caótica basado en la secuencia simbólica asociada con cualquier señal caótica, y la iteración hacia atrás. En segundo lugar, para mitigar la distorsión causada por el canal se propone combinar esta modulación con un sistema OFDM convencional.

Los dos elementos clave del sistema son la elección de un mapa caótico adecuado para la modulación, y el desarrollo de un detector eficiente y con un buen rendimiento. En relación con el primer problema, se compara el rendimiento para tres mapas diferentes: el mapa de tienda de campaña sesgado unipolar (SK-TM) y bipolar (BSK-TM), y un mapa de desplazamiento de Bernouilli (BSM) con tres intervalos. A partir de los resultados obtenidos se intentan extraer conclusiones generales en relación con el tipo de mapas más adecuados.

Respecto al segundo, aunque se han desarrollado estimadores de máxima verosimilitud (ML) [5] y Bayesianos [6] de la secuencia transmitida, su coste computacional crece exponencialmente con su longitud, y los diferentes algoritmos subóptimos propuestos presentan en general un rendimiento mucho menor (especialmente para valores de relación señal a ruido medios/bajos). En este artículo se propone el uso del algoritmo de Viterbi (VA) como un método eficiente (aunque subóptimo en este caso) de detectar los símbolos transmitidos.

II. Señales Caóticas y Secuencias Simbólicas

En este artículo se consideran únicamente señales generadas por mapas caóticos unidimensionales. Para estos mapas, la muestra n-ésima de la secuencia se obtiene iterando una condición inicial conocida, $x[0]$, de acuerdo con

$$x[n] = f(x[n-1]) = f^2(x[n-2]) = \ldots = f^n(x[0]), \quad (1)$$

donde $f(x)$ es una función no lineal y no invertible adecuada, $f^k(x)$ indica su composición funcional k-ésima, y $1 \leq n \leq N$.

La elección de $f(x)$ va a condicionar en gran medida las propiedades de la señal caótica, y en consecuencia del esquema de modulación propuesto en la Sección III. Aunque todo lo expuesto a continuación resulta válido en general para cualquier mapa caótico, en lo sucesivo se van a utilizar mapas lineales a tramos (PWL), cuya expresión genérica es

$$f(x) = \sum_{i=1}^{M} (a_i x + b_i)\chi_{E_i}(x), \quad (2)$$

donde M es el número de regiones del mapa, a_i es su pendiente en cada intervalo, b_i es el término de "offset", y

$\chi_{E_i}(x)$ es una *función característica* o *indicador*, que marca la pertenencia o no de x a la región i-ésima, E_i:

$$\chi_{E_i}(x) = \begin{cases} 1, & x \in E_i; \\ 0, & x \notin E_i. \end{cases} \tag{3}$$

En este artículo se van a estudiar dos clases de mapas: el *mapa de tienda de campaña sesgado* (tanto el unipolar, SK-TM, como el bipolar, BSK-TM) y un *mapa de desplazamiendo de Bernouilli* (BSM) con tres intervalos. Los valores de E_i, a_i y b_i para cada uno de estos tres mapas se muestran en la Tabla I, en función de p, que es un parámetro que controla la anchura de cada intervalo (y por lo tanto su pendiente).

Aunque los mapas PWL no son invertibles, están compuestos por M regiones dentro de las que $f(x)$ es lineal. En consecuencia, se pueden definir M funciones inversas. Para ello se va a definir la *secuencia simbólica* o *itinerario* asociado a una señal caótica como la secuencia de regiones del mapa que visita a lo largo de su evolución temporal,

$$s[n] = i \Leftrightarrow x[n] \in E_i, \qquad n = 0,\ \ldots,\ N; \tag{4}$$

con $0 \leq n \leq N$, y $1 \leq i \leq M$. Para los mapas PWL se puede demostrar que cada punto dentro del rango del mapa ([0,1] para el SK-TM, y [-1,1] para el BSK-TM y BSM) tiene asociado un único itinerario de longitud N, y que un itinerario de longitud infinita define una sola condición inicial [7].

De este modo, se pueden generar las señales caóticas sin ninguna ambigüedad iterando hacia atrás a partir de una condición final conocida, $x[N]$, en lugar de hacia delante:

$$x[n] = f^{-1}_{s[n]}(x[n+1]) = \ldots = f^{-(N-n)}_{s[n],\ \ldots,\ s[N-1]}(x[N]). \tag{5}$$

Donde $f_s^{-1}(x)$ indica el mapa inverso, cuya expresión es

$$f_s^{-1}(x) = \frac{x - b_s}{a_s}, \tag{6}$$

siendo $s \in \{1,\ \ldots,\ M\}$ el intervalo del mapa al que debe pertenecer la muestra generada. Esta manera de construir la señal caótica evita los problemas numéricos característicos de la iteración hacia delante (amplificación del error y pérdida de precisión), y sugiere el modulador/demodulador propuesto en la Sección III.

	E_i	a_i	b_i
SK-TM	$E_1 = [0, p)$	$a_1 = \frac{1}{p}$	$b_1 = 0$
	$E_2 = [p, 1]$	$a_2 = -\frac{1}{1-p}$	$b_2 = \frac{1}{1-p}$
BSK-TM	$E_1 = [-1, p)$	$a_1 = \frac{2}{1+p}$	$b_1 = \frac{1-p}{1+p}$
	$E_2 = [p, 1]$	$a_2 = -\frac{2}{1-p}$	$b_2 = \frac{1+p}{1-p}$
BSM	$E_1 = [-1, -p]$	$a_1 = \frac{2}{1-p}$	$b_1 = \frac{1+p}{1-p}$
	$E_2 = (-p, p)$	$a_2 = \frac{1}{p}$	$b_2 = 0$
	$E_3 = [p, 1]$	$a_3 = \frac{2}{1-p}$	$b_3 = -\frac{1+p}{1-p}$

TABLE I

PARÁMETROS DE LOS TRES MAPAS CAÓTICOS CONSIDERADOS.

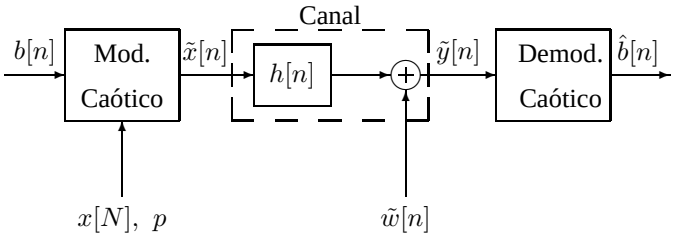

Fig. 1. Sistema de comunicaciones caóticas genérico.

III. MODULADOR CAÓTICO PARA CANAL GAUSSIANO

III-A. Estructura del Modulador Caótico

La estructura general del sistema de comunicaciones caóticas completo se muestra en la Figura 1. La idea básica del modulador caótico propuesto consiste en generar la señal caótica iterando hacia atrás a partir de una condición final conocida, $x[N]$, usando la secuencia de bits que se desean transmitir, $\mathbf{b} = [b[1],\ \ldots,\ b[N]]^T$, para construir la secuencia simbólica.

En el caso del SK-TM y BSK-TM la muestra n-ésima del itinerario es $\tilde{s}[n] = s[N-n] = 1 + b[n]$, mientras que para el BSM, $\tilde{s}[n] = s[N-n] = 1 + 2b[n]$. Nótese que en este último caso las señales generadas van a pertenecer únicamente a las dos regiones externas, E_1 y E_3, permaneciendo la región interna, E_2, como un intervalo de guarda utilizado para garantizar una separación mínima entre las formas de onda asociadas a un cero y un uno.

Este itinerario se utiliza para obtener la señal caótica en banda base iterando hacia atrás de acuerdo con (5),

$$\tilde{x}[n] = x[N-n] = f^{-1}_{\tilde{s}[n]}(\tilde{x}[n-1]), \tag{7}$$

para $n = 1,\ \ldots,\ N$. Esta señal se puede transportar posteriormente a cualquier frecuencia deseada para la transmisión paso banda. La Figura 2 muestra la estructura del modulador en banda base, mientras que la Figura 3 muestra ejemplos de secuencias obtenidas para los diferentes mapas estudiados.

III-B. Demodulación de Máxima Verosimilitud

Para un canal aditivo blanco Gaussiano $h[n] = \delta[n]$, y la señal recibida es simplemente

$$\tilde{y}[n] = \tilde{x}[n] + \tilde{w}[n], \tag{8}$$

siendo $\tilde{w}[n]$ AWGN con varianza σ^2. Dada la independencia de las muestras de ruido, resulta obvio que la secuencia

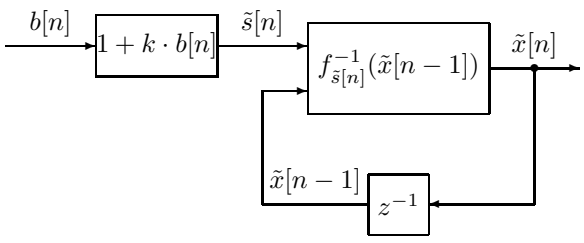

Fig. 2. Diagrama de bloques del modulador caótico propuesto.

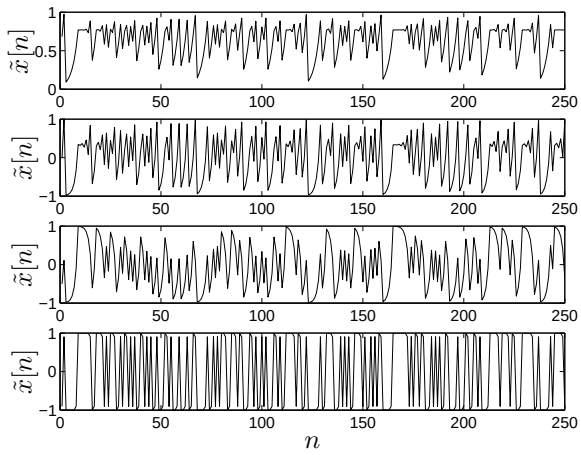

Fig. 3. Ejemplos de secuencias caóticas típicas: SK-TM con $p = 0{,}7$, BSK-TM con $p = 0$, BSM con $p = 0{,}1$ y BSM con $p = 0{,}9$.

recibida, $\mathbf{y} = [\tilde{y}[1],\ \ldots,\ \tilde{y}[N]]^T$, tiene una FDP Gaussiana con media $\mathbf{x} = [\tilde{x}[1],\ \ldots,\ \tilde{x}[N]]^T$ y varianza $\mathbf{C}_y = \sigma^2\mathbf{I}$.

En estas circunstancias, el estimador ML de la secuencia de bits transmitidos, que es el que proporciona la menor probabilidad de error, se puede obtener minimizando la siguiente función de coste cuadrática en $\mathbf{x}$,

$$J(\mathbf{y};\mathbf{b}) = (\mathbf{y}-\mathbf{x})^T(\mathbf{y}-\mathbf{x}), \tag{9}$$

donde $\mathbf{x}$ presenta una dependencia con $\mathbf{b}$ a través de la secuencia simbólica, como se ha visto en la Sección III-A.

Desafortunadamente, la estima ML de $\mathbf{b}$ no se puede encontrar derivando (9) e igualando a cero, ya que $J(\mathbf{y};\mathbf{b})$ es una función discontinua de $\mathbf{b}$. No obstante, dado que el número de itinerarios posibles es finito, 2^N, se puede proceder probando todos ellos y seleccionando el mejor. Esta es la solución adoptada en [5], y en general es la única que garantiza que el estimador obtenido es el ML para un mapa PWL genérico. Aunque esta solución proporciona muy buenos resultados, requiere un coste computacional que crece exponencialmente con la longitud de la secuencia, de modo que resulta imposible su aplicación para valores de N medios/altos.

III-C. Demodulación Eficiente con el Algoritmo de Viterbi

El algoritmo de Viterbi (VA) encuentra el camino más corto a través de un "trellis". Por lo tanto, para poder aplicar el VA en primer lugar es necesario construir un "trellis" de la señal caótica recibida. Resulta evidente que para una secuencia de longitud N es posible construir un "trellis" que represente de manera exacta la evolución de la señal caótica usando su itinerario para definir los estados. Sin embargo, un mapa caótico puede verse como un filtro de respuesta infinita al impulso (IIR) no lineal, de modo que su representación exacta requiere 2^N estados. En consecuencia, el VA exacto requiere un coste computacional similar al del algoritmo de fuerza bruta mostrado en la Sección III-B.

Como alternativa computacionalmente eficiente, se propone el uso del algoritmo de Viterbi con sólo dos estados: uno por cada intervalo utilizado del mapa. El lazo básico del "trellis" se muestra en la Figura 4. Para un mapa PWL genérico, el coste de la rama j-ésima, $j \in \{1,2\}$, que parte del estado i-ésimo, $i \in \{1,2\}$, en el instante n-ésimo es

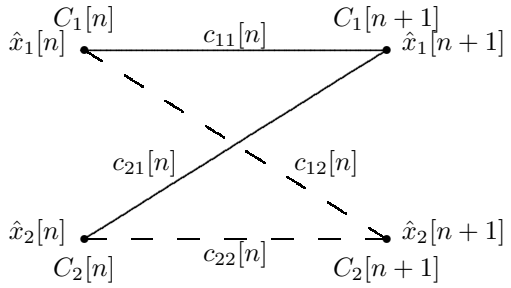

Fig. 4. Lazo básico para el "trellis" con sólo dos estados.

$$c_{ij}[n] = |\tilde{y}[n+1] - (\hat{x}_i[N] - b_j)/a_j|, \tag{10}$$

donde $\hat{x}_i[n]$ es la muestra obtenida iterando hacia atrás $N-n$ veces a partir de $x[N]$ utilizando la mejor secuencia que termina en el nodo i-ésimo. El coste de cada nodo en una cierta iteración se obtiene minimizando el coste de todos los posibles caminos que llegan a él desde la iteración anterior:

$$C_i[n+1] = \min_{j=1,2}\{C_j[n] + c_{ji}[n]\}. \tag{11}$$

Obviamente este es un algoritmo subóptimo. No obstante, su rendimiento es muy cercano al óptimo (como se muestra en la Sección III-D) debido a la rápida caída de la función de autocorrelación típica de los mapas caóticos: la señal caótica olvida rápidamente su pasado, y las muestras lejanas apenas influyen en la estima del itinerario actual [8].

III-D. Resultados para el Canal Gaussiano

En esta Sección se va a analizar el rendimiento del esquema de modulación caótica propuesto para canales Gaussianos. Se van a considerar secuencias cortas, con $N = 8$, para poder comparar el rendimiento del estimador ML real y el del VA con un número reducido de estados.

En la Figura 5 se muestran los resultados para el SK-TM con $p = 0{,}5$ y el BSM con $p = 0{,}1$. Mientras que el rendimiento del BSM se halla muy cercano al de una señal BPSK, acercándose cada vez más conforme p aumenta [8], el del BSM es mucho peor. No obstante, su probabilidad de error se puede disminuir en gran medida realizando un sencillo proceso de codificación consistente en mapear secuencias de entrada de k bits en aquellas 2^k secuencias de longitud n (precalculadas) con una mayor distancia a la frontera de las regiones asociadas al cero y al uno (en este caso $x = 0{,}5$).

No obstante, el peor rendimiento del SK-TM se ve compensado por un aumento en la protección frente a intercepción proporcionada. En la Figura 6 se muestra la probabilidad de error del BSK-TM frente al BSM. En el modulador las señales se han generado con $p = 0$, y en el demodulador se supone que un usuario no intencionado comete un error y estima $p = 0{,}05$. Mientras que el BSM no muestra protección alguna (esto es, ese pequeño error no afecta a la probabilidad de error) para el SK-TM los resultados son catastróficos.

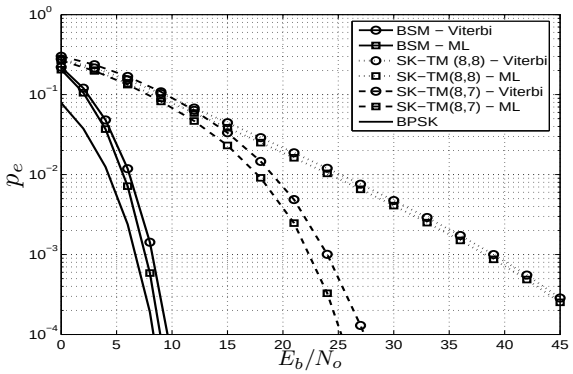

Fig. 5. Probabilidad de error para el SK-TM y BSM con el canal Gaussiano.

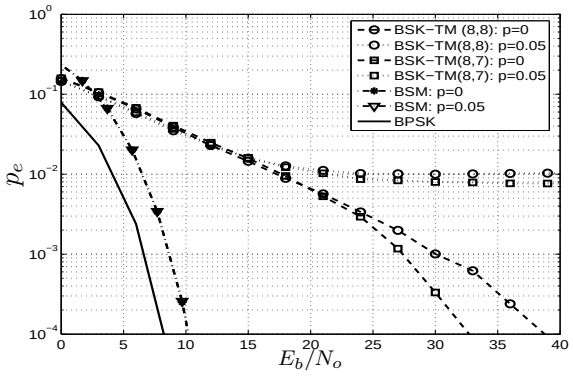

Fig. 6. Comparación de la protección frente a intercepción del BSK-TM y el BSM con el canal Gaussiano.

IV. Sistema OFDM con Modulación Caótica para Canales no Gaussianos

El esquema de comunicaciones caóticas propuesto presenta un buen rendimiento para un canal Gaussiano, pero puede sufrir una gran degradación para otros canales. En lugar de intentar diseñar un igualador para estos casos, en este artículo se propone combinar la modulación caótica con un esquema robusto frente a la distorsión introducida por el canal: OFDM.

En el sistema propuesto los bits de entrada se codifican usando el modulador caótico de la Figura 2, y a continuación estas señales caóticas se usan para generar la señal transmitida usando un modulador OFDM convencional: se realiza una conversión serie a paralelo de la secuencia de información, se insertan pilotos y símbolos de guarda (ceros), se realiza una IFFT, se inserta un prefijo cíclico, y se transmite la señal por el canal. En el receptor se realizan las operaciones inversas: se elimina el prefijo cíclico, se realiza una FFT, se estima el canal y se iguala en el dominio frecuencial, y se estiman los bits transmitidos mediante el VA.

El rendimiento de este esquema se ha probado utilizando los parámetros básicos del estándar HIPERLAN 2: 64 portadoras divididas en 48 de datos, 4 pilotos y 12 símbolos de guarda. Los resultados para el BSM se muestran en la Figura 7, apreciándose únicamente una ligera distorsión con respecto al canal Gaussiano similar a la del esquema OFDM+BPSK.

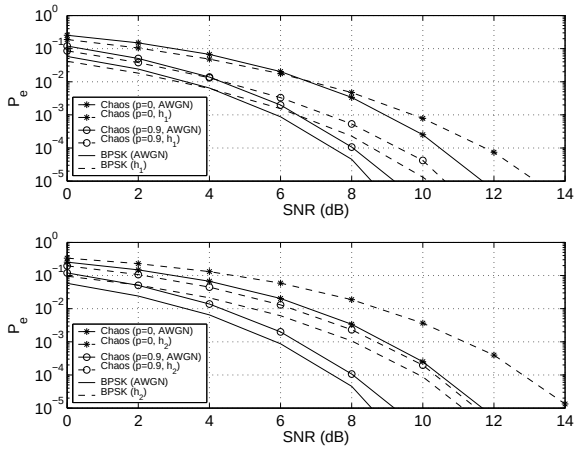

Fig. 7. Probabilidad de error para el Sistema OFDM+BSM con canales no Gaussianos.

V. Conclusiones

En este artículo se ha propuesto un esquema novedoso de comunicaciones caóticas basado en la dinámica simbólica y la iteración hacia atrás. Los elementos clave del sistema son la elección del mapa caótico (parece existir una relación inversa entre rendimiento y protección frente a intercepción), y la implementación eficiente del demodulador (lograda mediante el algoritmo de Viterbi). Para canales no Gaussianos se ha propuesto combinar la modulación caótica con OFDM para proporcionar cierta inmunidad frente a la distorsión del canal. Como líneas futuras destacan la búsqueda de un mapa que ofrezca un compromiso adecuado entre prestaciones y seguridad, el estudio de mapas con más de dos intervalos, y el desarrollo de estrategias de "bit loading" para los mismos.

Agradecimientos

Este trabajo ha sido financiado en parte por el Ministerio de Ciencia y Tecnología (MCYT) gracias al proyecto TIC2004-06451-C05-02.

References

[1] *Special Issue on Applications of Nonlinear Dynamics to Electronic and Information Engineering*, vol. 90, Proceedings of the IEEE, May 2002.

[2] Y. Hwang and H. C. Papadopoulos, "Physical-layer secrecy in AWGN via a class of chaotic DS/SS systems: Analysis and design," *IEEE Trans. on Signal Processing*, vol. 52, no. 9, pp. 2637–2649, Sep. 2004.

[3] F. C. M. Lau and C. K. Tse, *Chaos-Based Digital Communication Systems*, Springer-Verlag, Berlin, 2003.

[4] A. Tefas, A. Nikolaidis, N. Nikolaidis, V. Solachidis, S. Tsekeridou, and I. Pitas, "Performance analysis of correlation-based watermarking schemes employing Markov chaotic sequences," *IEEE Trans. on Signal Processing*, vol. 51, no. 7, pp. 1979–1994, Jul. 2003.

[5] C. Pantaleón, D. Luengo, and I. Santamaría, "Optimal estimation of chaotic signals generated by piecewise-linear maps," *IEEE Signal Processing Letters*, vol. 7, no. 8, pp. 235–237, Aug. 2000.

[6] C. Pantaleón, L. Vielva, D. Luengo, and I. Santamaría, "Bayesian estimation of chaotic signals generated by piecewise-linear maps," *Signal Processing*, vol. 83, pp. 659–664, Mar. 2003.

[7] R. L. Devaney, *An Introduction to Chaotic Dynamical Systems*, Perseus Books, Reading, MA (USA), 1989.

[8] D. Luengo and I. Santamaría, "Secure communications using OFDM with chaotic modulation in the subcarriers," in *Proc. IEEE 61st Semiannual Vehicular Technology Conference (VTC2005-Spring)*, Stockholm (Sweden), May 30 - Jun. 1 2005, Aceptado para su presentación.